READ THE DOCS

ForensicVM

MESI ESTIG BEJA PT

Autopsy ForensicVM Client Plugin

IPBeja
Instituto Politécnico de Beja
ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO - ESTIG

Eng. Nuno Mourinho, Eng. Mário Candeias and Dr. Rogério Bravo

USER MANUAL

https://forensicvm-autopsy-plugin-user-manual.readthedocs.io/

DOI 10.5281/ZENODO.8274586

FORENSICVM PLUGIN MANUAL

Fig. 1: Forensic VM logo

ForensicVM is a comprehensive project designed to assist forensic investigators in the virtualization of forensic images. By utilizing advanced technologies and tools, ForensicVM simplifies the process of analyzing and examining digital evidence in a virtualized environment.

The project consists of two essential components: the ForensicVM client, which is an Autopsy plugin, and the ForensicVM server. These components work seamlessly together to provide a powerful and efficient forensic virtualization solution.

The ForensicVM server, developed using Django and Python, serves as the backbone of the system. It is recommended to install the server on Debian 11, which in turn should be set up on a dedicated bare metal server. This configuration ensures optimal performance and stability for your forensic investigations.

Please note that installing the ForensicVM server on a hypervisor is not recommended. The ForensicVM server itself acts as the hypervisor, and running it within a nested setup may result in unpredictable behavior and performance issues. To maintain the integrity and reliability of your forensic analysis, it is advised to adhere to the recommended server installation setup.

To get started with ForensicVM, your first step is to install the server. For detailed instructions, please refer to the installation section, where you will find step-by-step guidance on setting up the server environment correctly.

Once the server is up and running, you can explore the various capabilities and features of ForensicVM by diving into the usage section. This section provides comprehensive information on how to make the most out of the project, including tips, best practices, and real-world scenarios.

Additionally, if you require a deeper understanding of the technical aspects and functionalities of ForensicVM, check in the addional tForensicVM server in api section. It offers an in-depth exploration of the project's application programming interface, empowering advanced users to leverage the full potential of the platform.

I would like to emphasize that ForensicVM is an actively developed project. I'm continuously working on enhancing its capabilities, improving performance, and adding new features. Stay tuned for updates and exciting developments as I strive to deliver the most effective and reliable forensic virtualization solution available.

Thank you for choosing ForensicVM. I am confident that it will greatly streamline your forensic investigations and contribute to the success of your work. The first step is to install the server. Head to installation

Check out the usage section for further information, including how to install the project.

CHAPTER

ONE

INTRODUCTION

1.1 Purpose of ForensicVM

ForensicVM is an innovative tool designed to streamline the process of digital forensics. By leveraging advanced virtualization technology, ForensicVM allows for the secure and efficient analysis of forensic images, making it an invaluable tool for cybersecurity professionals, digital forensics investigators, and information security teams.

1.2 Overview of Features

ForensicVM offers a range of features designed to enhance the forensic analysis process:

- **Virtualization of** Forensic Images: ForensicVM enables the creation and management of virtualized instances of forensic images, paving the way for a more flexible and scalable analysis process. This virtualization can be executed either through a snapshot linked to the investigator's storage for quick selection or by full conversion, which transfers and converts the image to a remote server to maximize the VM's performance and features.
- **Forensic Image Lifecycle Management**: ForensicVM equips users with tools for managing every step of a forensic image's lifecycle, from creation to decommissioning. Convert the forensic image into a VM, start, stop, reset, snapshot, and safely delete the forensic image when it is no longer required.
- **Advanced Analysis Tools**: Equipped with a suite of powerful analysis tools, ForensicVM assists investigators in uncovering vital evidence.
- **Integrated** Hypervisor: The ForensicVM Server features a robust hypervisor based on QEMU and KVM to guarantee efficient execution and management of virtual machines.
- **Collaboration**: ForensicVM employs a web development strategy that fosters remote and secure collaboration among forensic investigators. This method enables team members, regardless of their location, to work simultaneously on investigations in a digital space, enhancing productivity and communication. It leverages advanced encryption and security protocols to ensure that all collaborative efforts remain secure and confidential, protecting the integrity of investigations. In essence, ForensicVM's approach melds convenience, connectivity, and security, revolutionizing the way forensic investigations are conducted.
- **Plugin Architecture**: Plugins applied to the forensic virtual machine enable security bypassing, like creating new admins, resetting Windows activation, patching accessibility, and also allow the community to develop custom solutions that interact with ForensicVM.
- **Evidence Disk**: An additional disk is automatically created with all tags from Autopsy Software, enabling easy and practical gathering and importing of evidence back to Autopsy.
- **Optional** Network Card: It is disabled by default but when activated, this network card records all network traffic on the server while protecting local networking from potential attacks with pre-installed firewall rules. It also records traffic in Wireshark PCAP format.

- **On-the-Fly** Memory Dumps: Capability to create volatility memory dumps at any moment.
- **Integrated Screenshots**: Removes the need for an extra screenshot program.
- **Integrated Video Recording**: Ability to record individual videos with a maximum duration of three hours, providing additional evidence if required.
- **Media Management**: ISO management allows investigators to use their own tools during the investigation.
- **Snapshot Management**: Freeze the VM in time and recall a previous state to perform "what if" tests.
- **Fine-tuning**: Adjust machine memory size and set the VM start date as needed.

Warning: The network card is currently a work in progress. Under certain circumstances, the firewall rules may fail, potentially exposing your network to malicious actors. Please note that although the network safeguards your internal system, your external IP may still be visible if a C2C client is installed. Proceed with caution.

Important: Video recording is also still under development. Currently, the recordings lack audio. This limitation is expected to be addressed in future updates.

1.3 Use Cases

ForensicVM can be used in a variety of scenarios, including but not limited to:

- **Cybersecurity Investigations**: In the world of ever-evolving cyber threats, ForensicVM can be employed by investigators to thoroughly analyze cyberattacks. It allows experts to delve into the intricate details of these attacks, discover the tactics, techniques, and procedures (TTPs) deployed by adversaries, and thereby contribute to the broader understanding of emerging cyber threats.
- **Incident Response**: ForensicVM plays a pivotal role in the incident response process, helping to mitigate the impact of security incidents. In the aftermath of a security breach, it can quickly analyze the affected system, extracting crucial data that aids in understanding the extent of the compromise. This swift and thorough analysis can contribute to expedited recovery processes, aid in damage control, and provide insights for strengthening defenses to thwart future incidents.
- **Training and Education**: ForensicVM is an invaluable tool for training budding cybersecurity professionals. It offers a safe and controlled environment for trainees to learn and practice forensic analysis. Facilitating hands-on experience enables learners to understand the nuances of digital forensics, teaching them to uncover and interpret the digital evidence left behind after cyber incidents. In academic settings, ForensicVM can be integrated into cybersecurity curricula, ensuring that the future generation of cyber defenders is well-versed in the practical aspects of forensic analysis.
- **Legal Investigations**: ForensicVM can also be used in legal investigations where digital evidence plays a crucial role. Law enforcement agencies can use this tool to process and analyze digital evidence, which can provide vital leads in criminal investigations.
- **Corporate Audits and Investigations**: Organizations can utilize ForensicVM in their internal audits and investigations. This tool can assist in identifying suspicious activities or misconduct, ensuring the organization's policies and regulations are being adhered to, and maintaining a secure and compliant work environment.

CHAPTER

TWO

CITATION GUIDELINES

We greatly appreciate the academic and scientific community for recognizing and using this work. Citing us not only shows respect for our efforts but also makes it easy to trace the genealogy of scientific thought. Thus, if you find this work beneficial or you use parts of it in your own research, projects, or products, we kindly ask you to properly reference it.

2.1 Here's How You Can Cite Us

We offer two main contributions: our **Forensic VM Autopsy User Manual** and the **Autopsy ForensicVM Client Plugin Software** software. Below are their BibTeX entries for your convenience.

Autopsy ForensicVM Client Plugin Software

```
@software{Mourinho_AutopsyForensicVM_2023,
author = {Mourinho, Nuno},
doi = {10.5281/zenodo.8153316},
month = {07},
title = {{Autopsy ForensicVM Client}},
url = {https://github.com/nunomourinho/AutopsyForensicVM},
year = {2023}
}
```

Forensic VM Autopsy User Manual

```
@misc{Mourinho_forensicVmAutopsyUserManual_2023,
doi = {10.5281/ZENODO.8274587},
url = {https://zenodo.org/record/8274587},
author = {Mourinho, Nuno},
language = {en},
title = {nunomourinho/forensicVmAutopsyUserManual: v1.0.0},
publisher = {Zenodo},
year = {2023},
copyright = {European Union Public License 1.2}
}
```

CHAPTER

THREE

REQUIREMENTS

To ensure that ForensicVM runs smoothly on your system, your computer and your server should meet or exceed the following requirements.

3.1 Computer Requirements to use the Autopsy Plugin

To ensure that ForensicVM runs smoothly on your system, your computer and your server should meet or exceed the following requirements.

3.1.1 Computer Requirements

3.1.2 Operating System

ForensicVM was tested and supports the following operating systems:

- Windows 10 or later
- Autopsy 4.20 or later

3.1.3 Processor

- A 64-bit multi-core processor is recommended for optimal performance.

3.1.4 Memory

- A minimum of 16 GB RAM is required. From the oficial autopsy documentation website: “We recommend a minimum of 16GB of RAM. By default, Autopsy will use a maximum of 4GB of RAM (not including memory that the Solr text indexing server uses).”

3.1.5 Storage

- A minimum of 300 mb of free disk space is needed for the ForensicVM plugin installation.
- Additional storage will be required for forensic images. The amount will depend on the size of the images you will be working with.
- The use of Nvme or SSD is not strictly necessary but recommend as it speeds up the aquisition processes.

3.1.6 Networking

- A network connection is required for software updates and to access cloud-stored forensic images. Additionally, a robust internet connection with high upload speeds is necessary to expedite the virtualization process if there is a need to convert forensic images into forensic VMs.

3.1.7 Display

- A display with a resolution of 1980x1080 or higher is recommended for the best experience. If possible use a two monitor setup; one for the Autopsy plugin, and the other for forensicVM server control.

3.1.8 Software Dependencies

- Install Autopsy 4.20 or higher

3.1.9 Additional Notes

Important: ForensicVM plugin requires administrator or root privileges for installation and running certain high-privilege operations like creating readonly windows shares!

To ensure that ForensicVM operates efficiently on your system, our server must meet or exceed the following requirements:

3.2 Server Requirements

3.2.1 Operating System

ForensicVM has been tested and supports the following operating systems:

- Debian 11 (Bullseye)

3.2.2 Processor

- A 64-bit multi-core processor is recommended for optimal performance. This will facilitate smoother operation, particularly when managing complex tasks.

3.2.3 Memory

- A minimum of 16 GB RAM is required. However, 16 GB or more is recommended to handle the simultaneous virtualization of forensic images. This ensures that multiple tasks can be performed concurrently without a loss in performance.

3.2.4 Storage

- A minimum of 2 GB of free disk space is needed for the ForensicVM installation itself.
- Additional storage will be required for forensic images. The amount will depend on the size of the images you will be working with. At least 1 TB of disk space, configured in RAID 10, is recommended.
- The use of NVMe or SSD is not strictly necessary but is recommended, as it can significantly speed up the virtualization process.

Important: Remember to account for the extra space needed for virtual ISO CD-ROM or DVD with your own tools. These might require additional storage depending on your specific requirements.

3.2.5 Networking

- A network connection is necessary, with at least a gigabit connection recommended. The conversion of forensic images to a virtual machine, the downloading of Wireshark files, videos, or evidence disks all exert significant pressure on the network. Therefore, utilizing a reliable internet service hosting with robust upload and download rates is crucial.

3.2.6 Display

- No specific display requirements exist for the server. You only need SSH access or HP ILO or similar for server administration.

3.2.7 Software Dependencies

- The installation will handle dependencies automatically. A dedicated server with Debian Bullseye as bare metal is necessary. Dedicated hardware with virtualization support is essential. The installation will create a new forensic hypervisor server based on QEMU.

3.2.8 Additional Notes

Important: ForensicVM requires root privileges for installation and to execute specific high-privilege operations, such as converting forensic images to virtual machines, managing the ForensicVM lifecycle, and controlling various security and administrative functions within the system. These elevated permissions are essential in allowing the software to interact with core system components, manipulate disk images securely, and handle complex virtualization tasks.

CHAPTER

FOUR

INSTALLATION AND SETUP

This section will guide you through the steps necessary to install and set up ForensicVM on your system.

4.1 AutopsyVM Client Plugin Installation

4.1.1 Introduction

The AutopsyVM client plugin is a valuable addition to Autopsy, enhancing its functionality for digital forensics. Follow the steps below to install the plugin.

4.1.2 Step 1: Download ForensicVM.exe Setup File

Download the latest version of the ForensicVM.exe setup file from the [AutopsyForensicVM GitHub Releases](https://github.com/nunomourinho/AutopsyForensicVM/releases) page. Navigate to the "Assets" section and download the setup file.

4.1.3 Step 2: Run the ForensicVM.exe Setup

Run the ForensicVM.exe setup file to begin the installation process. The setup consists of four steps:

1. Welcome Screen: Displays an introduction to the installation process.
2. Component Installation: Proceed with the default settings. Do not make any changes.
3. Plugin Location: Specify the location where the AutopsyVM client plugin will be installed. Typically, this does not require any changes.
4. Install: Click the "Install" button to start the installation process.

4.1.4 Step 3: Complete the Installation

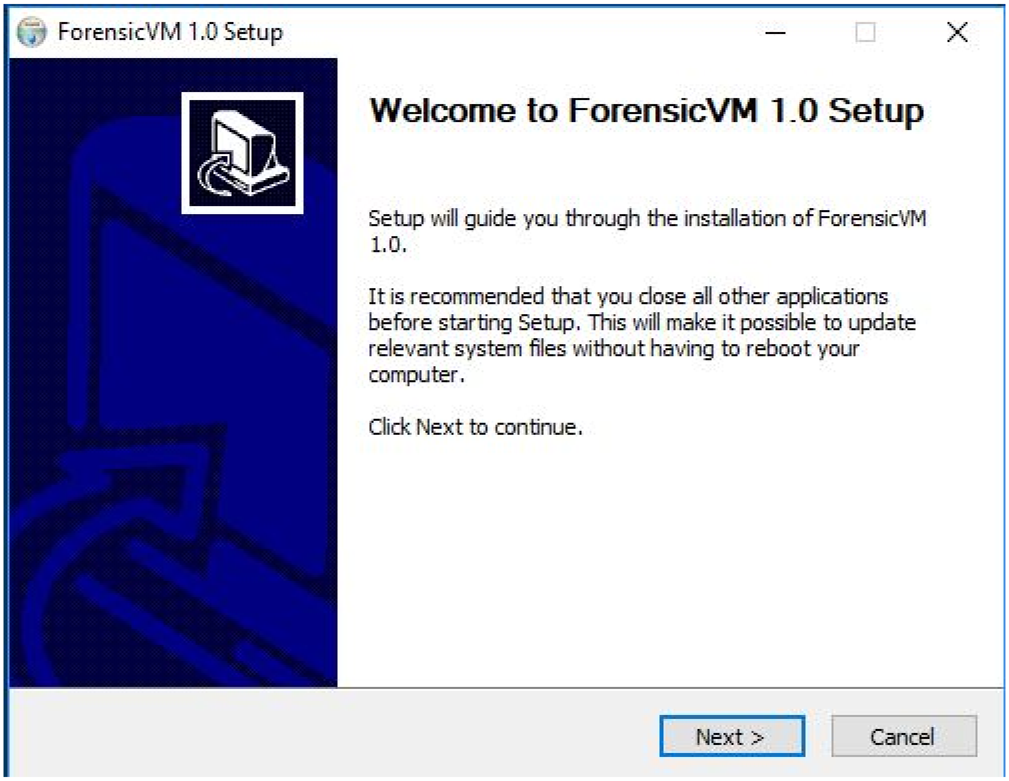
Follow the on-screen instructions to complete the installation. Once the installation is finished, you can proceed with using the AutopsyVM client plugin in Autopsy.

4.1.5 Step 4: Verify the Installation

To verify the successful installation of the AutopsyVM client plugin, open Autopsy and check if the plugin is available and functional.

4.1.6 Screenshots

Here are the screenshots that illustrate the installation process:



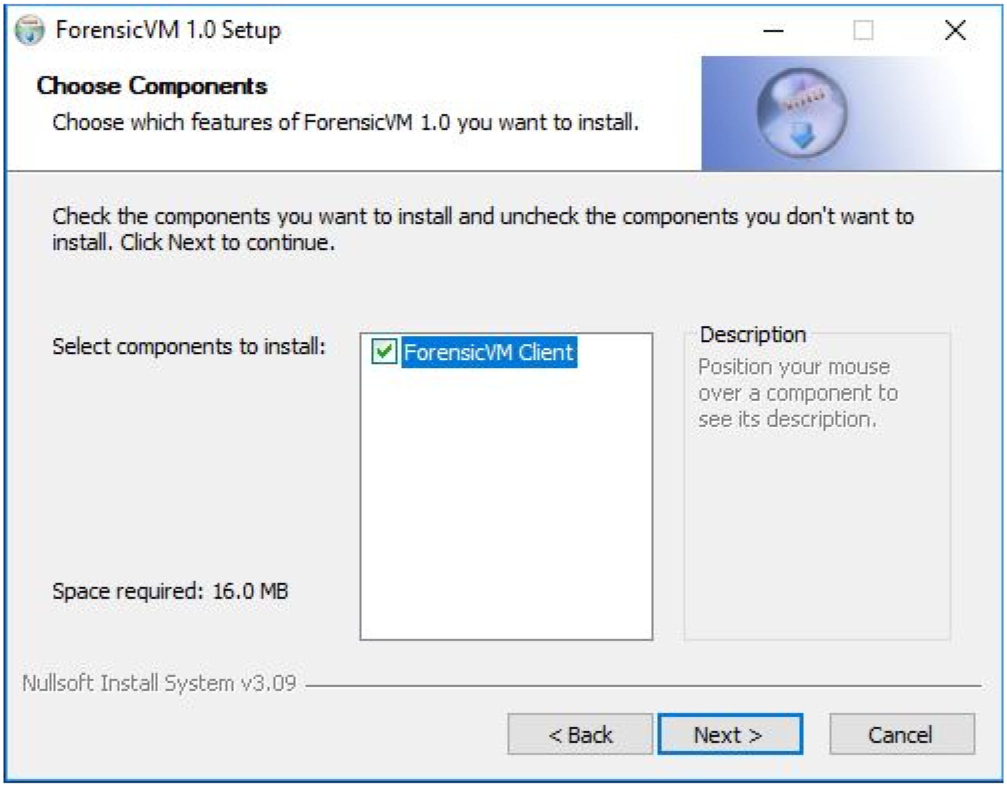
Welcome to ForensicVM 1.0 Setup

Setup will guide you through the installation of ForensicVM 1.0.

It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer.

Click Next to continue.

Fig. 4.1: Welcome Screen



ForensicVM 1.0 Setup

Choose Components

Choose which features of ForensicVM 1.0 you want to install.

Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.

Select components to install: ☑ ForensicVM Client

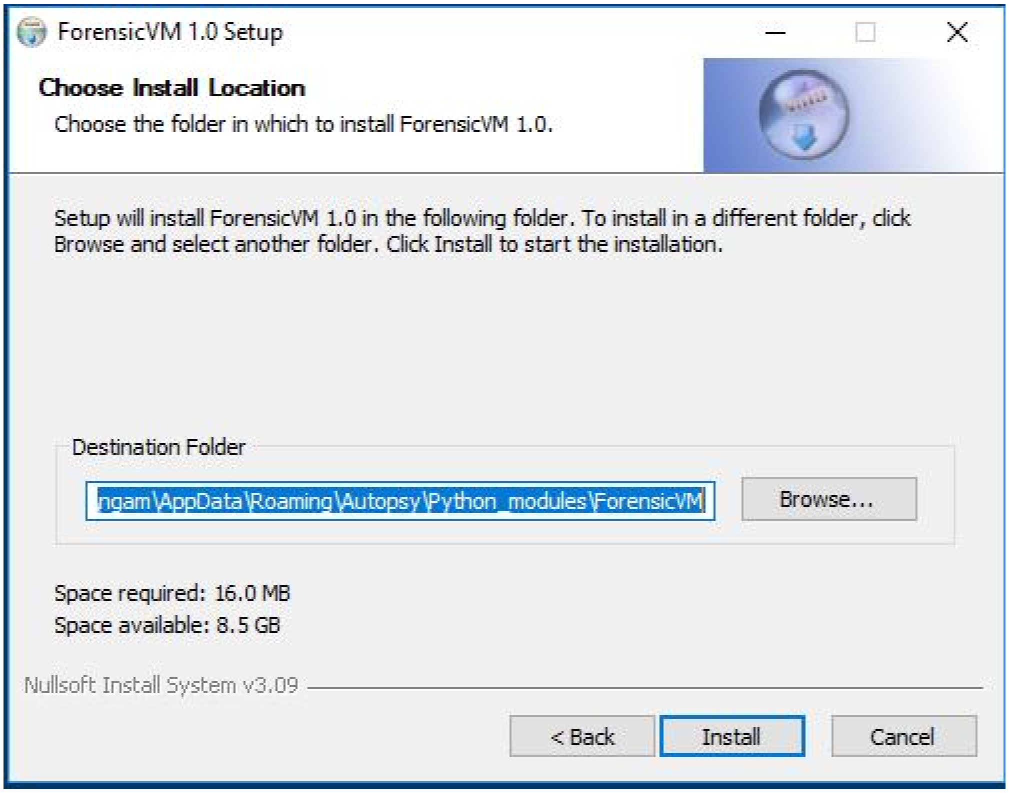
Description

Position your mouse over a component to see its description.

Space required: 16.0 MB

Nullsoft Install System v3.09

Fig. 4.2: Component Installation



ForensicVM 1.0 Setup

Choose Install Location

Choose the folder in which to install ForensicVM 1.0.

Setup will install ForensicVM 1.0 in the following folder. To install in a different folder, click Browse and select another folder. Click Install to start the installation.

Destination Folder

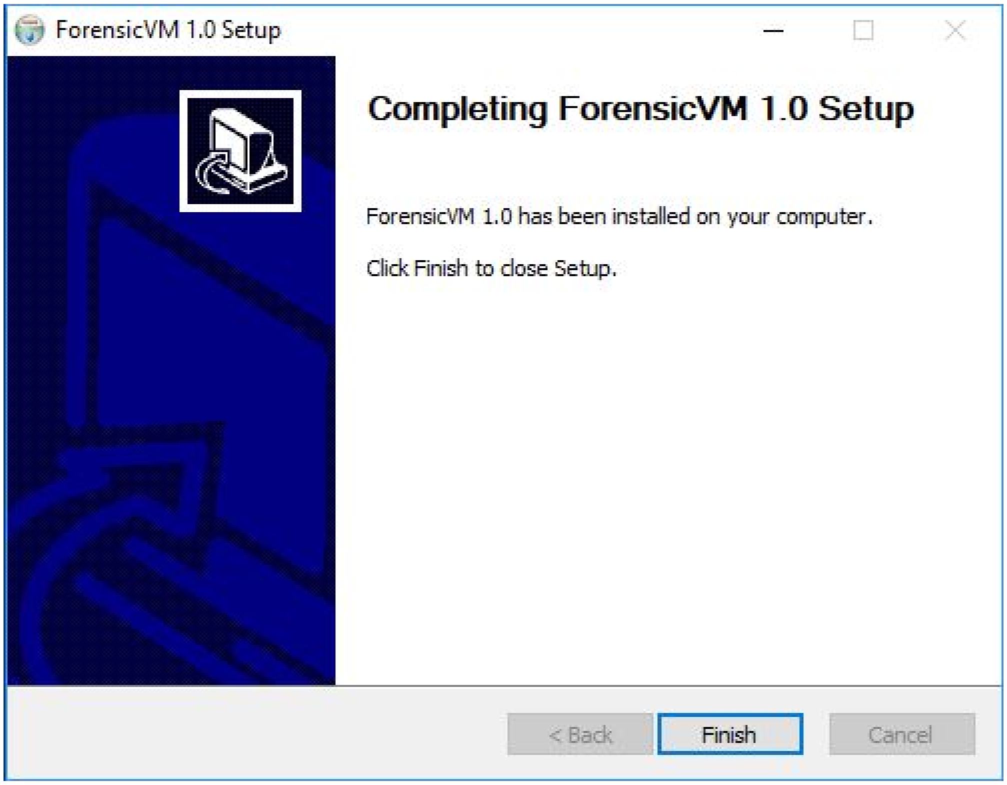
ngam\AppData\Roaming\Autopsy\Python_modules\ForensicVM

Space required: 16.0 MB

Space available: 8.5 GB

Nullsoft Install System v3.09

Fig. 4.3: Plugin Location



ForensicVM 1.0 Setup

Completing ForensicVM 1.0 Setup

ForensicVM 1.0 has been installed on your computer.

Click Finish to close Setup.

Fig. 4.4: Finish Screen

4.2 Initial Setup

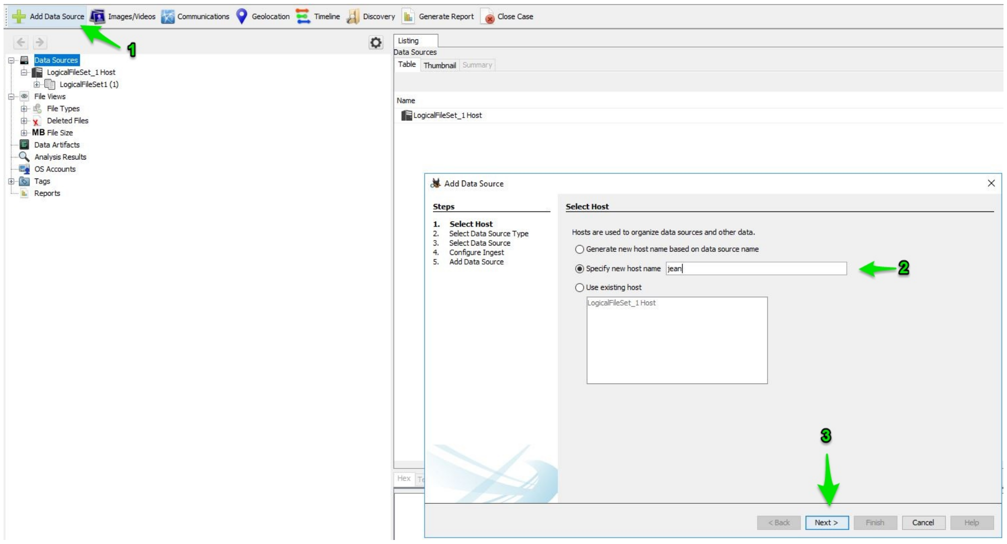
After successfully installing ForensicVM one needs to configure the AutopsyVM plugin. The initial configuration is composed of the following steps:

4.2.1 Step 1: In Autopsy: Add a new data source to Autopsy. This new data source is the forensic image that we need to convert to a forensicVM

1. Add datasource
2. Specify a new hostname
3. Next

4.2.2 Step 2: Select your Disk Image

1. Select the option disk image or VM FIle
2. Next



Add Data Source

Steps

1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source

Select Host

Hosts are used to organize data sources and other data.

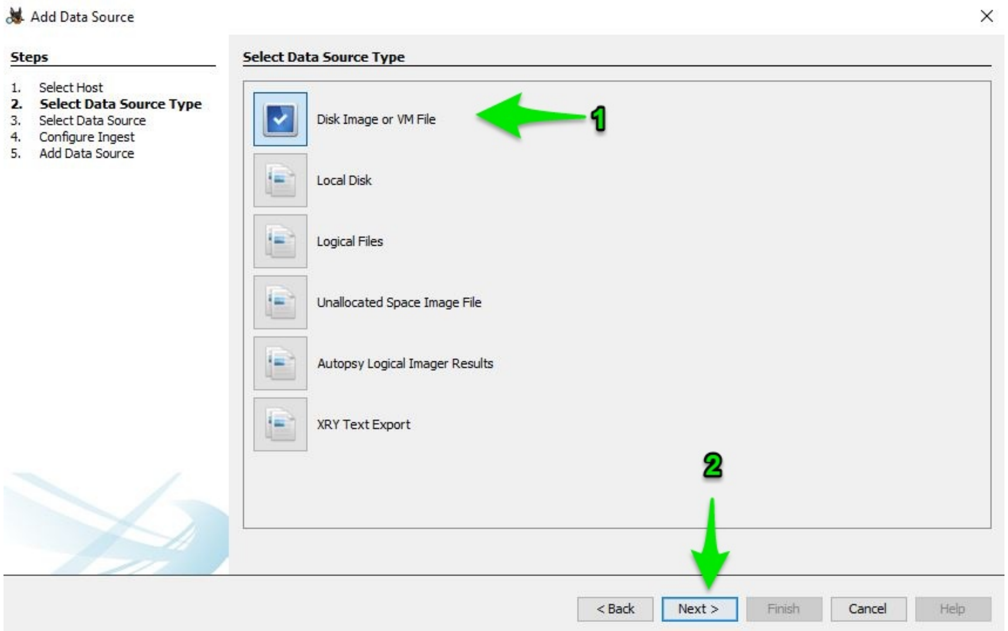
○ Generate new host name based on data source name

● Specify new host name: jean

○ Use existing host

LogicalFileSet_1 Host

Fig. 4.5: Add a new data source to Autopsy



Add Data Source

Steps

1. Select Host
2. **Select Data Source Type**
3. Select Data Source
4. Configure Ingest
5. Add Data Source

Select Data Source Type

☑ Disk Image or VM File

Local Disk

Logical Files

Unallocated Space Image File

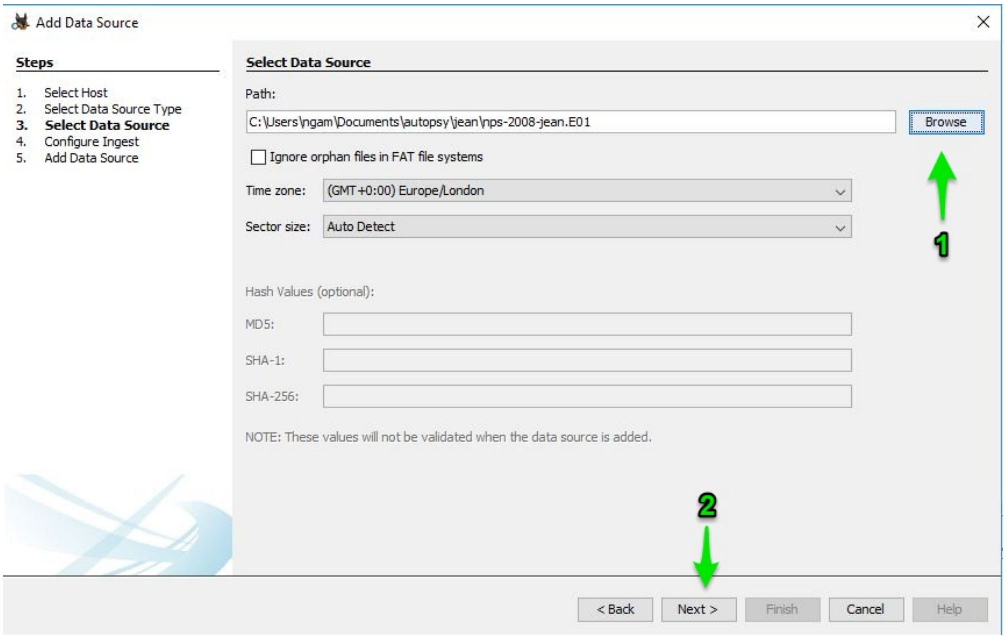
Autopsy Logical Imager Results

XRY Text Export

Fig. 4.6: Disk Image

4.2.3 Step 3: Select your forensic image

1. Browse for your forensic image, select it
2. Click Next



Add Data Source

Steps

1. Select Host
2. Select Data Source Type
3. **Select Data Source**
4. Configure Ingest
5. Add Data Source

Select Data Source

Path: C:\Users\ngam\Documents\autopsy\jean\nps-2008-jean.E01

□ Ignore orphan files in FAT file systems

Time zone: (GMT+0:00) Europe/London

Sector size: Auto Detect

Hash Values (optional):

MD5:

SHA-1:

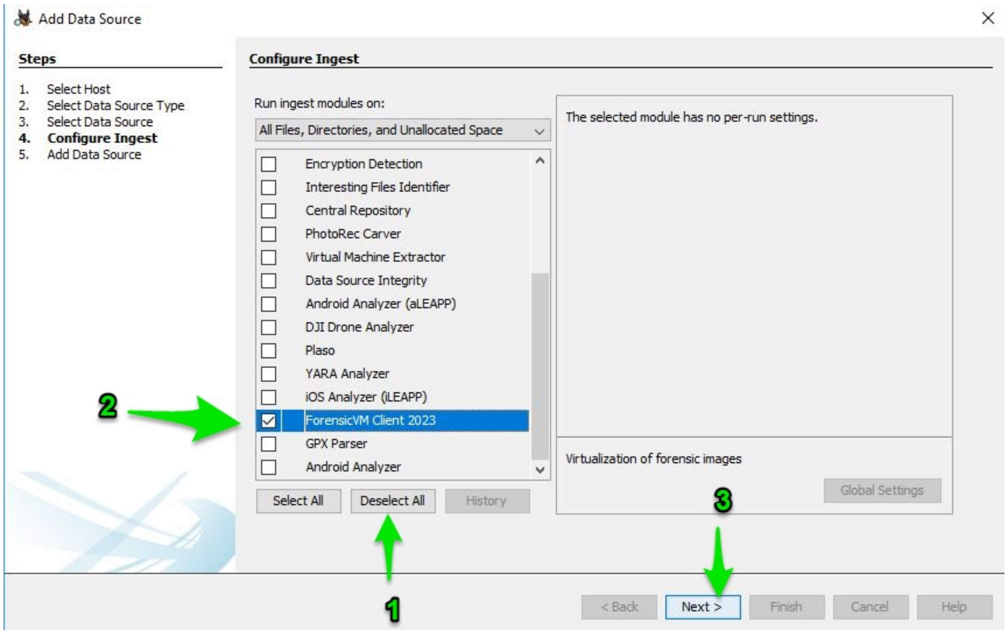
SHA-256:

NOTE: These values will not be validated when the data source is added.

Fig. 4.7: Forensic Image Selection

4.2.4 Step 4: Run the ForensicVM client plugin

1. Deselect all other plugins
2. Select the forensicVM Client plugin
3. Click next



Add Data Source

Steps

1. Select Host
2. Select Data Source Type
3. Select Data Source
4. **Configure Ingest**
5. Add Data Source

Configure Ingest

Run ingest modules on: All Files, Directories, and Unallocated Space

- ☐ Encryption Detection
- ☐ Interesting Files Identifier
- ☐ Central Repository
- ☐ PhotoRec Carver
- ☐ Virtual Machine Extractor
- ☐ Data Source Integrity
- ☐ Android Analyzer (aLEAPP)
- ☐ DJI Drone Analyzer
- ☐ Plaso
- ☐ YARA Analyzer
- ☐ iOS Analyzer (iLEAPP)
- ☑ ForensicVM Client 2023
- ☐ GPX Parser
- ☐ Android Analyzer

The selected module has no per-run settings.

Virtualization of forensic images

Fig. 4.8: Select Datasource

4.2.5 Step 5: Open your forensicVM Server web address in the admin. Ex: https://<ip-or-web>:port/admin

1. Enter user and password
2. Click the login button

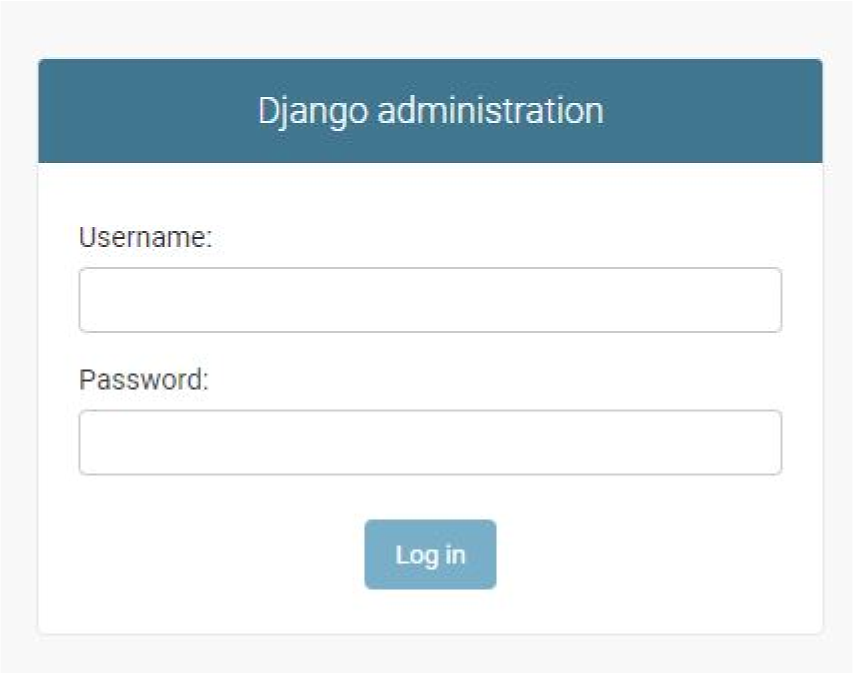
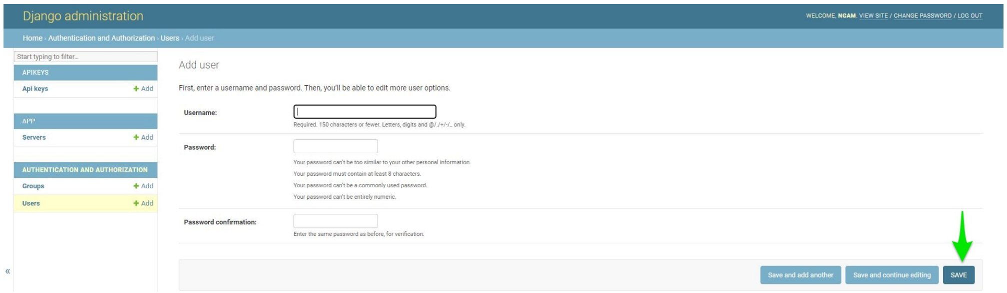


Fig. 4.9: Configure inject - Select ForensicVM Client plugin

4.2.6 Step 6: Add a new user

1. Enter user, password and password confirmation dialogues
2. Click SAVE


Django administration
WELCOME, NGAM. VIEW SITE / CHANGE PASSWORD / LOG OUT
Home › Authentication and Authorization › Users › Add user
Start typing to filter...
APIKEYS
Api keys
+ Add
APP
Servers
+ Add
AUTHENTICATION AND AUTHORIZATION
Groups
+ Add
Users
+ Add
«
Add user
Username:
Password:
Password confirmation:
Save and add another
Save and continue editing
SAVE

First, enter a username and password. Then, you'll be able to edit more user options.

Required. 150 characters or fewer. Letters, digits and @/./+/-/_ only.

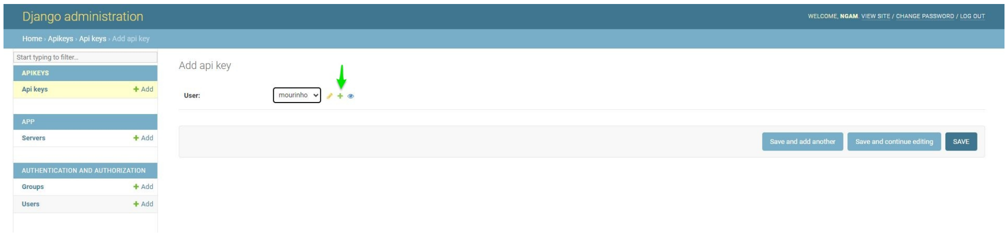
Your password can't be too similar to your other personal information.
Your password must contain at least 8 characters.
Your password can't be a commonly used password.
Your password can't be entirely numeric.

Enter the same password as before, for verification.

Fig. 4.10: Add user

4.2.7 Step 7: Add a new api key to the user

1. Click the add button on the api keys
2. Select the user
3. Click the plus sign


Django administration
WELCOME, NGAM. VIEW SITE / CHANGE PASSWORD / LOG OUT
Home › Apikeys › Api keys › Add api key
Start typing to filter...
APIKEYS
Api keys
+ Add
APP
Servers
+ Add
AUTHENTICATION AND AUTHORIZATION
Groups
+ Add
Users
+ Add
Save and add another
Save and continue editing
SAVE

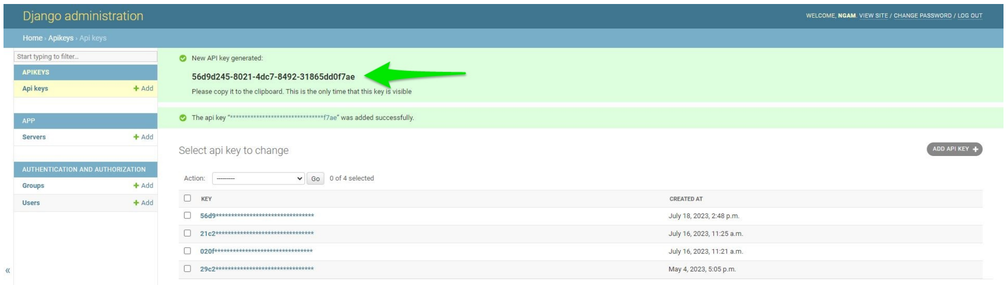
Add api key

User: mourinho

Fig. 4.11: Add API key to user

4.2.8 Step 8: Copy the user API key

1. Select the newly created API key
2. Press CTRL + C or copy it using the right mouse button and select copy


Django administration
WELCOME, NGAM. VIEW SITE / CHANGE PASSWORD / LOG OUT
Home › Apikeys › Api keys
Start typing to filter...
APIKEYS
Api keys
+ Add
APP
Servers
+ Add
AUTHENTICATION AND AUTHORIZATION
Groups
+ Add
Users
+ Add
ADD API KEY +
Go
«

New API key generated:

56d9d245-8021-4dc7-8492-31865dd0f7ae

Please copy it to the clipboard. This is the only time that this key is visible

The api key "********************************f7ae" was added successfully.

Select api key to change

Action: --------- 0 of 4 selected

□	KEY	CREATED AT
□	56d9********************************	July 18, 2023, 2:48 p.m.
□	21c2********************************	July 16, 2023, 11:25 a.m.
□	020f********************************	July 16, 2023, 11:21 a.m.
□	29c2********************************	May 4, 2023, 5:05 p.m.

Fig. 4.12: Copy user API key

4.2.9 Step 9: Paste the user API key

1. Put the mouse on the Forensic API field
2. Press CTRL + V or paste it using the right mouse button and select paste

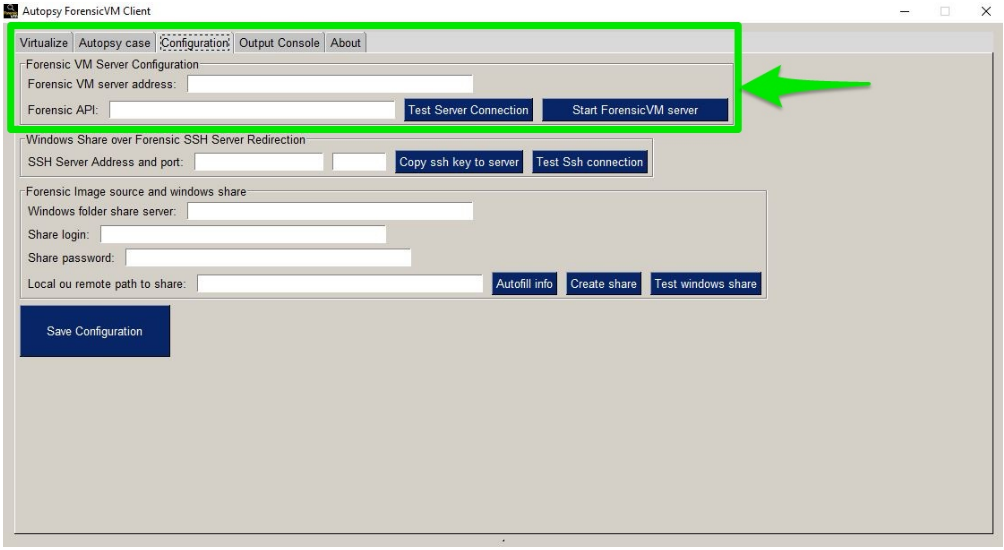
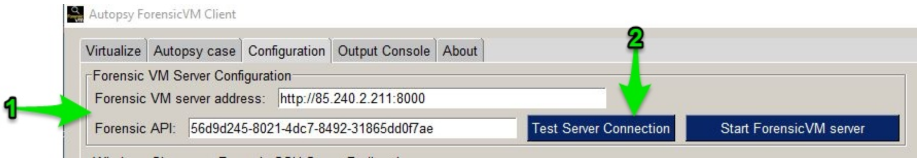

Autopsy ForensicVM Client
Virtualize
Autopsy case
Configuration
Output Console
About
Forensic VM Server Configuration
Forensic VM server address:
Forensic API:
Test Server Connection
Start ForensicVM server
Windows Share over Forensic SSH Server Redirection
SSH Server Address and port:
Copy ssh key to server
Test Ssh connection
Forensic Image source and windows share
Windows folder share server:
Share login:
Share password:
Local ou remote path to share:
Autofill info
Create share
Test windows share
Save Configuration

Fig. 4.13: Paste the user API key

4.2.10 Step 10: Fill and test the Forensic VM Server configuration

1. Put the mouse on the Forensic VM server address. Fill in the information with your server address
2. Click the Test Server Connection to test if API and server address are correct



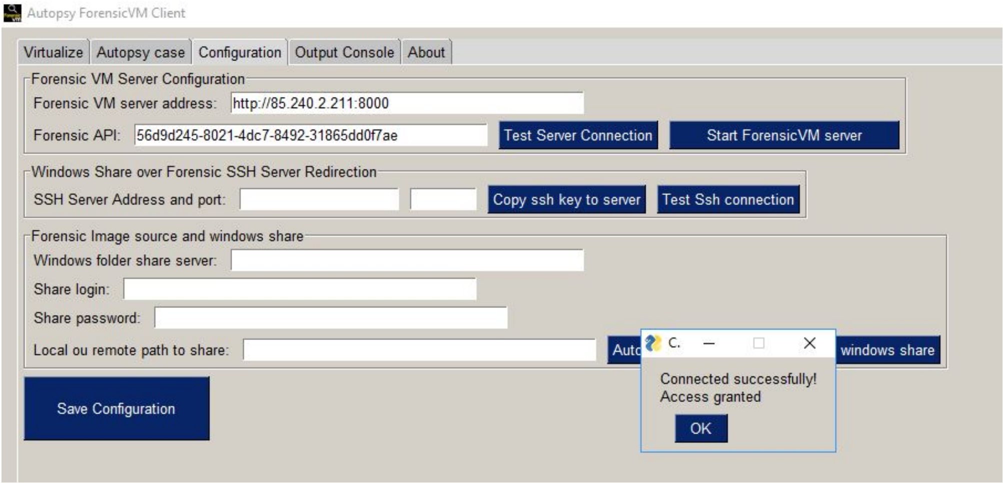
Forensic VM server address: http://85.240.2.211:8000

Forensic API: 56d9d245-8021-4dc7-8492-31865dd0f7ae

Fig. 4.14: Fill and test forensic VM Server Configuration

4.2.11 Step 11: Forensic VM Server configuration test success

1. If all pieces of information are correct and if the server is online you should see a connected successfully dialog box.
2. If there are any problems, you should see a red error dialogue. Please check and correct the field values.


Autopsy ForensicVM Client
Virtualize
Autopsy case
Configuration
Output Console
About
Forensic VM Server Configuration
Test Server Connection
Start ForensicVM server
Windows Share over Forensic SSH Server Redirection
Copy ssh key to server
Test Ssh connection
Forensic Image source and windows share
Windows folder share server:
Share login:
Share password:
Local ou remote path to share:
windows share
Save Configuration
C.
OK

Forensic VM server address: http://85.240.2.211:8000

Forensic API: 56d9d245-8021-4dc7-8492-31865dd0f7ae

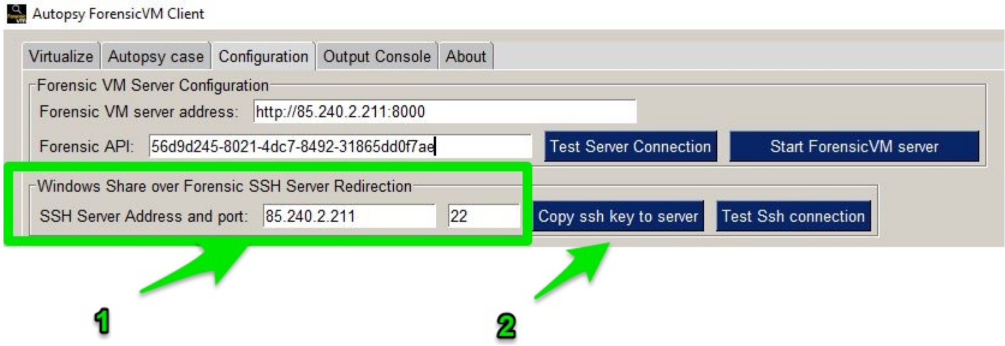
SSH Server Address and port:

Connected successfully!
Access granted

Fig. 4.15: Forensic VM server connection test

4.2.12 Step 12: Configure Windows Share over Forensic SSH Server Redirection

The way that forensicVM Server access the forensic images is by making a reverse ssh connection to your computer and accessing a local share via the internet. The reverse ssh connection is in need to make a safe Windows share access. You should configure now the forensicVM server SSH address and port number: #. Please fill in the SSH Server Address and port number. #. Press the button to copy the ssh key to the server



Forensic VM server address: http://85.240.2.211:8000

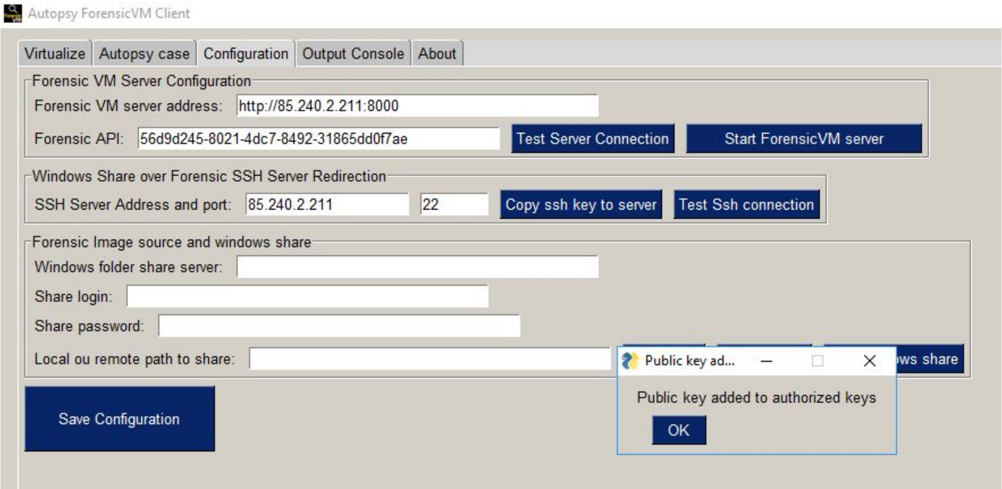
Forensic API: 56d9d245-8021-4dc7-8492-31865dd0f7ae

SSH Server Address and port: 85.240.2.211 22

Fig. 4.16: Configure and copy the ssh key to the server

4.2.13 Step 13: Windows Share over Forensic SSH copy ssh key status

1. If the configuration is correct you should see a dialog stating that a Public key added to authorized keys
2. If not, you should see an error dialogue or a dialogue stating that the ssh public key is already present on the remote server



Forensic VM Server Configuration

Forensic VM server address: http://85.240.2.211:8000

Forensic API: 56d9d245-8021-4dc7-8492-31865dd0f7ae

Windows Share over Forensic SSH Server Redirection

SSH Server Address and port: 85.240.2.211 22

Forensic Image source and windows share

Windows folder share server:

Share login:

Share password:

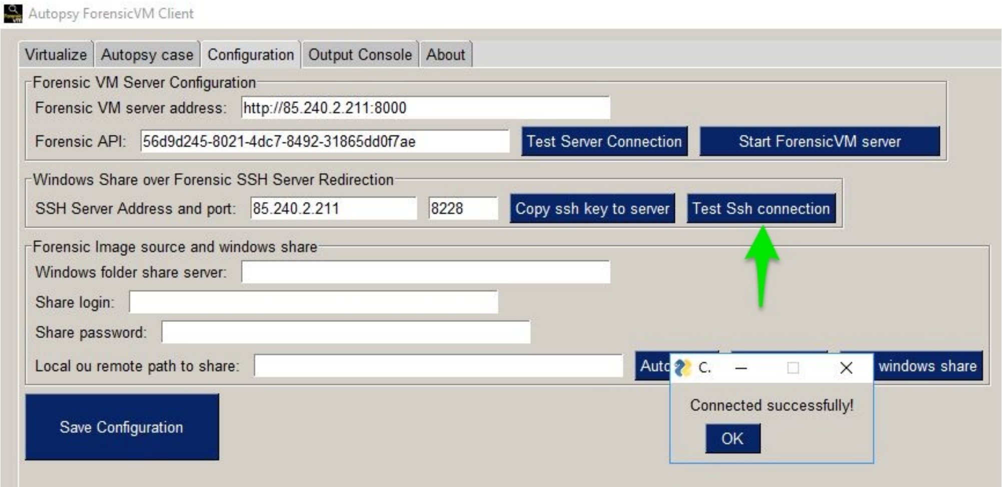
Local ou remote path to share:

Public key added to authorized keys

Fig. 4.17: Copy ssh key status

4.2.14 Step 14: Testing Windows Share over Forensic SSH Server Redirection

1. Click the Test Ssh connection button
2. If the configuration is correct you should see a dialog stating that the connection was successful
3. If not, you should see an error dialogue



Forensic VM Server Configuration

Forensic VM server address: http://85.240.2.211:8000

Forensic API: 56d9d245-8021-4dc7-8492-31865dd0f7ae

Windows Share over Forensic SSH Server Redirection

SSH Server Address and port: 85.240.2.211 8228

Forensic Image source and windows share

Windows folder share server:

Share login:

Share password:

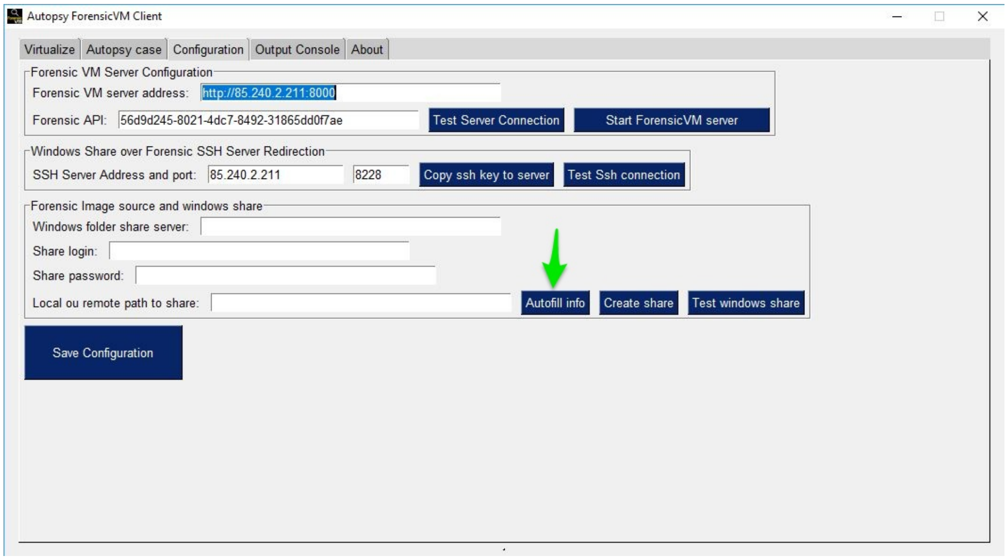
Local ou remote path to share:

Connected successfully!

Fig. 4.18: Test windows share over ssh

4.2.15 Step 15: Configure windows share over ssh

1. Press the Autofill info button to autofill the Windows share information with the Share login and local and the remote path to share. This info is extracted from the forensic image's current path.



Autopsy ForensicVM Client

Forensic VM Server Configuration

Forensic VM server address: http://85.240.2.211:8000

Forensic API: 56d9d245-8021-4dc7-8492-31865dd0f7ae

Windows Share over Forensic SSH Server Redirection

SSH Server Address and port: 85.240.2.211 8228

Forensic Image source and windows share

Windows folder share server:

Share login:

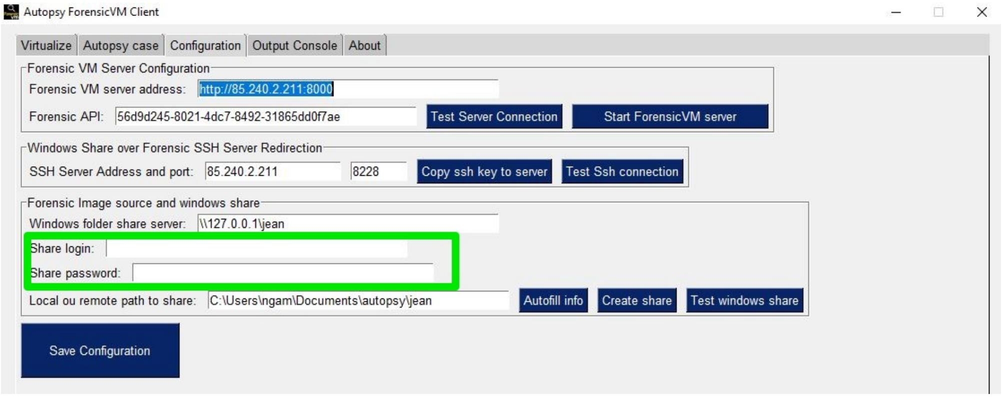
Share password:

Local ou remote path to share:

Fig. 4.19: Configure windows share over ssh

4.2.16 Step 16: Configure the share login and the share password

1. The share login and share password is a Windows local user and is password. It does not need to be an Administrator account. It can be a regular user. It also does not need to exist, since it is created if it does not exist when the user presses the create share button.



Autopsy ForensicVM Client

Forensic VM Server Configuration

Forensic VM server address: http://85.240.2.211:8000

Forensic API: 56d9d245-8021-4dc7-8492-31865dd0f7ae

Windows Share over Forensic SSH Server Redirection

SSH Server Address and port: 85.240.2.211 8228

Forensic Image source and windows share

Windows folder share server: \\127.0.0.1\jean

Share login:

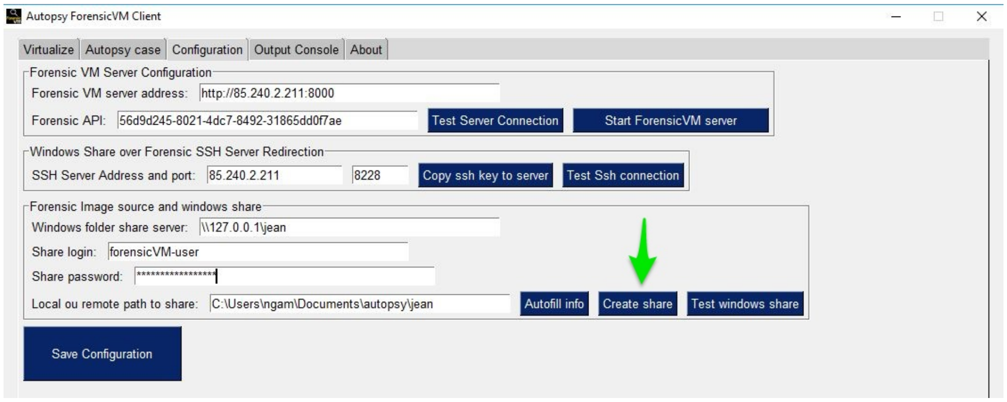
Share password:

Local ou remote path to share: C:\Users\ngam\Documents\autopsy\jean

Fig. 4.20: Share login and the share password configuration

4.2.17 Step 17: Create Share Button

1. After filling in the share login and password please press the create share button.



Autopsy ForensicVM Client

Forensic VM Server Configuration

Forensic VM server address: http://85.240.2.211:8000

Forensic API: 56d9d245-8021-4dc7-8492-31865dd0f7ae

Windows Share over Forensic SSH Server Redirection

SSH Server Address and port: 85.240.2.211 8228

Forensic Image source and windows share

Windows folder share server: \\127.0.0.1\jean

Share login: forensicVM-user

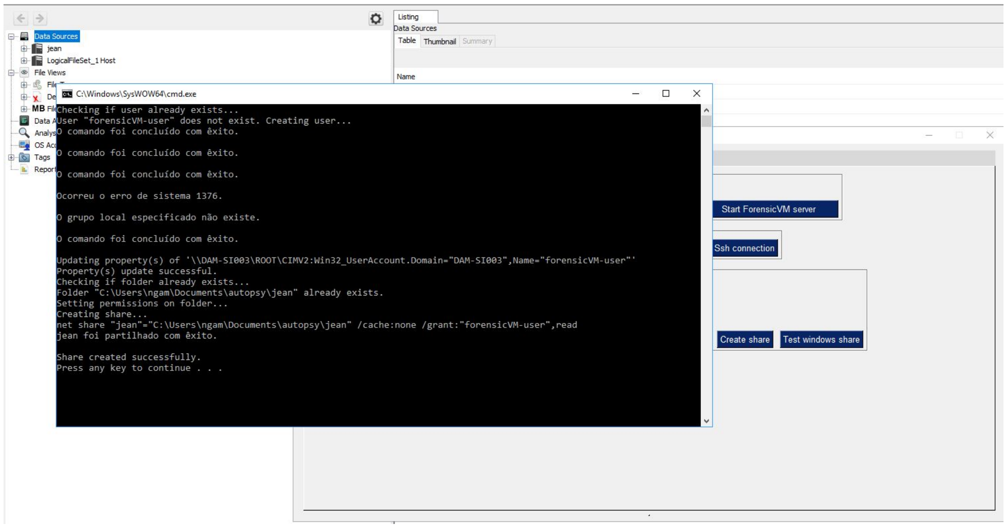
Share password: ****************

Local ou remote path to share: C:\Users\ngam\Documents\autopsy\jean

Fig. 4.21: Create share button

4.2.18 Step 18: Create a share Dialog

1. After pressing the create share button a command window will open. This will try to create the local user with the defined password.



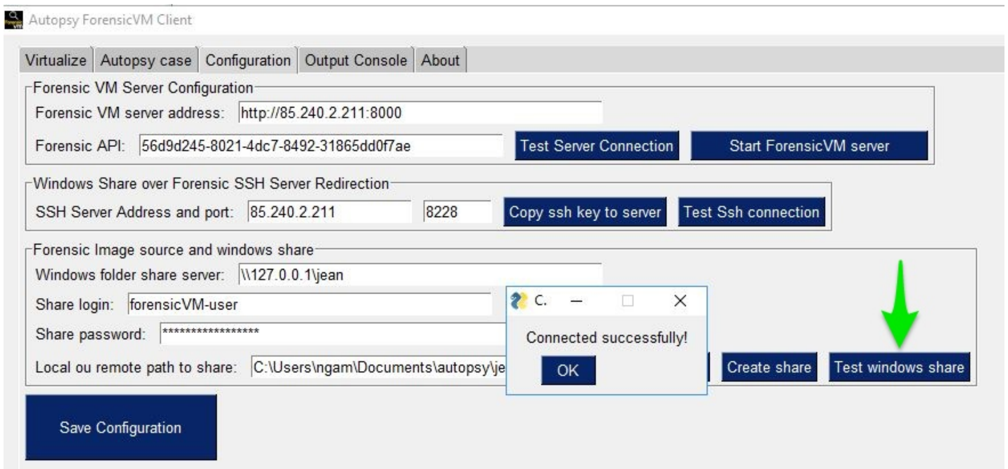
C:\Windows\SysWOW64\cmd.exe

```
Checking if user already exists...
User "forensicVM-user" does not exist. Creating user...
O comando foi concluído com êxito.

O comando foi concluído com êxito.

O comando foi concluído com êxito.

Ocorreu o erro de sistema 1376.

O grupo local especificado não existe.

O comando foi concluído com êxito.

Updating property(s) of '\\DAM-SI003\ROOT\CIMV2:Win32_UserAccount.Domain="DAM-SI003",Name="forensicVM-user"'
Property(s) update successful.
Checking if folder already exists...
Folder "C:\Users\ngam\Documents\autopsy\jean" already exists.
Setting permissions on folder...
Creating share...
net share "jean"="C:\Users\ngam\Documents\autopsy\jean" /cache:none /grant:"forensicVM-user",read
jean foi partilhado com êxito.

Share created successfully.
Press any key to continue . . .
```

Fig. 4.22: Create a share command window

4.2.19 Step 19: Testing the forensicVM image Windows share over ssh

1. Press Test Windows share button to test if it is possible to connect to the Windows share from the server using a reverse ssh connection. If all is ok you will be presented with a Windows alert stating that the connection was successful



Forensic VM server address: http://85.240.2.211:8000

Forensic API: 56d9d245-8021-4dc7-8492-31865dd0f7ae

SSH Server Address and port: 85.240.2.211 8228

Windows folder share server: \\127.0.0.1\jean

Share login: forensicVM-user

Share password: *****************

Local ou remote path to share: C:\Users\ngam\Documents\autopsy\je

Connected successfully!

Fig. 4.23: Testing the forensicVM image Windows share over ssh

Caution: Ensure to use a secure Windows username and password for your share. Although this share is protected over the internet by your SSH private key, on the Windows network, your username and password could be a potential vulnerability. We recommend a dedicated, strong username and password for your share, which can be reused for multiple forensic image shares if necessary.

Note: Please configure your firewall to allow local access to your Windows shares. You can restrict the Windows share to be accessible only by your own computer. If needed, please seek assistance from your system administrator to perform this task.

CHAPTER

FIVE

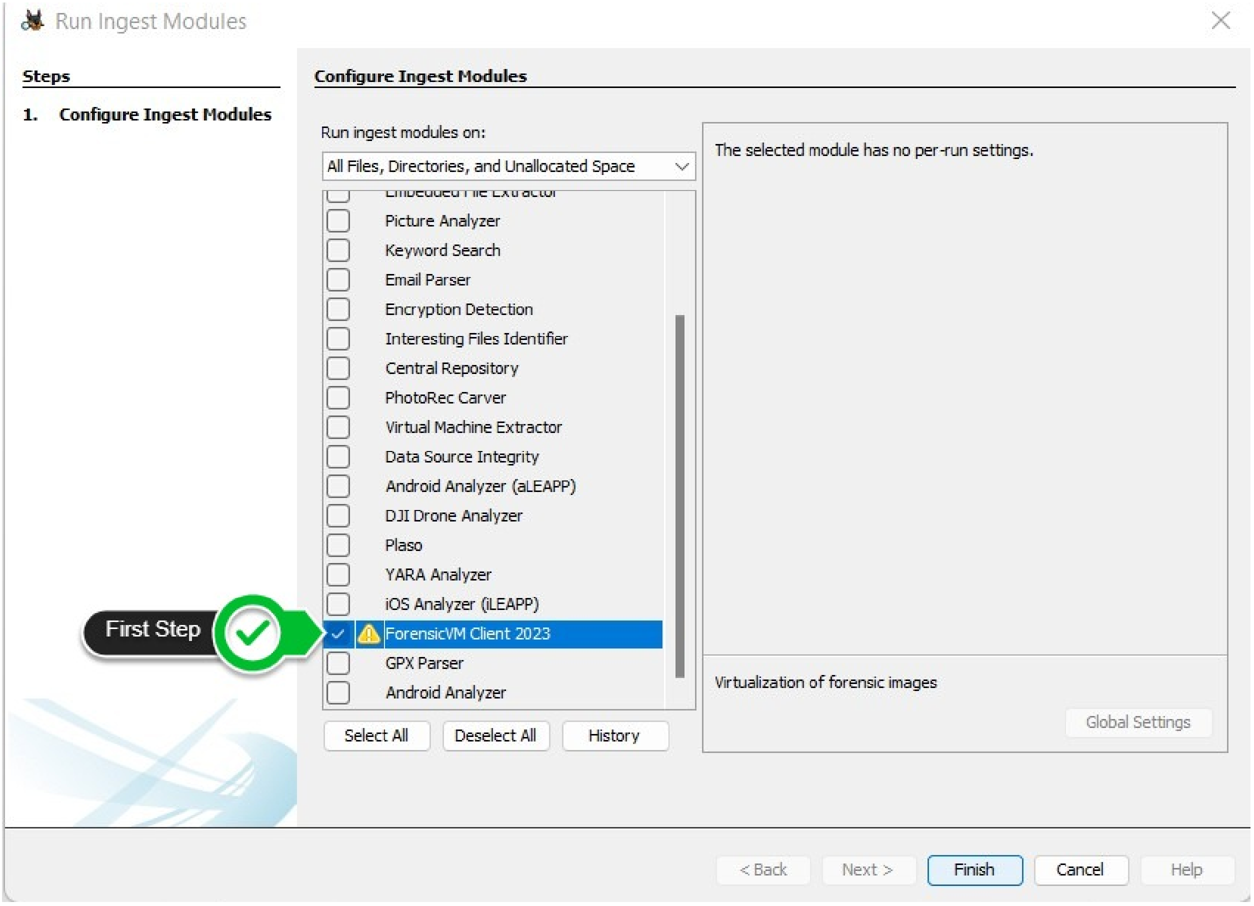
GETTING STARTED

5.1 Installing ForensicVM

Before you can use ForensicVM, you must first install the software on your system. To do this, follow the steps outlined in the *Installation and Setup*.

5.2 Navigating the Interface

Your first step is to run the ForensicVM Client Plugin in Autopsy Software. The main interface will open. Manage this by right-clicking the datasource and choosing "Run Ingest Modules". After this, the Forensic Client Plugin main program interface will open.



Run Ingest Modules

Steps

1. **Configure Ingest Modules**

Configure Ingest Modules

Run ingest modules on: All Files, Directories, and Unallocated Space

- □ Embedded File Extractor
- □ Picture Analyzer
- □ Keyword Search
- □ Email Parser
- □ Encryption Detection
- □ Interesting Files Identifier
- □ Central Repository
- □ PhotoRec Carver
- □ Virtual Machine Extractor
- □ Data Source Integrity
- □ Android Analyzer (aLEAPP)
- □ DJI Drone Analyzer
- □ Plaso
- □ YARA Analyzer
- □ iOS Analyzer (iLEAPP)
- ☑ ⚠ ForensicVM Client 2023
- □ GPX Parser
- □ Android Analyzer

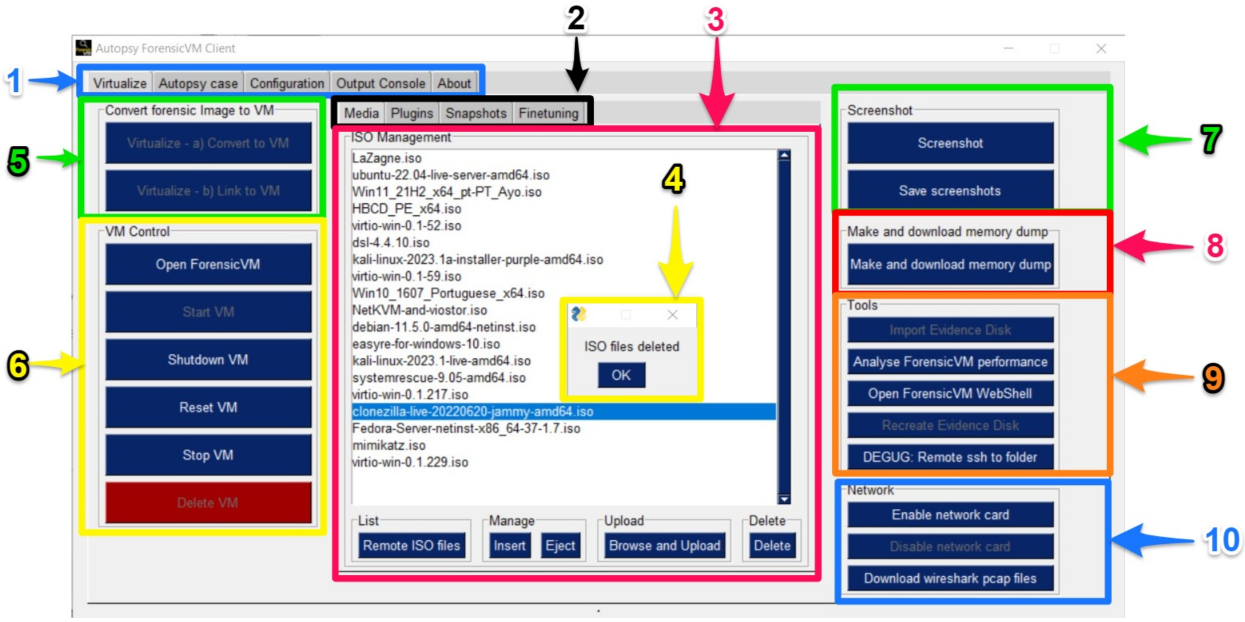
The selected module has no per-run settings.

Virtualization of forensic images

Fig. 5.1: Overview of ForensicVM Interface

5.3 Autopsy ForensicVM Client Plugin: A Comprehensive Interface Guide

The Autopsy ForensicVM Client Plugin serves as a pivotal hub for forensic analysts. This interface is designed for interactive engagement with forensic images, subsequently allowing users to transform these images into a forensic virtual machine (ForensicVM). Here's a breakdown of its primary functionalities on the Autopsy ForensicVM Client Plugin main interface:



```
LaZagne.iso
ubuntu-22.04-live-server-amd64.iso
Win11_21H2_x64_pt-PT_Ayo.iso
HBCD_PE_x64.iso
virtio-win-0.1-52.iso
dsl-4.4.10.iso
kali-linux-2023.1a-installer-purple-amd64.iso
virtio-win-0.1-59.iso
Win10_1607_Portuguese_x64.iso
NetKVM-and-viostor.iso
debian-11.5.0-amd64-netinst.iso
easyre-for-windows-10.iso
kali-linux-2023.1-live-amd64.iso
systemrescue-9.05-amd64.iso
virtio-win-0.1.217.iso
clonezilla-live-20220620-jammy-amd64.iso
Fedora-Server-netinst-x86_64-37-1.7.iso
mimikatz.iso
virtio-win-0.1.229.iso
```

ISO files deleted

Fig. 5.2: Autopsy ForensicVM Client Plugin Main

5.3.1 Main Toolbar Overview (1)

1. **Configuration**:

   - Prior to exploring the main functionalities, it's paramount to configure the plugin's settings. This preliminary setup is generally executed during the *Installation and Setup*.

2. **Virtualize Tab**:

   This tab houses the primary operations. Specifically, users can:

   - **Control the ForensicVM**: Open webscreen console, Start, Stop, Shutdown, Reset, or Delete.
   - **Manage Media**: Organize manage media relevant to forensic analysis.
   - **Manage Plugins**: Run individual plugins.
   - **Handle Snapshots**: Capture and revert the ForensicVM to various states.
   - **Capture Screenshots**: Record specific instances or frames within the ForensicVM.
   - **Memory Management**: Generate and retrieve memory dumps, vital for observing real-time operations within the ForensicVM.
   - **Virtual** Evidence Disk Management: Import and regenerate the virtual evidence disk, accumulating all potential pieces of evidence.

   - **Network Management**: Toggle network cards on or off, and capture pcap (packet capture) files for granular network investigations.
   - **ForensicVM Customization**: Modify the starting date/time, reallocate memory, among other settings.
   - **Performance Analysis**: Employ Netdata for comprehensive metric analysis of the ForensicVM's operations.
   - **Troubleshooting**: Secure an SSH connection to the ForensicVM machine, connecting directly to its remote directory. Additionally, avail an equivalent webshell for an internet-based SSH interaction with the server.

3. Autopsy Case:
   - This tab displays the Autopsy case details, including the extant case tags (utilized for case folder creation) and the generated UUID. This UUID is unique and becomes the name for the foundational directory of the forensic virtual machine.
4. Output Console:
   - This console captures all system messages. It's a valuable tool for debugging or ascertaining the final state of operations.
5. **About**:
   - Contains copyright details pertaining to the ForensicVM Client.

5.3.2 Secondary Toolbar Overview (2)

1. **Media Management**:

   This tab facilitates access to auxiliary virtualization functions:

   - **Media** - Oversee media operations. Upload ISO files to the server and manage actions such as insert, eject, and delete.
   - **Plugins** - Choose and execute a specific plugin. Introduce new forensic administrators, bypass passwords, reset activations, and navigate security protocols to delve into user profiles.
   - **Snapshots** - Take and revert the ForensicVM to various points in time.
   - **Finetuning** - Adjust memory capacity and define the initial start date.

5.3.3 Main Panel Overview (3)

Based on the selected tab option, the main panel showcases different functionalities. For instance, when the **Media** tab is chosen, the corresponding list or form materializes in this space. Action buttons are located at the bottom. Among these, enabled buttons signify available actions, while disabled ones represent currently unavailable actions. These buttons toggle between enabled and disabled based on the ForensicVM machine's status or existence.

5.3.4 Notification Area (4)

The notification area serves as the designated space for displaying notifications, warnings, and error pop-ups, tailored to specific events. Whenever there's a need to apprise the user or when the system requires user interaction, a pop-up emerges in this area, seeking the user's attention or input.

5.3.5 Convert Forensic Image to VM (5)

These two buttons facilitate the transformation of the forensic image into a forensic virtual machine:

- **Virtualize - a) Convert to VM:**
  This option converts the forensic image into a forensic virtual machine by copying it onto the forensicVM hypervisor server.
- **Virtualize - b) Link to VM:**
  This option establishes a link between the remote forensic virtual machine and the local forensic image.

For both methods, the remote forensicVM integrates an overlay of information. This includes additional drivers and outcomes from the execution of security plugins or actions taken by forensic investigators on the machine. Importantly, this approach ensures the preservation of the original forensic image's integrity.

5.3.6 VM Control (6)

Manage essential actions for the forensic virtual machine:

- **Start**: Power on the forensic virtual machine.
- **Stop**: Cease the operation of the forensic virtual machine.
- **Shutdown**: Gracefully power down the forensic virtual machine.
- **Reset**: Restart the forensic virtual machine.
- **Delete**: Remove the forensic virtual machine entirely.

5.3.7 Screenshot Management (7)

Manage the screenshots taken during your forensic investigations:

- **Screenshot**: Capture the current view of the forensic virtual machine, providing a visual record of its state at that moment.
- **Save Screenshots**: Compile and download all captured screenshots into a single ZIP file, allowing for easy storage and transfer.

5.3.8 Make and Download a Memory Dump (8)

Engage with the active memory data of the forensic virtual machine:

- **Make** Memory Dump: Generate a snapshot of the forensicVM's current memory state, capturing active processes, and other runtime details.
- **Download** Memory Dump: Retrieve the created memory dump for further analysis, facilitating deeper investigations using tools such as:
  - The Volatility plugin within the Autopsy software.

  - External utilities like Volatility 3.0.
  - Rekall: Another powerful framework for memory forensics.
  - MemProcFS: Useful for live RAM analysis and incident response.
  - Redline: Offers a user-friendly interface for in-depth memory and file analysis.

5.3.9 Tools (9)

Use auxiliary tools for various forensic operations:

- **Import evidence disk into autopsy:**
  Import a virtual disk allowing forensic investigators to collect and gather potential evidence. This option lets you import the disk as a vmdk disk into Autopsy for reporting purposes.
- **Recreate evidence disk:**
  Delete and recreate the evidence disk.

> **Warning:** This is a destructive action. Ensure to import the current evidence disk into Autopsy if it contains gathered evidence.

- **Analyze ForensicVM performance:**
  Utilize the Netdata software to pinpoint server bottlenecks, optimize server performance, and determine the root cause of any ForensicVM server issues.
- **Open ForensicVM Webshell:**
  Initiate an SSH-over-internet webshell connection to the server.
- **DEBUG: remote ssh to the folder:**
  Access an SSH shell inside the ForensicVM image folder, allowing edits and testing of the ForensicVM start script.

> **Note:** This is primarily used for debugging purposes.

5.3.10 Network (10)

Manage network settings and operations:

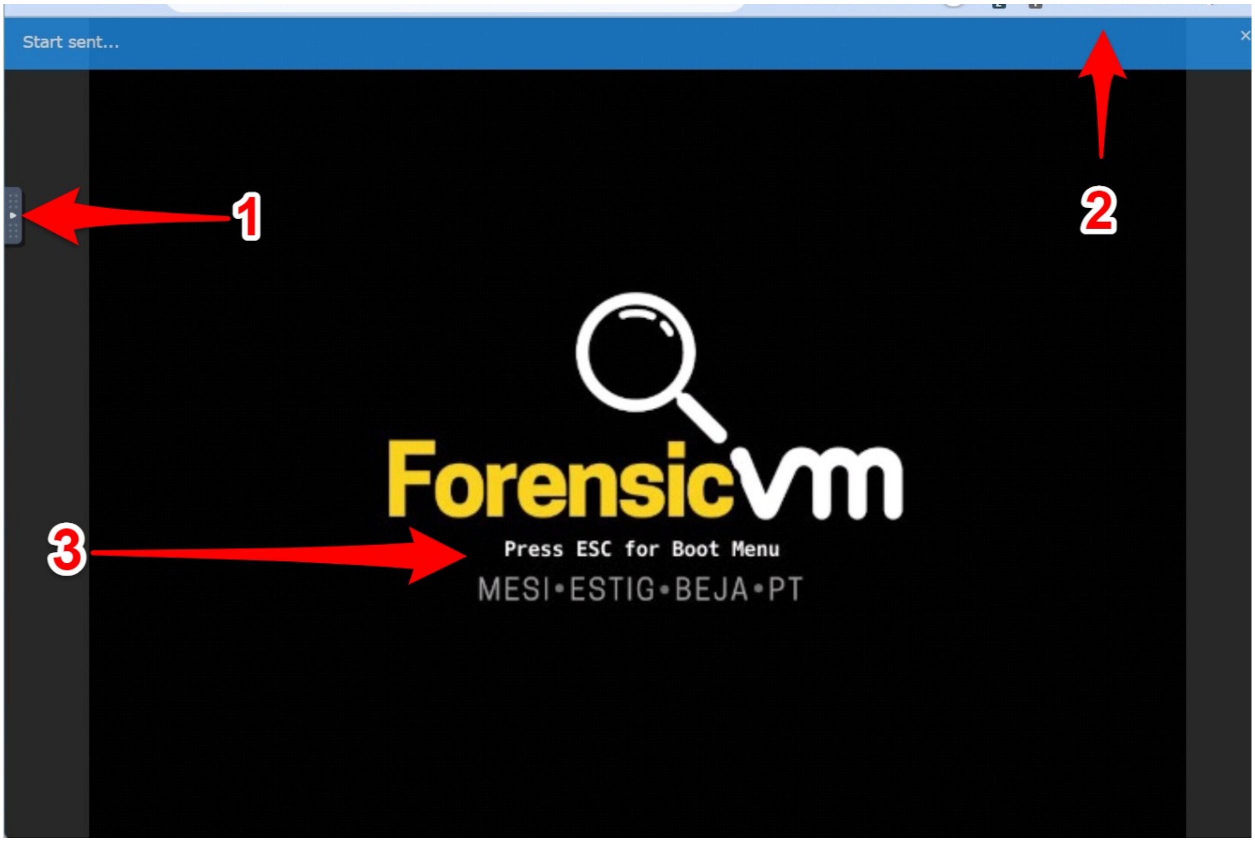
- **Enable network card:**
  For security reasons, the network is disabled by default. Given that a machine could be compromised by malware, use this option with caution. When enabled, an internet firewall activates, blocking traffic to the local network but permitting internet access. Additionally, all traffic is recorded in the pcap (packet capture) file format.
- **Disable network card:**
  Deactivates the network card and saves a pcap file with all captured traffic to the server.
- **Download Wireshark pcap files:**
  Download all generated pcap files as a zip file, enabling investigators to analyze captured network traffic using tools like Wireshark or other network traffic analysis software.

5.4 ForensicVM Webscreen Console

The webscreen console, developed on the HTML5 VNC technology known as NoVNC, provides a visual and interactive gateway to the virtual screen of the remote ForensicVM. Alongside basic interactions, it also offers an array of ForensicVM control options to augment the forensic investigation process. To access this feature-rich console, select the **Open ForensicVM** option. Delve deeper for more details:

5.4.1 Webscreen Console Main Area

The following figure elucidates the available options:



Start sent...

Fig. 5.3: Overview of the ForensicVM Webscreen Console functionalities.

- **(1) Control bar open icon**: By clicking on this icon, users can unveil the auto-hiding control bar that seamlessly overlays the main screen, bestowing access to an assortment of functionalities.
- **(2) Notification area**: Strategically positioned at the top, this zone is dedicated to presenting error, notification, and warning messages.
- **(3) Main screen**: Serving as the primary interface of the webscreen, during the boot sequence, users can hit the ESC key to dive into the BIOS or UEFI. This permits modifications to pivotal settings, with a prime focus on the boot device, especially when initiating a boot from an ISO.

5.4.2 ForensicVM Webscreen Console Control Toolbar

Upon clicking the control bar open icon, users are presented with the Control Toolbar, illustrated below:

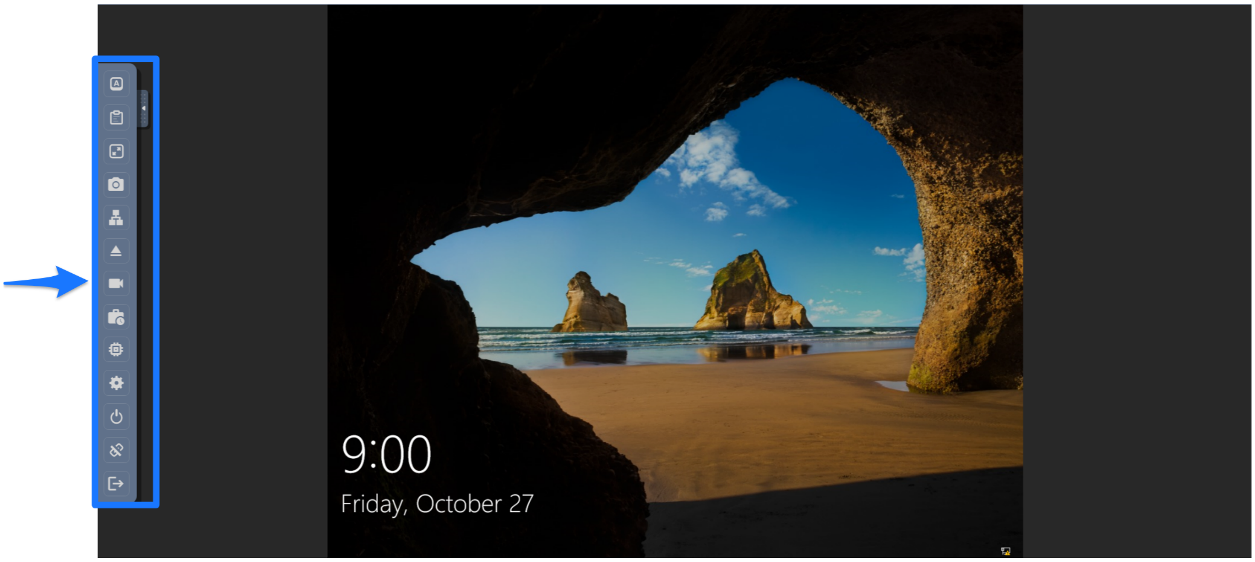


Fig. 5.4: Overview of the Control Toolbar in ForensicVM Webscreen Console

The Control Toolbar facilitates the following actions:

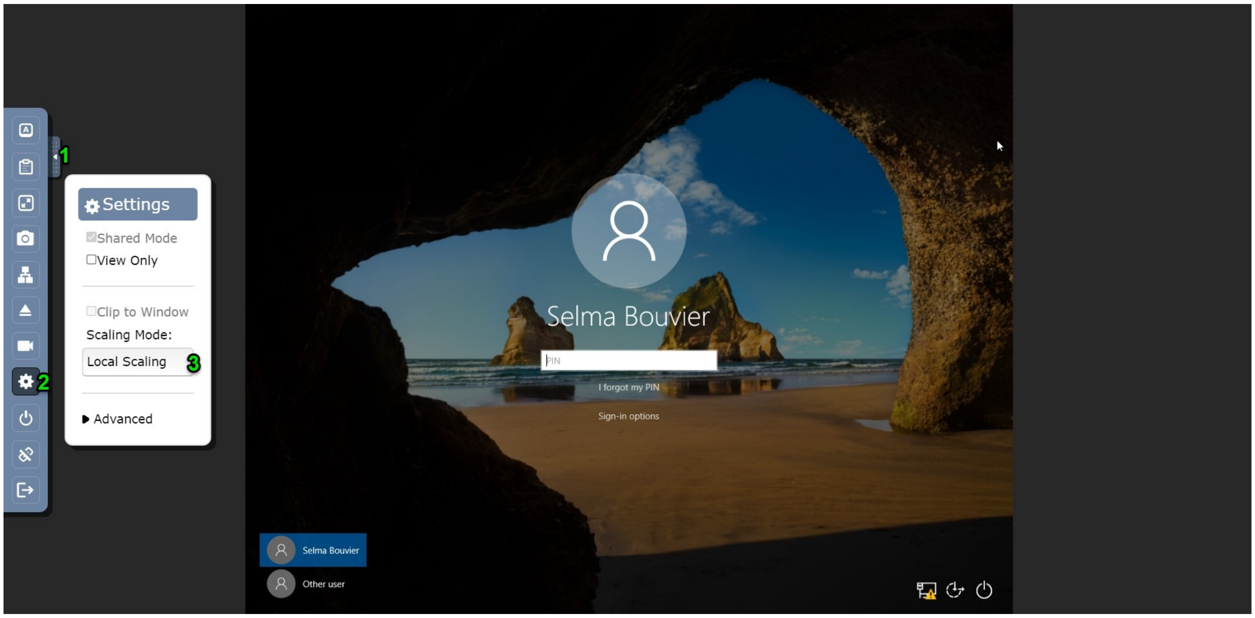
- **Show Extra Keys**: Displays icons representing frequently-used key combinations such as Ctrl+Alt+Del and the Windows key. Clicking these icons sends the corresponding key inputs to the ForensicVM.
- **Clipboard**: Enables basic data transfer between the user's environment and the ForensicVM, provided the QEMU agent is installed on the virtual machine.
- **Fullscreen**: Expands the ForensicVM webscreen to occupy the entire display area.
- **Take a Screenshot**: Captures the current view of the remote ForensicVM.
- **Enable or Disable the** Network Card: This function is self-explanatory.
- **Insert or Eject Media**: Facilitates the selection, insertion, and ejection of CD-ROMs or DVDs containing additional forensic tools.
- **Video Recording**: Initiates, terminates, and downloads video recordings at a rate of 30 frames per minute.
- **Manage Chain of Custody**: 1) Generate and download the chain of custody records document; 2) Save a comment on the chain of custody.
- **Virtual introspect**: Take a memory dump and analyse it automaticaly using memory introspection, with the help of volatility 3. See current process tree, Running command line with arguments, Enviroment Variables, Possible malware injection processes, Network Connections and Running Network Services.
- **Settings**: Provides access to several webscreen console preferences. Notably, users can adjust the scaling mode. Setting it to "Local Scaling" ensures the remote display fits the browser window perfectly.
- **Power**: Offers control over the ForensicVM's power states, including shutdown, stop, and reset actions.
- **Disconnect**: Ends the current webscreen session.
- **Logout**: Signs the user out of the ForensicVM server.

5.4.3 Adjusting Screen Scaling: Local Scaling

If you find that the screen appears cropped or that certain parts of the interface aren't fully visible, you can adjust the scaling settings for a more optimal viewing experience. Here's a comprehensive guide to making those adjustments:

Steps to Adjust Screen Scaling:

1. **Reveal the Control Bar**: - **Control Bar Open Icon**: The control bar is typically hidden to provide a cleaner viewing area. By clicking on this icon, you'll reveal a set of controls that overlay the main screen. These controls grant access to various functionalities.
2. **Access Scaling Settings**: - **Definitions Icon**: Once the control bar is visible, locate and click on the definitions icon. This action will lead you into the settings or preferences area, where you can manage various aspects of the ForensicVM interface.
3. **Modify Scaling Mode**: - **Scaling Mode Adjustment**: Inside the settings, find the option labeled **"Scaling mode."** From the available choices, select **"Local Scaling."** This adjustment ensures the interface perfectly fits within your screen, displaying all elements in their entirety.



Settings

☑ Shared Mode

☐ View Only

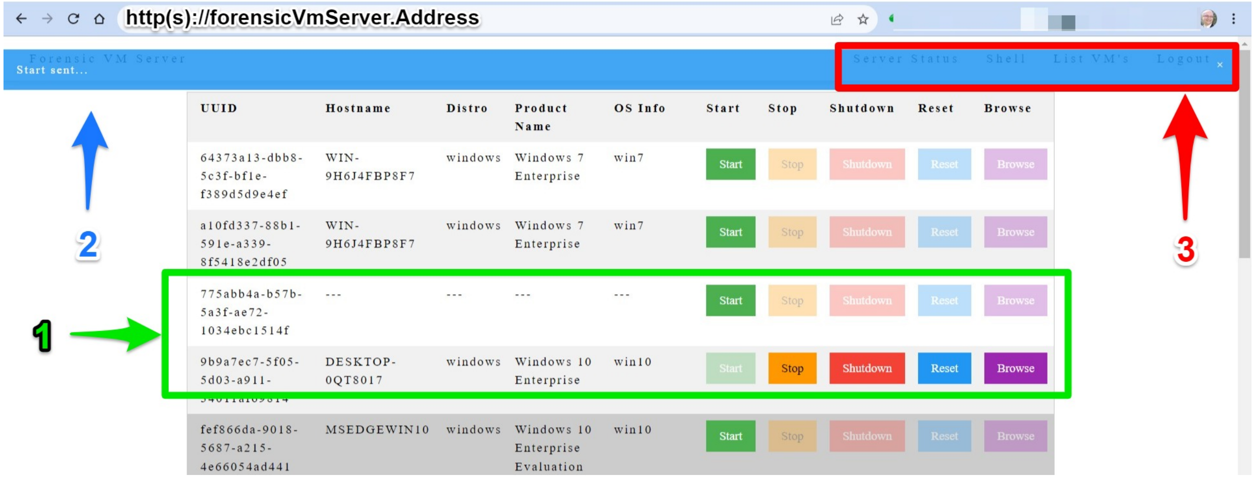
☐ Clip to Window

Scaling Mode: Local Scaling

Fig. 5.5: A visual representation showcasing the process of adjusting the webscreen scaling to "Local Scaling" for an optimized, full-screen experience.

5.5 ForensicVM Server Web Control Interface

For enhanced collaboration, remote forensic investigators have the capability to log into a dedicated web interface. This platform not only facilitates shared control of the remote web interface but also empowers multiple investigators to access the same ForensicVM simultaneously. This multi-user functionality enables diverse investigative actions such as capturing screenshots, collecting potential evidences onto the evidence disk, and initiating video recordings.



Start sent...

UUID	Hostname	Distro	Product Name	OS Info	Start	Stop	Shutdown	Reset	Browse
64373a13-dbb8-5c3f-bf1e-f389d5d9e4ef	WIN-9H6J4FBP8F7	windows	Windows 7 Enterprise	win7	Start	Stop	Shutdown	Reset	Browse
a10fd337-88b1-591e-a339-8f5418e2df05	WIN-9H6J4FBP8F7	windows	Windows 7 Enterprise	win7	Start	Stop	Shutdown	Reset	Browse
775abb4a-b57b-5a3f-ae72-1034ebc1514f	---	---	---	---	Start	Stop	Shutdown	Reset	Browse
9b9a7ec7-5f05-5d03-a911-	DESKTOP-0QT8017	windows	Windows 10 Enterprise	win10	Start	Stop	Shutdown	Reset	Browse
fef866da-9018-5687-a215-4e66054ad441	MSEDGEWIN10	windows	Windows 10 Enterprise Evaluation	win10	Start	Stop	Shutdown	Reset	Browse

Fig. 5.6: A visual representation of the ForensicVM Server Web Control Interface

Interface Breakdown:

- **(1) VM Control Options:**
  - **Start**: Power on the ForensicVM.
  - **Stop**: Power off the ForensicVM.
  - **Shutdown**: Properly shut down the ForensicVM, ensuring all processes are terminated correctly.
  - **Reset**: Reboot the ForensicVM.
  - **Browse**: Launch the ForensicVM's web console, offering a visual interface to the VM.
- **(2)** Notification Area: A dedicated space where various system communications such as messages, warnings, and error alerts are displayed.
- **(3) Server Management and Utilities:**
  - **Server Status (Netdata)**: Provides real-time performance metrics and monitoring using Netdata.
  - **Shell (webshell)**: Access to an SSH-over-web interface, allowing for direct server interactions.
  - **List VM**: Refresh and display the list of existing virtual machines on the server.
  - **Metrics**: 1) Export virtualization gather metrics as excel document. 2) Export analysis as a word or latex document.
  - **Logout**: Facilitates logging out of the web interface, ensuring secure closure of sessions.

After familiarizing yourself with ForensicVM, you may want to explore more advanced topic. Refer to the respective sections in this documentation for more information.

CHAPTER

SIX

PRODUCT OVERVIEW

ForensicVM is a powerful tool in digital forensics. It simplifies the investigation process by allowing the virtualization and management of forensic images.

6.1 ForensicVM Architecture

ForensicVM is composed of two main components:

- **The Client**: The client provides a user-friendly interface for managing forensic images, allowing users to create, run, and decommission instances as needed. It supports a variety of forensic image formats, ensuring compatibility with a wide range of existing tools and workflows.
- **The Hypervisor**: The hypervisor is responsible for the execution of the virtualized forensic images. It manages resources and isolation between instances, ensuring that each virtual machine runs effectively and securely.

6.2 Understanding the Interface

ForensicVM's interface is designed with usability in mind. It provides a clear view of the current state of your forensic images, including active instances, and the status of any ongoing analysis tasks. It also provides easy access to ForensicVM's suite of analysis tools, making it simple to start investigating a forensic image.

The Forensic Virtual Machine offers a plethora of features tailored to aid forensic analysts during their investigations. These features are systematically organized and can be accessed from various zones of the Autopsy interface. Each zone provides specific tools and functionalities, ensuring a seamless and comprehensive analysis experience.

In the table below, the distribution of features across the different zones of the interface is highlighted. This is to help users quickly identify where to locate and how to use each feature, maximizing efficiency and precision in their forensic operations.

Table 6.1: Features and Location

Feature	Web	Screer	Plugin	Autopsy	External
Convert Forensic Image to a Forensic Virtual Machine	.	.	X	.	.
• *Method 1: Copy the Local Forensic Image to a New Forensic Virtual Machine on the Server*	.	.	X	.	.

continues on next page

Table 6.1 – continued from previous page

Feature	Web	Screen	Plugin	Autopsy	External
- *Method 2: Link the Local Forensic Image to a New Forensic Virtual Machine on the Server*	.	.	X	.	.
Gather Evidence Using the Evidence Disk	.	.	X	.	.
- *Evidence Disk Creation*	.	X	X	.	.
- *Collecting Evidence: A Step-by-Step Guide*	.	X	.	.	.
- *Recreate Evidence Disk*	.	.	X	.	.
- *Import Possible Evidence Disk into Autopsy*	.	.	X	.	.
Deletion of ForensicVM at Investigation Conclusion	.	.	X	.	.
Fine-Tuning ForensicVM	.	.	X	.	.
Media Management in ForensicVM: Leveraging ISOs for Enhanced Forensic Investigations	.	X	X	.	.
- *Uploading an ISO to the ForensicVM Server*	.	.	X	.	.
- *List Remote ISO Files*	.	X	X	.	.
- *Insert ISO / Web Insert CD-ROM*	.	X	X	.	.
- *Run programs and utilities from ISO*	.	X	.	.	.
- *Bootable Media*	.	X	.	.	.
Making, Downloading, and Analyzing a Memory Dump (memory_dump_vm)	.	.	X	X	X
- *Making and download a Memory Dump*	.	.	X	.	.
- *Importing and Analyzing a Memory Dump in Autopsy*	.	.	.	X	X
Netdata on ForensicVM Server	X	.	X	.	.
Managing the Network Card to Capture and Analyse Network Traffic	.	X	X	.	X

continues on next page

Table 6.1 – continued from previous page

Feature	Web	Screer	Plu-gin	Au-topsy	Ex-ter-nal
- *Enable the Network Card*	.	X	X	.	.
- *Reseting the Operating System Network Card*	.	X	.	.	.
- *Disable the Network Card*	.	X	X	.	.
- *Download Wireshark pcap Files*	.	.	X	.	.
- *Analyze network traffic in Wireshark*	.	.	.	.	X
Open or Browse the Forensic Virtual Machine (VM)	X	X	X	.	.
Plugins - Security Bypass Utilities	.	.	X	.	.
- *Browsing Available Plugins*	.	.	X	.	.
- *Executing Plugins*	.	.	X	.	.
Resetting the Virtual Machine (VM)	X	X	X	.	.
Making and importing Screenshots	.	X	X	X	.
- *Making screenshots*	.	X	X	.	.
- *Downloading Screenshots as a ZIP File*	.	.	X	.	.
- *Importing Screenshots to Autopsy Software*	.	.	.	X	.
Shutting Down the Virtual Machine (VM)	X	X	X	.	.
Snapshots in ForensicVM: A Crucial Asset for Investigators	.	.	X	.	.
- *Create a new snapshot*	.	.	X	.	.
- *List Remote Snapshots*	.	.	X	.	.
- *Select and Rollback a Snapshot*	.	.	X	.	.
- *Delete a Snapshot*	.	.	X	.	.

continues on next page

Table 6.1 – continued from previous page

Feature	Web	Screer	Plugin	Autopsy	External
Starting the Virtual Machine (VM)	X	X	X	.	.
Stopping the Virtual Machine (VM)	X	X	X	.	.
Recording Video from a Forensic Virtual Machine	.	X	.	X	.
• *Record a video from the forensicVM*	.	X	.	.	.
• *Stop the video recording*	.	X	.	.	.
• *Download video recording*	.	X	.	.	.
• *Import video recording for analysis in Autopsy Software*	.	.	.	X	.
Chain of Custody Management in ForensicVM	.	X	.	.	.
Virtual Introspection	.	X	.	.	.
WebShell for Remote Administration	X	.	X	.	.
DEBUG: Remote ssh to folder	.	.	X	.	.

Table caption meaning:

- **Web** = ForensicVM Main Web Interface
- **Screen** = ForensicVM Web Remote Screen
- **Plugin** = ForensicVM Autopsy Client Plugin Interface
- **Autopsy** = Basis Technology Autopsy Software
- **External** = External Software: Volatility, wireshark, etc…

6.3 Plugin Architecture

One of the key features of ForensicVM is its plugin architecture, which enables the community to extend its functionality and interact with forensic images in innovative ways. This open architecture fosters the development of new software that can interact with forensic virtual images, providing flexibility and promoting active community involvement.

Through the plugin architecture, developers can create tools to perform a variety of tasks, including but not limited to:

- **Password Administration**: Reset forgotten passwords or generate new administrator accounts to gain access to the systems encapsulated in the forensic image.
- **Hibernate File Management**: Remove hibernation files to remove state of the system at the time of hibernation.
- **Data Extraction and Analysis**: Extract and analyze data from a forensic image to uncover evidence or gain insights into the operation of the system.

By contributing plugins to the community, developers can help to improve ForensicVM, enriching it with new features and capabilities. Moreover, by utilizing the plugins developed by the community, users can tailor ForensicVM to their specific needs, creating a more versatile and powerful forensic analysis environment.

You can contribute at: https://github.com/nunomourinho/forensicVM-Plugins

CHAPTER

SEVEN

USING FORENSICVM

This section provides a detailed guide on how to use ForensicVM in your forensic analysis.

7.1 Running Autopsy Forensic VM Plugin

To efficiently use the Autopsy ForensicVM plugin, it's essential to initialize a new case within the Autopsy framework and then seamlessly integrate a new data source. Below, the comprehensive procedure is outlined:

1) **Add a New Case to Autopsy**

   Initiate the Autopsy application and from the wizard interface, choose the option to add a new case. This is the first step in creating a structured environment for your forensic analysis.

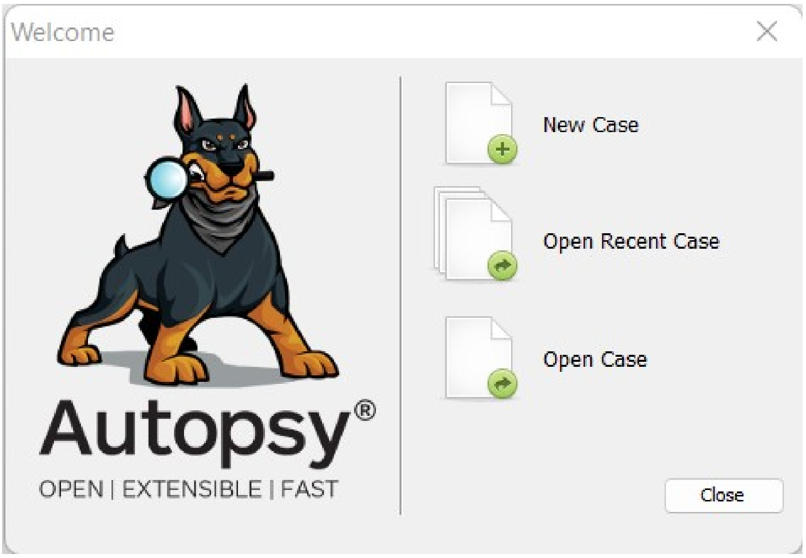


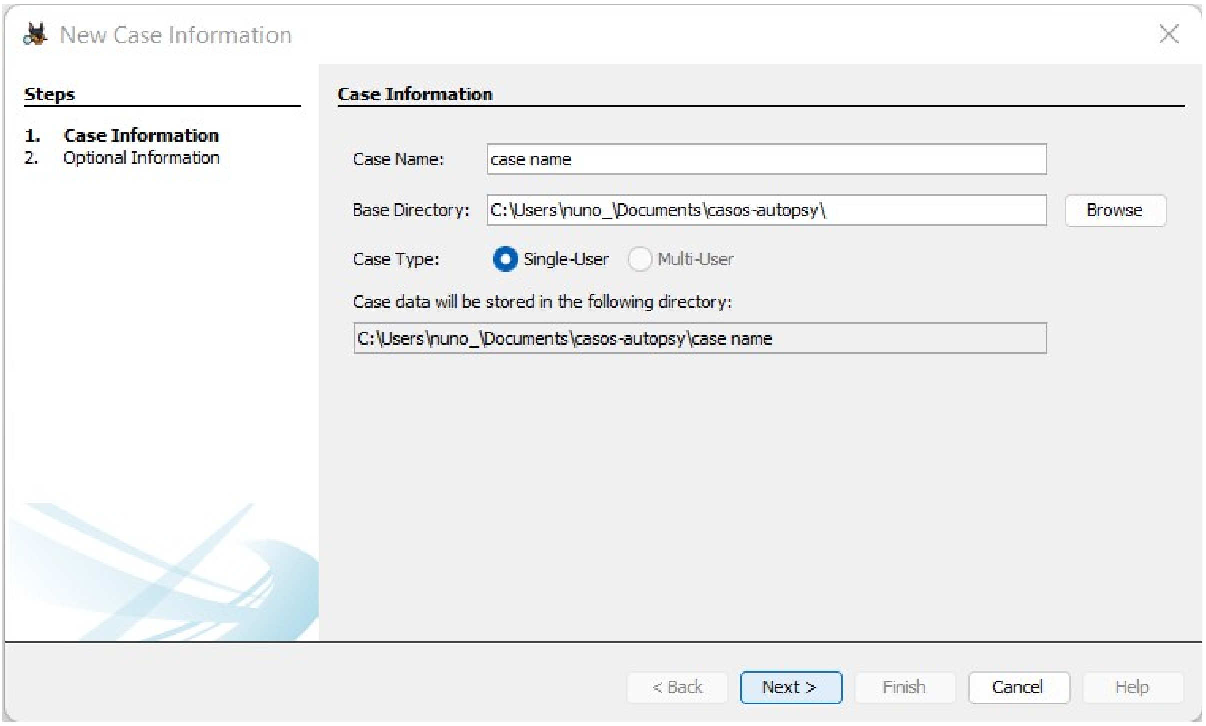
Fig. 7.1: Add a New Case to Autopsy

2) **Fill in Case Name in** Case Information

   Once the case addition window pops up, provide a unique and descriptive name for your case. This helps in distinguishing it from other cases in the future.

3) **Fill Optional Information**

   Here, you can include additional details about the case. While this is optional, it's recommended to fill in as much information as possible for thorough documentation.



Case Name: case name

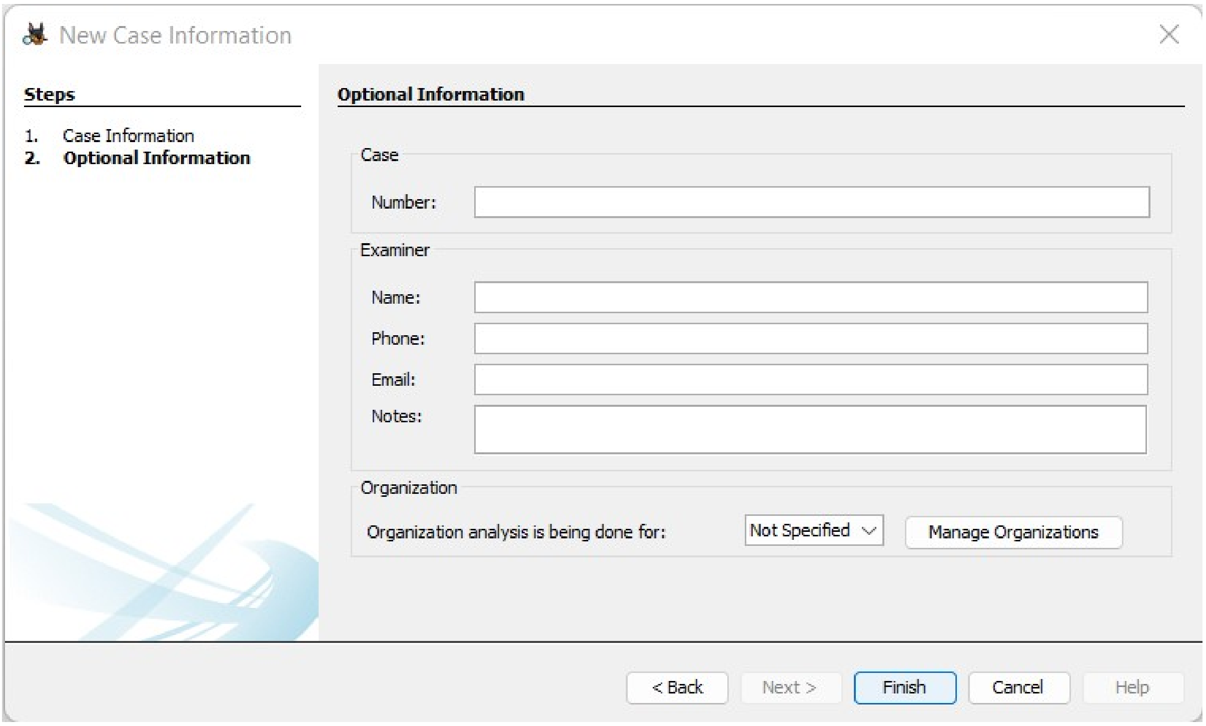
Base Directory: C:\Users\nuno_\Documents\casos-autopsy\

Case Type: ● Single-User ○ Multi-User

Case data will be stored in the following directory:

C:\Users\nuno_\Documents\casos-autopsy\case name

Fig. 7.2: Fill in Case Name in Case Information

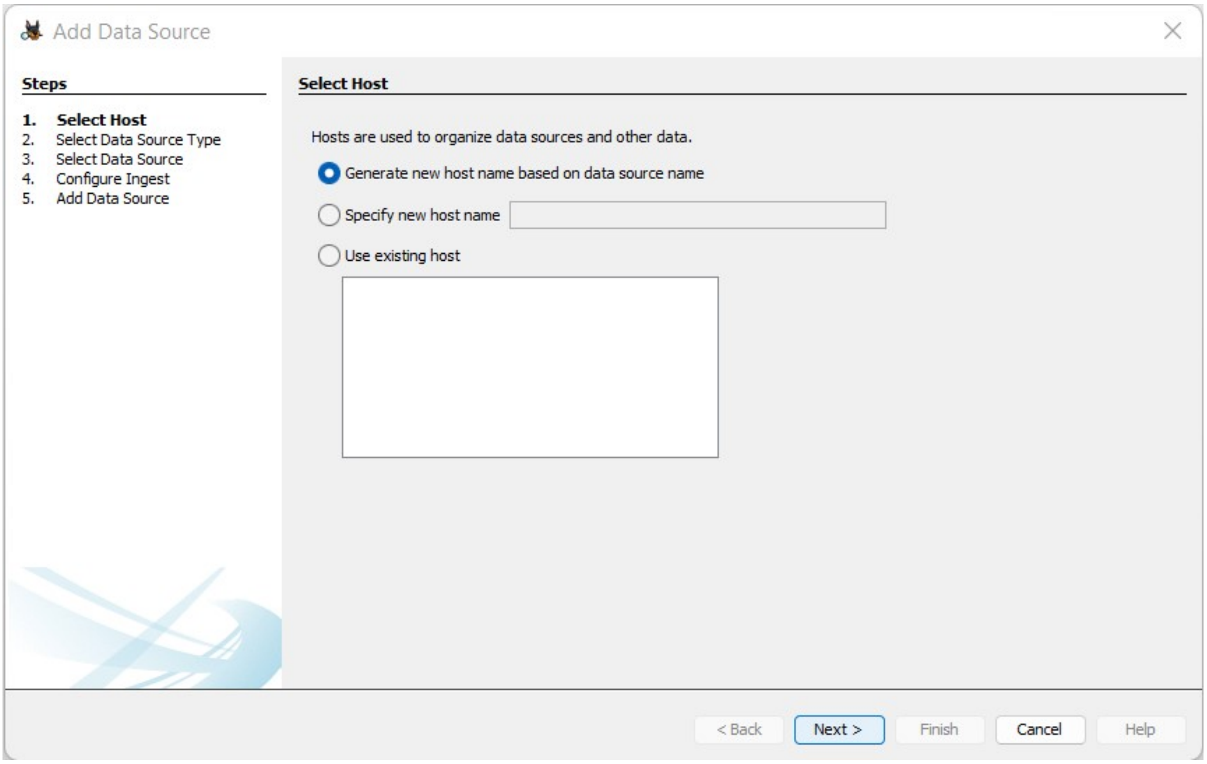


Organization analysis is being done for: Not Specified

Fig. 7.3: Fill Optional Information

4) **Choose Host Options**

   Decide on the host configuration for this case. You can either: - Generate a new host using the data source parameters. - Specify a new host name manually. - Or, utilize an existing host from a previous case or configuration.



Add Data Source

Steps

1. **Select Host**
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source

Select Host

Hosts are used to organize data sources and other data.

● Generate new host name based on data source name

○ Specify new host name

○ Use existing host

Fig. 7.4: Choose Host Options

5) **Select** Data Source **Type as** “Disk Image or VM File”

   Choose the type of data source you’re incorporating. For this procedure, select “term:*Disk Image or VM File*”, which allows Autopsy to process VM images and disk snapshots.

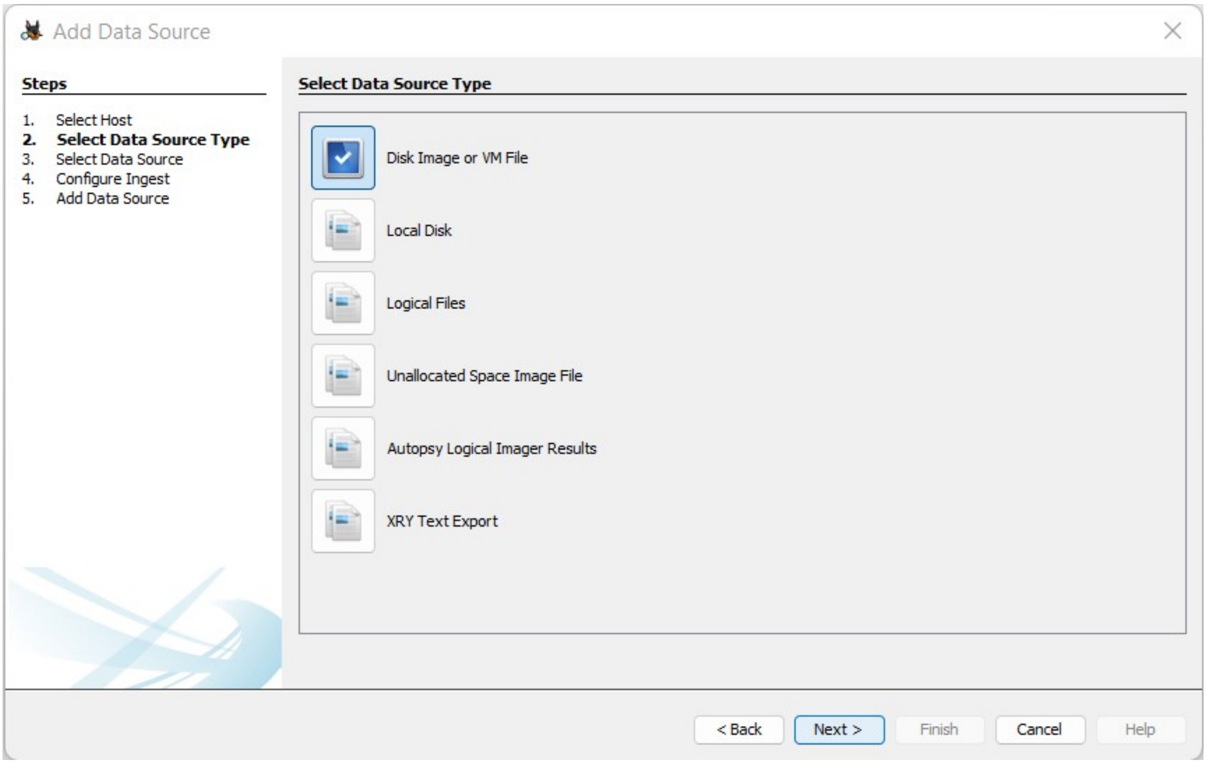
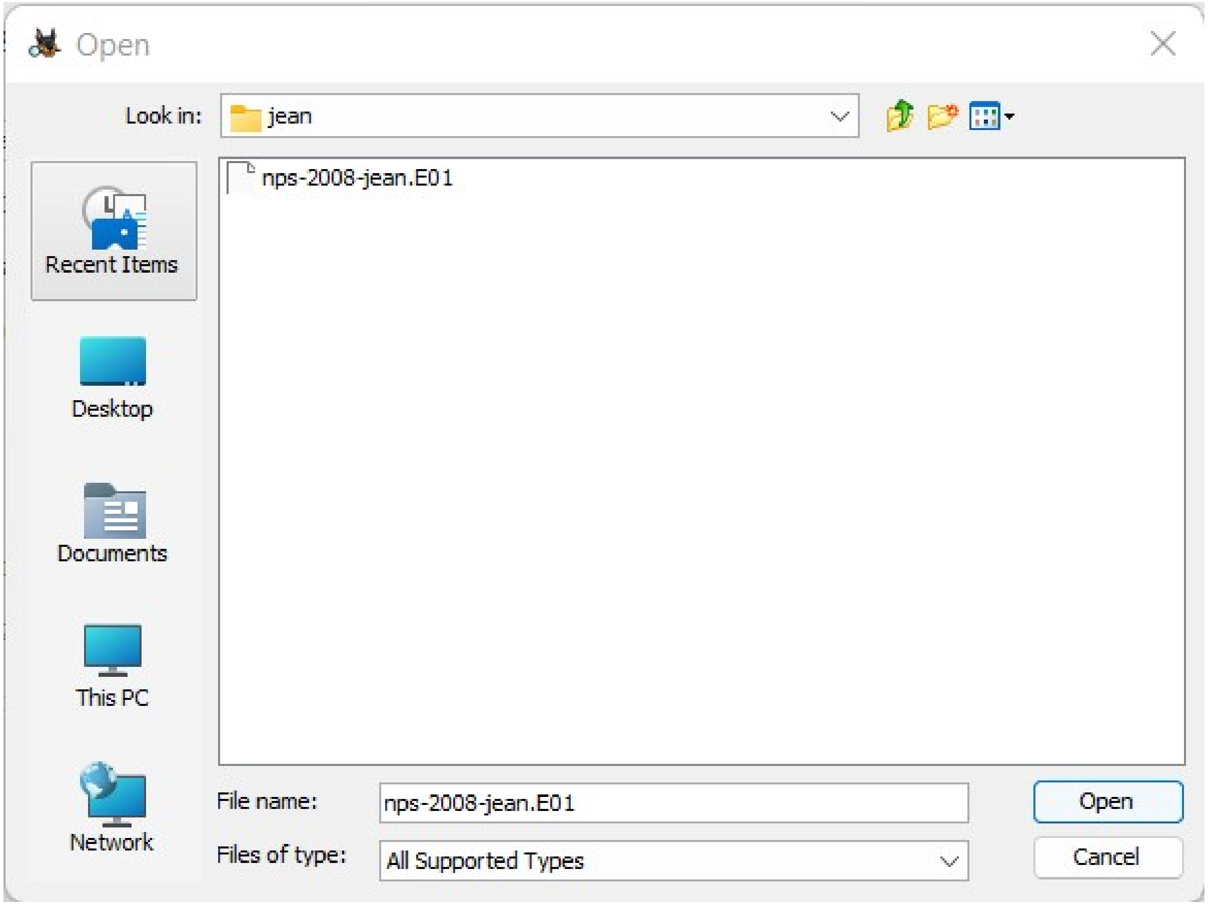


Fig. 7.5: Select Data Source Type

6) **Browse and Choose Your** Forensic Image

   Navigate through your file system and pick the appropriate forensic image or VM file. Ensure that the chosen file is compatible and accessible.



Look in: jean

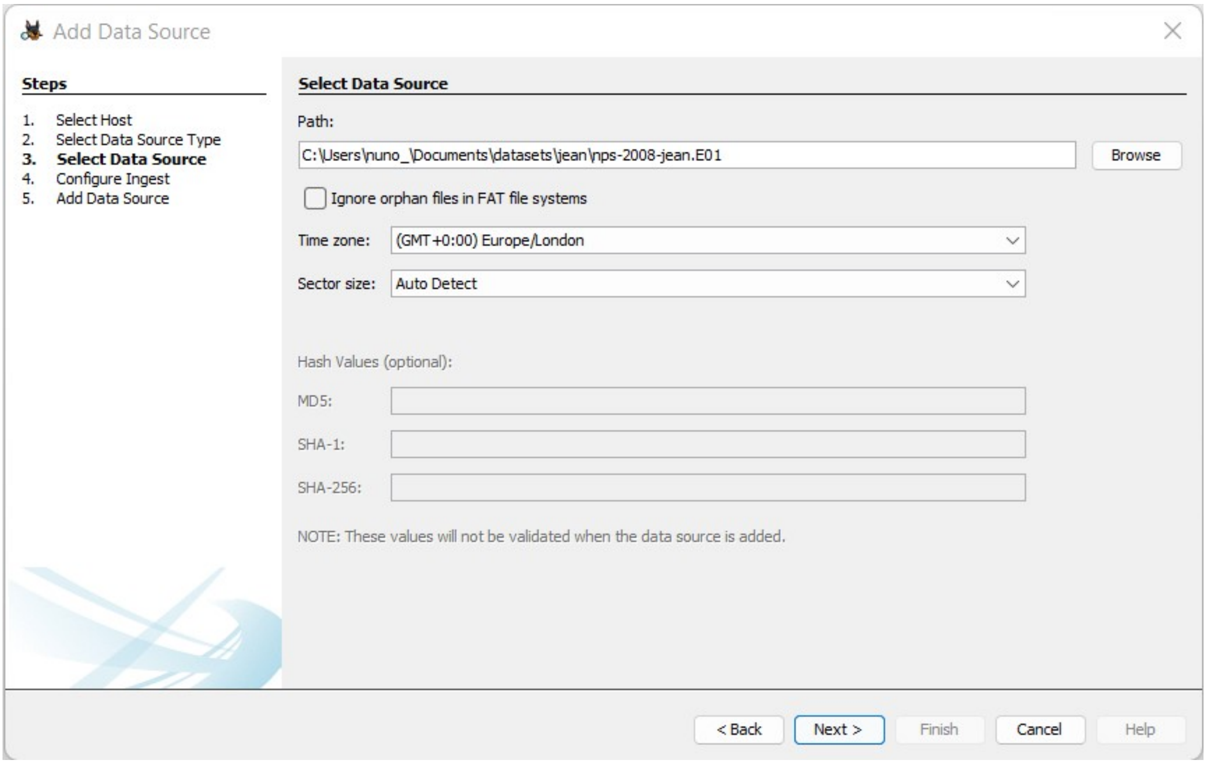
File name: nps-2008-jean.E01

Files of type: All Supported Types

Fig. 7.6: Choose Your Forensic Image

7) **Select Extra Parameters Like** Time Zone **and** Sector Size

   Fine-tune your forensic analysis by selecting the relevant time zone and determining the sector size. These parameters help in accurate data extraction and interpretation.



Add Data Source

Steps

1. Select Host
2. Select Data Source Type
3. **Select Data Source**
4. Configure Ingest
5. Add Data Source

Select Data Source

Path: C:\Users\nuno_\Documents\datasets\jean\nps-2008-jean.E01

□ Ignore orphan files in FAT file systems

Time zone: (GMT+0:00) Europe/London

Sector size: Auto Detect

Hash Values (optional):

MD5:

SHA-1:

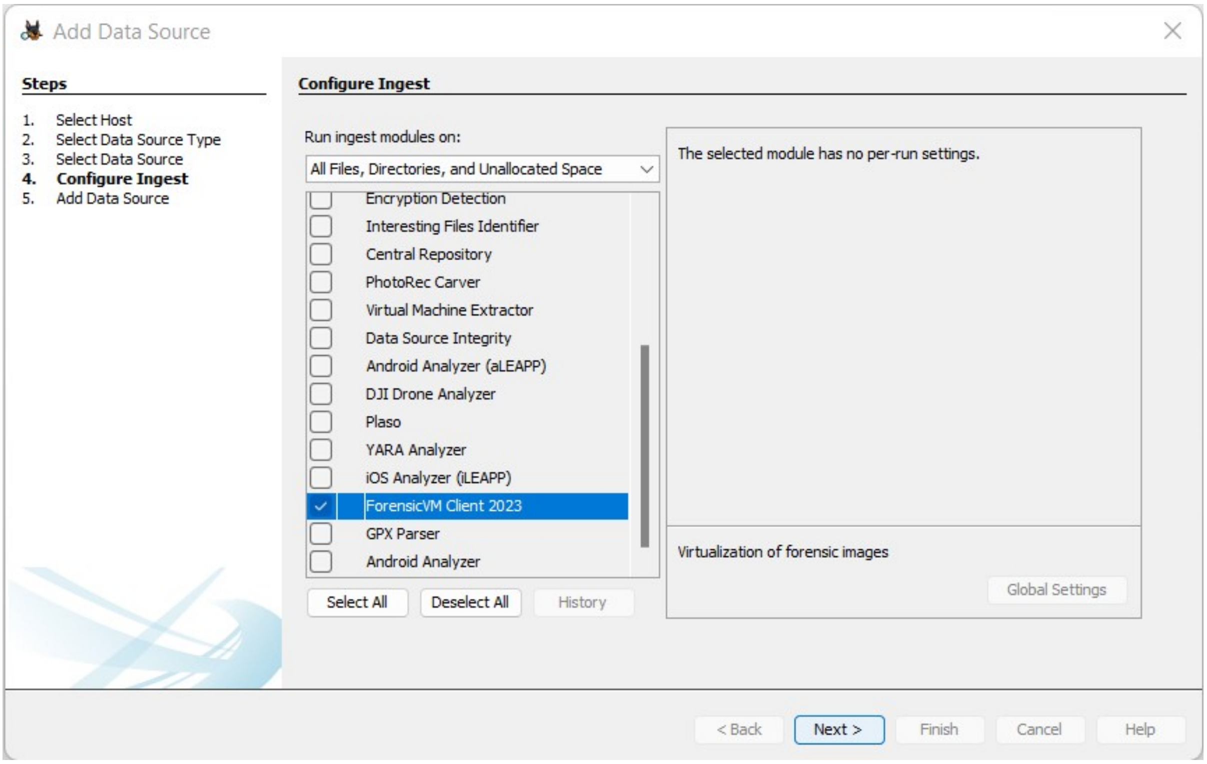
SHA-256:

NOTE: These values will not be validated when the data source is added.

Fig. 7.7: Select Extra Parameters

8) **Configure the** Python **Ingest Plugin to Run and Select the** ForensicVM Client Plugin

   Activate the Python Ingest Plugin for automated data ingestion. Also, ensure to select the ForensicVM Client plugin, which is pivotal for the VM forensic analysis.



Add Data Source

Steps

1. Select Host
2. Select Data Source Type
3. Select Data Source
4. **Configure Ingest**
5. Add Data Source

Configure Ingest

Run ingest modules on:

All Files, Directories, and Unallocated Space

- □ Encryption Detection
- □ Interesting Files Identifier
- □ Central Repository
- □ PhotoRec Carver
- □ Virtual Machine Extractor
- □ Data Source Integrity
- □ Android Analyzer (aLEAPP)
- □ DJI Drone Analyzer
- □ Plaso
- □ YARA Analyzer
- □ iOS Analyzer (iLEAPP)
- ☑ ForensicVM Client 2023
- □ GPX Parser
- □ Android Analyzer

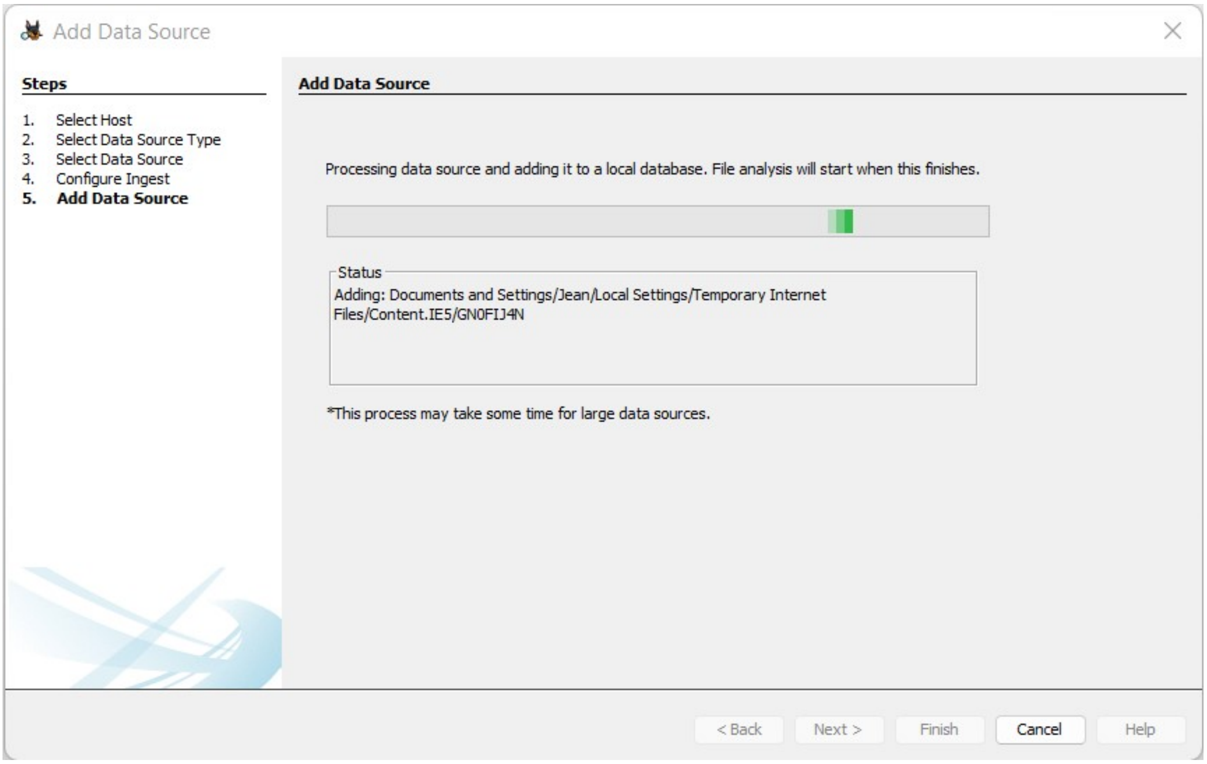
The selected module has no per-run settings.

Virtualization of forensic images

Fig. 7.8: Configure the :term:Python`` Ingest Plugin

9) **Monitor the** Data Source **Processing Progress**

As the data gets processed, an intuitive progress bar displays the ongoing activities and the completion percentage. Keep an eye on this to gauge the processing speed and potential completion time.



Processing data source and adding it to a local database. File analysis will start when this finishes.

Status
Adding: Documents and Settings/Jean/Local Settings/Temporary Internet Files/Content.IE5/GN0FIJ4N

*This process may take some time for large data sources.

Fig. 7.9: Data Source Processing Progress

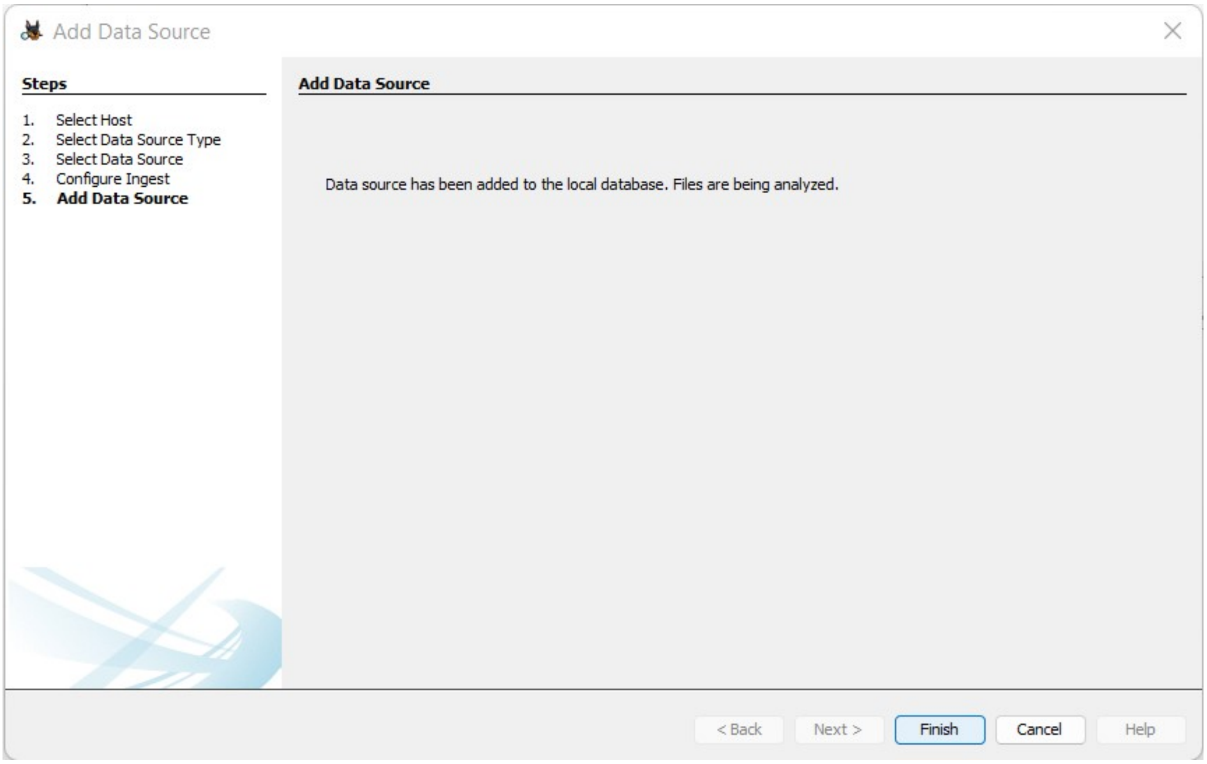
10) **Await the** ForensicVM Loader**'s Initialization**

The ForensicVM Loader will make a brief appearance. This indicates that the plugin is gearing up for execution. It will automatically close once the plugin is fully initialized.

Fig. 7.10: ForensicVM Loader Initialization

11) **Complete the Procedure and Minimize Autopsy Window**

    Click on the “Finish” button to round off the ‘Add Data Source’ wizard. For better visibility and multitasking, it’s advisable to minimize the main Autopsy window at this juncture.

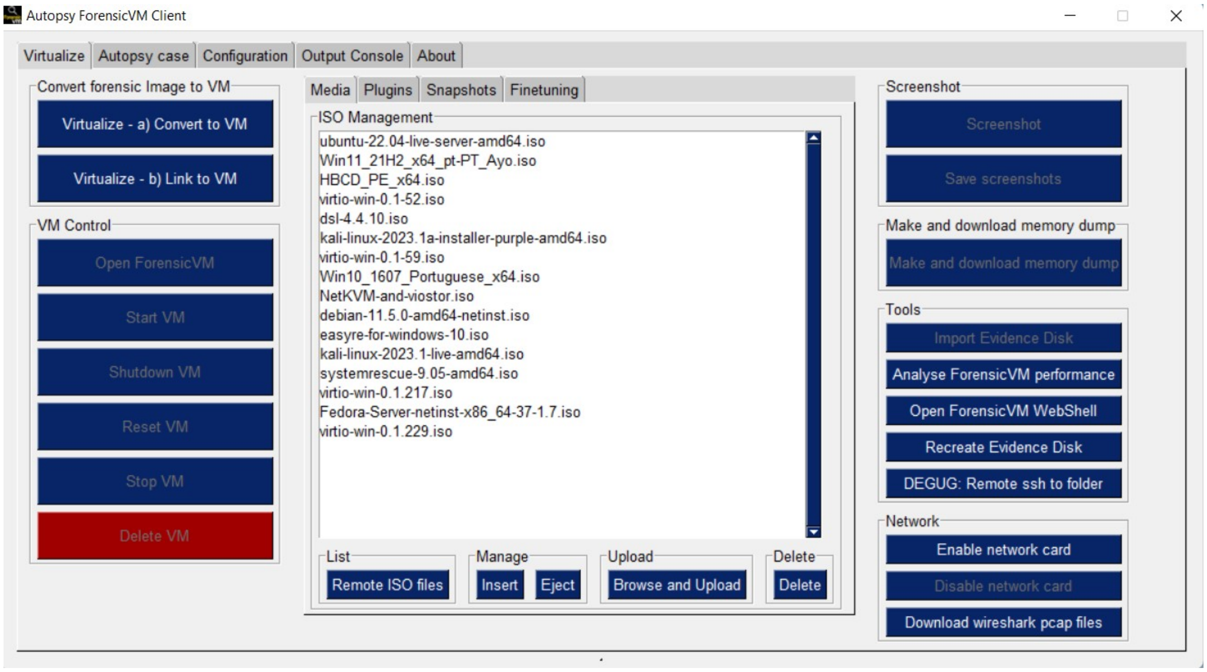


Data source has been added to the local database. Files are being analyzed.

Fig. 7.11: Finish Data Source Wizard

12) **Engage with the Autopsy ForensicVM Client** Plugin Interface

    Post the previous steps, the dedicated window for the Autopsy ForensicVM Client plugin will emerge. Here, you can conduct in-depth VM forensics using the myriad features offered by the plugin.



```
ubuntu-22.04-live-server-amd64.iso
Win11_21H2_x64_pt-PT_Ayo.iso
HBCD_PE_x64.iso
virtio-win-0.1-52.iso
dsl-4.4.10.iso
kali-linux-2023.1a-installer-purple-amd64.iso
virtio-win-0.1-59.iso
Win10_1607_Portuguese_x64.iso
NetKVM-and-viostor.iso
debian-11.5.0-amd64-netinst.iso
easyre-for-windows-10.iso
kali-linux-2023.1-live-amd64.iso
systemrescue-9.05-amd64.iso
virtio-win-0.1.217.iso
Fedora-Server-netinst-x86_64-37-1.7.iso
virtio-win-0.1.229.iso
```

Fig. 7.12: ForensicVM Client Plugin Interface

7.2 Convert Forensic Image to a Forensic Virtual Machine

When aiming to convert a local forensic image to a remote forensic virtual machine on a server, two primary methods are prevalent:

1. Direct Copy to Server: This approach duplicates the forensic image, creating a new forensic virtual machine on the server. It grants comprehensive access and utility of the forensicVM, making it the ideal choice for collaborative remote investigations.
2. Link Creation: In this method, a link is forged between the local forensic image and a new counterpart on the server. Although it's swifter (given that the image isn't transferred to the remote server), there are limitations. The conversion and previewing are quick, yet initiating the machine locally is mandatory. The investigator must resort to the Autopsy client plugin to start the machine, as the web interface is incompatible due to the dependency on the original forensic image.

Steps for Both Methods:

1. **Initiate SSH Connection**: An SSH link is established with the forensicVM server.
2. **Reverse Connection Establishment**: This connection triggers a reverse connection to a read-only samba CIFS share, often known as a Windows share. This maneuver enables the server to access the Windows share containing the forensic image.
3. **Initiate Conversion**: Here, the type of forensic image is identified, followed by the selection of an appropriate tool on the server to mount the image to a virtual raw device. This is especially vital when images span across multiple files.

Note: This tool selection process ensures that the appropriate software is utilized for optimal conversion.

4. **Snapshot Creation**: An initial forensic image snapshot is generated. Acting as a base snapshot, it retains the state tied to the forensic image's virtual raw. This facilitates the installation of drivers without altering the forensic

image's state or information, preserving the sanctity of the evidence.

5. **Image Conversion**: The image undergoes a transformation into the qcow2 format - the favored format for KVM virtualization. It not only supports snapshots but also ensures the image only occupies the space used by the forensic image.
6. **Partition Detection**: The system identifies any partitions present within the image.
7. **Operating System Detection**: The OS inside each partition is discerned. If recognized, KVM-optimized virtual drivers get pre-installed, which will initiate upon the forensic virtual machine's first boot.
8. Fallback Conversion: If the OS remains unidentified, the VM undergoes a full conversion without any driver installations. While this could potentially enable booting, post-conversion, manual scrutiny and possible KVM driver installations are essential.
9. **Partition Absence Handling**: In the event no partitions are identified, a virtual partition gets generated alongside a virtual boot device. This procedure aids in converting partition images into complete images. However, the user must invest additional effort to adapt this image for booting. They might need supplementary tools, like a virtual CD-ROM, to rectify and make the VM operational.

Tip: It's crucial to regularly monitor the conversion process to ensure all steps are proceeding as expected and that any necessary adjustments can be made promptly.

7.2.1 Method 1: Copy the Local Forensic Image to a New Forensic Virtual Machine on the Server

Direct Copy to Server: This approach duplicates the forensic image, creating a new forensic virtual machine on the server. It grants comprehensive access and utility of the forensicVM, making it the ideal choice for collaborative remote investigations.

Conversion steps:

1. **Begin the Conversion**:

   Initiate the conversion process by clicking on the button titled "Virtualize - a) Convert to VM". This action sets the process in motion.

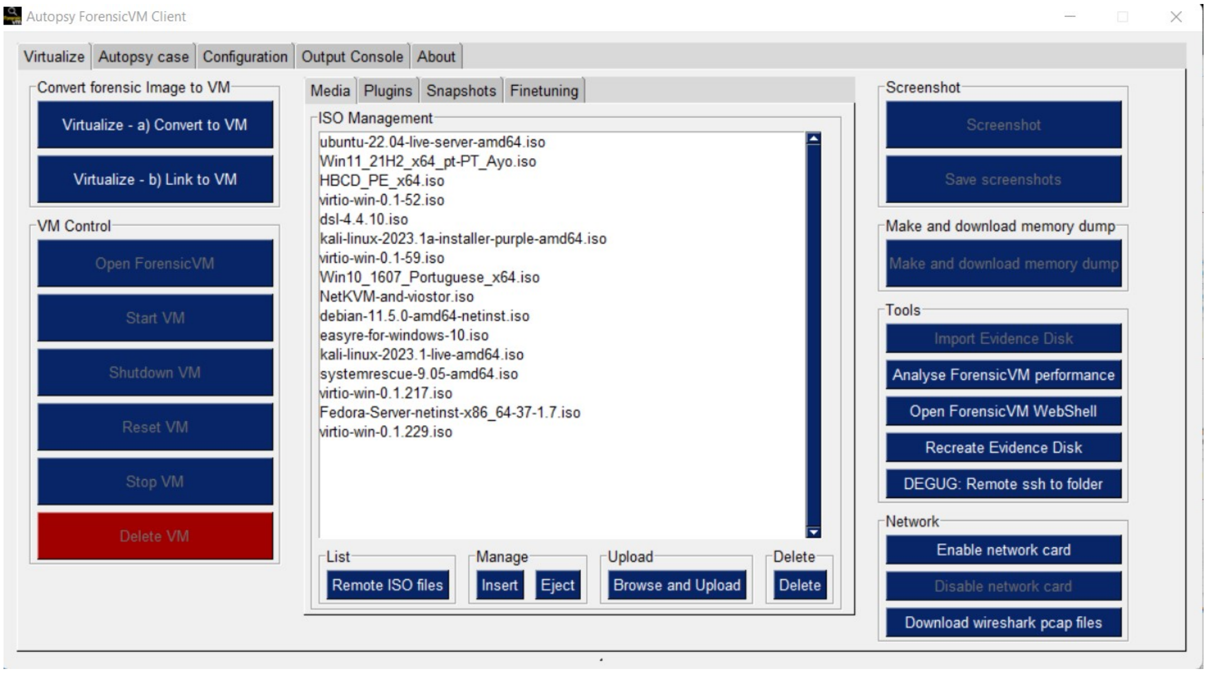
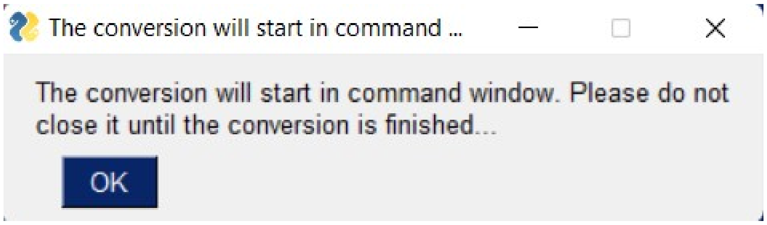

Autopsy ForensicVM Client
Virtualize
Autopsy case
Configuration
Output Console
About
Convert forensic Image to VM
Virtualize - a) Convert to VM
Virtualize - b) Link to VM
VM Control
Open ForensicVM
Start VM
Shutdown VM
Reset VM
Stop VM
Delete VM
Media
Plugins
Snapshots
Finetuning
ISO Management
ubuntu-22.04-live-server-amd64.iso
Win11_21H2_x64_pt-PT_Ayo.iso
HBCD_PE_x64.iso
virtio-win-0.1-52.iso
dsl-4.4.10.iso
kali-linux-2023.1a-installer-purple-amd64.iso
virtio-win-0.1-59.iso
Win10_1607_Portuguese_x64.iso
NetKVM-and-viostor.iso
debian-11.5.0-amd64-netinst.iso
easyre-for-windows-10.iso
kali-linux-2023.1-live-amd64.iso
systemrescue-9.05-amd64.iso
virtio-win-0.1.217.iso
Fedora-Server-netinst-x86_64-37-1.7.iso
virtio-win-0.1.229.iso
List
Remote ISO files
Manage
Insert
Eject
Upload
Browse and Upload
Delete
Delete
Screenshot
Screenshot
Save screenshots
Make and download memory dump
Make and download memory dump
Tools
Import Evidence Disk
Analyse ForensicVM performance
Open ForensicVM WebShell
Recreate Evidence Disk
DEGUG: Remote ssh to folder
Network
Enable network card
Disable network card
Download wireshark pcap files

Fig. 7.13: "Virtualize - a) Convert to VM" button

2. **Popup Confirmation**:

   Upon clicking the conversion button, a popup alert appears. This alert will display the message: "The conversion will start in a command window. Please do not close it until the conversion is finished…". Click on "OK" to commence the conversion process.

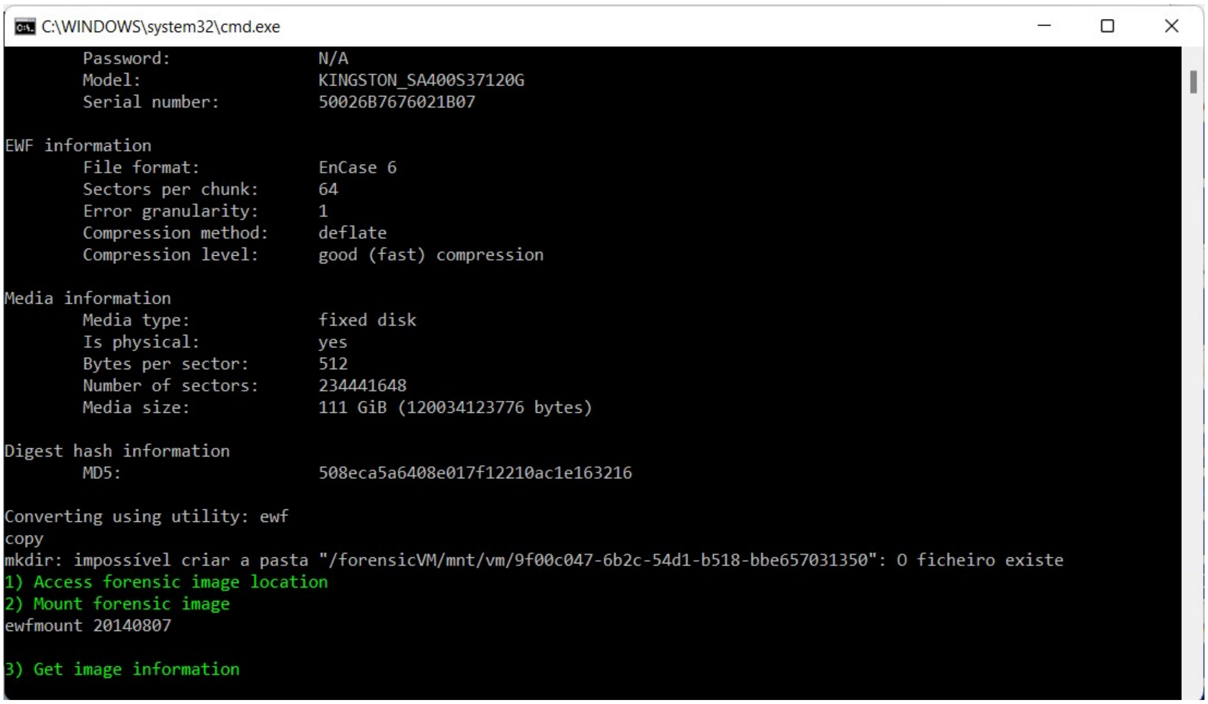


The conversion will start in command window. Please do not close it until the conversion is finished...

Fig. 7.14: Conversion Confirmation Popup

3. MS-DOS Command Window **Feedback**:

   A MS-DOS command window materializes post confirmation. This window is instrumental in detecting the image format, which will be visibly printed within. Ensure to keep an eye out for messages color-coded in green, indicating successful steps. However, should there be any errors, take note for future reference.



```
        Password:                N/A
        Model:                   KINGSTON_SA400S37120G
        Serial number:           50026B7676021B07

EWF information
        File format:             EnCase 6
        Sectors per chunk:       64
        Error granularity:       1
        Compression method:      deflate
        Compression level:       good (fast) compression

Media information
        Media type:              fixed disk
        Is physical:             yes
        Bytes per sector:        512
        Number of sectors:       234441648
        Media size:              111 GiB (120034123776 bytes)

Digest hash information
        MD5:                     508eca5a6408e017f12210ac1e163216

Converting using utility: ewf
copy
mkdir: impossível criar a pasta "/forensicVM/mnt/vm/9f00c047-6b2c-54d1-b518-bbe657031350": O ficheiro existe
1) Access forensic image location
2) Mount forensic image
ewfmount 20140807

3) Get image information
```

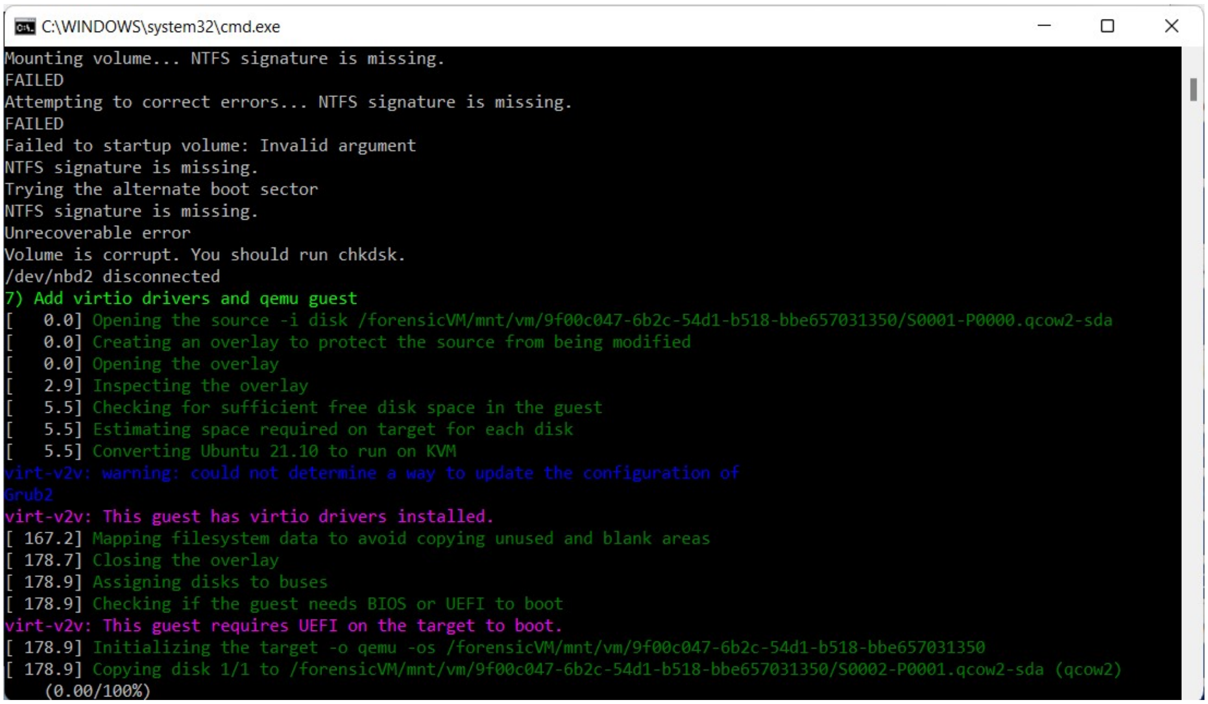
Fig. 7.15: MS-DOS Command Window Progress Display

4. **Driver Installation and Conversion Completion**:

   During this phase, the system installs the required KVM drivers. Various messages get displayed in this window. Here's a color code to understand them:

   - **Green**: Success messages.
   - **Blue**: Warnings.
   - **Magenta**: Special information messages.
   - **Red**: Error messages.

   The conversion progression is displayed as a percentage.

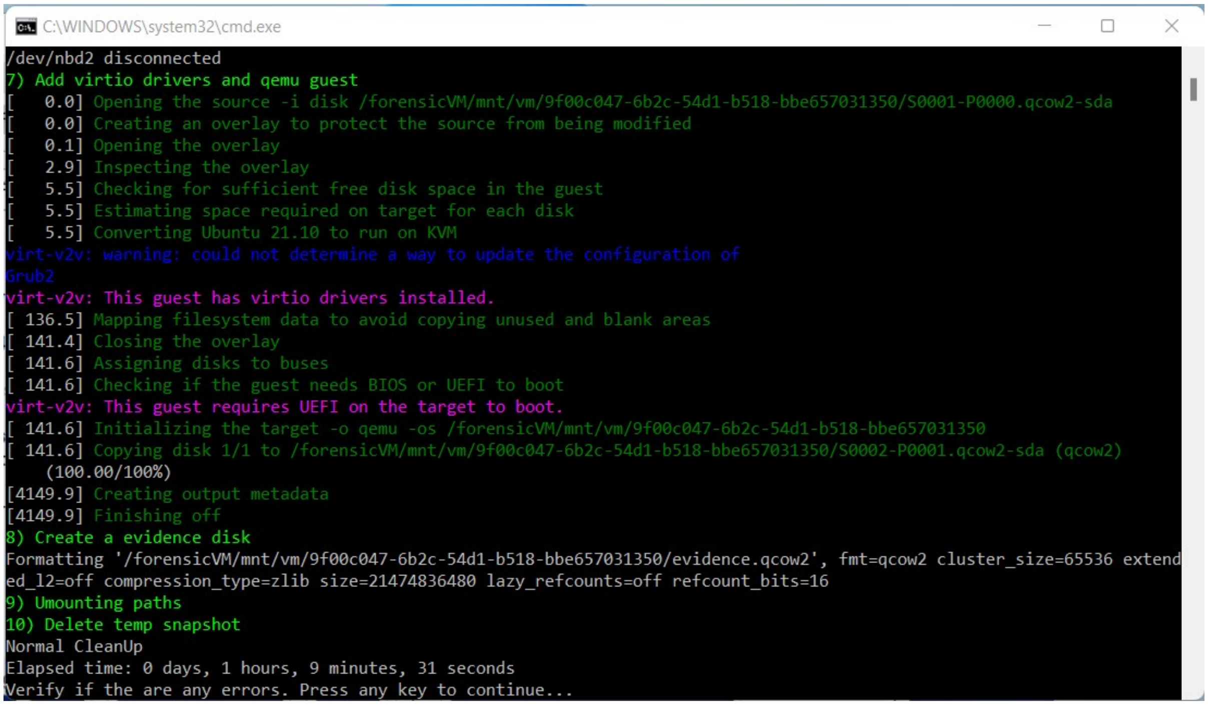


```
Mounting volume... NTFS signature is missing.
FAILED
Attempting to correct errors... NTFS signature is missing.
FAILED
Failed to startup volume: Invalid argument
NTFS signature is missing.
Trying the alternate boot sector
NTFS signature is missing.
Unrecoverable error
Volume is corrupt. You should run chkdsk.
/dev/nbd2 disconnected
7) Add virtio drivers and qemu guest
[   0.0] Opening the source -i disk /forensicVM/mnt/vm/9f00c047-6b2c-54d1-b518-bbe657031350/S0001-P0000.qcow2-sda
[   0.0] Creating an overlay to protect the source from being modified
[   0.0] Opening the overlay
[   2.9] Inspecting the overlay
[   5.5] Checking for sufficient free disk space in the guest
[   5.5] Estimating space required on target for each disk
[   5.5] Converting Ubuntu 21.10 to run on KVM
virt-v2v: warning: could not determine a way to update the configuration of
Grub2
virt-v2v: This guest has virtio drivers installed.
[ 167.2] Mapping filesystem data to avoid copying unused and blank areas
[ 178.7] Closing the overlay
[ 178.9] Assigning disks to buses
[ 178.9] Checking if the guest needs BIOS or UEFI to boot
virt-v2v: This guest requires UEFI on the target to boot.
[ 178.9] Initializing the target -o qemu -os /forensicVM/mnt/vm/9f00c047-6b2c-54d1-b518-bbe657031350
[ 178.9] Copying disk 1/1 to /forensicVM/mnt/vm/9f00c047-6b2c-54d1-b518-bbe657031350/S0002-P0001.qcow2-sda (qcow2)
    (0.00/100%)
```

Fig. 7.16: Conversion Progress Display

5. **Conversion completed**:

   Once completed, a success message paired with the elapsed time is showcased, signaling the end of the conversion.

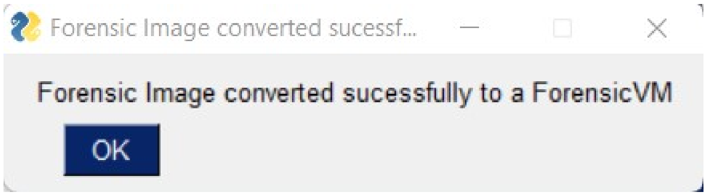


```
/dev/nbd2 disconnected
7) Add virtio drivers and qemu guest
[   0.0] Opening the source -i disk /forensicVM/mnt/vm/9f00c047-6b2c-54d1-b518-bbe657031350/S0001-P0000.qcow2-sda
[   0.0] Creating an overlay to protect the source from being modified
[   0.1] Opening the overlay
[   2.9] Inspecting the overlay
[   5.5] Checking for sufficient free disk space in the guest
[   5.5] Estimating space required on target for each disk
[   5.5] Converting Ubuntu 21.10 to run on KVM
virt-v2v: warning: could not determine a way to update the configuration of
Grub2
virt-v2v: This guest has virtio drivers installed.
[ 136.5] Mapping filesystem data to avoid copying unused and blank areas
[ 141.4] Closing the overlay
[ 141.6] Assigning disks to buses
[ 141.6] Checking if the guest needs BIOS or UEFI to boot
virt-v2v: This guest requires UEFI on the target to boot.
[ 141.6] Initializing the target -o qemu -os /forensicVM/mnt/vm/9f00c047-6b2c-54d1-b518-bbe657031350
[ 141.6] Copying disk 1/1 to /forensicVM/mnt/vm/9f00c047-6b2c-54d1-b518-bbe657031350/S0002-P0001.qcow2-sda (qcow2)
    (100.00/100%)
[4149.9] Creating output metadata
[4149.9] Finishing off
8) Create a evidence disk
Formatting '/forensicVM/mnt/vm/9f00c047-6b2c-54d1-b518-bbe657031350/evidence.qcow2', fmt=qcow2 cluster_size=65536 extend
ed_l2=off compression_type=zlib size=21474836480 lazy_refcounts=off refcount_bits=16
9) Umounting paths
10) Delete temp snapshot
Normal CleanUp
Elapsed time: 0 days, 1 hours, 9 minutes, 31 seconds
Verify if the are any errors. Press any key to continue...
```

Fig. 7.17: Conversion Completion Display

6. **Success Conversion Popup**:

   Once the image conversion completes, a success popup will appear confirming the conversion's successful completion.

   Forensic Image converted sucessfully to a ForensicVM

   Fig. 7.18: Screenshot of the success conversion popup.

7. **ForensicVM First Boot**:

   To boot up the machine for the first time, click the "Start" button available in the Autopsy ForensicVM Plugin.

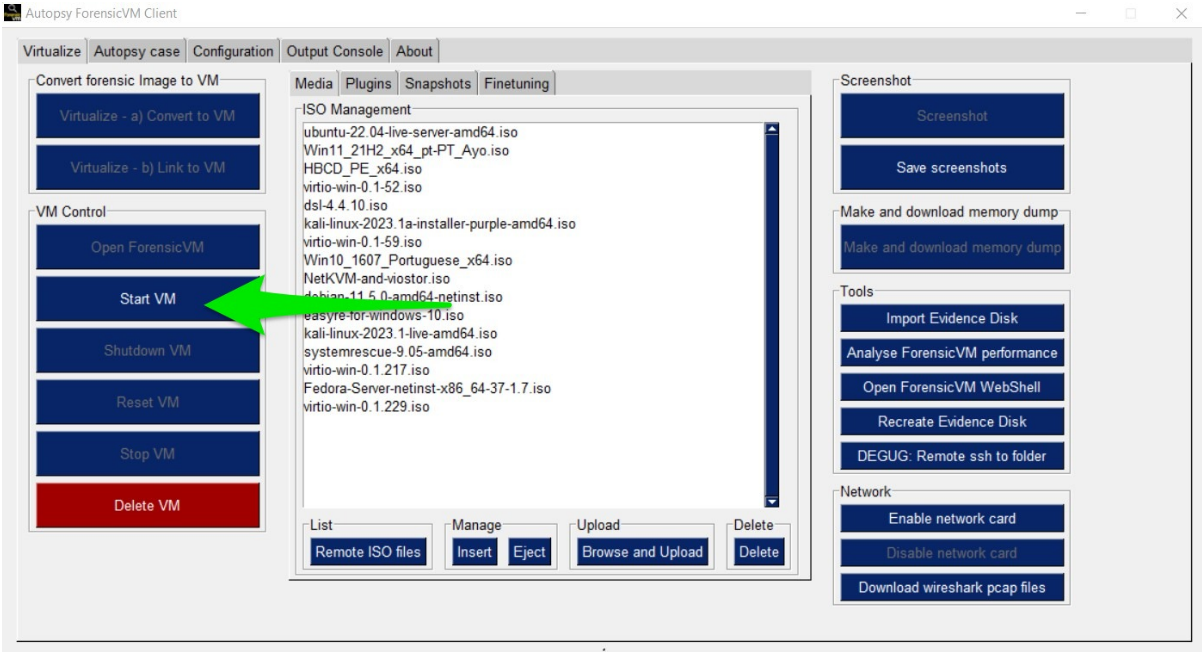
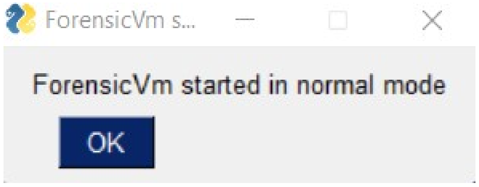

Autopsy ForensicVM Client
Virtualize
Autopsy case
Configuration
Output Console
About
Convert forensic Image to VM
Virtualize - a) Convert to VM
Virtualize - b) Link to VM
VM Control
Open ForensicVM
Start VM
Shutdown VM
Reset VM
Stop VM
Delete VM
Media
Plugins
Snapshots
Finetuning
ISO Management
ubuntu-22.04-live-server-amd64.iso
Win11_21H2_x64_pt-PT_Ayo.iso
HBCD_PE_x64.iso
virtio-win-0.1-52.iso
dsl-4.4.10.iso
kali-linux-2023.1a-installer-purple-amd64.iso
virtio-win-0.1-59.iso
Win10_1607_Portuguese_x64.iso
NetKVM-and-viostor.iso
debian-11.5.0-amd64-netinst.iso
easyre-for-windows-10.iso
kali-linux-2023.1-live-amd64.iso
systemrescue-9.05-amd64.iso
virtio-win-0.1.217.iso
Fedora-Server-netinst-x86_64-37-1.7.iso
virtio-win-0.1.229.iso
List
Remote ISO files
Manage
Insert
Eject
Upload
Browse and Upload
Delete
Delete
Screenshot
Screenshot
Save screenshots
Make and download memory dump
Make and download memory dump
Tools
Import Evidence Disk
Analyse ForensicVM performance
Open ForensicVM WebShell
Recreate Evidence Disk
DEGUG: Remote ssh to folder
Network
Enable network card
Disable network card
Download wireshark pcap files

Fig. 7.19: Screenshot of the "Start" button on the Autopsy ForensicVM Plugin.

8. **Informational Popup - Machine Started**:

   Post clicking the "Start" button, an informational popup will appear to inform you about the machine's status.

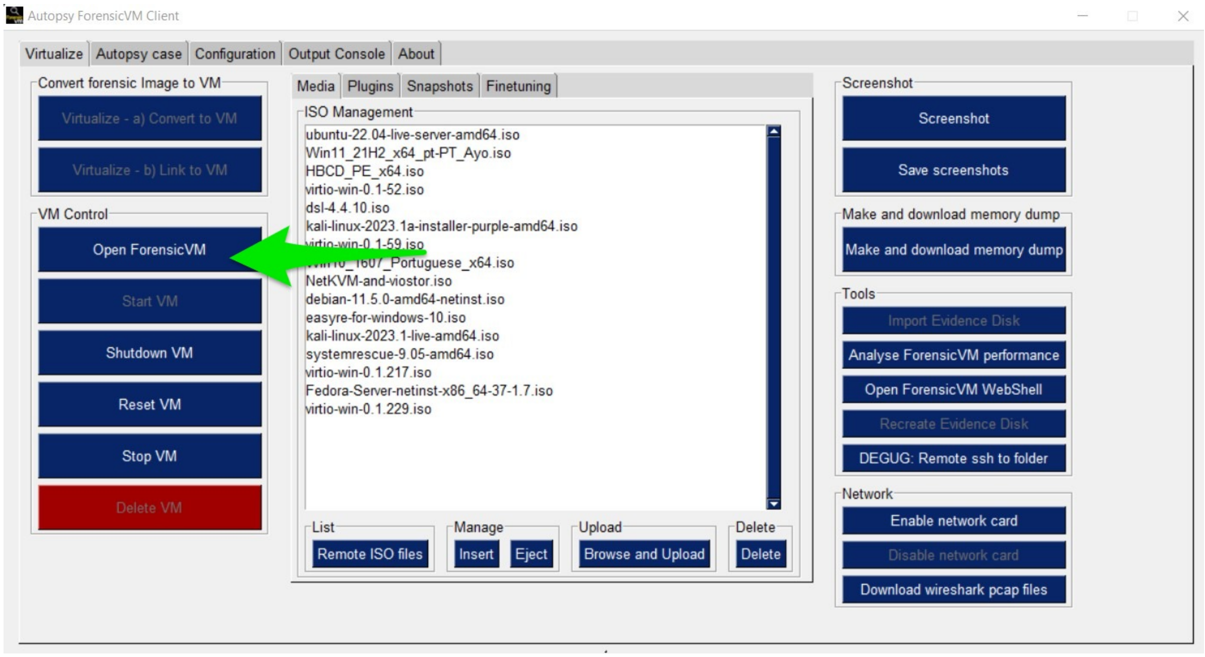


ForensicVm started in normal mode

Fig. 7.20: Screenshot of the informational popup after machine start.

9. **Opening the ForensicVM**:

   To access the ForensicVM's web screen interface, click the "Open ForensicVM" button. This interface will allow you to interact directly with the forensicVM.



```
ubuntu-22.04-live-server-amd64.iso
Win11_21H2_x64_pt-PT_Ayo.iso
HBCD_PE_x64.iso
virtio-win-0.1-52.iso
dsl-4.4.10.iso
kali-linux-2023.1a-installer-purple-amd64.iso
virtio-win-0.1-59.iso
Win10_1607_Portuguese_x64.iso
NetKVM-and-viostor.iso
debian-11.5.0-amd64-netinst.iso
easyre-for-windows-10.iso
kali-linux-2023.1-live-amd64.iso
systemrescue-9.05-amd64.iso
virtio-win-0.1.217.iso
Fedora-Server-netinst-x86_64-37-1.7.iso
virtio-win-0.1.229.iso
```

Fig. 7.21: Screenshot of the “Open ForensicVM” button.

10. **ForensicVM** Web Screen Interface:

    Once inside the web screen interface, click the prominent “Connect / Start” button to establish a connection with the forensicVM and view its virtual screen monitor.

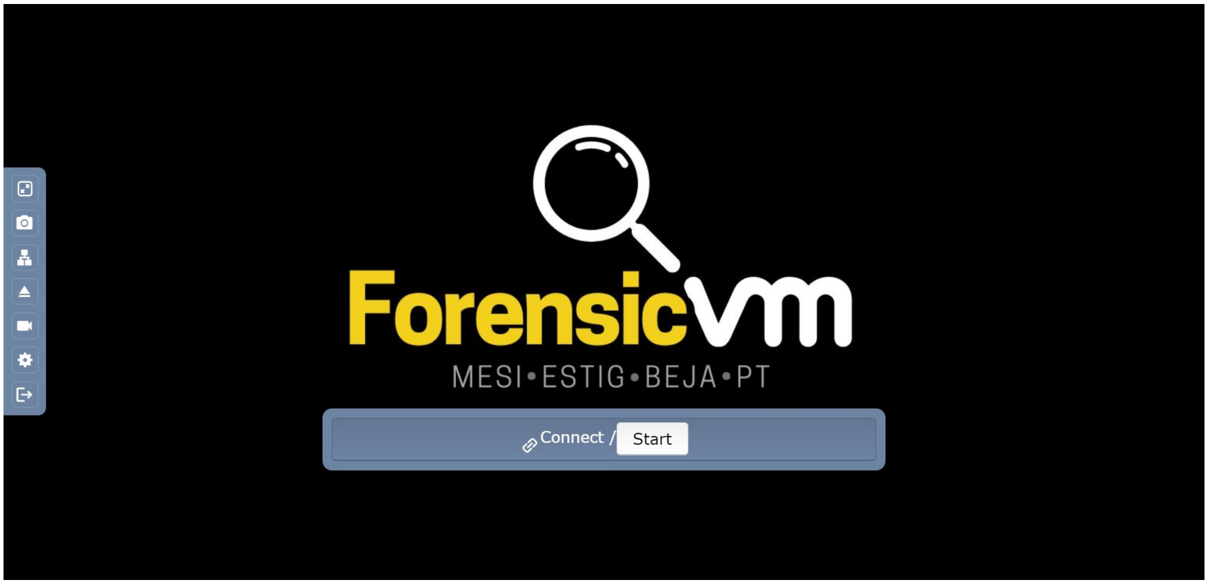


Fig. 7.22: Screenshot of the ForensicVM's "Connect / Start" button.

11. **Interact with the ForensicVM**:

    With the connection established, you can now freely interact with the forensicVM.

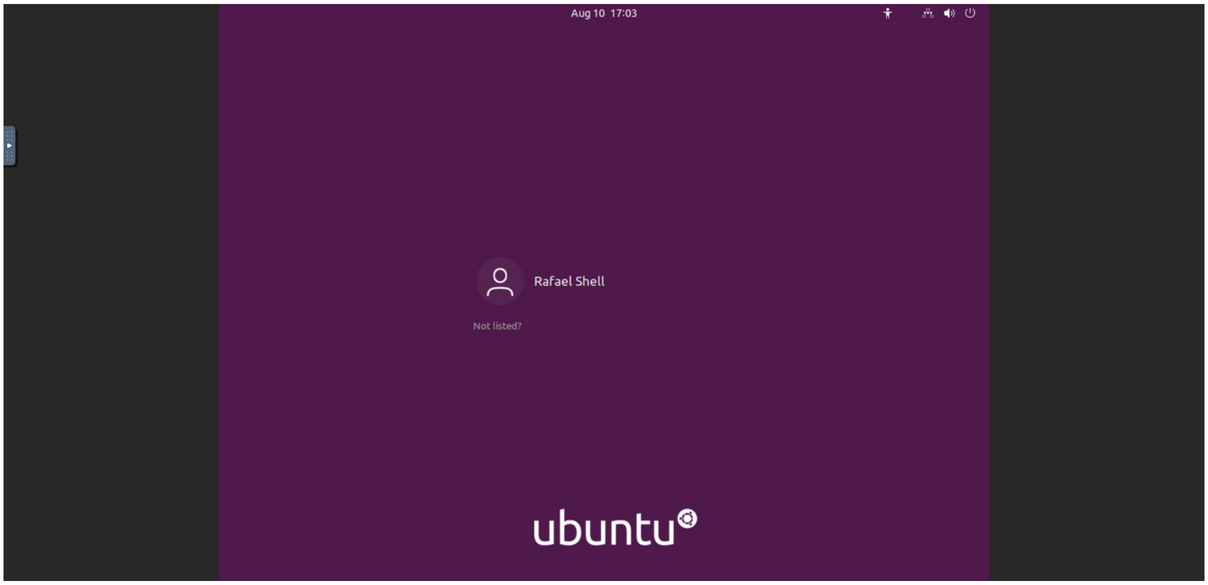


Fig. 7.23: Screenshot showcasing the ForensicVM's interactive interface.

7.2.2 Method 2: Link the Local Forensic Image to a New Forensic Virtual Machine on the Server

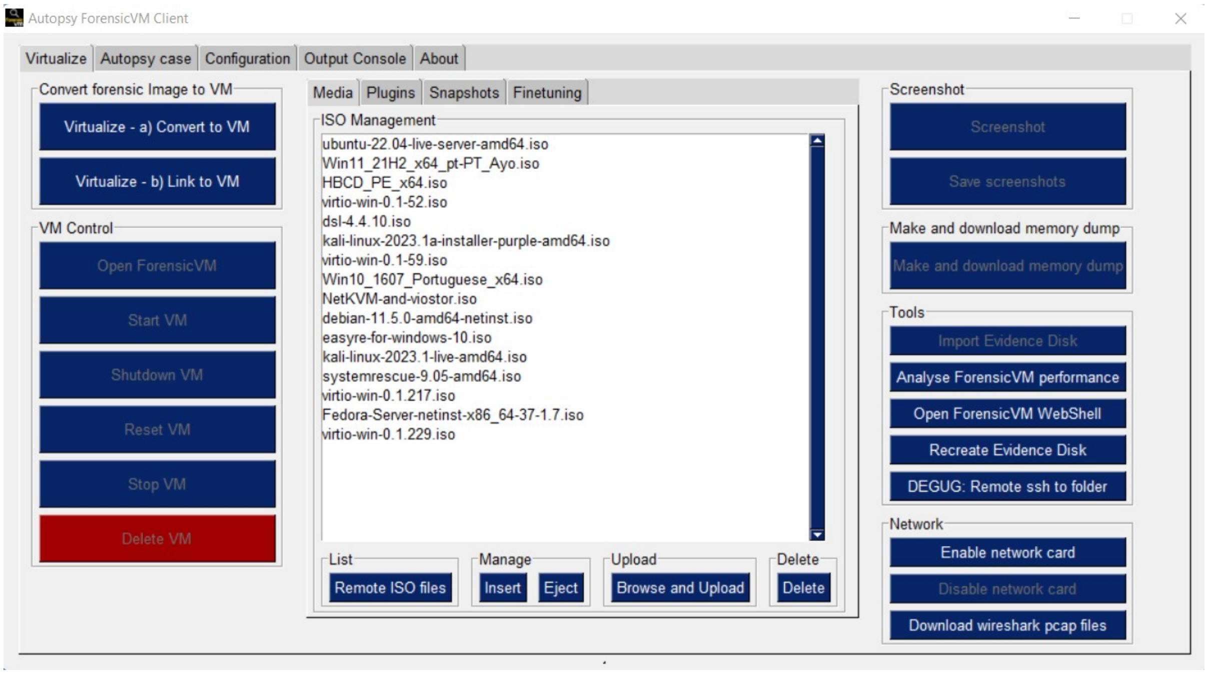
Link Creation:

In this method, a link is forged between the local forensic image and a new counterpart on the server. This approach is faster because it doesn't involve transferring the entire image to the remote server. However, there are some limitations. The conversion process and preview are swift, but starting the machine locally is a requirement. The investigator needs to use the Autopsy client plugin to initiate the machine since the web interface cannot be used due to its dependency on the original forensic image.

Conversion Steps:

1. **Begin the Conversion**:

   Start the conversion by clicking on the button labeled "Virtualize - b) Link to VM".

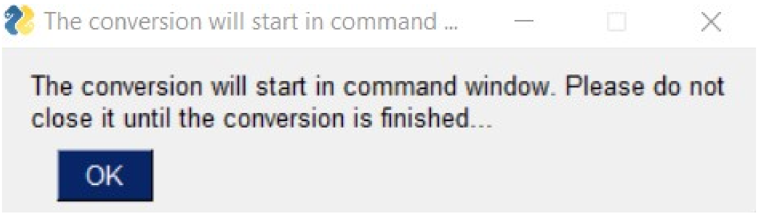


```
ubuntu-22.04-live-server-amd64.iso
Win11_21H2_x64_pt-PT_Ayo.iso
HBCD_PE_x64.iso
virtio-win-0.1-52.iso
dsl-4.4.10.iso
kali-linux-2023.1a-installer-purple-amd64.iso
virtio-win-0.1-59.iso
Win10_1607_Portuguese_x64.iso
NetKVM-and-viostor.iso
debian-11.5.0-amd64-netinst.iso
easyre-for-windows-10.iso
kali-linux-2023.1-live-amd64.iso
systemrescue-9.05-amd64.iso
virtio-win-0.1.217.iso
Fedora-Server-netinst-x86_64-37-1.7.iso
virtio-win-0.1.229.iso
```

Fig. 7.24: "Virtualize - b) Link to VM" button

2. **Popup Confirmation**:

   After activating the conversion, a popup will emerge. It will instruct: "The conversion will commence in a command window. Please refrain from shutting it until the process concludes." Press "OK" to proceed.

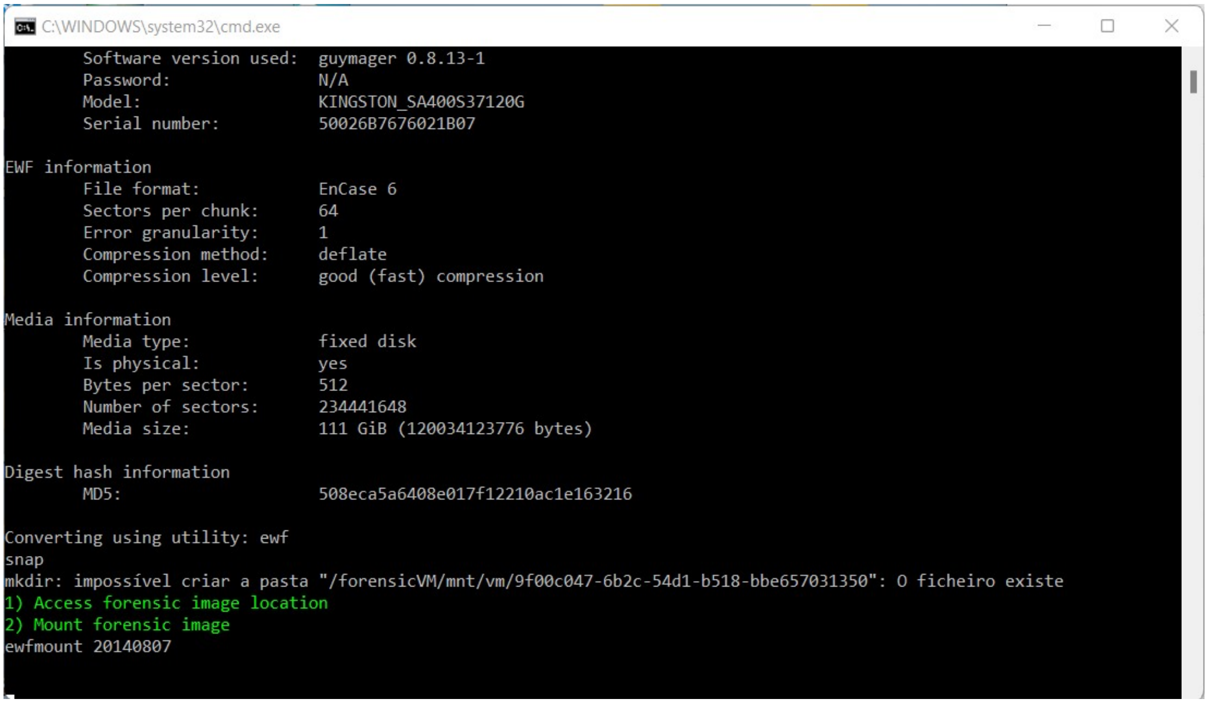


The conversion will start in command window. Please do not close it until the conversion is finished...

Fig. 7.25: Linking Confirmation Popup

3. MS-DOS Command Window **Feedback**:

The MS-DOS command window will surface, and the software will identify the image format, displaying it within the window. Successful actions are highlighted in green. However, be vigilant and record any errors that arise.



```
        Software version used:  guymager 0.8.13-1
        Password:               N/A
        Model:                  KINGSTON_SA400S37120G
        Serial number:          50026B7676021B07

EWF information
        File format:            EnCase 6
        Sectors per chunk:      64
        Error granularity:      1
        Compression method:     deflate
        Compression level:      good (fast) compression

Media information
        Media type:             fixed disk
        Is physical:            yes
        Bytes per sector:       512
        Number of sectors:      234441648
        Media size:             111 GiB (120034123776 bytes)

Digest hash information
        MD5:                    508eca5a6408e017f12210ac1e163216

Converting using utility: ewf
snap
mkdir: impossível criar a pasta "/forensicVM/mnt/vm/9f00c047-6b2c-54d1-b518-bbe657031350": O ficheiro existe
1) Access forensic image location
2) Mount forensic image
ewfmount 20140807
```

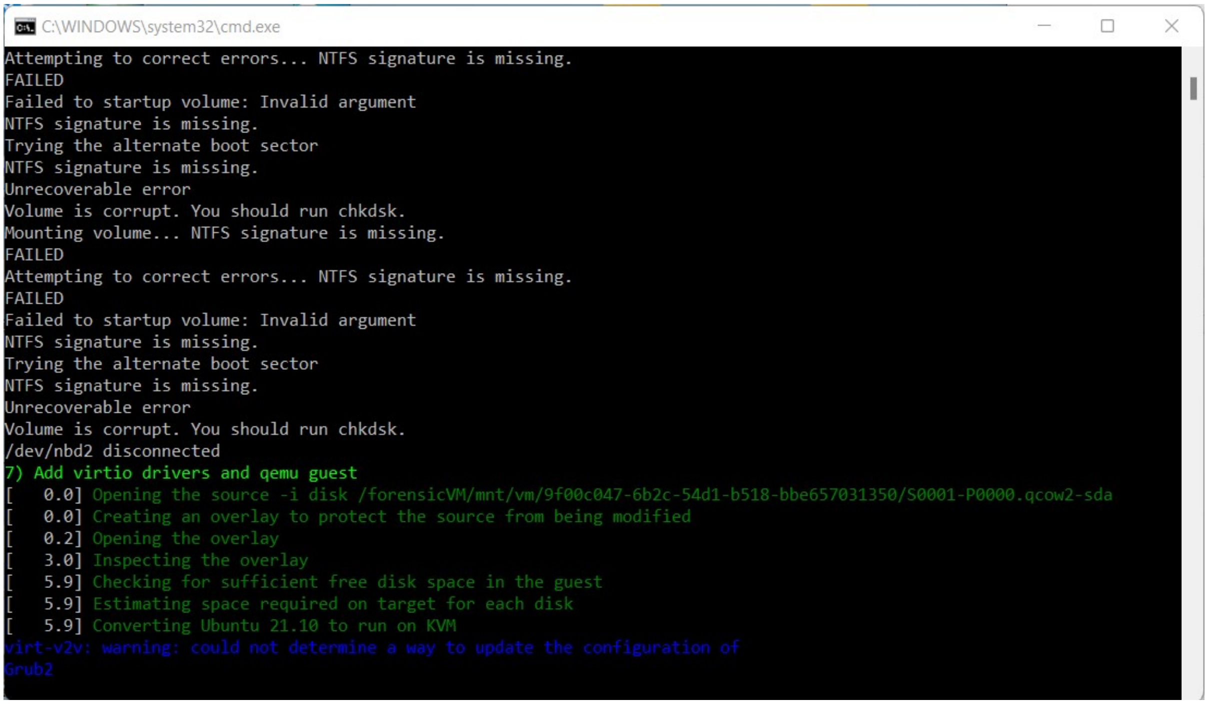
Fig. 7.26: MS-DOS Command Window Feedback

4. **Driver Installation Phase**:

   This step focuses on the installation of required KVM drivers. The messages in this phase are color-coded:

   - **Green**: Success indicators.
   - **Blue**: Warnings.
   - **Magenta**: Special informational messages.

   The linking process's progression is represented in percentage terms.



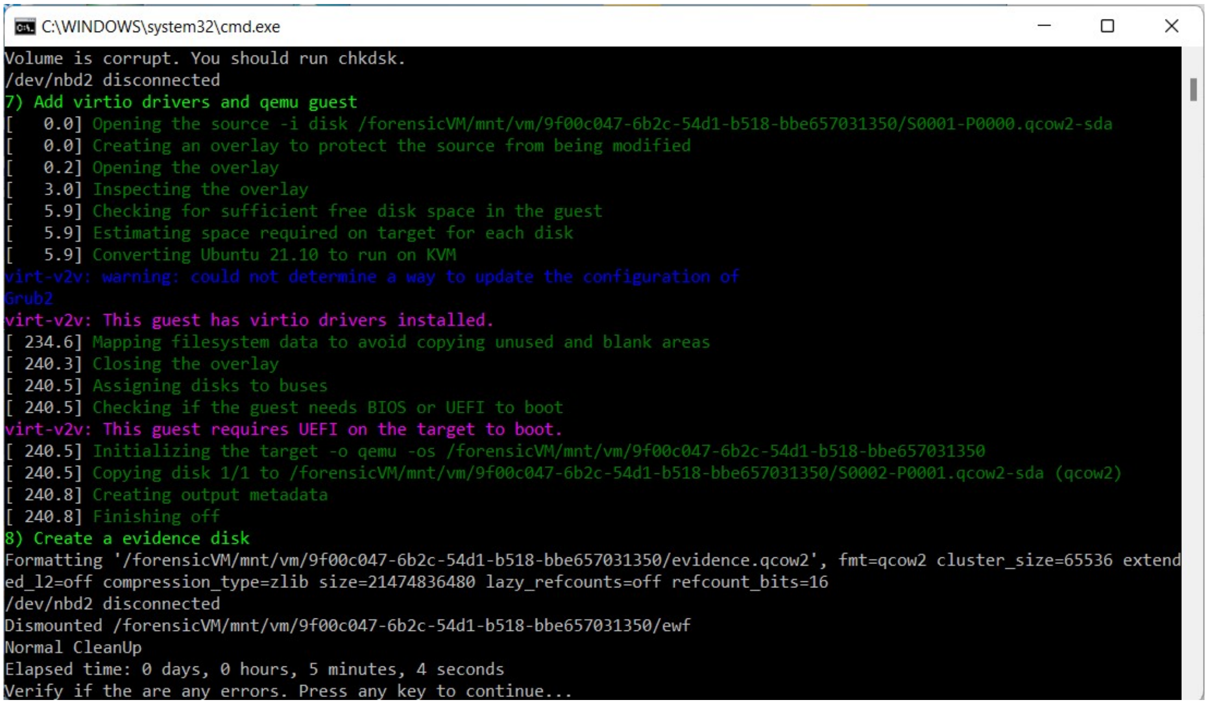
```
Attempting to correct errors... NTFS signature is missing.
FAILED
Failed to startup volume: Invalid argument
NTFS signature is missing.
Trying the alternate boot sector
NTFS signature is missing.
Unrecoverable error
Volume is corrupt. You should run chkdsk.
Mounting volume... NTFS signature is missing.
FAILED
Attempting to correct errors... NTFS signature is missing.
FAILED
Failed to startup volume: Invalid argument
NTFS signature is missing.
Trying the alternate boot sector
NTFS signature is missing.
Unrecoverable error
Volume is corrupt. You should run chkdsk.
/dev/nbd2 disconnected
7) Add virtio drivers and qemu guest
[   0.0] Opening the source -i disk /forensicVM/mnt/vm/9f00c047-6b2c-54d1-b518-bbe657031350/S0001-P0000.qcow2-sda
[   0.0] Creating an overlay to protect the source from being modified
[   0.2] Opening the overlay
[   3.0] Inspecting the overlay
[   5.9] Checking for sufficient free disk space in the guest
[   5.9] Estimating space required on target for each disk
[   5.9] Converting Ubuntu 21.10 to run on KVM
virt-v2v: warning: could not determine a way to update the configuration of
Grub2
```

Fig. 7.27: Driver Installation and Progress Display

5. **Conclusion of Conversion**:

   Upon the conversion's culmination, a success notification will display the elapsed time. Ensure to press any key to close the window.

   > **Warning:** Avoid manually shutting this window. Such an action could leave a Linux mount unsealed, leading to potential complications in the future.

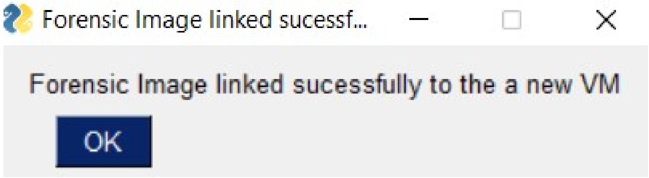


```
Volume is corrupt. You should run chkdsk.
/dev/nbd2 disconnected
7) Add virtio drivers and qemu guest
[   0.0] Opening the source -i disk /forensicVM/mnt/vm/9f00c047-6b2c-54d1-b518-bbe657031350/S0001-P0000.qcow2-sda
[   0.0] Creating an overlay to protect the source from being modified
[   0.2] Opening the overlay
[   3.0] Inspecting the overlay
[   5.9] Checking for sufficient free disk space in the guest
[   5.9] Estimating space required on target for each disk
[   5.9] Converting Ubuntu 21.10 to run on KVM
virt-v2v: warning: could not determine a way to update the configuration of
Grub2
virt-v2v: This guest has virtio drivers installed.
[ 234.6] Mapping filesystem data to avoid copying unused and blank areas
[ 240.3] Closing the overlay
[ 240.5] Assigning disks to buses
[ 240.5] Checking if the guest needs BIOS or UEFI to boot
virt-v2v: This guest requires UEFI on the target to boot.
[ 240.5] Initializing the target -o qemu -os /forensicVM/mnt/vm/9f00c047-6b2c-54d1-b518-bbe657031350
[ 240.5] Copying disk 1/1 to /forensicVM/mnt/vm/9f00c047-6b2c-54d1-b518-bbe657031350/S0002-P0001.qcow2-sda (qcow2)
[ 240.8] Creating output metadata
[ 240.8] Finishing off
8) Create a evidence disk
Formatting '/forensicVM/mnt/vm/9f00c047-6b2c-54d1-b518-bbe657031350/evidence.qcow2', fmt=qcow2 cluster_size=65536 extend
ed_l2=off compression_type=zlib size=21474836480 lazy_refcounts=off refcount_bits=16
/dev/nbd2 disconnected
Dismounted /forensicVM/mnt/vm/9f00c047-6b2c-54d1-b518-bbe657031350/ewf
Normal CleanUp
Elapsed time: 0 days, 0 hours, 5 minutes, 4 seconds
Verify if the are any errors. Press any key to continue...
```

Fig. 7.28: Conversion Completed Notification

6. **Success Notification**:

   A concluding popup emerges, affirming that the forensic image was successfully linked to the VM. Click “OK” to exit this dialog.



Forensic Image linked sucessfully to the a new VM

Fig. 7.29: Successful Linking Notification

7.3 Starting the Virtual Machine (VM)

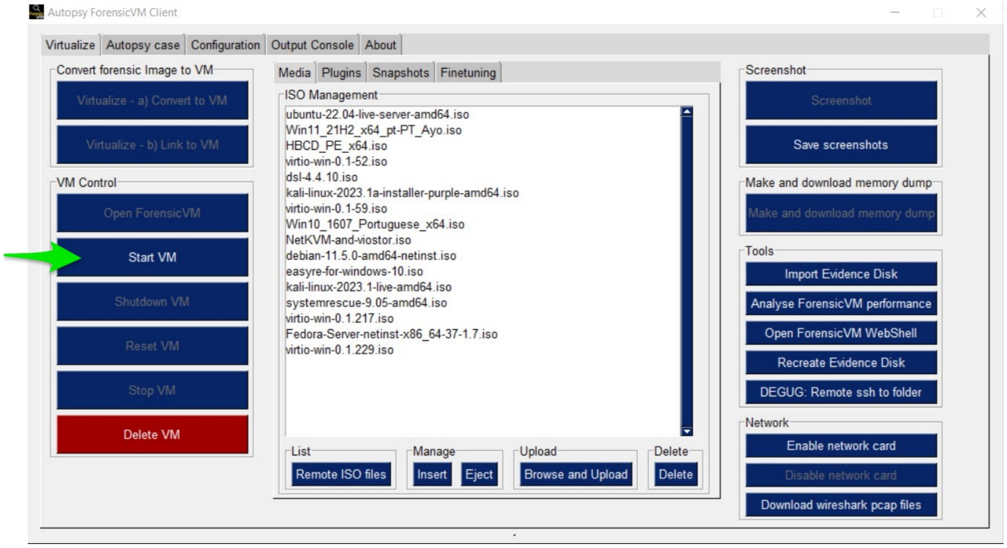
7.3.1 Three ways to start the forensicVM

There are three different ways to start the forensic virtual machine (forensicVM). These methods provide flexibility depending on your access level and location within the system interface:

1) Start ForensicVM in the Main Plugin Interface

To initiate the forensicVM from the main plugin interface, follow these simple steps:

a) Locate the start button on the main interface as depicted in the figure below.



ubuntu-22.04-live-server-amd64.iso
Win11_21H2_x64_pt-PT_Ayo.iso
HBCD_PE_x64.iso
virtio-win-0.1-52.iso
dsl-4.4.10.iso
kali-linux-2023.1a-installer-purple-amd64.iso
virtio-win-0.1-59.iso
Win10_1607_Portuguese_x64.iso
NetKVM-and-viostor.iso
debian-11.5.0-amd64-netinst.iso
easyre-for-windows-10.iso
kali-linux-2023.1-live-amd64.iso
systemrescue-9.05-amd64.iso
virtio-win-0.1.217.iso
Fedora-Server-netinst-x86_64-37-1.7.iso
virtio-win-0.1.229.iso

Fig. 7.30: Start VM on the main interface

b) Press the start button to activate the virtual machine.

2) Start ForensicVM after Logging in to the Web Interface

To start the forensicVM through the web interface after login, you need to:

a) Open the login main page.

b) Enter your username and password, and then click on the login button.

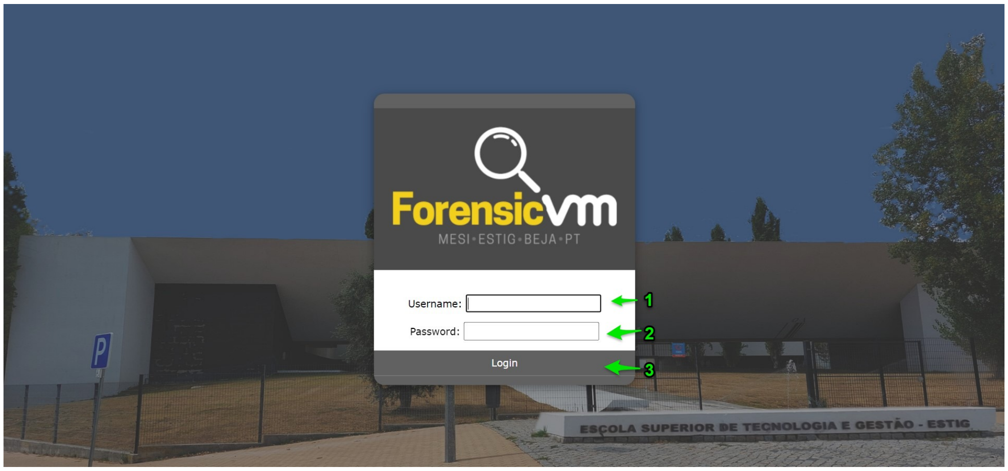
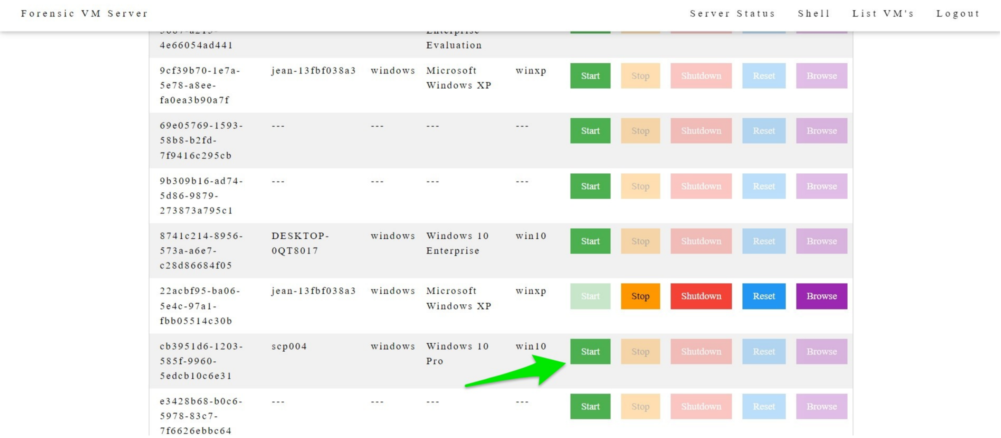


Fig. 7.31: Login on the main web interface

c) Once logged in, locate the start button for the selected forensicVM you wish to initiate.

d) Press the start button to activate the virtual machine.



4e66054ad441			Evaluation						
9cf39b70-1e7a-5e78-a8ee-fa0ea3b90a7f	jean-13fbf038a3	windows	Microsoft Windows XP	winxp	Start	Stop	Shutdown	Reset	Browse
69e05769-1593-58b8-b2fd-7f9416c295cb	---	---	---	---	Start	Stop	Shutdown	Reset	Browse
9b309b16-ad74-5d86-9879-273873a795c1	---	---	---	---	Start	Stop	Shutdown	Reset	Browse
8741c214-8956-573a-a6e7-c28d86684f05	DESKTOP-0QT8017	windows	Windows 10 Enterprise	win10	Start	Stop	Shutdown	Reset	Browse
22acbf95-ba06-5e4c-97a1-fbb05514c30b	jean-13fbf038a3	windows	Microsoft Windows XP	winxp	Start	Stop	Shutdown	Reset	Browse
cb3951d6-1203-585f-9960-5edcb10c6e31	scp004	windows	Windows 10 Pro	win10	Start	Stop	Shutdown	Reset	Browse
e3428b68-b0c6-5978-83c7-7f6626ebbc64	---	---	---	---	Start	Stop	Shutdown	Reset	Browse

Fig. 7.32: Start VM on the main web interface

3) Start ForensicVM on the Web Remote Screen

Another option to start the forensicVM is from the web remote screen. This method may be preferred if you are working remotely or through a particular service interface:

a) Navigate to the web remote screen.

b) Locate the start button, as shown in the figure below.

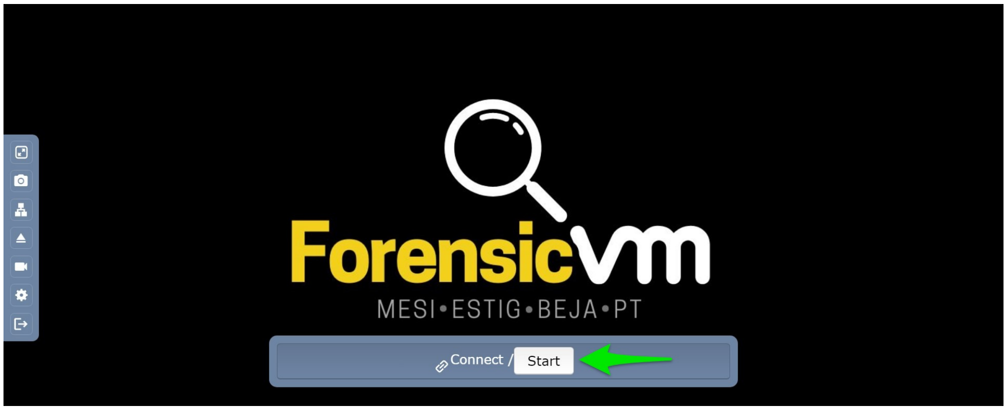


Fig. 7.33: Start VM on the web remote screen

c) Press the start button to initiate the virtual machine.

These three methods ensure that you can initiate the forensicVM from various points in the system.

7.3.2 Special Case: Starting the ForensicVM in Link Mode

Precautions and Considerations:

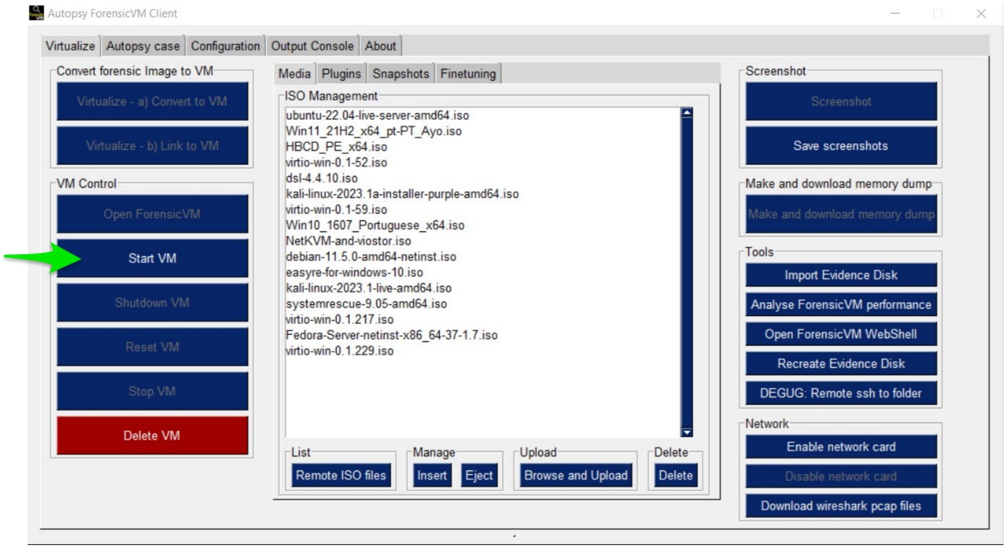
When a forensic image is converted to a forensic virtual machine using the “Virtualize b) Link to VM” option, it can only be started via the Autopsy Plugin. Ensure that you adhere to the following precautions to guarantee a smooth operation of the virtual machine:

> **Warning:**
>
> 1. Only initiate the linked forensicVM through the Autopsy Plugin. Avoid using the forensicVM web interface—it will be ineffective.
> 2. Utilize a reliable internet connection, such as fiber optics. Any connection disruptions could lead to machine disk timeouts, and potentially the virtual machine encountering a “blue screen of death.”
> 3. Maintain the command line window in an open state. This window must remain open at all times. To power off or stop the forensicVM, use the “Stop” or “Shutdown” options in the Autopsy Plugin. This method ensures the prevention of lingering mount points on your computer, which could cause issues.

Steps to Start, Stop, or Shutdown:

1. **Activate ForensicVM in the Main** Plugin Interface:

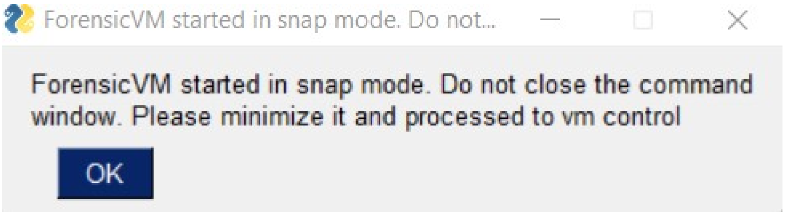
   To initiate the VM, click the “Start” button.



```
ubuntu-22.04-live-server-amd64.iso
Win11_21H2_x64_pt-PT_Ayo.iso
HBCD_PE_x64.iso
virtio-win-0.1-52.iso
dsl-4.4.10.iso
kali-linux-2023.1a-installer-purple-amd64.iso
virtio-win-0.1-59.iso
Win10_1607_Portuguese_x64.iso
NetKVM-and-viostor.iso
debian-11.5.0-amd64-netinst.iso
easyre-for-windows-10.iso
kali-linux-2023.1-live-amd64.iso
systemrescue-9.05-amd64.iso
virtio-win-0.1.217.iso
Fedora-Server-netinst-x86_64-37-1.7.iso
virtio-win-0.1.229.iso
```

Fig. 7.34: The “Start” button in the main plugin interface.

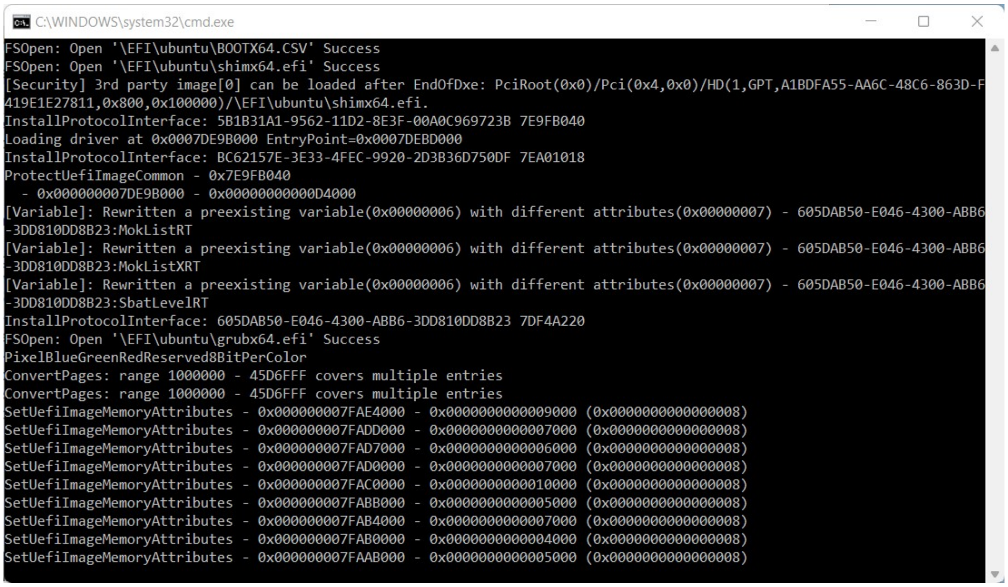
Following this action, a popup will inform you that the machine has launched in “snap” or link mode.



ForensicVM started in snap mode. Do not close the command window. Please minimize it and processed to vm control

Fig. 7.35: Machine's launch mode notification.

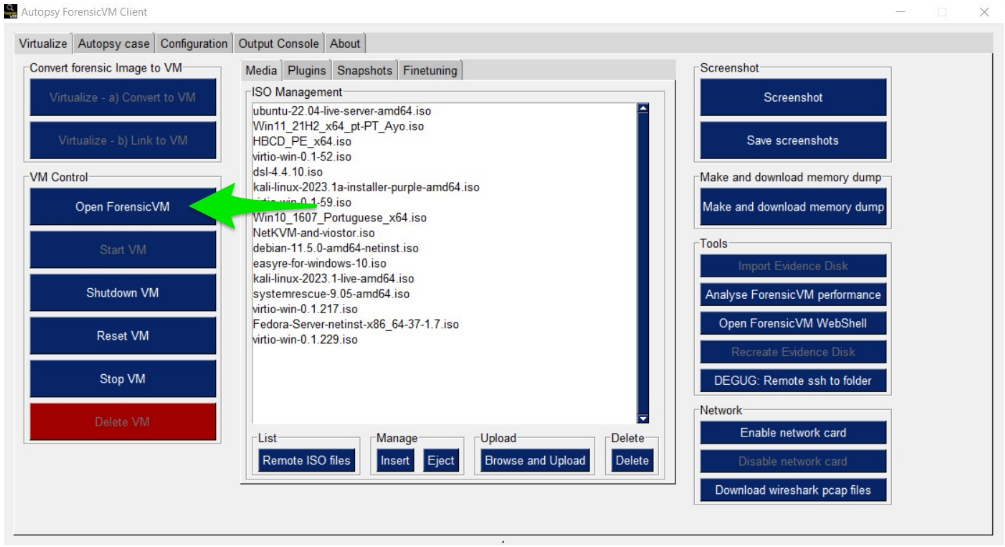
Next, a command line window will manifest. While you should minimize it, it's crucial not to close it. If you need to shut down the machine, kindly adhere to the subsequent steps to safely halt or power off the forensicVM.



```
FSOpen: Open '\EFI\ubuntu\BOOTX64.CSV' Success
FSOpen: Open '\EFI\ubuntu\shimx64.efi' Success
[Security] 3rd party image[0] can be loaded after EndOfDxe: PciRoot(0x0)/Pci(0x4,0x0)/HD(1,GPT,A1BDFA55-AA6C-48C6-863D-F
419E1E27811,0x800,0x100000)/\EFI\ubuntu\shimx64.efi.
InstallProtocolInterface: 5B1B31A1-9562-11D2-8E3F-00A0C969723B 7E9FB040
Loading driver at 0x0007DE9B000 EntryPoint=0x0007DEBD000
InstallProtocolInterface: BC62157E-3E33-4FEC-9920-2D3B36D750DF 7EA01018
ProtectUefiImageCommon - 0x7E9FB040
  - 0x000000007DE9B000 - 0x00000000000D4000
[Variable]: Rewritten a preexisting variable(0x00000006) with different attributes(0x00000007) - 605DAB50-E046-4300-ABB6
-3DD810DD8B23:MokListRT
[Variable]: Rewritten a preexisting variable(0x00000006) with different attributes(0x00000007) - 605DAB50-E046-4300-ABB6
-3DD810DD8B23:MokListXRT
[Variable]: Rewritten a preexisting variable(0x00000006) with different attributes(0x00000007) - 605DAB50-E046-4300-ABB6
-3DD810DD8B23:SbatLevelRT
InstallProtocolInterface: 605DAB50-E046-4300-ABB6-3DD810DD8B23 7DF4A220
FSOpen: Open '\EFI\ubuntu\grubx64.efi' Success
PixelBlueGreenRedReserved8BitPerColor
ConvertPages: range 1000000 - 45D6FFF covers multiple entries
ConvertPages: range 1000000 - 45D6FFF covers multiple entries
SetUefiImageMemoryAttributes - 0x000000007FAE4000 - 0x0000000000009000 (0x0000000000000008)
SetUefiImageMemoryAttributes - 0x000000007FADD000 - 0x0000000000007000 (0x0000000000000008)
SetUefiImageMemoryAttributes - 0x000000007FAD7000 - 0x0000000000006000 (0x0000000000000008)
SetUefiImageMemoryAttributes - 0x000000007FAD0000 - 0x0000000000007000 (0x0000000000000008)
SetUefiImageMemoryAttributes - 0x000000007FAC0000 - 0x0000000000010000 (0x0000000000000008)
SetUefiImageMemoryAttributes - 0x000000007FABB000 - 0x0000000000005000 (0x0000000000000008)
SetUefiImageMemoryAttributes - 0x000000007FAB4000 - 0x0000000000007000 (0x0000000000000008)
SetUefiImageMemoryAttributes - 0x000000007FAB0000 - 0x0000000000004000 (0x0000000000000008)
SetUefiImageMemoryAttributes - 0x000000007FAAB000 - 0x0000000000005000 (0x0000000000000008)
```

Fig. 7.36: Command line window – important not to close.

To interact with the machine through its graphical interface, hit the "Open ForensicVM" option.



```
ubuntu-22.04-live-server-amd64.iso
Win11_21H2_x64_pt-PT_Ayo.iso
HBCD_PE_x64.iso
virtio-win-0.1-52.iso
dsl-4.4.10.iso
kali-linux-2023.1a-installer-purple-amd64.iso
virtio-win-0.1-59.iso
Win10_1607_Portuguese_x64.iso
NetKVM-and-viostor.iso
debian-11.5.0-amd64-netinst.iso
easyre-for-windows-10.iso
kali-linux-2023.1-live-amd64.iso
systemrescue-9.05-amd64.iso
virtio-win-0.1.217.iso
Fedora-Server-netinst-x86_64-37-1.7.iso
virtio-win-0.1.229.iso
```

Fig. 7.37: “Open ForensicVM” button.

This action will lead to the machine’s manifestation within a web interface, allowing you to seamlessly interact with the system.

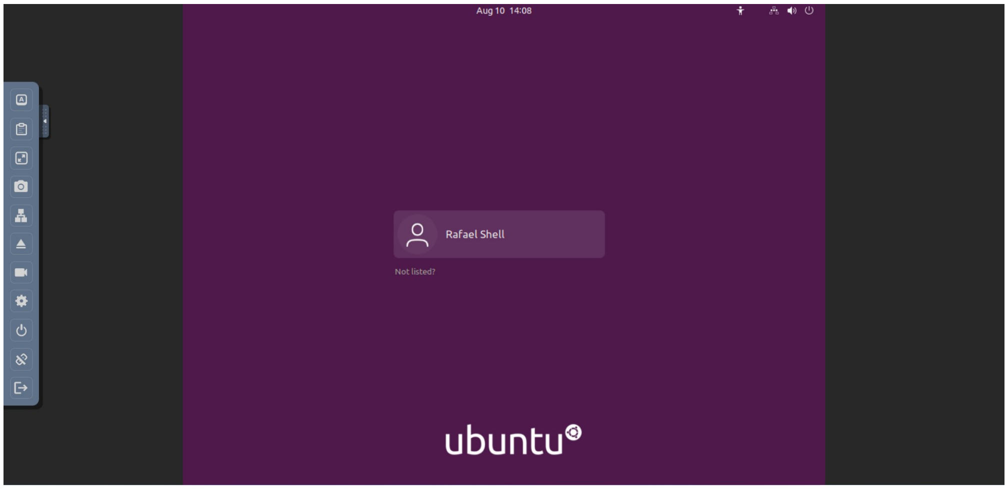


Fig. 7.38: ForensicVM web interface.

It’s imperative to note that the solitary and secure method to halt or power off the machine is by utilizing the “Shutdown” or “Stop” buttons available in the Autopsy Plugin.

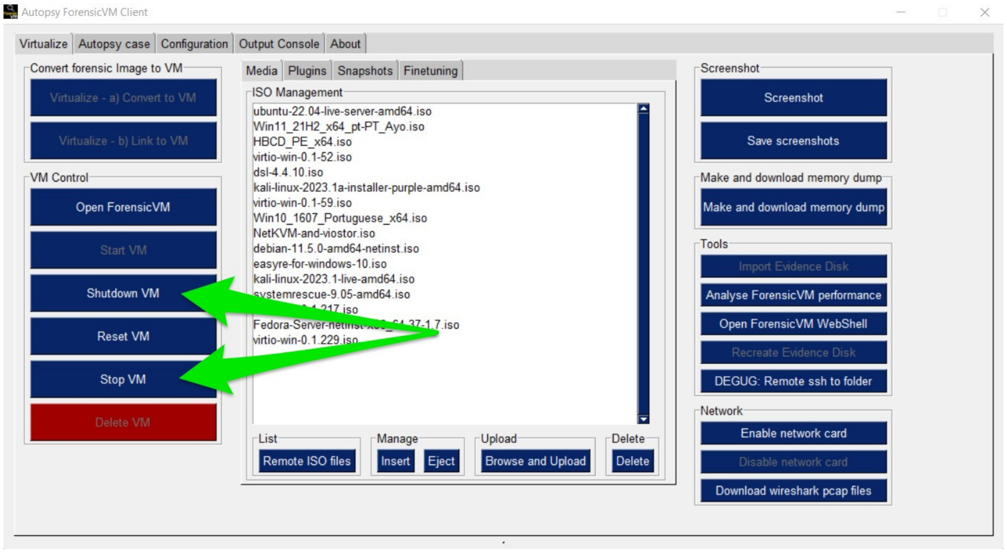

Autopsy ForensicVM Client
Virtualize
Autopsy case
Configuration
Output Console
About
Convert forensic Image to VM
Virtualize - a) Convert to VM
Virtualize - b) Link to VM
VM Control
Open ForensicVM
Start VM
Shutdown VM
Reset VM
Stop VM
Delete VM
Media
Plugins
Snapshots
Finetuning
ISO Management
ubuntu-22.04-live-server-amd64.iso
Win11_21H2_x64_pt-PT_Ayo.iso
HBCD_PE_x64.iso
virtio-win-0.1-52.iso
dsl-4.4.10.iso
kali-linux-2023.1a-installer-purple-amd64.iso
virtio-win-0.1-59.iso
Win10_1607_Portuguese_x64.iso
NetKVM-and-viostor.iso
debian-11.5.0-amd64-netinst.iso
easyre-for-windows-10.iso
kali-linux-2023.1-live-amd64.iso
systemrescue-9.05-amd64.iso
virtio-win-0.1.217.iso
Fedora-Server-netinst-x86_64-37-1.7.iso
virtio-win-0.1.229.iso
List
Remote ISO files
Manage
Insert
Eject
Upload
Browse and Upload
Delete
Delete
Screenshot
Screenshot
Save screenshots
Make and download memory dump
Make and download memory dump
Tools
Import Evidence Disk
Analyse ForensicVM performance
Open ForensicVM WebShell
Recreate Evidence Disk
DEGUG: Remote ssh to folder
Network
Enable network card
Disable network card
Download wireshark pcap files

Fig. 7.39: Autopsy Plugin's control buttons.

7.4 Open or Browse the Forensic Virtual Machine (VM)

There are two main ways to access the started forensicVM, each catering to different use cases and preferences:

7.4.1 1) Open ForensicVM through the Plugin Interface

You can access the forensicVM directly through the Autopsy plugin interface.

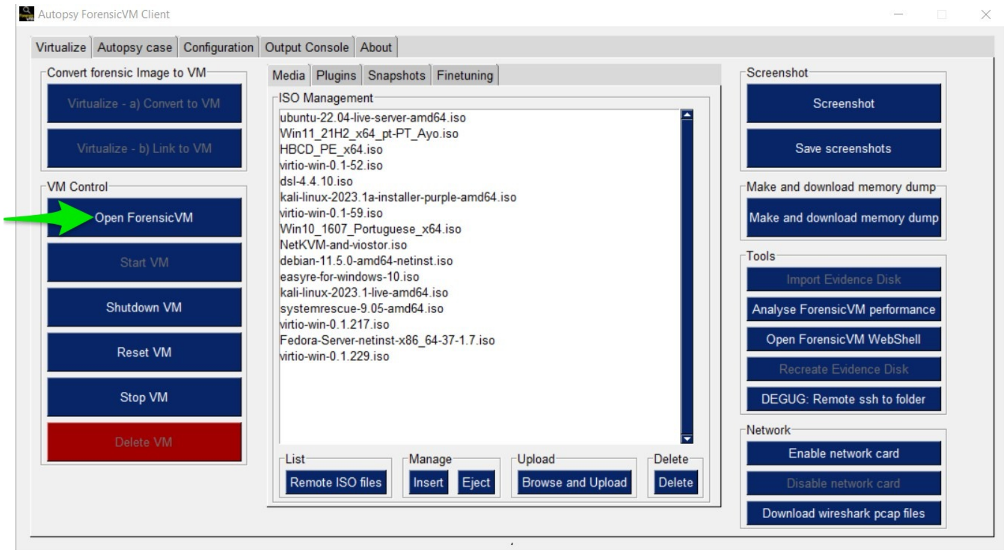
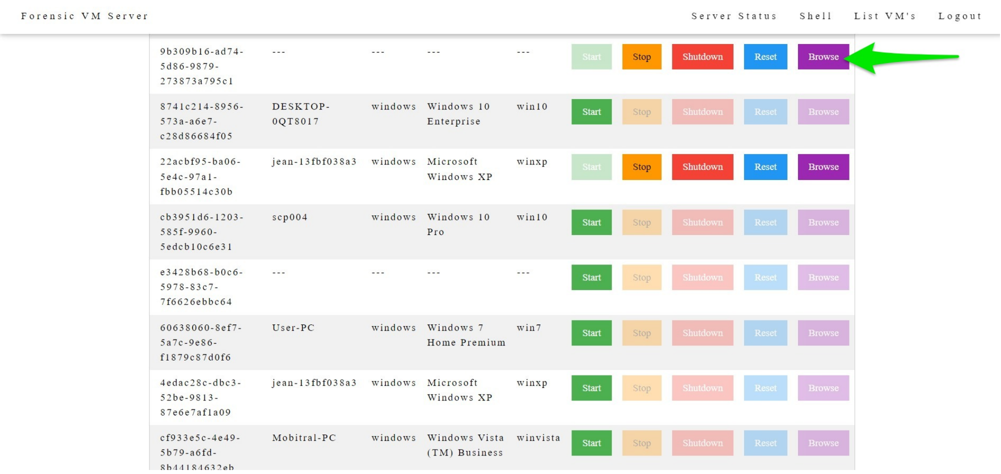

Autopsy ForensicVM Client
Virtualize
Autopsy case
Configuration
Output Console
About
Convert forensic Image to VM
Virtualize - a) Convert to VM
Virtualize - b) Link to VM
VM Control
Open ForensicVM
Start VM
Shutdown VM
Reset VM
Stop VM
Delete VM
Media
Plugins
Snapshots
Finetuning
ISO Management
ubuntu-22.04-live-server-amd64.iso
Win11_21H2_x64_pt-PT_Ayo.iso
HBCD_PE_x64.iso
virtio-win-0.1-52.iso
dsl-4.4.10.iso
kali-linux-2023.1a-installer-purple-amd64.iso
virtio-win-0.1-59.iso
Win10_1607_Portuguese_x64.iso
NetKVM-and-viostor.iso
debian-11.5.0-amd64-netinst.iso
easyre-for-windows-10.iso
kali-linux-2023.1-live-amd64.iso
systemrescue-9.05-amd64.iso
virtio-win-0.1.217.iso
Fedora-Server-netinst-x86_64-37-1.7.iso
virtio-win-0.1.229.iso
List
Remote ISO files
Manage
Insert
Eject
Upload
Browse and Upload
Delete
Delete
Screenshot
Screenshot
Save screenshots
Make and download memory dump
Make and download memory dump
Tools
Import Evidence Disk
Analyse ForensicVM performance
Open ForensicVM WebShell
Recreate Evidence Disk
DEGUG: Remote ssh to folder
Network
Enable network card
Disable network card
Download wireshark pcap files

Fig. 7.40: Open forensicVM on the main interface

7.4.2 2) Browse ForensicVM using the Main Web Interface

Alternatively, you can browse the forensicVM through the main web interface. This approach is generally more accessible and can be used from any web browser that supports the required protocols.



Forensic VM Server   Server Status   Shell   List VM's   Logout

9b309b16-ad74-5d86-9879-273873a795c1	---	---	---	---	Start	Stop	Shutdown	Reset	Browse
8741c214-8956-573a-a6e7-c28d86684f05	DESKTOP-0QT8017	windows	Windows 10 Enterprise	win10	Start	Stop	Shutdown	Reset	Browse
22acbf95-ba06-5e4c-97a1-fbb05514c30b	jean-13fbf038a3	windows	Microsoft Windows XP	winxp	Start	Stop	Shutdown	Reset	Browse
cb3951d6-1203-585f-9960-5edcb10c6e31	scp004	windows	Windows 10 Pro	win10	Start	Stop	Shutdown	Reset	Browse
e3428b68-b0c6-5978-83c7-7f6626ebbc64	---	---	---	---	Start	Stop	Shutdown	Reset	Browse
60638060-8ef7-5a7c-9e86-f1879c87d0f6	User-PC	windows	Windows 7 Home Premium	win7	Start	Stop	Shutdown	Reset	Browse
4edac28c-dbc3-52be-9813-87e6e7af1a09	jean-13fbf038a3	windows	Microsoft Windows XP	winxp	Start	Stop	Shutdown	Reset	Browse
cf933e5c-4e49-5b79-a6fd-8b44184632eb	Mobitral-PC	windows	Windows Vista (TM) Business	winvista	Start	Stop	Shutdown	Reset	Browse

Fig. 7.41: Open forensicVM on the web interface

Steps: a) Navigate to the web interface URL. b) Log in with your credentials, if required. c) Locate the forensicVM you wish to access. d) Click the appropriate control, such as “Start,” “Stop,” “Reset”, etc., to manage the forensicVM.

7.4.3 ForensicVM remote screen interface

An example of the forensic image converted to a forensicVM

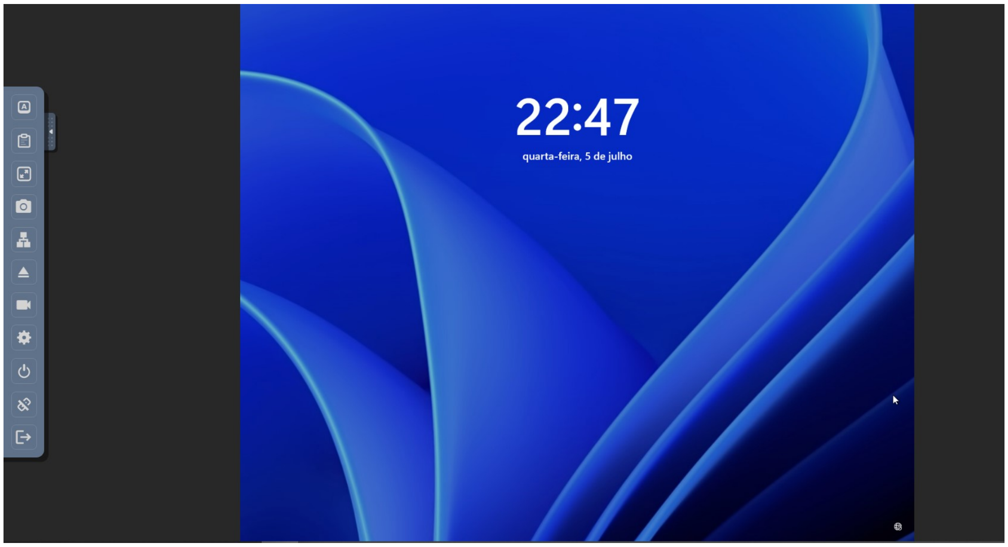


Fig. 7.42: Open forensicVM main screen on the web interface

Summary: Both methods provide control over the forensicVM, allowing you to perform a variety of tasks like starting, stopping, resetting, and more. Choosing between the plugin interface and the web interface depends on your specific needs, available tools, and personal preferences.

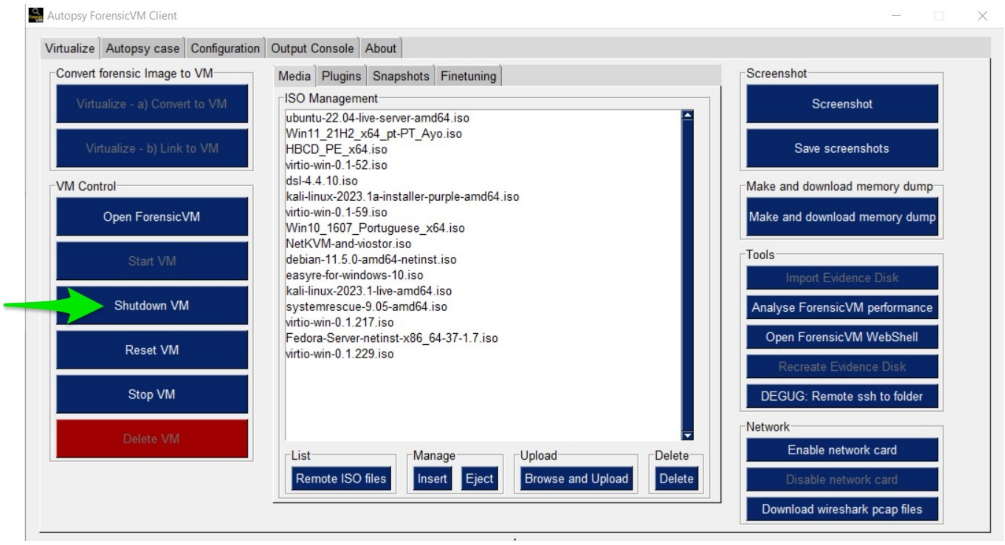
7.5 Shutting Down the Virtual Machine (VM)

There are three different ways to shut down the forensic virtual machine (forensicVM). These methods provide flexibility depending on your access level and location within the system interface:

7.5.1 1) Shut Down ForensicVM in the Main Plugin Interface

To shut down the forensicVM from the main plugin interface, follow these simple steps:

a) Locate the shutdown button on the main interface as depicted in the figure below.



```
ubuntu-22.04-live-server-amd64.iso
Win11_21H2_x64_pt-PT_Ayo.iso
HBCD_PE_x64.iso
virtio-win-0.1-52.iso
dsl-4.4.10.iso
kali-linux-2023.1a-installer-purple-amd64.iso
virtio-win-0.1-59.iso
Win10_1607_Portuguese_x64.iso
NetKVM-and-viostor.iso
debian-11.5.0-amd64-netinst.iso
easyre-for-windows-10.iso
kali-linux-2023.1-live-amd64.iso
systemrescue-9.05-amd64.iso
virtio-win-0.1.217.iso
Fedora-Server-netinst-x86_64-37-1.7.iso
virtio-win-0.1.229.iso
```

Fig. 7.43: Shut down VM on the main interface

b) Press the shutdown button to deactivate the virtual machine.

7.5.2 2) Shut Down ForensicVM after Logging in to the Web Remote Screen

To shut down the forensicVM through the web remote screen interface, you need to:

1) Locate the shutdown icon.

2) Press the shutdown button to deactivate the virtual machine.

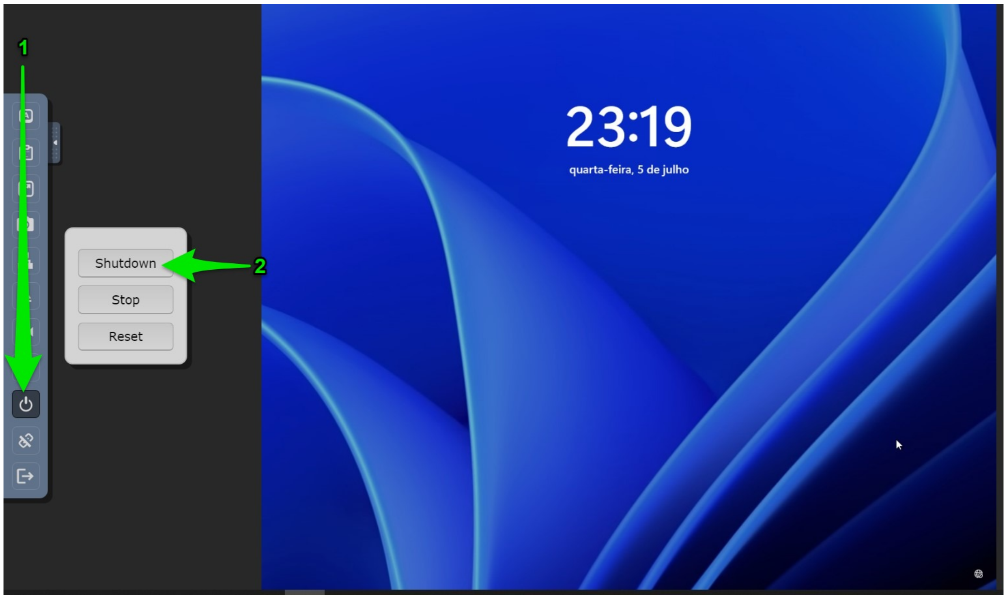


Fig. 7.44: Login on the main web interface

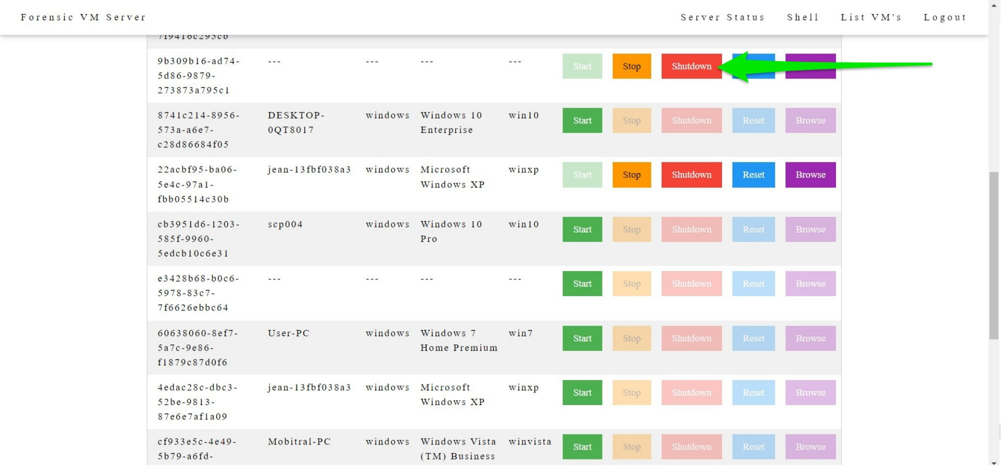
7.5.3 3) Shut Down ForensicVM on the Web Interface

Another option to shut down the forensicVM is from the web remote screen. This method may be preferred if you are working remotely or through a particular service interface:

a) Navigate to the web interface.

b) Locate the machine that you need to shutdown.

c) Locate and click the shutdown button, as shown in the figure below.



719416c295cb									
9b309b16-ad74-5d86-9879-273873a795c1	---	---	---	---	Start	Stop	Shutdown		
8741c214-8956-573a-a6e7-c28d86684f05	DESKTOP-0QT8017	windows	Windows 10 Enterprise	win10	Start	Stop	Shutdown	Reset	Browse
22acbf95-ba06-5e4c-97a1-fbb05514c30b	jean-13fbf038a3	windows	Microsoft Windows XP	winxp	Start	Stop	Shutdown	Reset	Browse
cb3951d6-1203-585f-9960-5edcb10c6e31	scp004	windows	Windows 10 Pro	win10	Start	Stop	Shutdown	Reset	Browse
e3428b68-b0c6-5978-83c7-7f6626ebbc64	---	---	---	---	Start	Stop	Shutdown	Reset	Browse
60638060-8ef7-5a7c-9e86-f1879c87d0f6	User-PC	windows	Windows 7 Home Premium	win7	Start	Stop	Shutdown	Reset	Browse
4edac28c-dbc3-52be-9813-87e6e7af1a09	jean-13fbf038a3	windows	Microsoft Windows XP	winxp	Start	Stop	Shutdown	Reset	Browse
cf933e5c-4e49-5b79-a6fd-	Mobitral-PC	windows	Windows Vista (TM) Business	winvista	Start	Stop	Shutdown	Reset	Browse

Fig. 7.45: Shut down VM on the web interface

These three methods ensure that you can shut down the forensicVM from various points in the system, allowing for seamless control depending on your needs and preferences.

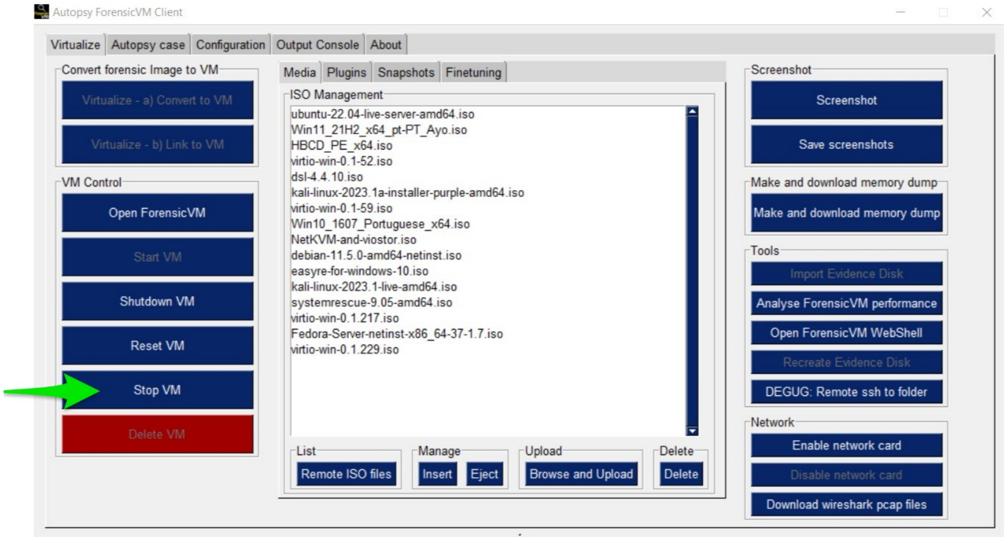
7.6 Stopping the Virtual Machine (VM)

There are three different ways to stop the forensic virtual machine (forensicVM). These methods provide flexibility depending on your access level and location within the system interface:

7.6.1 1) Stop ForensicVM in the Main Plugin Interface

To stop the forensicVM from the main plugin interface, follow these simple steps:

a) Locate the stop button on the main interface as depicted in the figure below.



```
ubuntu-22.04-live-server-amd64.iso
Win11_21H2_x64_pt-PT_Ayo.iso
HBCD_PE_x64.iso
virtio-win-0.1-52.iso
dsl-4.4.10.iso
kali-linux-2023.1a-installer-purple-amd64.iso
virtio-win-0.1-59.iso
Win10_1607_Portuguese_x64.iso
NetKVM-and-viostor.iso
debian-11.5.0-amd64-netinst.iso
easyre-for-windows-10.iso
kali-linux-2023.1-live-amd64.iso
systemrescue-9.05-amd64.iso
virtio-win-0.1.217.iso
Fedora-Server-netinst-x86_64-37-1.7.iso
virtio-win-0.1.229.iso
```

Fig. 7.46: Stop VM on the main interface

b) Press the stop button to halt the virtual machine.

7.6.2 2) Stop ForensicVM after Logging in to the Web Remote Screen

To stop the forensicVM through the web remote screen interface, you need to:

1) Locate the stop icon.

2) Press the stop button to halt the virtual machine.

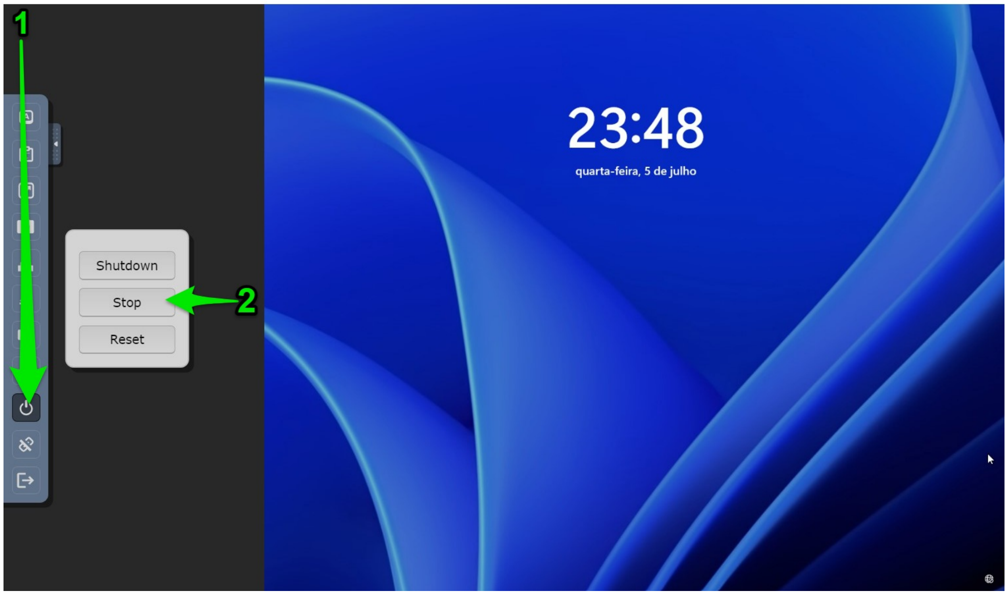


Fig. 7.47: Stop VM on the web remote screen

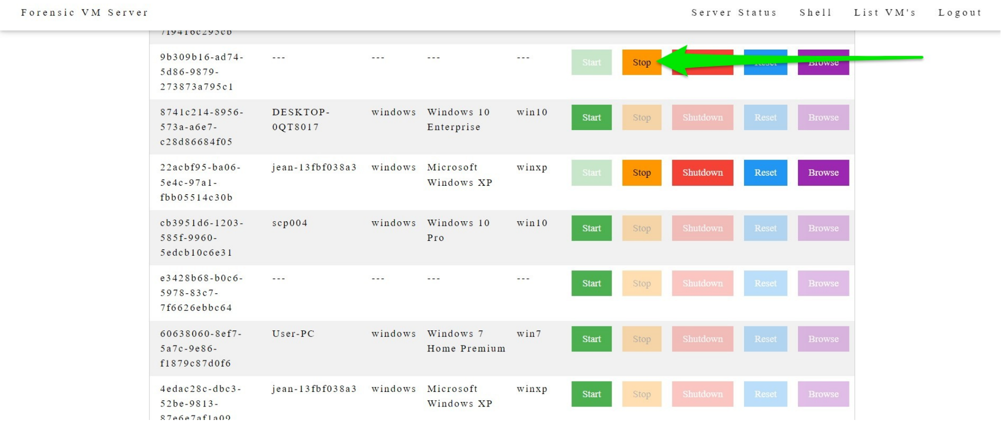
7.6.3 3) Stop ForensicVM on the Web Interface

Another option to stop the forensicVM is from the web interface. This method may be preferred if you are working remotely or through a particular service interface:

a) Navigate to the web interface.

b) Locate the machine that you need to stop.

c) Locate and click the stop button, as shown in the figure below.


Forensic VM Server   Server Status   Shell   List VM's   Logout

719416c295cb									
9b309b16-ad74-5d86-9879-273873a795c1	---	---	---	---	Start	Stop		Reset	Browse
8741c214-8956-573a-a6e7-c28d86684f05	DESKTOP-0QT8017	windows	Windows 10 Enterprise	win10	Start	Stop	Shutdown	Reset	Browse
22acbf95-ba06-5e4c-97a1-fbb05514c30b	jean-13fbf038a3	windows	Microsoft Windows XP	winxp	Start	Stop	Shutdown	Reset	Browse
cb3951d6-1203-585f-9960-5edcb10c6e31	scp004	windows	Windows 10 Pro	win10	Start	Stop	Shutdown	Reset	Browse
e3428b68-b0c6-5978-83c7-7f6626ebbc64	---	---	---	---	Start	Stop	Shutdown	Reset	Browse
60638060-8ef7-5a7c-9e86-f1879c87d0f6	User-PC	windows	Windows 7 Home Premium	win7	Start	Stop	Shutdown	Reset	Browse
4edac28c-dbc3-52be-9813-87e6e7af1a09	jean-13fbf038a3	windows	Microsoft Windows XP	winxp	Start	Stop	Shutdown	Reset	Browse

Fig. 7.48: Stop VM on the web interface

These three methods ensure that you can stop the forensicVM from various points in the system, allowing for seamless control depending on your needs and preferences.

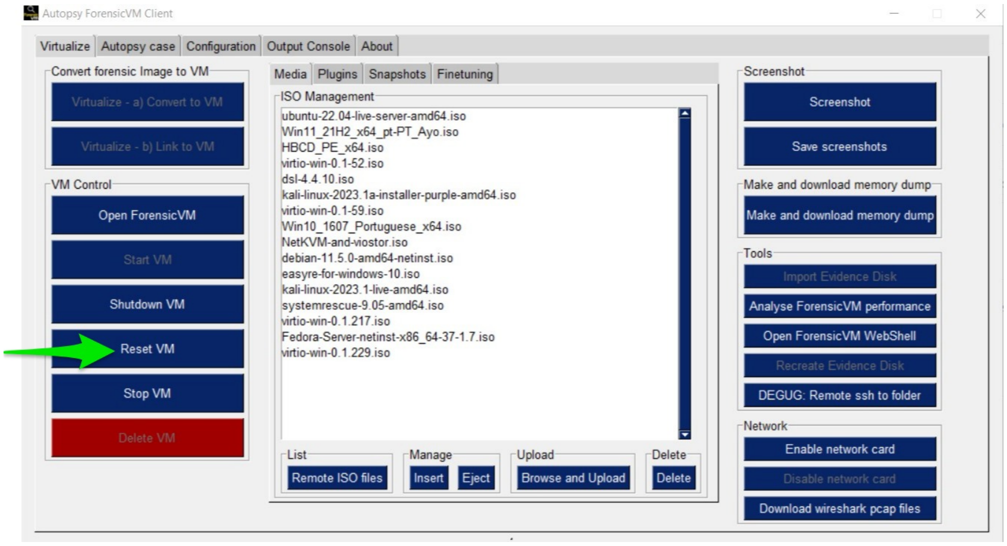
7.7 Resetting the Virtual Machine (VM)

Resetting the forensic virtual machine (forensicVM) is akin to an immediate reboot, and there are three different ways to do so. These methods provide flexibility depending on your access level and location within the system interface:

7.7.1 Reset ForensicVM in the Main Plugin Interface

To reset the forensicVM from the main plugin interface, follow these simple steps:

a) Locate the reset button on the main interface as depicted in the figure below.



```
ubuntu-22.04-live-server-amd64.iso
Win11_21H2_x64_pt-PT_Ayo.iso
HBCD_PE_x64.iso
virtio-win-0.1-52.iso
dsl-4.4.10.iso
kali-linux-2023.1a-installer-purple-amd64.iso
virtio-win-0.1-59.iso
Win10_1607_Portuguese_x64.iso
NetKVM-and-viostor.iso
debian-11.5.0-amd64-netinst.iso
easyre-for-windows-10.iso
kali-linux-2023.1-live-amd64.iso
systemrescue-9.05-amd64.iso
virtio-win-0.1.217.iso
Fedora-Server-netinst-x86_64-37-1.7.iso
virtio-win-0.1.229.iso
```

Fig. 7.49: Reset VM on the main interface

b) Press the reset button to immediately reboot the virtual machine.

7.7.2 Reset ForensicVM after Logging in to the Web Remote Screen

To reset the forensicVM through the web remote screen interface, you need to:

1) Locate the reset icon.

2) Press the reset button to immediately reboot the virtual machine.

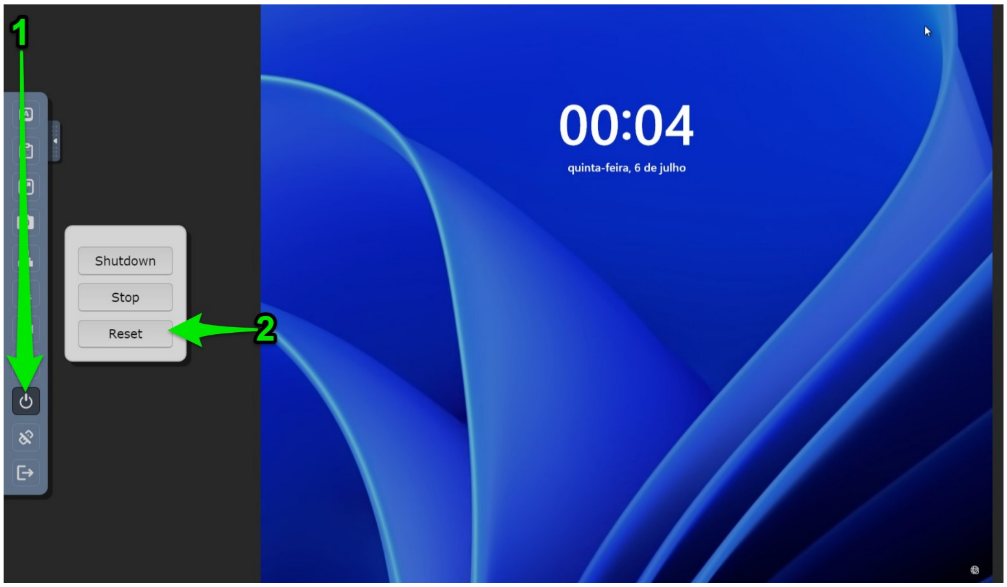


Fig. 7.50: Reset VM on the web remote screen

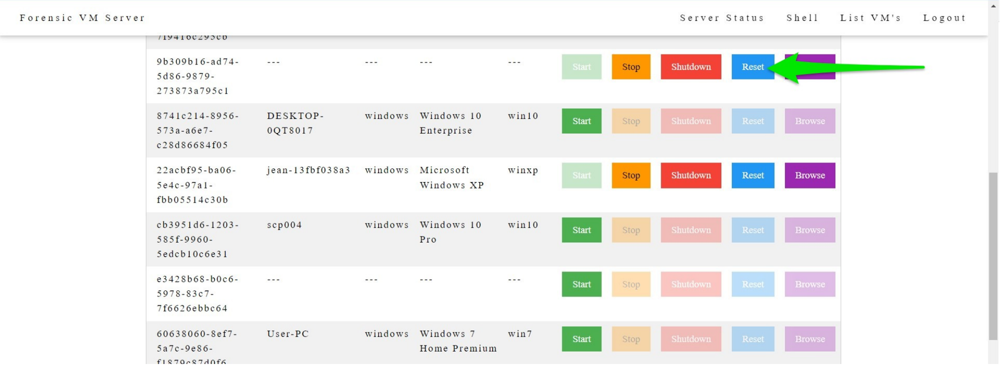
7.7.3 Reset ForensicVM on the Web Interface

Another option to reset the forensicVM is from the web interface. This method may be preferred if you are working remotely or through a particular service interface:

a) Navigate to the web interface.

b) Locate the machine that you need to reset.

c) Locate and click the reset button, as shown in the figure below.



719416c295cb									
9b309b16-ad74-5d86-9879-273873a795c1	---	---	---	---	Start	Stop	Shutdown	Reset	
8741c214-8956-573a-a6e7-c28d86684f05	DESKTOP-0QT8017	windows	Windows 10 Enterprise	win10	Start	Stop	Shutdown	Reset	Browse
22acbf95-ba06-5e4c-97a1-fbb05514c30b	jean-13fbf038a3	windows	Microsoft Windows XP	winxp	Start	Stop	Shutdown	Reset	Browse
cb3951d6-1203-585f-9960-5edcb10c6e31	scp004	windows	Windows 10 Pro	win10	Start	Stop	Shutdown	Reset	Browse
e3428b68-b0c6-5978-83c7-7f6626ebbc64	---	---	---	---	Start	Stop	Shutdown	Reset	Browse
60638060-8ef7-5a7c-9e86-f1879c87d0f6	User-PC	windows	Windows 7 Home Premium	win7	Start	Stop	Shutdown	Reset	Browse

Fig. 7.51: Reset VM on the web interface

These three methods ensure that you can reset the forensicVM from various points in the system, allowing for immediate rebooting as needed. This can be useful in various scenarios, such as when troubleshooting, testing, or managing different virtual machine states.

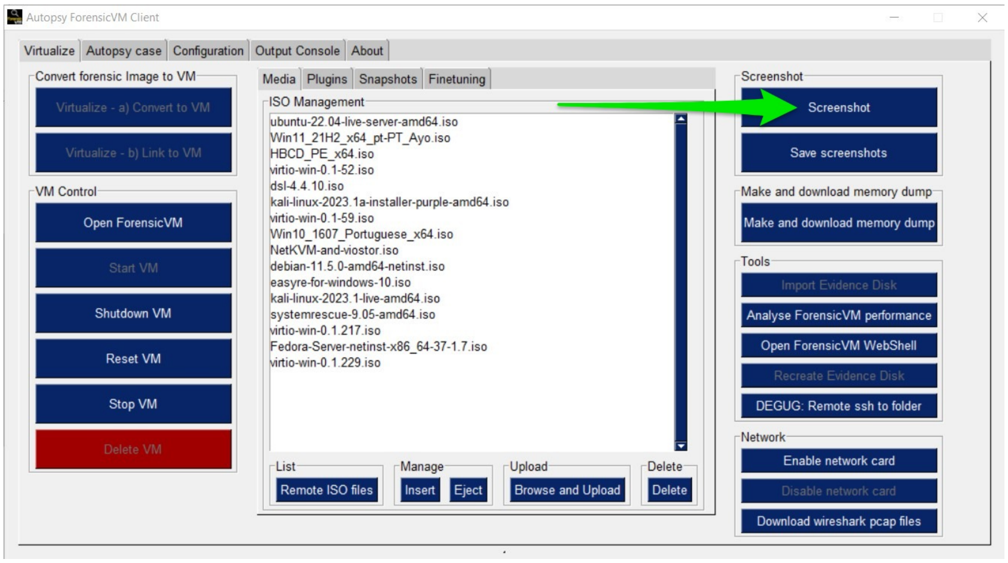
7.8 Making and importing Screenshots

7.8.1 Making screenshots

It is often necessary to take screenshots of the forensic virtual machine (forensicVM) for documentation, analysis, or reporting purposes. There are two primary ways to capture a screenshot, depending on your location within the system interface:

1) Capture Screenshot in the Main Autopsy Plugin Interface

To take a screenshot of the forensicVM from the main Autopsy plugin interface, please press the Screenshot button on the screenshot panel:



ubuntu-22.04-live-server-amd64.iso
Win11_21H2_x64_pt-PT_Ayo.iso
HBCD_PE_x64.iso
virtio-win-0.1-52.iso
dsl-4.4.10.iso
kali-linux-2023.1a-installer-purple-amd64.iso
virtio-win-0.1-59.iso
Win10_1607_Portuguese_x64.iso
NetKVM-and-viostor.iso
debian-11.5.0-amd64-netinst.iso
easyre-for-windows-10.iso
kali-linux-2023.1-live-amd64.iso
systemrescue-9.05-amd64.iso
virtio-win-0.1.217.iso
Fedora-Server-netinst-x86_64-37-1.7.iso
virtio-win-0.1.229.iso

Fig. 7.52: Screenshot VM on the main Autopsy plugin interface

2) Capture Screenshot in the Web Screen Interface

Capturing a screenshot from the web screen interface is similarly straightforward:

a) Navigate to the web interface where the forensicVM is displayed. Expand the tools panel.

b) Locate the screenshot icon or use the appropriate key command within the web interface.

c) Press the camera icon to take a screenshot.

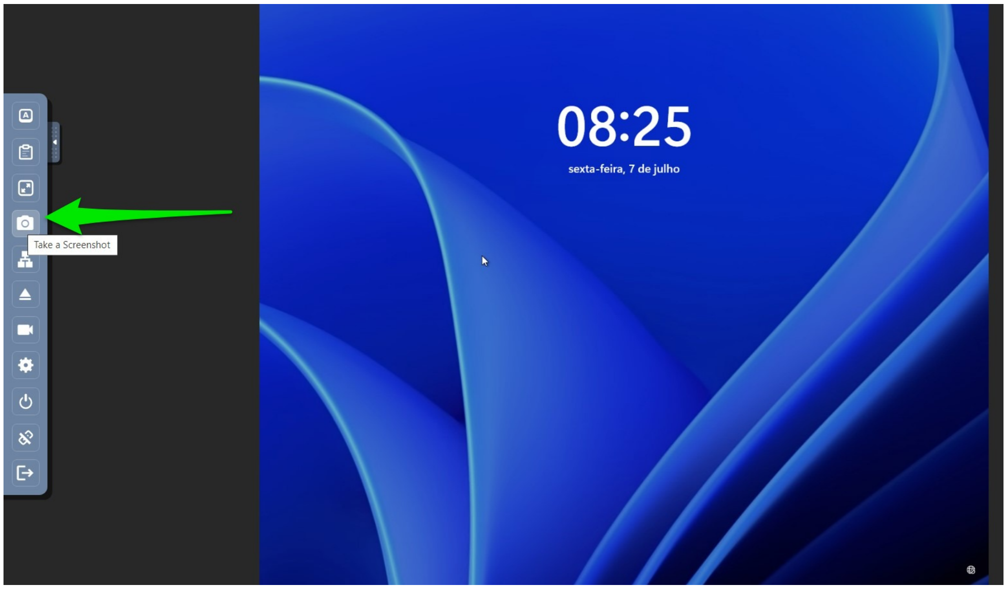


Fig. 7.53: Screenshot VM on the web screen interface

These methods enable you to capture visual records of the forensicVM from different points within the system, providing flexibility for various operational needs.

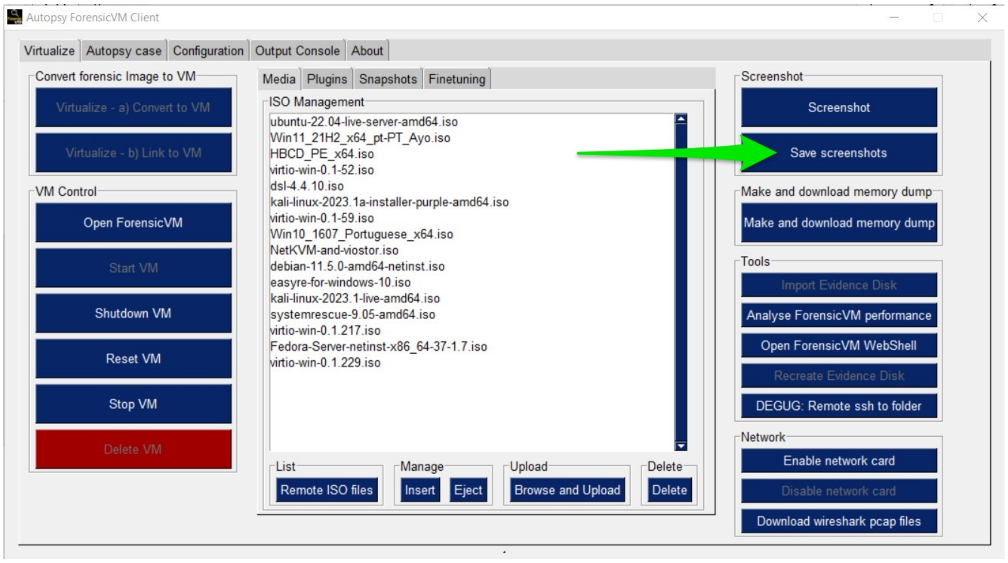
7.8.2 Downloading Screenshots as a ZIP File

After capturing the necessary screenshots of the forensic virtual machine (forensicVM), you can download them all as a ZIP file. This process is done in four steps:

1) Press the Save Screenshots Button

a) Navigate to the screenshots panel within the plugin interface.

b) Locate and press the “Save Screenshots” button.



```
ubuntu-22.04-live-server-amd64.iso
Win11_21H2_x64_pt-PT_Ayo.iso
HBCD_PE_x64.iso
virtio-win-0.1-52.iso
dsl-4.4.10.iso
kali-linux-2023.1a-installer-purple-amd64.iso
virtio-win-0.1-59.iso
Win10_1607_Portuguese_x64.iso
NetKVM-and-viostor.iso
debian-11.5.0-amd64-netinst.iso
easyre-for-windows-10.iso
kali-linux-2023.1-live-amd64.iso
systemrescue-9.05-amd64.iso
virtio-win-0.1.217.iso
Fedora-Server-netinst-x86_64-37-1.7.iso
virtio-win-0.1.229.iso
```

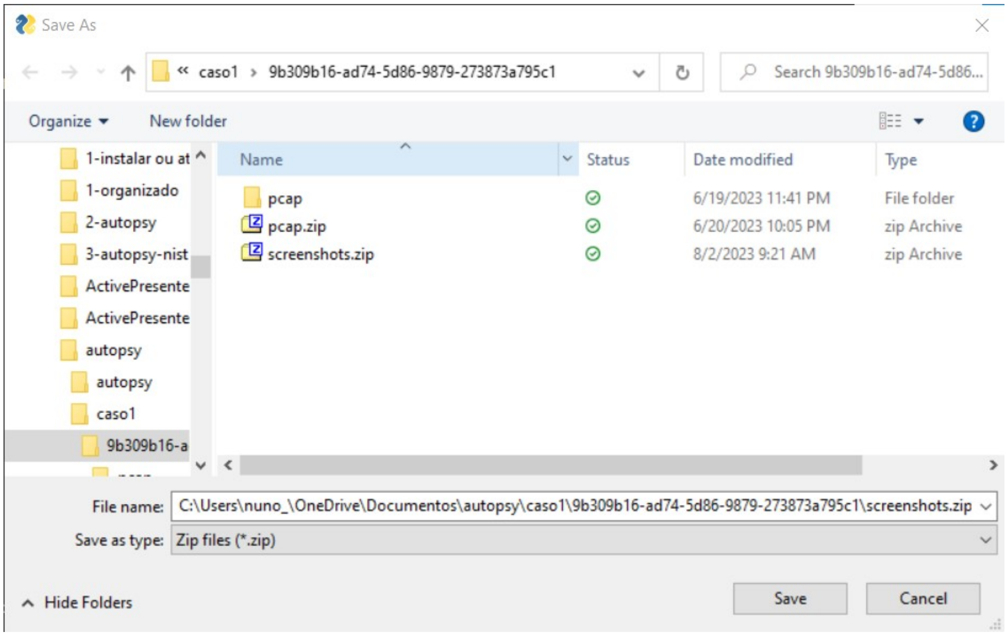
Fig. 7.54: Save screenshots button on the plugin interface

2) Save As Dialogue with Default Path

a) You will be presented with a “Save As” dialog box.

b) The default path for saving will be the forensic image path inside the Autopsy case path.

c) Confirm the save location and proceed.



Name	Status	Date modified	Type
pcap	✓	6/19/2023 11:41 PM	File folder
pcap.zip	✓	6/20/2023 10:05 PM	zip Archive
screenshots.zip	✓	8/2/2023 9:21 AM	zip Archive

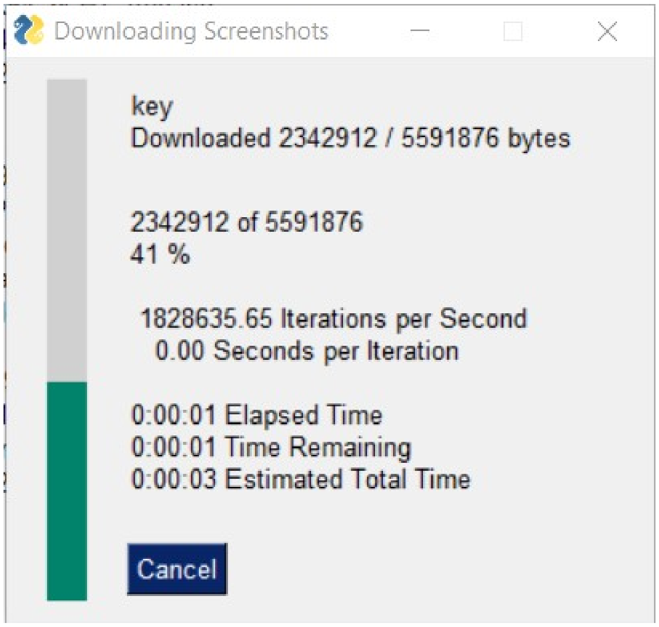
File name: C:\Users\nuno_\OneDrive\Documentos\autopsy\caso1\9b309b16-ad74-5d86-9879-273873a795c1\screenshots.zip

Save as type: Zip files (*.zip)

Fig. 7.55: Save As dialog with default path

3) Download Progress and Success Alert

a) A download progress bar will appear, showing the status of the download.



key
Downloaded 2342912 / 5591876 bytes

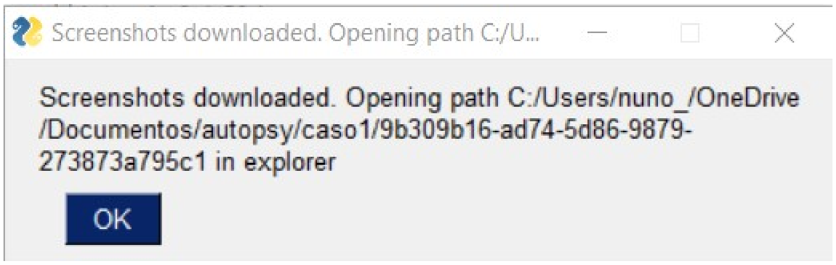
2342912 of 5591876
41 %

1828635.65 Iterations per Second
0.00 Seconds per Iteration

0:00:01 Elapsed Time
0:00:01 Time Remaining
0:00:03 Estimated Total Time

Fig. 7.56: Download progress

b) Once the download is complete, an alert box will appear, saying that the screenshots were successfully downloaded.



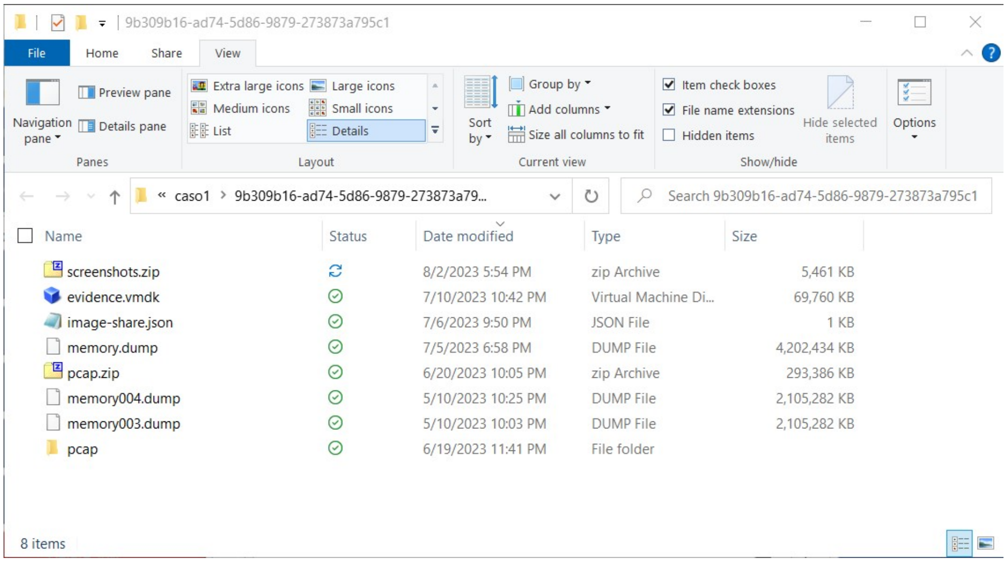
Screenshots downloaded. Opening path C:/Users/nuno_/OneDrive /Documentos/autopsy/caso1/9b309b16-ad74-5d86-9879-273873a795c1 in explorer

Fig. 7.57: Success alert

4) Open Windows Path with Screenshots.zip

a) The Windows path where the *screenshots.zip* file is saved will be opened in Windows Explorer.

b) You can then access the ZIP file containing all the screenshots.



Name	Status	Date modified	Type	Size
screenshots.zip		8/2/2023 5:54 PM	zip Archive	5,461 KB
evidence.vmdk		7/10/2023 10:42 PM	Virtual Machine Di...	69,760 KB
image-share.json		7/6/2023 9:50 PM	JSON File	1 KB
memory.dump		7/5/2023 6:58 PM	DUMP File	4,202,434 KB
pcap.zip		6/20/2023 10:05 PM	zip Archive	293,386 KB
memory004.dump		5/10/2023 10:25 PM	DUMP File	2,105,282 KB
memory003.dump		5/10/2023 10:03 PM	DUMP File	2,105,282 KB
pcap		6/19/2023 11:41 PM	File folder	

Fig. 7.58: Windows path with screenshots.zip

These steps ensure an efficient and organized process for downloading the captured screenshots of the forensicVM, making it convenient for further use or analysis.

7.8.3 Importing Screenshots to Autopsy Software

1) Unzip Your Screenshots with Your Favorite ZIP Program (e.g., 7-Zip)

Start by extracting the ZIP file containing your screenshots. Using a tool like 7-Zip, right-click the ZIP file and choose the extraction option.

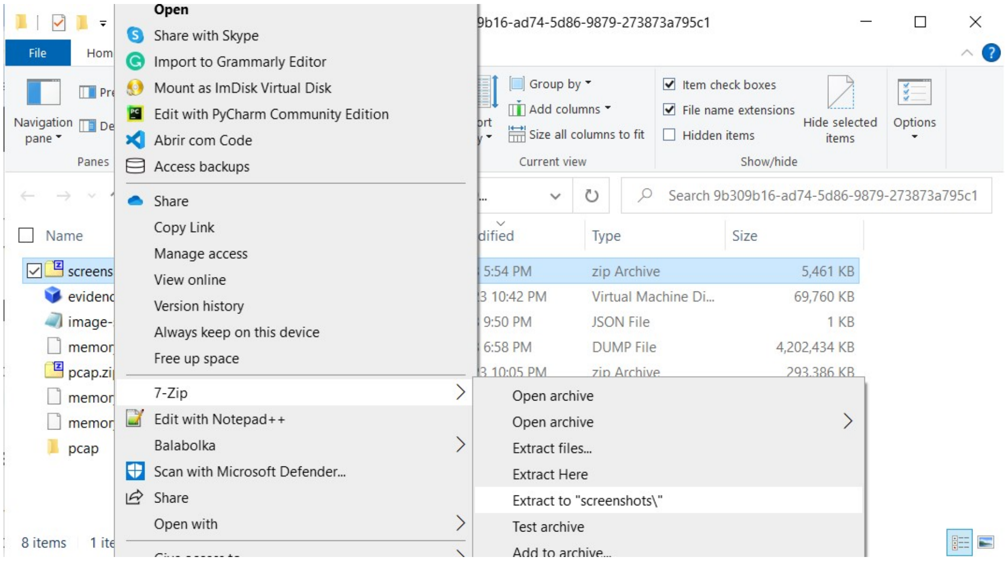
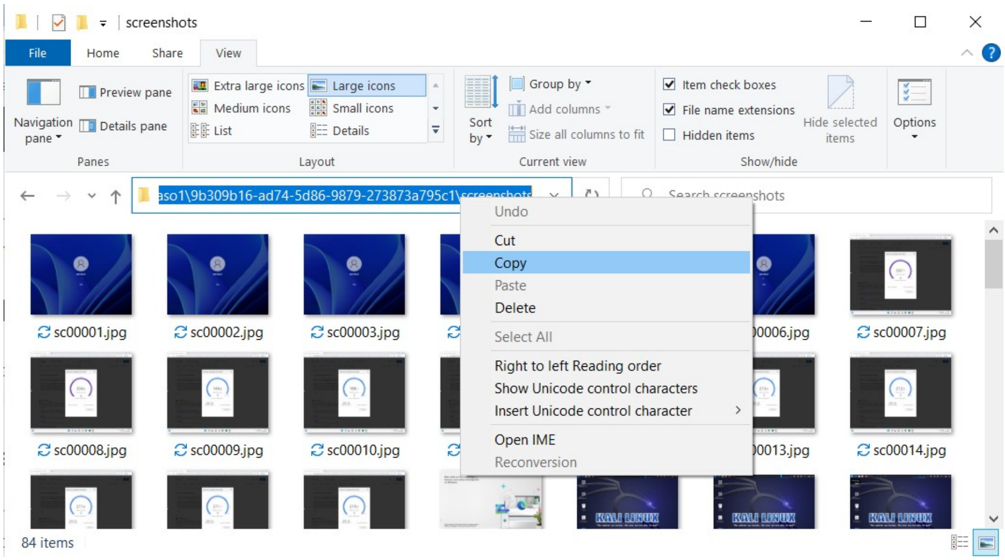


Fig. 7.59: Unzip screenshots using 7-Zip

2) Copy Screenshot Path in Explorer

Navigate to the folder where the screenshots were extracted and copy the full path from the address bar in Explorer.

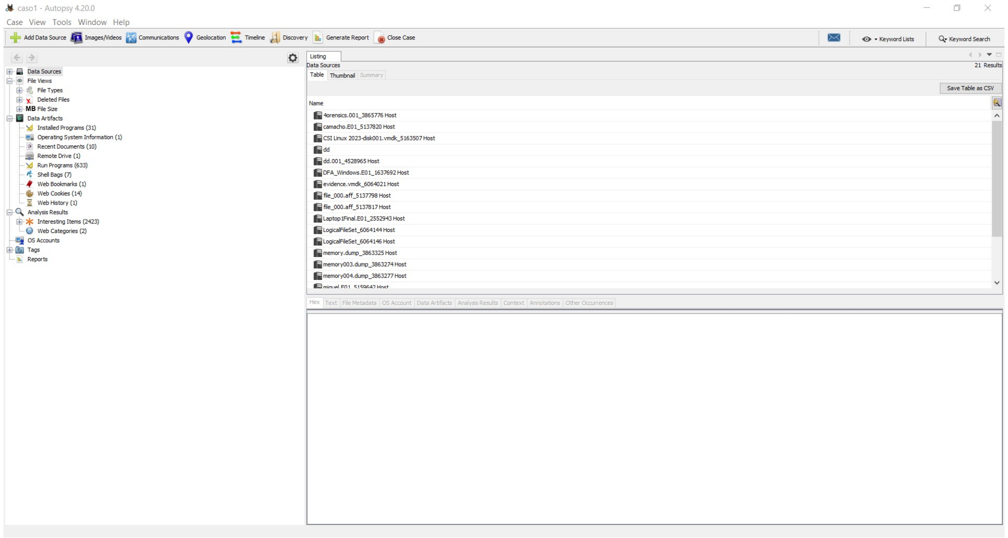


aso1\9b309b16-ad74-5d86-9879-273873a795c1\screenshots

Fig. 7.60: Copy screenshot path in Explorer

3) Add a New Data Source

Open Autopsy and initiate the process of adding a new data source by selecting the relevant option in the interface.

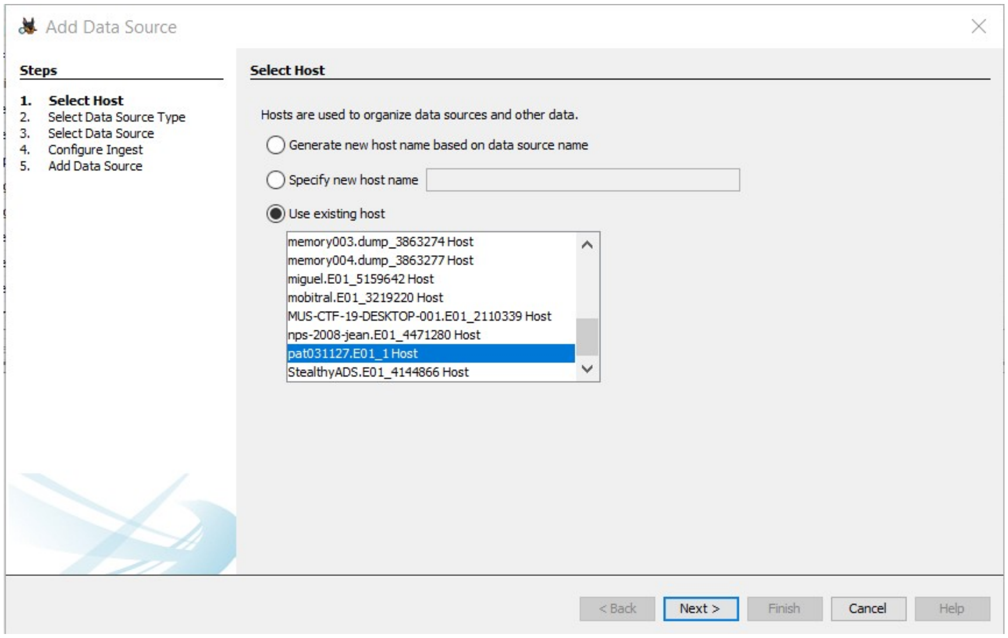


Name
4orensics.001_3865776 Host
camacho.E01_5137820 Host
CSI Linux 2023-disk001.vmdk_5163507 Host
dd
dd.001_4528965 Host
DFA_Windows.E01_1637692 Host
evidence.vmdk_6064021 Host
file_000.aff_5137798 Host
file_000.aff_5137817 Host
Laptop1Final.E01_2552943 Host
LogicalFileSet_6064144 Host
LogicalFileSet_6064146 Host
memory.dump_3863325 Host
memory003.dump_3863274 Host
memory004.dump_3863277 Host
miguel.E01_5159642 Host

Fig. 7.61: Add a new data source

4) Select the Host for Which You Have to Import the Screenshots

Choose the appropriate host for which you want to import the screenshots.



Add Data Source

Steps

1. **Select Host**
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source

Select Host

Hosts are used to organize data sources and other data.

○ Generate new host name based on data source name

○ Specify new host name

● Use existing host

- memory003.dump_3863274 Host
- memory004.dump_3863277 Host
- miguel.E01_5159642 Host
- mobitral.E01_3219220 Host
- MUS-CTF-19-DESKTOP-001.E01_2110339 Host
- nps-2008-jean.E01_4471280 Host
- pat031127.E01_1 Host
- StealthyADS.E01_4144866 Host

Fig. 7.62: Select the host

5) Select Logical Files as the Data Source

Select “Logical Files” as the type of data source for importing the screenshots.

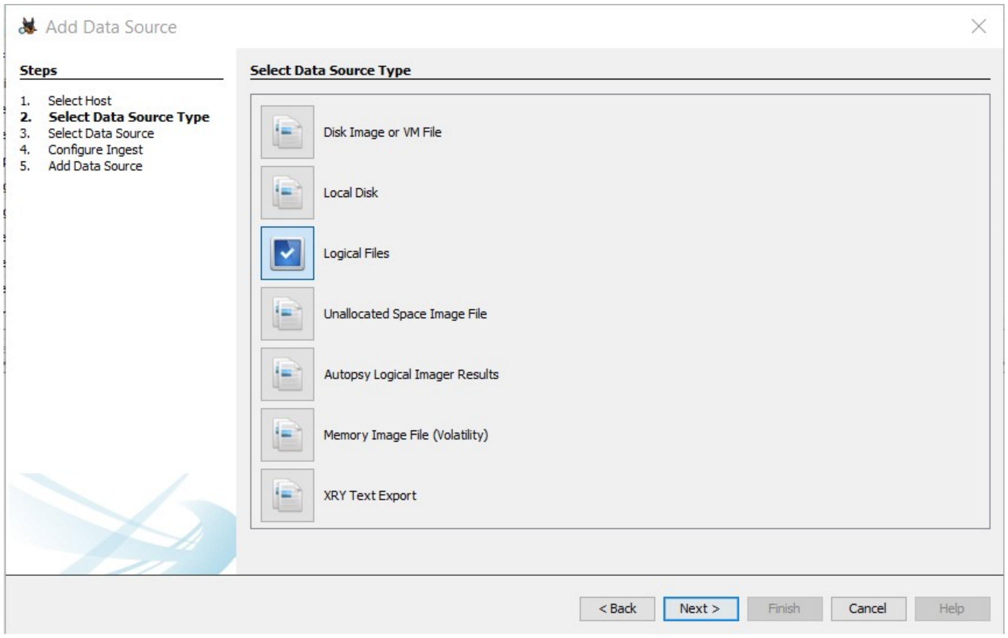
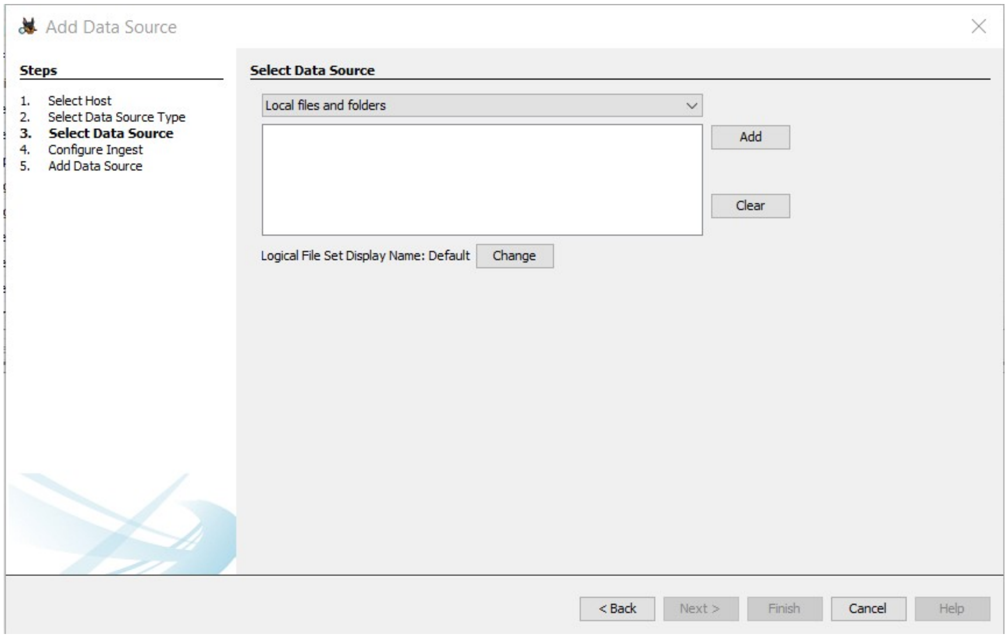


Fig. 7.63: Select Logical Files as the data source

6) Click the Button “Add” to Add a New Logical Data Source Folder

Click the “Add” button to create a new folder for the logical data source where the screenshots are stored.



Add Data Source

Steps

1. Select Host
2. Select Data Source Type
3. **Select Data Source**
4. Configure Ingest
5. Add Data Source

Select Data Source

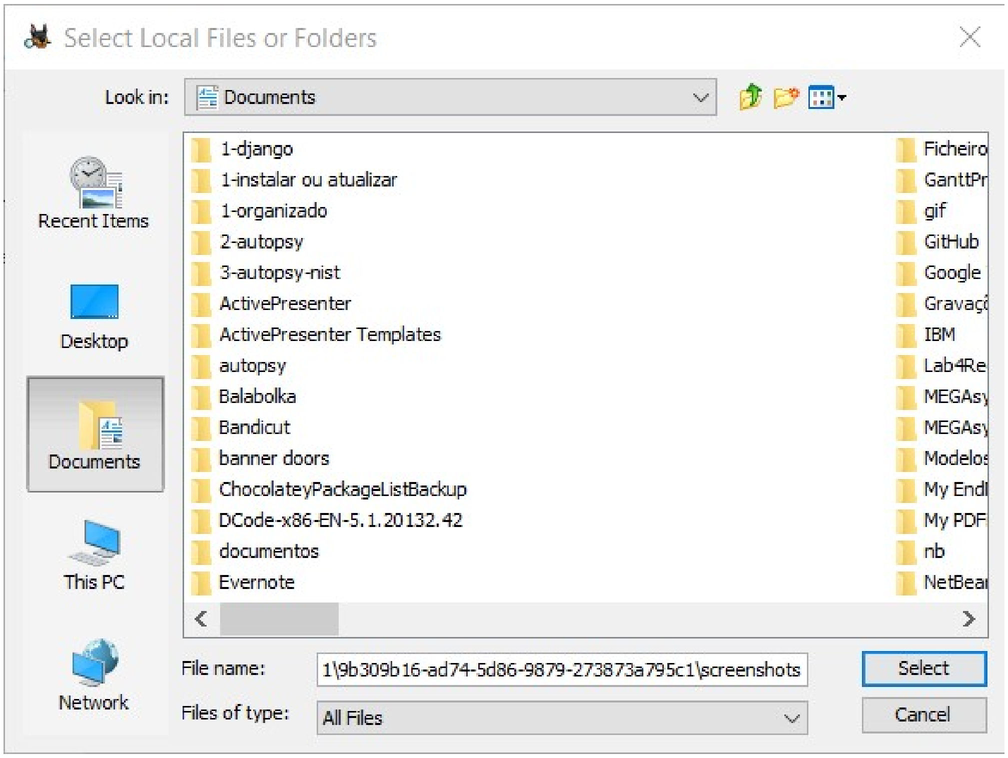
Local files and folders

Logical File Set Display Name: Default

Fig. 7.64: Click “Add” button

7) Paste the Path of the Screenshots and Press “Select”

Paste the previously copied path of the screenshots into the designated field and press the “Select” button.



Look in: Documents

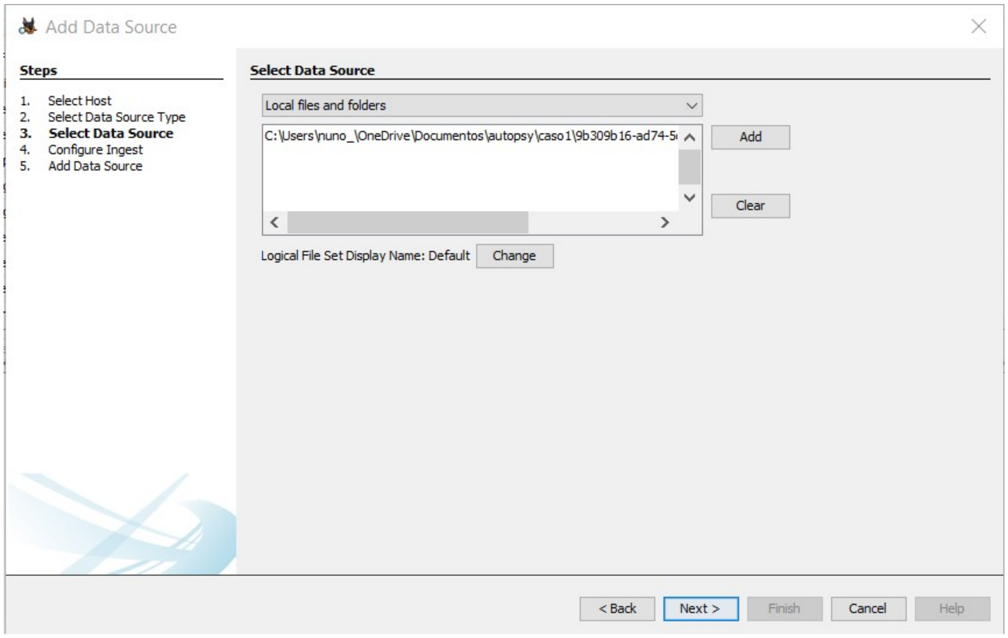
File name: 1\9b309b16-ad74-5d86-9879-273873a795c1\screenshots

Files of type: All Files

Fig. 7.65: Paste the path and press “Select”

8) Press “Next”

Press the “Next” button to proceed to the following step of the configuration.



Local files and folders

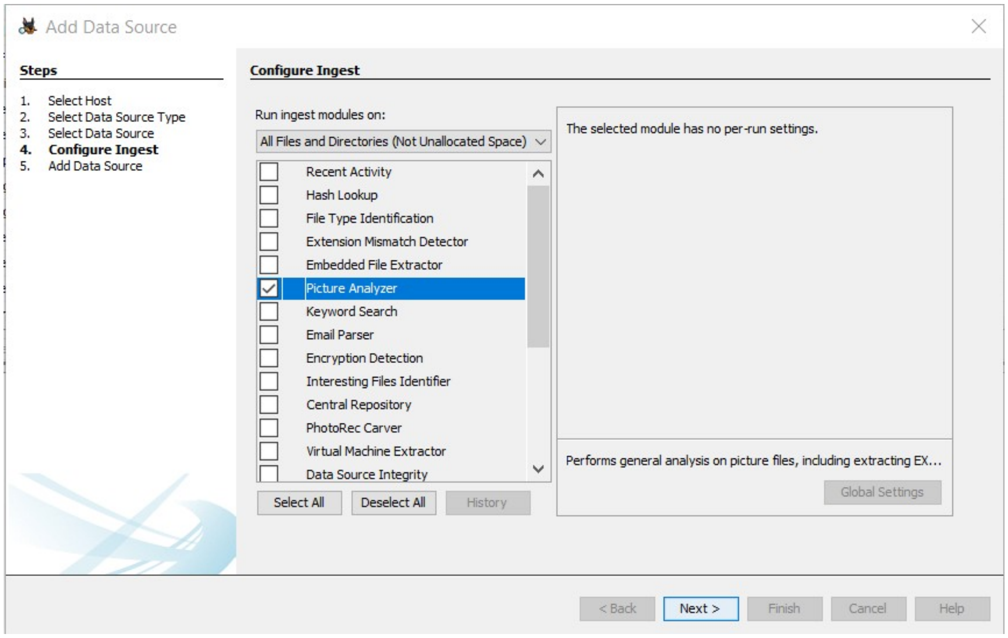
C:\Users\nuno_\OneDrive\Documentos\autopsy\caso1\9b309b16-ad74-5

Logical File Set Display Name: Default

Fig. 7.66: Press “Next”

9) Deselect All Plugins. Select the Ingest Plugin “Picture Analyser.” Press “Next”

Deselect any unnecessary plugins and select only the “Picture Analyser” plugin, then press “Next.”



Run ingest modules on: All Files and Directories (Not Unallocated Space)

- □ Recent Activity
- □ Hash Lookup
- □ File Type Identification
- □ Extension Mismatch Detector
- □ Embedded File Extractor
- ☑ Picture Analyzer
- □ Keyword Search
- □ Email Parser
- □ Encryption Detection
- □ Interesting Files Identifier
- □ Central Repository
- □ PhotoRec Carver
- □ Virtual Machine Extractor
- □ Data Source Integrity

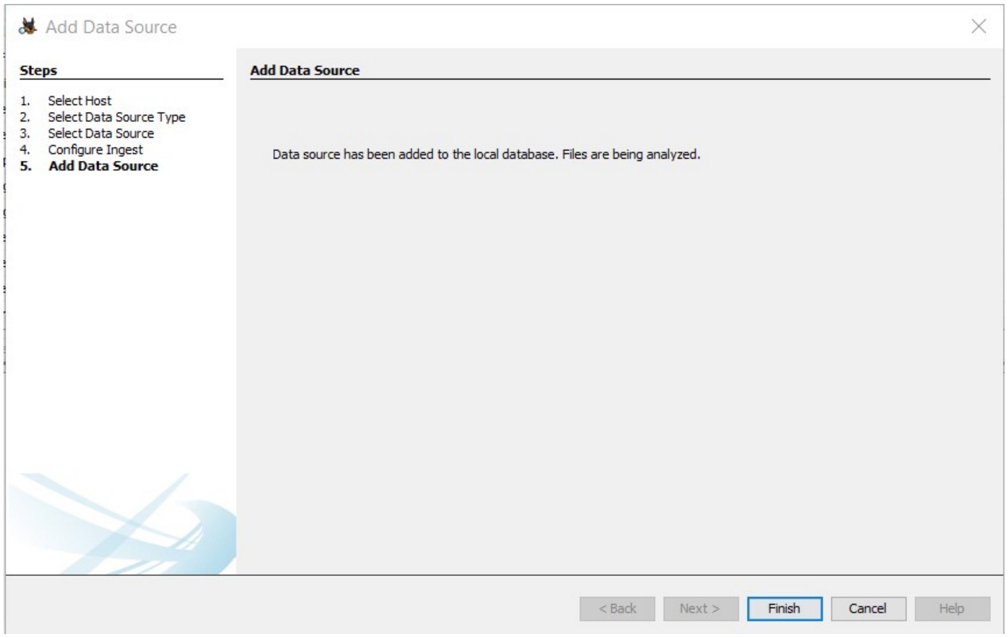
The selected module has no per-run settings.

Performs general analysis on picture files, including extracting EX...

Fig. 7.67: Select “Picture Analyser” plugin

10) Press “Finish”

Press the “Finish” button to complete the configuration and begin the import process.



Add Data Source

Steps

1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. **Add Data Source**

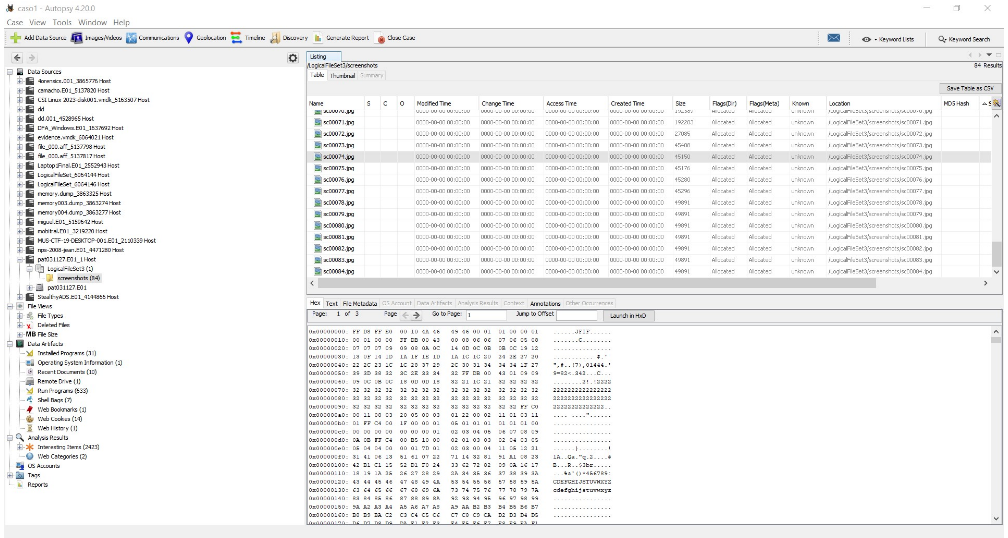
Add Data Source

Data source has been added to the local database. Files are being analyzed.

Fig. 7.68: Press "Finish"

11) Browse into the Imported LogicalFileSet Inside the Data Source. Right-click the Mouse

Browse the imported LogicalFileSet inside the data source, and right-click on the specific file you want to view.



caso1 - Autopsy 4.20.0

- Data Sources
  - 4orensics.001_3865776 Host
  - camacho.E01_5137820 Host
  - CSI Linux 2023-disk001.vmdk_5163507 Host
  - dd
  - dd.001_4528965 Host
  - DFA_Windows.E01_1637692 Host
  - evidence.vmdk_6064021 Host
  - file_000.aff_5137798 Host
  - file_000.aff_5137817 Host
  - Laptop1Final.E01_2552943 Host
  - LogicalFileSet_6064144 Host
  - LogicalFileSet_6064146 Host
  - memory.dump_3863325 Host
  - memory003.dump_3863274 Host
  - memory004.dump_3863277 Host
  - miguel.E01_5159642 Host
  - mobitral.E01_3219220 Host
  - MUS-CTF-19-DESKTOP-001.E01_2110339 Host
  - nps-2008-jean.E01_4471280 Host
  - pat031127.E01_1 Host
    - LogicalFileSet3 (1)
      - screenshots (84)
    - pat031127.E01
  - StealthyADS.E01_4144866 Host
- File Views
  - File Types
  - Deleted Files
  - MB File Size
- Data Artifacts
  - Installed Programs (31)
  - Operating System Information (1)
  - Recent Documents (10)
  - Remote Drive (1)
  - Run Programs (633)
  - Shell Bags (7)
  - Web Bookmarks (1)
  - Web Cookies (14)
  - Web History (1)
- Analysis Results
  - Interesting Items (2423)
  - Web Categories (2)
- OS Accounts
- Tags
- Reports

Listing

/LogicalFileSet3/screenshots 84 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location	MD5 Hash
sc00070.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	192389	Allocated	Allocated	unknown	/LogicalFileSet3/screenshots/sc00070.jpg	
sc00071.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	192283	Allocated	Allocated	unknown	/LogicalFileSet3/screenshots/sc00071.jpg	
sc00072.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	27085	Allocated	Allocated	unknown	/LogicalFileSet3/screenshots/sc00072.jpg	
sc00073.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	45408	Allocated	Allocated	unknown	/LogicalFileSet3/screenshots/sc00073.jpg	
sc00074.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	45150	Allocated	Allocated	unknown	/LogicalFileSet3/screenshots/sc00074.jpg	
sc00075.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	45176	Allocated	Allocated	unknown	/LogicalFileSet3/screenshots/sc00075.jpg	
sc00076.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	45280	Allocated	Allocated	unknown	/LogicalFileSet3/screenshots/sc00076.jpg	
sc00077.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	45296	Allocated	Allocated	unknown	/LogicalFileSet3/screenshots/sc00077.jpg	
sc00078.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	49891	Allocated	Allocated	unknown	/LogicalFileSet3/screenshots/sc00078.jpg	
sc00079.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	49891	Allocated	Allocated	unknown	/LogicalFileSet3/screenshots/sc00079.jpg	
sc00080.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	49891	Allocated	Allocated	unknown	/LogicalFileSet3/screenshots/sc00080.jpg	
sc00081.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	49891	Allocated	Allocated	unknown	/LogicalFileSet3/screenshots/sc00081.jpg	
sc00082.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	49891	Allocated	Allocated	unknown	/LogicalFileSet3/screenshots/sc00082.jpg	
sc00083.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	49891	Allocated	Allocated	unknown	/LogicalFileSet3/screenshots/sc00083.jpg	
sc00084.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	49891	Allocated	Allocated	unknown	/LogicalFileSet3/screenshots/sc00084.jpg	

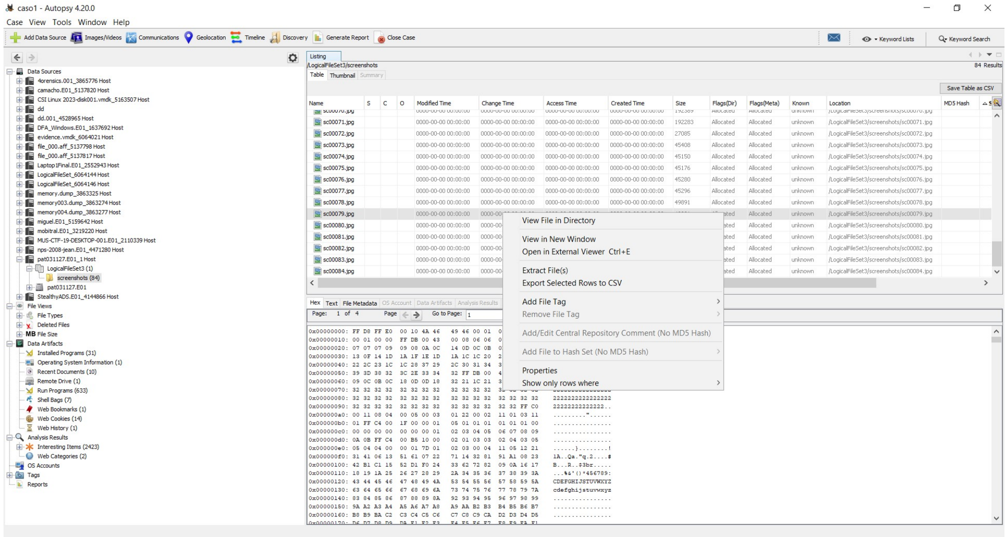
Page: 1 of 3 Page Go to Page: 1 Jump to Offset

```
0x00000000: FF D8 FF E0  00 10 4A 46  49 46 00 01  01 00 00 01   ......JFIF......
0x00000010: 00 01 00 00  FF DB 00 43  00 08 06 06  07 06 05 08   .......C........
0x00000020: 07 07 07 09  09 08 0A 0C  14 0D 0C 0B  0B 0C 19 12   ................
0x00000030: 13 0F 14 1D  1A 1F 1E 1D  1A 1C 1C 20  24 2E 27 20   ........... $.'
0x00000040: 22 2C 23 1C  1C 28 37 29  2C 30 31 34  34 34 1F 27   ",#..(7),01444.'
0x00000050: 39 3D 38 32  3C 2E 33 34  32 FF DB 00  43 01 09 09   9=82<.342...C...
0x00000060: 09 0C 0B 0C  18 0D 0D 18  32 21 1C 21  32 32 32 32   ........2!.!2222
0x00000070: 32 32 32 32  32 32 32 32  32 32 32 32  32 32 32 32   2222222222222222
0x00000080: 32 32 32 32  32 32 32 32  32 32 32 32  32 32 32 32   2222222222222222
0x00000090: 32 32 32 32  32 32 32 32  32 32 32 32  32 32 FF C0   22222222222222..
0x000000a0: 00 11 08 03  20 05 00 03  01 22 00 02  11 01 03 11   .... ....".......
0x000000b0: 01 FF C4 00  1F 00 00 01  05 01 01 01  01 01 01 00   ................
0x000000c0: 00 00 00 00  00 00 00 01  02 03 04 05  06 07 08 09   ................
0x000000d0: 0A 0B FF C4  00 B5 10 00  02 01 03 03  02 04 03 05   ................
0x000000e0: 05 04 04 00  00 01 7D 01  02 03 00 04  11 05 12 21   ......}........!
0x000000f0: 31 41 06 13  51 61 07 22  71 14 32 81  91 A1 08 23   1A..Qa."q.2....#
0x00000100: 42 B1 C1 15  52 D1 F0 24  33 62 72 82  09 0A 16 17   B...R..$3br.....
0x00000110: 18 19 1A 25  26 27 28 29  2A 34 35 36  37 38 39 3A   ...%&'()*456789:
0x00000120: 43 44 45 46  47 48 49 4A  53 54 55 56  57 58 59 5A   CDEFGHIJSTUVWXYZ
0x00000130: 63 64 65 66  67 68 69 6A  73 74 75 76  77 78 79 7A   cdefghijstuvwxyz
0x00000140: 83 84 85 86  87 88 89 8A  92 93 94 95  96 97 98 99   ................
0x00000150: 9A A2 A3 A4  A5 A6 A7 A8  A9 AA B2 B3  B4 B5 B6 B7   ................
0x00000160: B8 B9 BA C2  C3 C4 C5 C6  C7 C8 C9 CA  D2 D3 D4 D5   ................
```

Fig. 7.69: Browse into LogicalFileSet

12) Select "Open in External Viewer" or Press CTRL+E

Select the "Open in External Viewer" option from the context menu, or simply press CTRL+E on your keyboard.



/LogicalFileSet3/screenshots

84 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location	MD5 Hash
sc00071.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	192283	Allocated	Allocated	unknown	/LogicalFileSet3/screenshots/sc00071.jpg	
sc00072.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	27085	Allocated	Allocated	unknown	/LogicalFileSet3/screenshots/sc00072.jpg	
sc00073.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	45408	Allocated	Allocated	unknown	/LogicalFileSet3/screenshots/sc00073.jpg	
sc00074.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	45150	Allocated	Allocated	unknown	/LogicalFileSet3/screenshots/sc00074.jpg	
sc00075.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	45176	Allocated	Allocated	unknown	/LogicalFileSet3/screenshots/sc00075.jpg	
sc00076.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	45280	Allocated	Allocated	unknown	/LogicalFileSet3/screenshots/sc00076.jpg	
sc00077.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	45296	Allocated	Allocated	unknown	/LogicalFileSet3/screenshots/sc00077.jpg	
sc00078.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	49891	Allocated	Allocated	unknown	/LogicalFileSet3/screenshots/sc00078.jpg	
sc00079.jpg				0000-00-00 00:00:00						Allocated	unknown	/LogicalFileSet3/screenshots/sc00079.jpg	
sc00080.jpg				0000-00-00 00:00:00						Allocated	unknown	/LogicalFileSet3/screenshots/sc00080.jpg	
sc00081.jpg				0000-00-00 00:00:00						Allocated	unknown	/LogicalFileSet3/screenshots/sc00081.jpg	
sc00082.jpg				0000-00-00 00:00:00						Allocated	unknown	/LogicalFileSet3/screenshots/sc00082.jpg	
sc00083.jpg				0000-00-00 00:00:00						Allocated	unknown	/LogicalFileSet3/screenshots/sc00083.jpg	
sc00084.jpg				0000-00-00 00:00:00						Allocated	unknown	/LogicalFileSet3/screenshots/sc00084.jpg	

Page: 1 of 4

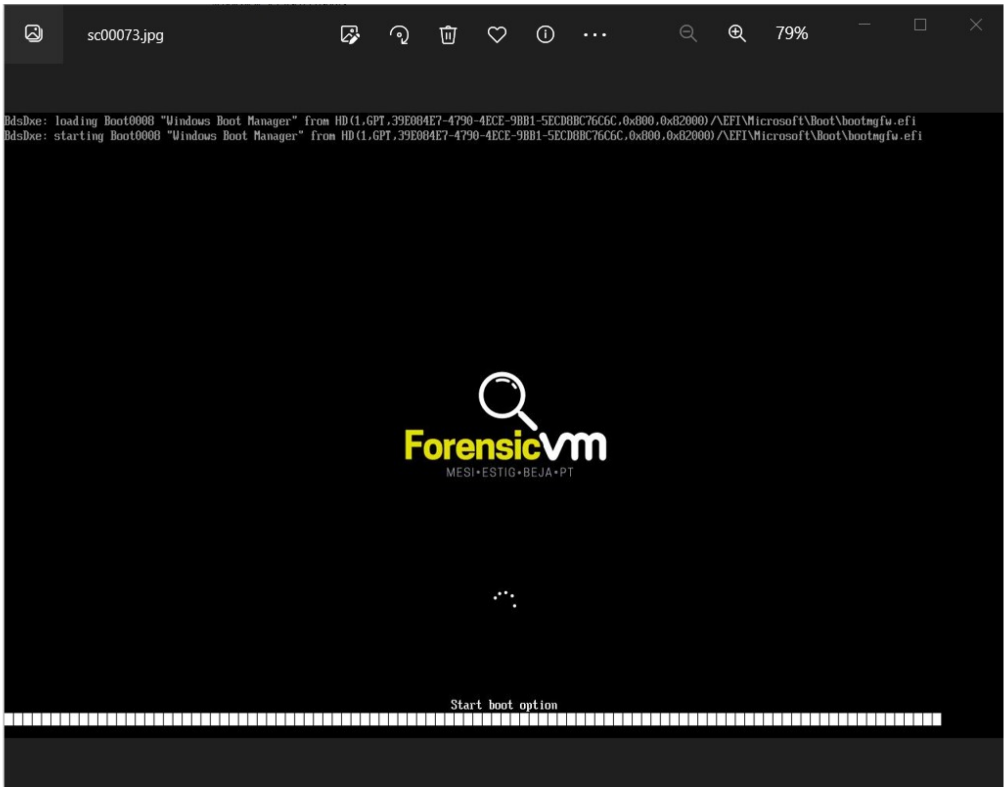
Go to Page: 1

```
0x00000000: FF D8 FF E0  00 10 4A 46  49 46 00 01
0x00000010: 00 01 00 00  FF DB 00 43  00 08 06 06
0x00000020: 07 07 07 09  09 08 0A 0C  14 0D 0C 0B
0x00000030: 13 0F 14 1D  1A 1F 1E 1D  1A 1C 1C 20
0x00000040: 22 2C 23 1C  1C 28 37 29  2C 30 31 34
0x00000050: 39 3D 38 32  3C 2E 33 34  32 FF DB 00
0x00000060: 09 0C 0B 0C  18 0D 0D 18  32 21 1C 21
0x00000070: 32 32 32 32  32 32 32 32  32 32 32 32
0x00000080: 32 32 32 32  32 32 32 32  32 32 32 32  32 32 32 32   2222222222222222
0x00000090: 32 32 32 32  32 32 32 32  32 32 32 32  32 32 FF C0   22222222222222..
0x000000a0: 00 11 08 04  00 05 00 03  01 22 00 02  11 01 03 11   ........."......
0x000000b0: 01 FF C4 00  1F 00 00 01  05 01 01 01  01 01 01 00   ................
0x000000c0: 00 00 00 00  00 00 00 01  02 03 04 05  06 07 08 09   ................
0x000000d0: 0A 0B FF C4  00 B5 10 00  02 01 03 03  02 04 03 05   ................
0x000000e0: 05 04 04 00  00 01 7D 01  02 03 00 04  11 05 12 21   ......}........!
0x000000f0: 31 41 06 13  51 61 07 22  71 14 32 81  91 A1 08 23   1A..Qa."q.2....#
0x00000100: 42 B1 C1 15  52 D1 F0 24  33 62 72 82  09 0A 16 17   B...R..$3br.....
0x00000110: 18 19 1A 25  26 27 28 29  2A 34 35 36  37 38 39 3A   ...%&'()*456789:
0x00000120: 43 44 45 46  47 48 49 4A  53 54 55 56  57 58 59 5A   CDEFGHIJSTUVWXYZ
0x00000130: 63 64 65 66  67 68 69 6A  73 74 75 76  77 78 79 7A   cdefghijstuvwxyz
0x00000140: 83 84 85 86  87 88 89 8A  92 93 94 95  96 97 98 99   ................
0x00000150: 9A A2 A3 A4  A5 A6 A7 A8  A9 AA B2 B3  B4 B5 B6 B7   ................
0x00000160: B8 B9 BA C2  C3 C4 C5 C6  C7 C8 C9 CA  D2 D3 D4 D5   ................
```

Fig. 7.70: Open in External Viewer

13) The Image is Displayed

The selected image is now displayed, allowing you to view and analyze it as needed.



```
BdsDxe: loading Boot0008 "Windows Boot Manager" from HD(1,GPT,39E084E7-4790-4ECE-9BB1-5ECD8BC76C6C,0x800,0x82000)/\EFI\Microsoft\Boot\bootmgfw.efi
BdsDxe: starting Boot0008 "Windows Boot Manager" from HD(1,GPT,39E084E7-4790-4ECE-9BB1-5ECD8BC76C6C,0x800,0x82000)/\EFI\Microsoft\Boot\bootmgfw.efi
```

```
Start boot option
```

Fig. 7.71: Image displayed

This step-by-step guide helps you efficiently import the screenshots from the forensic virtual machine into Autopsy software for in-depth analysis, enabling a streamlined workflow and enhancing your investigation process.

Note: Importance of Tagging Screenshots for Evidence

Tagging screenshots in Autopsy forensic software is a pivotal step in digital investigations. It allows forensic professionals to systematically identify, analyze, and report on crucial visual information. Tagged screenshots can be included in final reports, where they may be presented as potential evidence in legal proceedings. The process ensures the integrity of visual data and contributes significantly to building a solid case.

In the realm of digital forensics, Autopsy forensic software plays a crucial role in analyzing and managing evidence. A key feature of this powerful tool is its ability to handle screenshots, which are often vital in investigations.

Tagging Relevant Screenshots: With Autopsy, investigators can sift through various images and screenshots collected during the forensic analysis. If certain images are identified as potentially relevant to a case, they can be tagged for further scrutiny. This tagging function is more than a mere organizational tool; it's a systematic way to highlight essential visual information that may prove crucial in understanding the digital activities related to a case.

How to Tag: Simply right-click on the desired screenshot and select the "Tag" option. You may create custom tags or use predefined ones, adding notes or comments as necessary. This flexibility ensures that you can organize your screenshots in a way that suits your specific investigative needs.

Inclusion in the Final Report: Tagged screenshots are not merely an intermediate step in the investigation. They often form an integral part of the final report. When compiling your findings, all tagged screenshot photos can be automatically included as potential evidence. They are presented in a well-organized manner, often alongside corresponding notes or observations made during the analysis phase.

How to Include in Report: Typically, there's an option to include tagged items in the report generation process. Make sure to select this option to have all tagged screenshots appear in the final document. Presenting as Evidence: The end report, including the tagged screenshots, can be used in legal proceedings as possible evidence. The organized and systematic way in which these images are handled, analyzed, and reported in Autopsy ensures their integrity and admissibility in a court of law.

In conclusion, the ability to tag relevant screenshots in Autopsy forensic software is not merely a feature but an essential process that enables precise analysis, reporting, and legal utilization of visual data. It allows forensic professionals to efficiently identify and focus on critical visual information, contributing to a more comprehensive and convincing presentation of evidence in any given case.

7.9 Making, Downloading, and Analyzing a Memory Dump (memory_dump_vm)

7.9.1 Making and download a Memory Dump

Making a memory dump refers to the process of capturing the content of a computer's memory (RAM) at a specific moment in time. This snapshot can include various elements, ranging from currently running processes to user credentials and even the contents of open files. The practice is critical for several reasons:

Security Analysis

In the realm of cybersecurity, memory dumps have become an essential tool. Here's how they contribute:

- **Uncovering Malware Behavior**: Memory dumps allow security professionals to see what is happening inside the system's memory, including hidden or obfuscated malware activities. By analyzing these dumps, one can reveal the behavior of malicious code, tracking its origin, and how it interacts with the system.
- **Detecting Hidden Processes**: Sophisticated malware often hides from standard detection methods. Memory analysis helps in uncovering these hidden processes, providing a more transparent view of unauthorized activities.
- **Injected Code Analysis**: Attackers may inject malicious code into legitimate processes to conceal their actions. A memory dump helps in identifying these code injections, leading to better understanding and mitigation of such threats.
- **User Credential Analysis**: Sometimes, credentials might be stored in memory. A memory dump could reveal these details, helping in understanding potential security breaches or vulnerabilities.

Forensic Analysis

Digital forensic analysts often use memory dumps to investigate suspicious or malicious activities:

- **Timeline Analysis**: Memory dumps can provide a chronological view of the activities that transpired on the device, aiding in reconstructing events leading up to an incident.
- **Data Recovery**: Even if data is deleted or encrypted, remnants might still exist in the system's memory. Analyzing memory dumps may allow the recovery of this vital information.
- **Artifact Analysis**: Various artifacts related to user activities, system interactions, and file usage can be extracted and analyzed from memory dumps, painting a comprehensive picture of user behavior.

Legal Evidence

In the context of legal proceedings, memory dumps might provide crucial evidence:

- **Computer Usage**: Evidence regarding the usage of specific applications or accessing specific files or websites can be derived from a memory dump.
- **Unauthorized Access**: In cases of hacking or unauthorized access, memory dumps may hold evidence of the intrusion, including the tools used and the data targeted.
- **Intellectual Property Theft**: If there is a suspicion of intellectual property theft, memory dumps can reveal whether sensitive documents were accessed, modified, or transferred.

Follow the steps below to make and download a memory dump:

1) Press the “Make and Download Memory Dump” Button

Press the button labeled “Make and Download Memory Dump” to initiate the process.

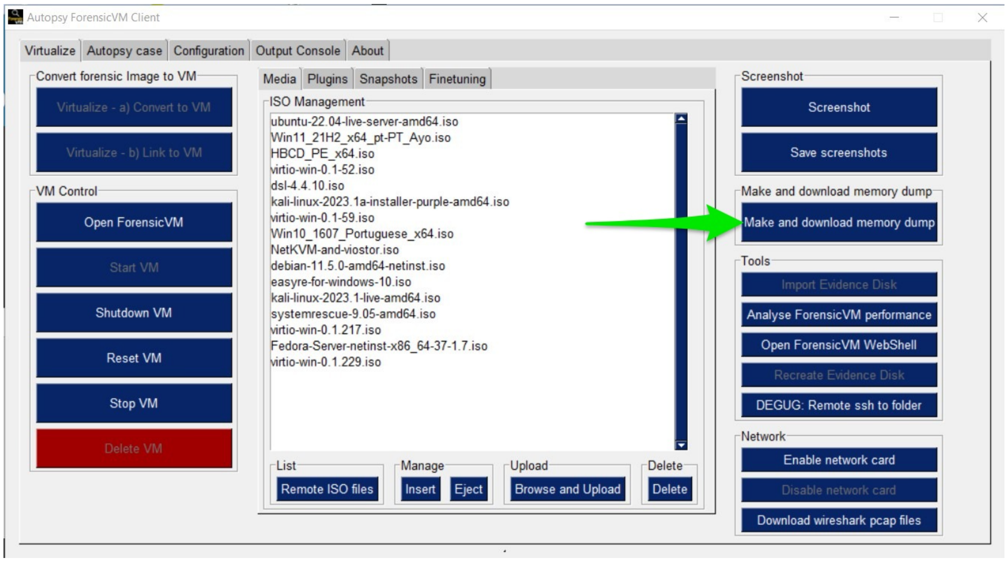
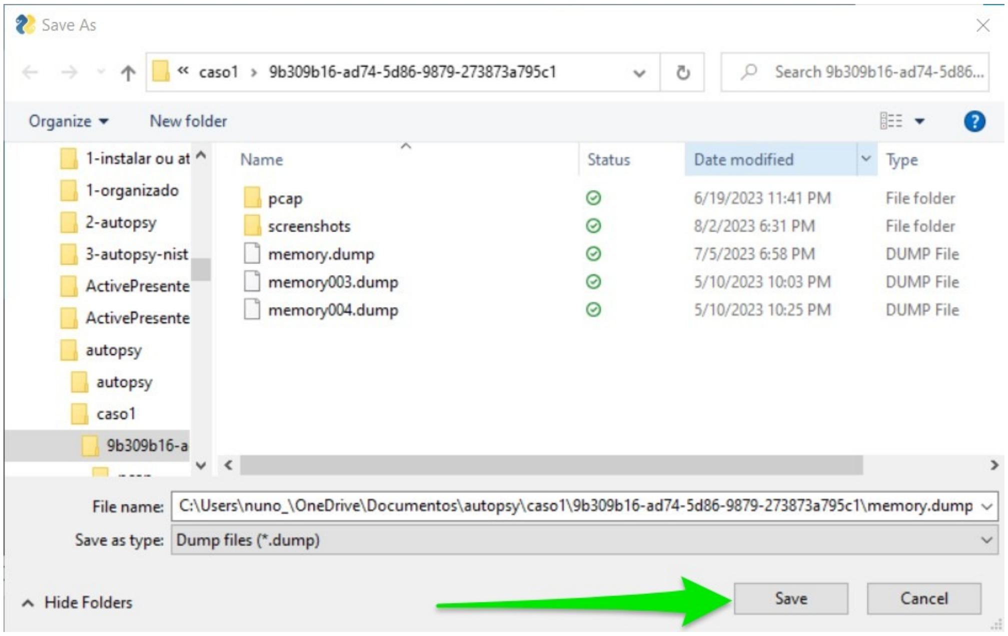

Autopsy ForensicVM Client
Virtualize
Autopsy case
Configuration
Output Console
About
Convert forensic Image to VM
Virtualize - a) Convert to VM
Virtualize - b) Link to VM
VM Control
Open ForensicVM
Start VM
Shutdown VM
Reset VM
Stop VM
Delete VM
Media
Plugins
Snapshots
Finetuning
ISO Management
ubuntu-22.04-live-server-amd64.iso
Win11_21H2_x64_pt-PT_Ayo.iso
HBCD_PE_x64.iso
virtio-win-0.1-52.iso
dsl-4.4.10.iso
kali-linux-2023.1a-installer-purple-amd64.iso
virtio-win-0.1-59.iso
Win10_1607_Portuguese_x64.iso
NetKVM-and-viostor.iso
debian-11.5.0-amd64-netinst.iso
easyre-for-windows-10.iso
kali-linux-2023.1-live-amd64.iso
systemrescue-9.05-amd64.iso
virtio-win-0.1.217.iso
Fedora-Server-netinst-x86_64-37-1.7.iso
virtio-win-0.1.229.iso
List
Remote ISO files
Manage
Insert
Eject
Upload
Browse and Upload
Delete
Delete
Screenshot
Screenshot
Save screenshots
Make and download memory dump
Make and download memory dump
Tools
Import Evidence Disk
Analyse ForensicVM performance
Open ForensicVM WebShell
Recreate Evidence Disk
DEGUG: Remote ssh to folder
Network
Enable network card
Disable network card
Download wireshark pcap files

Fig. 7.72: Press “Make and Download Memory Dump” button

2) Save the Memory Dump on the Default ForensicVM Image Case Path

Choose the default forensicVM image case path to save the memory dump.



Name	Status	Date modified	Type
pcap	✓	6/19/2023 11:41 PM	File folder
screenshots	✓	8/2/2023 6:31 PM	File folder
memory.dump	✓	7/5/2023 6:58 PM	DUMP File
memory003.dump	✓	5/10/2023 10:03 PM	DUMP File
memory004.dump	✓	5/10/2023 10:25 PM	DUMP File

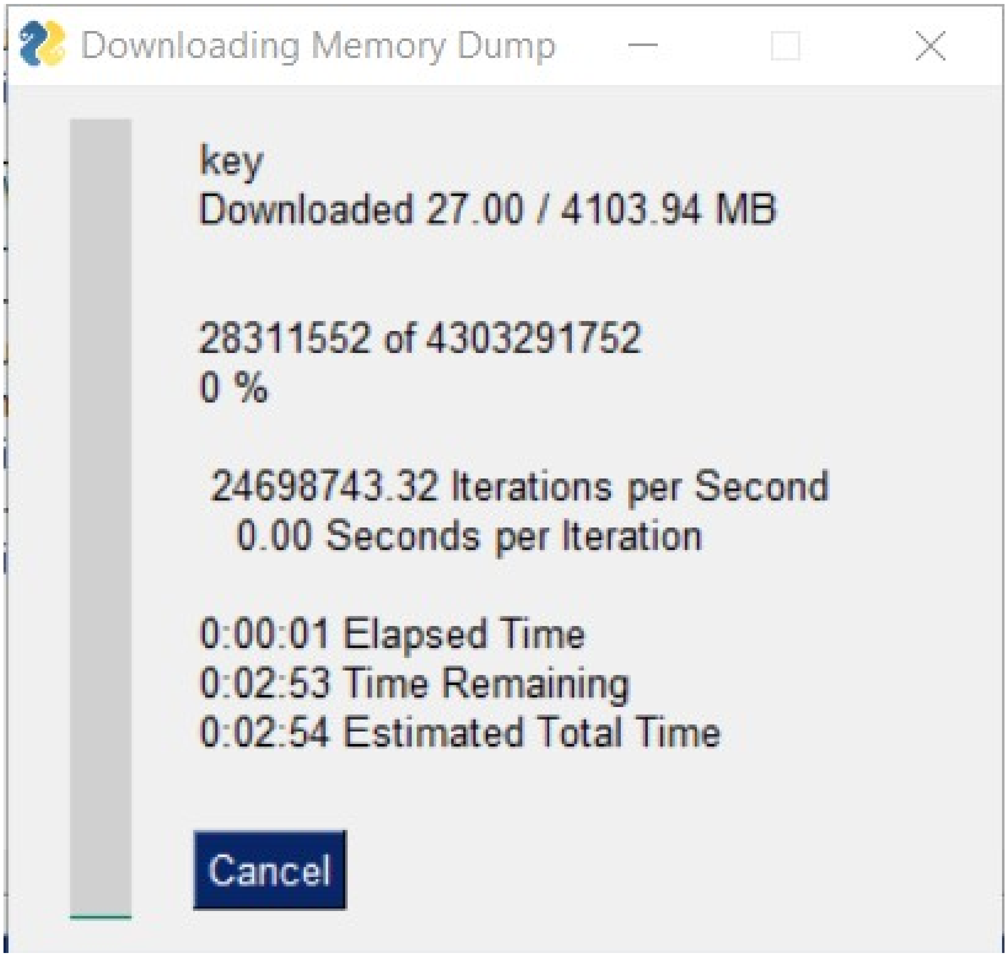
File name: C:\Users\nuno_\OneDrive\Documentos\autopsy\caso1\9b309b16-ad74-5d86-9879-273873a795c1\memory.dump

Save as type: Dump files (*.dump)

Fig. 7.73: Save the memory dump

3) Monitor Memory Download Progress with Time Estimation

Keep track of the download progress, including an estimated time remaining for the download to complete.



Downloading Memory Dump

key
Downloaded 27.00 / 4103.94 MB

28311552 of 4303291752
0 %

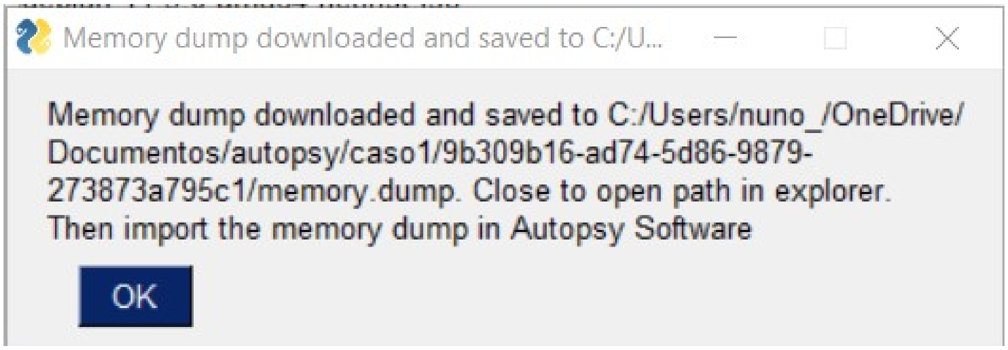
24698743.32 Iterations per Second
0.00 Seconds per Iteration

0:00:01 Elapsed Time
0:02:53 Time Remaining
0:02:54 Estimated Total Time

Fig. 7.74: Memory Download progress

4) Success Message Stating that the Memory was Saved as "memory.dump"

A success message will appear, stating that the memory was saved as "memory.dump." The explorer will automatically open afterward.

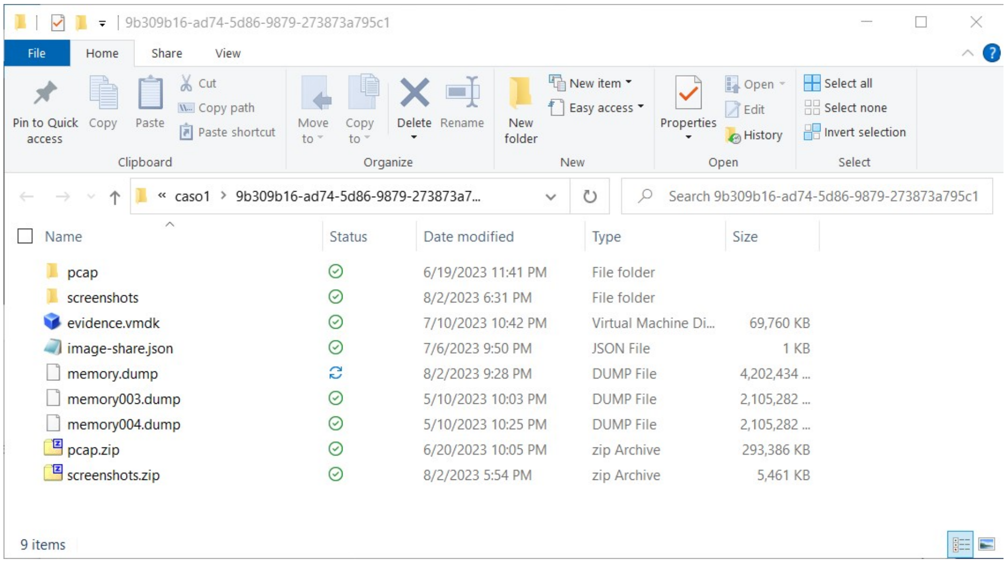

Memory dump downloaded and saved to C:/U...

Memory dump downloaded and saved to C:/Users/nuno_/OneDrive/Documentos/autopsy/caso1/9b309b16-ad74-5d86-9879-273873a795c1/memory.dump. Close to open path in explorer. Then import the memory dump in Autopsy Software

Fig. 7.75: Success message

5) Windows Explorer Open on the Memory Dump Folder

The Windows explorer will open automatically, displaying the folder containing the memory dump.


9b309b16-ad74-5d86-9879-273873a795c1

« caso1 › 9b309b16-ad74-5d86-9879-273873a7...

Search 9b309b16-ad74-5d86-9879-273873a795c1

Name	Status	Date modified	Type	Size
pcap	✓	6/19/2023 11:41 PM	File folder	
screenshots	✓	8/2/2023 6:31 PM	File folder	
evidence.vmdk	✓	7/10/2023 10:42 PM	Virtual Machine Di...	69,760 KB
image-share.json	✓	7/6/2023 9:50 PM	JSON File	1 KB
memory.dump	⟳	8/2/2023 9:28 PM	DUMP File	4,202,434 ...
memory003.dump	✓	5/10/2023 10:03 PM	DUMP File	2,105,282 ...
memory004.dump	✓	5/10/2023 10:25 PM	DUMP File	2,105,282 ...
pcap.zip	✓	6/20/2023 10:05 PM	zip Archive	293,386 KB
screenshots.zip	✓	8/2/2023 5:54 PM	zip Archive	5,461 KB

9 items

Fig. 7.76: Windows explorer open on the memory dump folder

7.9.2 Importing and Analyzing a Memory Dump in Autopsy

Analyzing a memory dump can provide critical insights into the state of a system at a particular point in time. Memory dumps may contain valuable information that helps investigators understand what processes were running, what files were open, and even what keys were being pressed.

Autopsy enables an investigator to examine memory dumps by following a series of steps to import and analyze the data. Here's an expanded walkthrough:

1. Locate the Memory Dump **File** Begin by identifying the file you wish to analyze. This could be a file that you have obtained from a machine you are investigating. Make sure to have the file accessible and note its location on your system.

2. Prepare Autopsy for Importing the Memory Dump Launch Autopsy and create a new case or open an existing one where you want the memory dump to be analyzed. The case structure in Autopsy helps in organizing different data sources and findings related to an investigation.

3. Add the Memory Dump **as a** Data Source Inside your case, look for an option to add a new data source. This is usually achieved by clicking on the "Add Data Source" button. You'll be guided through a series of prompts to configure the import.

4. Choose the Host and Data Source Type You'll need to select a host, which typically refers to the system from which the memory dump was obtained. Then, choose "Memory Image File (Volatility)" as the Data Source Type, a common format for memory dumps.

5. Navigate to the Memory Dump **File** Click the "Browse" button and use the file dialog to locate the memory dump file on your system. You may need to paste the exact path if you have copied it earlier.

6. Configure the Analysis Settings This involves setting the timezone, memory profile (which should correspond to the OS of the dumped system), and selecting or deselecting specific plugins. Plugins in Autopsy extend its functionality and can be used to run specific analyses on the data.

7. Ingest the Memory Dump After confirming your settings, Autopsy will begin the process of ingesting the memory dump. This might take a significant amount of time, depending on the size of the dump and the capabilities of your system.

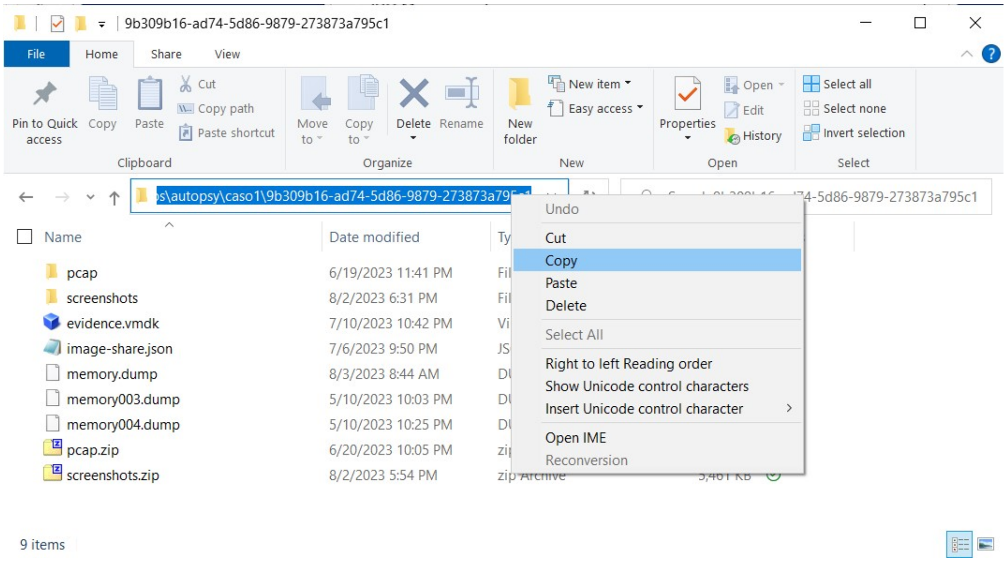
8. Review the Results and Check for Errors Upon completion, review the log to check for any errors or warnings. This is a vital step to ensure that the data was imported correctly and that all selected analyses were performed successfully.

9. Analyze the Memory Dump Finally, you can start analyzing the memory dump. Autopsy provides various tools and views to help you explore the data. You can browse through processes, network connections, registry keys, and more. Look for anomalies or signs of malicious activity.

10. Tag and Document Findings As you proceed with your analysis, make sure to tag any interesting findings. Autopsy provides features to annotate and comment on your discoveries, making it easier to reference them later or include them in your final report.

1) Copy the Path of the Memory Dump from Windows Explorer

Start by locating the memory dump file on your system. Open Windows Explorer, navigate to the directory containing the memory dump, right-click on the path, and select "Copy" This action will copy the path's location to your clipboard, allowing you to easily paste it later in the Autopsy software.

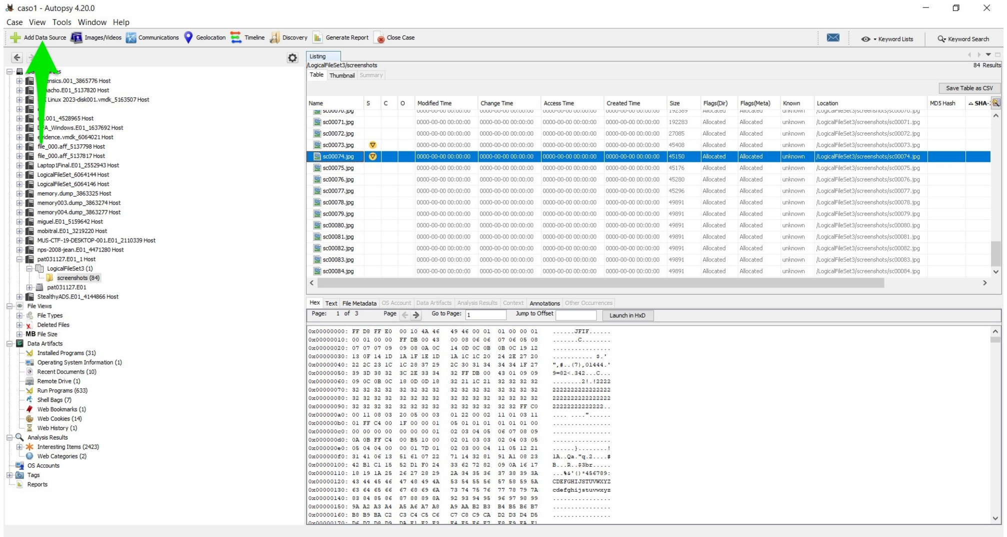


Name	Date modified	Ty
pcap	6/19/2023 11:41 PM	Fi
screenshots	8/2/2023 6:31 PM	Fi
evidence.vmdk	7/10/2023 10:42 PM	Vi
image-share.json	7/6/2023 9:50 PM	JS
memory.dump	8/3/2023 8:44 AM	DU
memory003.dump	5/10/2023 10:03 PM	DU
memory004.dump	5/10/2023 10:25 PM	DU
pcap.zip	6/20/2023 10:05 PM	zi
screenshots.zip	8/2/2023 5:54 PM	zip Archive

Fig. 7.77: Copy the path of the memory dump

2) Press the "Add Data Source" Button on the Autopsy Software

Open Autopsy and initiate the process of adding a new data source by pressing the "Add Data Source" button. This button typically resides in the main toolbar.



/LogicalFileSet3/screenshots

84 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location	MD5 Hash	SHA-:
sc00071.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	192283	Allocated	Allocated	unknown	/LogicalFileSet3/screenshots/sc00071.jpg		
sc00072.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	27085	Allocated	Allocated	unknown	/LogicalFileSet3/screenshots/sc00072.jpg		
sc00073.jpg	▽			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	45408	Allocated	Allocated	unknown	/LogicalFileSet3/screenshots/sc00073.jpg		
sc00074.jpg	▽			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	45150	Allocated	Allocated	unknown	/LogicalFileSet3/screenshots/sc00074.jpg		
sc00075.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	45176	Allocated	Allocated	unknown	/LogicalFileSet3/screenshots/sc00075.jpg		
sc00076.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	45280	Allocated	Allocated	unknown	/LogicalFileSet3/screenshots/sc00076.jpg		
sc00077.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	45296	Allocated	Allocated	unknown	/LogicalFileSet3/screenshots/sc00077.jpg		
sc00078.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	49891	Allocated	Allocated	unknown	/LogicalFileSet3/screenshots/sc00078.jpg		
sc00079.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	49891	Allocated	Allocated	unknown	/LogicalFileSet3/screenshots/sc00079.jpg		
sc00080.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	49891	Allocated	Allocated	unknown	/LogicalFileSet3/screenshots/sc00080.jpg		
sc00081.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	49891	Allocated	Allocated	unknown	/LogicalFileSet3/screenshots/sc00081.jpg		
sc00082.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	49891	Allocated	Allocated	unknown	/LogicalFileSet3/screenshots/sc00082.jpg		
sc00083.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	49891	Allocated	Allocated	unknown	/LogicalFileSet3/screenshots/sc00083.jpg		
sc00084.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	49891	Allocated	Allocated	unknown	/LogicalFileSet3/screenshots/sc00084.jpg		

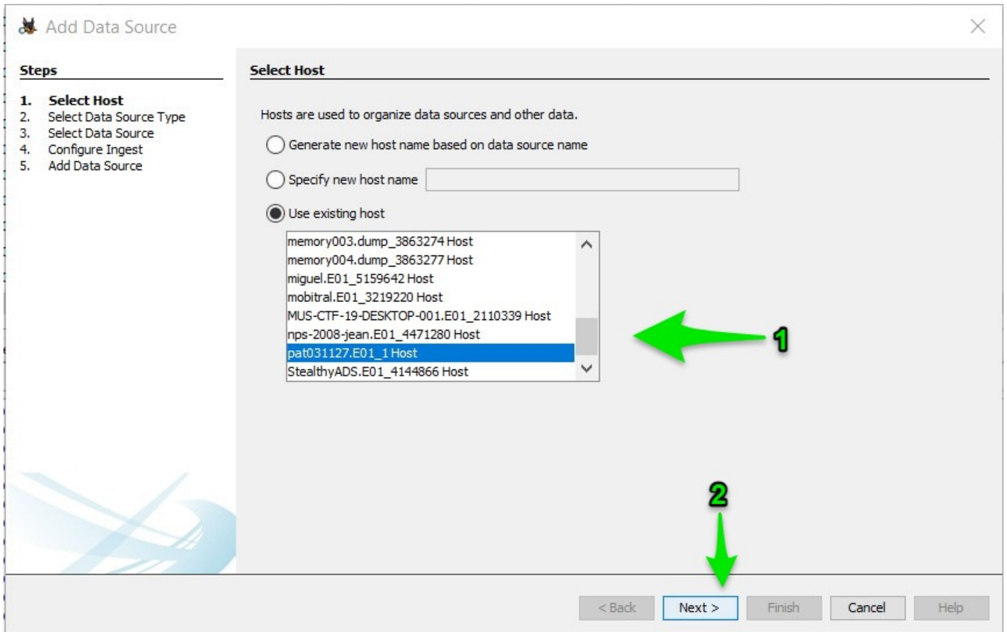
Page: 1 of 3 Page Go to Page: 1 Jump to Offset

```
0x00000000: FF D8 FF E0  00 10 4A 46  49 46 00 01  01 00 00 01   ......JFIF......
0x00000010: 00 01 00 00  FF DB 00 43  00 08 06 06  07 06 05 08   .......C........
0x00000020: 07 07 07 09  09 08 0A 0C  14 0D 0C 0B  0B 0C 19 12   ................
0x00000030: 13 0F 14 1D  1A 1F 1E 1D  1A 1C 1C 20  24 2E 27 20   ........... $.'
0x00000040: 22 2C 23 1C  1C 28 37 29  2C 30 31 34  34 34 1F 27   ",#..(7),01444.'
0x00000050: 39 3D 38 32  3C 2E 33 34  32 FF DB 00  43 01 09 09   9=82<.342...C...
0x00000060: 09 0C 0B 0C  18 0D 0D 18  32 21 1C 21  32 32 32 32   ........2!.!2222
0x00000070: 32 32 32 32  32 32 32 32  32 32 32 32  32 32 32 32   2222222222222222
0x00000080: 32 32 32 32  32 32 32 32  32 32 32 32  32 32 32 32   2222222222222222
0x00000090: 32 32 32 32  32 32 32 32  32 32 32 32  32 32 FF C0   22222222222222..
0x000000a0: 00 11 08 03  20 05 00 03  01 22 00 02  11 01 03 11   .... ....".....
0x000000b0: 01 FF C4 00  1F 00 00 01  05 01 01 01  01 01 01 00   ................
0x000000c0: 00 00 00 00  00 00 00 01  02 03 04 05  06 07 08 09   ................
0x000000d0: 0A 0B FF C4  00 B5 10 00  02 01 03 03  02 04 03 05   ................
0x000000e0: 05 04 04 00  00 01 7D 01  02 03 00 04  11 05 12 21   ......}........!
0x000000f0: 31 41 06 13  51 61 07 22  71 14 32 81  91 A1 08 23   1A..Qa."q.2....#
0x00000100: 42 B1 C1 15  52 D1 F0 24  33 62 72 82  09 0A 16 17   B...R..$3br.....
0x00000110: 18 19 1A 25  26 27 28 29  2A 34 35 36  37 38 39 3A   ...%&'()*456789:
0x00000120: 43 44 45 46  47 48 49 4A  53 54 55 56  57 58 59 5A   CDEFGHIJSTUVWXYZ
0x00000130: 63 64 65 66  67 68 69 6A  73 74 75 76  77 78 79 7A   cdefghijstuvwxyz
0x00000140: 83 84 85 86  87 88 89 8A  92 93 94 95  96 97 98 99   ................
0x00000150: 9A A2 A3 A4  A5 A6 A7 A8  A9 AA B2 B3  B4 B5 B6 B7   ................
0x00000160: B8 B9 BA C2  C3 C4 C5 C6  C7 C8 C9 CA  D2 D3 D4 D5   ................
```

Fig. 7.78: Press "Add Data Source"

3) Select the Host to Where the Memory Dump Should be Made and Press Next

You will be prompted to select a host, which is the computer or device where the memory dump will be analyzed. Choose the appropriate host from the list provided, and then press “Next” to continue.



Hosts are used to organize data sources and other data.

○ Generate new host name based on data source name

○ Specify new host name

● Use existing host

- memory003.dump_3863274 Host
- memory004.dump_3863277 Host
- miguel.E01_5159642 Host
- mobitral.E01_3219220 Host
- MUS-CTF-19-DESKTOP-001.E01_2110339 Host
- nps-2008-jean.E01_4471280 Host
- pat031127.E01_1 Host
- StealthyADS.E01_4144866 Host

Fig. 7.79: Select the host

4) Select as Data Source Type the “Memory Image File (Volatility)” and Press Next

In this step, you will specify the type of data you are importing. Select “Memory Image File (Volatility)” from the list of data source types, as this is the appropriate option for memory dumps. Once selected, click “Next.”

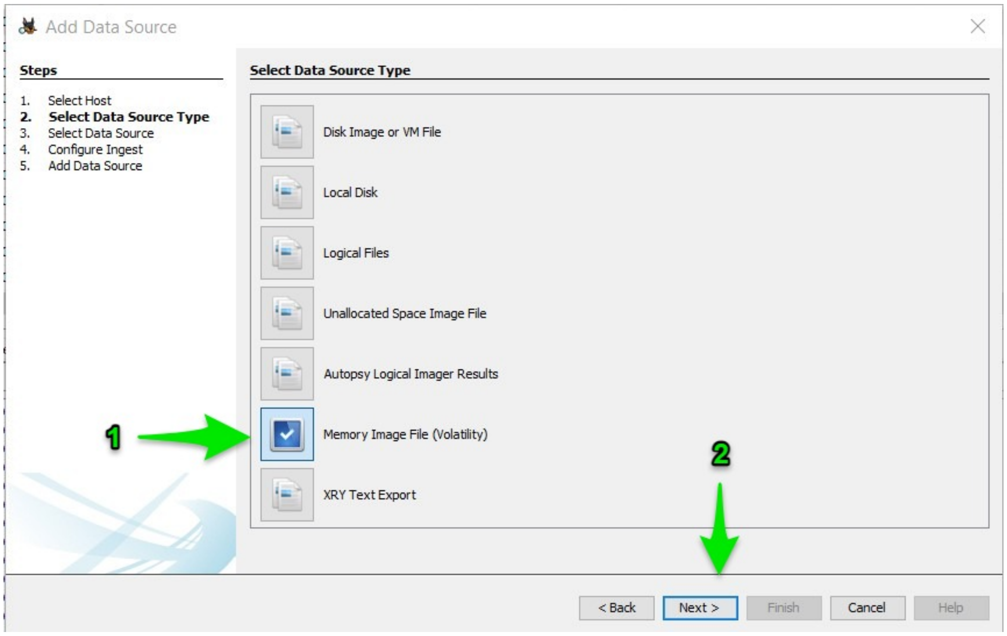
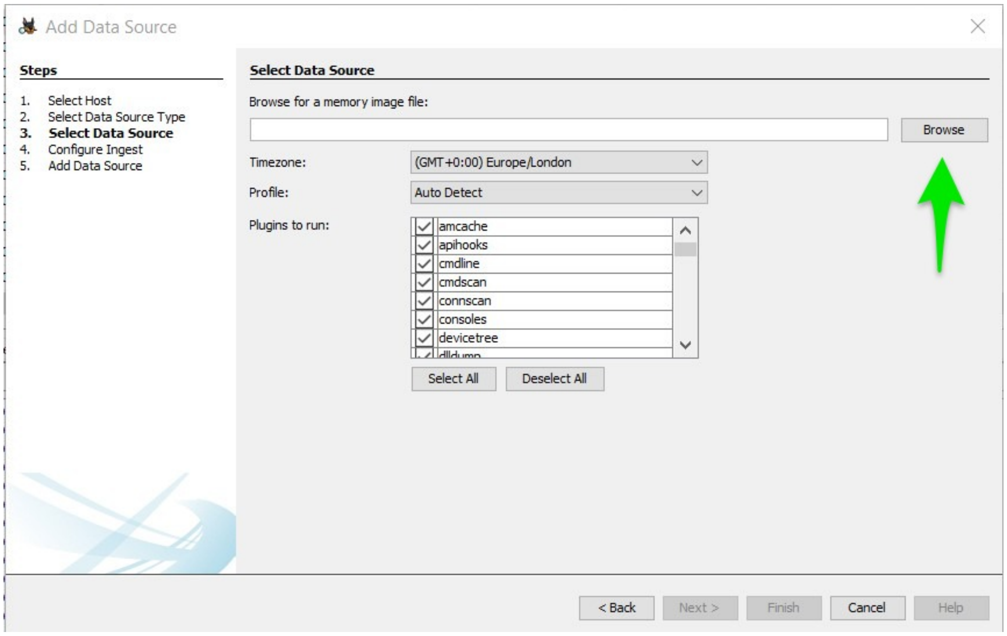


Fig. 7.80: Select Memory Image File (Volatility)

5) Click the "Browse" Button to Select the Path Where the Memory Dump Is

A file browser window will appear. Click the "Browse" button, navigate to the location where the memory dump is stored, and select the file. If you copied the path earlier, you could paste it into the file path field to quickly locate the file.



Steps

1. Select Host
2. Select Data Source Type
3. **Select Data Source**
4. Configure Ingest
5. Add Data Source

Select Data Source

Browse for a memory image file:

Timezone: (GMT+0:00) Europe/London

Profile: Auto Detect

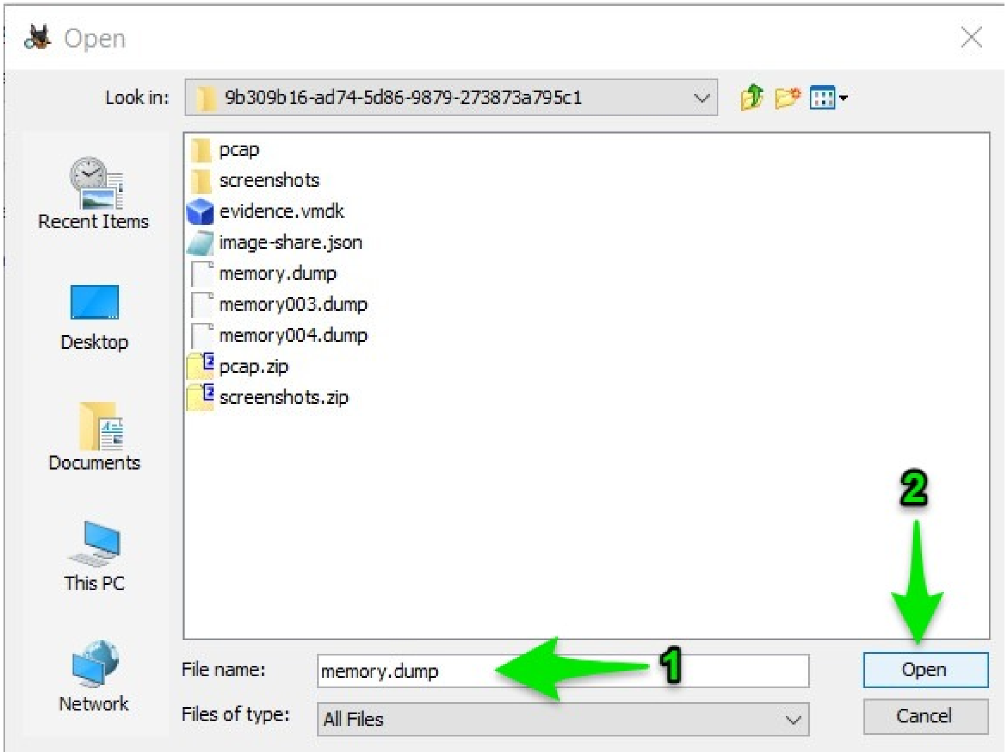
Plugins to run:

- ☑ amcache
- ☑ apihooks
- ☑ cmdline
- ☑ cmdscan
- ☑ connscan
- ☑ consoles
- ☑ devicetree
- ☑ dlldump

Fig. 7.81: Click “Browse” button

6) Paste the “memory.dump” Path, Select the memory.dump File, and Press Open

Once you have located the “memory.dump” file, select it by clicking on it, then press the “Open” button to confirm your selection.



Look in: 9b309b16-ad74-5d86-9879-273873a795c1

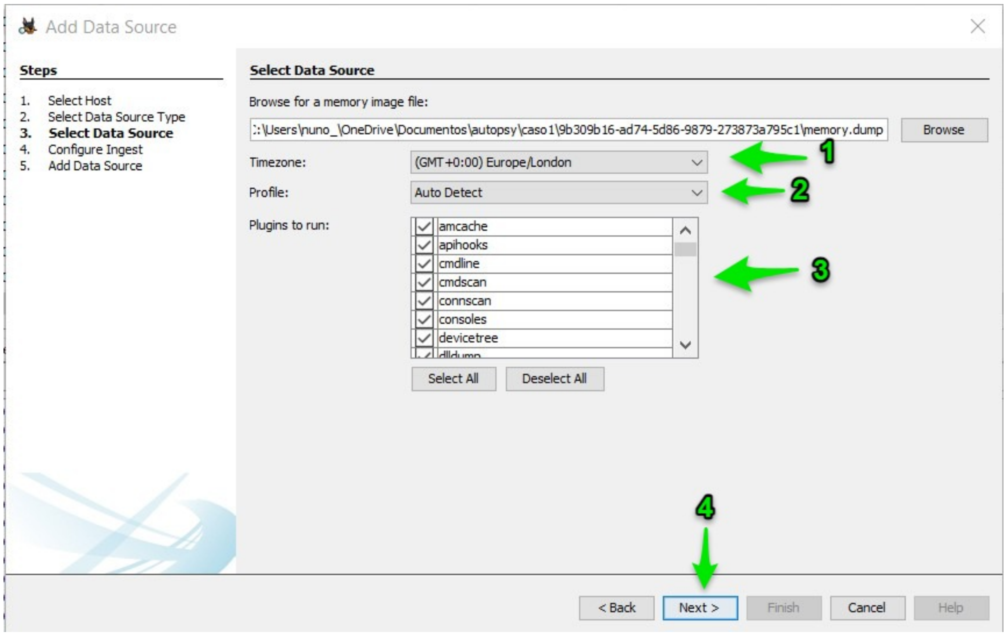
File name: memory.dump

Files of type: All Files

Fig. 7.82: Paste and select the memory.dump file

7) Configure Timezone, Memory Profile, and Plugins to Run. Press Next

You will now be asked to configure several settings specific to your analysis. Set the appropriate timezone to match the original system's time setting. Choose the correct memory profile, which should match the operating system of the analyzed machine. Optionally, select any plugins you want to run during the analysis. Click "Next" to proceed.



Add Data Source

Steps

1. Select Host
2. Select Data Source Type
3. **Select Data Source**
4. Configure Ingest
5. Add Data Source

Select Data Source

Browse for a memory image file: :\Users\nuno_\OneDrive\Documentos\autopsy\caso1\9b309b16-ad74-5d86-9879-273873a795c1\memory.dump

Timezone: (GMT+0:00) Europe/London

Profile: Auto Detect

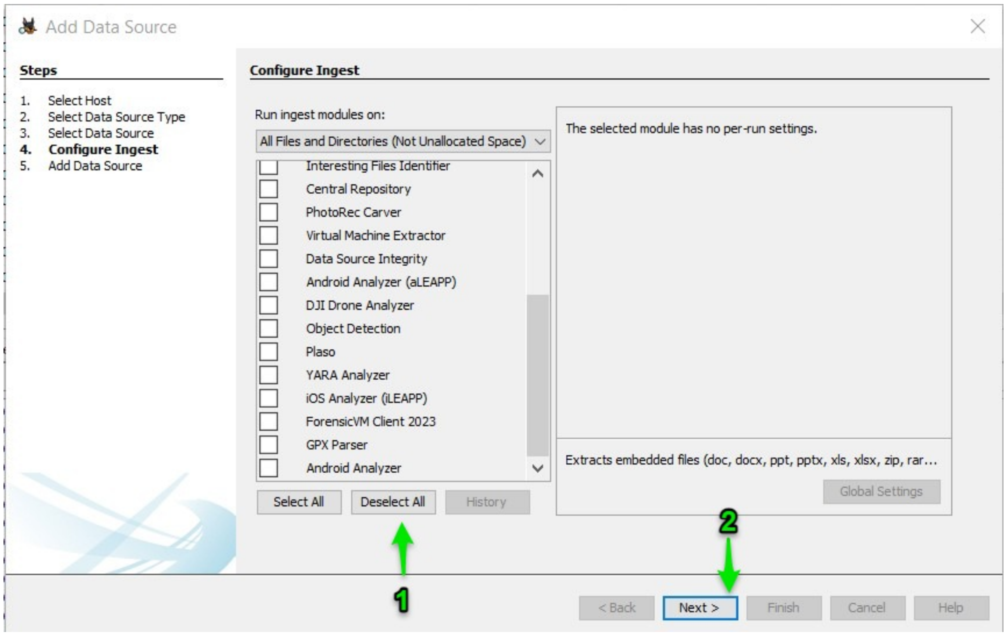
Plugins to run:

- ☑ amcache
- ☑ apihooks
- ☑ cmdline
- ☑ cmdscan
- ☑ connscan
- ☑ consoles
- ☑ devicetree
- ☑ dlldump

Fig. 7.83: Configure settings

8) Deselect All Plugins and Press Next

Deselect all plugins in this step. Then, press “Next.”



Add Data Source

Steps

1. Select Host
2. Select Data Source Type
3. Select Data Source
4. **Configure Ingest**
5. Add Data Source

Configure Ingest

Run ingest modules on:

All Files and Directories (Not Unallocated Space)

- □ Interesting Files Identifier
- □ Central Repository
- □ PhotoRec Carver
- □ Virtual Machine Extractor
- □ Data Source Integrity
- □ Android Analyzer (aLEAPP)
- □ DJI Drone Analyzer
- □ Object Detection
- □ Plaso
- □ YARA Analyzer
- □ iOS Analyzer (iLEAPP)
- □ ForensicVM Client 2023
- □ GPX Parser
- □ Android Analyzer

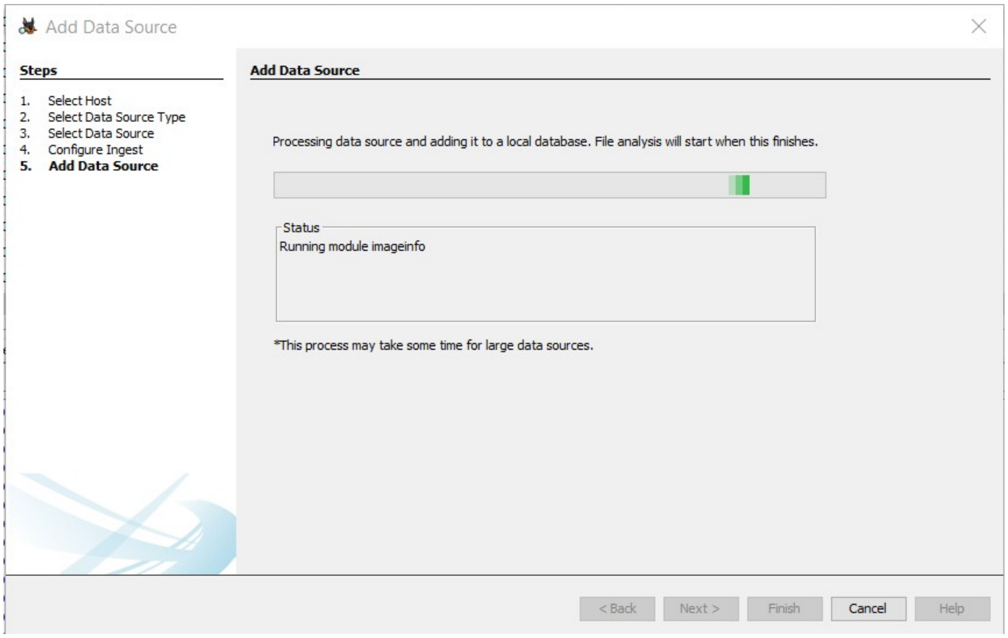
The selected module has no per-run settings.

Extracts embedded files (doc, docx, ppt, pptx, xls, xlsx, zip, rar...

Fig. 7.84: Deselect plugins

9) Wait Until the Memory Ingest Module is Finished

This step may take some time, as Autopsy processes the memory dump. Depending on the size of the file and your computer's capabilities, this could take several minutes or even hours. A progress bar or other indicator may be available to monitor the process. Please be patient.



Processing data source and adding it to a local database. File analysis will start when this finishes.

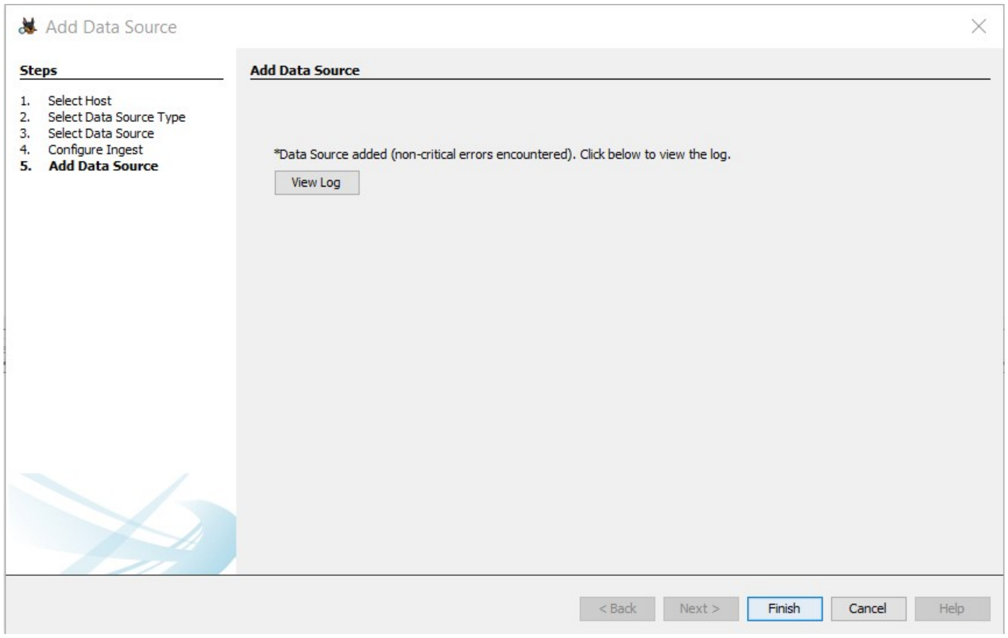
Status
Running module imageinfo

*This process may take some time for large data sources.

Fig. 7.85: Ingesting memory

10) Check for Errors and Press "Finish"

Upon completion, a dialog will appear, summarizing the process and any issues encountered. Press the "View Log" button to inspect any errors or warnings in detail. Finally, press the "Finish" button to conclude the process and close the dialog.



Add Data Source

Steps

1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. **Add Data Source**

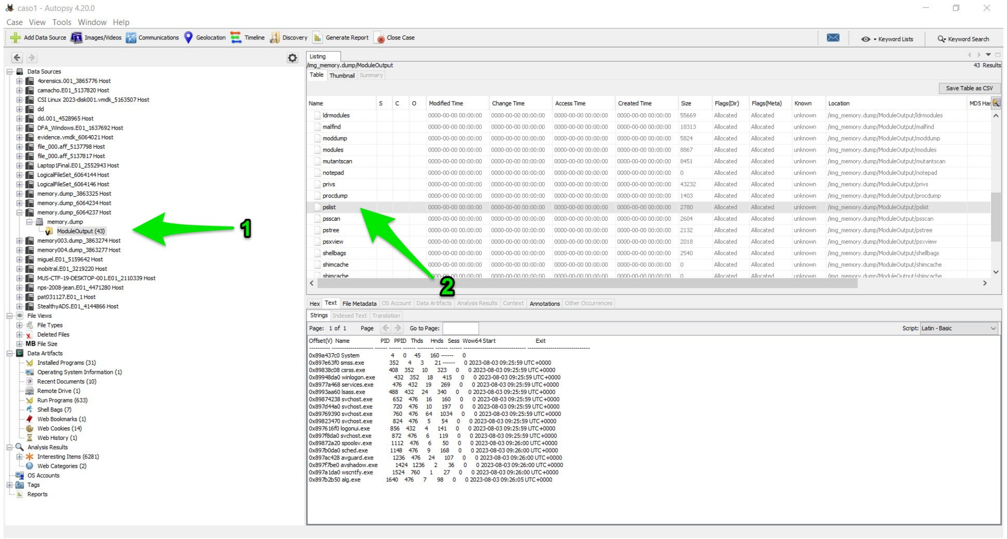
Add Data Source

*Data Source added (non-critical errors encountered). Click below to view the log.

Fig. 7.86: Press "Finish"

11) Locate the Memory Dump on the Interface and Browse the Results

With the import process complete, you can now find the imported memory dump within Autopsy's interface. Browse through the results, and use Autopsy's various tools to examine the data. Remember to tag any findings that may be of interest, as these can be critical to your investigation.



- Data Sources
  - 4orensics.001_3865776 Host
  - camacho.E01_5137820 Host
  - CSI Linux 2023-disk001.vmdk_5163507 Host
  - dd
  - dd.001_4528965 Host
  - DFA_Windows.E01_1637692 Host
  - evidence.vmdk_6064021 Host
  - file_000.aff_5137798 Host
  - file_000.aff_5137817 Host
  - Laptop1Final.E01_2552943 Host
  - LogicalFileSet_6064144 Host
  - LogicalFileSet_6064146 Host
  - memory.dump_3863325 Host
  - memory.dump_6064234 Host
  - memory.dump_6064237 Host
    - memory.dump
      - ModuleOutput (43)
  - memory003.dump_3863274 Host
  - memory004.dump_3863277 Host
  - miguel.E01_5159642 Host
  - mobitral.E01_3219220 Host
  - MUS-CTF-19-DESKTOP-001.E01_2110339 Host
  - nps-2008-jean.E01_4471280 Host
  - pat031127.E01_1 Host
  - StealthyADS.E01_4144866 Host
- File Views
  - File Types
  - Deleted Files
  - MB File Size
- Data Artifacts
  - Installed Programs (31)
  - Operating System Information (1)
  - Recent Documents (10)
  - Remote Drive (1)
  - Run Programs (633)
  - Shell Bags (7)
  - Web Bookmarks (1)
  - Web Cookies (14)
  - Web History (1)
- Analysis Results
  - Interesting Items (6281)
  - Web Categories (2)
- OS Accounts
- Tags
- Reports

/img_memory.dump/ModuleOutput 43 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location	MD5 Hash
ldrmodules				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	55669	Allocated	Allocated	unknown	/img_memory.dump/ModuleOutput/ldrmodules	
malfind				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	18313	Allocated	Allocated	unknown	/img_memory.dump/ModuleOutput/malfind	
moddump				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	5824	Allocated	Allocated	unknown	/img_memory.dump/ModuleOutput/moddump	
modules				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	8867	Allocated	Allocated	unknown	/img_memory.dump/ModuleOutput/modules	
mutantscan				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	8451	Allocated	Allocated	unknown	/img_memory.dump/ModuleOutput/mutantscan	
notepad				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/img_memory.dump/ModuleOutput/notepad	
privs				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	43232	Allocated	Allocated	unknown	/img_memory.dump/ModuleOutput/privs	
procdump				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1403	Allocated	Allocated	unknown	/img_memory.dump/ModuleOutput/procdump	
pslist				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	2780	Allocated	Allocated	unknown	/img_memory.dump/ModuleOutput/pslist	
psscan				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	2604	Allocated	Allocated	unknown	/img_memory.dump/ModuleOutput/psscan	
pstree				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	2132	Allocated	Allocated	unknown	/img_memory.dump/ModuleOutput/pstree	
psxview				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	2018	Allocated	Allocated	unknown	/img_memory.dump/ModuleOutput/psxview	
shellbags				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	2540	Allocated	Allocated	unknown	/img_memory.dump/ModuleOutput/shellbags	
shimcache				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/img_memory.dump/ModuleOutput/shimcache	
shimcache				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/img_memory.dump/ModuleOutput/shimcache	

```
Offset(V) Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0x89a437c0 System                    4      0     45      160 ------      0
0x897e63f0 smss.exe                352      4      3       21 ------      0 2023-08-03 09:25:59 UTC+0000
0x89838c08 csrss.exe               408    352     10      323      0      0 2023-08-03 09:25:59 UTC+0000
0x89948da0 winlogon.exe            432    352     18      415      0      0 2023-08-03 09:25:59 UTC+0000
0x8977a468 services.exe            476    432     19      269      0      0 2023-08-03 09:25:59 UTC+0000
0x8993aa60 lsass.exe               488    432     24      340      0      0 2023-08-03 09:25:59 UTC+0000
0x89874238 svchost.exe             652    476     16      160      0      0 2023-08-03 09:25:59 UTC+0000
0x897d44a0 svchost.exe             720    476     10      197      0      0 2023-08-03 09:25:59 UTC+0000
0x89769390 svchost.exe             760    476     64     1034      0      0 2023-08-03 09:25:59 UTC+0000
0x89823470 svchost.exe             824    476      5       54      0      0 2023-08-03 09:25:59 UTC+0000
0x897616f0 logonui.exe             856    432      4      141      0      0 2023-08-03 09:25:59 UTC+0000
0x897f8da0 svchost.exe             872    476      6      119      0      0 2023-08-03 09:25:59 UTC+0000
0x89872a20 spoolsv.exe            1112    476      6       50      0      0 2023-08-03 09:26:00 UTC+0000
0x897b0da0 sched.exe              1148    476      9      168      0      0 2023-08-03 09:26:00 UTC+0000
0x897ac428 avguard.exe            1236    476     24      107      0      0 2023-08-03 09:26:00 UTC+0000
0x897f7be0 avshadow.exe           1424   1236      2       36      0      0 2023-08-03 09:26:00 UTC+0000
0x897a1da0 wscntfy.exe            1524    760      1       27      0      0 2023-08-03 09:26:00 UTC+0000
0x897b2b50 alg.exe                1640    476      7       98      0      0 2023-08-03 09:26:05 UTC+0000
```

Fig. 7.87: Locate and browse the memory dump

7.9.3 Aditional Tools to analyse memory dumps

Analyzing memory dumps is a vital task in computer forensics, malware analysis, and system diagnostics. Several tools have been developed to support this task. Here's an overview of some widely-used tools other than Autopsy for memory dump analysis:

1. Volatility: Volatility is an open-source memory forensics framework. Documentation.
2. Rekall: Rekall offers a set of features for memory forensics. Documentation.
3. WinDbg: Microsoft's WinDbg for debugging Windows applications and analyzing memory dumps.
4. Magnet RAM Capture: Magnet RAM Capture is a free tool for capturing physical RAM.
5. FTK Imager: AccessData's FTK Imager for capturing and analyzing memory dumps.
6. MoonSols DumpIt: MoonSols DumpIt for creating memory dumps from Windows systems.
7. Redline: Provided by FireEye, Redline offers advanced memory and file analysis capabilities.
8. GRR (Google Rapid Response): GRR an incident response framework that includes memory analysis capabilities. Documentation.
9. Belkasoft Evidence Center: Belkasoft Evidence Center includes the ability to analyze computer memory.
10. X-Ways Forensics: X-Ways Forensics a commercial product with strong memory analysis features.

These tools offer a wide range of capabilities, from capturing memory images to detailed analysis. Depending on the specific requirements of the analysis, an investigator might choose one or several of these tools.

7.10 Recording Video from a Forensic Virtual Machine

Recording video from a forensic virtual machine (VM) that was created from a forensic image is not just a technical procedure; it's a crucial part of preserving and analyzing digital evidence in a meticulous and traceable manner. Below are the reasons why this approach is essential:

Immutable Record

When a virtual machine is created from a forensic image, it's a snapshot of a system at a specific point in time. Recording a video of the interactions and findings within this VM provides an immutable and chronological record. It ensures that every action taken can be reviewed, analyzed, and presented, leaving no room for doubt or ambiguity.

Transparency and Accountability

The video serves as a transparent and detailed log of what was done during the investigation. This helps in maintaining the integrity of the process, proving that the examination was conducted ethically and without alteration of the original data. If questions arise later, the video can be referred back to, to demonstrate exactly what was done.

Legal Compliance

In legal scenarios, the chain of custody must be robust and without breaks. Video recordings from the forensic VM provide a visual and auditable trail that can be an integral part of court proceedings. They offer judges, lawyers, and juries a clear and understandable view of the digital evidence, often aiding in decisions.

Training and Collaboration

The videos are not only useful for the case at hand but can be utilized for training purposes. They offer a real-world insight into how a forensic examination is conducted, the tools used, and the methodologies followed. Furthermore, they facilitate collaboration between teams and experts, allowing them to review and discuss findings visually.

Error Detection

If mistakes are made during the investigation, video recordings enable forensic analysts to backtrack and understand where things went wrong. This can be vital for correcting errors and learning from them for future investigations.

Enhancing Public Trust

Lastly, the practice of recording video from forensic VMs can also contribute to enhancing public trust in digital forensic processes. It sends a strong signal that the work is conducted with utmost professionalism, thoroughness, and adherence to legal standards.

7.10.1 Record a video from the forensicVM

1. **Show the control bar on the forensicVM web screen web interface by clicking the arrow button.**

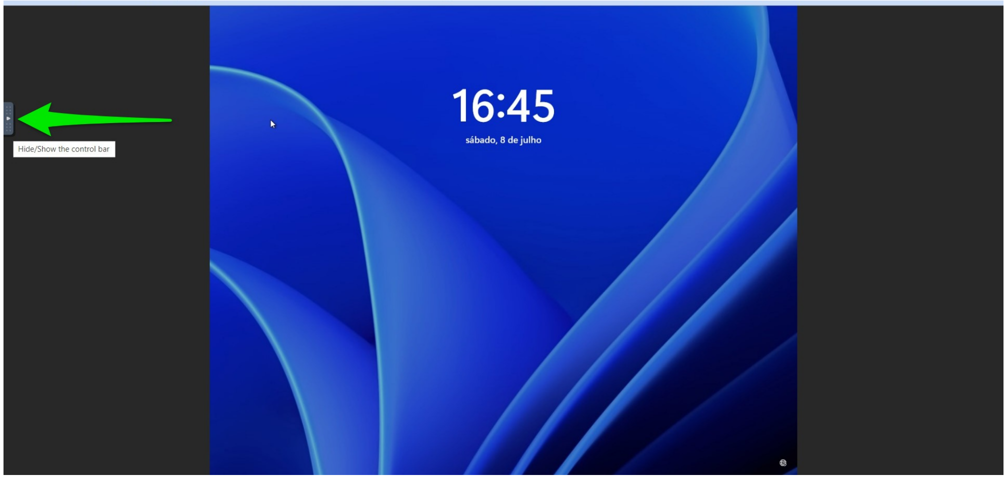


Fig. 7.88: Show the control bar

2. **Press the video recording icon. This icon will open a modal box.**

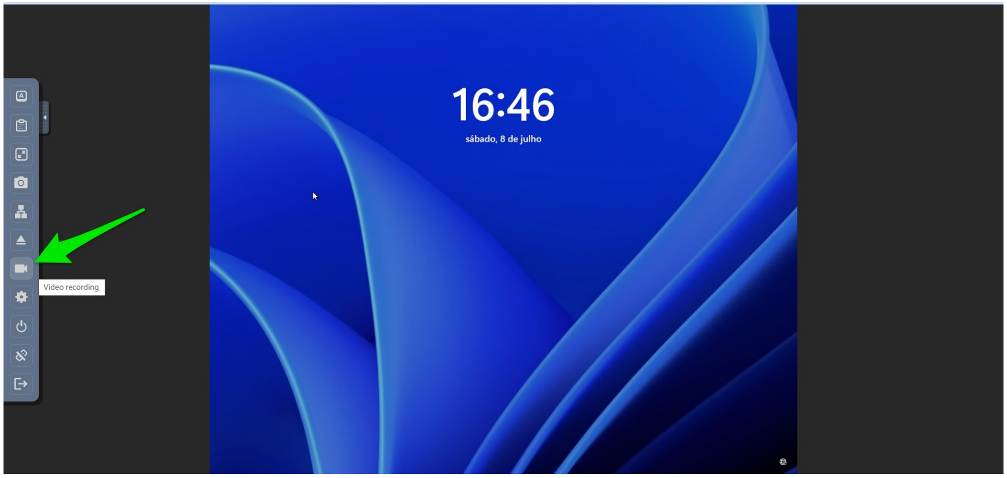
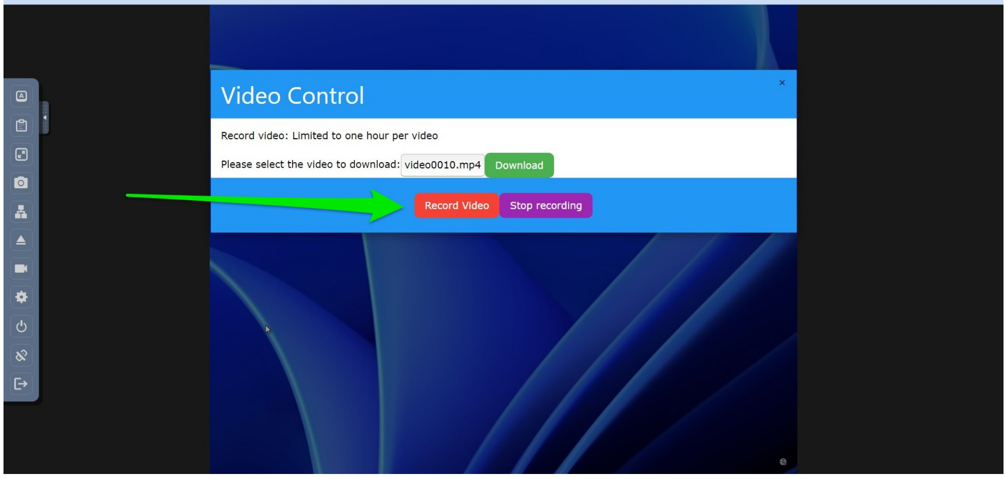


Fig. 7.89: Press the video recording icon

3. **Press the red "Record Video" button.**



Record video: Limited to one hour per video

Please select the video to download: video0010.mp4

Fig. 7.90: Press "Record Video" button

4. **The recording is in progress; it can be up to 3 hours of recording before the video stops. The "rec" animation on the top right will show that the recording is in progress on the server.**

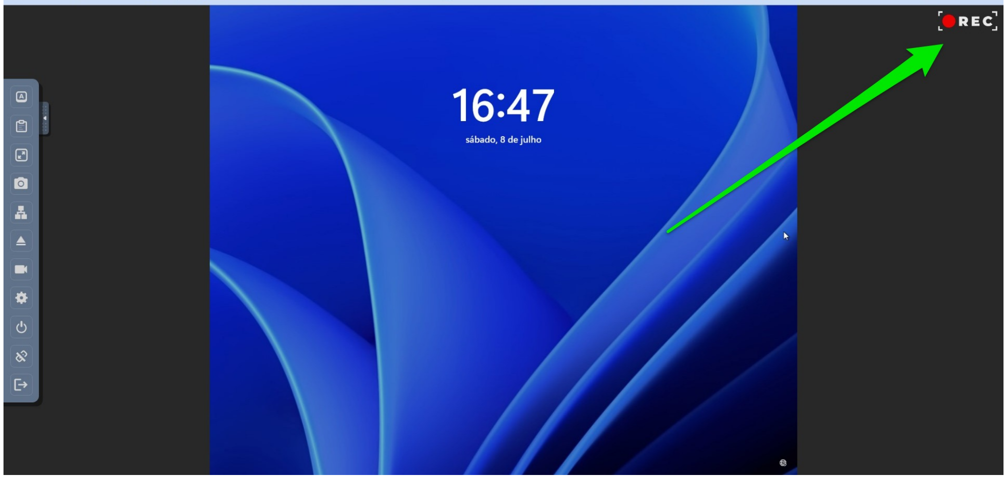


Fig. 7.91: Recording in progress

7.10.2 Stop the video recording

1. **To stop the recording, first press the record icon on the control bar.**

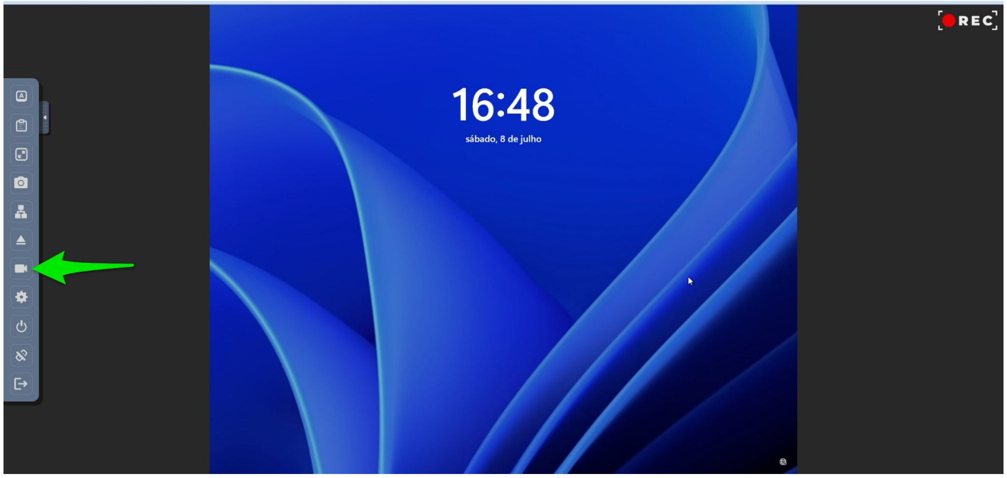
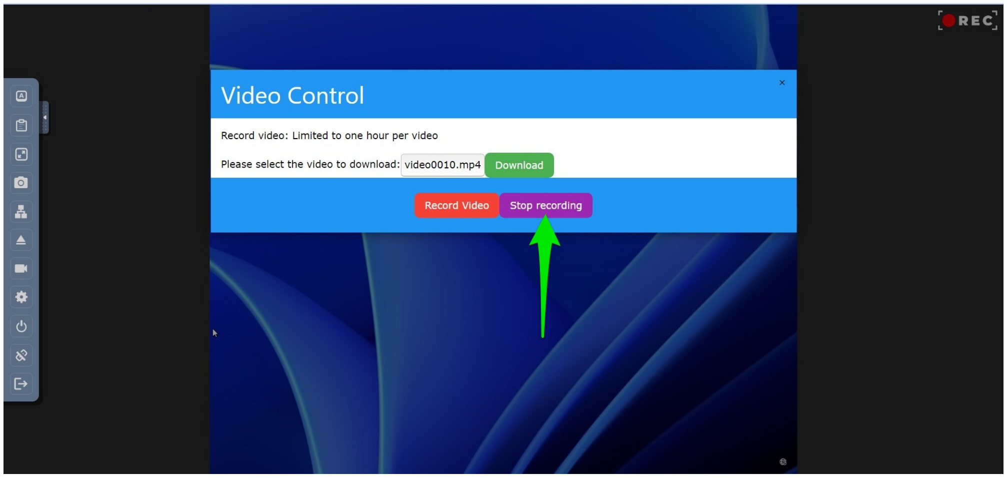


Fig. 7.92: Stop recording

2. **On the modal box, please press the "Stop recording button".**

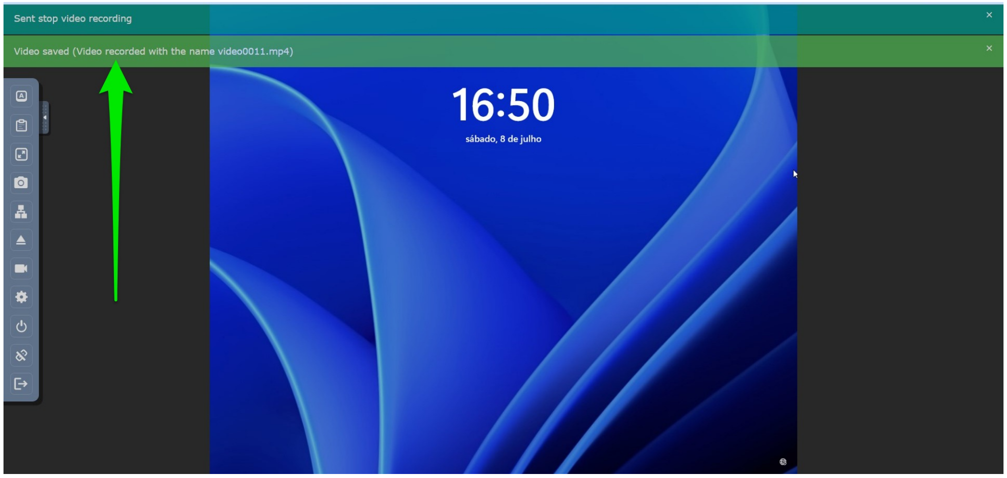


Record video: Limited to one hour per video

Please select the video to download: video0010.mp4

Fig. 7.93: Stop recording button

3. **You will see two notification messages. The first one says, "Sent stop video recording," to indicate that the video has stopped recording. The video has to be processed on the server to download. When the video is completed on the server, you will see a second notification message stating, "Video saved (Video recorder with the name videoNNNN.mp4)", where NNNN is the video number. Please note down this number.**



Sent stop video recording ×

Video saved (Video recorded with the name video0011.mp4) ×

Fig. 7.94: Notifications

7.10.3 Download video recording

1. **To download, please press the record video icon again on the control bar.**

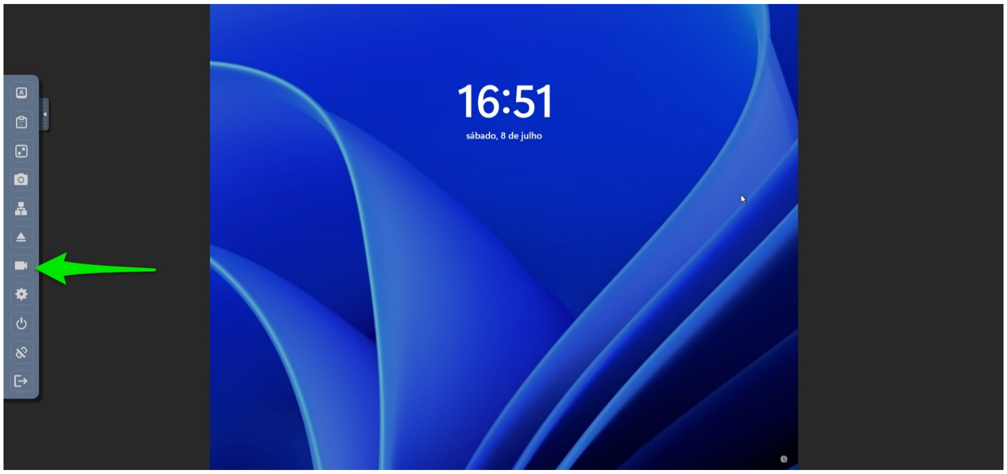
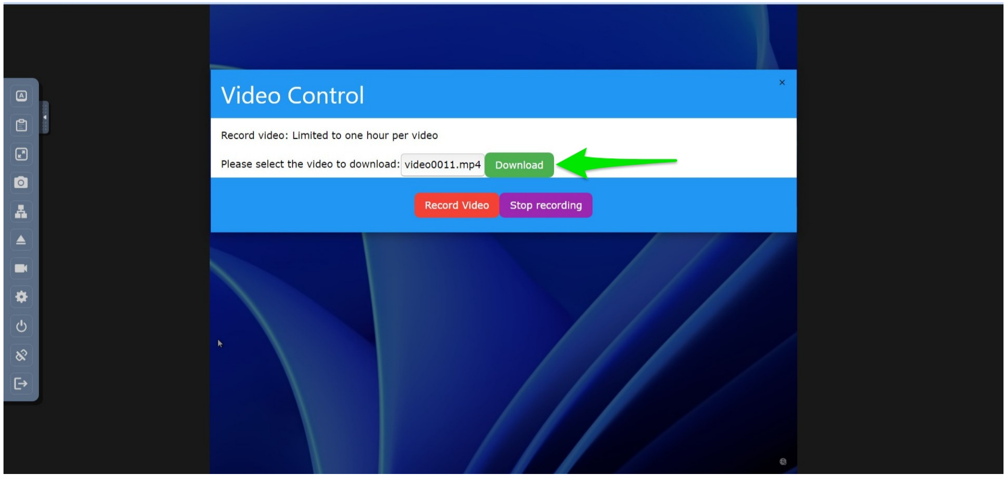


Fig. 7.95: Download icon

2. **Now, press the "Download" button. You should now wait until the download is ready. It will start download automatically, so please do not close the webpage. The video preparation time and the download time will directly depend on the video size.**



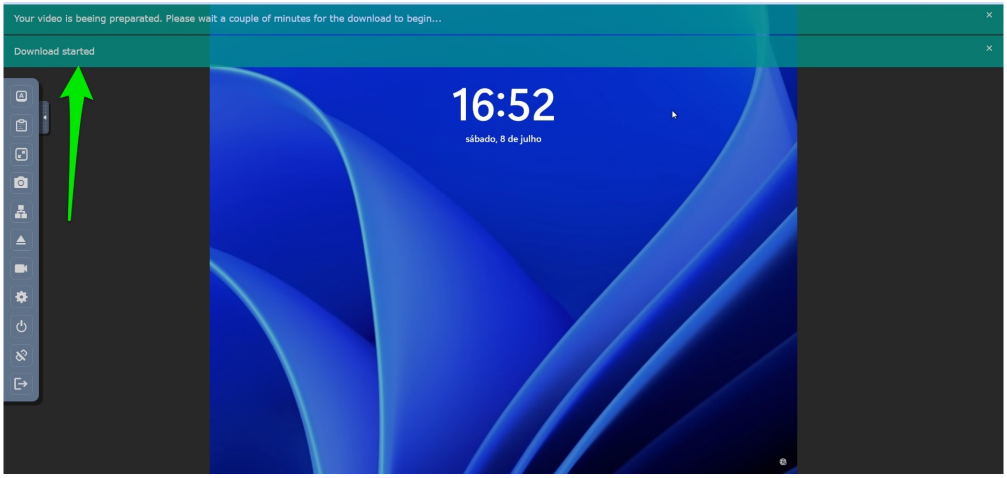
Video Control

Record video: Limited to one hour per video

Please select the video to download: video0011.mp4

Fig. 7.96: Press “Download” button

3. **Download started message**



Your video is beeing prepared. Please wait a couple of minutes for the download to begin...

Download started

Fig. 7.97: Download started message

4. **After the video is downloaded, in the web browser, please open the download folder where the video file is.**

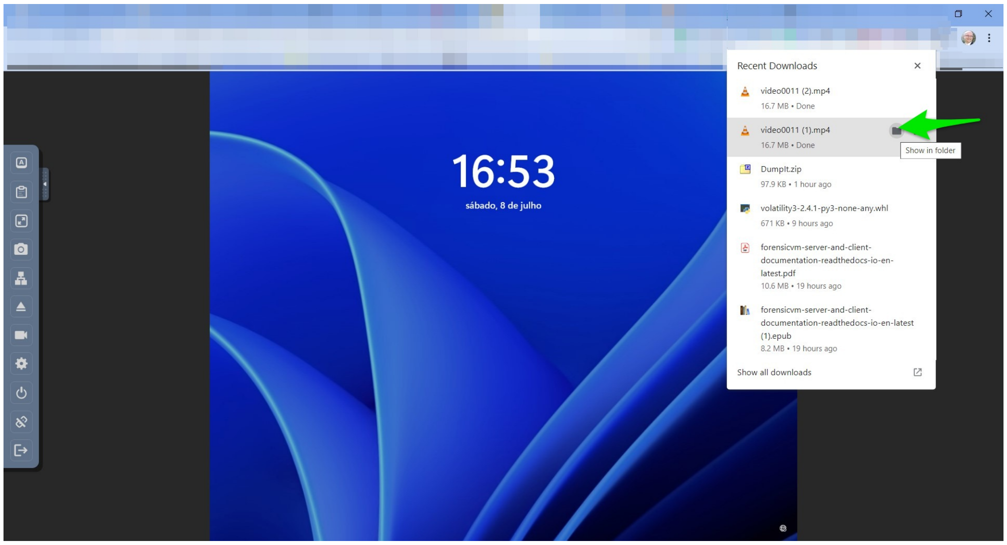


Fig. 7.98: Locate downloaded file

7.10.4 Import video recording for analysis in Autopsy Software

1. **With the shift key pressed, press the right-click on the mouse over the video file. Then select the "Copy as path" option on the menu.**

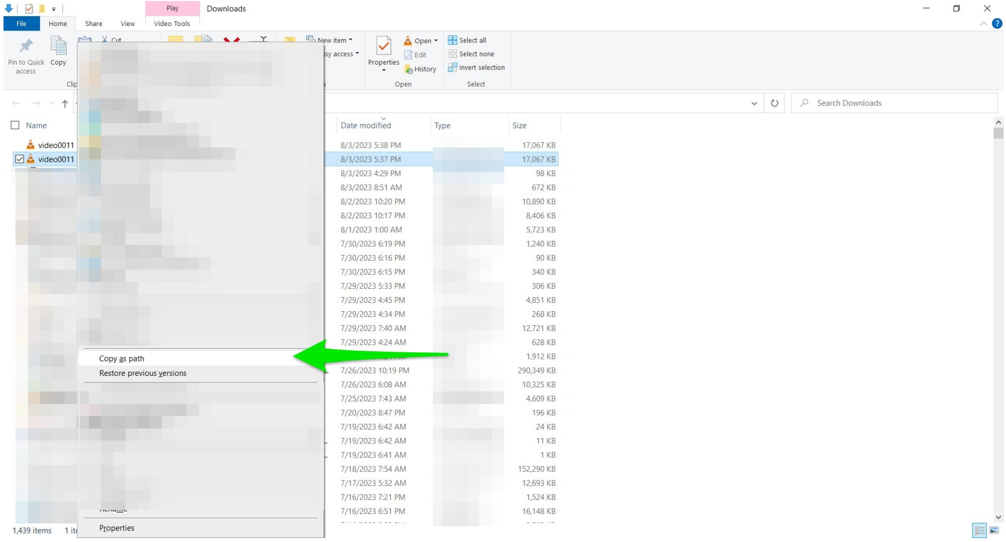
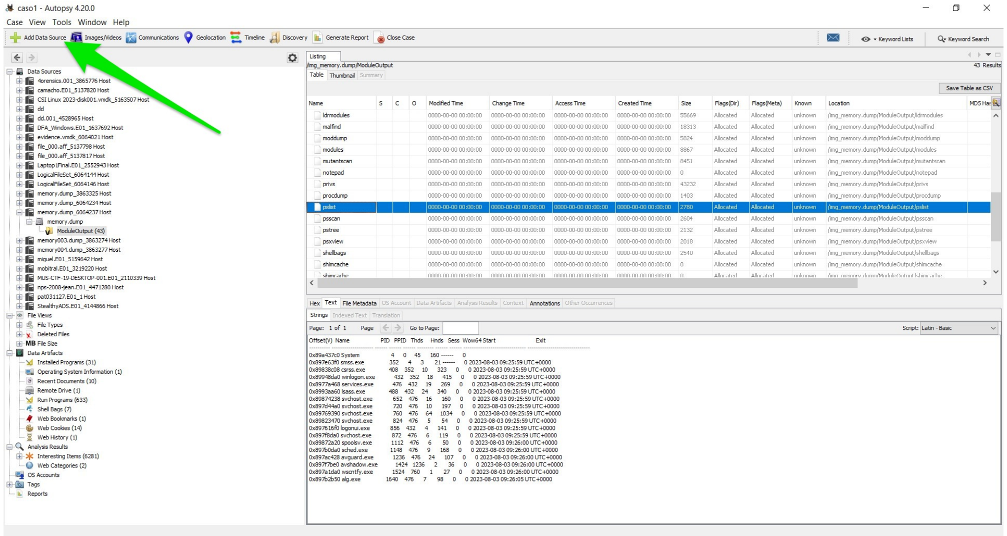


Fig. 7.99: Copy as path

2. **Open Autopsy software. On the menu bar, please click the "Add Data Source" button.**



Data Sources
- 4orensics.001_3865776 Host
- camacho.E01_5137820 Host
- CSI Linux 2023-disk001.vmdk_5163507 Host
- dd
- dd.001_4528965 Host
- DFA_Windows.E01_1637692 Host
- evidence.vmdk_6064021 Host
- file_000.aff_5137798 Host
- file_000.aff_5137817 Host
- Laptop1Final.E01_2552943 Host
- LogicalFileSet_6064144 Host
- LogicalFileSet_6064146 Host
- memory.dump_3863325 Host
- memory.dump_6064234 Host
- memory.dump_6064237 Host
  - memory.dump
    - ModuleOutput (43)
- memory003.dump_3863274 Host
- memory004.dump_3863277 Host
- miguel.E01_5159642 Host
- mobitral.E01_3219220 Host
- MUS-CTF-19-DESKTOP-001.E01_2110339 Host
- nps-2008-jean.E01_4471280 Host
- pat031127.E01_1 Host
- StealthyADS.E01_4144866 Host

File Views
- File Types
- Deleted Files
- MB File Size

Data Artifacts
- Installed Programs (31)
- Operating System Information (1)
- Recent Documents (10)
- Remote Drive (1)
- Run Programs (633)
- Shell Bags (7)
- Web Bookmarks (1)
- Web Cookies (14)
- Web History (1)

Analysis Results
- Interesting Items (6281)
- Web Categories (2)

OS Accounts

Tags

Reports

/img_memory.dump/ModuleOutput

43 Results

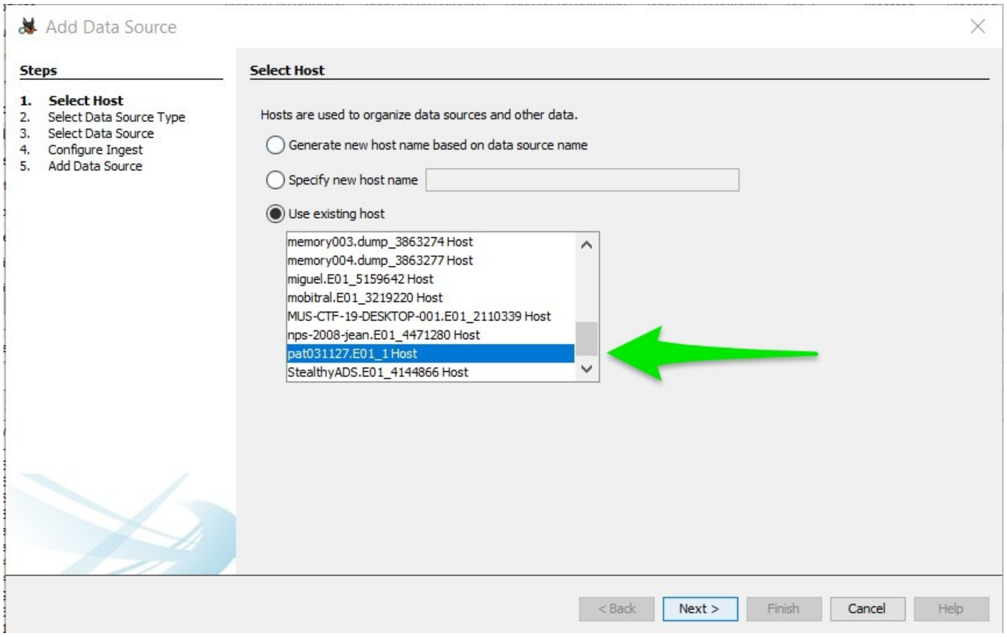
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location	MD5 Has
ldrmodules				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	55669	Allocated	Allocated	unknown	/img_memory.dump/ModuleOutput/ldrmodules	
malfind				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	18313	Allocated	Allocated	unknown	/img_memory.dump/ModuleOutput/malfind	
moddump				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	5824	Allocated	Allocated	unknown	/img_memory.dump/ModuleOutput/moddump	
modules				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	8867	Allocated	Allocated	unknown	/img_memory.dump/ModuleOutput/modules	
mutantscan				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	8451	Allocated	Allocated	unknown	/img_memory.dump/ModuleOutput/mutantscan	
notepad				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/img_memory.dump/ModuleOutput/notepad	
privs				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	43232	Allocated	Allocated	unknown	/img_memory.dump/ModuleOutput/privs	
procdump				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1403	Allocated	Allocated	unknown	/img_memory.dump/ModuleOutput/procdump	
pslist				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	2780	Allocated	Allocated	unknown	/img_memory.dump/ModuleOutput/pslist	
psscan				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	2604	Allocated	Allocated	unknown	/img_memory.dump/ModuleOutput/psscan	
pstree				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	2132	Allocated	Allocated	unknown	/img_memory.dump/ModuleOutput/pstree	
psxview				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	2018	Allocated	Allocated	unknown	/img_memory.dump/ModuleOutput/psxview	
shellbags				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	2540	Allocated	Allocated	unknown	/img_memory.dump/ModuleOutput/shellbags	
shimcache				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/img_memory.dump/ModuleOutput/shimcache	
shimcache				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/img_memory.dump/ModuleOutput/shimcache	

Page: 1 of 1 Page Go to Page:

```
Offset(V)  Name                 PID   PPID   Thds   Hnds   Sess  Wow64 Start                          Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0x89a437c0 System                 4      0     45     160 ------      0
0x897e63f0 smss.exe             352      4      3      21 ------      0 2023-08-03 09:25:59 UTC+0000
0x89838c08 csrss.exe            408    352     10     323      0      0 2023-08-03 09:25:59 UTC+0000
0x89948da0 winlogon.exe         432    352     18     415      0      0 2023-08-03 09:25:59 UTC+0000
0x8977a468 services.exe         476    432     19     269      0      0 2023-08-03 09:25:59 UTC+0000
0x8993aa60 lsass.exe            488    432     24     340      0      0 2023-08-03 09:25:59 UTC+0000
0x89874238 svchost.exe          652    476     16     160      0      0 2023-08-03 09:25:59 UTC+0000
0x897d44a0 svchost.exe          720    476     10     197      0      0 2023-08-03 09:25:59 UTC+0000
0x89769390 svchost.exe          760    476     64    1034      0      0 2023-08-03 09:25:59 UTC+0000
0x89823470 svchost.exe          824    476      5      54      0      0 2023-08-03 09:25:59 UTC+0000
0x897616f0 logonui.exe          856    432      4     141      0      0 2023-08-03 09:25:59 UTC+0000
0x897f8da0 svchost.exe          872    476      6     119      0      0 2023-08-03 09:25:59 UTC+0000
0x89872a20 spoolsv.exe         1112    476      6      50      0      0 2023-08-03 09:26:00 UTC+0000
0x897b0da0 sched.exe           1148    476      9     168      0      0 2023-08-03 09:26:00 UTC+0000
0x897ac428 avguard.exe         1236    476     24     107      0      0 2023-08-03 09:26:00 UTC+0000
0x897f7be0 avshadow.exe        1424   1236      2      36      0      0 2023-08-03 09:26:00 UTC+0000
0x897a1da0 wscntfy.exe         1524    760      1      27      0      0 2023-08-03 09:26:00 UTC+0000
0x897b2b50 alg.exe             1640    476      7      98      0      0 2023-08-03 09:26:05 UTC+0000
```

Fig. 7.100: Open Autopsy

3. **Select the host and click next.**



Steps

1. **Select Host**
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source

Select Host

Hosts are used to organize data sources and other data.

○ Generate new host name based on data source name

○ Specify new host name

● Use existing host

- memory003.dump_3863274 Host
- memory004.dump_3863277 Host
- miguel.E01_5159642 Host
- mobitral.E01_3219220 Host
- MUS-CTF-19-DESKTOP-001.E01_2110339 Host
- nps-2008-jean.E01_4471280 Host
- pat031127.E01_1 Host
- StealthyADS.E01_4144866 Host

Fig. 7.101: Select host

4. **Select** Logical Files **and click next.**

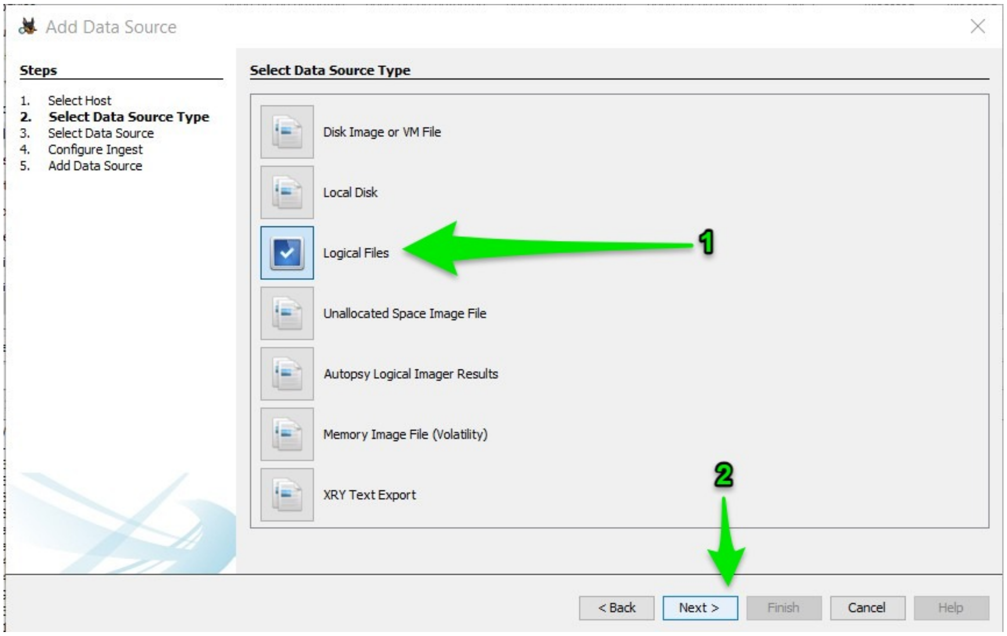
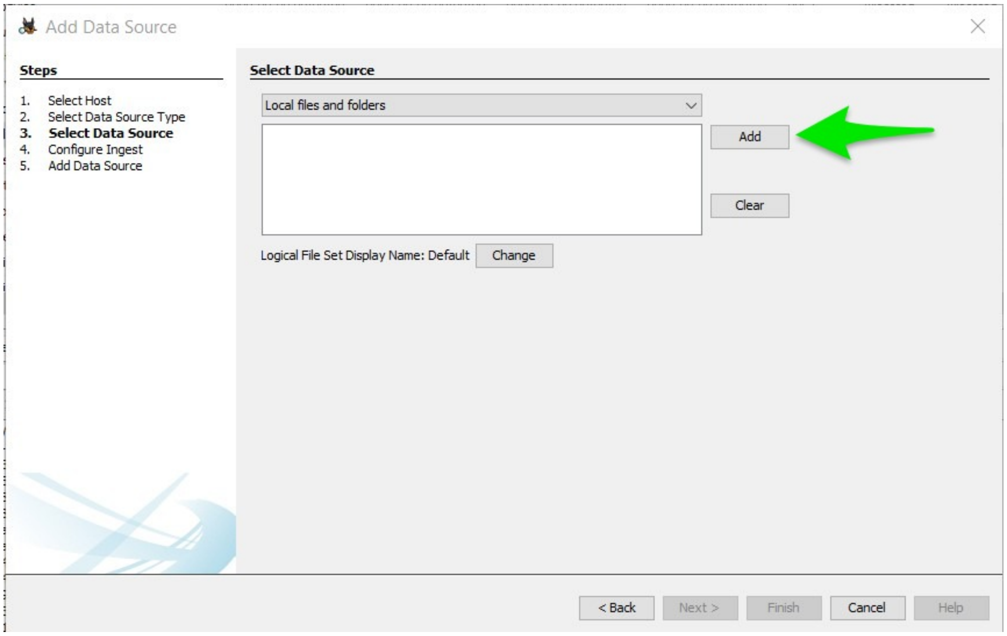


Fig. 7.102: Select Logical Files

5. **Click Add to select the video.**

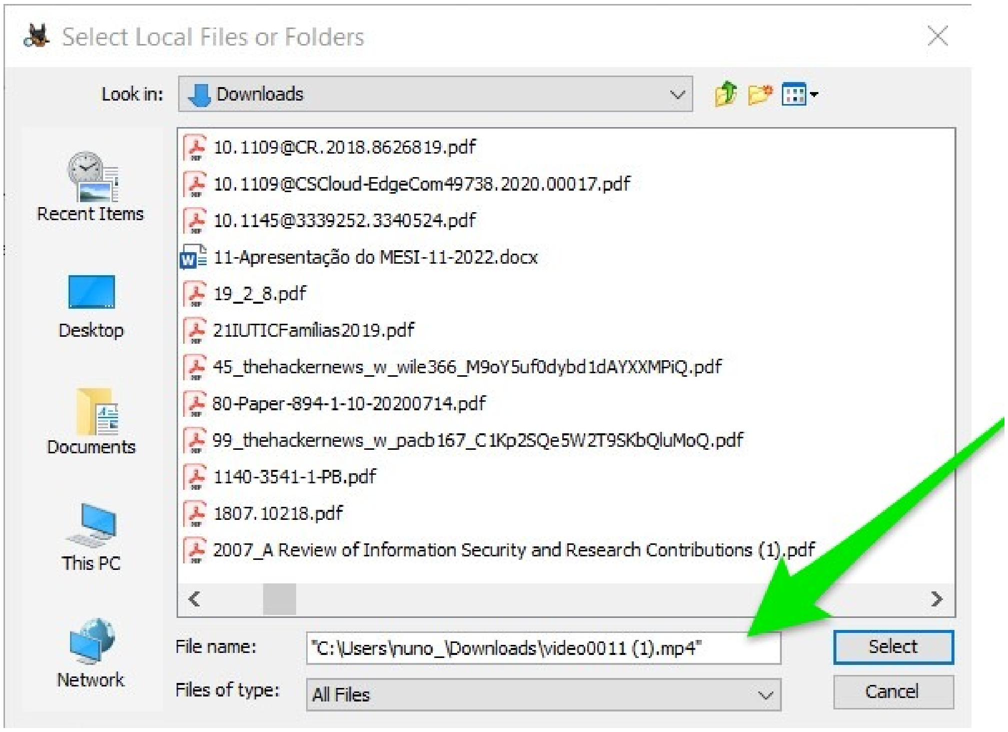


Local files and folders

Logical File Set Display Name: Default

Fig. 7.103: Click Add to select video

6. **Paste the path in the “File name:” field and click the “Select” button.**



Select Local Files or Folders

Look in: Downloads

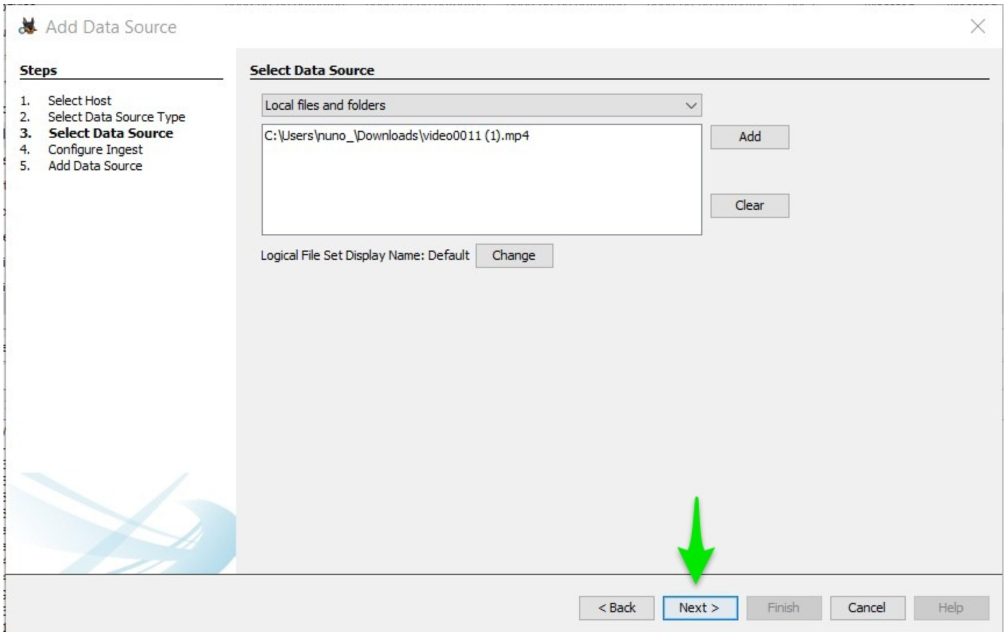
- 10.1109@CR.2018.8626819.pdf
- 10.1109@CSCloud-EdgeCom49738.2020.00017.pdf
- 10.1145@3339252.3340524.pdf
- 11-Apresentação do MESI-11-2022.docx
- 19_2_8.pdf
- 21IUTICFamílias2019.pdf
- 45_thehackernews_w_wile366_M9oY5uf0dybd1dAYXXMPiQ.pdf
- 80-Paper-894-1-10-20200714.pdf
- 99_thehackernews_w_pacb167_C1Kp2SQe5W2T9SKbQluMoQ.pdf
- 1140-3541-1-PB.pdf
- 1807.10218.pdf
- 2007_A Review of Information Security and Research Contributions (1).pdf

File name: "C:\Users\nuno_\Downloads\video0011 (1).mp4"

Files of type: All Files

Fig. 7.104: Select video to import

7. **Click Next.**



Add Data Source

Steps

1. Select Host
2. Select Data Source Type
3. **Select Data Source**
4. Configure Ingest
5. Add Data Source

Select Data Source

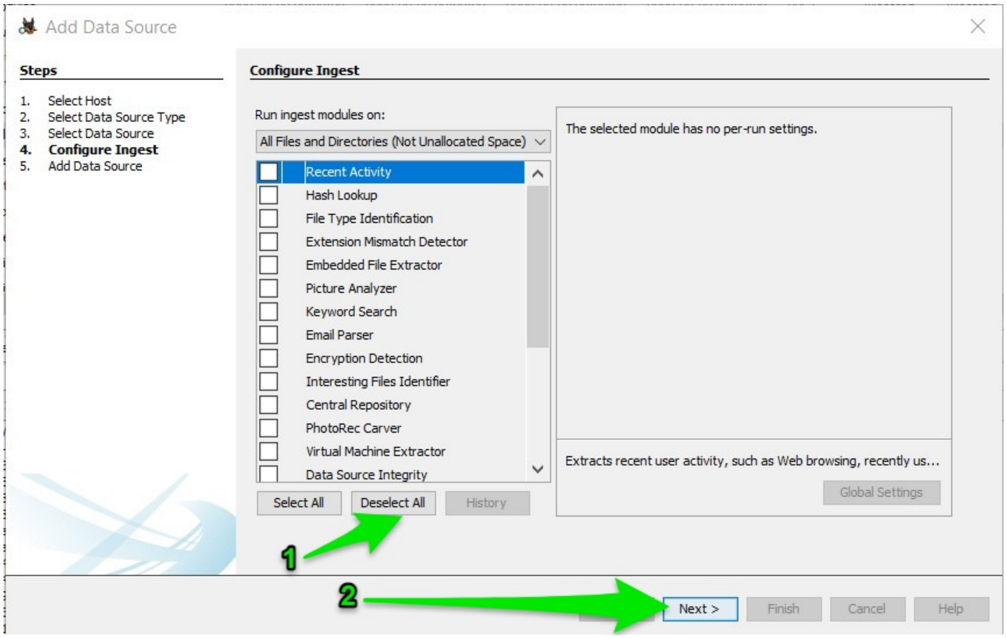
Local files and folders

C:\Users\nuno_\Downloads\video0011 (1).mp4

Logical File Set Display Name: Default

Fig. 7.105: Click Next

8. **Deselect all ingest plugins and click next.**



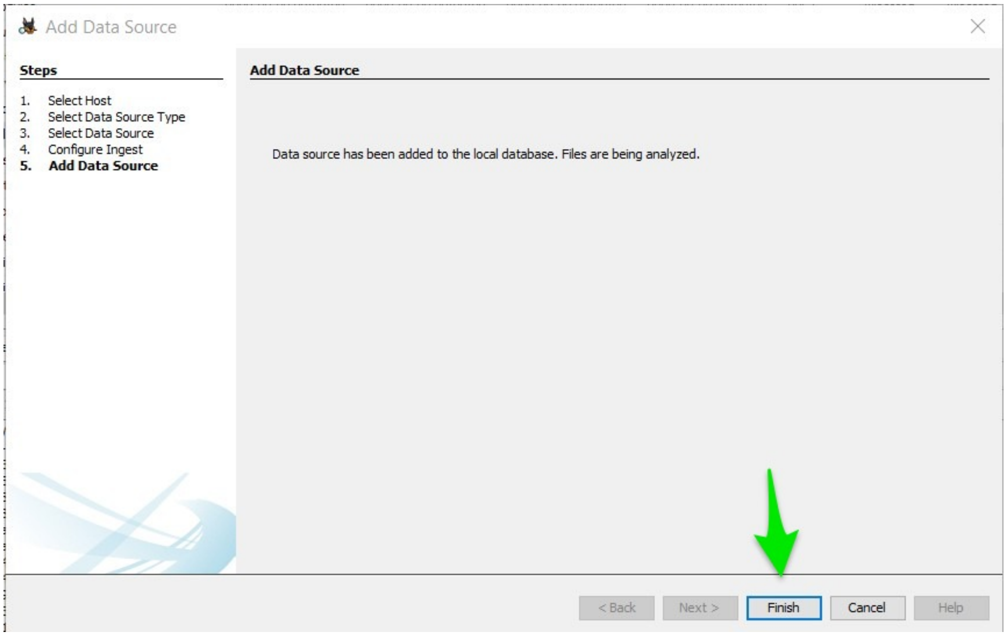
Run ingest modules on: All Files and Directories (Not Unallocated Space)

The selected module has no per-run settings.

Extracts recent user activity, such as Web browsing, recently us...

Fig. 7.106: Deselect plugins

9. **Click Finish.**



Data source has been added to the local database. Files are being analyzed.

Fig. 7.107: Click Finish

10. **1. Select the video file, 2. With the mouse right-click, "Add a File Tag", 3. Select the tag that is relevant to the forensic investigation.**

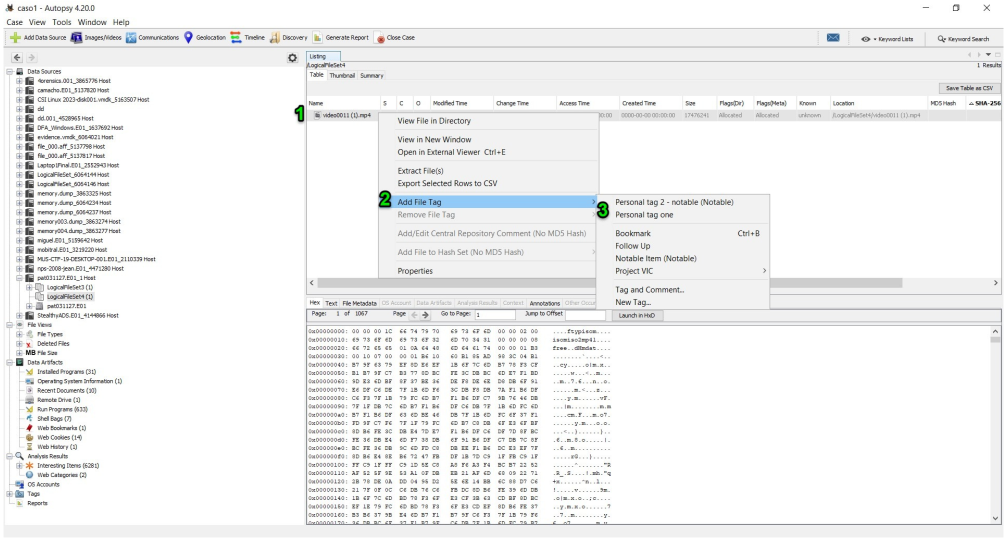


Fig. 7.108: Tagging video

Note: Video Recording Sound The current version of the video recording feature within the forensic virtual machine does not include sound. It captures only the visual interactions and activities within the system. We recognize the importance of sound in some investigations, and we are actively working to add this capability in a forthcoming version of our software.

In the meantime, if sound recording is a necessary component of your forensic analysis, we advise utilizing third-party tools specifically designed for video and audio capture. Please ensure that any third-party tool used complies with your legal and organizational requirements.

7.11 Gather Evidence Using the Evidence Disk

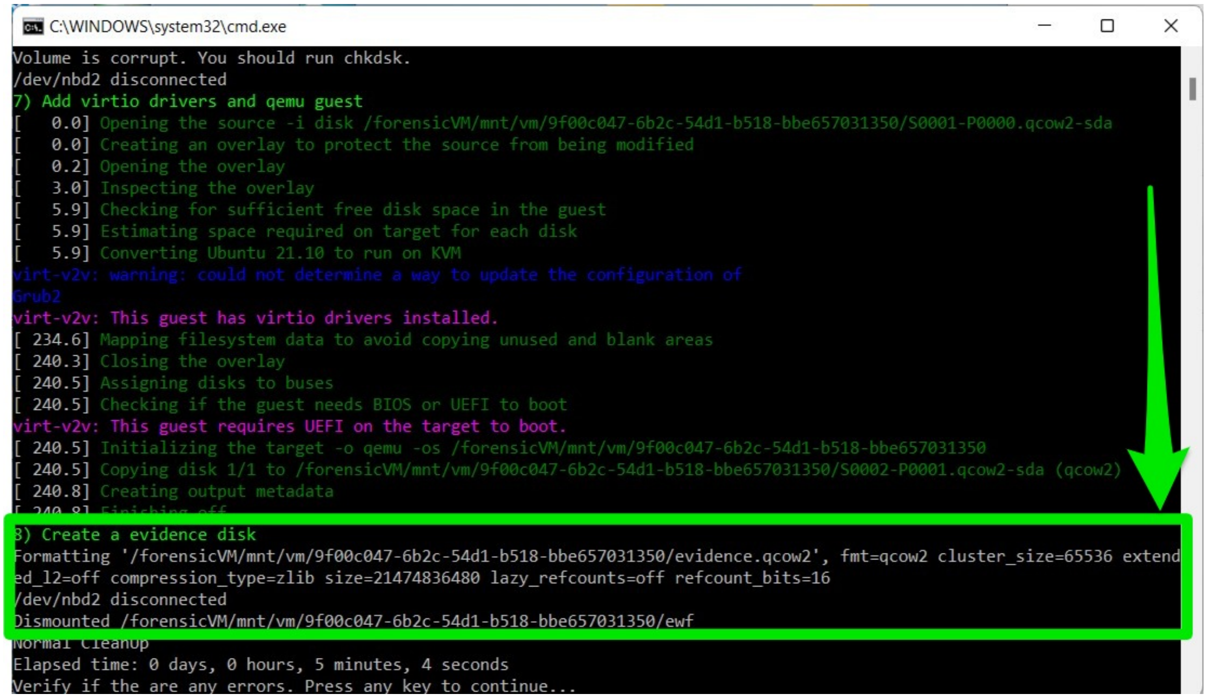
The evidence disk is an automatically generated drive that materializes during the conversion of a forensic image to a ForensicVM. This utility drive is populated with directories that carry the same names as the Autopsy tags. These directories serve as designated containers, wherein the forensic investigator is expected to compile and organize evidence relevant to each tag. If ever the need arises, the investigator has the option to reset the evidence disk to its initial state. However, such an action should be approached with caution, as it would entail the deletion of all previously gathered evidence.

In the event that new tags are introduced in Autopsy, corresponding folders for these tags will be fashioned once the plugin is restarted.

Tip: In order to fabricate any missing tag directories, it's essential to first halt the ForensicVM's operations. It's advised to shut down the ForensicVM, subsequently close the plugin, and then reopen it via the Autopsy ForensicVM Client Plugin. This procedure ensures that the environment is refreshed and ready to incorporate new changes.

7.11.1 Evidence Disk Creation

The creation of the evidence disk is an automated process. When you transition a forensic image into a ForensicVM, regardless of whether the method employed is virtualization copy or linking to the forensic image, the evidence disk is fashioned during the final phase of this procedure.



C:\WINDOWS\system32\cmd.exe

```
Volume is corrupt. You should run chkdsk.
/dev/nbd2 disconnected
7) Add virtio drivers and qemu guest
[   0.0] Opening the source -i disk /forensicVM/mnt/vm/9f00c047-6b2c-54d1-b518-bbe657031350/S0001-P0000.qcow2-sda
[   0.0] Creating an overlay to protect the source from being modified
[   0.2] Opening the overlay
[   3.0] Inspecting the overlay
[   5.9] Checking for sufficient free disk space in the guest
[   5.9] Estimating space required on target for each disk
[   5.9] Converting Ubuntu 21.10 to run on KVM
virt-v2v: warning: could not determine a way to update the configuration of
Grub2
virt-v2v: This guest has virtio drivers installed.
[ 234.6] Mapping filesystem data to avoid copying unused and blank areas
[ 240.3] Closing the overlay
[ 240.5] Assigning disks to buses
[ 240.5] Checking if the guest needs BIOS or UEFI to boot
virt-v2v: This guest requires UEFI on the target to boot.
[ 240.5] Initializing the target -o qemu -os /forensicVM/mnt/vm/9f00c047-6b2c-54d1-b518-bbe657031350
[ 240.5] Copying disk 1/1 to /forensicVM/mnt/vm/9f00c047-6b2c-54d1-b518-bbe657031350/S0002-P0001.qcow2-sda (qcow2)
[ 240.8] Creating output metadata
[ 240.8] Finishing off
8) Create a evidence disk
Formatting '/forensicVM/mnt/vm/9f00c047-6b2c-54d1-b518-bbe657031350/evidence.qcow2', fmt=qcow2 cluster_size=65536 extend
ed_l2=off compression_type=zlib size=21474836480 lazy_refcounts=off refcount_bits=16
/dev/nbd2 disconnected
Dismounted /forensicVM/mnt/vm/9f00c047-6b2c-54d1-b518-bbe657031350/ewf
Normal CleanUp
Elapsed time: 0 days, 0 hours, 5 minutes, 4 seconds
Verify if the are any errors. Press any key to continue...
```

Fig. 7.109: Screenshot depicting the final phase of the ForensicVM conversion, showcasing the creation of the evidence disk.

7.11.2 Collecting Evidence: A Step-by-Step Guide

Collecting digital evidence is a meticulous process, demanding precision, patience, and an understanding of the system you are investigating. When using the ForensicVM, this process is facilitated, yet there are still specific steps to follow. Here's a comprehensive guide on how to go about it:

1. **Initiation of the ForensicVM**:

   Before you can begin your evidence collection, ensure that the ForensicVM is up and running. Start the virtual machine and patiently wait for it to boot up completely.

2. **Logging In**:

   Once the ForensicVM has completely loaded, proceed to log in using the credentials provided or set during the initial configuration. Remember, maintaining the security and integrity of the login process is crucial in a forensic investigation.

3. **System Exploration**:

   With access to the ForensicVM, you can now begin your deep dive into the system. Navigate through the directories, files, applications, and logs. Always keep an eye out for suspicious or relevant files, unusual patterns, or any anomalies that might serve as potential evidence.

4. **Copying Relevant Files to the** Evidence Disk:

   As you uncover potential pieces of evidence:

   - **For Windows Users**:

     The process is quite straightforward. Simply copy the relevant files or data and save them to the evidence disk, which is typically represented as the D: drive. This dedicated drive serves as a safe repository, ensuring that the original data remains uncompromised.

   - **For Linux Investigation**:

     Things might be quite different. Instead of having immediate access to the evidence disk, you might need to locate it first. Once found, proceed to mount the disk manually. After which, you can copy and save the necessary files or data to this disk.

Note: Remember, while the process might seem technical, the key is to maintain the integrity of the evidence and ensure that all actions are documented and reproducible. It's not just about finding the evidence, but also about ensuring its admissibility in a court of law.

Collect Evidence on Windows

Log into Windows

Begin by logging into the operating system. Should there be a need, employ a plugin to either craft a **forensicAdministrator** user or reset an existing user's password.

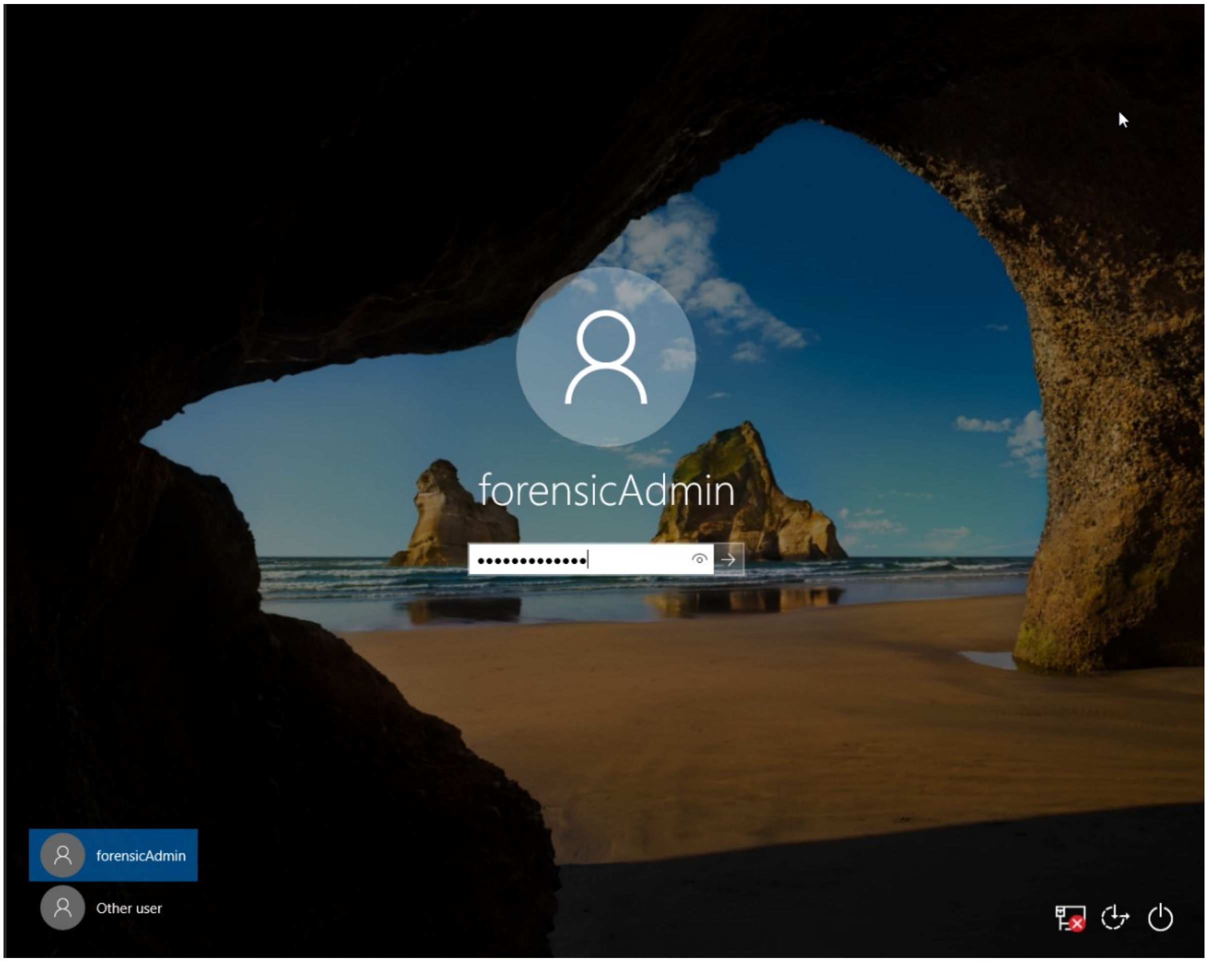
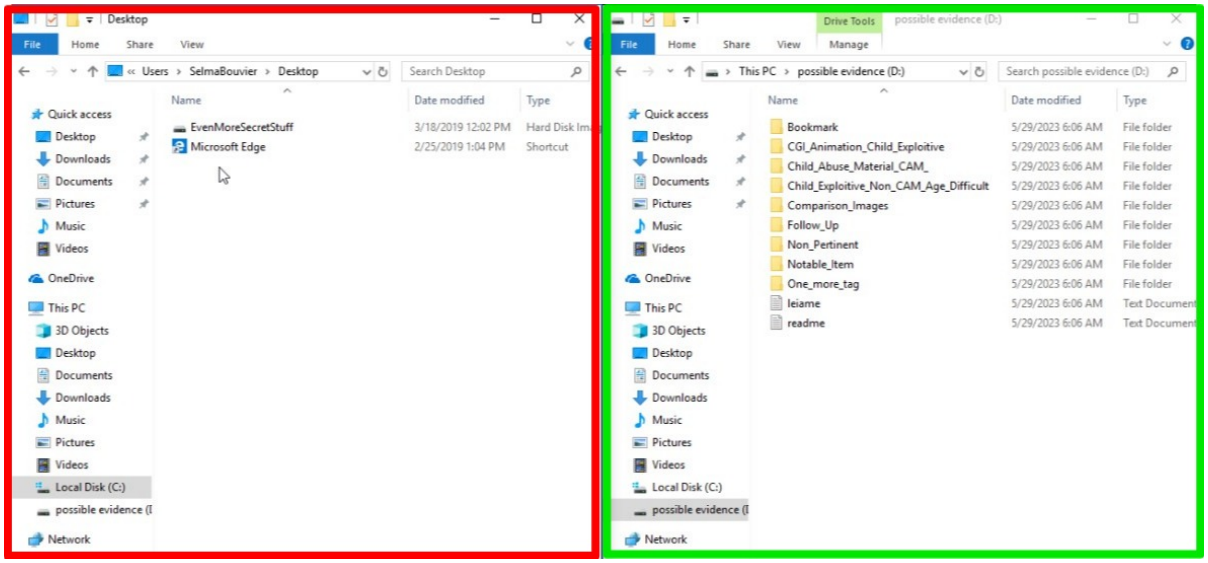


Fig. 7.110: Windows login screen.

Identify Evidence and the Evidence Disk

Post login, your next objective is to pinpoint the evidence disk. This specific disk is marked with the label **possible evidence**. Conventionally, it's designated as drive **D:**. The very essence of this disk is a collection of folders; each bearing the name of tags available in Autopsy. Though investigators have the liberty to tailor-make folders or sub-folders as per the requirements of their investigation, a suggested practice is to either refine or instate new tags in Autopsy. Post this step, both the Autopsy Plugin and the ForensicVM should be restarted.



Name	Date modified	Type
EvenMoreSecretStuff	3/18/2019 12:02 PM	Hard Disk Im
Microsoft Edge	2/25/2019 1:04 PM	Shortcut

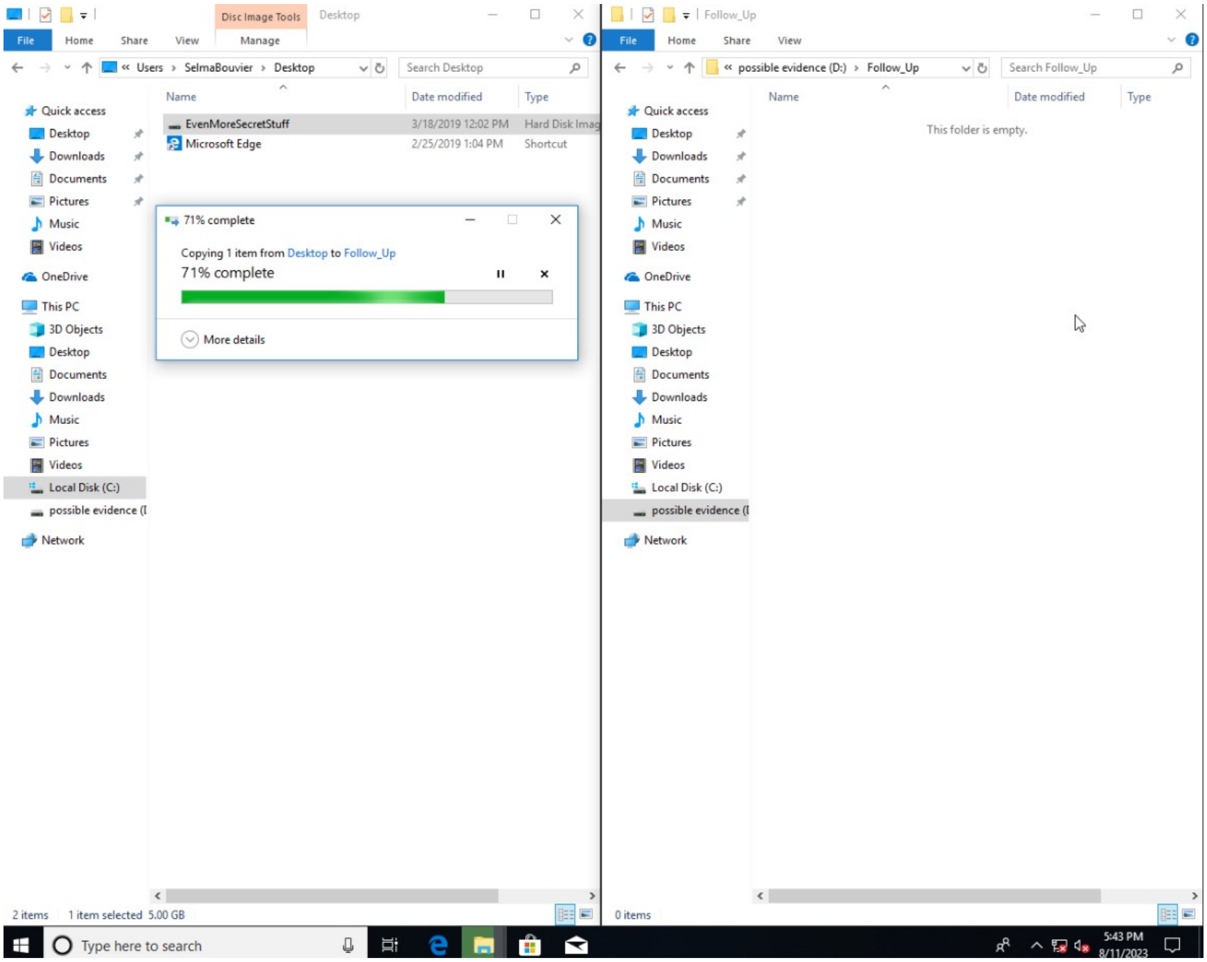
Name	Date modified	Type
Bookmark	5/29/2023 6:06 AM	File folder
CGI_Animation_Child_Exploitive	5/29/2023 6:06 AM	File folder
Child_Abuse_Material_CAM_	5/29/2023 6:06 AM	File folder
Child_Exploitive_Non_CAM_Age_Difficult	5/29/2023 6:06 AM	File folder
Comparison_Images	5/29/2023 6:06 AM	File folder
Follow_Up	5/29/2023 6:06 AM	File folder
Non_Pertinent	5/29/2023 6:06 AM	File folder
Notable_Item	5/29/2023 6:06 AM	File folder
One_more_tag	5/29/2023 6:06 AM	File folder
leiame	5/29/2023 6:06 AM	Text Document
readme	5/29/2023 6:06 AM	Text Document

Fig. 7.111: Identification and transfer of evidence.

The Fig. 7.111 offers a visual guide: The evidence drive is demarcated by a green rectangle, while the Windows Explorer - which is in the process of identifying potential evidence - is enclosed within a red rectangle. The objective here is to locate and transfer the identified evidence into the "possible evidence" drive, ensuring they're nestled under the appropriate Autopsy Folder Tags.

Example: Transferring the Entire Encrypted BitLocker Drive

The illustration below showcases the entirety of an encrypted BitLocker drive being transferred to the Autopsy 'Follow Up' tag. The foundational principle of this process lies in ensuring that the full, unaltered encrypted drive is copied, preserving its integrity for forensic examination. By copying the entire encrypted disk file, forensic analysts can ensure they are working with a complete and untampered set of data.



Name	Date modified	Type
EvenMoreSecretStuff	3/18/2019 12:02 PM	Hard Disk Imag
Microsoft Edge	2/25/2019 1:04 PM	Shortcut

2 items 1 item selected 5.00 GB

71% complete

Copying 1 item from Desktop to Follow_Up

71% complete

This folder is empty.

Fig. 7.112: Transferring the full encrypted BitLocker drive to the Autopsy ‘Follow Up’ tag.

Pre-importing Considerations for Autopsy

Before integrating the possible evidence drive into Autopsy, it's imperative to either shut down or stop the forensicVM. Opting for a shutdown is highly recommended. Choosing to merely stop the virtual machine introduces the risk of data corruption which could compromise the integrity of the evidence or render parts of it unusable.

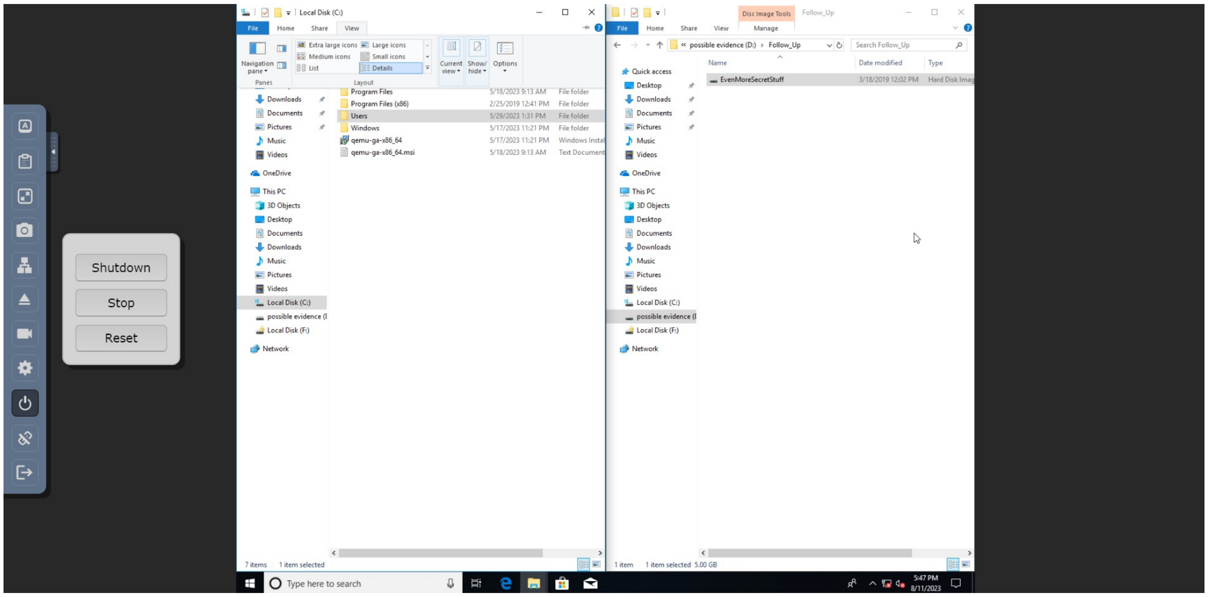


Fig. 7.113: Options available for safely preserving the BitLocker drive before importing to Autopsy.

Collecting Evidence on Linux

Accessing the System

To embark on evidence collection, the primary step involves gaining access to the Linux system. Knowledge of user credentials is essential. If you find yourself without the necessary credentials, consider utilizing available plugins to assist. Alternatively, developing and sharing a new plugin with the community could be a valuable contribution! The illustration below presents the login process for an Ubuntu 22.10 system featuring a comprehensive desktop environment.

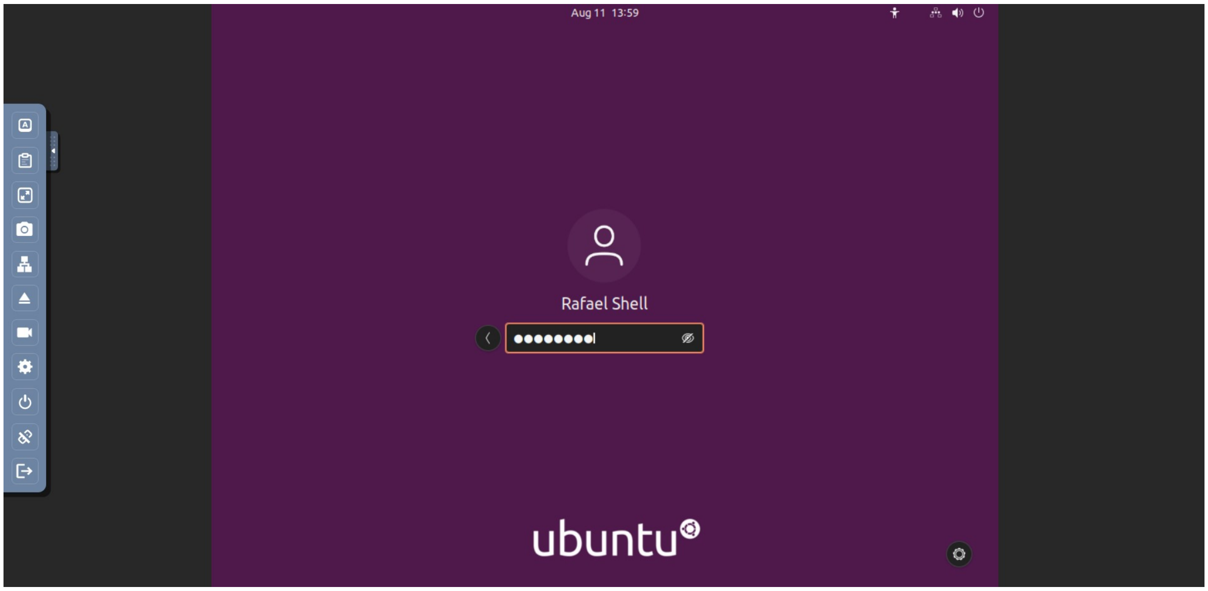


Fig. 7.114: Ubuntu 22.10 login screen with a full desktop.

Identifying the Evidence Disk

After successfully logging in, launch the file explorer to identify the evidence disk. In the given instance, one would navigate to “Other locations” and subsequently double-click on “possible evidence” to initiate its mounting.

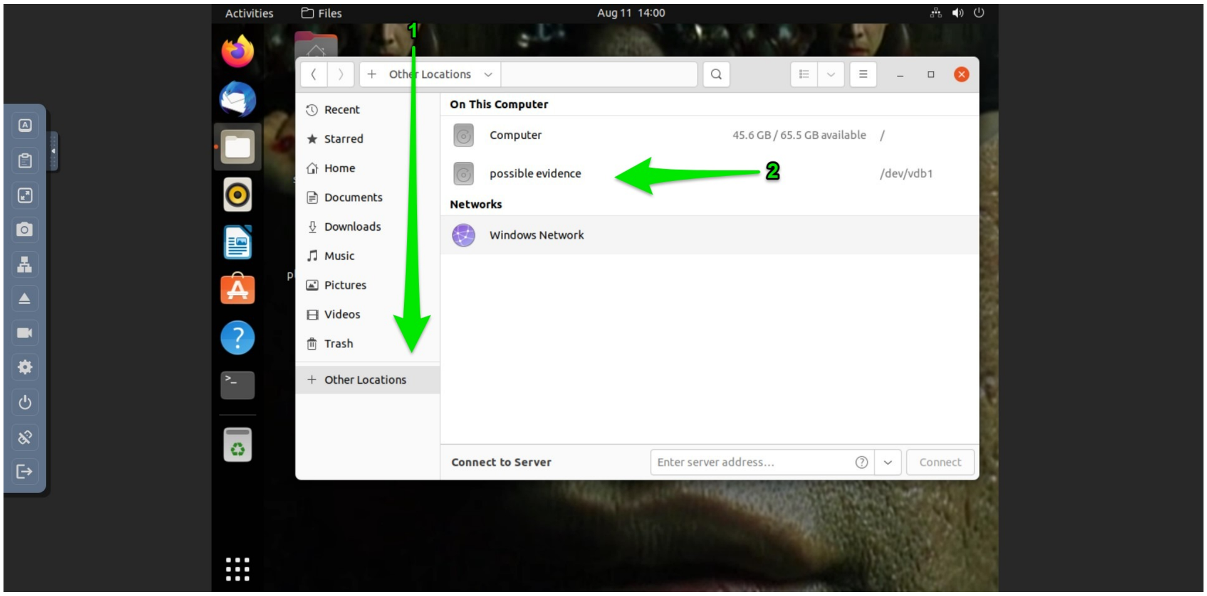


Fig. 7.115: Identifying the "possible evidence" disk in the file explorer.

Plan Evidence Gathering

Once the evidence drive is appropriately mounted, you're primed to delve into your evidence search. Displayed in the subsequent figure are folders corresponding to various Autopsy Tags, offering a structured approach to evidence organization.

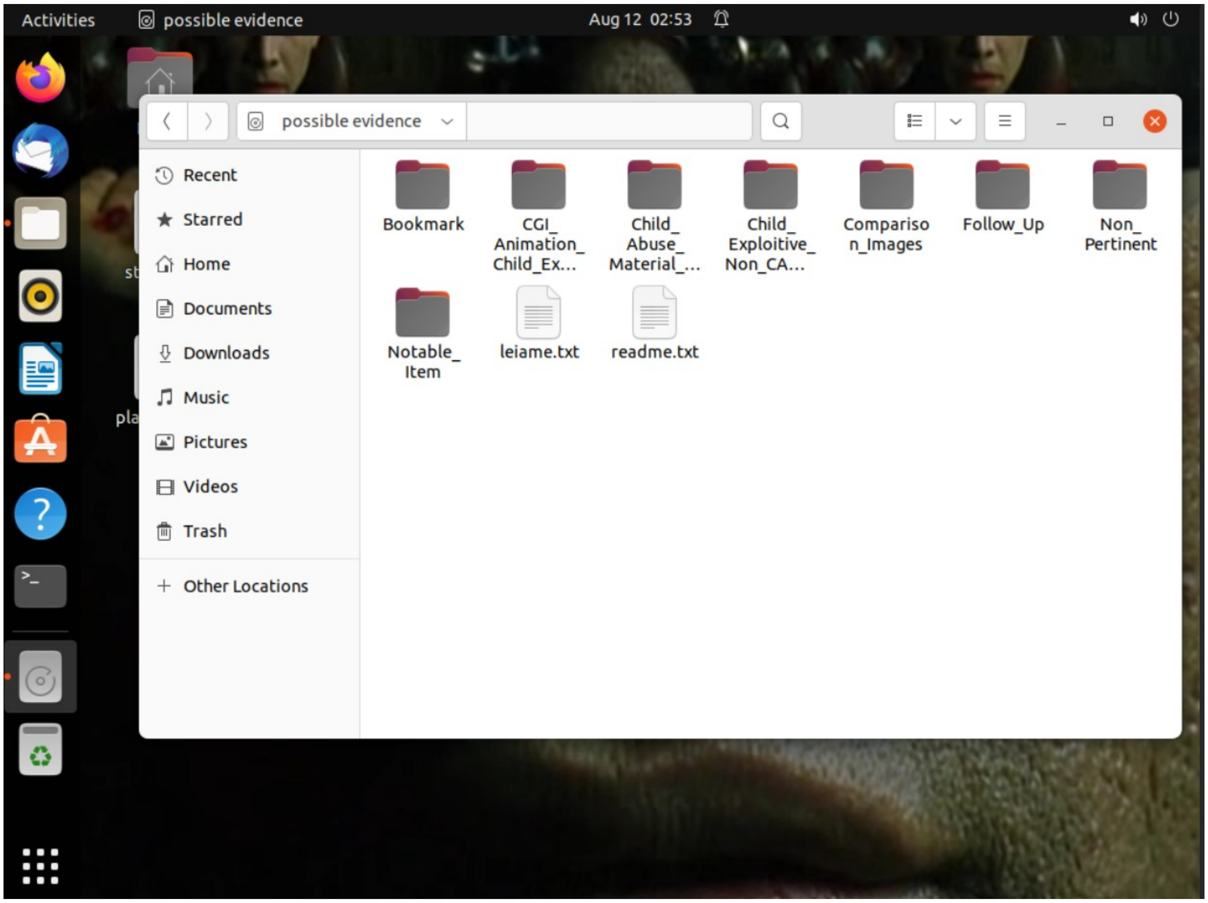
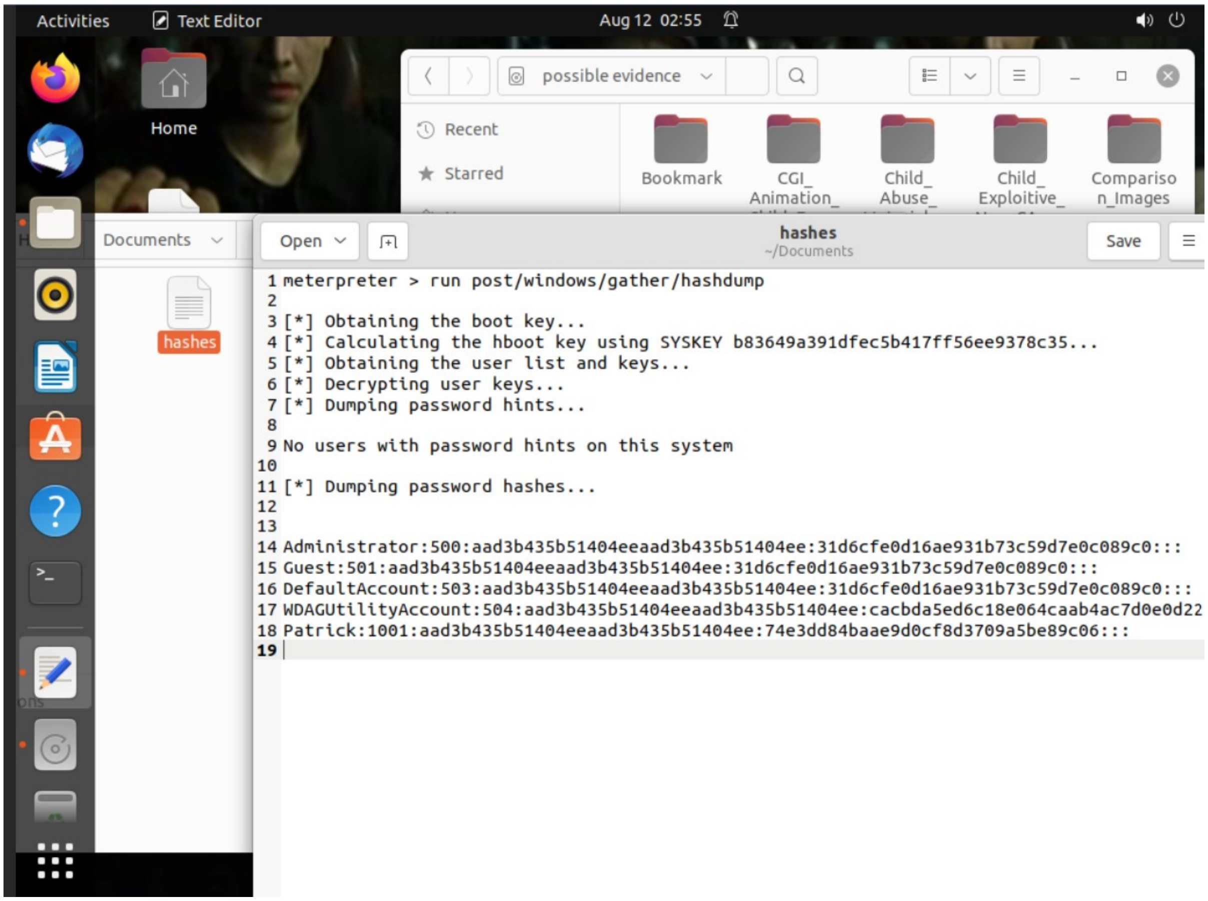


Fig. 7.116: Autopsy Tags folders for structured evidence organization.

Explore and find possible evidence

Navigating to the designated folder, we discern a hash dump file alongside potential evidence pointing to the deployment of a meterpreter.



```
meterpreter > run post/windows/gather/hashdump

[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY b83649a391dfec5b417ff56ee9378c35...
[*] Obtaining the user list and keys...
[*] Decrypting user keys...
[*] Dumping password hints...

No users with password hints on this system

[*] Dumping password hashes...


Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:cacbda5ed6c18e064caab4ac7d0e0d22
Patrick:1001:aad3b435b51404eeaad3b435b51404ee:74e3dd84baae9d0cf8d3709a5be89c06:::
```

Fig. 7.117: Highlighting a hash dump file and indications of meterpreter usage.

Organize and Transfer Potential Evidence to the Evidence Drive

Now, to preserve this crucial data, ensure you copy the identified potential evidence to the designated "possible evidence" folder.

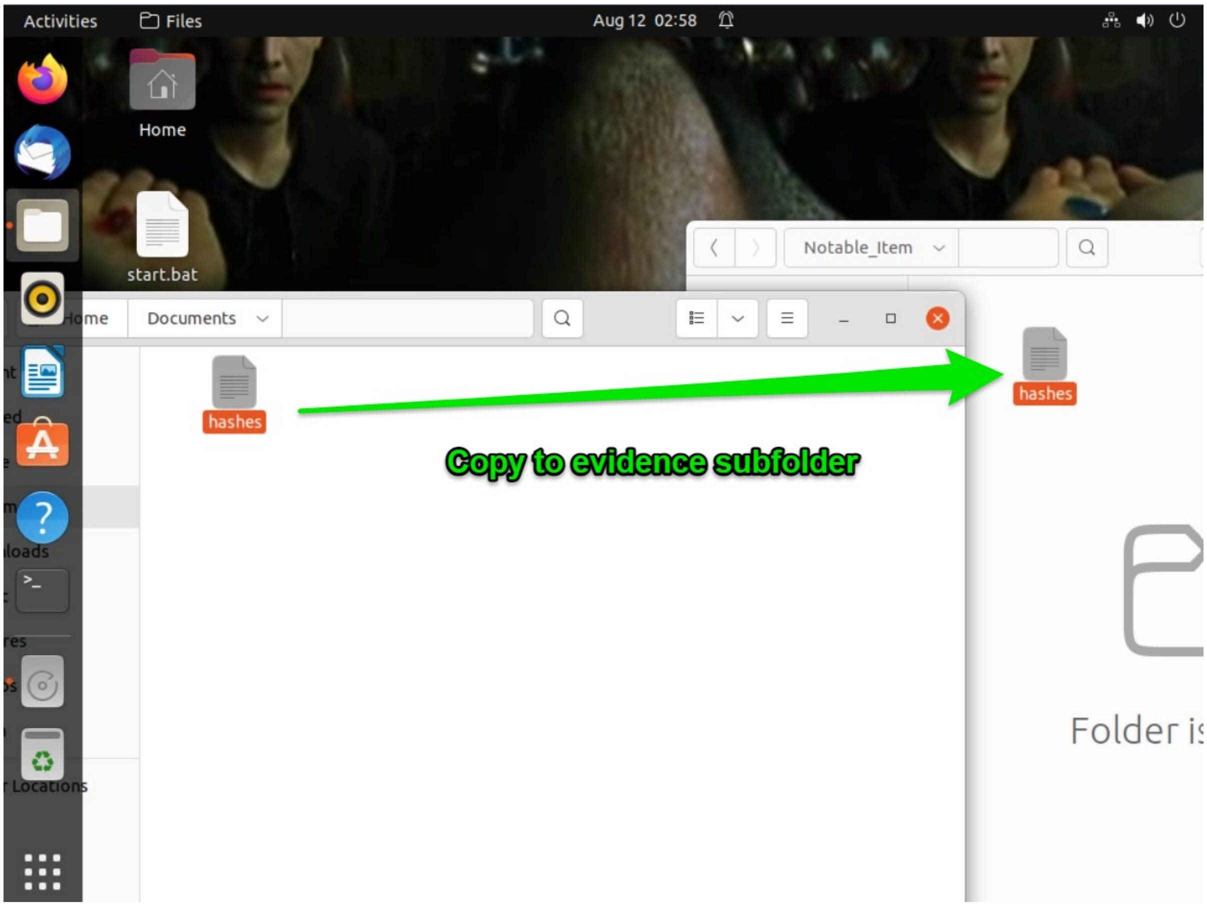


Fig. 7.118: Transferring discovered evidence to the "possible evidence" folder.

Preparing for Autopsy Integration

Before channeling the evidence disk into Autopsy, it's paramount to adopt one of two measures: either halt the forensicVM operations or completely shut it down. Favoring the shutdown route comes strongly advised, as a mere halt could inadvertently introduce data corruption. Such anomalies might jeopardize evidence integrity or entirely nullify certain data segments. In our context, you'd initiate this by selecting the power icon, followed by the "Power Off/Log Out" option from the ensuing menu.

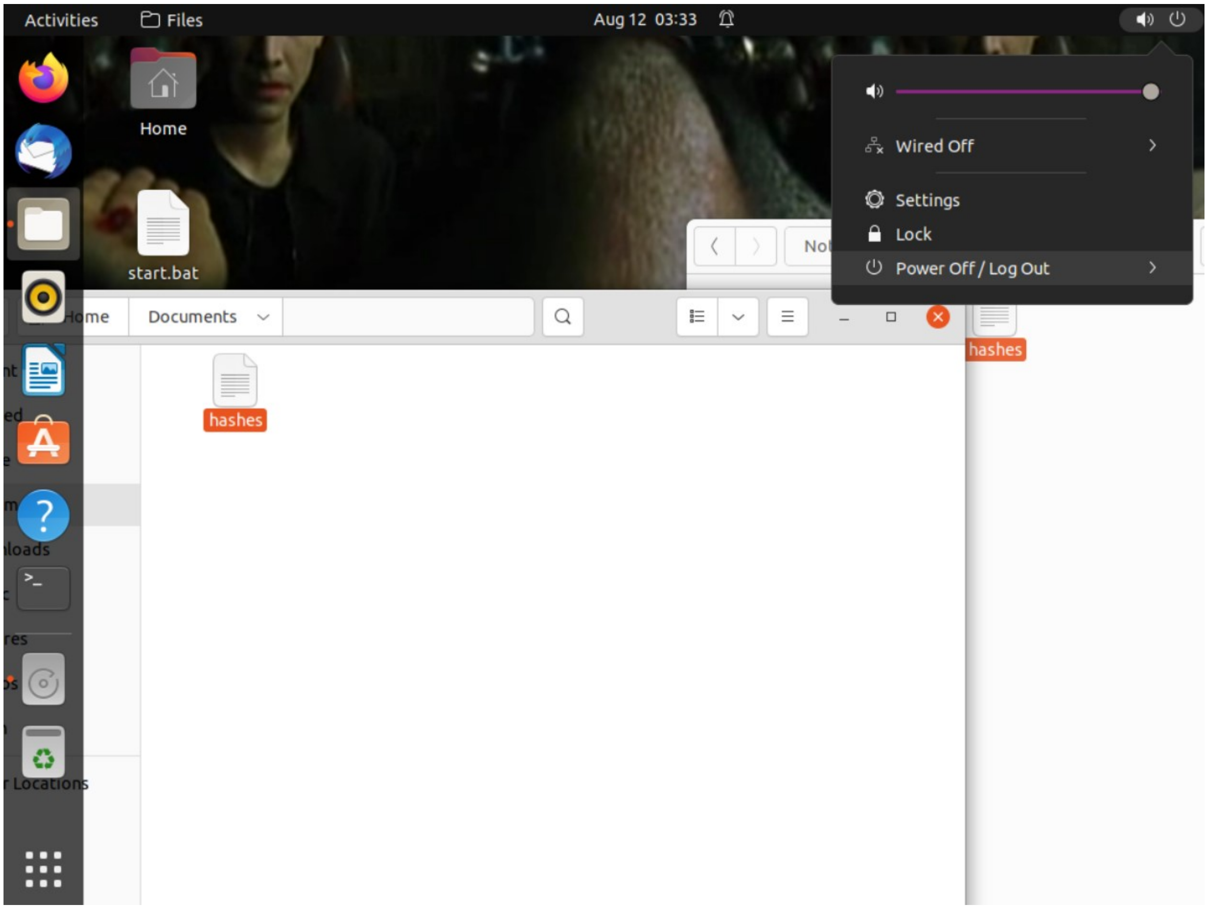
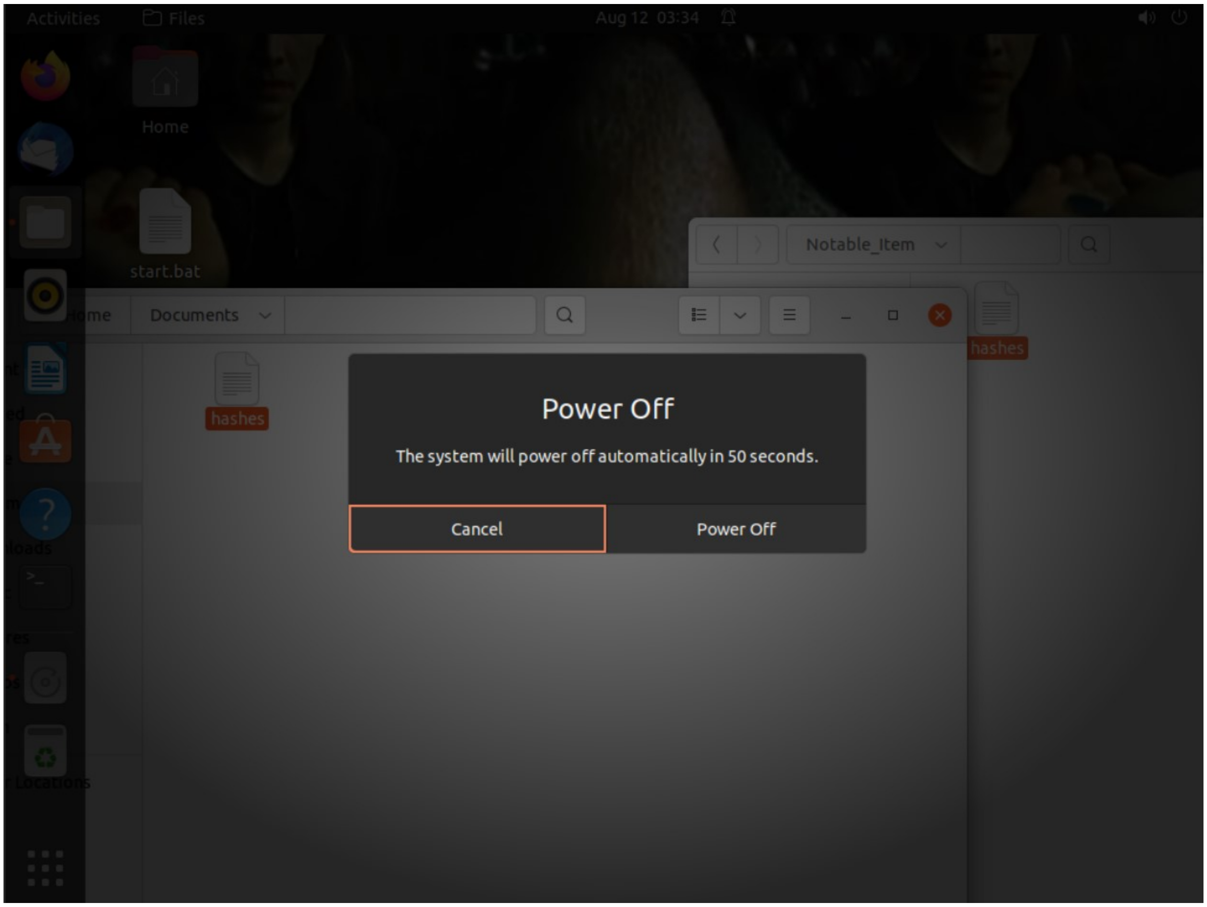


Fig. 7.119: Accessing the power options on Ubuntu 22.10.

Concluding the Process

To safeguard all collected evidence, conclude the procedure by opting for "Power Off", thereby initiating the system's shutdown.



Power Off

The system will power off automatically in 50 seconds.

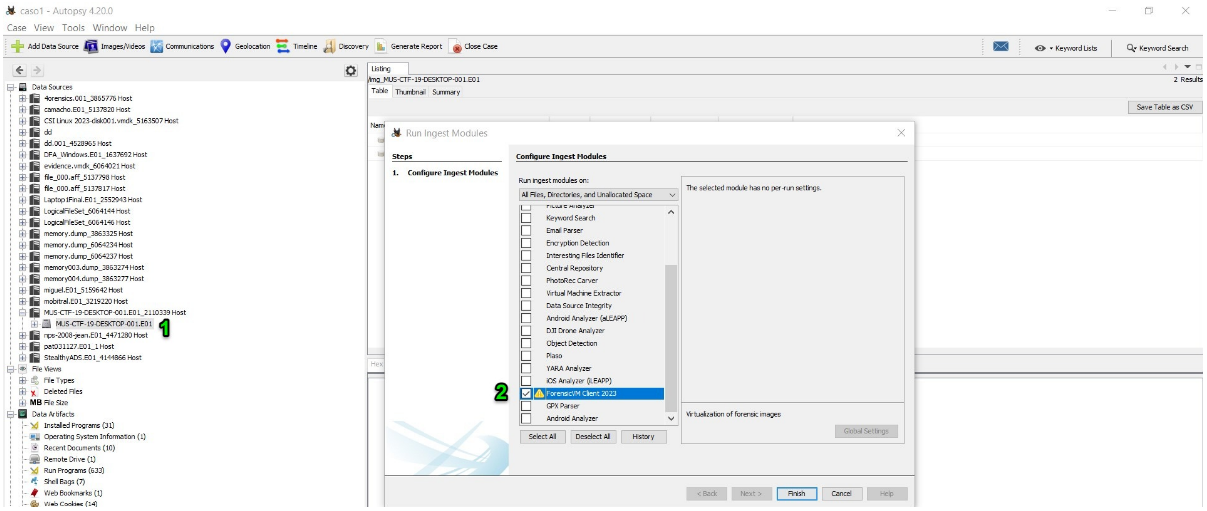
Fig. 7.120: Promptly shutting down the system to ensure evidence safety.

7.11.3 Import Possible Evidence Disk into Autopsy

Autopsy is a digital forensics platform. To import a qcow2 evidence disk, first convert it to vmdk. Follow the guide below:

Run the Autopsy ForensicVM plugin on the intended datasource

1. Begin by launching the Autopsy Case.
2. Execute the Autopsy ForensicVM plugin on the case datasource.



Configure Ingest Modules

Run ingest modules on: All Files, Directories, and Unallocated Space

- □ Picture Analyzer
- □ Keyword Search
- □ Email Parser
- □ Encryption Detection
- □ Interesting Files Identifier
- □ Central Repository
- □ PhotoRec Carver
- □ Virtual Machine Extractor
- □ Data Source Integrity
- □ Android Analyzer (aLEAPP)
- □ DJI Drone Analyzer
- □ Object Detection
- □ Plaso
- □ YARA Analyzer
- □ iOS Analyzer (iLEAPP)
- ☑ ⚠ ForensicVM Client 2023
- □ GPX Parser
- □ Android Analyzer

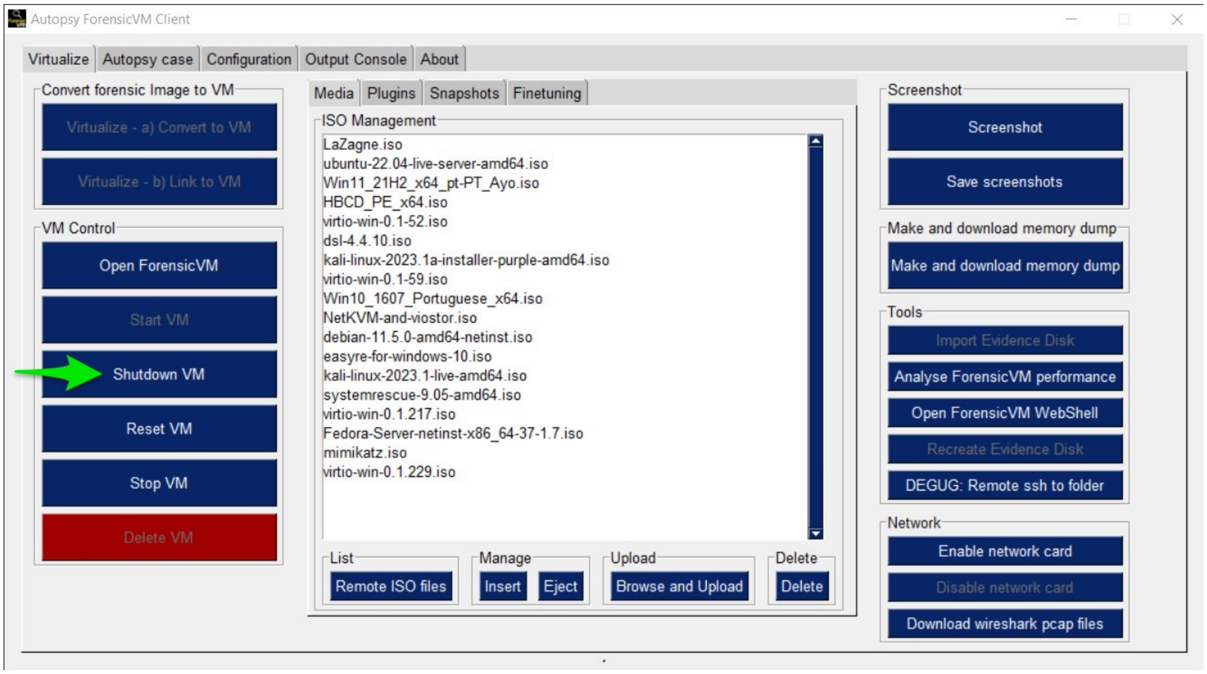
The selected module has no per-run settings.

Virtualization of forensic images

Fig. 7.121: *Autopsy ForensicVM* Plugin Interface

Securely Shutdown the forensicVM

1. Ensure the forensicVM machine is shut down.
2. If not, shut down using the “Shutdown VM” button in the Autopsy ForensicVM Client interface.

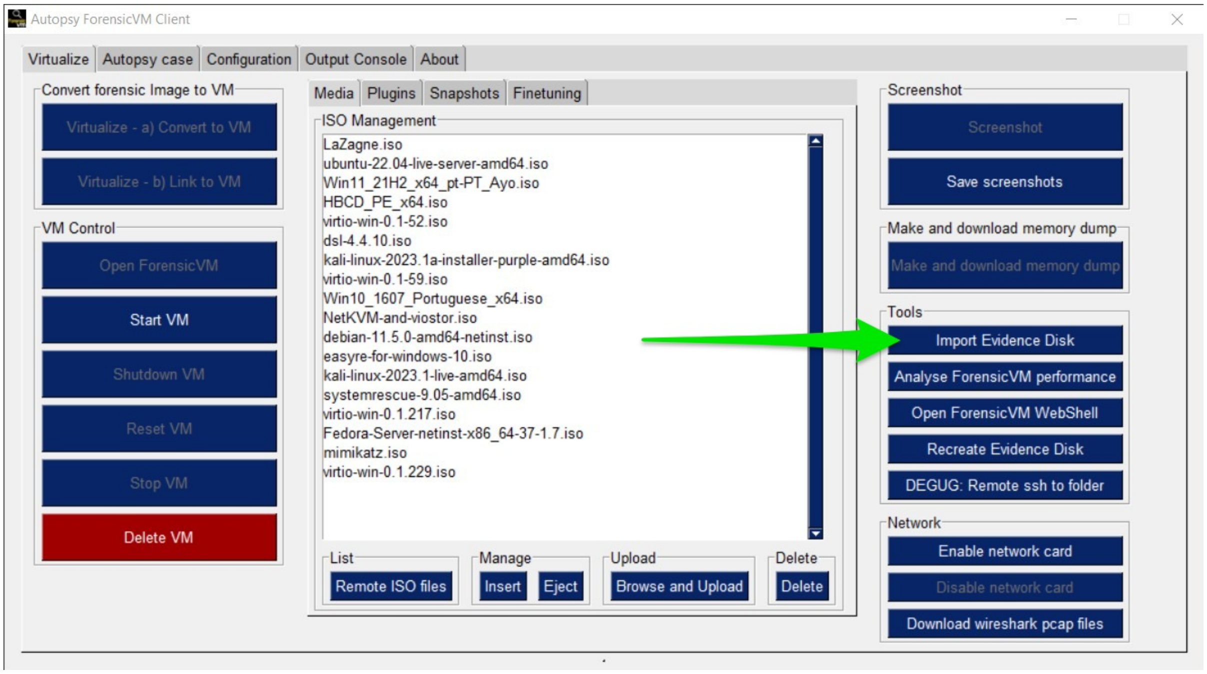


```
LaZagne.iso
ubuntu-22.04-live-server-amd64.iso
Win11_21H2_x64_pt-PT_Ayo.iso
HBCD_PE_x64.iso
virtio-win-0.1-52.iso
dsl-4.4.10.iso
kali-linux-2023.1a-installer-purple-amd64.iso
virtio-win-0.1-59.iso
Win10_1607_Portuguese_x64.iso
NetKVM-and-viostor.iso
debian-11.5.0-amd64-netinst.iso
easyre-for-windows-10.iso
kali-linux-2023.1-live-amd64.iso
systemrescue-9.05-amd64.iso
virtio-win-0.1.217.iso
Fedora-Server-netinst-x86_64-37-1.7.iso
mimikatz.iso
virtio-win-0.1.229.iso
```

Fig. 7.122: *Shutdown VM Interface*

Import evidence disk

Click the “Import Evidence Disk” button.

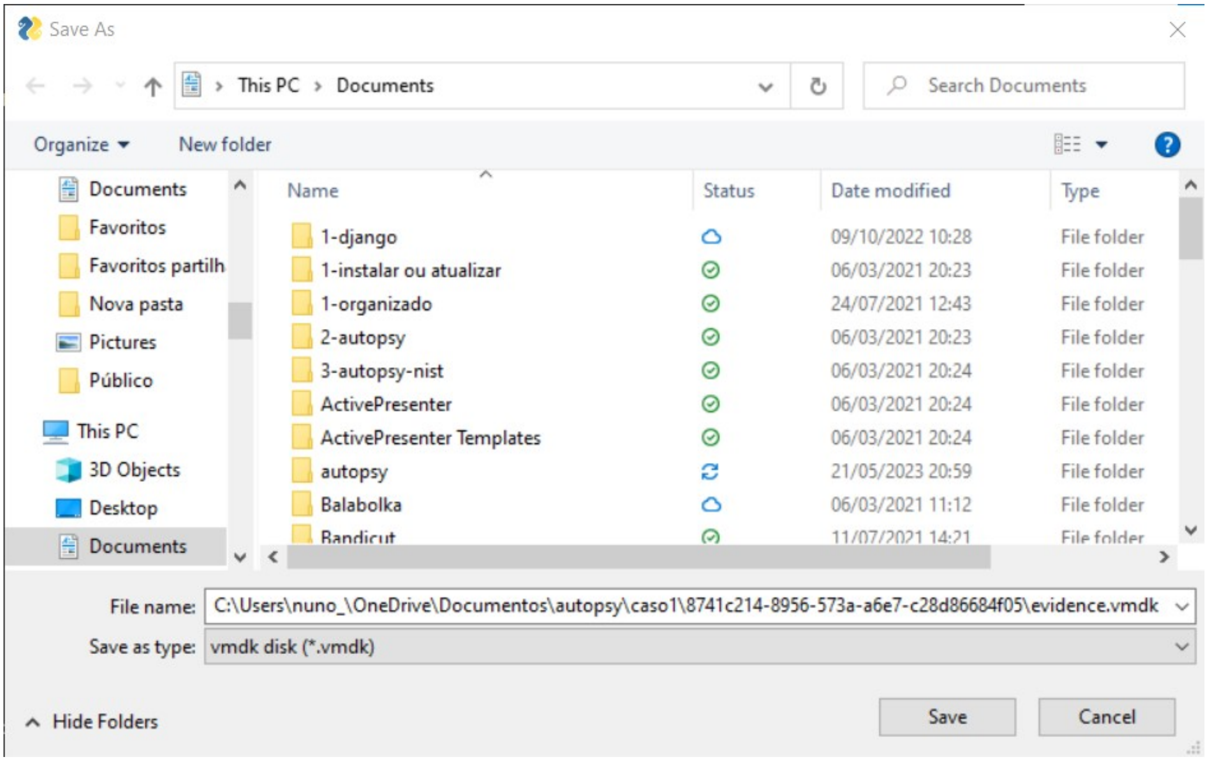


```
LaZagne.iso
ubuntu-22.04-live-server-amd64.iso
Win11_21H2_x64_pt-PT_Ayo.iso
HBCD_PE_x64.iso
virtio-win-0.1-52.iso
dsl-4.4.10.iso
kali-linux-2023.1a-installer-purple-amd64.iso
virtio-win-0.1-59.iso
Win10_1607_Portuguese_x64.iso
NetKVM-and-viostor.iso
debian-11.5.0-amd64-netinst.iso
easyre-for-windows-10.iso
kali-linux-2023.1-live-amd64.iso
systemrescue-9.05-amd64.iso
virtio-win-0.1.217.iso
Fedora-Server-netinst-x86_64-37-1.7.iso
mimikatz.iso
virtio-win-0.1.229.iso
```

Fig. 7.123: *Import* Evidence Disk *Interface*

Save evidence disk to default path

A Windows Explorer "Save As" dialog will appear. Retain the suggested path.



Name	Status	Date modified	Type
1-django		09/10/2022 10:28	File folder
1-instalar ou atualizar	✓	06/03/2021 20:23	File folder
1-organizado	✓	24/07/2021 12:43	File folder
2-autopsy	✓	06/03/2021 20:23	File folder
3-autopsy-nist	✓	06/03/2021 20:24	File folder
ActivePresenter	✓	06/03/2021 20:24	File folder
ActivePresenter Templates	✓	06/03/2021 20:24	File folder
autopsy		21/05/2023 20:59	File folder
Balabolka		06/03/2021 11:12	File folder
Bandicut	✓	11/07/2021 14:21	File folder

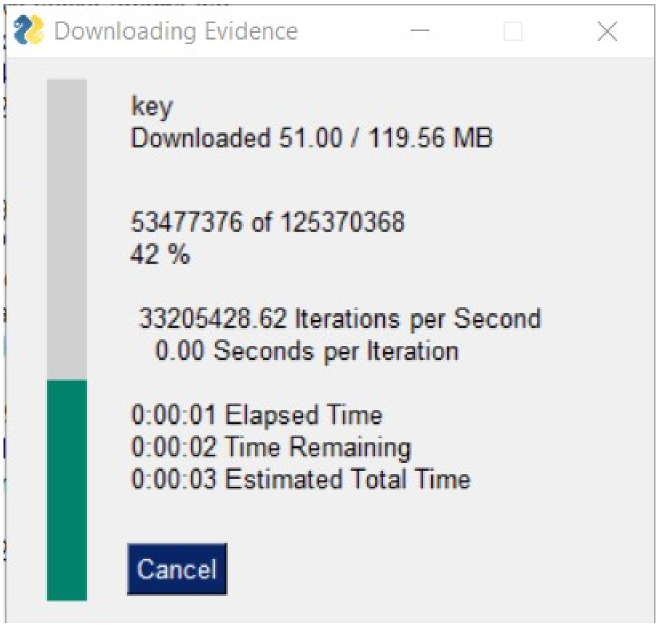
File name: C:\Users\nuno_\OneDrive\Documentos\autopsy\caso1\8741c214-8956-573a-a6e7-c28d86684f05\evidence.vmdk

Save as type: vmdk disk (*.vmdk)

Fig. 7.124: *Save As Dialog*

Monitor the Download Progress

Wait for the evidence disk download to complete.



key
Downloaded 51.00 / 119.56 MB

53477376 of 125370368
42 %

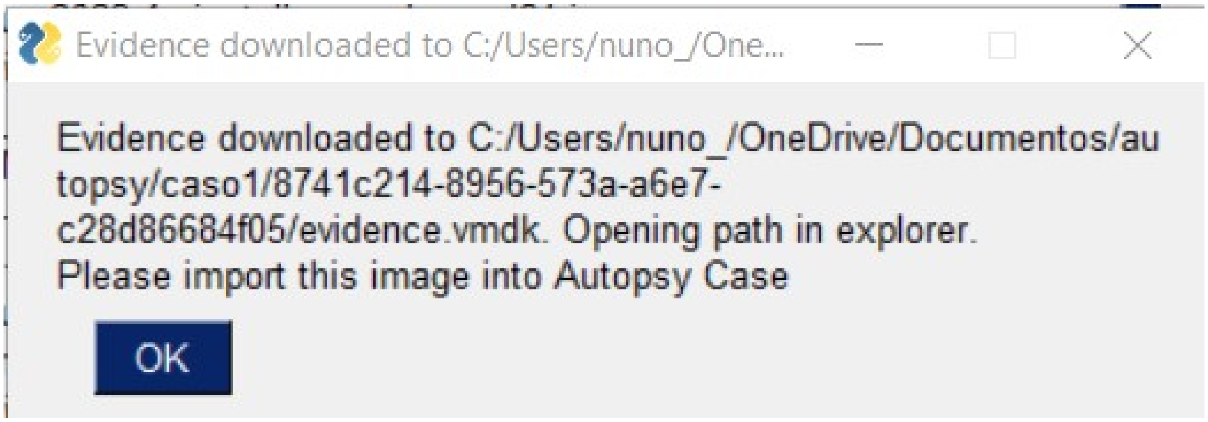
33205428.62 Iterations per Second
0.00 Seconds per Iteration

0:00:01 Elapsed Time
0:00:02 Time Remaining
0:00:03 Estimated Total Time

Fig. 7.125: Download Progress *Bar*

Evidence Disk **Informational Popup**

A notification popup will display the evidence path.

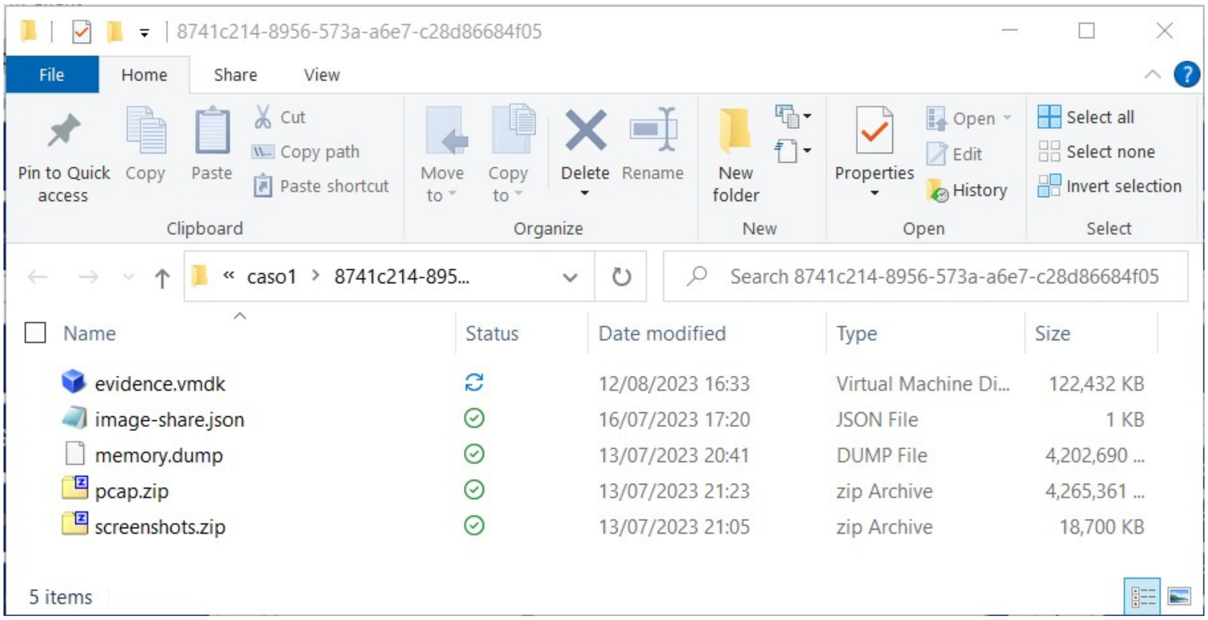


Evidence downloaded to C:/Users/nuno_/OneDrive/Documentos/autopsy/caso1/8741c214-8956-573a-a6e7-c28d86684f05/evidence.vmdk. Opening path in explorer. Please import this image into Autopsy Case

Fig. 7.126: Evidence Disk *Popup Notification*

Locate the Evidence in the Path

Windows Explorer will display the evidence.vmdk path. Copy this path.

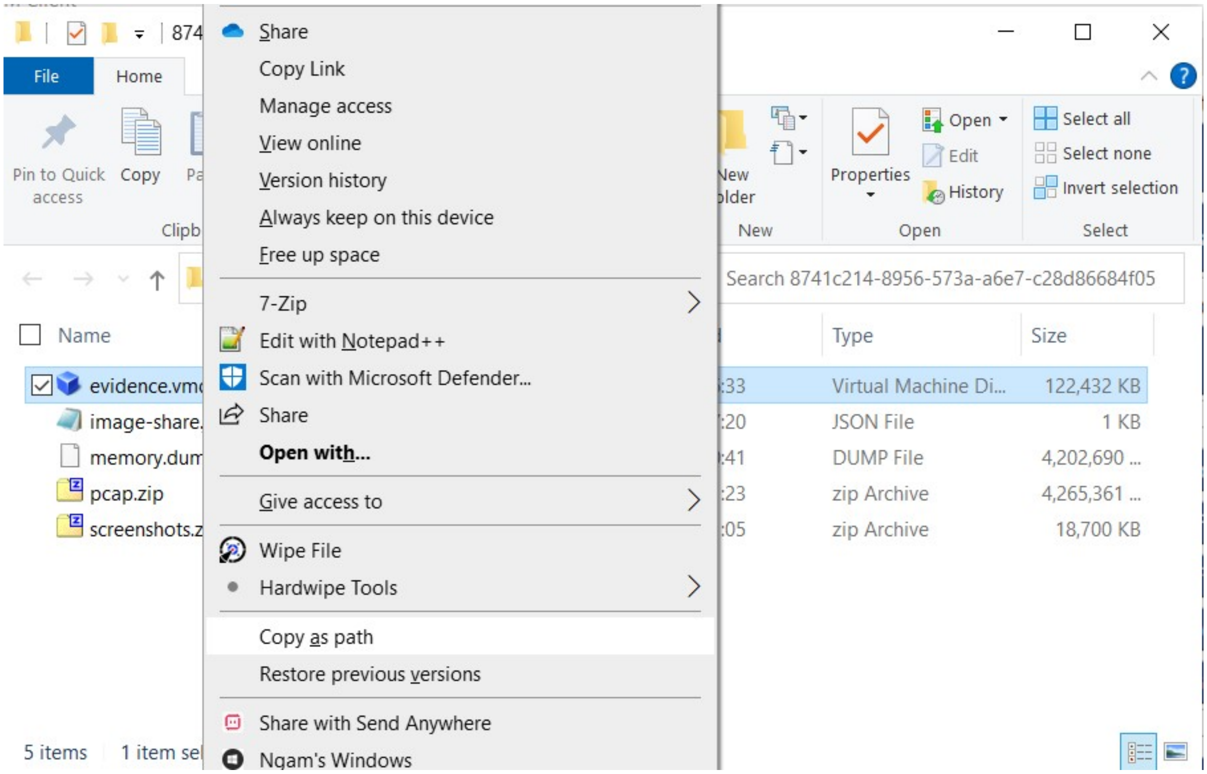


Name	Status	Date modified	Type	Size
evidence.vmdk		12/08/2023 16:33	Virtual Machine Di...	122,432 KB
image-share.json	✓	16/07/2023 17:20	JSON File	1 KB
memory.dump	✓	13/07/2023 20:41	DUMP File	4,202,690 ...
pcap.zip	✓	13/07/2023 21:23	zip Archive	4,265,361 ...
screenshots.zip	✓	13/07/2023 21:05	zip Archive	18,700 KB

Fig. 7.127: *Evidence.*vmdk *in* Windows Explorer

Copy evidence disk path

Hold Shift, right-click on evidence.vmdk, and select “Copy as path”.

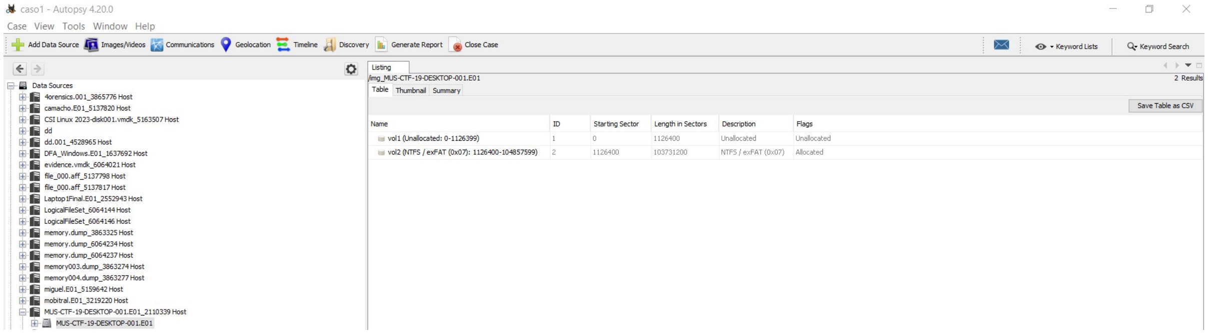


Name		Type	Size
☑ evidence.vm	:33	Virtual Machine Di...	122,432 KB
image-share.	:20	JSON File	1 KB
memory.dum	:41	DUMP File	4,202,690 ...
pcap.zip	:23	zip Archive	4,265,361 ...
screenshots.z	:05	zip Archive	18,700 KB

Fig. 7.128: *Copying evidence.*vmdk *Path*

Integrate a New Data Source in Autopsy Software

Click "Add Data Source" in Autopsy.



- Data Sources
  - 4orensics.001_3865776 Host
  - camacho.E01_5137820 Host
  - CSI Linux 2023-disk001.vmdk_5163507 Host
  - dd
  - dd.001_4528965 Host
  - DFA_Windows.E01_1637692 Host
  - evidence.vmdk_6064021 Host
  - file_000.aff_5137798 Host
  - file_000.aff_5137817 Host
  - Laptop1Final.E01_2552943 Host
  - LogicalFileSet_6064144 Host
  - LogicalFileSet_6064146 Host
  - memory.dump_3863325 Host
  - memory.dump_6064234 Host
  - memory.dump_6064237 Host
  - memory003.dump_3863274 Host
  - memory004.dump_3863277 Host
  - miguel.E01_5159642 Host
  - mobitral.E01_3219220 Host
  - MUS-CTF-19-DESKTOP-001.E01_2110339 Host
    - MUS-CTF-19-DESKTOP-001.E01

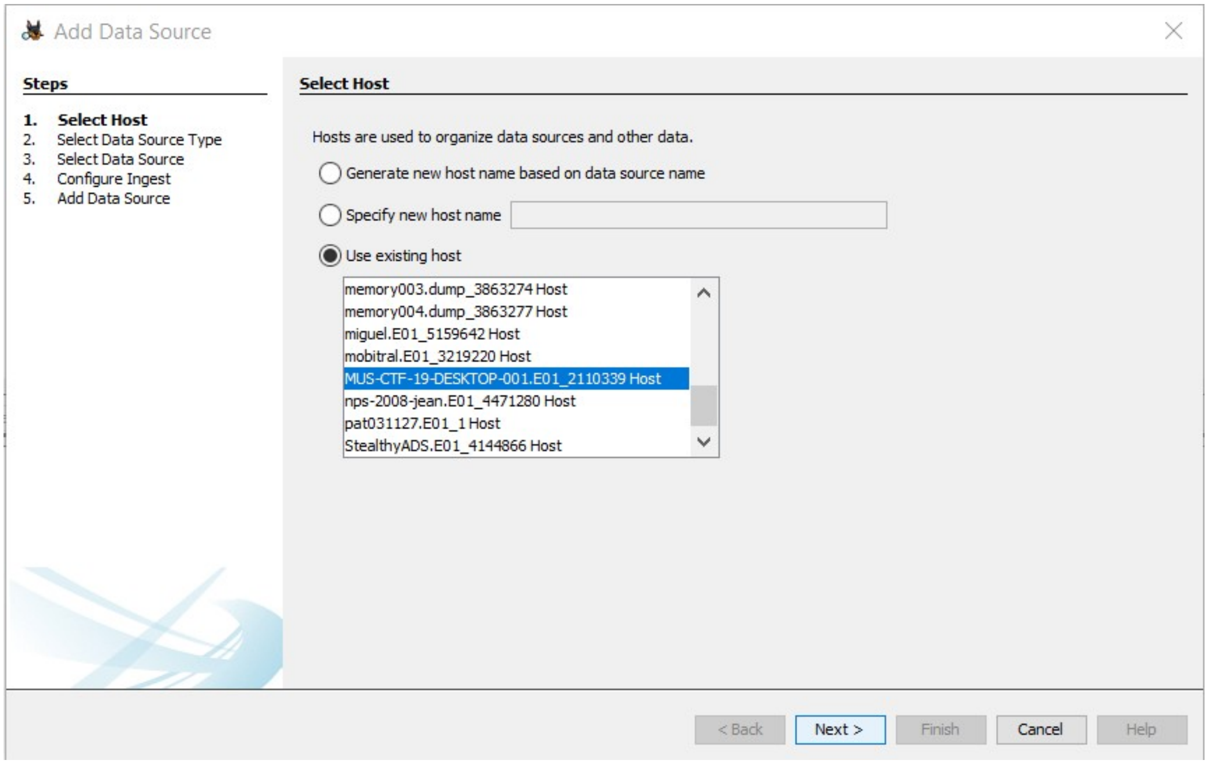
/img_MUS-CTF-19-DESKTOP-001.E01

Name	ID	Starting Sector	Length in Sectors	Description	Flags
vol1 (Unallocated: 0-1126399)	1	0	1126400	Unallocated	Unallocated
vol2 (NTFS / exFAT (0x07): 1126400-104857599)	2	1126400	103731200	NTFS / exFAT (0x07)	Allocated

Fig. 7.129: *Add Data Source Option in Autopsy*

Select the Appropriate Host

Select the same host when importing the evidence disk.



Hosts are used to organize data sources and other data.

○ Generate new host name based on data source name

○ Specify new host name

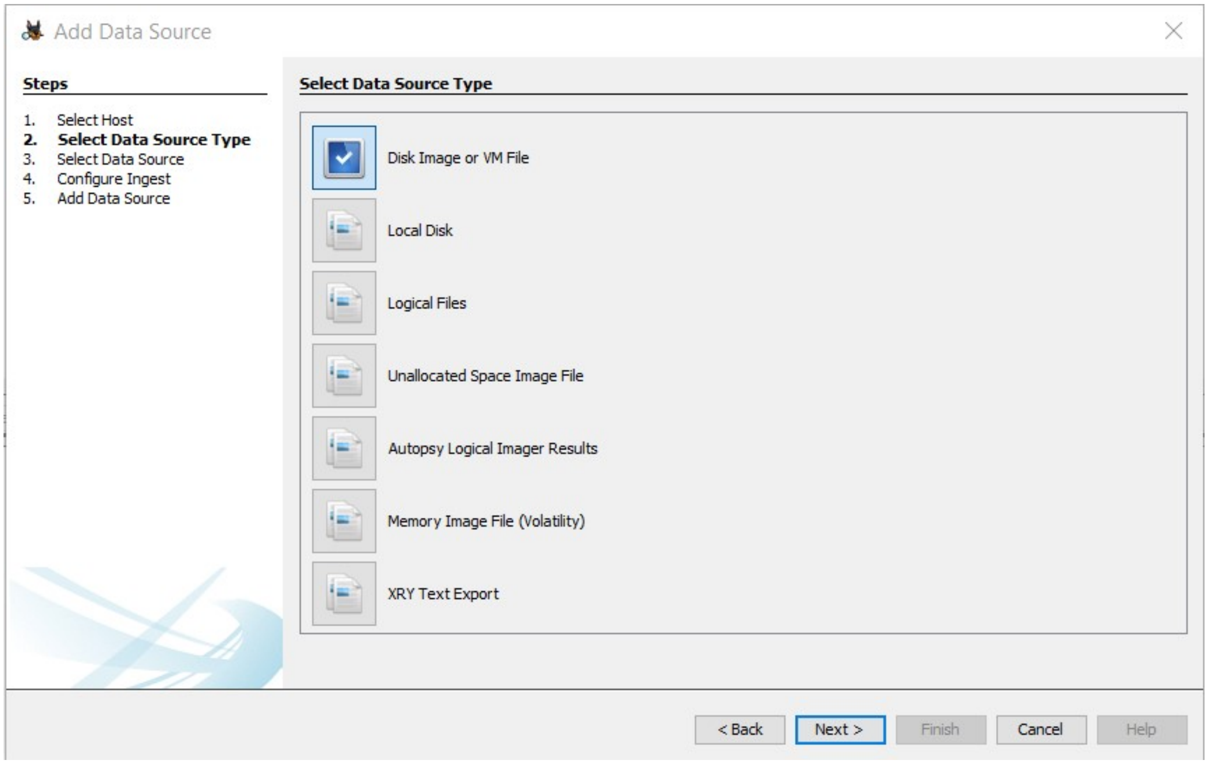
● Use existing host

- memory003.dump_3863274 Host
- memory004.dump_3863277 Host
- miguel.E01_5159642 Host
- mobitral.E01_3219220 Host
- MUS-CTF-19-DESKTOP-001.E01_2110339 Host
- nps-2008-jean.E01_4471280 Host
- pat031127.E01_1 Host
- StealthyADS.E01_4144866 Host

Fig. 7.130: *Selecting Host in Autopsy*

Specify Data Source Type as VM Image

Choose “Disk Image or VM File” as the data source type.



Add Data Source

Steps

1. Select Host
2. **Select Data Source Type**
3. Select Data Source
4. Configure Ingest
5. Add Data Source

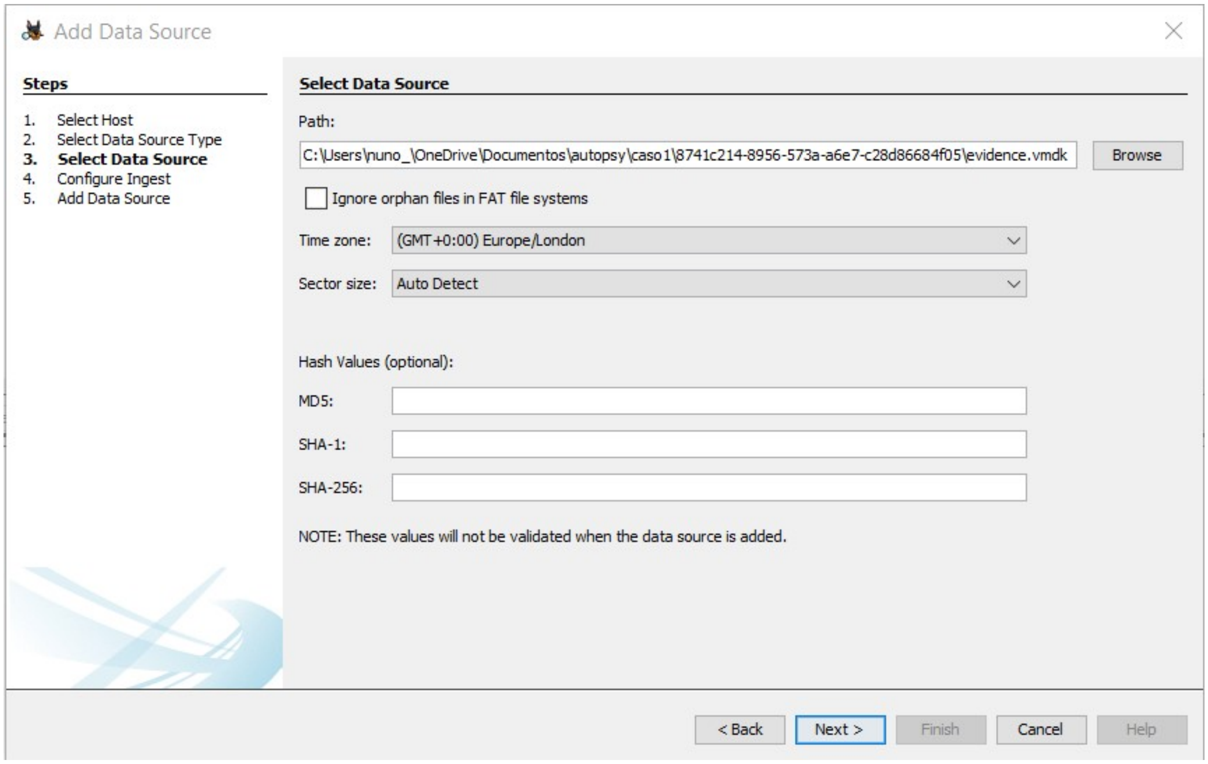
Select Data Source Type

- ☑ Disk Image or VM File
- Local Disk
- Logical Files
- Unallocated Space Image File
- Autopsy Logical Imager Results
- Memory Image File (Volatility)
- XRY Text Export

Fig. 7.131: Selecting Data Source *Type in Autopsy*

Enter the previously copied evidence.vmdk **path**

Paste the evidence.vmdk path and set the “Time zone”.



Path: C:\Users\nuno_\OneDrive\Documentos\autopsy\caso1\8741c214-8956-573a-a6e7-c28d86684f05\evidence.vmdk

□ Ignore orphan files in FAT file systems

Time zone: (GMT+0:00) Europe/London

Sector size: Auto Detect

Hash Values (optional):

MD5:

SHA-1:

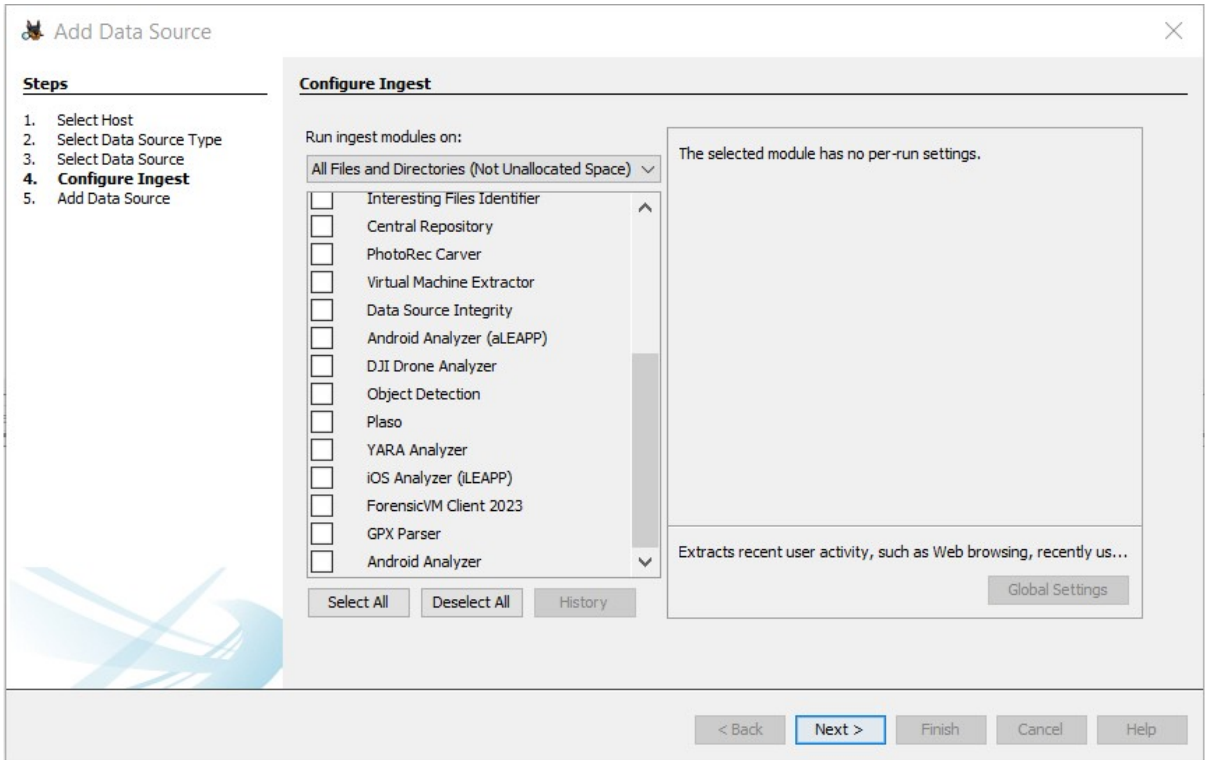
SHA-256:

NOTE: These values will not be validated when the data source is added.

Fig. 7.132: *Inputting evidence.*vmdk *Path in Autopsy*

Deselect All Plugins

Deselect all plugins and click “Next”.



Steps

1. Select Host
2. Select Data Source Type
3. Select Data Source
4. **Configure Ingest**
5. Add Data Source

Configure Ingest

Run ingest modules on:

All Files and Directories (Not Unallocated Space)

- ☐ Interesting Files Identifier
- ☐ Central Repository
- ☐ PhotoRec Carver
- ☐ Virtual Machine Extractor
- ☐ Data Source Integrity
- ☐ Android Analyzer (aLEAPP)
- ☐ DJI Drone Analyzer
- ☐ Object Detection
- ☐ Plaso
- ☐ YARA Analyzer
- ☐ iOS Analyzer (iLEAPP)
- ☐ ForensicVM Client 2023
- ☐ GPX Parser
- ☐ Android Analyzer

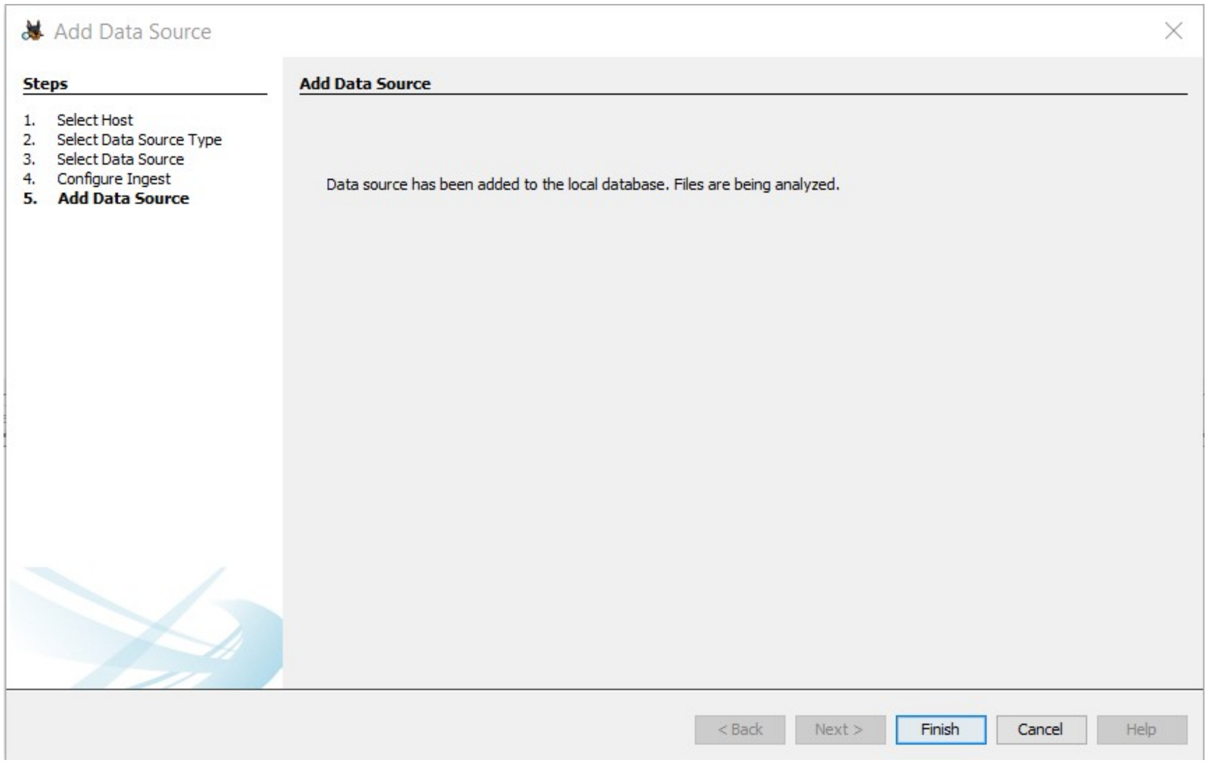
The selected module has no per-run settings.

Extracts recent user activity, such as Web browsing, recently us...

Fig. 7.133: *Deselecting Plugins in Autopsy*

Conclude the Data Source **Addition**

Click “Finish”.

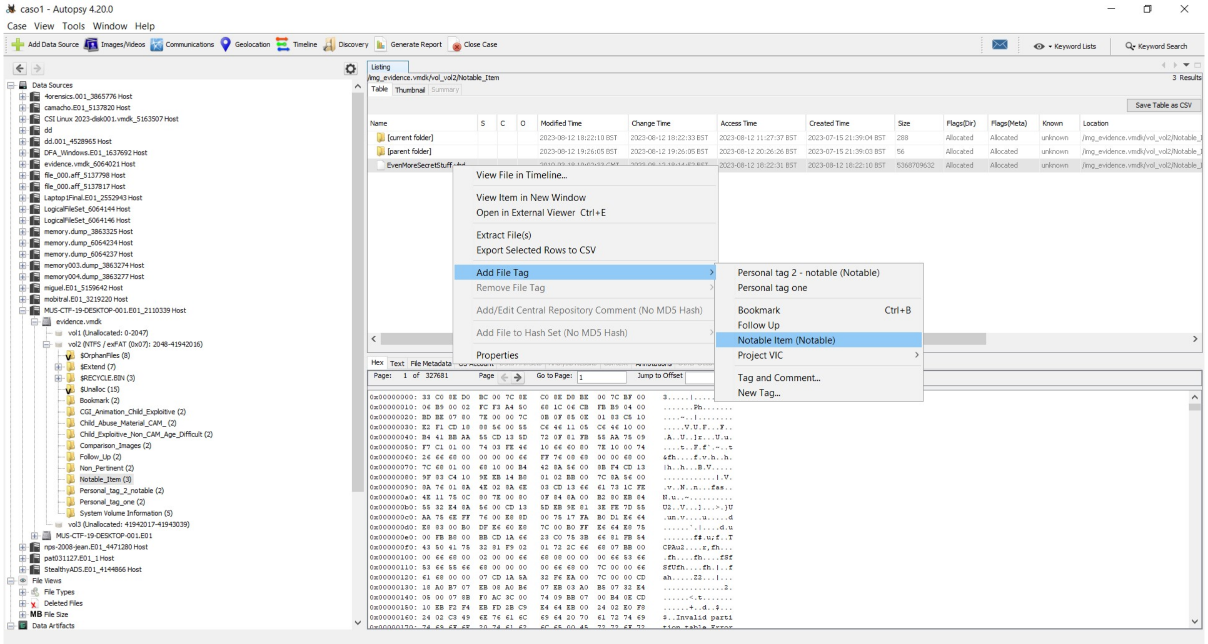


Data source has been added to the local database. Files are being analyzed.

Fig. 7.134: *Finish Button in Autopsy*

Locate and Label Potential Evidence

Navigate to each folder and assign the “Notable Item” tag.


caso1 - Autopsy 4.20.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Data Sources
4orensics.001_3865776 Host
camacho.E01_5137820 Host
CSI Linux 2023-disk001.vmdk_5163507 Host
dd
dd.001_4528965 Host
DFA_Windows.E01_1637692 Host
evidence.vmdk_6064021 Host
file_000.aff_5137798 Host
file_000.aff_5137817 Host
Laptop1Final.E01_2552943 Host
LogicalFileSet_6064144 Host
LogicalFileSet_6064146 Host
memory.dump_3863325 Host
memory.dump_6064234 Host
memory.dump_6064237 Host
memory003.dump_3863274 Host
memory004.dump_3863277 Host
miguel.E01_5159642 Host
mobitral.E01_3219220 Host
MUS-CTF-19-DESKTOP-001.E01_2110339 Host
evidence.vmdk
vol1 (Unallocated: 0-2047)
vol2 (NTFS / exFAT (0x07): 2048-41942016)
$OrphanFiles (8)
$Extend (7)
$RECYCLE.BIN (3)
$Unalloc (15)
Bookmark (2)
CGI_Animation_Child_Exploitive (2)
Child_Abuse_Material_CAM_ (2)
Child_Exploitive_Non_CAM_Age_Difficult (2)
Comparison_Images (2)
Follow_Up (2)
Non_Pertinent (2)
Notable_Item (3)
Personal_tag_2_notable (2)
Personal_tag_one (2)
System Volume Information (5)
vol3 (Unallocated: 41942017-41943039)
MUS-CTF-19-DESKTOP-001.E01
nps-2008-jean.E01_4471280 Host
pat031127.E01_1 Host
StealthyADS.E01_4144866 Host
File Views
File Types
Deleted Files
MB File Size
Data Artifacts
Listing
Table
Thumbnail
Summary
Save Table as CSV
View File in Timeline...
View Item in New Window
Open in External Viewer Ctrl+E
Extract File(s)
Export Selected Rows to CSV
Add File Tag
Remove File Tag
Add/Edit Central Repository Comment (No MD5 Hash)
Add File to Hash Set (No MD5 Hash)
Properties
Personal tag 2 - notable (Notable)
Personal tag one
Bookmark Ctrl+B
Follow Up
Notable Item (Notable)
Project VIC
Tag and Comment...
New Tag...
Hex
Text
File Metadata
Page: 1 of 327681
Page
Go to Page: 1
Jump to Offset

/img_evidence.vmdk/vol_vol2/Notable_Item

3 Results

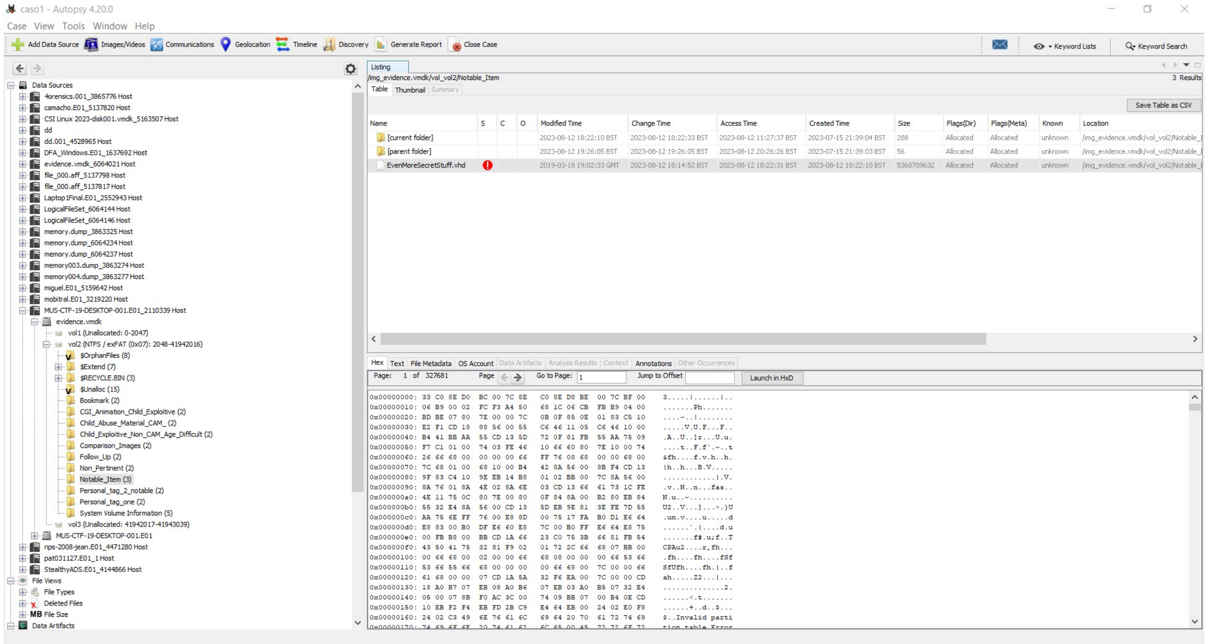
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
[current folder]				2023-08-12 18:22:10 BST	2023-08-12 18:22:33 BST	2023-08-12 11:27:37 BST	2023-07-15 21:39:04 BST	288	Allocated	Allocated	unknown	/img_evidence.vmdk/vol_vol2/Notable_I
[parent folder]				2023-08-12 19:26:05 BST	2023-08-12 19:26:05 BST	2023-08-12 20:26:26 BST	2023-07-15 21:39:03 BST	56	Allocated	Allocated	unknown	/img_evidence.vmdk/vol_vol2/Notable_I
EvenMoreSecretStuff.vhd				[illegible]	[illegible]	2023-08-12 18:22:31 BST	2023-08-12 18:22:10 BST	5368709632	Allocated	Allocated	unknown	/img_evidence.vmdk/vol_vol2/Notable_I

```
0x00000000: 33 C0 8E D0  BC 00 7C 8E   C0 8E D8 BE  00 7C BF 00    3.....|.....
0x00000010: 06 B9 00 02  FC F3 A4 50   68 1C 06 CB  FB B9 04 00    .......Ph.......
0x00000020: BD BE 07 80  7E 00 00 7C   0B 0F 85 0E  01 83 C5 10    ....~..|........
0x00000030: E2 F1 CD 18  88 56 00 55   C6 46 11 05  C6 46 10 00    .....V.U.F...F..
0x00000040: B4 41 BB AA  55 CD 13 5D   72 0F 81 FB  55 AA 75 09    .A..U..]r...U.u.
0x00000050: F7 C1 01 00  74 03 FE 46   10 66 60 80  7E 10 00 74    ....t..F.f`.~..t
0x00000060: 26 66 68 00  00 00 00 66   FF 76 08 68  00 00 68 00    &fh....f.v.h..h.
0x00000070: 7C 68 01 00  68 10 00 B4   42 8A 56 00  8B F4 CD 13    |h..h...B.V.....
0x00000080: 9F 83 C4 10  9E EB 14 B8   01 02 BB 00  7C 8A 56 00    ............|.V.
0x00000090: 8A 76 01 8A  4E 02 8A 6E   03 CD 13 66  61 73 1C FE    .v..N..n...fas..
0x000000a0: 4E 11 75 0C  80 7E 00 80   0F 84 8A 00  B2 80 EB 84    N.u..~..........
0x000000b0: 55 32 E4 8A  56 00 CD 13   5D EB 9E 81  3E FE 7D 55    U2..V...]...>.}U
0x000000c0: AA 75 6E FF  76 00 E8 8D   00 75 17 FA  B0 D1 E6 64    .un.v....u.....d
0x000000d0: E8 83 00 B0  DF E6 60 E8   7C 00 B0 FF  E6 64 E8 75    ......`.|....d.u
0x000000e0: 00 FB B8 00  BB CD 1A 66   23 C0 75 3B  66 81 FB 54    .......f#.u;f..T
0x000000f0: 43 50 41 75  32 81 F9 02   01 72 2C 66  68 07 BB 00    CPAu2....r,fh...
0x00000100: 00 66 68 00  02 00 00 66   68 08 00 00  00 66 53 66    .fh....fh....fSf
0x00000110: 53 66 55 66  68 00 00 00   00 66 68 00  7C 00 00 66    SfUfh....fh.|..f
0x00000120: 61 68 00 00  07 CD 1A 5A   32 F6 EA 00  7C 00 00 CD    ah.....Z2...|...
0x00000130: 18 A0 B7 07  EB 08 A0 B6   07 EB 03 A0  B5 07 32 E4    ..............2.
0x00000140: 05 00 07 8B  F0 AC 3C 00   74 09 BB 07  00 B4 0E CD    ......<.t.......
0x00000150: 10 EB F2 F4  EB FD 2B C9   E4 64 EB 00  24 02 E0 F8    ......+..d..$...
0x00000160: 24 02 C3 49  6E 76 61 6C   69 64 20 70  61 72 74 69    $..Invalid parti
0x00000170: 74 69 6F 6E  20 74 61 62   6C 65 00 45  72 72 6F 72    tion table.Error
```

Fig. 7.135: Tagging *Evidence in Autopsy*

Evidence Successfully Tagged

Tagged evidence will be highlighted.



/img_evidence.vmdk/vol_vol2/Notable_Item

3 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
[current folder]				2023-08-12 18:22:10 BST	2023-08-12 18:22:33 BST	2023-08-12 11:27:37 BST	2023-07-15 21:39:04 BST	288	Allocated	Allocated	unknown	/img_evidence.vmdk/vol_vol2/Notable_I
[parent folder]				2023-08-12 19:26:05 BST	2023-08-12 19:26:05 BST	2023-08-12 20:26:26 BST	2023-07-15 21:39:03 BST	56	Allocated	Allocated	unknown	/img_evidence.vmdk/vol_vol2/Notable_I
EvenMoreSecretStuff.vhd	●			2019-03-18 19:02:33 GMT	2023-08-12 18:14:52 BST	2023-08-12 18:22:31 BST	2023-08-12 18:22:10 BST	5368709632	Allocated	Allocated	unknown	/img_evidence.vmdk/vol_vol2/Notable_I

Fig. 7.136: *Tagged Evidence Display in Autopsy*

7.11.4 Update Evidence Disk Tags

During the course of a forensic investigation, there may be instances when you need to append additional tags. Ensuring that the "possible evidence disk" reflects these changes is crucial. The following steps guide you on making sure the tag folders are created on the evidence disk:

Add a New Tag to Autopsy

1. Navigate to the desired file in Autopsy.
2. Right-click on the file.
3. From the context menu, hover over "Add file tag".
4. Select the last sub-menu option "New tag…".

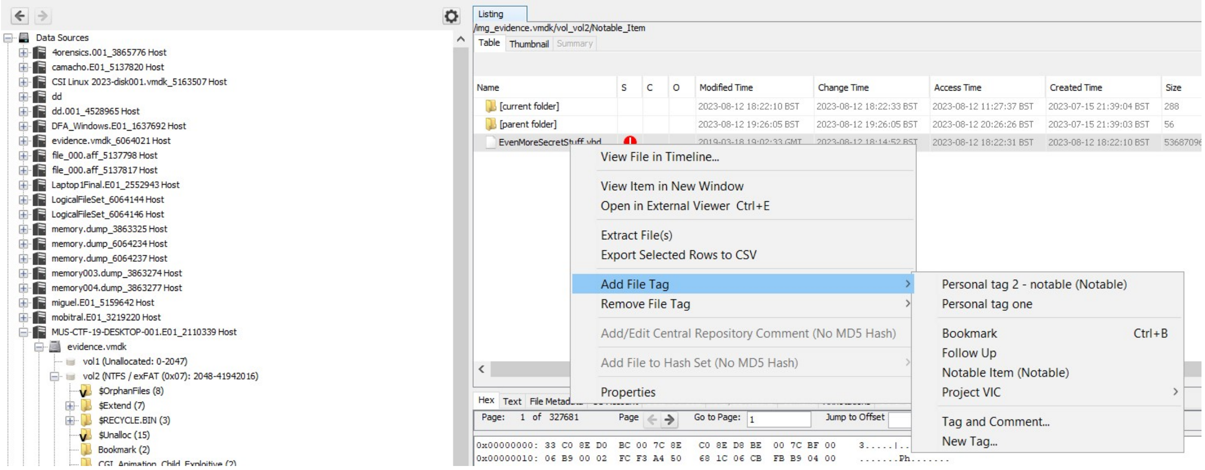
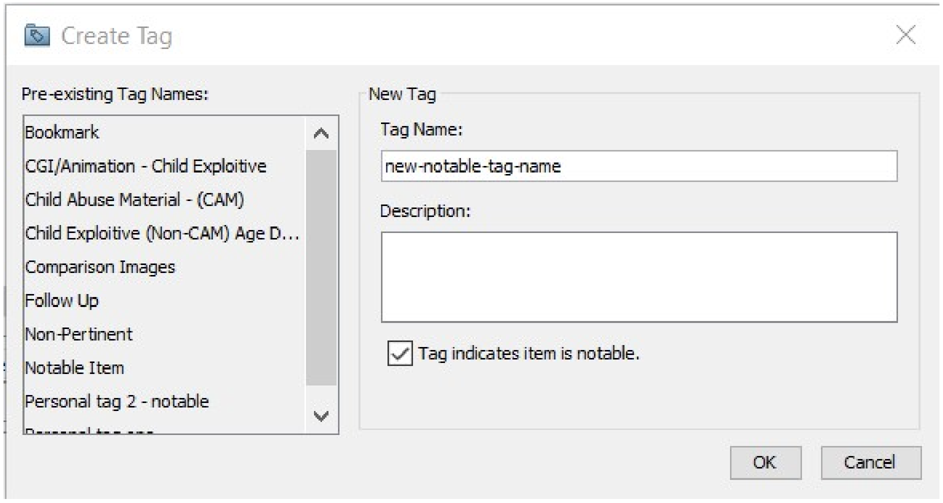


Fig. 7.137: *Adding New Tag in Autopsy*

Define the New Tag Name and Type

1. Input the desired "Tag Name".
2. If the new tag denotes something significant or noteworthy, ensure to check the box labeled "Tag indicates item is notable".



Pre-existing Tag Names:

- Bookmark
- CGI/Animation - Child Exploitive
- Child Abuse Material - (CAM)
- Child Exploitive (Non-CAM) Age D...
- Comparison Images
- Follow Up
- Non-Pertinent
- Notable Item
- Personal tag 2 - notable

New Tag

Tag Name: new-notable-tag-name

Description:

☑ Tag indicates item is notable.

Fig. 7.138: *Defining New Tag Name and Type in Autopsy*

Initiate Ingest Modules

1. Right-click within Autopsy.
2. Select "Run Ingest Modules" from the dropdown menu.

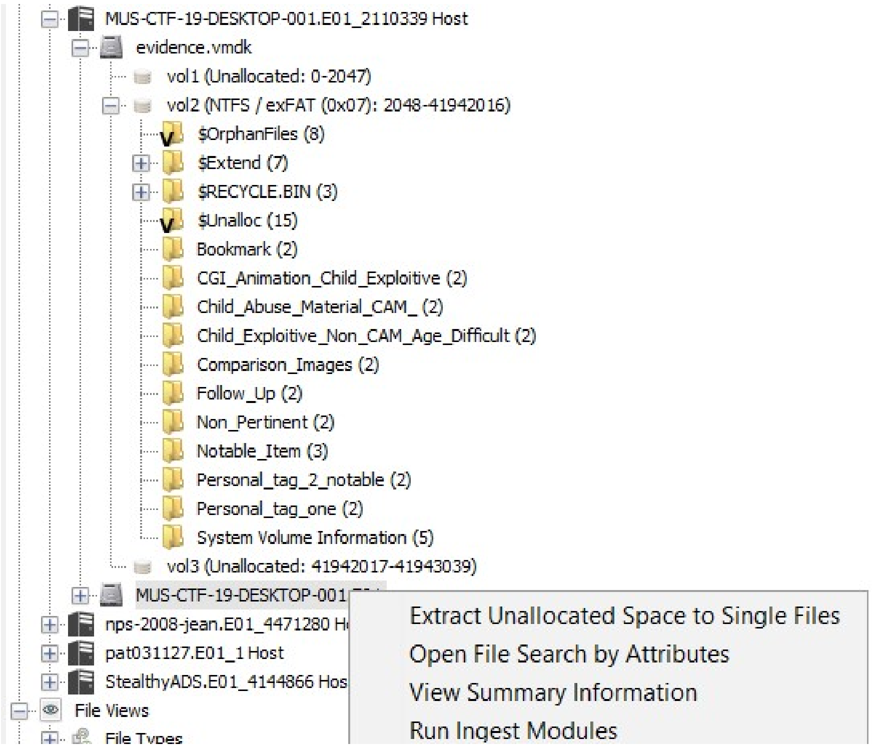
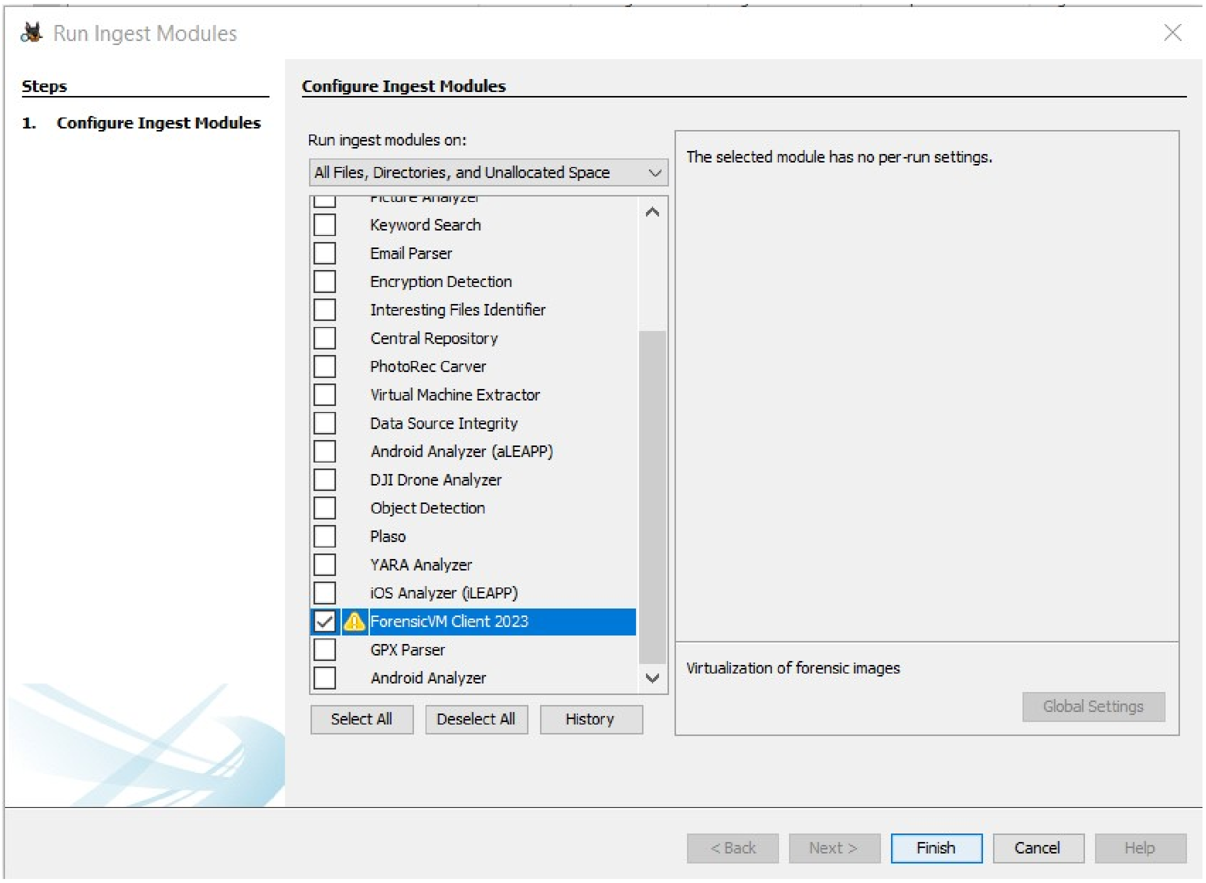

MUS-CTF-19-DESKTOP-001.E01_2110339 Host
evidence.vmdk
vol1 (Unallocated: 0-2047)
vol2 (NTFS / exFAT (0x07): 2048-41942016)
$OrphanFiles (8)
$Extend (7)
$RECYCLE.BIN (3)
$Unalloc (15)
Bookmark (2)
CGI_Animation_Child_Exploitive (2)
Child_Abuse_Material_CAM_ (2)
Child_Exploitive_Non_CAM_Age_Difficult (2)
Comparison_Images (2)
Follow_Up (2)
Non_Pertinent (2)
Notable_Item (3)
Personal_tag_2_notable (2)
Personal_tag_one (2)
System Volume Information (5)
vol3 (Unallocated: 41942017-41943039)
MUS-CTF-19-DESKTOP-001
nps-2008-jean.E01_4471280 H
pat031127.E01_1 Host
StealthyADS.E01_4144866 Hos
File Views
File Types
Extract Unallocated Space to Single Files
Open File Search by Attributes
View Summary Information
Run Ingest Modules

Fig. 7.139: *Running* Ingest Modules *in Autopsy*

Activate the ForensicVM Client Python **Plugin**

1. Deselect all plugins within Autopsy.
2. Specifically select the "ForensicVM Client" plugin.
3. Click on "Finish".



Run Ingest Modules

Steps

1. Configure Ingest Modules

Configure Ingest Modules

Run ingest modules on:

All Files, Directories, and Unallocated Space

□ Picture Analyzer
□ Keyword Search
□ Email Parser
□ Encryption Detection
□ Interesting Files Identifier
□ Central Repository
□ PhotoRec Carver
□ Virtual Machine Extractor
□ Data Source Integrity
□ Android Analyzer (aLEAPP)
□ DJI Drone Analyzer
□ Object Detection
□ Plaso
□ YARA Analyzer
□ iOS Analyzer (iLEAPP)
☑ ⚠ ForensicVM Client 2023
□ GPX Parser
□ Android Analyzer

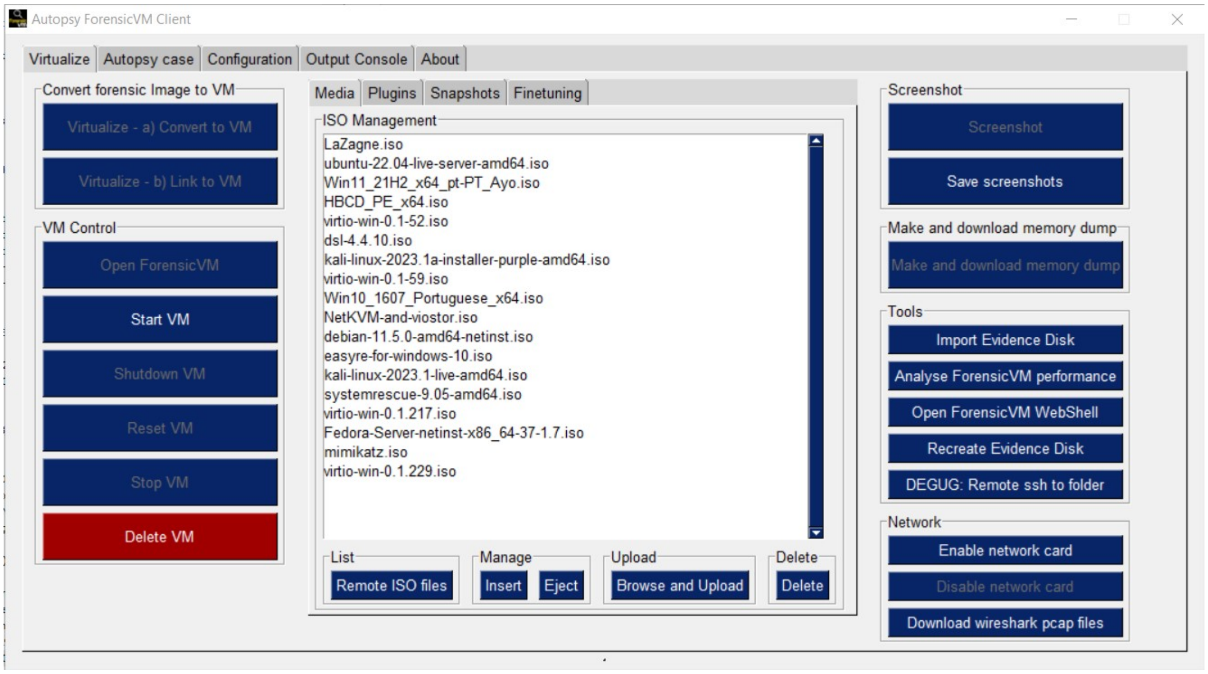
The selected module has no per-run settings.

Virtualization of forensic images

Fig. 7.140: *Selecting the* ForensicVM Client Plugin *in Autopsy*

Boot up the ForensicVM

Start the forensicVM system.



```
LaZagne.iso
ubuntu-22.04-live-server-amd64.iso
Win11_21H2_x64_pt-PT_Ayo.iso
HBCD_PE_x64.iso
virtio-win-0.1-52.iso
dsl-4.4.10.iso
kali-linux-2023.1a-installer-purple-amd64.iso
virtio-win-0.1-59.iso
Win10_1607_Portuguese_x64.iso
NetKVM-and-viostor.iso
debian-11.5.0-amd64-netinst.iso
easyre-for-windows-10.iso
kali-linux-2023.1-live-amd64.iso
systemrescue-9.05-amd64.iso
virtio-win-0.1.217.iso
Fedora-Server-netinst-x86_64-37-1.7.iso
mimikatz.iso
virtio-win-0.1.229.iso
```

Fig. 7.141: *Starting the ForensicVM System*

Access the ForensicVM Interface

Click on “Open ForensicVM”.

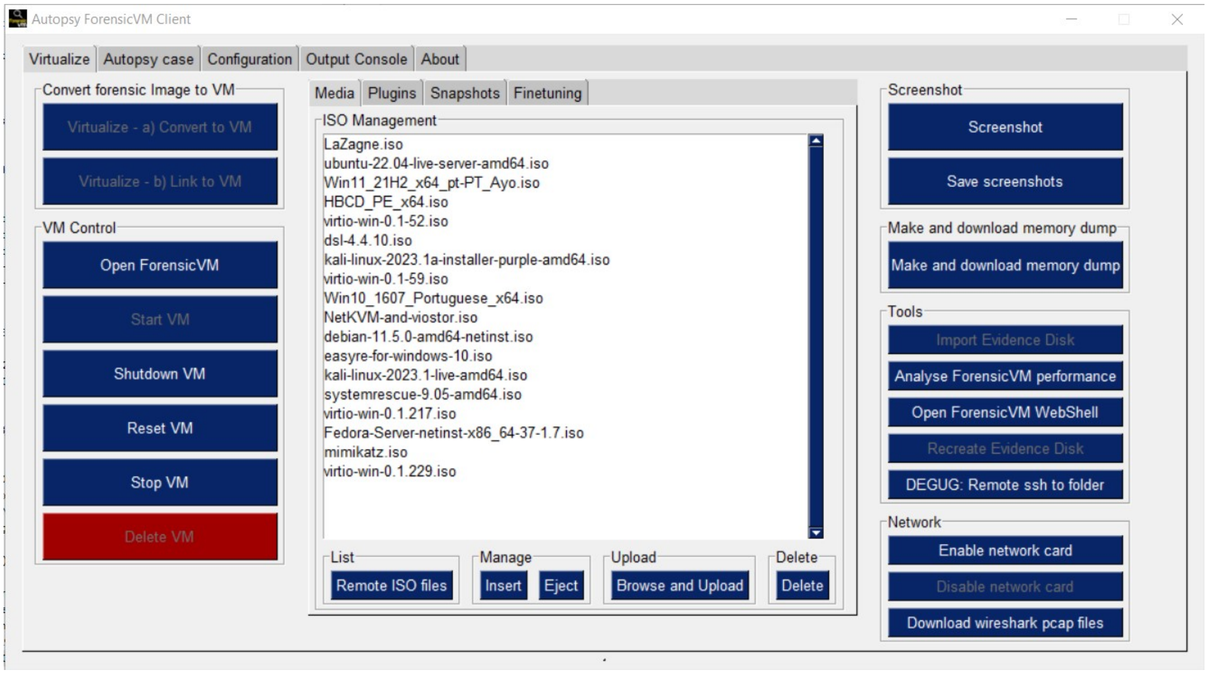
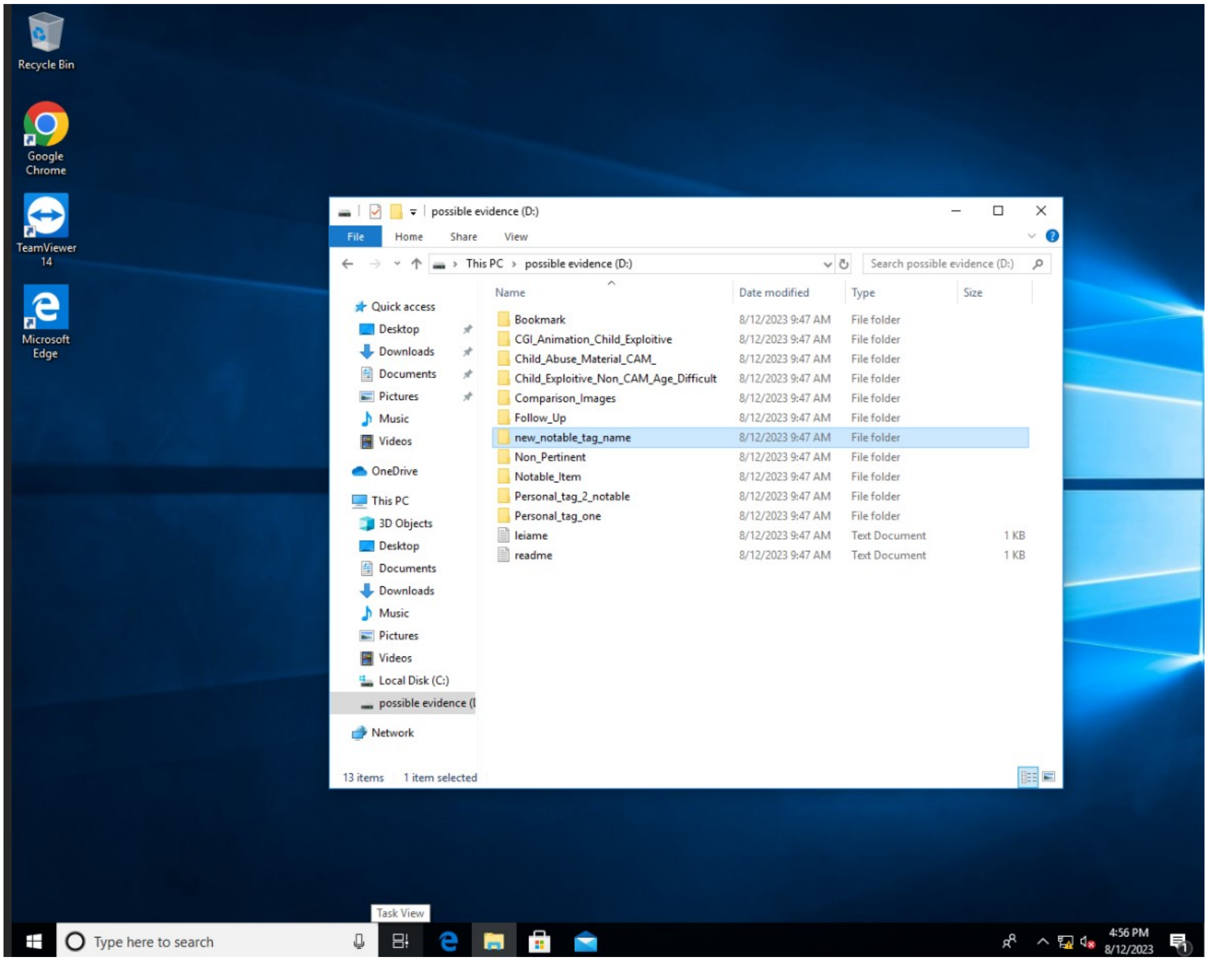


Fig. 7.142: *Accessing the ForensicVM Interface*

Identify the New Folder Tag

Log into the forensicVM and identify the freshly generated tag folder.



Name	Date modified	Type	Size
Bookmark	8/12/2023 9:47 AM	File folder	
CGI_Animation_Child_Exploitive	8/12/2023 9:47 AM	File folder	
Child_Abuse_Material_CAM_	8/12/2023 9:47 AM	File folder	
Child_Exploitive_Non_CAM_Age_Difficult	8/12/2023 9:47 AM	File folder	
Comparison_Images	8/12/2023 9:47 AM	File folder	
Follow_Up	8/12/2023 9:47 AM	File folder	
new_notable_tag_name	8/12/2023 9:47 AM	File folder	
Non_Pertinent	8/12/2023 9:47 AM	File folder	
Notable_Item	8/12/2023 9:47 AM	File folder	
Personal_tag_2_notable	8/12/2023 9:47 AM	File folder	
Personal_tag_one	8/12/2023 9:47 AM	File folder	
leiame	8/12/2023 9:47 AM	Text Document	1 KB
readme	8/12/2023 9:47 AM	Text Document	1 KB

13 items 1 item selected

Fig. 7.143: *Identify the New Folder Tag*

Tip: For users operating on Windows versions later than 8: If the evidence folder is elusive, ensure Windows is not in hibernation instead of being completely shut down. To bypass this, while shutting down the forensicVM, hold down the [Shift] key on your keyboard. This ensures the hibernation file is removed and the drive is primed to receive instructions. You can then retry the procedure.

7.11.5 Recreate Evidence Disk

Danger: Opting for this action will irrevocably erase all data on the evidence disk! Data recovery will not be possible afterward. Prior to initiating this, ensure to follow the guidelines to *Import evidence disk*.

Safely Shut Down Windows

To ensure that the evidence.vmdk disk is unlocked, shut down Windows while pressing and holding the [Shift] key. This action ensures the hibernation file is deleted.

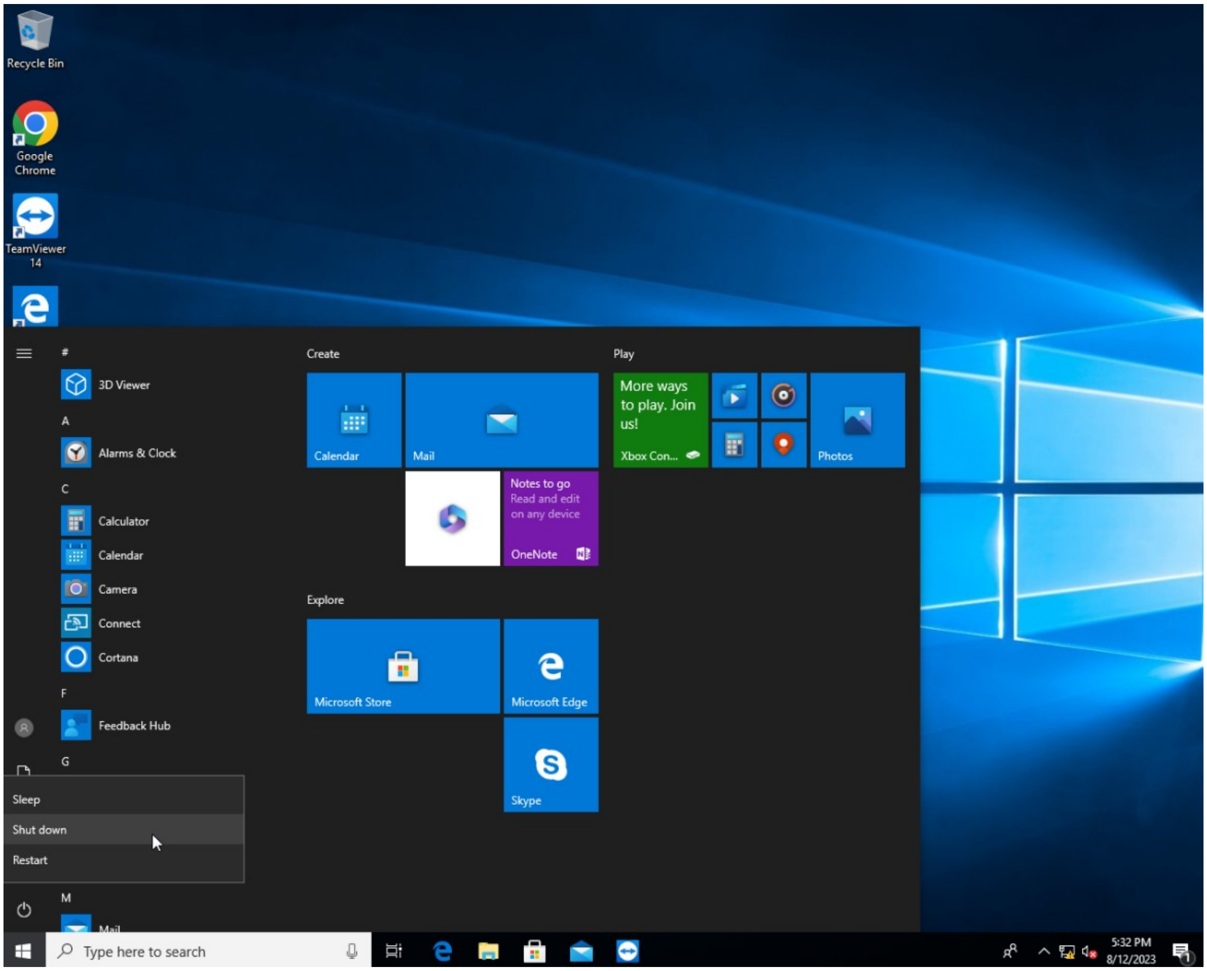


Fig. 7.144: *Safely Shutting Down Windows*

Initiate Evidence Disk **Recreation**

Once the machine is completely shut down, press the “Recreate Evidence Disk” button found on the Autopsy ForensicVM Client Plugin interface.

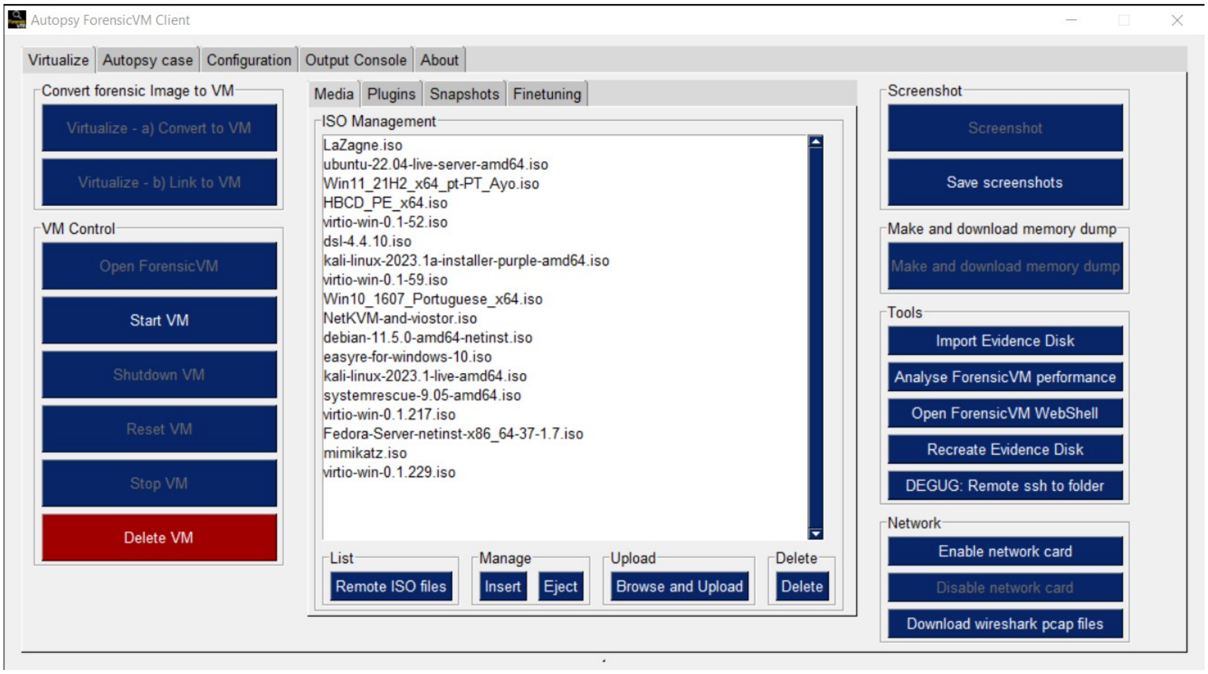
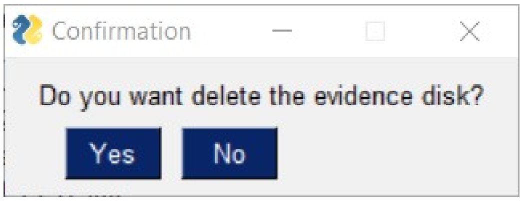


Fig. 7.145: *Recreate* Evidence Disk *Button*

First Confirmation Dialog

Recreating the evidence disk necessitates its deletion—a critical action. A prompt will appear asking for confirmation on this deletion.

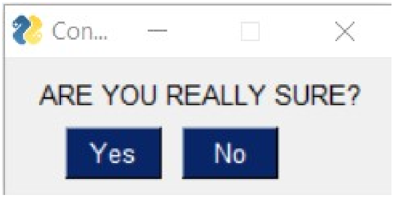


Do you want delete the evidence disk?

Fig. 7.146: *First Confirmation Dialog*

Final Confirmation Message

A subsequent confirmation dialog will be displayed. Click on “YES” only if you are absolutely certain about erasing the current evidence disk.

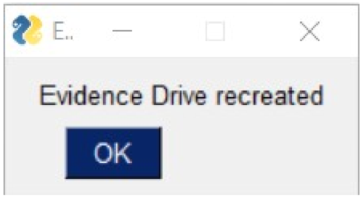


ARE YOU REALLY SURE?

Fig. 7.147: *Final Confirmation Message*

Confirmation of Successful Recreation

Upon successful recreation of the evidence disk, a notification will appear to confirm the action.

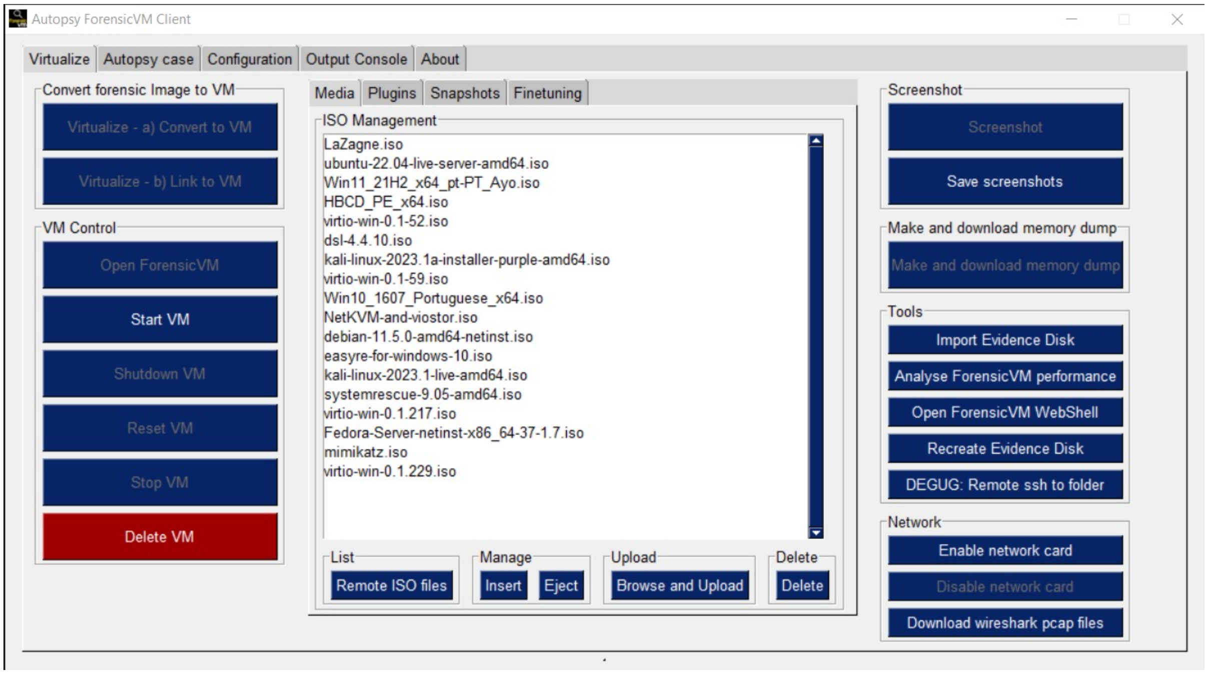


Evidence Drive recreated

Fig. 7.148: *Successful Recreation Notification*

Boot Up the ForensicVM

Proceed to start, access, and log into the forensicVM.

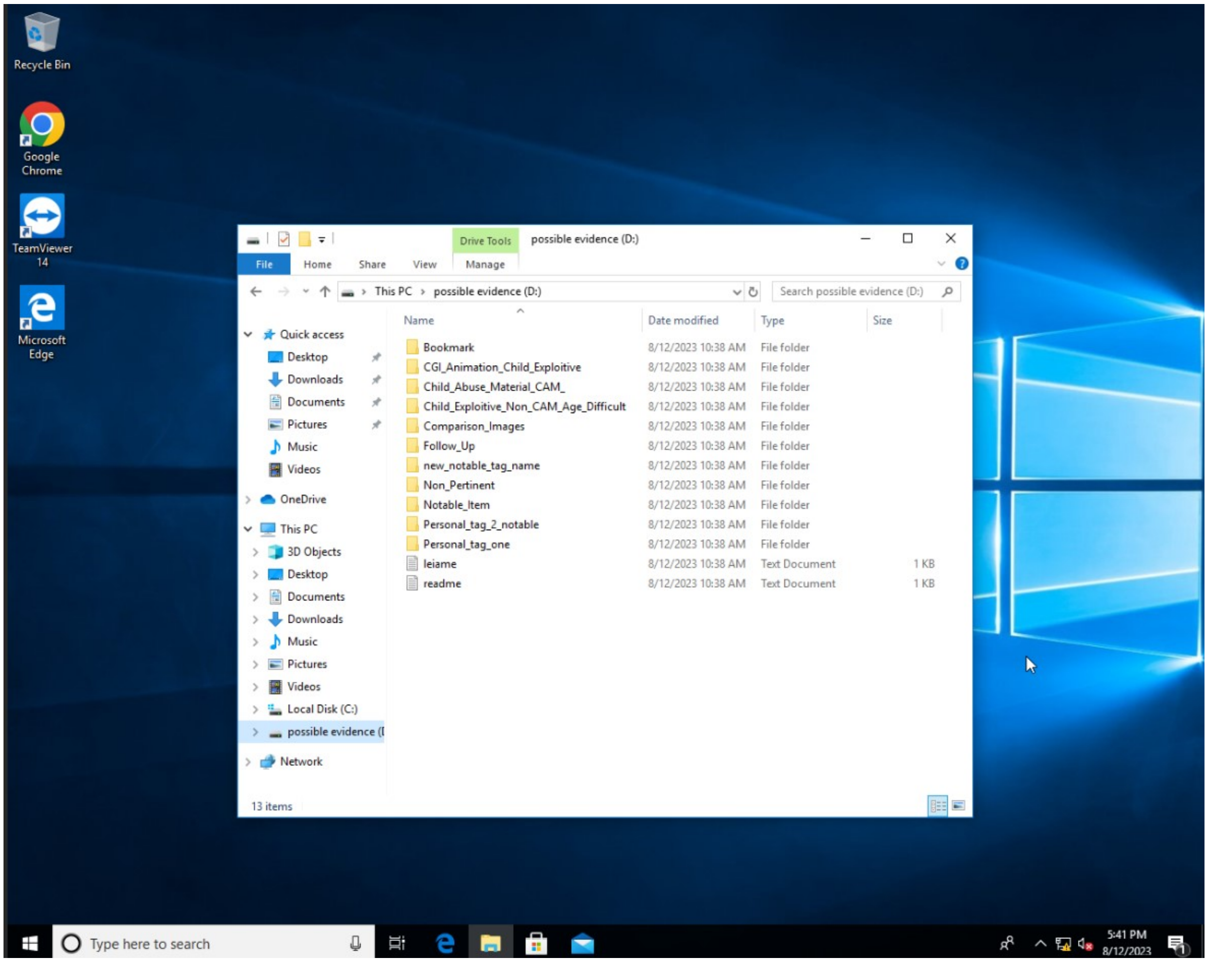


```
LaZagne.iso
ubuntu-22.04-live-server-amd64.iso
Win11_21H2_x64_pt-PT_Ayo.iso
HBCD_PE_x64.iso
virtio-win-0.1-52.iso
dsl-4.4.10.iso
kali-linux-2023.1a-installer-purple-amd64.iso
virtio-win-0.1-59.iso
Win10_1607_Portuguese_x64.iso
NetKVM-and-viostor.iso
debian-11.5.0-amd64-netinst.iso
easyre-for-windows-10.iso
kali-linux-2023.1-live-amd64.iso
systemrescue-9.05-amd64.iso
virtio-win-0.1.217.iso
Fedora-Server-netinst-x86_64-37-1.7.iso
mimikatz.iso
virtio-win-0.1.229.iso
```

Fig. 7.149: *Booting Up the ForensicVM*

Inspect the New Evidence Disk

A freshly recreated evidence disk will be generated with the current Autopsy evidence tags structured as folders. No previously acquired evidence will be included. As a crucial step, remember to *Import evidence disk* before recreating the evidence disk.



Name	Date modified	Type	Size
Bookmark	8/12/2023 10:38 AM	File folder	
CGI_Animation_Child_Exploitive	8/12/2023 10:38 AM	File folder	
Child_Abuse_Material_CAM_	8/12/2023 10:38 AM	File folder	
Child_Exploitive_Non_CAM_Age_Difficult	8/12/2023 10:38 AM	File folder	
Comparison_Images	8/12/2023 10:38 AM	File folder	
Follow_Up	8/12/2023 10:38 AM	File folder	
new_notable_tag_name	8/12/2023 10:38 AM	File folder	
Non_Pertinent	8/12/2023 10:38 AM	File folder	
Notable_Item	8/12/2023 10:38 AM	File folder	
Personal_tag_2_notable	8/12/2023 10:38 AM	File folder	
Personal_tag_one	8/12/2023 10:38 AM	File folder	
leiame	8/12/2023 10:38 AM	Text Document	1 KB
readme	8/12/2023 10:38 AM	Text Document	1 KB

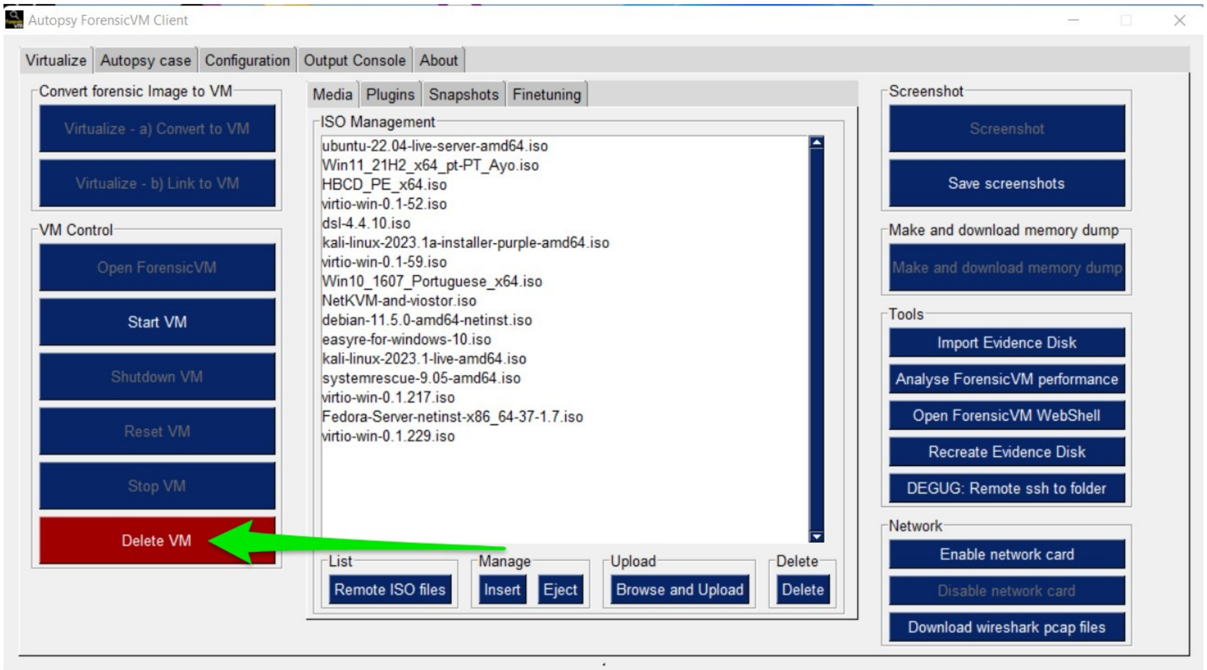
Fig. 7.150: *New Evidence Disk Overview*

7.12 Deletion of ForensicVM at Investigation Conclusion

Once your forensic investigation comes to an end, it's a best practice to eliminate the ForensicVM to free up resources and maintain system hygiene. Here's a detailed guide on how to accomplish this:

1) **Initiate the Deletion Process**

   Begin by clicking the red "Delete VM" button. This action will instigate the process to remove the ForensicVM.

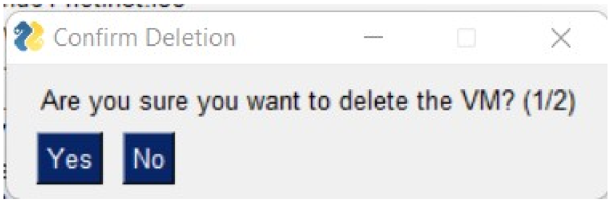


```
ubuntu-22.04-live-server-amd64.iso
Win11_21H2_x64_pt-PT_Ayo.iso
HBCD_PE_x64.iso
virtio-win-0.1-52.iso
dsl-4.4.10.iso
kali-linux-2023.1a-installer-purple-amd64.iso
virtio-win-0.1-59.iso
Win10_1607_Portuguese_x64.iso
NetKVM-and-viostor.iso
debian-11.5.0-amd64-netinst.iso
easyre-for-windows-10.iso
kali-linux-2023.1-live-amd64.iso
systemrescue-9.05-amd64.iso
virtio-win-0.1.217.iso
Fedora-Server-netinst-x86_64-37-1.7.iso
virtio-win-0.1.229.iso
```

Fig. 7.151: Clicking the "Delete VM" button

2) **First Confirmation for Deletion**

   A confirmation popup box will emerge, requesting validation of your decision. Click the "Yes" button to confirm your intention to delete the VM.

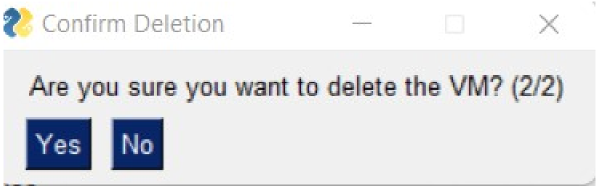


Are you sure you want to delete the VM? (1/2)

Fig. 7.152: First confirmation popup

3) **Second Confirmation for Deletion**

   An additional confirmation popup box will appear to double-check your decision. This is to ensure no inadvertent deletions occur. Once again, click the "Yes" button to proceed.



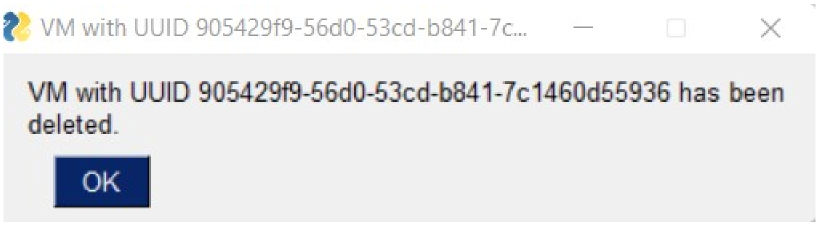
Confirm Deletion

Are you sure you want to delete the VM? (2/2)

Fig. 7.153: Second confirmation popup

4) **Deletion Success Confirmation**

   If the ForensicVM is successfully deleted, a final confirmation popup will appear, mentioning the UUID of the VM that was eradicated. It serves as a record of the recently deleted VM.



VM with UUID 905429f9-56d0-53cd-b841-7c...

VM with UUID 905429f9-56d0-53cd-b841-7c1460d55936 has been deleted.

Fig. 7.154: Deletion success confirmation

7.13 Managing the Network Card to Capture and Analyse Network Traffic

By default, the forensicVM initiates with its network card disabled. This design choice is deliberate, to minimize the potential risks of activating a network card on a possibly compromised virtual forensic machine. Activating such a network card could jeopardize not only your individual computer but the broader network environment.

For many forensic investigations, an active network connection is unnecessary. When evidence is solely contained within a local device, it's recommended to keep the network card deactivated. This approach ensures the machine's safe operation and the security of your enterprise network or domain.

However, in certain situations, there may be a need to activate the network card. For instance, when the forensic virtual machine is deemed safe and requires an internet connection to retrieve cloud-based data—data sourced from cached cloud access credentials like those from OneDrive, Google Drive, Nextcloud, OwnCloud, etc. In such cases, the forensicVM's network card can be enabled. This card has an inbuilt firewall designed to block access to identified local networks while permitting internet connections. Additionally, every time the network card is toggled on or off, all inbound and outbound traffic is recorded. This leads to the creation of a Wireshark pcap file for each activation and deactivation event.

Danger: It's paramount to treat the activation of the network card as a method of last resort. Alternatively, consider using a remotely hosted forensicVM server. The integrity of the firewall isn't foolproof, meaning there's always a risk that malicious software might infiltrate your network. Furthermore, a compromised machine could ping back to an attacker, potentially revealing your external IP address and inadvertently notifying a malicious actor that they are under active investigation!

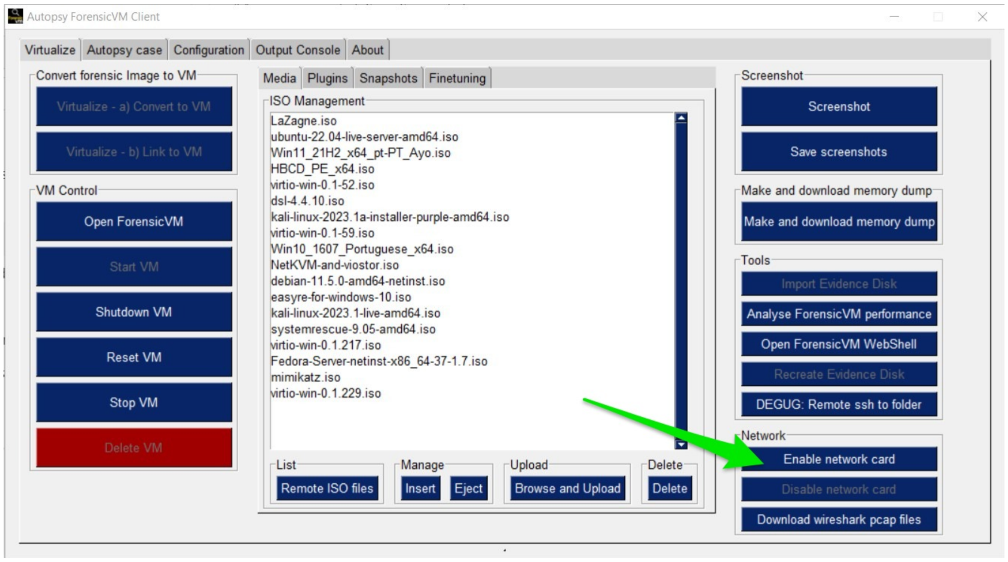
7.13.1 Enable the Network Card

To activate the network card on the forensicVM, there are two methods available. The first method involves using the Autopsy ForensicVM client plugin interface, and the second requires directly interacting with the web screen interface through the network icon.

Enable network card using the Autopsy ForensicVM Client Plugin Interface

Activate Network Card **Button**

1. Start the forensicVM machine.
2. Navigate to the Network Panel within the interface.
3. Look for the “Enable network card” button and click on it.

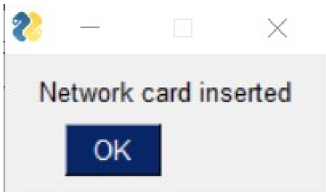


LaZagne.iso
ubuntu-22.04-live-server-amd64.iso
Win11_21H2_x64_pt-PT_Ayo.iso
HBCD_PE_x64.iso
virtio-win-0.1-52.iso
dsl-4.4.10.iso
kali-linux-2023.1a-installer-purple-amd64.iso
virtio-win-0.1-59.iso
Win10_1607_Portuguese_x64.iso
NetKVM-and-viostor.iso
debian-11.5.0-amd64-netinst.iso
easyre-for-windows-10.iso
kali-linux-2023.1-live-amd64.iso
systemrescue-9.05-amd64.iso
virtio-win-0.1.217.iso
Fedora-Server-netinst-x86_64-37-1.7.iso
mimikatz.iso
virtio-win-0.1.229.iso

Fig. 7.155: Enabling the network card through the Autopsy ForensicVM Client interface

Confirmation of Network Card **Activation**

After clicking the button, a popup window will appear to confirm the successful activation of the network card.



Network card inserted

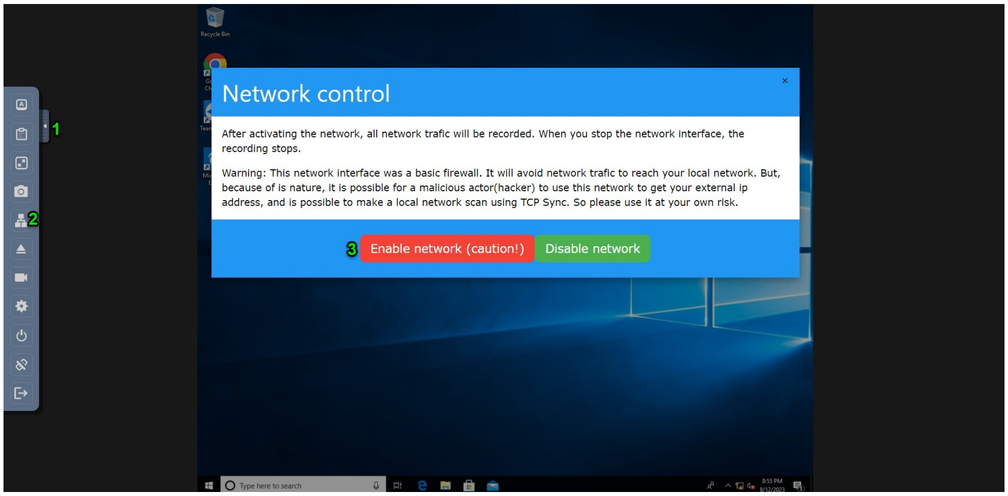
Fig. 7.156: Confirmation popup for network card activation

Enable Network Using the Web Screen Interface

Activating the network card can also be achieved via the Web Screen Interface. This method allows users to manage network settings without diving into the main software interface. Here's how to enable the network card using the Web Screen Interface:

Activating Network through Web Screen Interface **Steps**

1. Initiate the **Panel Opener (1)** to reveal the available options.
2. Locate and click on the **network icon (2)** to access network settings.
3. Identify and click the red button labeled **Enable network (caution) (3)** to activate the network card.



Network control

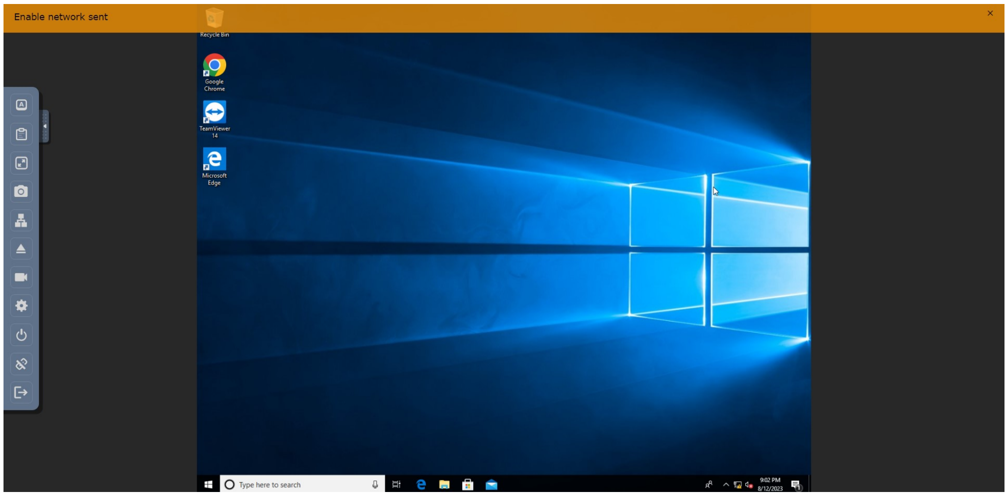
After activating the network, all network trafic will be recorded. When you stop the network interface, the recording stops.

Warning: This network interface was a basic firewall. It will avoid network trafic to reach your local network. But, because of is nature, it is possible for a malicious actor(hacker) to use this network to get your external ip address, and is possible to make a local network scan using TCP Sync. So please use it at your own risk.

Fig. 7.157: Steps to activate the network through the Web Screen Interface

Acknowledgement of Successful Activation

Once the network card is activated, an orange notification will pop up at the top of the screen. This message serves to confirm that the network card has been successfully activated.



Enable network sent

Fig. 7.158: Notification confirming successful activation of the network card

Reseting the Operating System Network Card

From time to time, due to various reasons such as IP conflicts, connectivity issues, or configuration errors, it might be necessary to reset the network card. Resetting can re-establish a proper connection and can often solve common networking problems. Below are methods to reset the network card in Windows and Linux.

Windows 10

In Windows 10, the Network Troubleshooter can assist in diagnosing and resolving common network-related problems.

1. Navigate to the system tray located in the bottom right corner of your screen.
2. Right-click the network icon.
3. From the context menu, select the "Troubleshoot problems" option. The Network Troubleshooter will now start, and it will attempt to diagnose and resolve any detected issues.

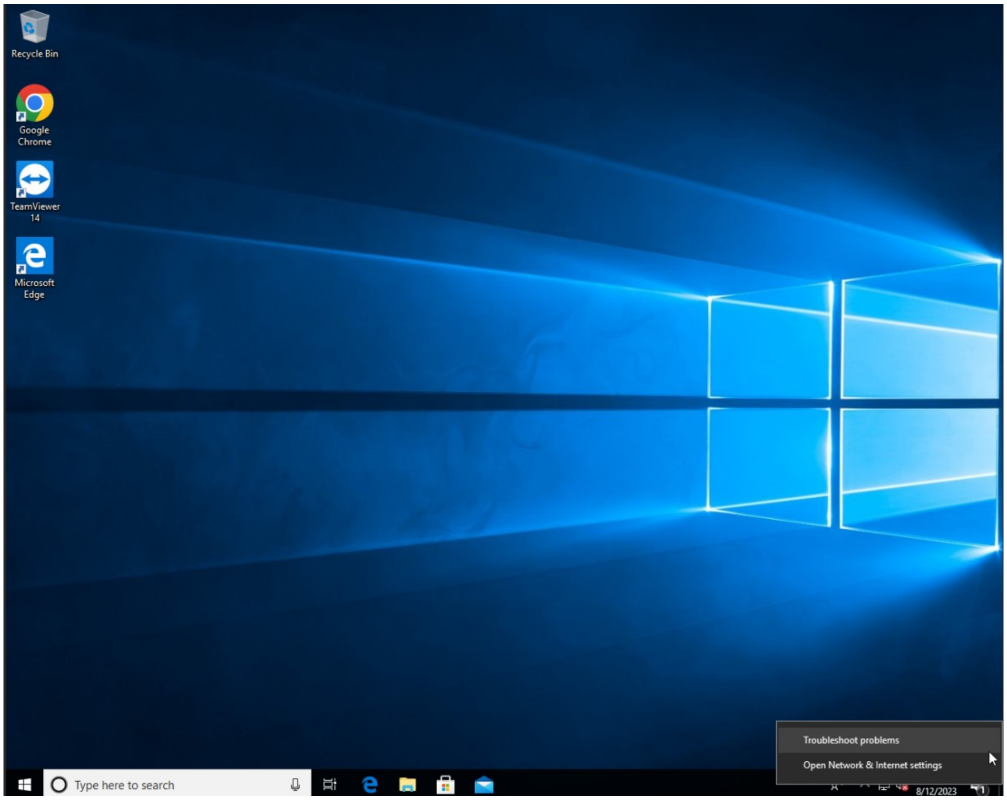


Fig. 7.159: Using the Network Troubleshooter in Windows 10

Other Windows Versions

In older versions of Windows, the process might slightly differ. Usually, there's a network troubleshooting tool available but its location or name may vary. Check under "Network and Sharing Center" or within Control Panel for related options.

Linux

In Linux, depending on the distribution and the desktop environment, you can manage the network card through the graphical interface. However, for a more universal method:

1. Open a terminal.
2. To disable the network card (assuming it's named *eth0*), type:

```
sudo ifconfig eth0 down
```

3. To enable it again, type:

```
sudo ifconfig eth0 up
```

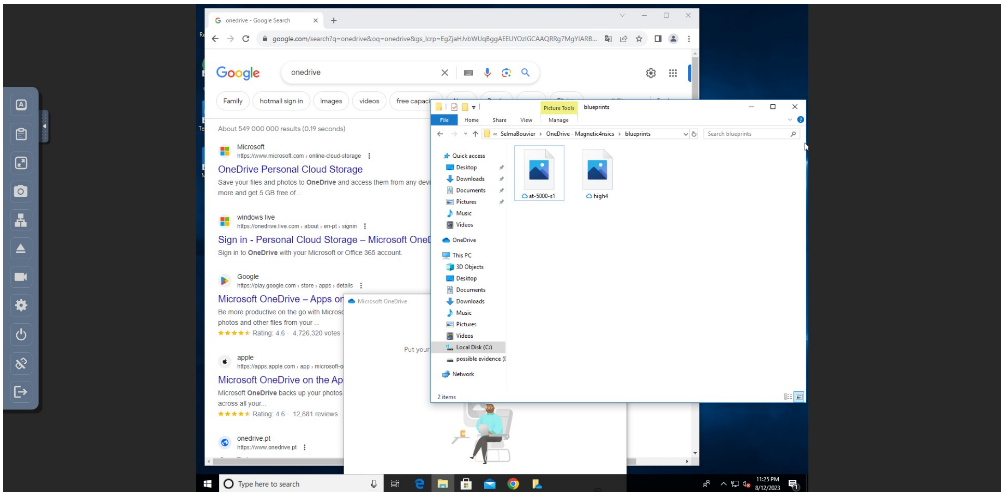
> **Danger:** Always proceed with caution when enabling the network, especially on systems that are meant for forensic investigations or are potentially compromised. It's vital to ensure systems and network security and to be aware of the risks involved.

7.13.2 Collect Network Evidence

Enabling the network card is often crucial for forensic investigations, especially when collecting evidence from cloud services. This is particularly relevant when users have not logged out from a service or when session cookies remain in the browser. Such scenarios allow forensic investigators to trace digital breadcrumbs and gather additional evidence that may be inaccessible from offline forensic images. Below are two illustrative examples:

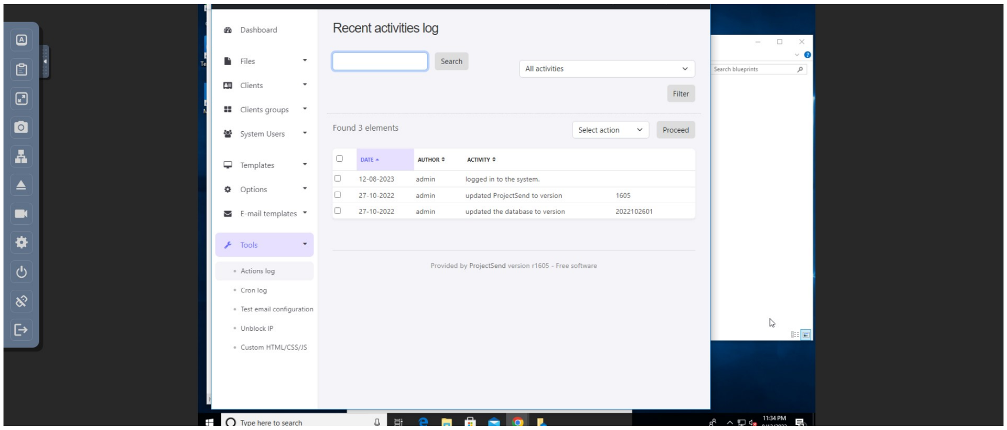
Gathering Data from Cloud Services **- OneDrive Example**

The following figure demonstrates data extraction from OneDrive, a popular online cloud service.



Gathering Data from Cloud Services **- Online Storage Example**

In this next example, an online file storage platform is accessed using cached credentials:



Recent activities log

Found 3 elements

□	DATE	AUTHOR	ACTIVITY	
□	12-08-2023	admin	logged in to the system.	
□	27-10-2022	admin	updated ProjectSend to version	1605
□	27-10-2022	admin	updated the database to version	2022102601

Provided by ProjectSend version r1605 - Free software

7.13.3 Disable the Network Card

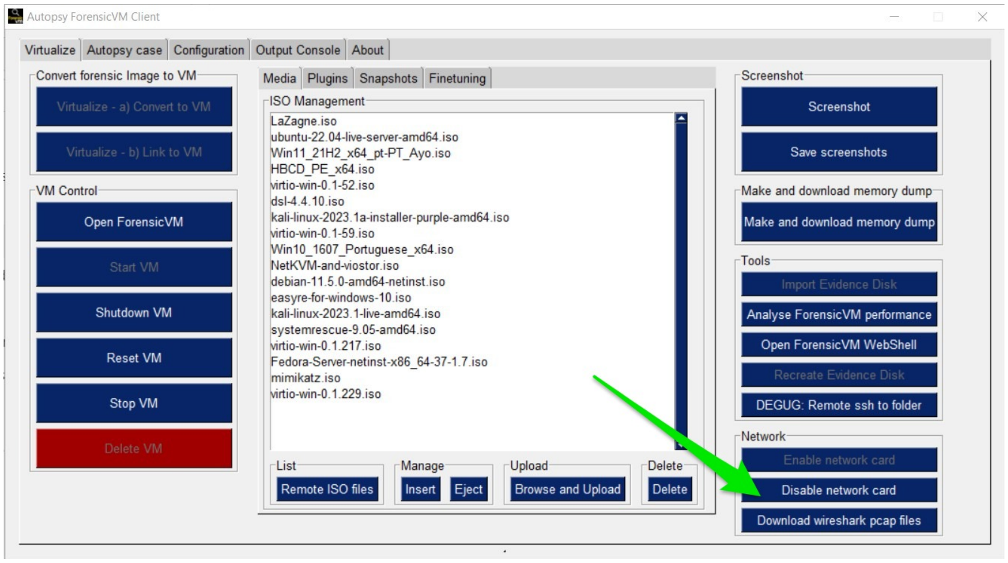
There are two primary methods to deactivate the network card on the forensicVM:

1. Using the Autopsy ForensicVM client plugin interface.
2. Directly interacting with the web screen interface.

Disable Network Card with the Autopsy ForensicVM Client Plugin Interface

Steps to Deactivate Network Card:

1. Ensure that the forensicVM machine is running.
2. Within the interface, go to the Network Panel.
3. Click on the “Disable network card” button.



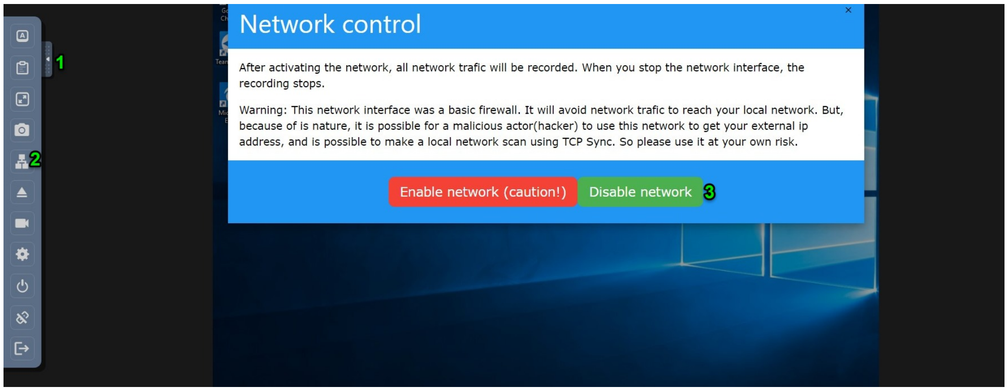
LaZagne.iso
ubuntu-22.04-live-server-amd64.iso
Win11_21H2_x64_pt-PT_Ayo.iso
HBCD_PE_x64.iso
virtio-win-0.1-52.iso
dsl-4.4.10.iso
kali-linux-2023.1a-installer-purple-amd64.iso
virtio-win-0.1-59.iso
Win10_1607_Portuguese_x64.iso
NetKVM-and-viostor.iso
debian-11.5.0-amd64-netinst.iso
easyre-for-windows-10.iso
kali-linux-2023.1-live-amd64.iso
systemrescue-9.05-amd64.iso
virtio-win-0.1.217.iso
Fedora-Server-netinst-x86_64-37-1.7.iso
mimikatz.iso
virtio-win-0.1.229.iso

Using the Web Screen Interface to Disable the Network Card

The Web Screen Interface offers an alternative approach for users who prefer to manage network settings without engaging with the main software interface.

Steps to Disable Network:

1. Activate the **Panel Opener (1)** to view more options.
2. Click on the **network icon (2)**.
3. Press the green **Disable network (3)** button to turn off the network card.



Network control

After activating the network, all network trafic will be recorded. When you stop the network interface, the recording stops.

Warning: This network interface was a basic firewall. It will avoid network trafic to reach your local network. But, because of is nature, it is possible for a malicious actor(hacker) to use this network to get your external ip address, and is possible to make a local network scan using TCP Sync. So please use it at your own risk.

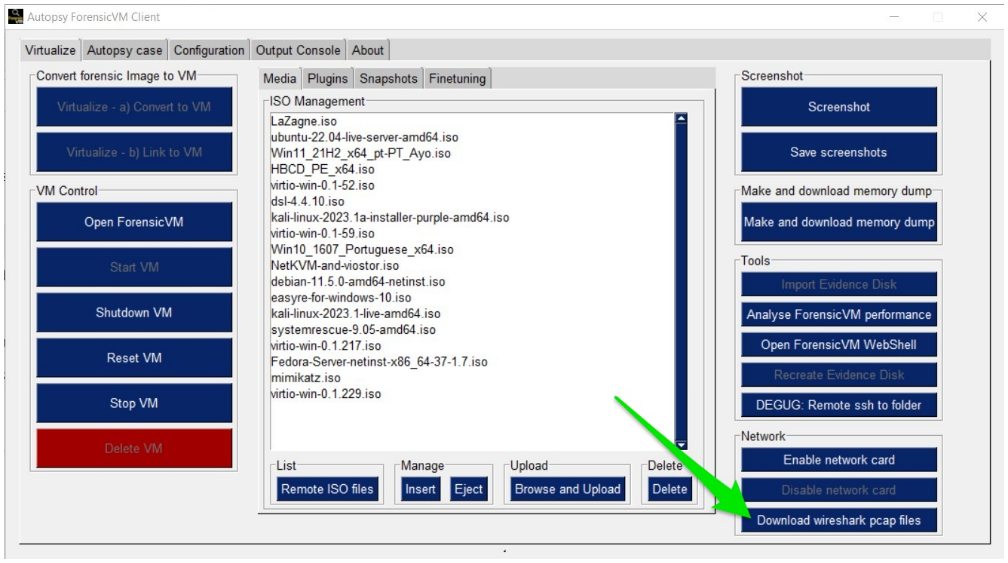
Fig. 7.160: Process to disable the network card using the Web Screen Interface

7.13.4 Download Wireshark pcap Files

Downloading pcap Files

To obtain the Wireshark pcap files, follow the instructions below:

1. Click the "Download Wireshark pcap files" button located on the Autopsy ForensicVM client plugin interface.

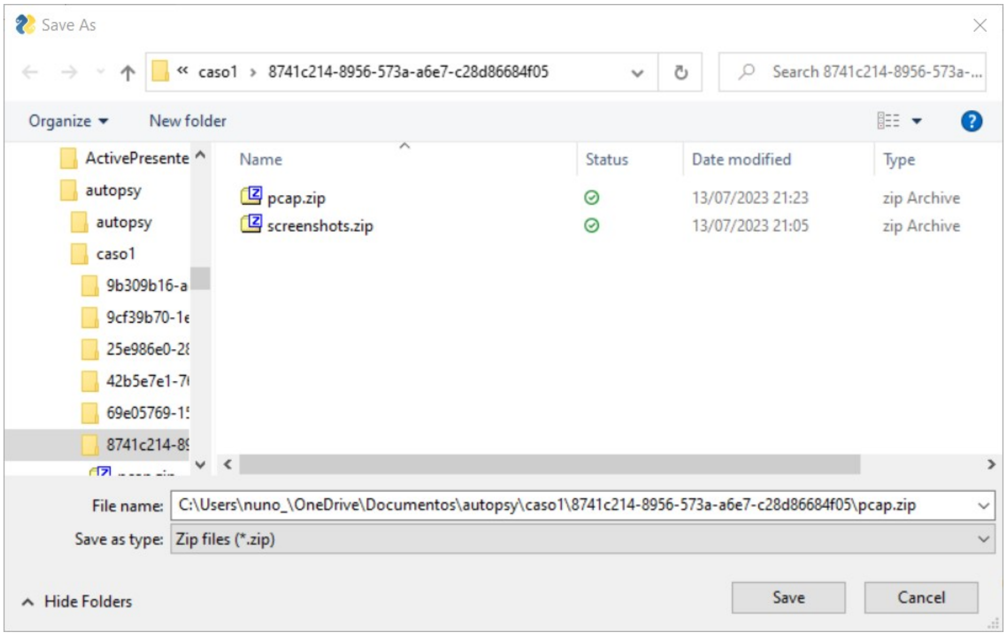


ISO Management

LaZagne.iso
ubuntu-22.04-live-server-amd64.iso
Win11_21H2_x64_pt-PT_Ayo.iso
HBCD_PE_x64.iso
virtio-win-0.1-52.iso
dsl-4.4.10.iso
kali-linux-2023.1a-installer-purple-amd64.iso
virtio-win-0.1-59.iso
Win10_1607_Portuguese_x64.iso
NetKVM-and-viostor.iso
debian-11.5.0-amd64-netinst.iso
easyre-for-windows-10.iso
kali-linux-2023.1-live-amd64.iso
systemrescue-9.05-amd64.iso
virtio-win-0.1.217.iso
Fedora-Server-netinst-x86_64-37-1.7.iso
mimikatz.iso
virtio-win-0.1.229.iso

Fig. 7.161: Downloading pcap files

2. A Windows Explorer window will prompt you to select a save location for the pcap.zip file. It's recommended to maintain the default save path, which is typically set to the image case folder.



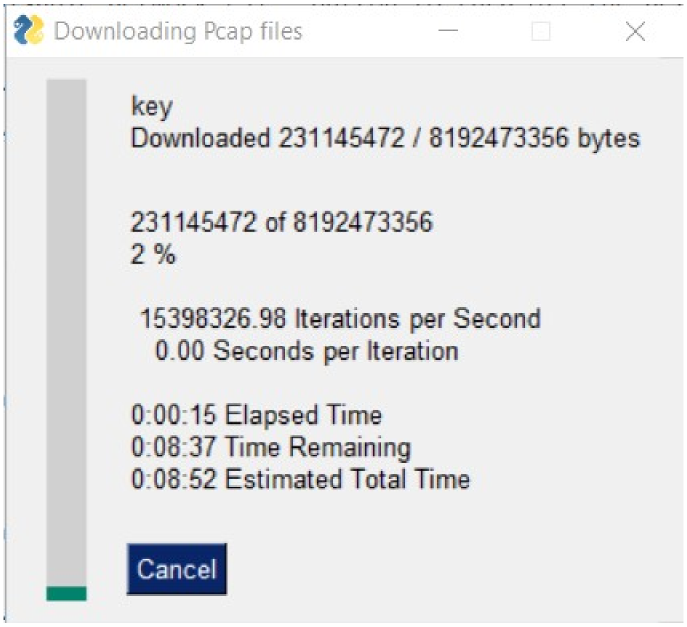
Name	Status	Date modified	Type
pcap.zip	✓	13/07/2023 21:23	zip Archive
screenshots.zip	✓	13/07/2023 21:05	zip Archive

File name: C:\Users\nuno_\OneDrive\Documentos\autopsy\caso1\8741c214-8956-573a-a6e7-c28d86684f05\pcap.zip

Save as type: Zip files (*.zip)

Fig. 7.162: Saving pcap.zip file path

3. The download progress will be displayed, indicating the time required to complete the download. This duration can vary depending on the size of the pcap.zip file.



key
Downloaded 231145472 / 8192473356 bytes

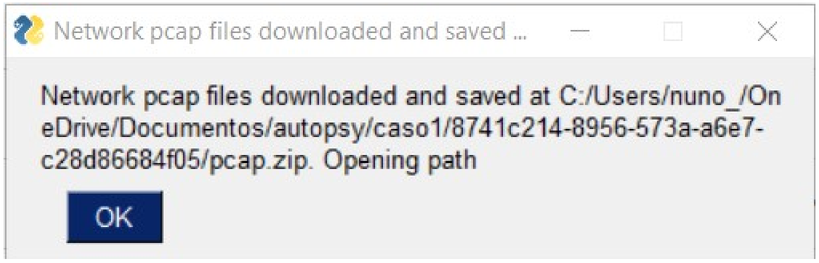
231145472 of 8192473356
2 %

15398326.98 Iterations per Second
0.00 Seconds per Iteration

0:00:15 Elapsed Time
0:08:37 Time Remaining
0:08:52 Estimated Total Time

Fig. 7.163: Download progress

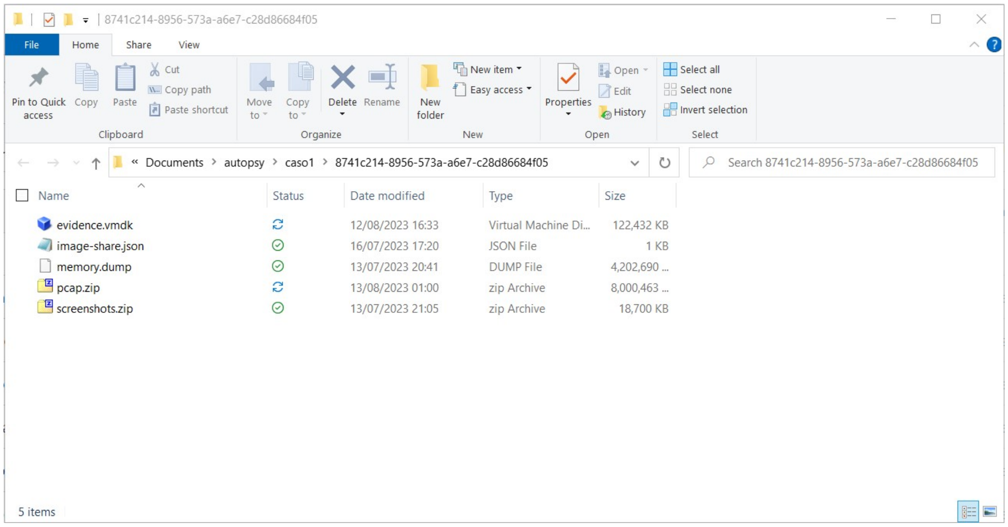
4. Once the download is completed, a confirmation pop-up will appear, indicating the successful download and save location.



Network pcap files downloaded and saved at C:/Users/nuno_/OneDrive/Documentos/autopsy/caso1/8741c214-8956-573a-a6e7-c28d86684f05/pcap.zip. Opening path

Fig. 7.164: Network pcap downloaded and saved

5. The Windows Explorer will automatically open to the default save location of pcap.zip.



Name	Status	Date modified	Type	Size
evidence.vmdk	↻	12/08/2023 16:33	Virtual Machine Di...	122,432 KB
image-share.json	✓	16/07/2023 17:20	JSON File	1 KB
memory.dump	✓	13/07/2023 20:41	DUMP File	4,202,690 ...
pcap.zip	↻	13/08/2023 01:00	zip Archive	8,000,463 ...
screenshots.zip	✓	13/07/2023 21:05	zip Archive	18,700 KB

Fig. 7.165: Default pcap.zip path in explorer

6. To decompress the pcap.zip` file, you can use a program like 7-zip. The extraction can take some time, especially if the pcap files are large.

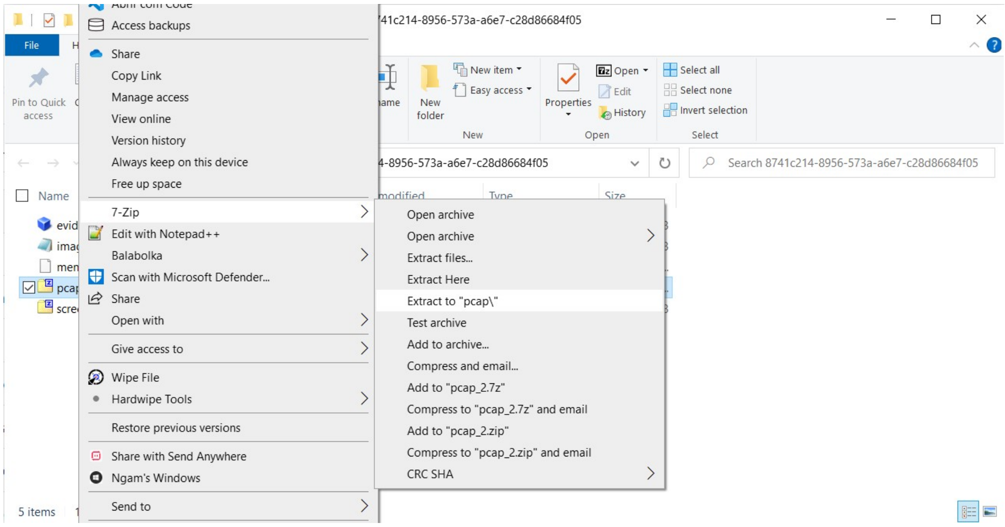
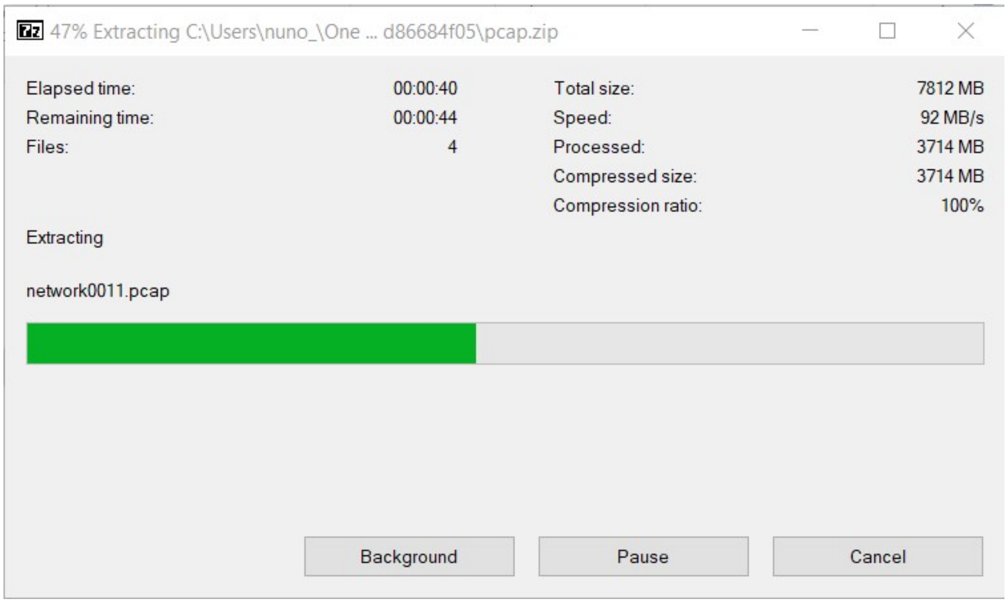


Fig. 7.166: Extracting pcap.zip file using 7-zip



47% Extracting C:\Users\nuno_\One ... d86684f05\pcap.zip

Elapsed time:	00:00:40	Total size:	7812 MB
Remaining time:	00:00:44	Speed:	92 MB/s
Files:	4	Processed:	3714 MB
		Compressed size:	3714 MB
		Compression ratio:	100%

Extracting

network0011.pcap

Fig. 7.167: Extraction progress

7.13.5 Analyze network traffic in Wireshark

Analyzing network traffic is an integral part of digital forensic investigations, especially when attempting to reconstruct a sequence of events or identify malicious activities. Using a tool like Wireshark to analyze traffic from a forensic image virtual machine can provide investigators with a wealth of information. However, this approach comes with its advantages and potential pitfalls.

Importance of Analyzing Traffic in Forensic Investigations

1. Evidence Collection: Analyzing traffic can reveal communication with suspicious IP addresses, hinting at potential data exfiltration or command-and-control servers.
2. **User Behavior**: Network traffic can provide clues about user behavior, including sites visited, files downloaded, or apps used.
3. Timestamps: Traffic analysis can help in reconstructing timelines of events, crucial for correlating actions across different evidence sources.
4. **Detect Malware**: Unusual network traffic patterns can be indicative of malware communication.

Advantages

1. **Comprehensive Data View**: Wireshark offers a detailed view of packets, allowing forensic investigators to delve deep into the network interactions.
2. **Filtering and Searching**: With its advanced filtering options, investigators can isolate relevant data quickly.
3. Decoding Protocols: Wireshark can decode a vast array of protocols, aiding in understanding the specifics of network conversations.
4. **Visualization**: Graphical features like flow graphs help in visualizing communication patterns.

Dangers

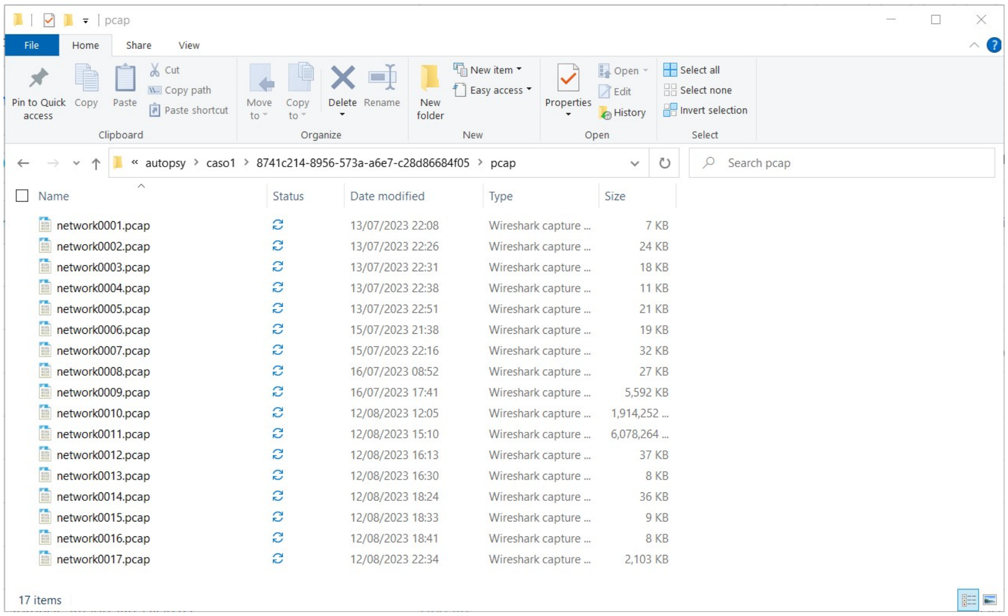
1. Data Overload: The volume of data in pcap files can be overwhelming, and without proper focus, important details might be missed.

2. **Privacy Concerns**: Analyzing traffic can inadvertently capture personal or sensitive information of innocent users.
3. Tampered Data: If the forensic image virtual machine is compromised, the network data might be tampered with, leading to incorrect conclusions.
4. **Misinterpretation**: Without proper expertise, normal traffic can be misinterpreted as malicious or vice versa.

Note: While Wireshark is a powerful tool for forensic investigations, it's essential to approach the analysis with a clear understanding of the goals, the data's context, and the potential pitfalls. Proper training and experience can help in maximizing the benefits of traffic analysis while minimizing risks. Given the complexity and subtleties involved in network traffic analysis, it's recommended that forensic investigators continuously update their training and remain informed about the latest techniques and threats in the domain.

After extracting the pcap files, the next step is to analyze the network traffic captured during the period the network card was active. Here's how to proceed:

1. Navigate to the extracted pcap directory. If Wireshark isn't installed on your system, visit wireshark.org to download and install it. Once installed, Wireshark-associated icons will appear next to each pcap file.
2. Double-click the pcap file you wish to analyze.



« autopsy › caso1 › 8741c214-8956-573a-a6e7-c28d86684f05 › pcap

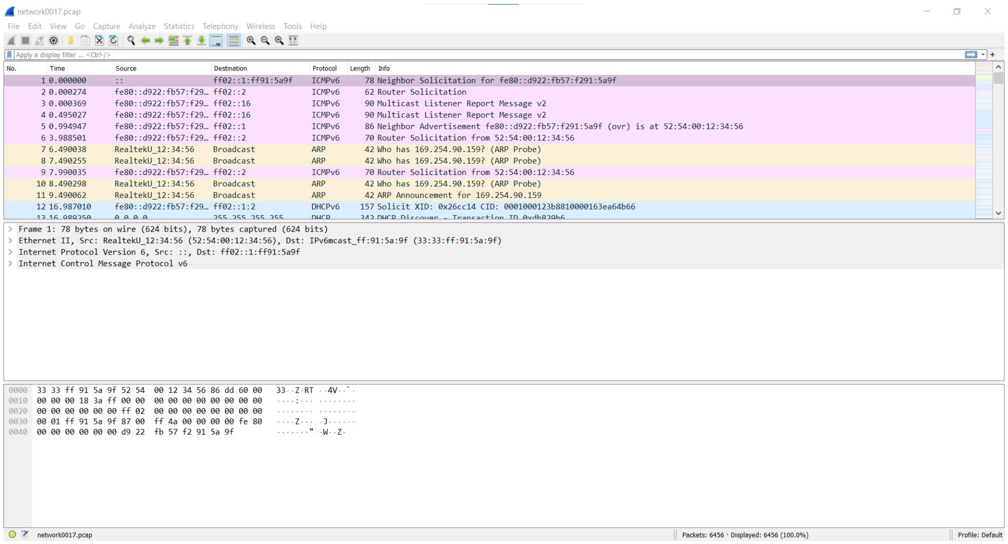
Name	Status	Date modified	Type	Size
network0001.pcap	⟳	13/07/2023 22:08	Wireshark capture ...	7 KB
network0002.pcap	⟳	13/07/2023 22:26	Wireshark capture ...	24 KB
network0003.pcap	⟳	13/07/2023 22:31	Wireshark capture ...	18 KB
network0004.pcap	⟳	13/07/2023 22:38	Wireshark capture ...	11 KB
network0005.pcap	⟳	13/07/2023 22:51	Wireshark capture ...	21 KB
network0006.pcap	⟳	15/07/2023 21:38	Wireshark capture ...	19 KB
network0007.pcap	⟳	15/07/2023 22:16	Wireshark capture ...	32 KB
network0008.pcap	⟳	16/07/2023 08:52	Wireshark capture ...	27 KB
network0009.pcap	⟳	16/07/2023 17:41	Wireshark capture ...	5,592 KB
network0010.pcap	⟳	12/08/2023 12:05	Wireshark capture ...	1,914,252 ...
network0011.pcap	⟳	12/08/2023 15:10	Wireshark capture ...	6,078,264 ...
network0012.pcap	⟳	12/08/2023 16:13	Wireshark capture ...	37 KB
network0013.pcap	⟳	12/08/2023 16:30	Wireshark capture ...	8 KB
network0014.pcap	⟳	12/08/2023 18:24	Wireshark capture ...	36 KB
network0015.pcap	⟳	12/08/2023 18:33	Wireshark capture ...	9 KB
network0016.pcap	⟳	12/08/2023 18:41	Wireshark capture ...	8 KB
network0017.pcap	⟳	12/08/2023 22:34	Wireshark capture ...	2,103 KB

17 items

Fig. 7.168: Selecting pcap file for analysis

3. The Wireshark interface will open, displaying the captured traffic. Adjust the view settings and apply filters as required based on your forensic goals. .. raw:: latex

   FloatBarrier



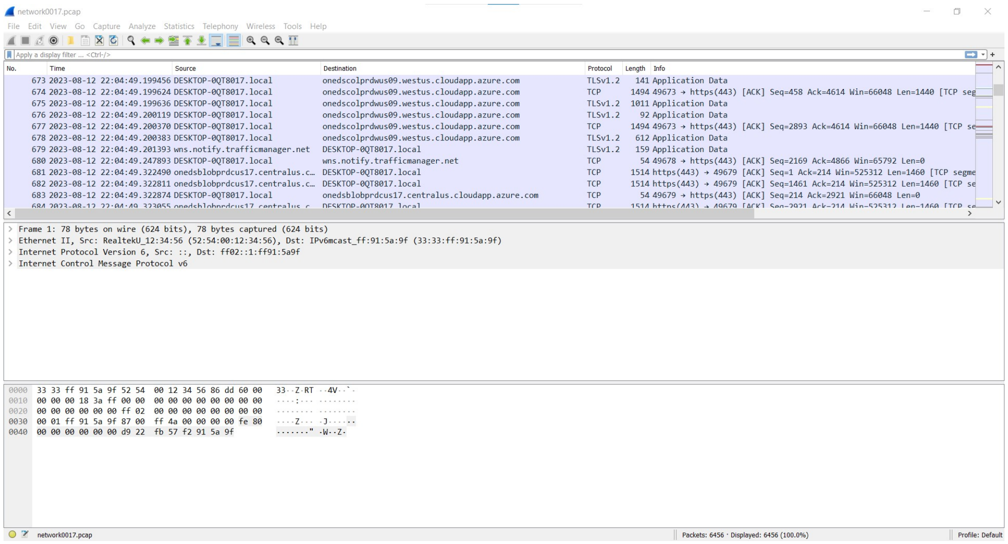
network0017.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time        Source                  Destination        Protocol Length Info
   1 0.000000    ::                      ff02::1:ff91:5a9f  ICMPv6     78 Neighbor Solicitation for fe80::d922:fb57:f291:5a9f
   2 0.000274    fe80::d922:fb57:f29…    ff02::2            ICMPv6     62 Router Solicitation
   3 0.000369    fe80::d922:fb57:f29…    ff02::16           ICMPv6     90 Multicast Listener Report Message v2
   4 0.495027    fe80::d922:fb57:f29…    ff02::16           ICMPv6     90 Multicast Listener Report Message v2
   5 0.994947    fe80::d922:fb57:f29…    ff02::1            ICMPv6     86 Neighbor Advertisement fe80::d922:fb57:f291:5a9f (ovr) is at 52:54:00:12:34:56
   6 3.988501    fe80::d922:fb57:f29…    ff02::2            ICMPv6     70 Router Solicitation from 52:54:00:12:34:56
   7 6.490038    RealtekU_12:34:56       Broadcast          ARP        42 Who has 169.254.90.159? (ARP Probe)
   8 7.490255    RealtekU_12:34:56       Broadcast          ARP        42 Who has 169.254.90.159? (ARP Probe)
   9 7.990035    fe80::d922:fb57:f29…    ff02::2            ICMPv6     70 Router Solicitation from 52:54:00:12:34:56
  10 8.490298    RealtekU_12:34:56       Broadcast          ARP        42 Who has 169.254.90.159? (ARP Probe)
  11 9.490062    RealtekU_12:34:56       Broadcast          ARP        42 ARP Announcement for 169.254.90.159
  12 16.987010   fe80::d922:fb57:f29…    ff02::1:2          DHCPv6    157 Solicit XID: 0x26cc14 CID: 0001000123b8810000163ea64b66
  13 16.989250   0.0.0.0                 255.255.255.255    DHCP      342 DHCP Discover - Transaction ID 0xdb829b6
```

```
> Frame 1: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
> Ethernet II, Src: RealtekU_12:34:56 (52:54:00:12:34:56), Dst: IPv6mcast_ff:91:5a:9f (33:33:ff:91:5a:9f)
> Internet Protocol Version 6, Src: ::, Dst: ff02::1:ff91:5a9f
> Internet Control Message Protocol v6
```

```
0000  33 33 ff 91 5a 9f 52 54  00 12 34 56 86 dd 60 00   33··Z·RT ··4V··`·
0010  00 00 00 18 3a ff 00 00  00 00 00 00 00 00 00 00   ····:··· ········
0020  00 00 00 00 00 00 ff 02  00 00 00 00 00 00 00 00   ········ ········
0030  00 01 ff 91 5a 9f 87 00  ff 4a 00 00 00 00 fe 80   ····Z··· ·J······
0040  00 00 00 00 00 00 d9 22  fb 57 f2 91 5a 9f         ·······" ·W··Z·
```

4. The following is an example of network traffic analysis with a focus on cloud traffic.



network0017.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time                       Source                           Destination                                     Protocol Length Info
 673 2023-08-12 22:04:49.199456 DESKTOP-0QT8017.local            onedscolprdwus09.westus.cloudapp.azure.com      TLSv1.2   141 Application Data
 674 2023-08-12 22:04:49.199624 DESKTOP-0QT8017.local            onedscolprdwus09.westus.cloudapp.azure.com      TCP      1494 49673 → https(443) [ACK] Seq=458 Ack=4614 Win=66048 Len=1440 [TCP seg
 675 2023-08-12 22:04:49.199636 DESKTOP-0QT8017.local            onedscolprdwus09.westus.cloudapp.azure.com      TLSv1.2  1011 Application Data
 676 2023-08-12 22:04:49.200119 DESKTOP-0QT8017.local            onedscolprdwus09.westus.cloudapp.azure.com      TLSv1.2    92 Application Data
 677 2023-08-12 22:04:49.200370 DESKTOP-0QT8017.local            onedscolprdwus09.westus.cloudapp.azure.com      TCP      1494 49673 → https(443) [ACK] Seq=2893 Ack=4614 Win=66048 Len=1440 [TCP se
 678 2023-08-12 22:04:49.200383 DESKTOP-0QT8017.local            onedscolprdwus09.westus.cloudapp.azure.com      TLSv1.2   612 Application Data
 679 2023-08-12 22:04:49.201393 wns.notify.trafficmanager.net    DESKTOP-0QT8017.local                           TLSv1.2   159 Application Data
 680 2023-08-12 22:04:49.247893 DESKTOP-0QT8017.local            wns.notify.trafficmanager.net                   TCP        54 49678 → https(443) [ACK] Seq=2169 Ack=4866 Win=65792 Len=0
 681 2023-08-12 22:04:49.322490 onedsblobprdcus17.centralus.c…   DESKTOP-0QT8017.local                           TCP      1514 https(443) → 49679 [ACK] Seq=1 Ack=214 Win=525312 Len=1460 [TCP segme
 682 2023-08-12 22:04:49.322811 onedsblobprdcus17.centralus.c…   DESKTOP-0QT8017.local                           TCP      1514 https(443) → 49679 [ACK] Seq=1461 Ack=214 Win=525312 Len=1460 [TCP se
 683 2023-08-12 22:04:49.322874 DESKTOP-0QT8017.local            onedsblobprdcus17.centralus.cloudapp.azure.com  TCP        54 49679 → https(443) [ACK] Seq=214 Ack=2921 Win=66048 Len=0
 684 2023-08-12 22:04:49.323055 onedsblobprdcus17.centralus.c…   DESKTOP-0QT8017.local                           TCP      1514 https(443) → 49679 [ACK] Seq=2921 Ack=214 Win=525312 Len=1460 [TCP se
```

```
> Frame 1: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
> Ethernet II, Src: RealtekU_12:34:56 (52:54:00:12:34:56), Dst: IPv6mcast_ff:91:5a:9f (33:33:ff:91:5a:9f)
> Internet Protocol Version 6, Src: ::, Dst: ff02::1:ff91:5a9f
> Internet Control Message Protocol v6
```

```
0000  33 33 ff 91 5a 9f 52 54  00 12 34 56 86 dd 60 00   33··Z·RT ··4V··`·
0010  00 00 00 18 3a ff 00 00  00 00 00 00 00 00 00 00   ····:··· ········
0020  00 00 00 00 00 00 ff 02  00 00 00 00 00 00 00 00   ········ ········
0030  00 01 ff 91 5a 9f 87 00  ff 4a 00 00 00 00 fe 80   ····Z··· ·J······
0040  00 00 00 00 00 00 d9 22  fb 57 f2 91 5a 9f         ·······" ·W··Z·
```

Fig. 7.169: Example of analyzing cloud traffic in Wireshark

Note: Analyzing pcap files requires a sound understanding of network traffic patterns and potential security threats. It's crucial to interpret the data accurately to avoid misleading conclusions.

7.14 Media Management in ForensicVM: Leveraging ISOs for Enhanced Forensic Investigations

In forensic investigations, the ability to access and utilize a wide array of specialized tools is of utmost importance. Different cases present unique challenges and often require specific utilities or software to effectively extract, analyze, or visualize evidence. ISO files, serving as encapsulations of entire file systems, are adept at housing a myriad of these specialized tools, thereby ensuring forensic professionals are always equipped with the right utilities.

The management and utilization of ISO files within ForensicVM is precisely tailored to meet the multifaceted demands of modern forensic investigations. Herein, a meticulously crafted procedure allows investigators to seamlessly navigate, upload, select, insert, eject, delete, and even boot from these ISO files. This integration ensures that forensic experts are never bound by just the in-built tools in ForensicVM, offering the flexibility to dynamically introduce and employ auxiliary resources as the situation demands.

From a safety vantage point, employing ISOs within a virtual domain like ForensicVM comes with its set of undeniable perks:

1. Network Isolation: Leveraging tools from ISOs eliminates the need for network connectivity. This not only curtails risks associated with internet connectivity but also guarantees that neither evidence nor the operating environment is inadvertently compromised owing to network-centric threats or malware.
2. Protective Shield: Operating tools within ForensicVM's virtual periphery ensures the host system and its network remain insulated from looming threats. Any potentially malignant operations remain confined to the virtual environment, thereby preserving the sanctity of the primary forensic setup.
3. Evidence Preservation: Operating in a controlled ambit significantly reduces risks associated with evidence contamination or inadvertent alterations. The sacrosanct nature of evidence remains unchallenged, a pivotal aspect for its admissibility in legal arenas.

ForensicVM's adeptness at ISO management not only broadens the forensic toolkit available to investigators but also accentuates the safety, security, and integrity quotient of the investigative process. This section unravels the nuances of these operations, offering insights into harnessing the full might of ISOs in your forensic pursuits.

In the realm of digital forensics, every tool and capability at an investigator's disposal can be the difference between uncovering critical evidence or hitting a dead end. ISO files, in particular, offer a versatile medium to house a myriad of investigative utilities. With ForensicVM, managing and utilizing these ISO files becomes a straightforward endeavor, optimizing both efficiency and efficacy. Here's an overview of the key operations:

- Browse and Upload ISO: Discover how to navigate the interface to select and upload essential ISO files to the ForensicVM environment.
- **Select ISO / Web Select CD-ROM**: Instructions on choosing the right ISO file or CD-ROM from the Autopsy ForensicVM Client Plugin or from the web interface.
- List Remote ISO Files: Get an overview of all ISO files stored remotely on the ForensicVM server.
- Insert ISO / Web Insert CD-ROM: Learn how to virtually insert an ISO file or CD-ROM for access within the virtualized forensic image, from the Autopsy ForensicVM Client Plugin or from the web interface.
- Eject ISO / Web Eject CD-ROM: Step-by-step guidance on safely ejecting a mounted ISO file or CD-ROM, from the Autopsy ForensicVM Client Plugin or from the web interface.
- **Delete ISO**: Understand how to remove ISO files that are no longer needed, ensuring a clutter-free workspace.
- Bootable Media: Dive into the specifics of booting from an ISO or CD-ROM, a critical capability for certain forensic tasks.

Proceed to the relevant subsections for detailed instructions and best practices to make the most of the media management features in ForensicVM.

7.14.1 Uploading an ISO to the ForensicVM Server

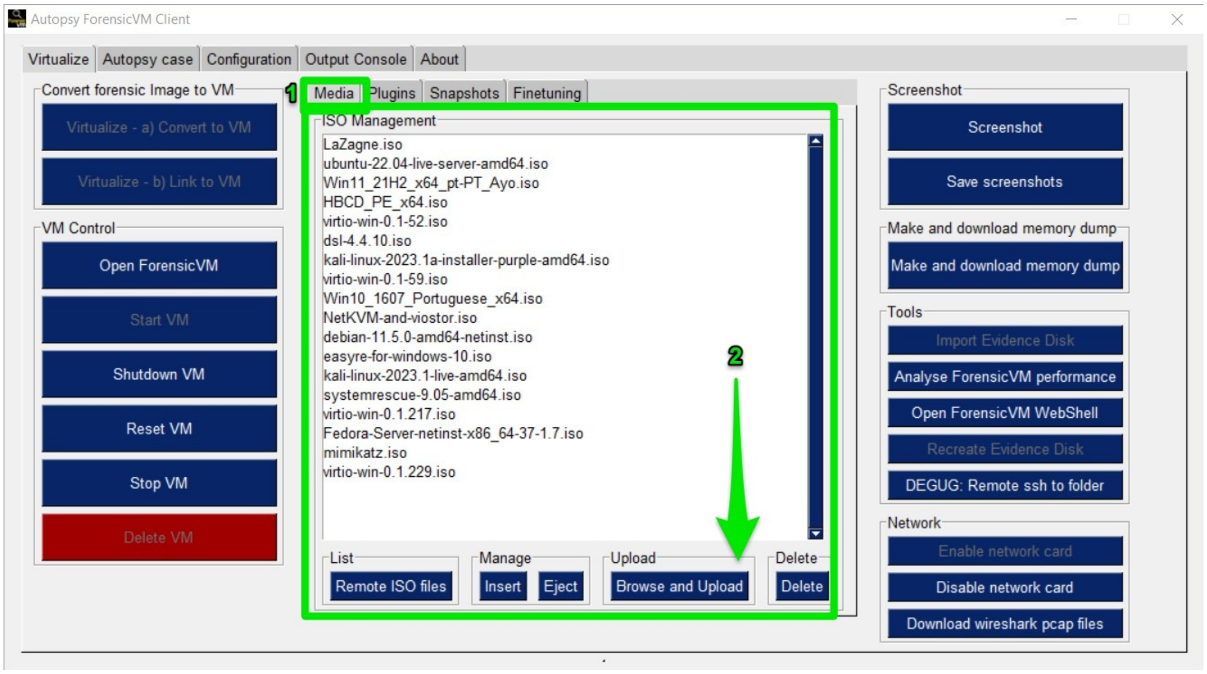
When conducting a forensic investigation, specialized tools are often required to aid in the extraction or analysis of data. Many of these tools are conveniently bundled into ISO files. With ForensicVM, you can seamlessly upload these ISO files, making them readily accessible for your investigation tasks. Here's a step-by-step guide to doing so:

Step 1: Access the Media Panel

- Navigate to the Autopsy VM and locate the ForensicVM Client Plugin.
- Click on the Media Panel Separator.

Step 2: Initiate the ISO Upload

- Click the "Browse and Upload" button.

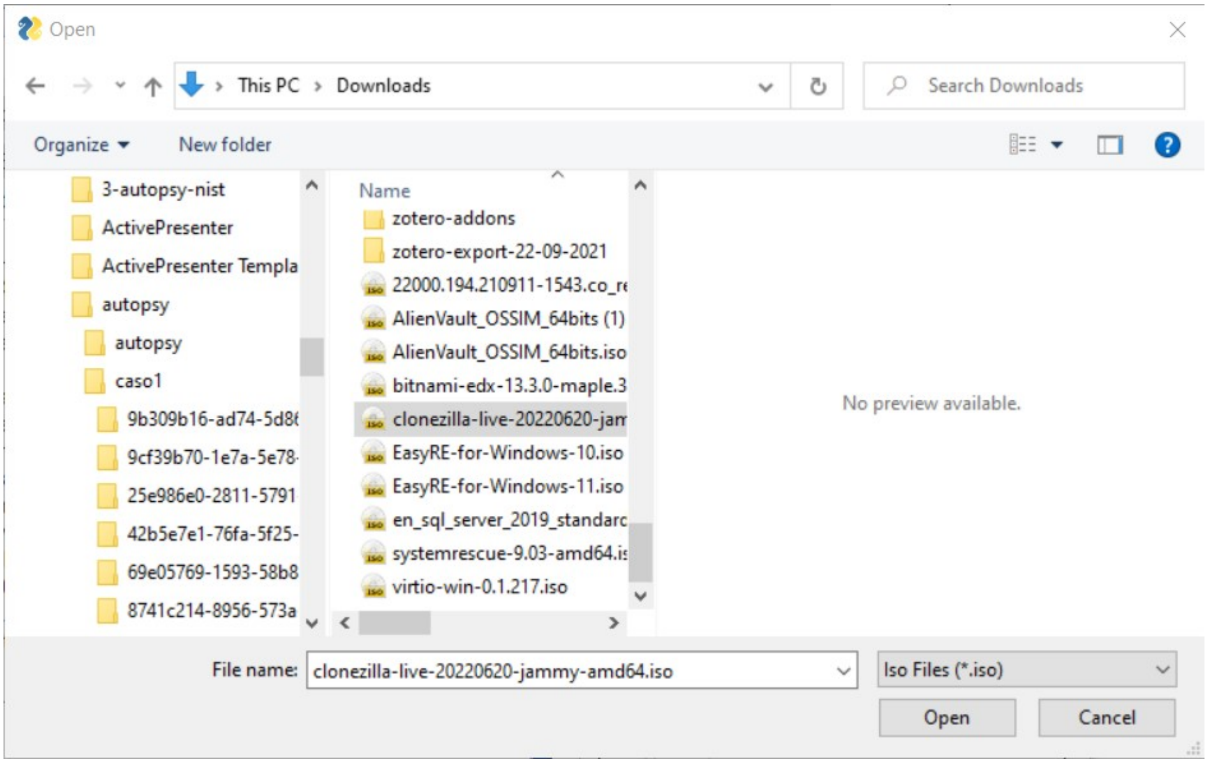


```
LaZagne.iso
ubuntu-22.04-live-server-amd64.iso
Win11_21H2_x64_pt-PT_Ayo.iso
HBCD_PE_x64.iso
virtio-win-0.1-52.iso
dsl-4.4.10.iso
kali-linux-2023.1a-installer-purple-amd64.iso
virtio-win-0.1-59.iso
Win10_1607_Portuguese_x64.iso
NetKVM-and-viostor.iso
debian-11.5.0-amd64-netinst.iso
easyre-for-windows-10.iso
kali-linux-2023.1-live-amd64.iso
systemrescue-9.05-amd64.iso
virtio-win-0.1.217.iso
Fedora-Server-netinst-x86_64-37-1.7.iso
mimikatz.iso
virtio-win-0.1.229.iso
```

Fig. 7.170: Browse and Upload

Step 3: Locate and Select the ISO File

- Browse your computer's directories and select the desired ISO file to upload.



3-autopsy-nist
ActivePresenter
ActivePresenter Templa
autopsy
autopsy
caso1
9b309b16-ad74-5d8
9cf39b70-1e7a-5e78-
25e986e0-2811-5791
42b5e7e1-76fa-5f25-
69e05769-1593-58b8
8741c214-8956-573a

zotero-addons
zotero-export-22-09-2021
22000.194.210911-1543.co_r
AlienVault_OSSIM_64bits (1)
AlienVault_OSSIM_64bits.iso
bitnami-edx-13.3.0-maple.3
clonezilla-live-20220620-jam
EasyRE-for-Windows-10.iso
EasyRE-for-Windows-11.iso
en_sql_server_2019_standarc
systemrescue-9.03-amd64.i
virtio-win-0.1.217.iso

File name: clonezilla-live-20220620-jammy-amd64.iso

Iso Files (*.iso)

Fig. 7.171: Locate and Select the ISO File

Step 4: Upload Confirmation

The upload process might take some time, depending on the size of the ISO file. There's no progress bar available currently, so please be patient and wait for a confirmation message to appear, indicating a successful upload.

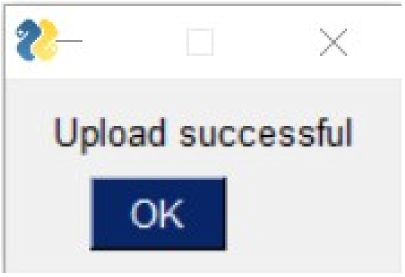
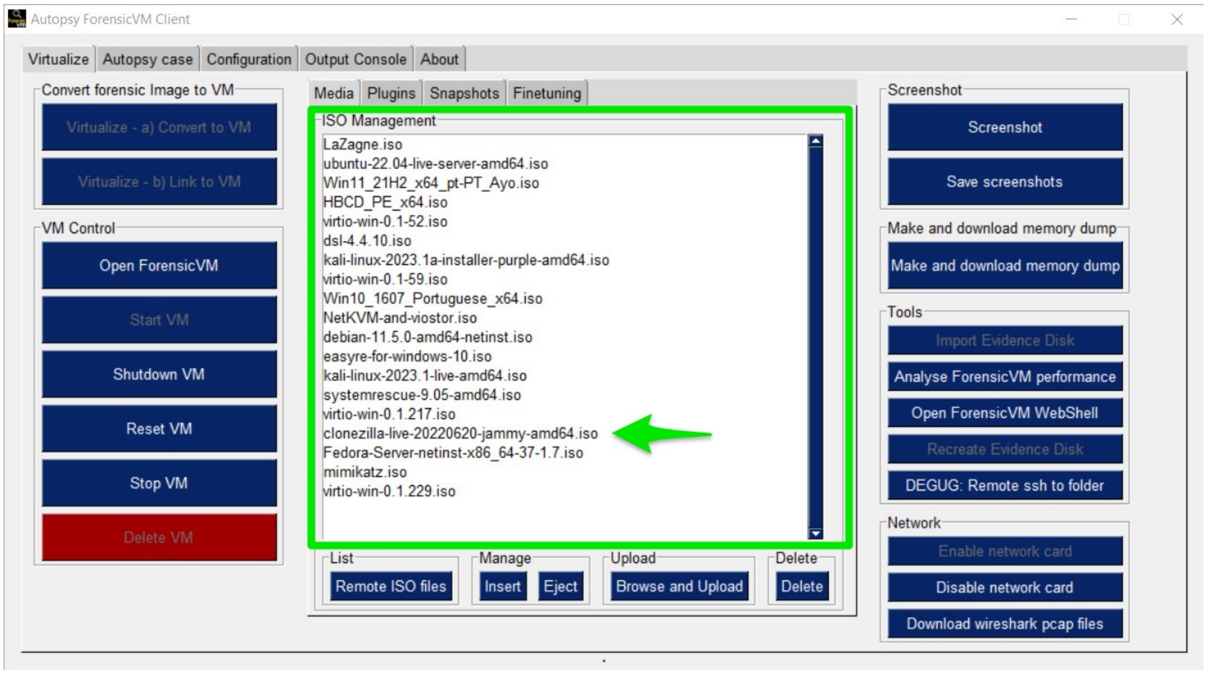

Upload successful

Fig. 7.172: Upload Confirmation

Note: During the upload process, the Autopsy ForensicVM Client Plugin might become unresponsive. This is expected behavior. Please wait patiently until the upload completes.

Step 5: Verify the Uploaded ISO

Once uploaded, you should be able to see the ISO file listed in the ISO Management section of the ForensicVM server. This ensures your tools are now ready to be utilized in your ongoing investigation.



LaZagne.iso
ubuntu-22.04-live-server-amd64.iso
Win11_21H2_x64_pt-PT_Ayo.iso
HBCD_PE_x64.iso
virtio-win-0.1-52.iso
dsl-4.4.10.iso
kali-linux-2023.1a-installer-purple-amd64.iso
virtio-win-0.1-59.iso
Win10_1607_Portuguese_x64.iso
NetKVM-and-viostor.iso
debian-11.5.0-amd64-netinst.iso
easyre-for-windows-10.iso
kali-linux-2023.1-live-amd64.iso
systemrescue-9.05-amd64.iso
virtio-win-0.1.217.iso
clonezilla-live-20220620-jammy-amd64.iso
Fedora-Server-netinst-x86_64-37-1.7.iso
mimikatz.iso
virtio-win-0.1.229.iso

Fig. 7.173: Verifying the Uploaded ISO

7.14.2 List Remote ISO Files

When investigating digital evidence, it’s crucial to maintain a catalog of tools and resources available for the task. ForensicVM facilitates this by allowing users to store ISO files remotely on its server. This section outlines the procedures to access and view this list of remotely stored ISO files.

There are two primary methods to view these files:

Using the Autopsy ForensicVM Client Plugin

Step 1: Access the Media Panel

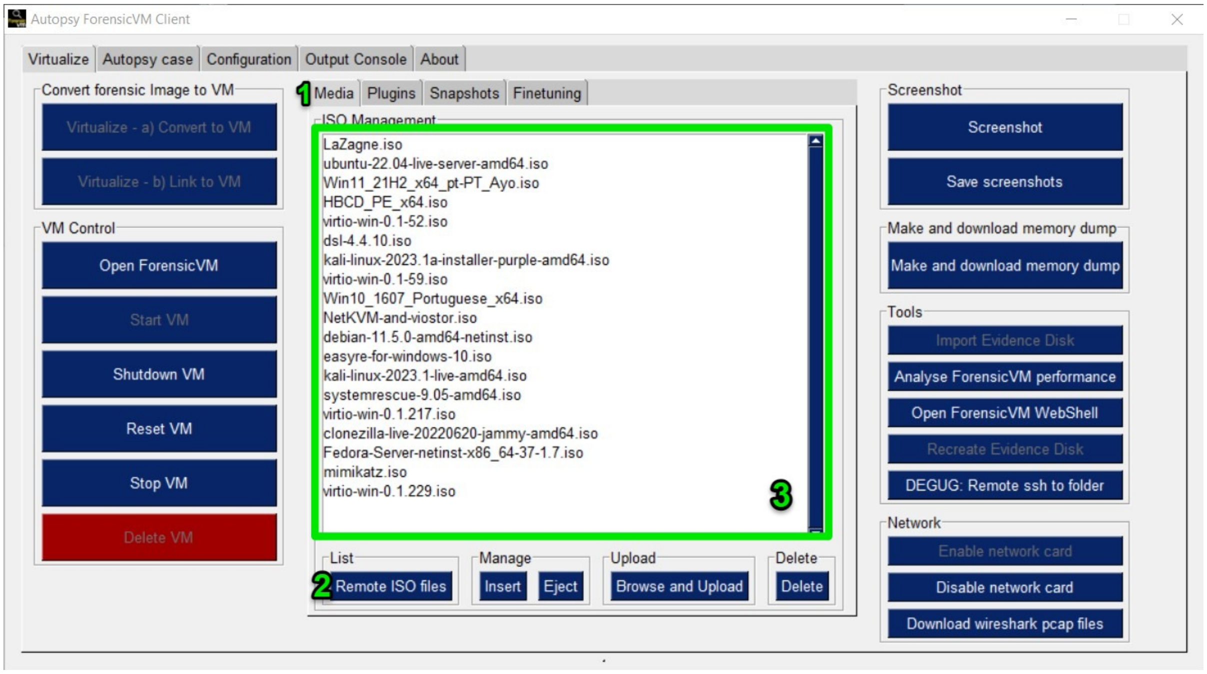
- Navigate to the Autopsy VM.
- Click on the **Media Panel Tab**.

Step 2: View Remote ISO Files

- Once in the media panel, click on the **Remote ISO Files** button.

Step 3: Review Available ISO Files

- The ISO file list will update.
- Browse through the list to review available tools and resources.
- If you find any tools missing or outdated, consider downloading or creating the necessary ISO files, and then upload them to the ForensicVM Server.



```
LaZagne.iso
ubuntu-22.04-live-server-amd64.iso
Win11_21H2_x64_pt-PT_Ayo.iso
HBCD_PE_x64.iso
virtio-win-0.1-52.iso
dsl-4.4.10.iso
kali-linux-2023.1a-installer-purple-amd64.iso
virtio-win-0.1-59.iso
Win10_1607_Portuguese_x64.iso
NetKVM-and-viostor.iso
debian-11.5.0-amd64-netinst.iso
easyre-for-windows-10.iso
kali-linux-2023.1-live-amd64.iso
systemrescue-9.05-amd64.iso
virtio-win-0.1.217.iso
clonezilla-live-20220620-jammy-amd64.iso
Fedora-Server-netinst-x86_64-37-1.7.iso
mimikatz.iso
virtio-win-0.1.229.iso
```

Viewing Remote ISO Files using Autopsy ForensicVM Client Plugin

Method 1: Using the Web Interface

Step 1: Access the Tool Panel

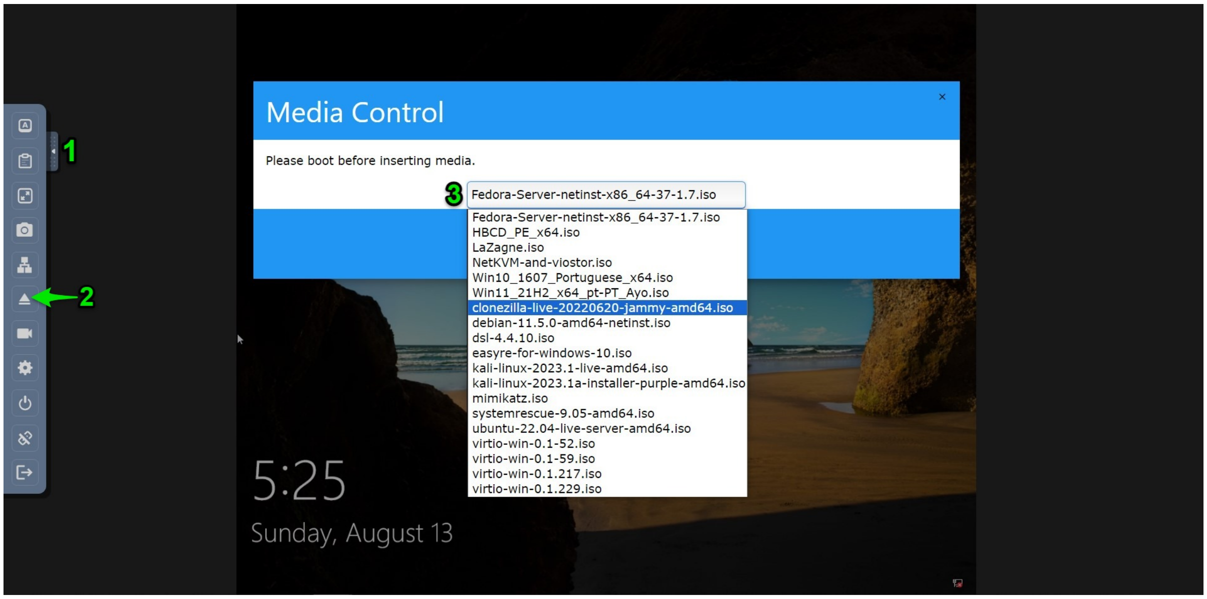
- On the main screen, click on the **Control Bar** icon to reveal the tool panel.

Step 2: Open the Media Control Modal Box

- Within the tool panel, locate and click the **Eject** icon. This action will open the Media Control Modal Box.

Step 3: View ISO Dropdown

- Click on the **ISO Dropdown**.
- This dropdown will display a list of all ISO files stored on the ForensicVM server, which can be utilized as virtual CD-ROMs.


Media Control
×
1
2
3
Fedora-Server-netinst-x86_64-37-1.7.iso
Fedora-Server-netinst-x86_64-37-1.7.iso
HBCD_PE_x64.iso
LaZagne.iso
NetKVM-and-viostor.iso
Win10_1607_Portuguese_x64.iso
Win11_21H2_x64_pt-PT_Ayo.iso
clonezilla-live-20220620-jammy-amd64.iso
debian-11.5.0-amd64-netinst.iso
dsl-4.4.10.iso
easyre-for-windows-10.iso
kali-linux-2023.1-live-amd64.iso
kali-linux-2023.1a-installer-purple-amd64.iso
mimikatz.iso
systemrescue-9.05-amd64.iso
ubuntu-22.04-live-server-amd64.iso
virtio-win-0.1-52.iso
virtio-win-0.1-59.iso
virtio-win-0.1.217.iso
virtio-win-0.1.229.iso
5:25
Sunday, August 13

Please boot before inserting media.

Fig. 7.174: Viewing Remote ISO Files using the Web Interface

7.14.3 Insert ISO / Web Insert CD-ROM

Being able to virtually insert an ISO file or CD-ROM into the virtualized forensic image is pivotal during a digital investigation. Different tools and utilities can be loaded on the fly without compromising the integrity of the original image. This flexibility speeds up the forensic workflow and allows investigators to adapt to different scenarios quickly. The following sections guide you on how to accomplish this task using either the Autopsy ForensicVM Client Plugin or the web interface.

Using the Autopsy ForensicVM Client Plugin

Step 1: Access the Media Panel

- Launch the Autopsy VM.
- Within the interface, click on the **Media Panel Tab**.

Step 2: Select the Desired ISO File

- In the media panel, browse through the ISO files.
- Click on the desired ISO file that you wish to insert.

Step 3: Insert the ISO File

- Locate and click the **Insert** button. This action will mount the selected ISO file as a virtual CD-ROM within the ForensicVM environment.
- Upon successful insertion, a success popup will appear, confirming the action.

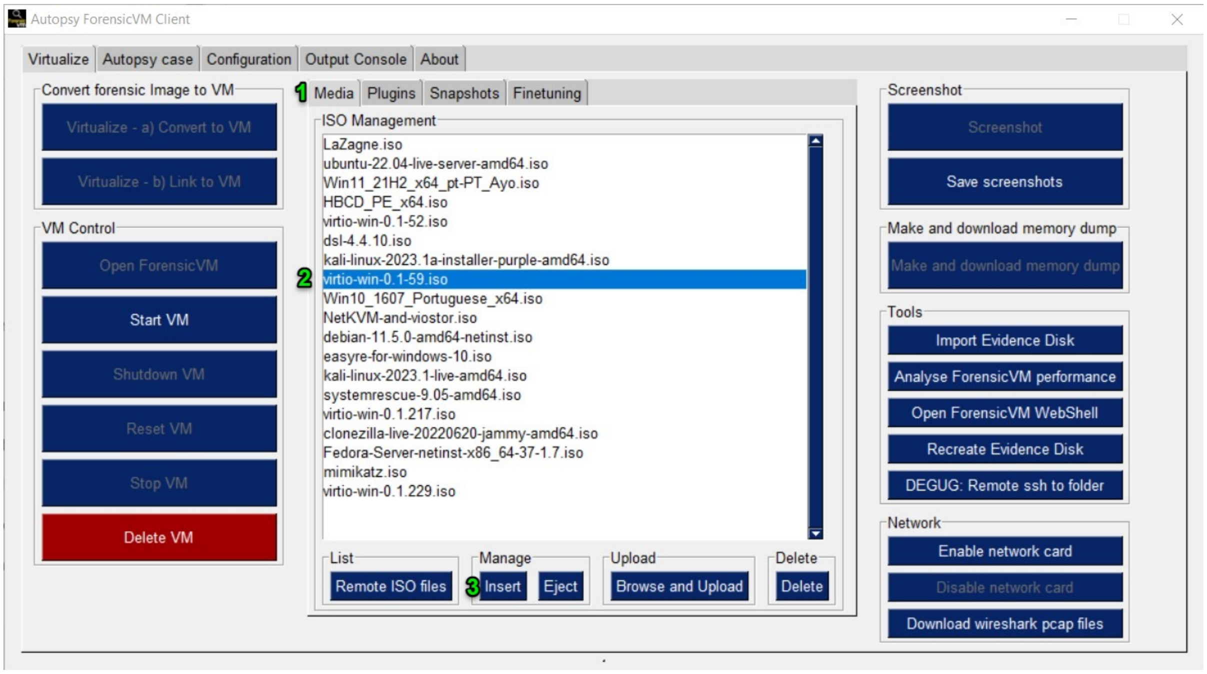

Autopsy ForensicVM Client
Virtualize
Autopsy case
Configuration
Output Console
About
Convert forensic Image to VM
Virtualize - a) Convert to VM
Virtualize - b) Link to VM
VM Control
Open ForensicVM
Start VM
Shutdown VM
Reset VM
Stop VM
Delete VM
1
Media
Plugins
Snapshots
Finetuning
ISO Management
LaZagne.iso
ubuntu-22.04-live-server-amd64.iso
Win11_21H2_x64_pt-PT_Ayo.iso
HBCD_PE_x64.iso
virtio-win-0.1-52.iso
dsl-4.4.10.iso
kali-linux-2023.1a-installer-purple-amd64.iso
2
virtio-win-0.1-59.iso
Win10_1607_Portuguese_x64.iso
NetKVM-and-viostor.iso
debian-11.5.0-amd64-netinst.iso
easyre-for-windows-10.iso
kali-linux-2023.1-live-amd64.iso
systemrescue-9.05-amd64.iso
virtio-win-0.1.217.iso
clonezilla-live-20220620-jammy-amd64.iso
Fedora-Server-netinst-x86_64-37-1.7.iso
mimikatz.iso
virtio-win-0.1.229.iso
List
Remote ISO files
Manage
3
Insert
Eject
Upload
Browse and Upload
Delete
Delete
Screenshot
Screenshot
Save screenshots
Make and download memory dump
Make and download memory dump
Tools
Import Evidence Disk
Analyse ForensicVM performance
Open ForensicVM WebShell
Recreate Evidence Disk
DEGUG: Remote ssh to folder
Network
Enable network card
Disable network card
Download wireshark pcap files

Fig. 7.175: Inserting ISO using the Autopsy ForensicVM Client Plugin

Using the Web Interface

Step 1: Access the Tool Panel

- From the main screen, identify and click on the **Control Bar** icon. This will reveal the tool panel.

Step 2: Navigate to the Media Control Modal Box

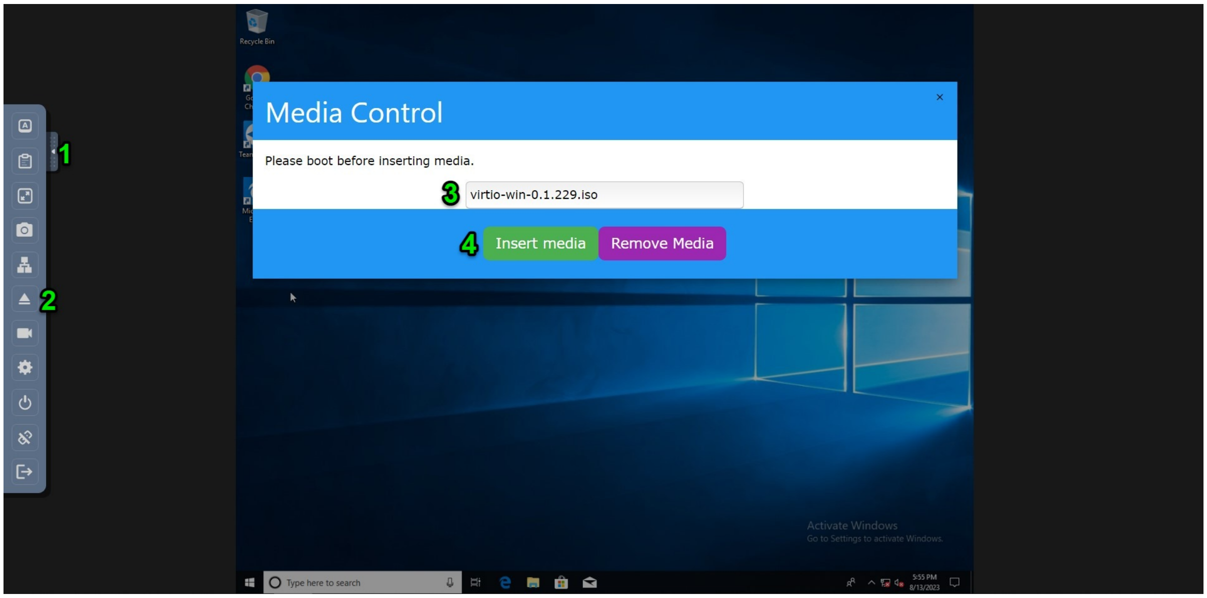
- Inside the tool panel, find and click on the **Eject** icon. Activating this icon will present the Media Control Modal Box.

Step 3: Select from the ISO Dropdown

- Within the Modal Box, locate and click the **ISO Dropdown**.
- This dropdown will display all ISO files saved on the ForensicVM server.
- Scroll and click on the desired ISO file or virtual CD-ROM you wish to insert.

Step 4: Confirm the Insertion

- After selecting the desired ISO, click the **Insert Media** button.
- This action mounts the chosen ISO as a virtual CD-ROM.
- A success notification will appear, signaling that the insertion was successful.



Media Control

Please boot before inserting media.

virtio-win-0.1.229.iso

Fig. 7.176: Inserting ISO using the Web Interface

7.14.4 Run programs and utilities from ISO

After successfully uploading and inserting an ISO into the virtualized forensic environment, the next step is to leverage the tools within. This section will guide you through accessing and utilizing the programs and utilities contained in the ISO.

Step 1: Locate the Virtual CD-ROM Drive

- Once you've inserted the ISO as a virtual CD-ROM, navigate to your operating system's file explorer or equivalent.
- Locate the virtual CD-ROM drive which should appear similar to a physical CD-ROM drive.
- Open the drive to view its contents.

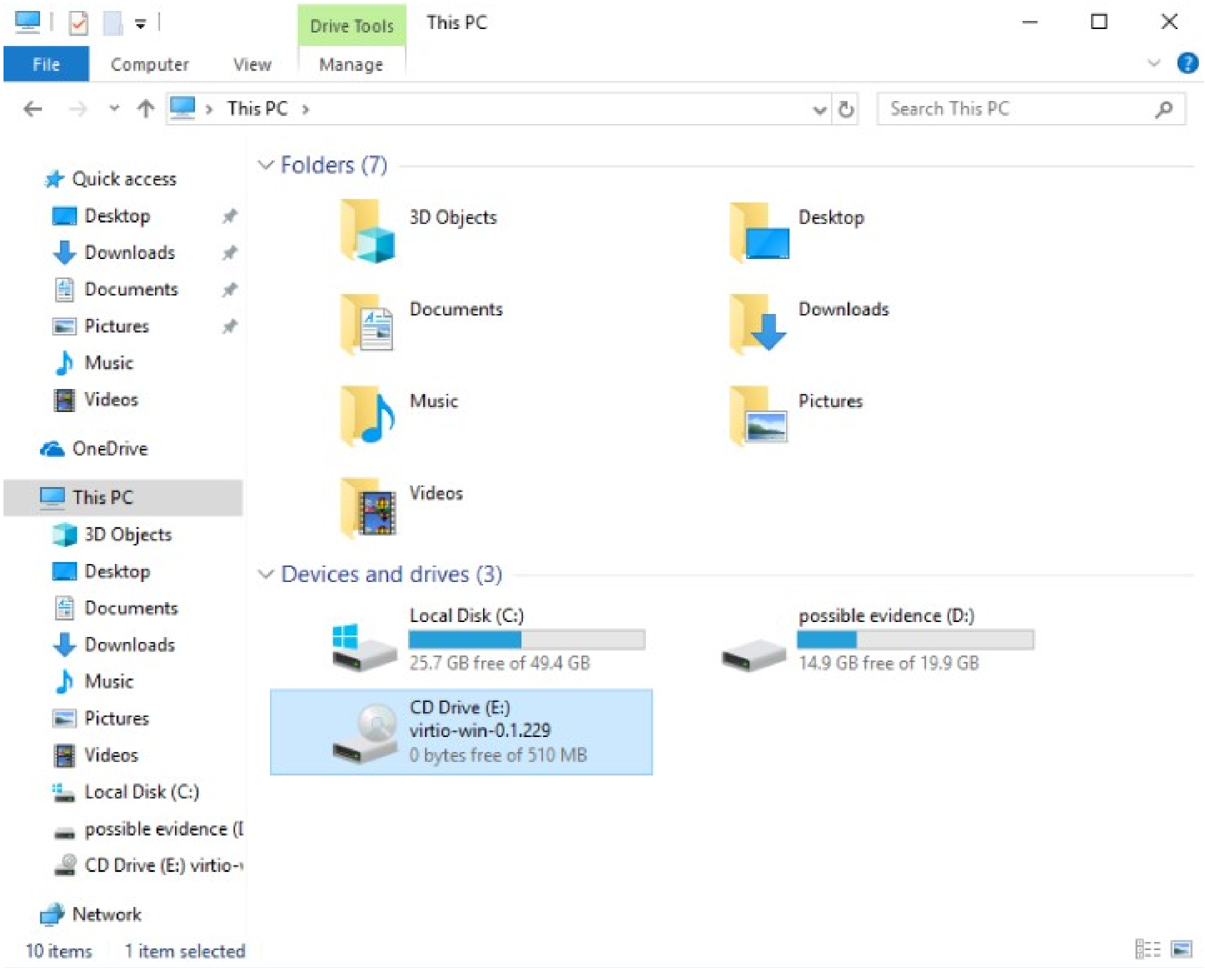
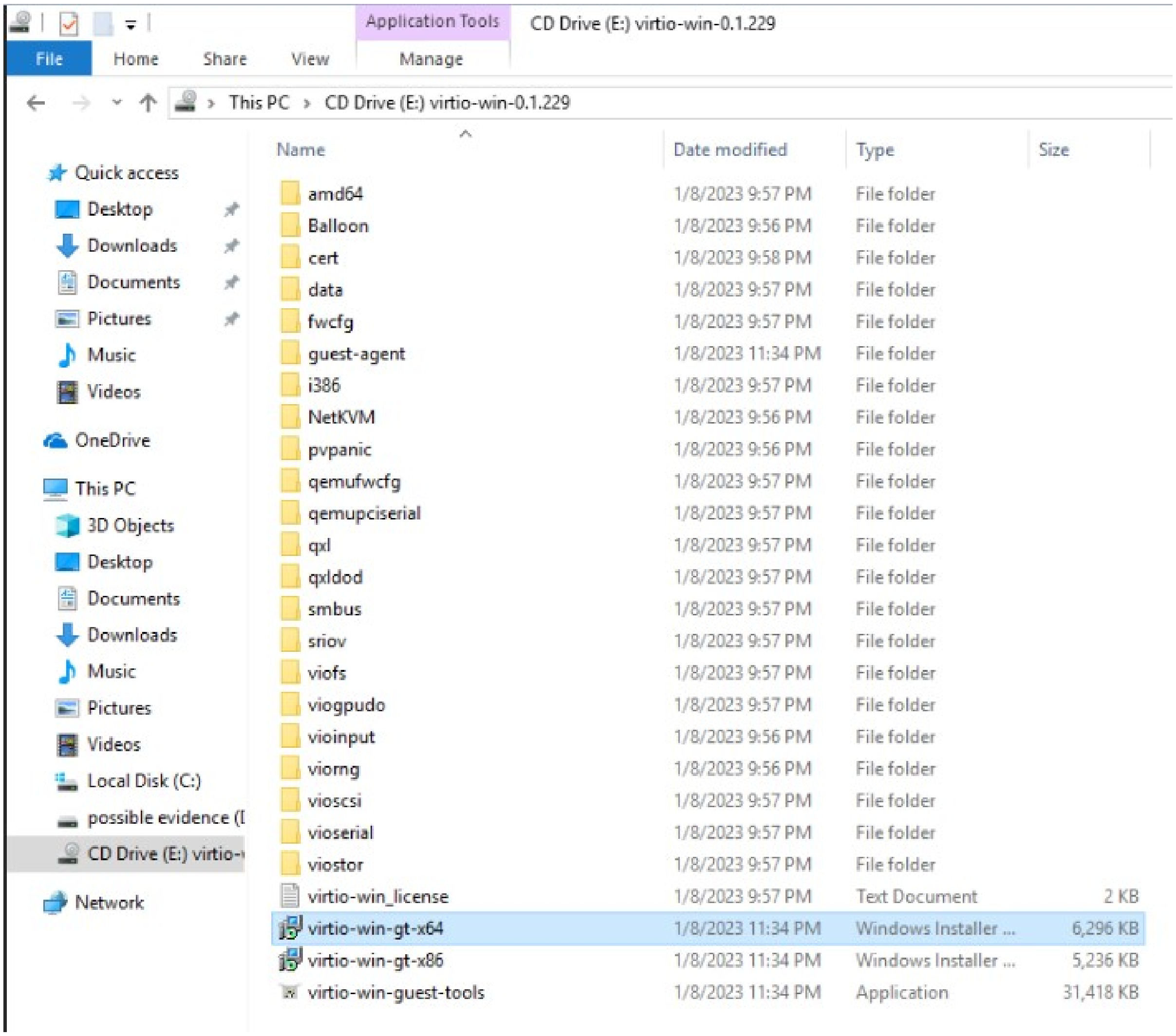


Fig. 7.177: Locating the Virtual CD-ROM Drive

Step 2: Identify and Launch the Desired Tool

- Inside the virtual CD-ROM content, sift through the directories and files to locate the specific program or tool you intend to run.
- Once found, initiate the program or utility. Depending on the nature of the tool, you might have to run it as an administrator or follow specific launch procedures.

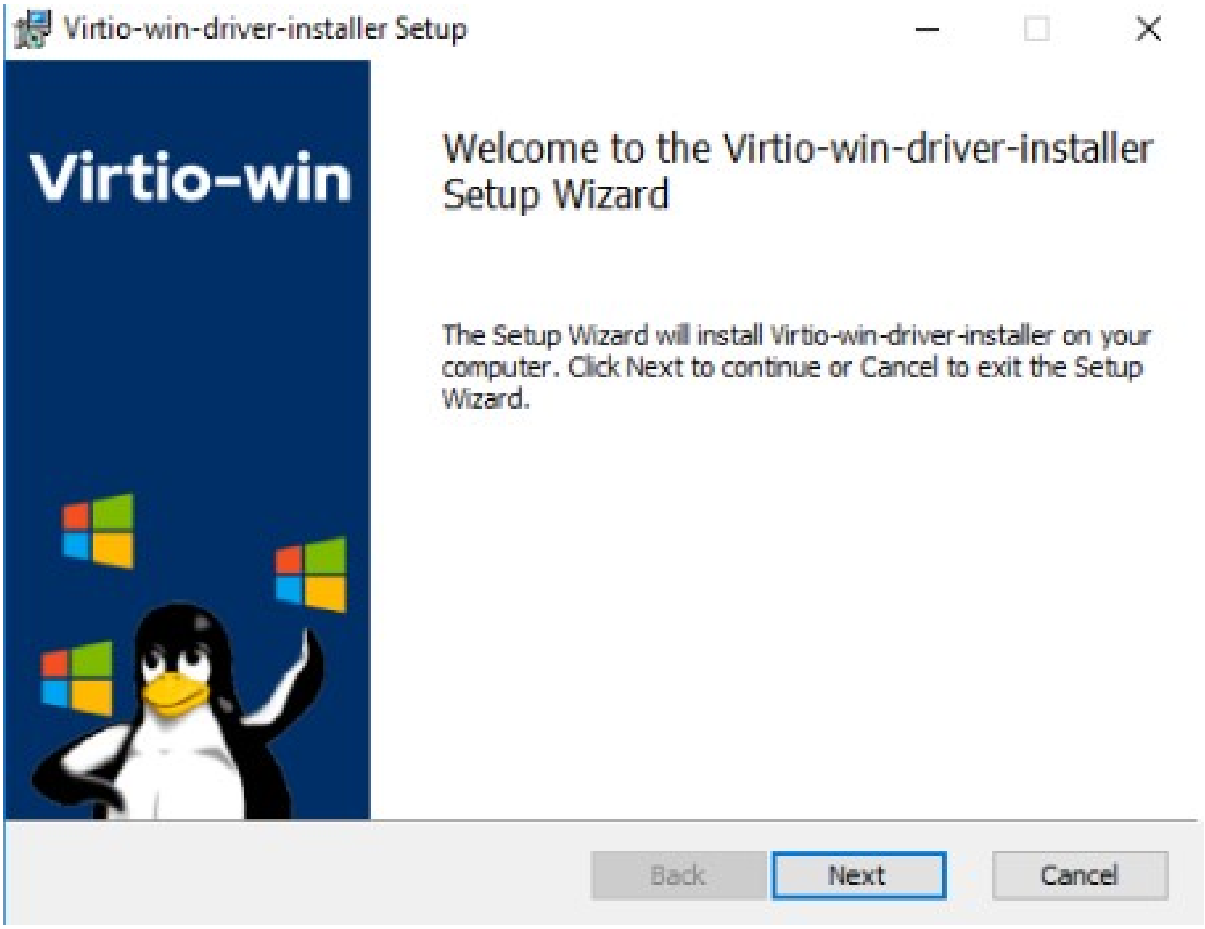


Name	Date modified	Type	Size
amd64	1/8/2023 9:57 PM	File folder	
Balloon	1/8/2023 9:56 PM	File folder	
cert	1/8/2023 9:58 PM	File folder	
data	1/8/2023 9:57 PM	File folder	
fwcfg	1/8/2023 9:57 PM	File folder	
guest-agent	1/8/2023 11:34 PM	File folder	
i386	1/8/2023 9:57 PM	File folder	
NetKVM	1/8/2023 9:56 PM	File folder	
pvpanic	1/8/2023 9:56 PM	File folder	
qemufwcfg	1/8/2023 9:57 PM	File folder	
qemupciserial	1/8/2023 9:57 PM	File folder	
qxl	1/8/2023 9:57 PM	File folder	
qxldod	1/8/2023 9:57 PM	File folder	
smbus	1/8/2023 9:57 PM	File folder	
sriov	1/8/2023 9:57 PM	File folder	
viofs	1/8/2023 9:57 PM	File folder	
viogpudo	1/8/2023 9:57 PM	File folder	
vioinput	1/8/2023 9:56 PM	File folder	
viorng	1/8/2023 9:56 PM	File folder	
vioscsi	1/8/2023 9:57 PM	File folder	
vioserial	1/8/2023 9:57 PM	File folder	
viostor	1/8/2023 9:57 PM	File folder	
virtio-win_license	1/8/2023 9:57 PM	Text Document	2 KB
virtio-win-gt-x64	1/8/2023 11:34 PM	Windows Installer ...	6,296 KB
virtio-win-gt-x86	1/8/2023 11:34 PM	Windows Installer ...	5,236 KB
virtio-win-guest-tools	1/8/2023 11:34 PM	Application	31,418 KB

Fig. 7.178: Launching Tools from the ISO

Step 3: Adhere to the Program's Instructions

- Each forensic tool or utility will have its set of instructions, either embedded within its interface or provided as a separate README file.
- Follow these instructions meticulously to ensure accurate and efficient processing.
- Should your investigation involve extracting or marking potential evidence, utilize the "Possible Evidence" virtual drive. This virtual drive is specially designed within ForensicVM to store and segregate potential pieces of evidence without contaminating the original data.



Virtio-win-driver-installer Setup

Welcome to the Virtio-win-driver-installer Setup Wizard

The Setup Wizard will install Virtio-win-driver-installer on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

Fig. 7.179: Using the Program within ForensicVM

7.14.5 Bootable Media

There are instances during a forensic investigation where analysts may need to interact directly with the operating system or leverage specific tools that necessitate booting into a virtual machine (VM). ForensicVM's virtual CD-ROM drive has a unique characteristic: it can only accept CD-ROM insertions when the VM is running.

The booting process of a CD-ROM involves the following steps:

1. Boot into the operating system or access the BIOS/UEFI screen.
2. Insert the virtual CD-ROM into the drive.
3. Perform a reboot or reset operation.
4. Access the BIOS or UEFI by pressing the "ESC" key.
5. Navigate to the boot device selection menu and confirm your choice.

Method 1: Boot from Virtual CD-ROM Post-OS Bootup (BIOS showcase)

Step 1: Boot into the Operating System

- Initiate a boot sequence and load the operating system.

Tip: While the example showcases a user login, you don't necessarily need to log in. Simply booting into the operating system is sufficient.

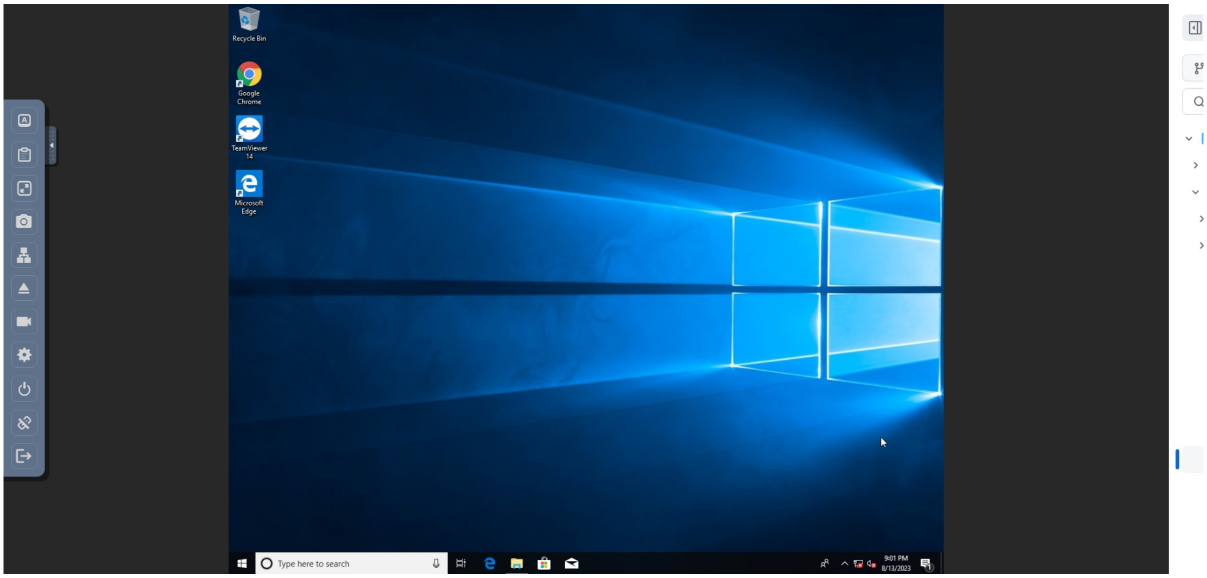
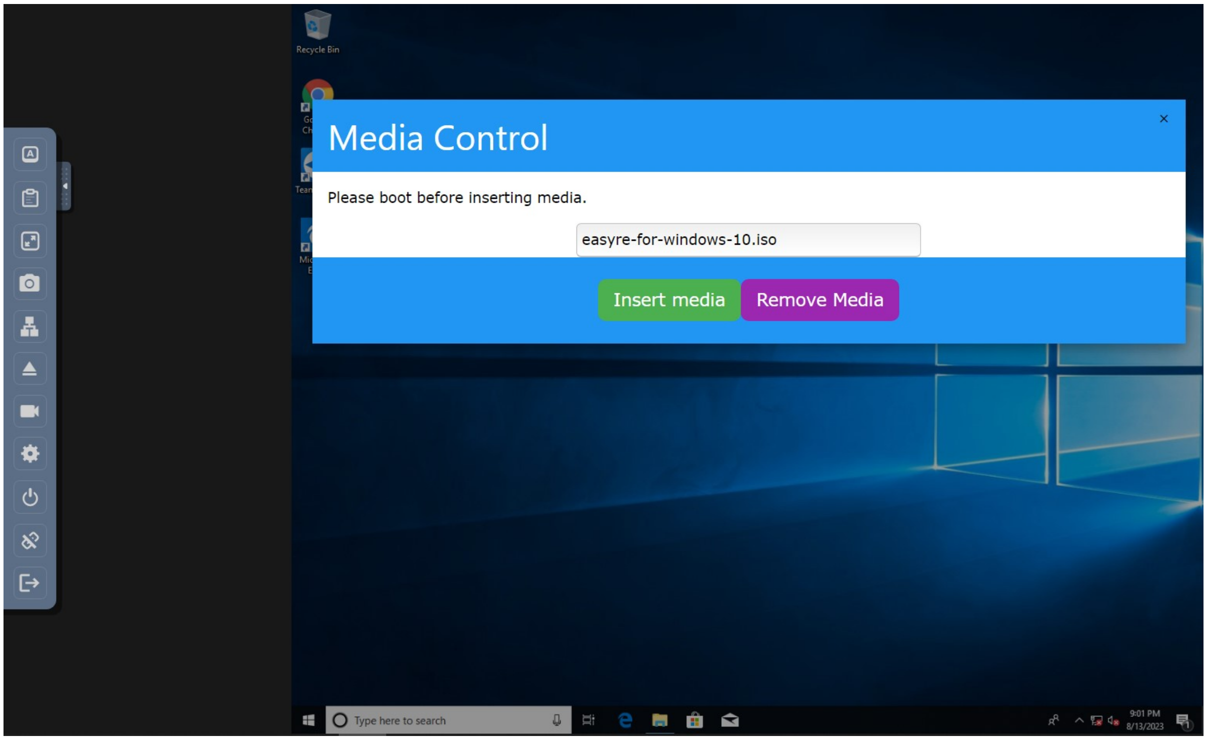


Fig. 7.180: Operating System Boot Screen

Step 2: Insert the Virtual Bootable CD-ROM

- Adhere to the previous guidelines to insert the virtual media into the CD-ROM drive.



Media Control

Please boot before inserting media.

easyre-for-windows-10.iso

Fig. 7.181: Inserting Virtual Media

Step 3: Initiate a System Restart

- Command the operating system to restart and wait for the BIOS boot screen to emerge.

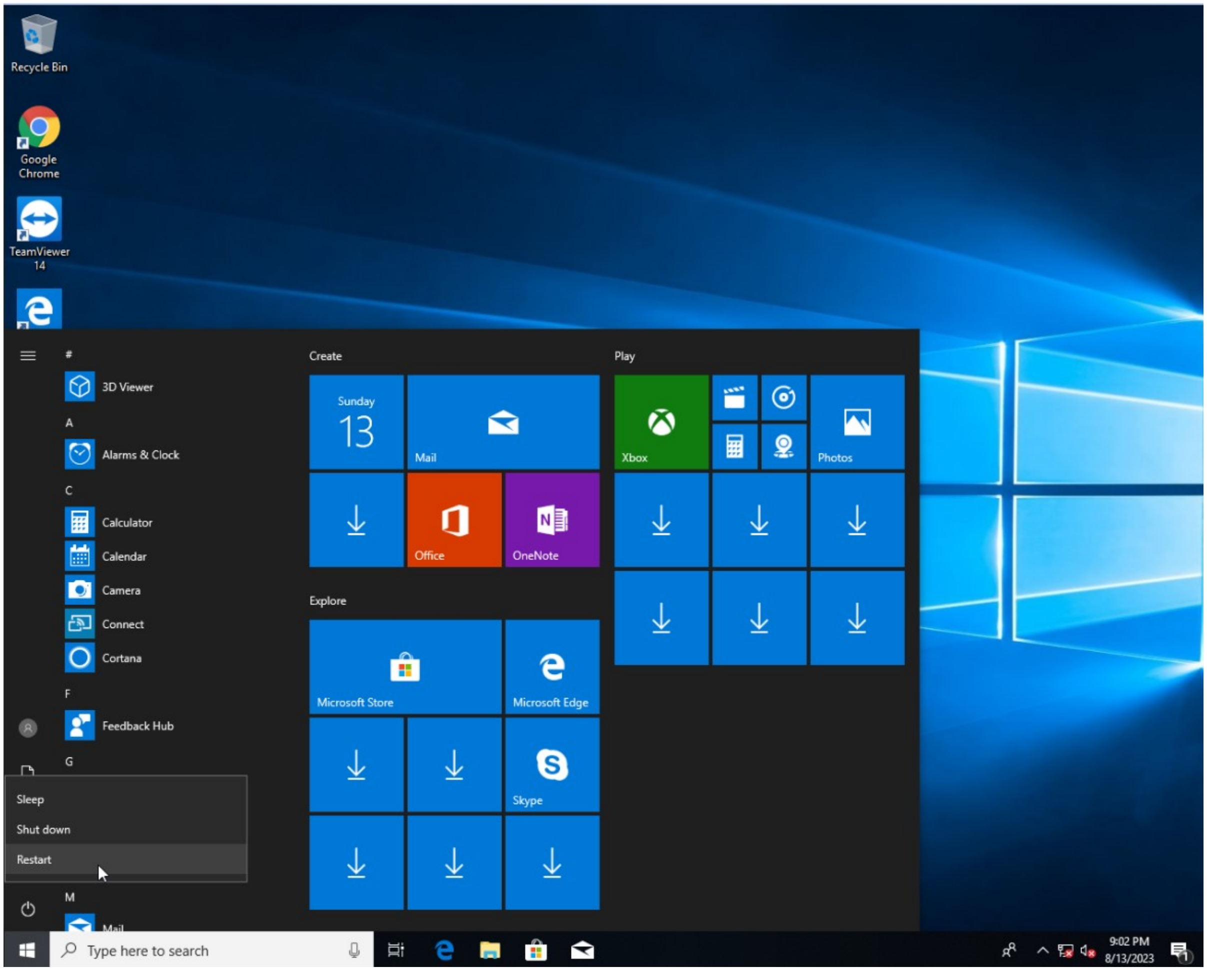


Fig. 7.182: System Restart

Step 4: Access Boot Options with "ESC"

- As the system initializes, press the "ESC" key within a 15-second window to access the boot options.

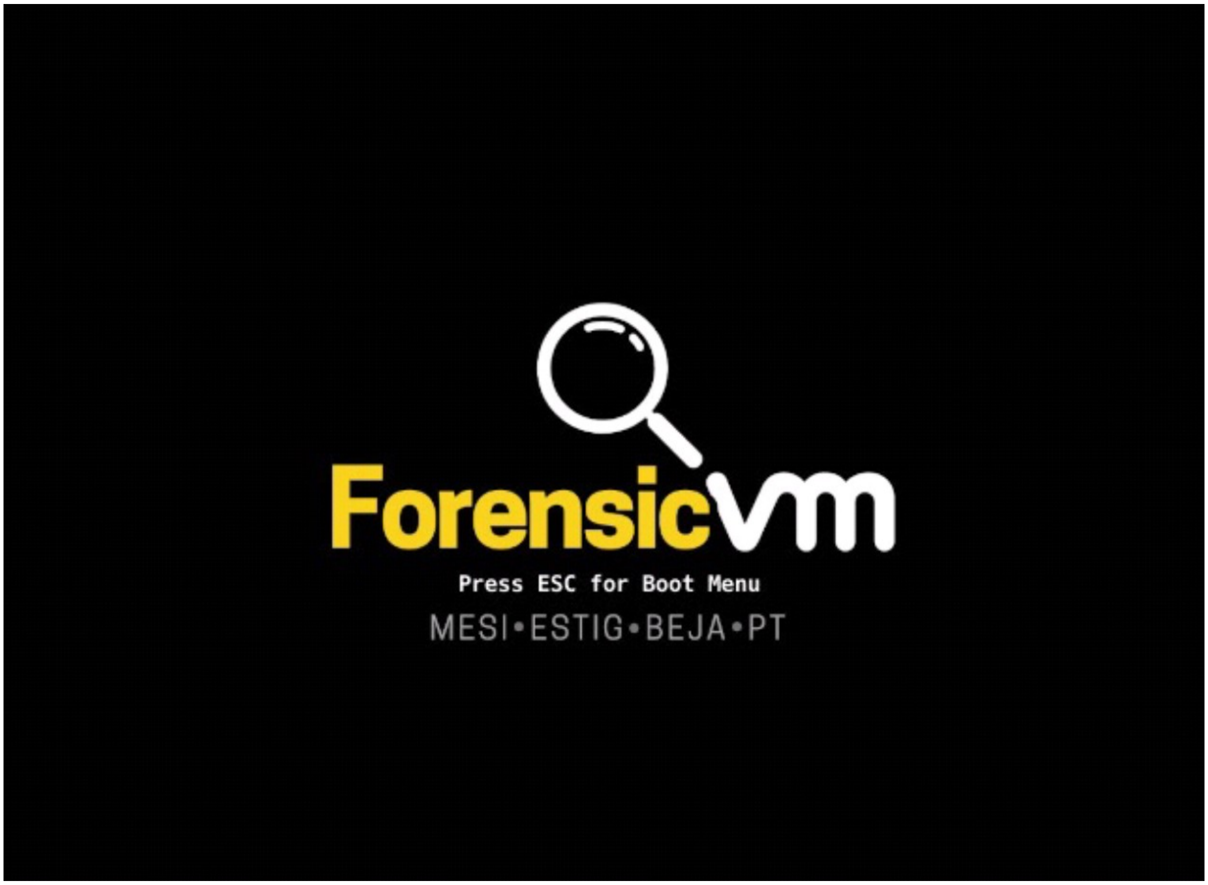
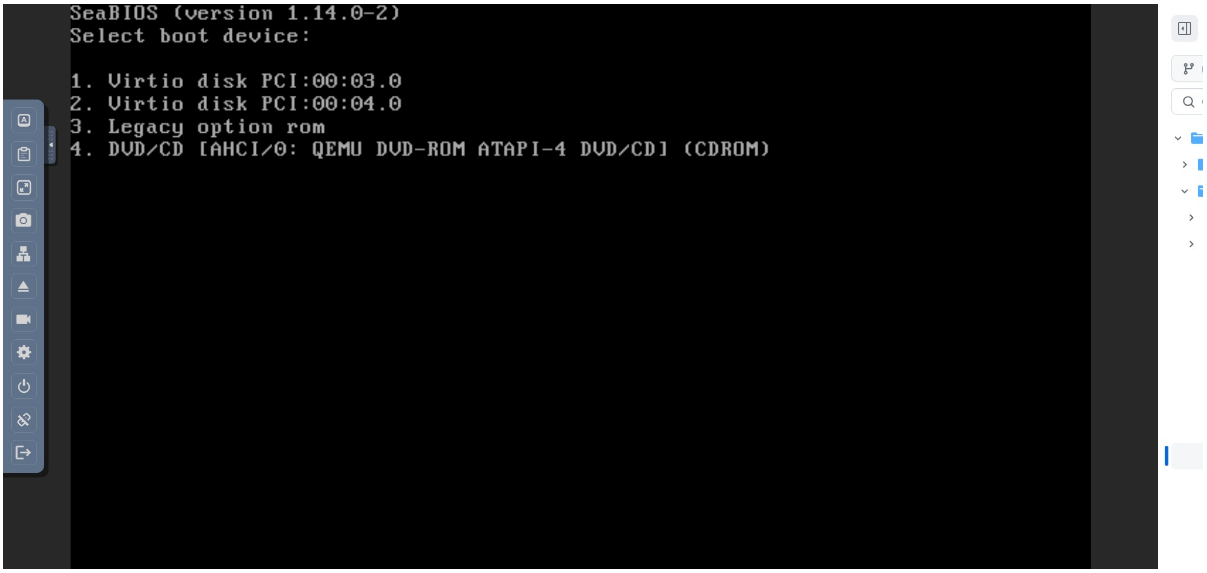


Fig. 7.183: Boot Options Screen

Step 5: Opt for the Virtual CD-ROM Drive

- From the available boot options, select the corresponding number for the virtual CD-ROM or DVD-ROM drive. For instance, in the example given, you'd press "4".

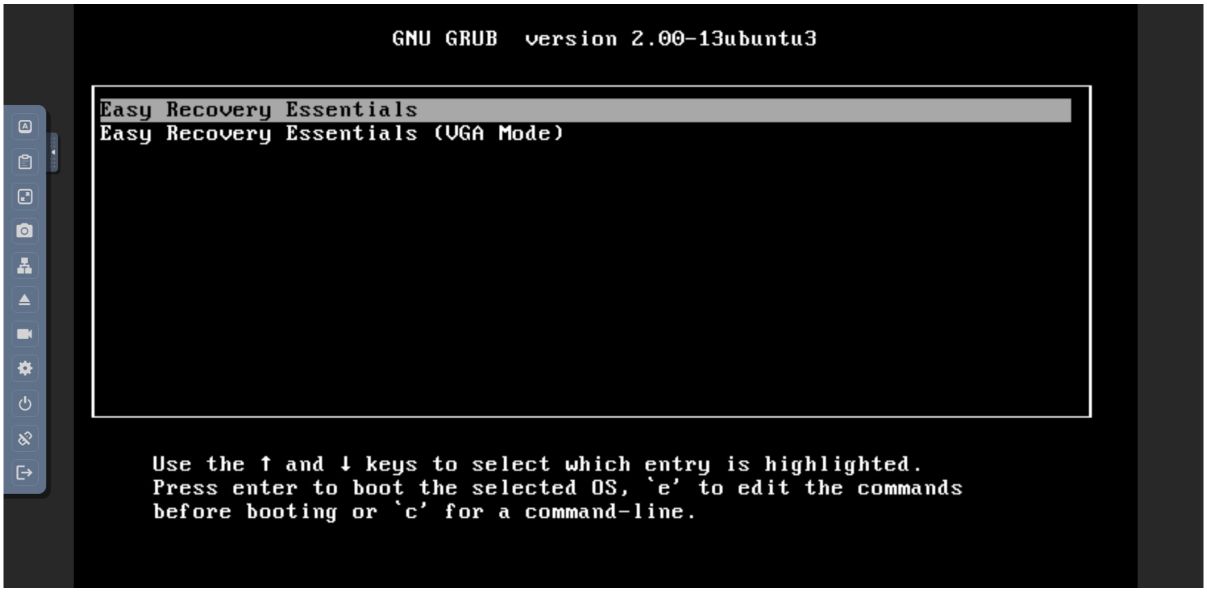


```
SeaBIOS (version 1.14.0-2)
Select boot device:

1. Virtio disk PCI:00:03.0
2. Virtio disk PCI:00:04.0
3. Legacy option rom
4. DVD/CD [AHCI/0: QEMU DVD-ROM ATAPI-4 DVD/CD] (CDROM)
```

Fig. 7.184: Selecting Virtual CD-ROM

Step 6: Boot into the ISO

- If the operations proceed without hitches, the virtual media will boot. Depending on the media's nature, it might present a selection menu or lead straight to its primary function.

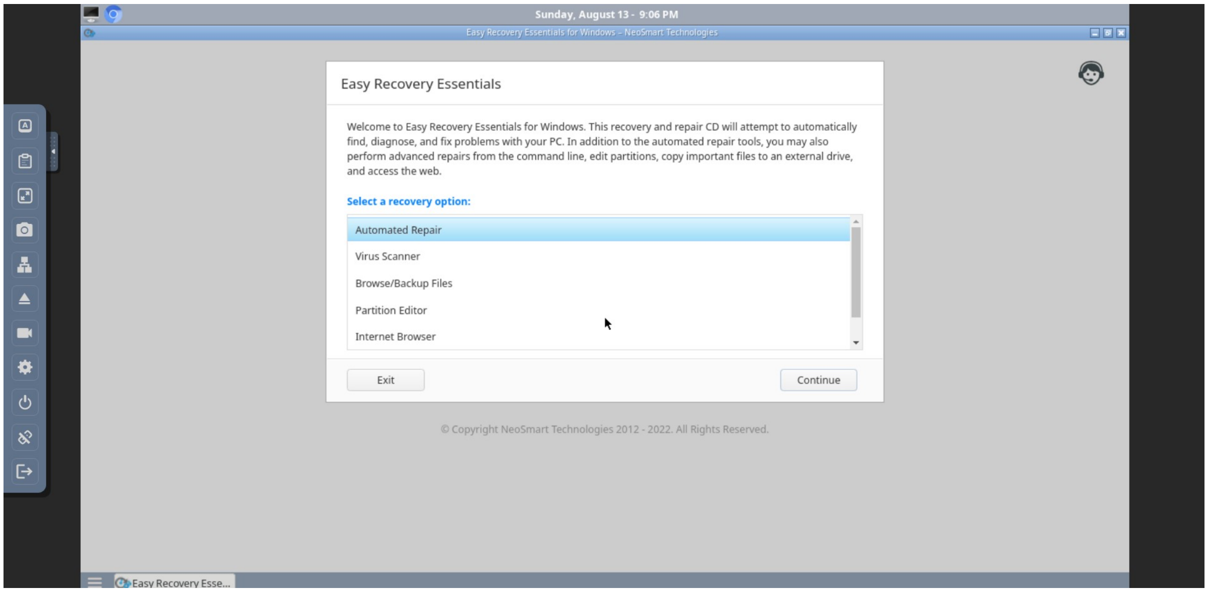


```
                    GNU GRUB  version 2.00-13ubuntu3

 Easy Recovery Essentials
 Easy Recovery Essentials (VGA Mode)

     Use the ↑ and ↓ keys to select which entry is highlighted.
     Press enter to boot the selected OS, `e' to edit the commands
     before booting or `c' for a command-line.
```

Fig. 7.185: Booting into ISO

Step 7: Operate the Booted Tools

- With the ISO booted, you can now access and employ the forensic tools contained therein, tailoring your investigative approach based on the utilities available.



Sunday, August 13 - 9:06 PM
Easy Recovery Essentials for Windows – NeoSmart Technologies
Easy Recovery Essentials

Welcome to Easy Recovery Essentials for Windows. This recovery and repair CD will attempt to automatically find, diagnose, and fix problems with your PC. In addition to the automated repair tools, you may also perform advanced repairs from the command line, edit partitions, copy important files to an external drive, and access the web.

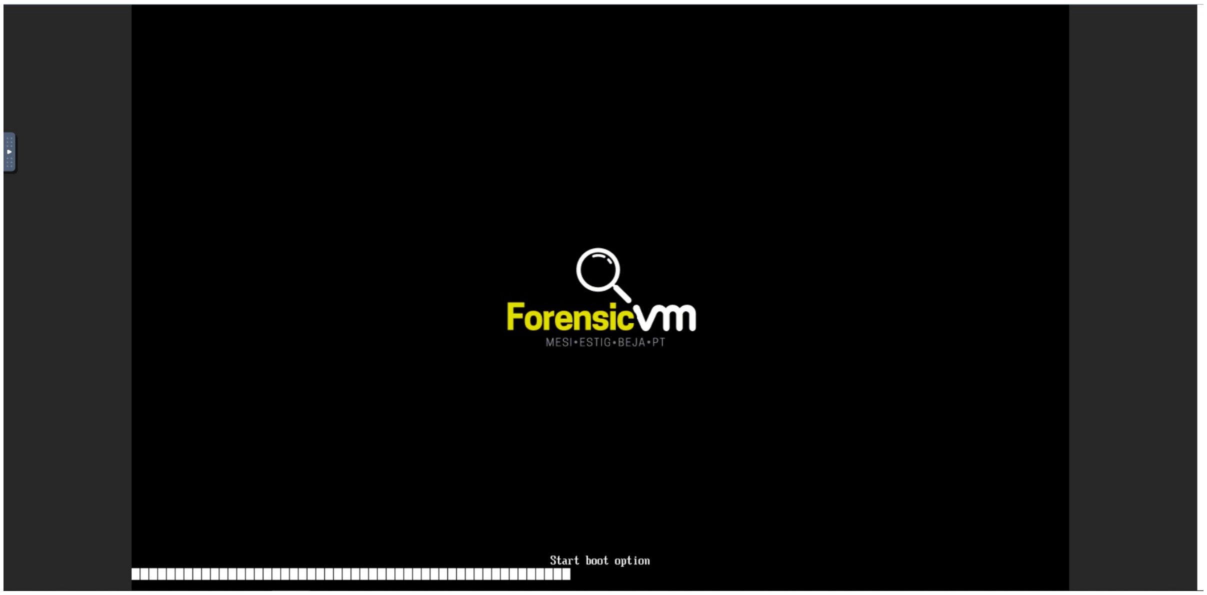
Select a recovery option:
Automated Repair
Virus Scanner
Browse/Backup Files
Partition Editor
Internet Browser
Exit
Continue
© Copyright NeoSmart Technologies 2012 - 2022. All Rights Reserved.
Easy Recovery Esse...

Fig. 7.186: Accessing Tools from Booted ISO

Method 2: Boot from Virtual CD-ROM at Boot Time (Showcasing UEFI)

Step 1: Access the UEFI **Boot Options**

- Power on the ForensicVM.
- Rapidly access the web interface and press the “ESC” key to intercept the boot sequence.

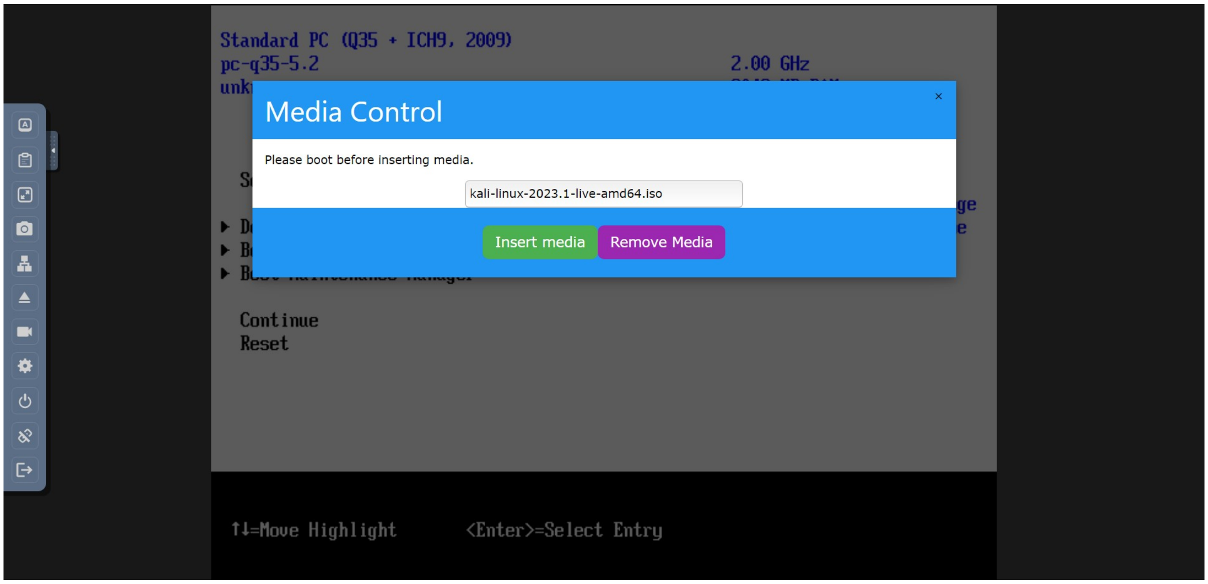


Start boot option

Fig. 7.187: Accessing UEFI Boot Options

Step 2: Insert the Bootable ISO into Virtual CD-ROM

- Load your desired bootable ISO into the virtual CD-ROM. Refer to the previously provided steps if needed.


```
Standard PC (Q35 + ICH9, 2009)
pc-q35-5.2                                       2.00 GHz
unk
```

Media Control

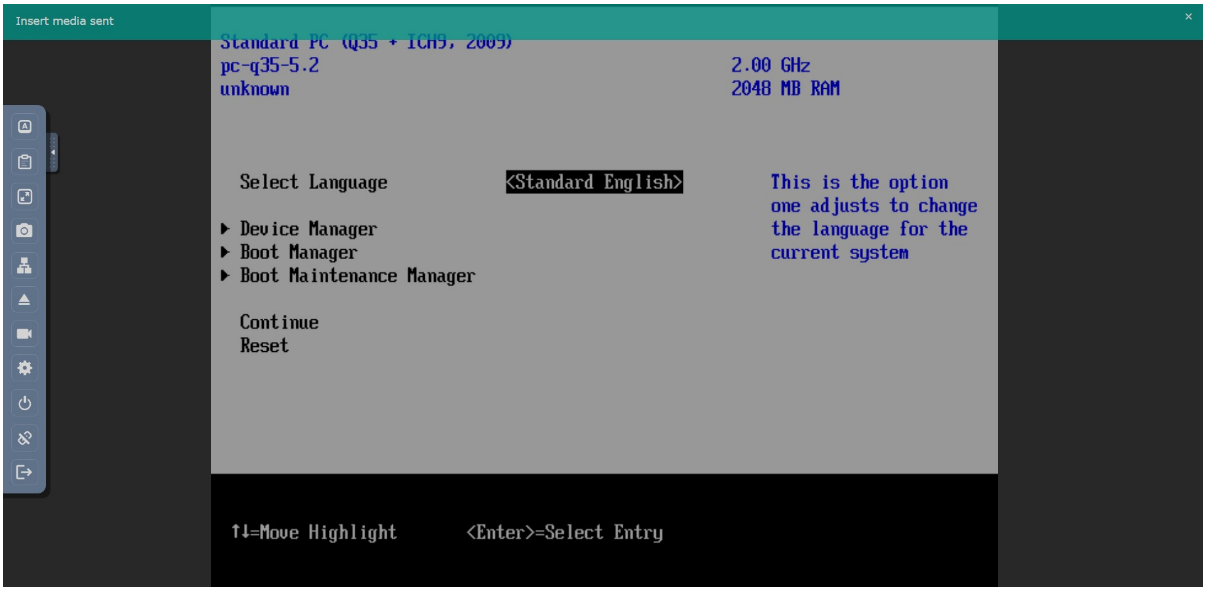
Please boot before inserting media.

kali-linux-2023.1-live-amd64.iso

Fig. 7.188: Inserting Bootable ISO

Step 3: Acknowledge the Successful Insertion Notification

- The web console screen should display a “Insert media sent” message, confirming the ISO’s successful insertion into the drive.



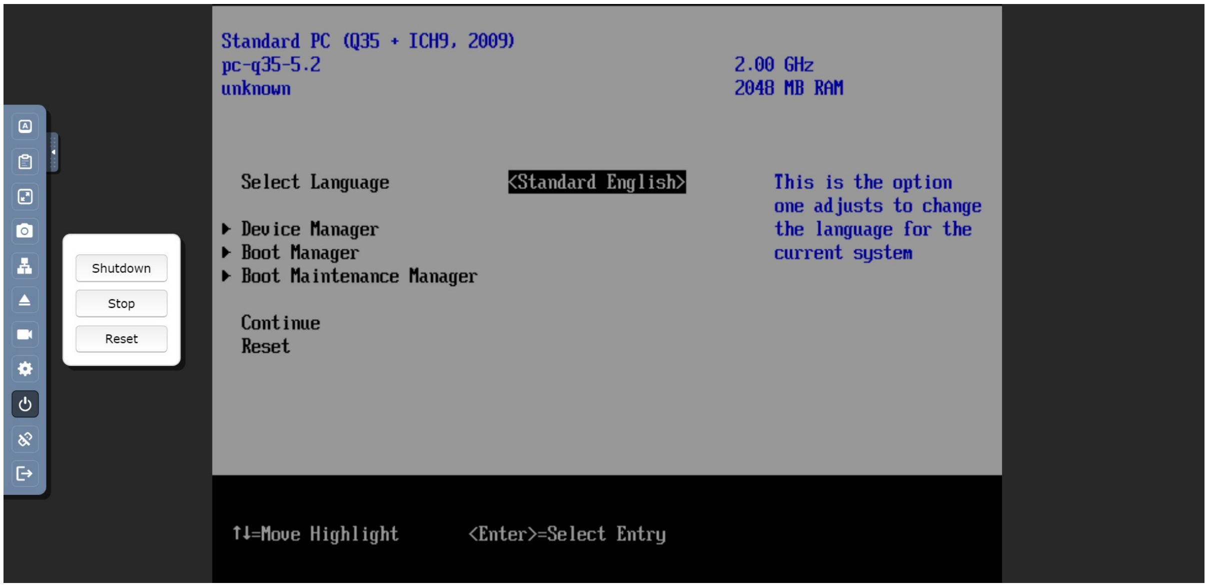
Insert media sent

```
Standard PC (Q35 + ICH9, 2009)
pc-q35-5.2                                           2.00 GHz
unknown                                              2048 MB RAM

  Select Language          <Standard English>     This is the option
                                                  one adjusts to change
▶ Device Manager                                  the language for the
▶ Boot Manager                                    current system
▶ Boot Maintenance Manager

  Continue
  Reset

 ↑↓=Move Highlight      <Enter>=Select Entry
```

Fig. 7.189: Successful Insertion Notification

Step 4: Command a Reset of ForensicVM

- Trigger a system reset by clicking the “Reset” button. The ForensicVM will undergo a reboot process.



```
Standard PC (Q35 + ICH9, 2009)
pc-q35-5.2                                           2.00 GHz
unknown                                              2048 MB RAM

  Select Language          <Standard English>     This is the option
                                                  one adjusts to change
▶ Device Manager                                  the language for the
▶ Boot Manager                                    current system
▶ Boot Maintenance Manager

  Continue
  Reset

 ↑↓=Move Highlight      <Enter>=Select Entry
```

Fig. 7.190: Resetting ForensicVM

Step 5: Navigate to UEFI **Menu**

- Upon reboot, press the “ESC” key once more. This will usher you into the UEFI menu.

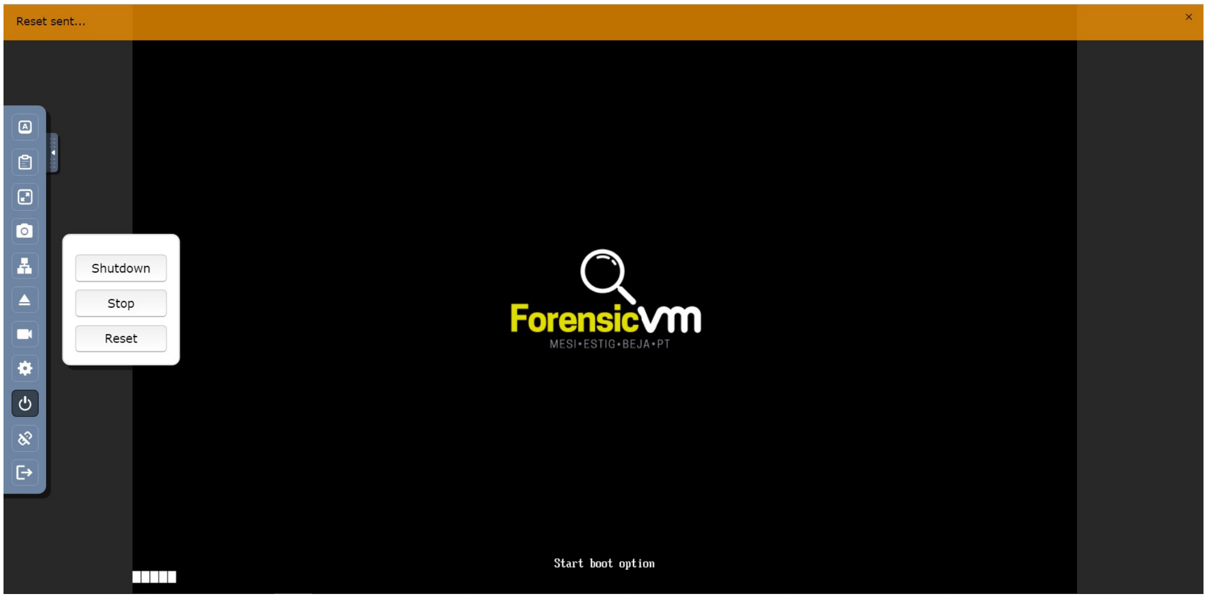
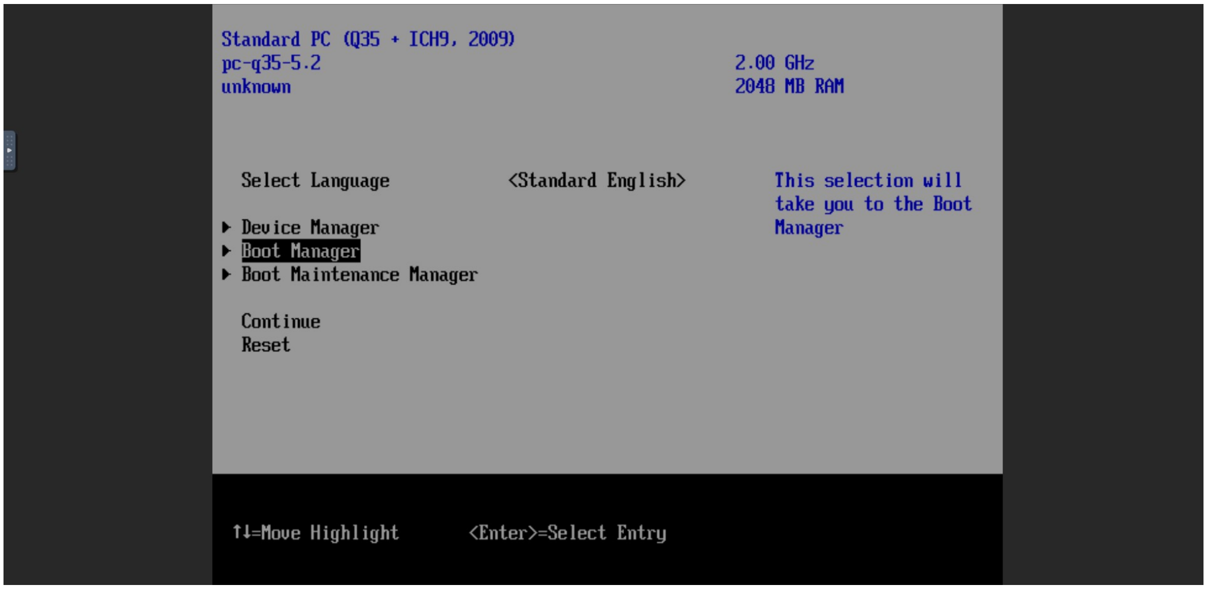


Fig. 7.191: Accessing UEFI Menu

Step 6: Opt for "Boot Manager"

- In the UEFI menu, navigate to the "Boot Manager" using arrow keys and confirm your selection with the <ENTER> key.

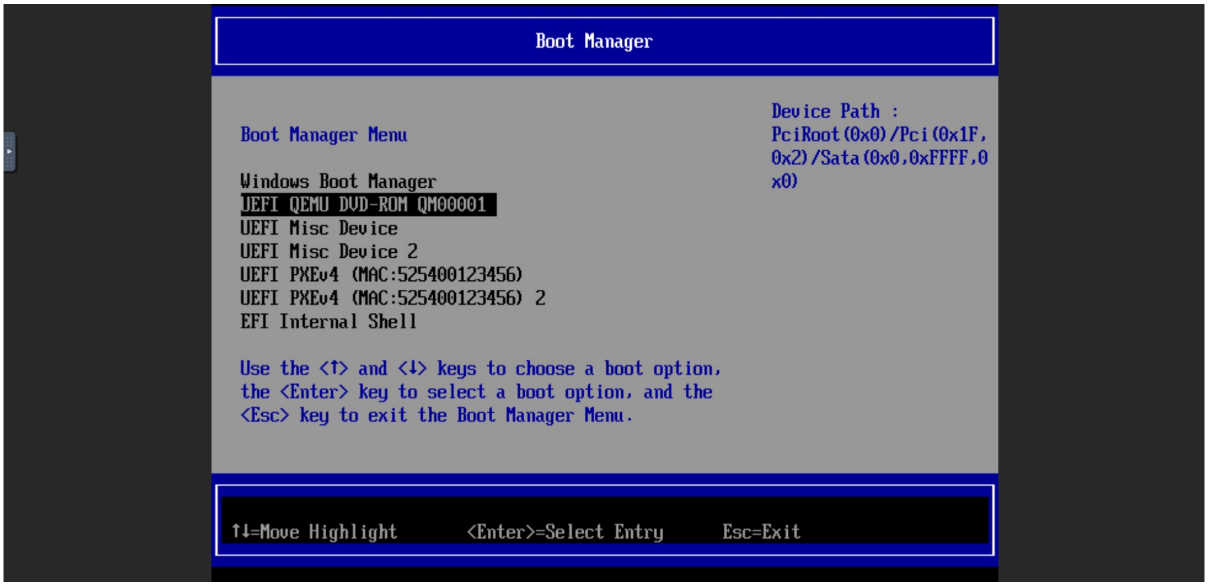


```
Standard PC (Q35 + ICH9, 2009)
pc-q35-5.2                                           2.00 GHz
unknown                                              2048 MB RAM


  Select Language            <Standard English>        This selection will
                                                       take you to the Boot
▶ Device Manager                                       Manager
▶ Boot Manager
▶ Boot Maintenance Manager

  Continue
  Reset


 ↑↓=Move Highlight       <Enter>=Select Entry
```

Fig. 7.192: Selecting Boot Manager

Step 7: Choose “UEFI QEMU **DVD-ROM”**

- From the available options, locate and select “UEFI QEMU DVD-ROM”. Use the arrow keys for navigation and confirm with <ENTER>.



```
                          Boot Manager

                                                   Device Path :
 Boot Manager Menu                                 PciRoot(0x0)/Pci(0x1F,
                                                   0x2)/Sata(0x0,0xFFFF,0
 Windows Boot Manager                              x0)
 UEFI QEMU DVD-ROM QM00001
 UEFI Misc Device
 UEFI Misc Device 2
 UEFI PXEv4 (MAC:525400123456)
 UEFI PXEv4 (MAC:525400123456) 2
 EFI Internal Shell

 Use the <↑> and <↓> keys to choose a boot option,
 the <Enter> key to select a boot option, and the
 <Esc> key to exit the Boot Manager Menu.

 ↑↓=Move Highlight       <Enter>=Select Entry      Esc=Exit
```

Fig. 7.193: UEFI QEMU DVD-ROM Option

Step 8: Await the Virtual CD-ROM Boot Sequence

- If a selection menu is presented, choose the appropriate option. If not, patiently wait as the ForensicVM initializes the ISO media.

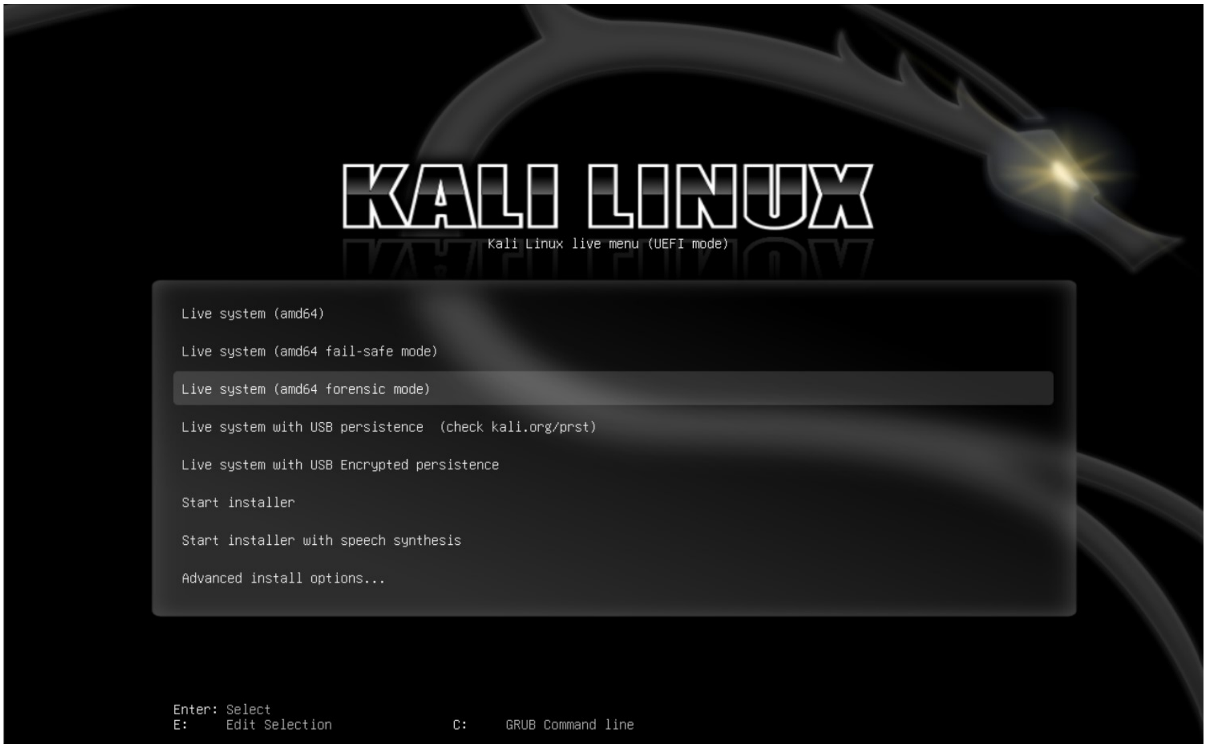

KALI LINUX
Kali Linux live menu (UEFI mode)
Live system (amd64)
Live system (amd64 fail-safe mode)
Live system (amd64 forensic mode)
Live system with USB persistence (check kali.org/prst)
Live system with USB Encrypted persistence
Start installer
Start installer with speech synthesis
Advanced install options...
Enter: Select
E: Edit Selection
C: GRUB Command line

Fig. 7.194: Virtual CD-ROM Booting

Step 9: Access and Execute Forensic Tools

- Once booted, you can now select and run your preferred forensic tools. This example demonstrates utilizing forensic tools from Kali Linux.

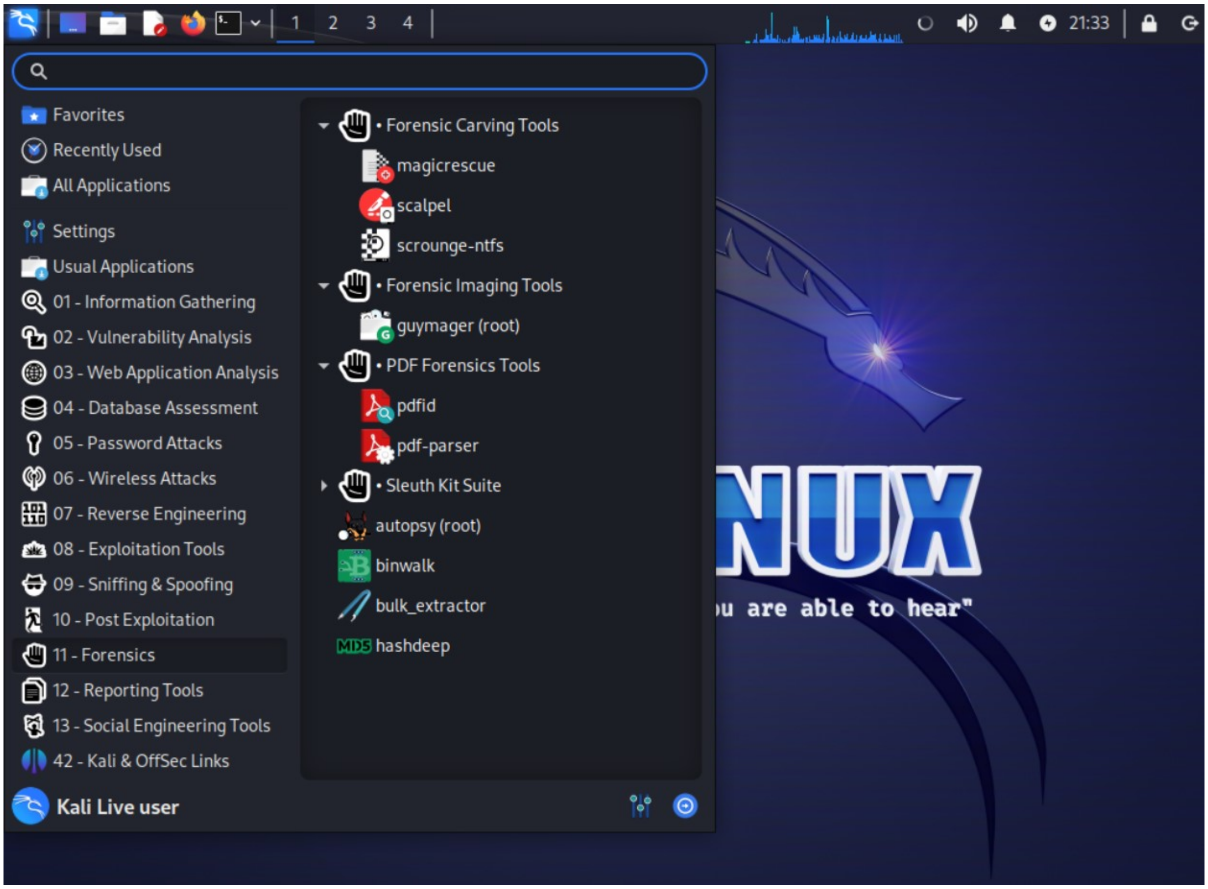


Fig. 7.195: Kali Linux Forensic Tools

7.14.6 Eject ISO / Web Eject CD-ROM

There are two methods to eject an ISO from the virtual CD-ROM drive:

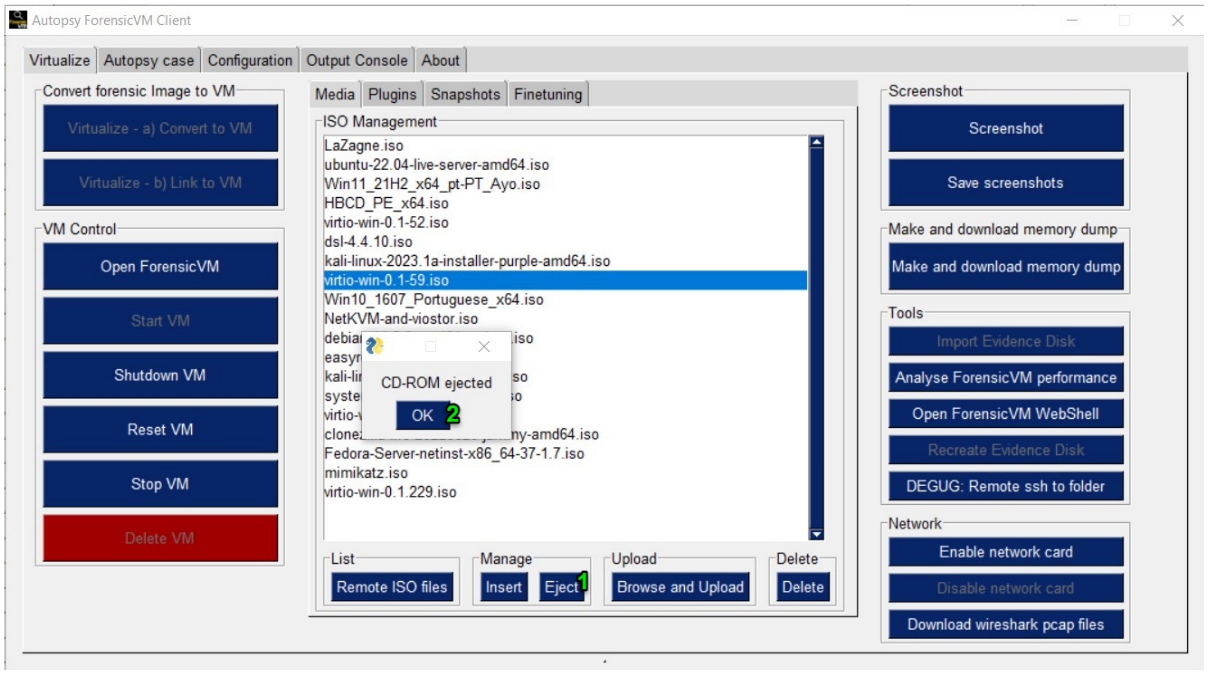
1. Using the Autopsy ForensicVM Client Plugin interface.
2. Using the web screen interface.

Below are detailed steps for each method:

Method 1: Eject using the Autopsy ForensicVM Client Plugin Interface

Step 1: Activate the "Eject" Function

- Click on the "Eject" button. A confirmation will appear, indicating that the media has been successfully ejected.



CD-ROM ejected

Fig. 7.196: Ejecting via Autopsy ForensicVM Client Plugin

Method 2: Eject using the Web Screen Interface

Step 1: Access the Web Toolbar

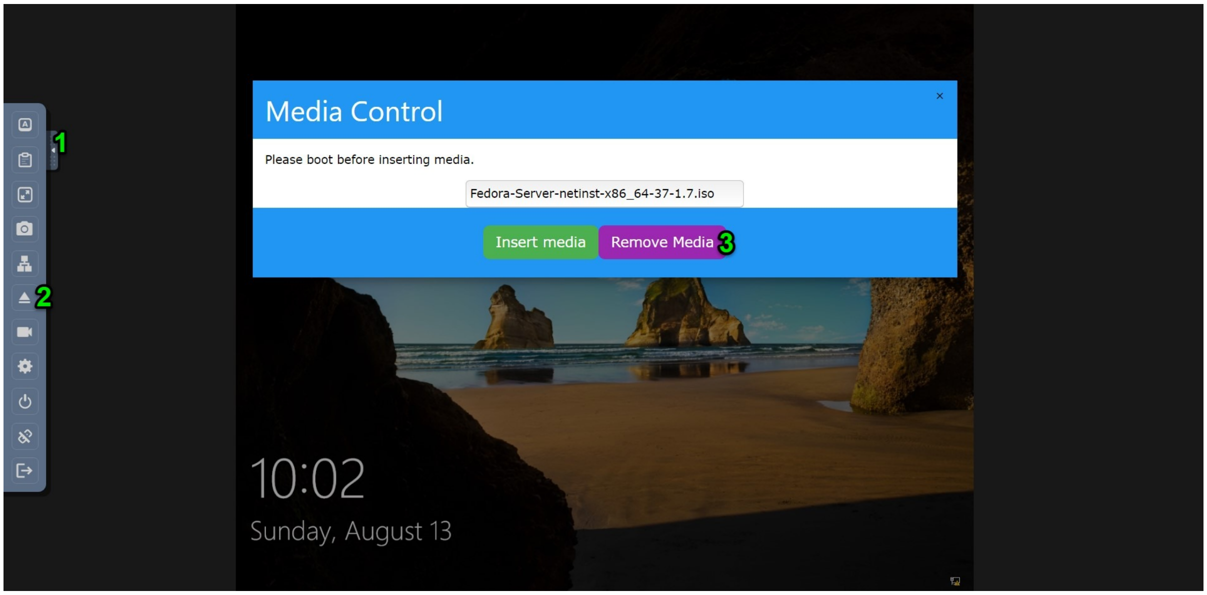
- Click on the open bar icon. This action will expand the web toolbar for further options.

Step 2: Initiate the Eject Process

- Click on the "Eject" icon (depicted with a "2" in the reference image). This will bring up the Media Control Modal Panel.

Step 3: Finalize the Ejection

- Click the "Remove Media" button (marked as "3" in the reference image). The media will subsequently be disengaged from the virtual CD-ROM drive.



Media Control

Please boot before inserting media.

Fedora-Server-netinst-x86_64-37-1.7.iso

Fig. 7.197: Ejecting via Web Screen Interface

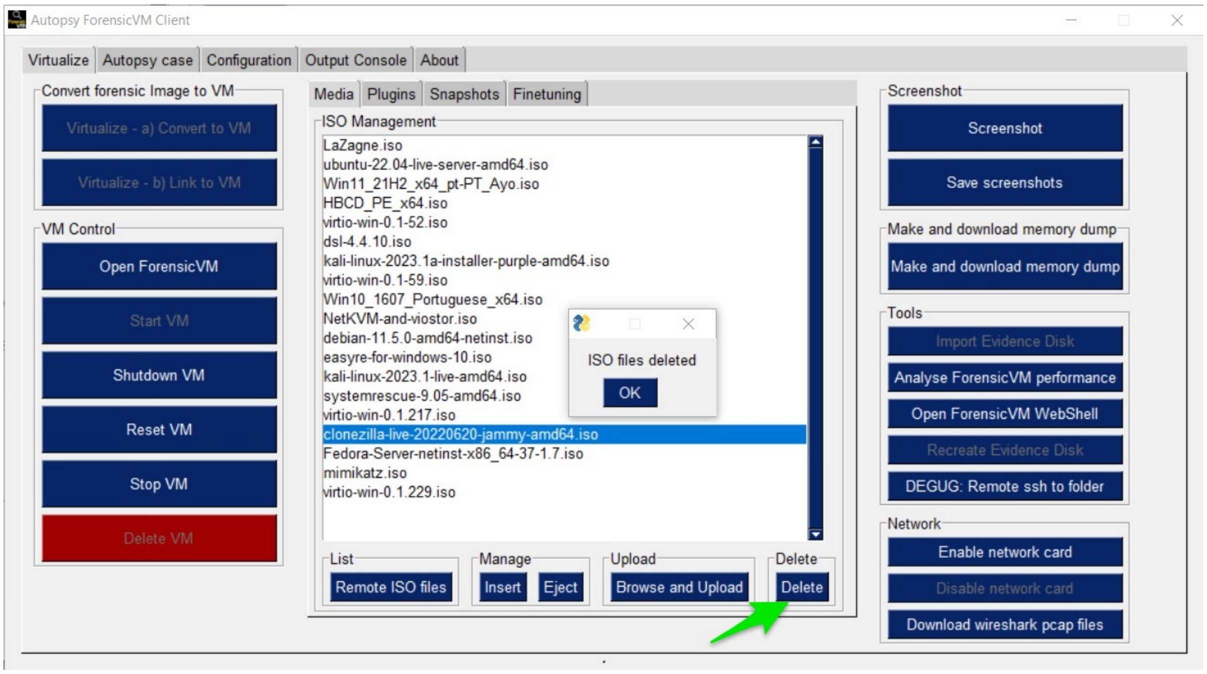
7.14.7 Delete ISO Using the Autopsy ForensicVM Client Plugin Interface

To delete an ISO file, follow the steps below:

Step 1: Navigate to the Media Panel within the Autopsy ForensicVM Client Plugin interface.

Step 2: Identify and select the ISO file you wish to delete.

Step 3: Click on the "Delete" button associated with the desired ISO file.



```
LaZagne.iso
ubuntu-22.04-live-server-amd64.iso
Win11_21H2_x64_pt-PT_Ayo.iso
HBCD_PE_x64.iso
virtio-win-0.1-52.iso
dsl-4.4.10.iso
kali-linux-2023.1a-installer-purple-amd64.iso
virtio-win-0.1-59.iso
Win10_1607_Portuguese_x64.iso
NetKVM-and-viostor.iso
debian-11.5.0-amd64-netinst.iso
easyre-for-windows-10.iso
kali-linux-2023.1-live-amd64.iso
systemrescue-9.05-amd64.iso
virtio-win-0.1.217.iso
clonezilla-live-20220620-jammy-amd64.iso
Fedora-Server-netinst-x86_64-37-1.7.iso
mimikatz.iso
virtio-win-0.1.229.iso
```

ISO files deleted

Fig. 7.198: Deleting an ISO Media

Warning: Deleting an ISO file through this method does not prompt any confirmation dialog. Proceed with caution. It's assumed that users have the original ISO file stored elsewhere (e.g., on their local computer) and can re-upload it if necessary.

7.15 Snapshots in ForensicVM: A Crucial Asset for Investigators

7.15.1 Why snapshots are so important for a forensic investigation

In the dynamic realm of digital forensics, the ability to preserve, replicate, and revert to specific states of digital evidence is paramount. Snapshots in ForensicVM offer this essential capability. Here's an in-depth look at why snapshots are indispensable for forensic investigators:

Base Snapshot: The Pristine Beginning

The *base snapshot* or sometimes referred to as the ‘first snapshot,’ is a reflection of the initial state of a system or a piece of evidence. Just as a crime scene investigator would secure a scene to ensure no contamination occurs, in digital forensics, the base snapshot acts as that secured, untouched crime scene. It represents the data in its original, unaltered form, enabling investigators to always have a pristine reference point.

Preserving Evidence Integrity

Digital evidence, by its very nature, is volatile. A single action, intentional or accidental, can alter the evidence, possibly rendering it inadmissible in court. Snapshots act as safety nets. Should the evidence be unintentionally modified or corrupted, investigators can easily revert to a previous snapshot, ensuring the integrity of the evidence remains uncompromised.

Embracing "What-If" Analysis

Forensic investigation often involves a series of "what-if" scenarios. Investigators may want to test a hypothesis or simulate actions that a suspect might have taken. With snapshots, these simulations can be executed without the risk of permanently altering the evidence. After an analysis, the system can be reverted to its original state using the snapshot, ready for another hypothesis to be tested.

Additional Considerations

1. **Documentation and** Chain of Custody: Every snapshot can serve as a documented step in the investigative process, aiding in maintaining a clear chain of custody.
2. **Efficiency and Speed**: Instead of restoring from backups or original sources, which can be time-consuming, snapshots allow for quick reversion, making the investigative process more efficient.
3. **Risk Mitigation**: Especially in complex cases involving malware or unknown data structures, snapshots provide a safety mechanism, allowing investigators to explore without risking the primary evidence source or the investigation platform.

Note: Working with Snapshots and ForensicVM

Before diving into the functionalities associated with snapshots, it's crucial to understand a fundamental prerequisite: the ForensicVM needs to be up and running. Snapshots essentially capture the state of a virtual machine at a specific point in time. As such, to make the snapshot meaningful and functional, the ForensicVM has to be in an operational state.

If you haven't started your ForensicVM yet, please do so by following these steps:

1. **Open the Autopsy ForensicVM Client**: Ensure that you have the client interface open and accessible.

2. **Locate the 'Start' Option**: Within the interface, navigate to the main control panel where you have options to 'Start', 'Stop', 'Shutdown', etc., for the ForensicVM.
3. **Initiate the ForensicVM**: Click on the 'Start' option to boot up the ForensicVM. It might take a few moments for the virtual machine to initialize and be fully operational.

Once the ForensicVM is running, you can proceed with snapshot-related tasks, ensuring accurate capture and representation of the virtual machine's state.

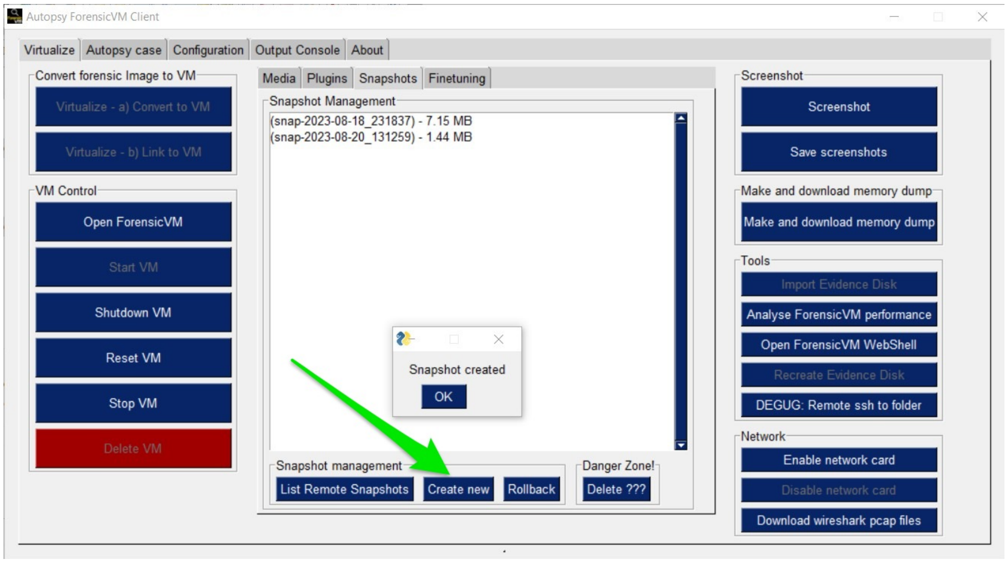
7.15.2 Create a new snapshot

It is highly recommended to create your first snapshot immediately after the machine begins its booting process. Doing so preserves the initial state of the ForensicVM, making it easier to revert back to a clean state at any time during your investigation. Snapshots can be invaluable during forensic investigations, especially when you need to return to a specific point in time or recover from potential mistakes.

Create a snapshot

1. **Open the Autopsy ForensicVM Client**: Ensure you have the Autopsy ForensicVM Client interface launched and ready.
2. **Navigate to** Snapshot Management: This section is dedicated to creating, viewing, and managing snapshots of your ForensicVM.
3. **Initiate Snapshot Creation**:

- Click on the "Create new" button located within the Snapshot management area.



(snap-2023-08-18_231837) - 7.15 MB
(snap-2023-08-20_131259) - 1.44 MB

Snapshot created

Fig. 7.199: A visual representation of the 'Create new' button used for initiating a snapshot creation in the Autopsy ForensicVM Client interface.

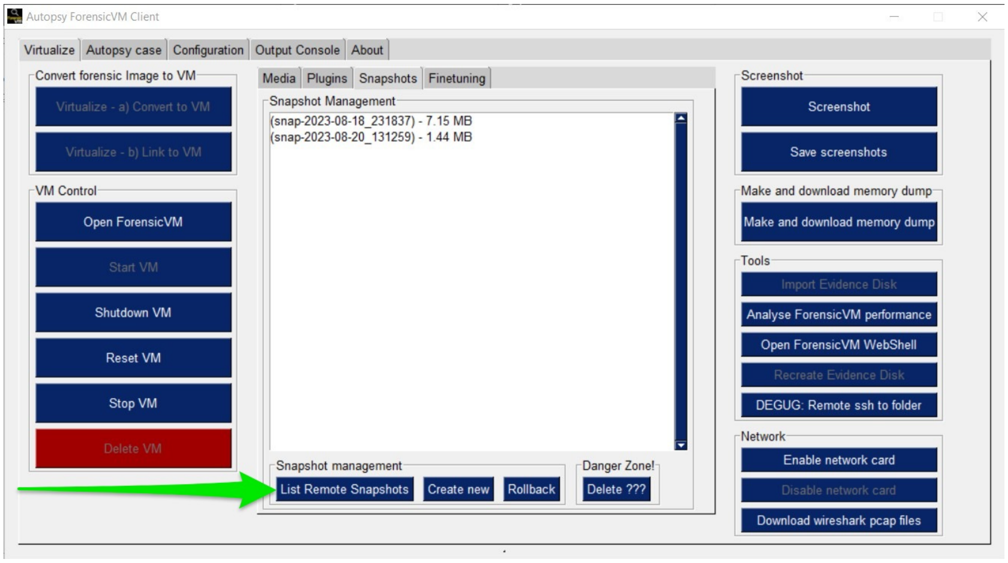
Once you've successfully created a snapshot, it will be saved and listed in the Snapshot management section. You can then access this snapshot whenever needed to revert your ForensicVM to that particular state.

7.15.3 List Remote Snapshots

While the Autopsy ForensicVM Client interface typically auto-updates to display all available snapshots, there may be occasions where the list isn't refreshed in real-time. In such scenarios, it's beneficial to use the "List Remote Snapshots" feature to manually fetch and view the list of all remote snapshots associated with the current ForensicVM.

List snapshots 1. **Open the Autopsy ForensicVM Client**: If not already open, launch the Autopsy ForensicVM Client interface to access the snapshot management features.

2. **Navigate to the** Snapshot Management **Area**: This section provides tools and options related to creating, viewing, and managing snapshots of your ForensicVM.
3. **Manually** List Remote Snapshots:
   - Look for the "List Remote Snapshots" button. This button is specifically designed to fetch the list of snapshots from the remote server and display them within the interface.
   - Click on the "List Remote Snapshots" button to initiate the listing process.



```
(snap-2023-08-18_231837) - 7.15 MB
(snap-2023-08-20_131259) - 1.44 MB
```

Fig. 7.200: A visual guide highlighting the 'List Remote Snapshots' button within the Autopsy ForensicVM Client interface.

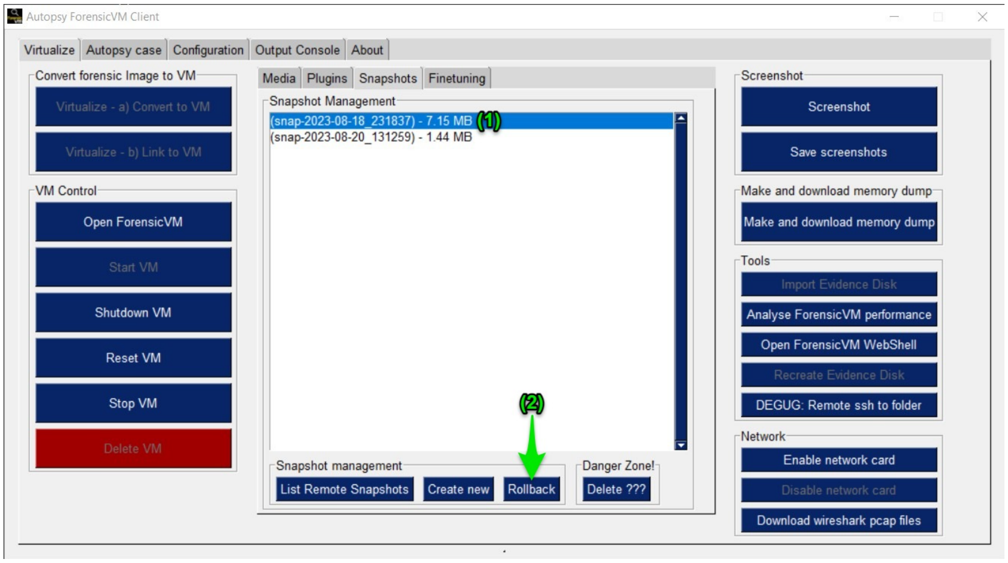
Once clicked, the interface should update and display all the remote snapshots associated with the current ForensicVM. If any issues persist, ensure that the ForensicVM Client has proper network access and permissions to communicate with the remote server. I've expanded on the process by offering a bit more context and breaking down the steps in a detailed manner.

7.15.4 Select and Rollback a Snapshot

If you ever find yourself needing to undo changes and revert the forensicVM to a previous state, the snapshot functionality is a powerful tool that allows you to do so. Here's a step-by-step guide to help you navigate the rollback process.

Steps to Reverse to a Snapshot

1. **Locate the Desired Snapshot**:
   - Snapshots are typically named in the format *snap-YYYY-MM-DD_HHMMSS*.
   - Browse through the list and find the snapshot that represents the state you wish to revert to.
   - Click on the intended snapshot. Once selected, it will be highlighted with a blue background and a white foreground, indicating your selection.
2. **Initiate the Rollback**:
   - With the desired snapshot selected, locate and click the *rollback* button.



(snap-2023-08-18_231837) - 7.15 MB

(snap-2023-08-20_131259) - 1.44 MB

Warning: Potential Issues & Solutions:

At times, the rollback process might not go as smoothly as intended. Here's what to do if you encounter issues:

- **Stalled ForensicVM**: If the forensicVM doesn't return to its previous state or appears to be stalled: 1. Use the **Reset VM** option to reset the virtual machine. 2. Once reset, attempt the **Rollback** action again to revert to the desired state.
- **Undoing the Rollback**: Regrettably, once a rollback has been executed, it is irreversible. This means that the state of the forensicVM just prior to the rollback will be permanently lost.

Best Practice Recommendation:

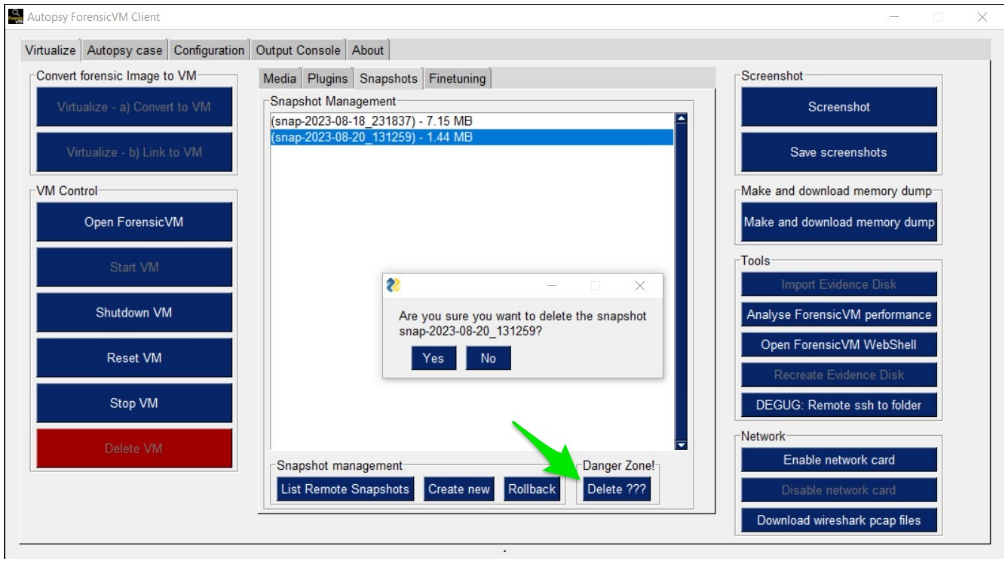
Before initiating a rollback, it's highly recommended to create a new snapshot of the current state. This way, if you later decide you want to revert to the state that existed just before the rollback, you'll have that option available. Simply rollback to the snapshot you took immediately before executing the rollback.

Remember, handling snapshots requires care, as they represent specific points in time of the ForensicVM's state. Always ensure that you've selected the correct snapshot before initiating a rollback.

7.15.5 Delete a Snapshot

Snapshots can become redundant or unnecessary over time, and you might want to reclaim some storage space. Deleting a snapshot will free up this space without affecting the current state of your forensicVM. Here's a step-by-step guide:

1. **Select the Snapshot**:
   - In the list of snapshots, click on the one you wish to delete. The selected snapshot will be highlighted, indicating your selection.
2. **Navigate to the *Danger Zone!* Section**:
   - Once you have the desired snapshot selected, move to the section labeled "Danger Zone!".
3. **Initiate the Deletion**:
   - Find and click on the button labeled *Delete ???*.
   - A confirmation popup will appear to ensure that you truly want to delete the selected snapshot. If certain, proceed by pressing the "OK" button.



(snap-2023-08-18_231837) - 7.15 MB
(snap-2023-08-20_131259) - 1.44 MB

Are you sure you want to delete the snapshot
snap-2023-08-20_131259?

Snapshot Deletion Interface

Warning: Always double-check the snapshot you are deleting. Once deleted, it cannot be recovered. It's a good habit to ensure you have backups or other necessary snapshots before deleting any.

7.15.6 In Conclusion

Snapshots in ForensicVM are not just a feature; they are a cornerstone of effective and responsible digital forensic investigations. They safeguard evidence, enable exploratory analysis, and provide peace of mind to investigators, ensuring that the quest for truth remains both accurate and uncompromised.

7.16 Plugins - Security Bypass Utilities

Plugins serve as a vital component of the forensicVM, offering an array of capabilities that can greatly assist forensic investigators. Often, forensic investigators encounter forensicVM machines that are locked or protected by certain security measures, making it difficult to access them. One common scenario is where the forensicVM is locked behind a user account, with the suspect not revealing the password. Plugins provide methods to bypass these protections.

7.16.1 Authentication Bypass Features

The suite of plugins specifically designed to bypass authentication includes:

- Add Windows Forensic Admin:
  - This plugin creates a new Windows admin user under the "Administrator" group. The credentials for this user are:
    - **Username**: forensicAdmin
    - **Password**: forensicAdmin

    The newly created user can also be used to reset the password for any local account.
- Add Linux Forensic Admin:
  - Creates a new Linux user with the following credentials:
    - **Username**: forensicAdmin
    - **Password**: forensicAdmin

    This user is granted 'sudo' permissions, allowing elevated access.
- Patch Accessibility:
  - A strategic patch that enables forensic administrators to invoke a system-level cmd.exe prompt. This can be triggered by pressing the shift key five times consecutively on the Windows login screen.
- Bypass Windows Password:
  - This plugin patches the "ntlmshared.dll" file, effectively allowing a bypass of Windows authentication. While the login screen will accept any password entered, it will still utilize the cached user password hash. This is particularly crucial when trying to access encrypted auto-mounted BitLocker files that depend on the original user's credentials for access.

7.16.2 Additional Security Bypass Features

Apart from authentication bypass, there are plugins designed to circumvent other security measures:

- **Disable Windows Defender and** Firewall:
  - Certain external security tools like NirSoft or Mimikatz necessitate the deactivation of antivirus programs. This plugin disables both Windows Defender and the firewall to accommodate such tools.
- Reset Windows 2003 or XP Activation:
  - This is required for instances where a forensic investigator needs to access machines that are awaiting activation, like Windows 2003 or XP. The plugin resets the activation to allow unobstructed login.
- BOOTFIX: Disable Driver Enforcement:
  - When working with older systems or in scenarios where you've converted a forensic image, you might encounter certain constraints related to driver signatures. The "Disable Driver Enforcement" utility addresses these challenges:
    - **Allow Unsigned Drivers**: By default, many operating systems, especially modern ones, enforce driver signing for security reasons. Disabling this enforcement lets you run unsigned drivers. This can be particularly handy for running drivers like *virtio* on older systems.
    - **Support for Programs Using Unsigned Drivers**: Some utilities or programs require the use of unsigned drivers. Disabling the driver enforcement provides flexibility to run these applications without any hitches.
    - **Blue Screen Issue Resolution**: After converting a forensic image, systems may sometimes experience the infamous Blue Screen of Death (BSOD) due to driver issues. This tool can assist in resolving those problems by ensuring that all drivers, even the unsigned ones, can run without any enforcement barriers.

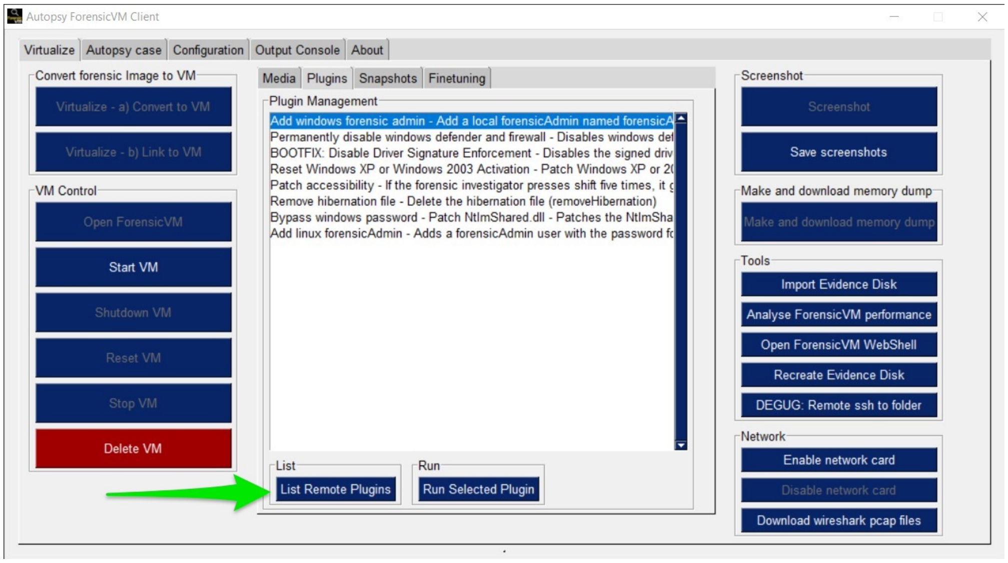
Note: While these plugins provide powerful capabilities, they should be used responsibly and ethically. Misuse could lead to unintended consequences or legal issues.

7.16.3 Browsing Available Plugins

Forensic investigations often require an adaptable approach, and the ability to extend functionality through plugins makes the ForensicVM tool particularly versatile. To stay updated with the latest available plugins or to review the catalog of installed plugins, the Autopsy ForensicVM Client provides an easy-to-use interface.

Steps to List Available Plugins

1. **Navigate to the 'Plugins' Tab**: Open the Autopsy ForensicVM Client and access the **Plugins** tab. This tab consolidates all plugin-related functionalities, making it easier to manage and deploy extensions.
2. **Refresh the Plugin List**: To get the most recent list of plugins, simply click on the **List Remote Plugins** button. This action fetches and displays all available plugins from the remote repository, ensuring you're working with the latest toolset.



```
Add windows forensic admin - Add a local forensicAdmin named forensicA
Permanently disable windows defender and firewall - Disables windows de
BOOTFIX: Disable Driver Signature Enforcement - Disables the signed driv
Reset Windows XP or Windows 2003 Activation - Patch Windows XP or 2
Patch accessibility - If the forensic investigator presses shift five times, it
Remove hibernation file - Delete the hibernation file (removeHibernation)
Bypass windows password - Patch NtlmShared.dll - Patches the NtlmSha
Add linux forensicAdmin - Adds a forensicAdmin user with the password fo
```

Fig. 7.201: Browsing and refreshing the available plugins

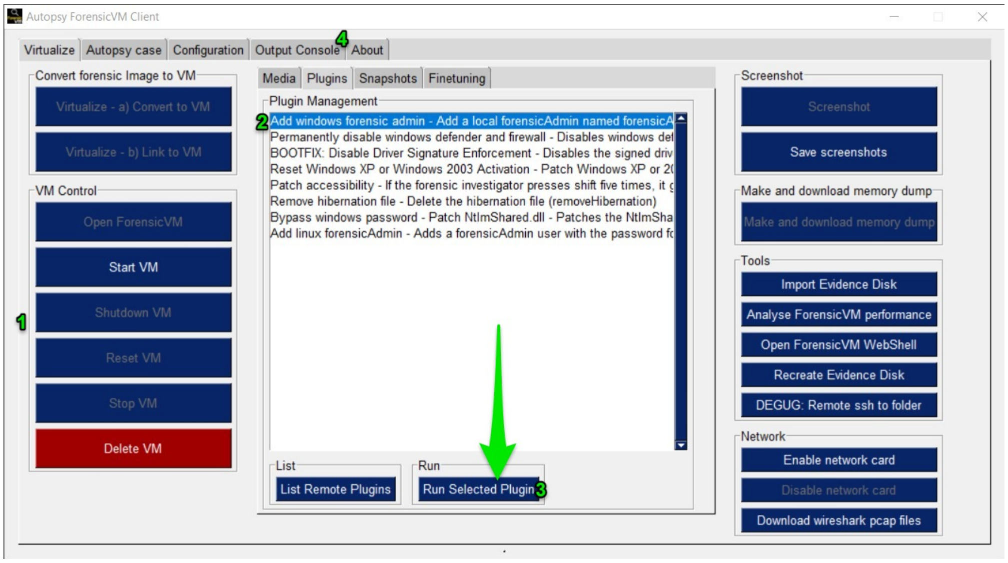
7.16.4 Executing Plugins

The capability to execute plugins enhances the versatility of the ForensicVM, allowing for specialized tasks and bypassing certain security measures. However, prior to running any plugin, precautions are necessary to ensure the integrity of the investigation and to minimize potential issues.

Important: Pre-plugin Execution Recommendation: Before initiating any plugin, it is imperative to capture the current state of the machine using a snapshot. This provision safeguards against any unintended or adverse actions by the plugin, facilitating a revert to the original state if necessary. Start the machine, create a snapshot, and then proceed to shut down the ForensicVM.

Procedure to Execute a Plugin:

1. **Ensure ForensicVM is Stopped**: Before running any plugins, verify in the VM control area that the forensic virtual machine is in a stopped state.
2. **Select the Desired Plugin**: Navigate to the plugin management area and designate the specific plugin you intend to run.
3. **Execute the Selected Plugin**: Initiate the plugin execution by pressing the **Run Selected Plugin** button.
4. **Review the Plugin Output**: Post execution, it's vital to inspect the results and logs. These can be found within the Output Console tab.



Add windows forensic admin - Add a local forensicAdmin named forensicA
Permanently disable windows defender and firewall - Disables windows def
BOOTFIX: Disable Driver Signature Enforcement - Disables the signed driv
Reset Windows XP or Windows 2003 Activation - Patch Windows XP or 20
Patch accessibility - If the forensic investigator presses shift five times, it g
Remove hibernation file - Delete the hibernation file (removeHibernation)
Bypass windows password - Patch NtlmShared.dll - Patches the NtlmSha
Add linux forensicAdmin - Adds a forensicAdmin user with the password fo

Fig. 7.202: Running a plugin

Warning: For the integrity of the process, always ensure a complete shutdown of the ForensicVM before executing any plugins. In the context of Windows, pressing the shift key while initiating the shutdown ensures the machine isn't placed in hibernation and undergoes a full shutdown. This step is crucial as hibernation can interfere with the functionality of certain plugins and the snapshot reverting process.

7.16.5 Join the Community Plugins Project and Shape ForensicVM's Future!

The Community Plugins Project for AutoPsy ForensicVM is an open initiative aimed at driving innovation and enhancing the functionalities of the ForensicVM tool. As a community-driven platform, we invite individuals from all backgrounds to contribute. Whether you're a seasoned developer, a forensic investigator with a penchant for coding, or a user with an innovative idea, your input can make a difference!

Here's how you can get involved:

Access the Project Repository

The entire project is hosted on GitHub. You can view, clone, or fork the repository by visiting:

ForensicVM Plugins on GitHub

Contributing Code

If you've developed a new plugin or made improvements to existing ones, follow these steps to contribute:

1. **Fork the Project**: Fork the main repository to create a personal copy you can work on.
2. **Commit Your Changes**: Make your changes, ensuring they adhere to the project's coding standards and best practices.
3. **Suggest a Merge**: Once ready, submit a pull request. Our team will review your code, and if it meets our quality standards, it will be merged into the next release.

Feature Suggestions and Plugin Requests

If you have ideas for new plugins, features, or improvements, but aren't looking to code them yourself, you can still contribute:

1. **Open an Issue**: Navigate to the Issues section on our GitHub page.
2. **Describe Your Idea**: Provide as much detail as possible. This helps in understanding and potentially implementing your suggestion.
3. **Engage with the Community**: Once your issue is posted, community members might join the discussion, providing feedback, insights, or offering to develop your idea.

Note: Collaboration is the backbone of open-source projects. By sharing ideas, providing feedback, or contributing code, you're not just enhancing a tool; you're building a community.

7.17 Chain of Custody Management in ForensicVM

Recording and maintaining a chain of custody in digital forensics is paramount to ensuring the integrity and veracity of digital evidence. When it comes to making comments or annotations about the custody of particular items, it is essential to have a robust system in place that captures these comments accurately and provides mechanisms for their retrieval. The following elaborates on the importance of such a system:

7.17.1 Transparency and Accountability

By having a system that records all chain of custody comments, it ensures transparency in the process. If there are any questions about how evidence was handled, one can refer back to the comments made at any given point in time. This keeps all stakeholders accountable.

7.17.2 Legal Compliance

For any digital forensic evidence to be admissible in court, the chain of custody must be clearly documented. A system that saves comments regarding custody and allows for their retrieval ensures that this requirement is met.

7.17.3 Collaboration and Consistency

Multiple investigators may handle a piece of evidence. By having a centralized system for comments, it ensures that all investigators have access to the same information, promoting consistency in the process.

7.17.4 Error Detection

Within ForensicVM, investigators have the capability to take snapshots and add comments at various stages of their analysis. If any errors are made regarding the custody of evidence or during the investigation, these snapshots provide a safe point to which investigators can roll back. This ensures that mistakes can be swiftly corrected without affecting the integrity of the ongoing analysis. Furthermore, the ability to review comments alongside these snapshots can assist investigators in pinpointing exactly where the mistake occurred, providing valuable insights for learning and improvement in future investigations.

7.17.5 Chain of Custody: Document, Save, and Download as DOCX

Save a comment

Open the chain of custody web modal popup by clicking on the designated button and enter your comment in the textbox provided. Once done, click the button to submit your comment to the database.

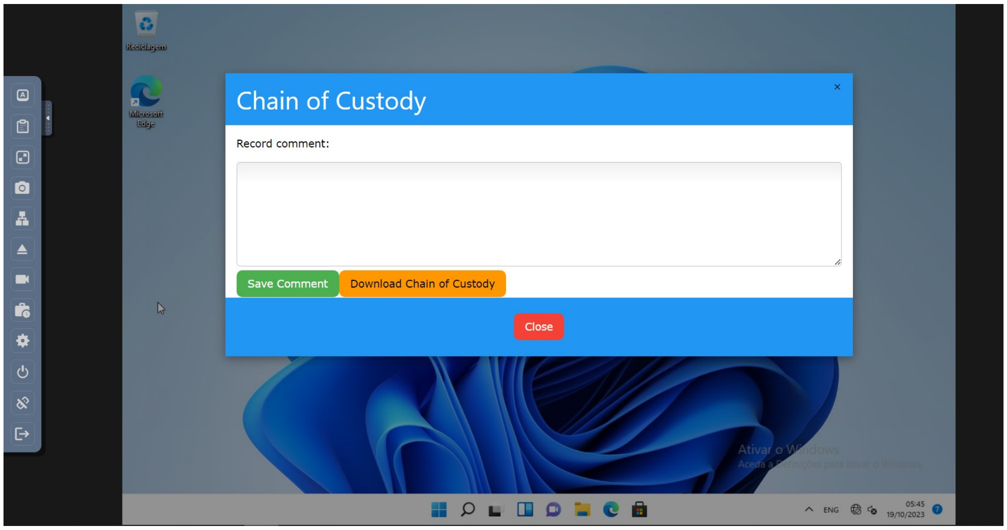
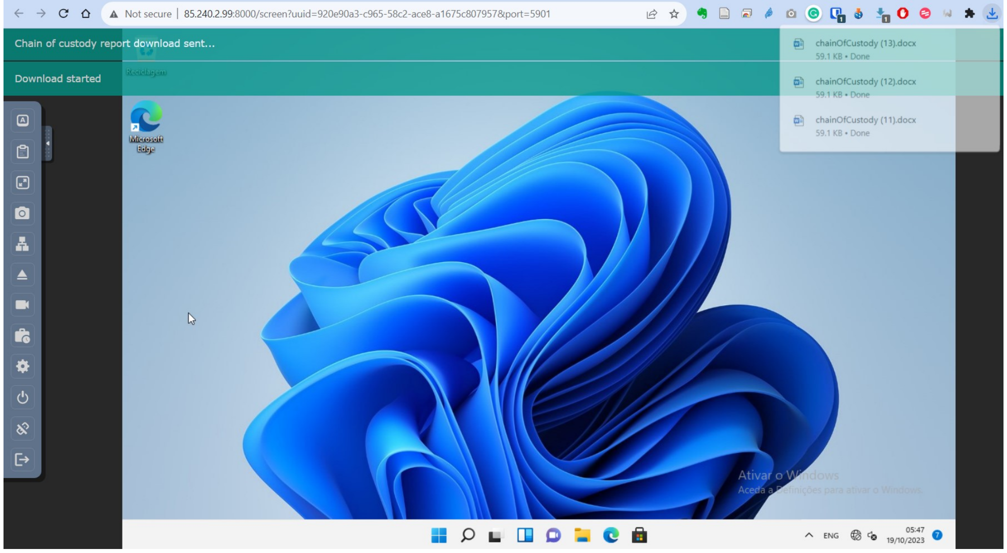


Fig. 7.203: Open the chain of custody web modal popup and submit comment

Download chain of custody docx

To download the chain of custody report, click on the "Download" button. This action will trigger a download on your browser.



Not secure | 85.240.2.99:8000/screen?uuid=920e90a3-c965-58c2-ace8-a1675c807957&port=5901

Chain of custody report download sent...

Download started

chainOfCustody (13).docx
59.1 KB • Done

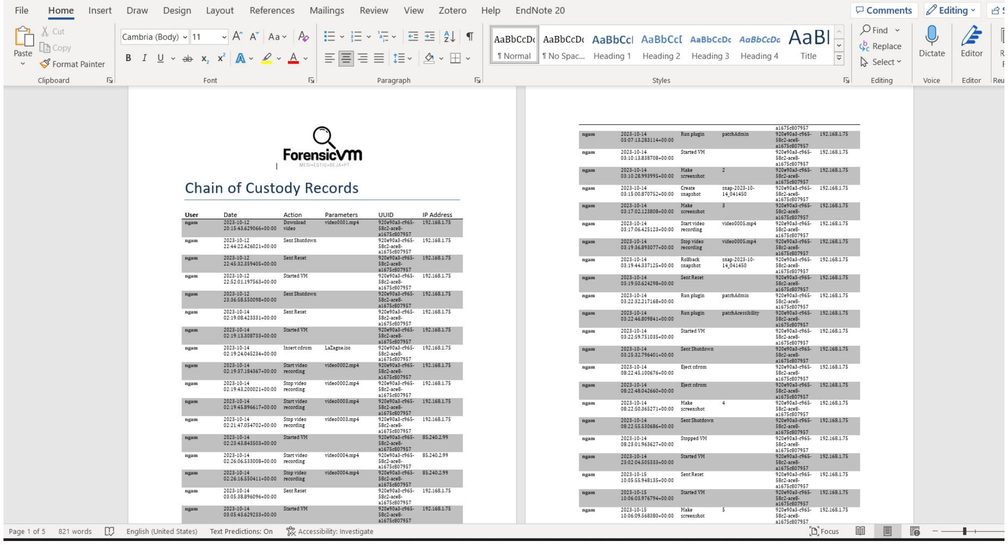
chainOfCustody (12).docx
59.1 KB • Done

chainOfCustody (11).docx
59.1 KB • Done

Fig. 7.204: Trigger the download action

Chain of custody document format

Review the downloaded chain of custody report. The report will display details such as the user, date, action, parameters of the action, UUID of the forensicVM, and the IP address of the user.



Chain of Custody Records

User	Date	Action	Parameters	UUID	IP Address
ngam	2023-10-12 20:15:43.629066+00:00	Download video	video0001.mp4	920e90a3-c965-58c2-ace8-a1675c807957	192.168.1.75
ngam	2023-10-12 22:44:22.426021+00:00	Sent Shutdown		920e90a3-c965-58c2-ace8-a1675c807957	192.168.1.75
ngam	2023-10-12 22:45:32.359405+00:00	Sent Reset		920e90a3-c965-58c2-ace8-a1675c807957	192.168.1.75
ngam	2023-10-12 22:52:01.197563+00:00	Started VM		920e90a3-c965-58c2-ace8-a1675c807957	192.168.1.75
ngam	2023-10-12 23:36:58.550098+00:00	Sent Shutdown		920e90a3-c965-58c2-ace8-a1675c807957	192.168.1.75
ngam	2023-10-14 02:19:08.423331+00:00	Sent Reset		920e90a3-c965-58c2-ace8-a1675c807957	192.168.1.75
ngam	2023-10-14 02:19:13.308733+00:00	Started VM		920e90a3-c965-58c2-ace8-a1675c807957	192.168.1.75
ngam	2023-10-14 02:19:24.045234+00:00	Insert cdrom	LaZagne.iso	920e90a3-c965-58c2-ace8-a1675c807957	192.168.1.75
ngam	2023-10-14 02:19:37.184367+00:00	Start video recording	video0002.mp4	920e90a3-c965-58c2-ace8-a1675c807957	192.168.1.75
ngam	2023-10-14 02:19:43.200021+00:00	Stop video recording	video0002.mp4	920e90a3-c965-58c2-ace8-a1675c807957	192.168.1.75
ngam	2023-10-14 02:19:45.896617+00:00	Start video recording	video0003.mp4	920e90a3-c965-58c2-ace8-a1675c807957	192.168.1.75
ngam	2023-10-14 02:21:47.054702+00:00	Stop video recording	video0003.mp4	920e90a3-c965-58c2-ace8-a1675c807957	192.168.1.75
ngam	2023-10-14 02:23:43.843503+00:00	Started VM		920e90a3-c965-58c2-ace8-a1675c807957	85.240.2.99
ngam	2023-10-14 02:26:06.533008+00:00	Start video recording	video0004.mp4	920e90a3-c965-58c2-ace8-a1675c807957	85.240.2.99
ngam	2023-10-14 02:26:16.550411+00:00	Stop video recording	video0004.mp4	920e90a3-c965-58c2-ace8-a1675c807957	85.240.2.99
ngam	2023-10-14 03:05:38.896096+00:00	Sent Reset		920e90a3-c965-58c2-ace8-a1675c807957	192.168.1.75
ngam	2023-10-14 03:05:43.629233+00:00	Started VM		920e90a3-c965-58c2-ace8-a1675c807957	192.168.1.75
				a1675c807957	
ngam	2023-10-14 03:07:13.283114+00:00	Run plugin	patchAdmin	920e90a3-c965-58c2-ace8-a1675c807957	192.168.1.75
ngam	2023-10-14 03:10:13.838708+00:00	Started VM		920e90a3-c965-58c2-ace8-a1675c807957	192.168.1.75
ngam	2023-10-14 03:10:28.993995+00:00	Make screenshot	2	920e90a3-c965-58c2-ace8-a1675c807957	192.168.1.75
ngam	2023-10-14 03:15:00.870752+00:00	Create snapshot	snap-2023-10-14_041450	920e90a3-c965-58c2-ace8-a1675c807957	192.168.1.75
ngam	2023-10-14 03:17:02.123808+00:00	Make screenshot	3	920e90a3-c965-58c2-ace8-a1675c807957	192.168.1.75
ngam	2023-10-14 03:17:06.425123+00:00	Start video recording	video0005.mp4	920e90a3-c965-58c2-ace8-a1675c807957	192.168.1.75
ngam	2023-10-14 03:19:36.893077+00:00	Stop video recording	video0005.mp4	920e90a3-c965-58c2-ace8-a1675c807957	192.168.1.75
ngam	2023-10-14 03:19:44.337125+00:00	Rollback snapshot	snap-2023-10-14_041450	920e90a3-c965-58c2-ace8-a1675c807957	192.168.1.75
ngam	2023-10-14 03:19:50.624298+00:00	Sent Reset		920e90a3-c965-58c2-ace8-a1675c807957	192.168.1.75
ngam	2023-10-14 03:22:32.217168+00:00	Run plugin	patchAdmin	920e90a3-c965-58c2-ace8-a1675c807957	192.168.1.75
ngam	2023-10-14 03:22:46.809841+00:00	Run plugin	patchAcessibility	920e90a3-c965-58c2-ace8-a1675c807957	192.168.1.75
ngam	2023-10-14 03:22:59.751035+00:00	Started VM		920e90a3-c965-58c2-ace8-a1675c807957	192.168.1.75
ngam	2023-10-14 03:25:32.796401+00:00	Sent Shutdown		920e90a3-c965-58c2-ace8-a1675c807957	192.168.1.75
ngam	2023-10-14 08:22:45.100676+00:00	Eject cdrom		920e90a3-c965-58c2-ace8-a1675c807957	192.168.1.75
ngam	2023-10-14 08:22:48.042660+00:00	Eject cdrom		920e90a3-c965-58c2-ace8-a1675c807957	192.168.1.75
ngam	2023-10-14 08:22:50.365271+00:00	Make screenshot	4	920e90a3-c965-58c2-ace8-a1675c807957	192.168.1.75
ngam	2023-10-14 08:22:55.530686+00:00	Sent Shutdown		920e90a3-c965-58c2-ace8-a1675c807957	192.168.1.75
ngam	2023-10-14 08:23:01.963627+00:00	Stopped VM		920e90a3-c965-58c2-ace8-a1675c807957	192.168.1.75
ngam	2023-10-14 23:02:04.505333+00:00	Started VM		920e90a3-c965-58c2-ace8-a1675c807957	192.168.1.75
ngam	2023-10-15 10:05:55.948135+00:00	Sent Reset		920e90a3-c965-58c2-ace8-a1675c807957	192.168.1.75
ngam	2023-10-15 10:06:03.976794+00:00	Started VM		920e90a3-c965-58c2-ace8-a1675c807957	192.168.1.75
ngam	2023-10-15 10:06:09.568380+00:00	Make screenshot	5	920e90a3-c965-58c2-ace8-a1675c807957	192.168.1.75

Fig. 7.205: Review the chain of custody report

7.18 Virtual Introspection

Virtual introspection, a pioneering feature in ForensicVM, revolutionizes the way forensic analysts, IT professionals, and cybersecurity experts interact with and analyze virtual machines. This tool is indispensable for in-depth digital investigations and cybersecurity assessments, as it provides an exhaustive and unobstructed view into the virtual machine's operating environment. Through virtual introspection, users can meticulously examine real-time processes, command line executions, memory-loaded files, active handles, and the entire system's status, gaining critical insights that are often elusive in traditional analysis.

The power of virtual introspection in ForensicVM is harnessed through the advanced capabilities of QEMU, an esteemed open-source machine emulator and virtualizer. QEMU's sophisticated technology enables the creation of precise memory snapshots of the virtual machine at any given instance. These snapshots encapsulate the VM's exact state at the moment of capture, providing a rich dataset for thorough forensic examination. To analyze these memory snapshots, ForensicVM integrates Volatility 3, a state-of-the-art memory forensics framework known for its robust analytical tools and detailed insights. Volatility 3 processes the captured data, uncovering intricate details about the VM's internal operations and activities.

The integration of virtual introspection in ForensicVM represents a significant leap in virtual machine forensics. It not only simplifies the investigative process but also elevates the depth and quality of the analysis. Whether it's uncovering hidden processes, detecting signs of malware, or exploring system anomalies, virtual introspection equips users with the necessary tools to conduct comprehensive and efficient examinations. This capability is especially crucial in today's digital landscape, where virtual environments are increasingly complex and security threats are constantly evolving.

As the digital world continues to expand and evolve, tools like virtual introspection in ForensicVM become essential for maintaining cybersecurity and understanding the intricacies of virtual systems. Its ability to provide detailed snapshots and in-depth analysis of the Windows operating system makes it an invaluable asset for any professional dealing with digital forensics, cybersecurity, and IT management. By staying ahead with such advanced technologies, ForensicVM ensures that its users are well-equipped to face the challenges of modern digital forensics and cybersecurity.

The current iteration of ForensicVM's virtual introspection is specialized and optimized exclusively for Windows operating systems. This focus is not without its limitations, particularly in its exclusion of Linux operating systems. While the specialized design for Windows ensures that the tool is precisely attuned to the distinct characteristics and complexities of Windows environments, enhancing its effectiveness and accuracy, it does mean that users working with Linux systems are currently unsupported.

Starting Virtual Introspection: To begin virtual introspection, first run the forensicVM until the operating system has fully booted. Then, press the 'Virtual Introspect' button located on the forensicVM web client interface:

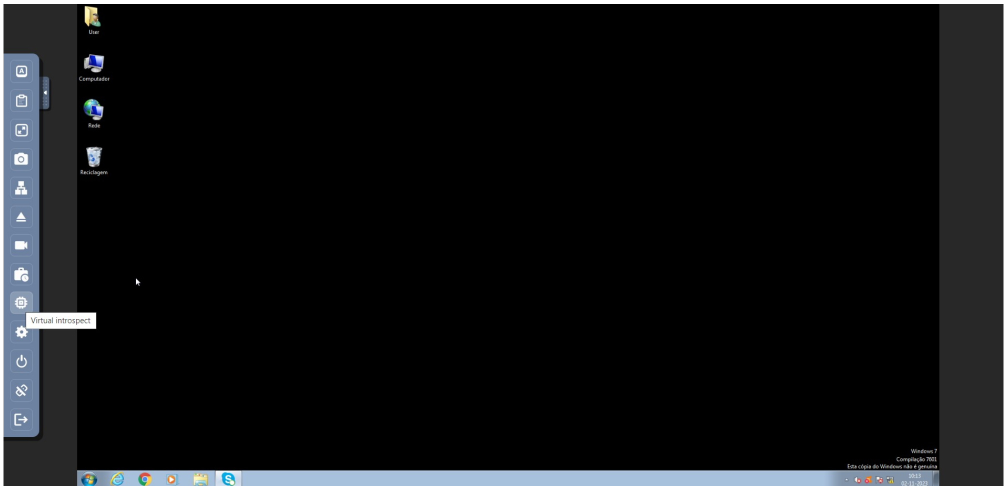
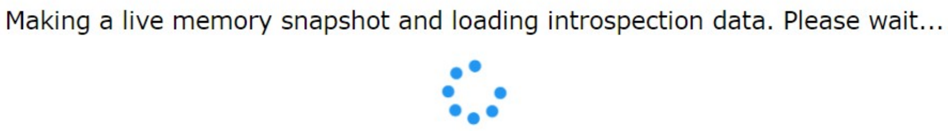


Fig. 7.206: Screenshot of the Virtual Introspect button in the forensicVM web client

Once you press the button, a progress window will appear. This window will automatically display the results of the introspection process upon completion.

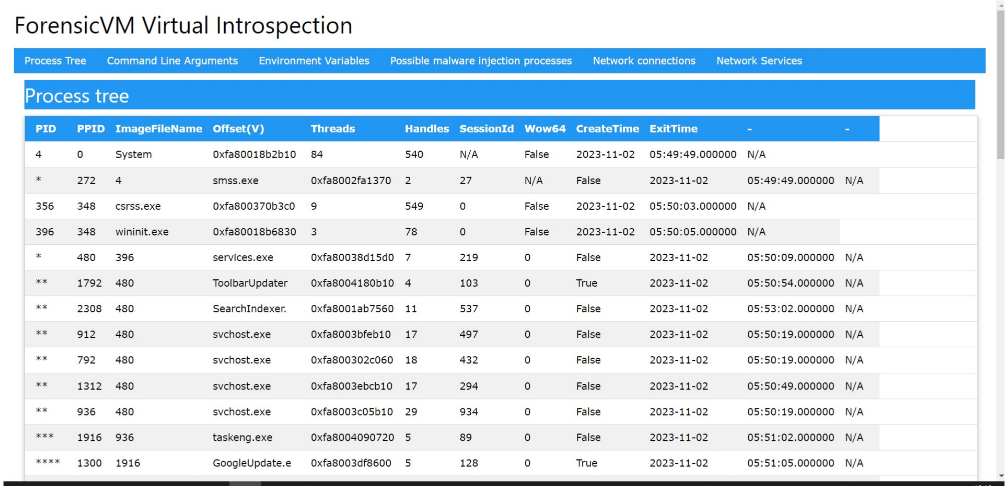


Making a live memory snapshot and loading introspection data. Please wait...

Fig. 7.207: Progress window for Virtual Introspection in forensicVM

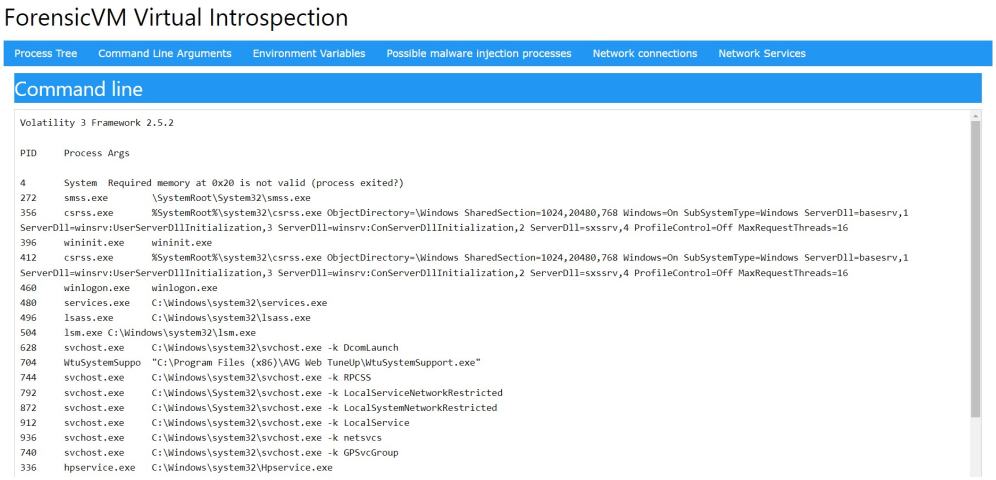
Components of ForensicVM Introspection: The ForensicVM introspection process comprises seven informative tabs:

1) **Process Tree:** Displays a list of all active processes within the system, providing insight even when the forensicVM is locked on the login screen.
2) **Command Line Arguments:** Shows the commands and arguments that are or were being executed in the system.



PID	PPID	ImageFileName	Offset(V)	Threads	Handles	SessionId	Wow64	CreateTime	ExitTime	-	-
4	0	System	0xfa80018b2b10	84	540	N/A	False	2023-11-02	05:49:49.000000	N/A	
*	272	4	smss.exe	0xfa8002fa1370	2	27	N/A	False	2023-11-02	05:49:49.000000	N/A
356	348	csrss.exe	0xfa800370b3c0	9	549	0	False	2023-11-02	05:50:03.000000	N/A	
396	348	wininit.exe	0xfa80018b6830	3	78	0	False	2023-11-02	05:50:05.000000	N/A	
*	480	396	services.exe	0xfa80038d15d0	7	219	0	False	2023-11-02	05:50:09.000000	N/A
**	1792	480	ToolbarUpdater	0xfa8004180b10	4	103	0	True	2023-11-02	05:50:54.000000	N/A
**	2308	480	SearchIndexer.	0xfa8001ab7560	11	537	0	False	2023-11-02	05:53:02.000000	N/A
**	912	480	svchost.exe	0xfa8003bfeb10	17	497	0	False	2023-11-02	05:50:19.000000	N/A
**	792	480	svchost.exe	0xfa800302c060	18	432	0	False	2023-11-02	05:50:19.000000	N/A
**	1312	480	svchost.exe	0xfa8003ebcb10	17	294	0	False	2023-11-02	05:50:49.000000	N/A
**	936	480	svchost.exe	0xfa8003c05b10	29	934	0	False	2023-11-02	05:50:19.000000	N/A
***	1916	936	taskeng.exe	0xfa8004090720	5	89	0	False	2023-11-02	05:51:02.000000	N/A
****	1300	1916	GoogleUpdate.e	0xfa8003df8600	5	128	0	True	2023-11-02	05:51:05.000000	N/A

Fig. 7.208: Process Tree tab in ForensicVM Introspection

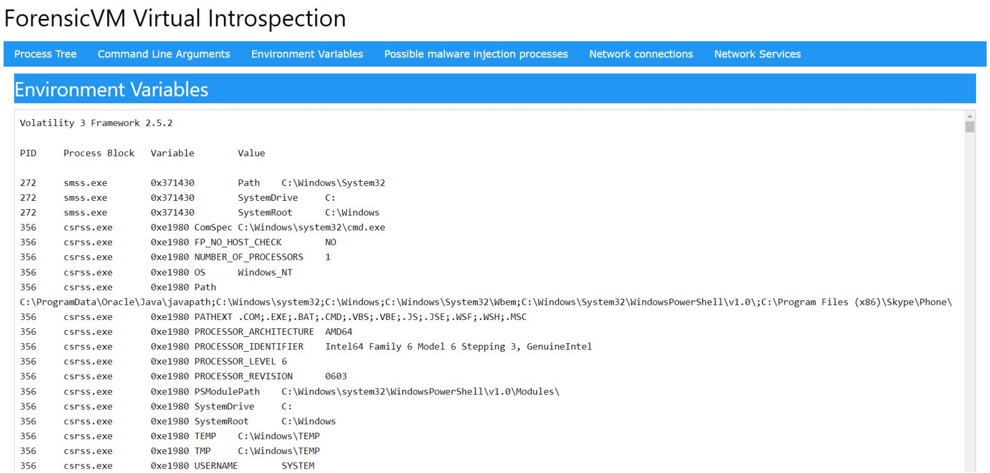


```
Volatility 3 Framework 2.5.2

PID     Process Args

4       System  Required memory at 0x20 is not valid (process exited?)
272     smss.exe        \SystemRoot\System32\smss.exe
356     csrss.exe       %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDll=basesrv,1
ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=winsrv:ConServerDllInitialization,2 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16
396     wininit.exe     wininit.exe
412     csrss.exe       %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDll=basesrv,1
ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=winsrv:ConServerDllInitialization,2 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16
460     winlogon.exe    winlogon.exe
480     services.exe    C:\Windows\system32\services.exe
496     lsass.exe       C:\Windows\system32\lsass.exe
504     lsm.exe C:\Windows\system32\lsm.exe
628     svchost.exe     C:\Windows\system32\svchost.exe -k DcomLaunch
704     WtuSystemSuppo  "C:\Program Files (x86)\AVG Web TuneUp\WtuSystemSupport.exe"
744     svchost.exe     C:\Windows\system32\svchost.exe -k RPCSS
792     svchost.exe     C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted
872     svchost.exe     C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted
912     svchost.exe     C:\Windows\system32\svchost.exe -k LocalService
936     svchost.exe     C:\Windows\system32\svchost.exe -k netsvcs
740     svchost.exe     C:\Windows\system32\svchost.exe -k GPSvcGroup
336     hpservice.exe   C:\Windows\system32\Hpservice.exe
```

Fig. 7.209: Command Line Arguments tab in ForensicVM Introspection

3) **Environment Variables:** Lists the environment variables associated with each running process.

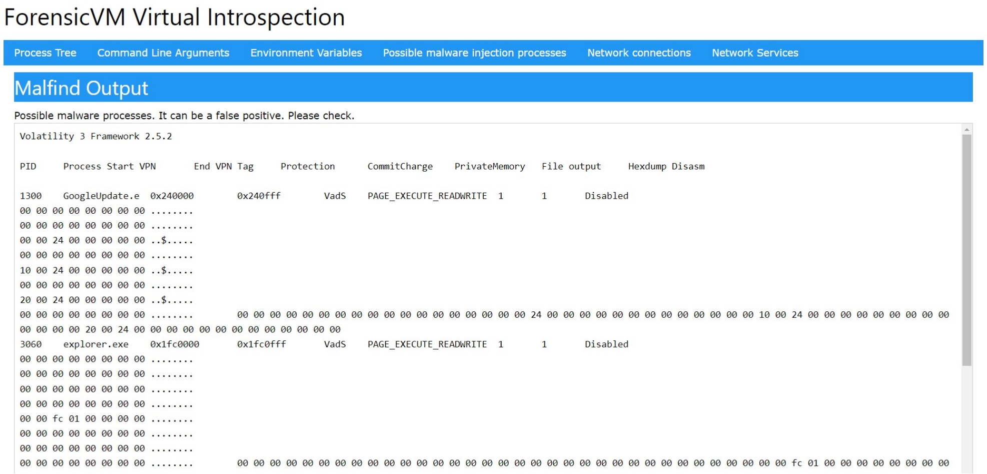
4) **Possible Malware Injection Processes:** Identifies processes that may have been injected or run with elevated privileges, which could suggest malware activity but also include false positives.



Environment Variables

```
Volatility 3 Framework 2.5.2

PID     Process Block   Variable        Value

272     smss.exe        0x371430        Path    C:\Windows\System32
272     smss.exe        0x371430        SystemDrive     C:
272     smss.exe        0x371430        SystemRoot      C:\Windows
356     csrss.exe       0xe1980 ComSpec C:\Windows\system32\cmd.exe
356     csrss.exe       0xe1980 FP_NO_HOST_CHECK        NO
356     csrss.exe       0xe1980 NUMBER_OF_PROCESSORS    1
356     csrss.exe       0xe1980 OS      Windows_NT
356     csrss.exe       0xe1980 Path
C:\ProgramData\Oracle\Java\javapath;C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0\;C:\Program Files (x86)\Skype\Phone\
356     csrss.exe       0xe1980 PATHEXT .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
356     csrss.exe       0xe1980 PROCESSOR_ARCHITECTURE  AMD64
356     csrss.exe       0xe1980 PROCESSOR_IDENTIFIER    Intel64 Family 6 Model 6 Stepping 3, GenuineIntel
356     csrss.exe       0xe1980 PROCESSOR_LEVEL 6
356     csrss.exe       0xe1980 PROCESSOR_REVISION      0603
356     csrss.exe       0xe1980 PSModulePath    C:\Windows\system32\WindowsPowerShell\v1.0\Modules\
356     csrss.exe       0xe1980 SystemDrive     C:
356     csrss.exe       0xe1980 SystemRoot      C:\Windows
356     csrss.exe       0xe1980 TEMP    C:\Windows\TEMP
356     csrss.exe       0xe1980 TMP     C:\Windows\TEMP
356     csrss.exe       0xe1980 USERNAME        SYSTEM
```

Fig. 7.210: Environment Variables tab in ForensicVM Introspection



Malfind Output

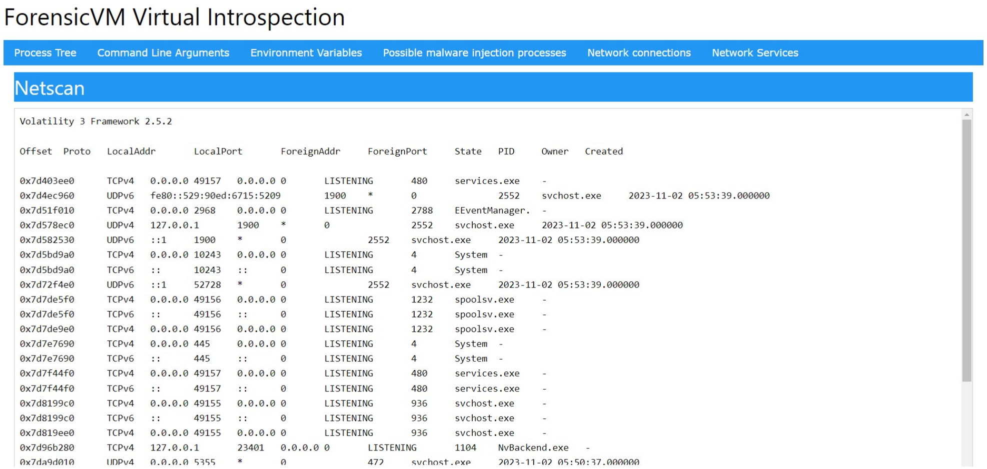
Possible malware processes. It can be a false positive. Please check.

```
Volatility 3 Framework 2.5.2

PID     Process Start VPN       End VPN Tag     Protection      CommitCharge    PrivateMemory   File output     Hexdump Disasm

1300    GoogleUpdate.e  0x240000        0x240fff        VadS    PAGE_EXECUTE_READWRITE  1       1       Disabled
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 24 00 00 00 00 00 ..$.....
00 00 00 00 00 00 00 00 ........
10 00 24 00 00 00 00 00 ..$.....
00 00 00 00 00 00 00 00 ........
20 00 24 00 00 00 00 00 ..$.....
00 00 00 00 00 00 00 00 ........        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 24 00 00 00 00 00 00 00 00 00 00 00 10 00 24 00 00 00 00 00 00 00 00
00 00 00 00 20 00 24 00 00 00 00 00 00 00 00 00 00 00 00
3060    explorer.exe    0x1fc0000       0x1fc0fff       VadS    PAGE_EXECUTE_READWRITE  1       1       Disabled
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 fc 01 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fc 01 00 00 00 00 00 00 00
```

Fig. 7.211: Possible Malware Injection Processes tab in ForensicVM Introspection

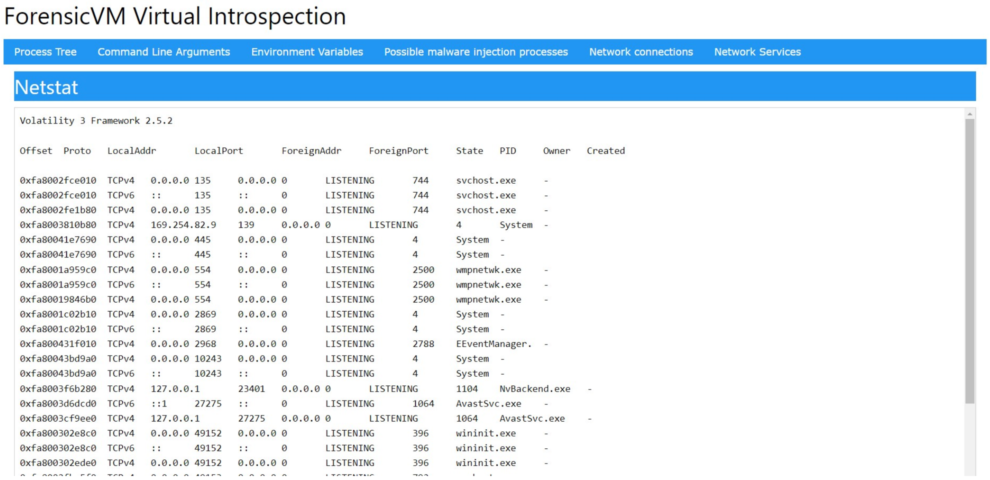
5) **Netscan Results:** Provides a list of open network connections, which can be indicators of compromise, especially if connections to known malicious sites are detected.

6) **Netstat:** Shows running network services, with potential signs of compromise if unknown systems are opening ports on the local forensicVM.



```
Volatility 3 Framework 2.5.2

Offset  Proto   LocalAddr       LocalPort       ForeignAddr     ForeignPort     State   PID     Owner   Created

0x7d403ee0      TCPv4   0.0.0.0 49157   0.0.0.0 0       LISTENING       480     services.exe    -
0x7d4ec960      UDPv6   fe80::529:90ed:6715:5209        1900    *       0               2552    svchost.exe     2023-11-02 05:53:39.000000
0x7d51f010      TCPv4   0.0.0.0 2968    0.0.0.0 0       LISTENING       2788    EEventManager.  -
0x7d578ec0      UDPv4   127.0.0.1       1900    *       0               2552    svchost.exe     2023-11-02 05:53:39.000000
0x7d582530      UDPv6   ::1     1900    *       0               2552    svchost.exe     2023-11-02 05:53:39.000000
0x7d5bd9a0      TCPv4   0.0.0.0 10243   0.0.0.0 0       LISTENING       4       System  -
0x7d5bd9a0      TCPv6   ::      10243   ::      0       LISTENING       4       System  -
0x7d72f4e0      UDPv6   ::1     52728   *       0               2552    svchost.exe     2023-11-02 05:53:39.000000
0x7d7de5f0      TCPv4   0.0.0.0 49156   0.0.0.0 0       LISTENING       1232    spoolsv.exe     -
0x7d7de5f0      TCPv6   ::      49156   ::      0       LISTENING       1232    spoolsv.exe     -
0x7d7de9e0      TCPv4   0.0.0.0 49156   0.0.0.0 0       LISTENING       1232    spoolsv.exe     -
0x7d7e7690      TCPv4   0.0.0.0 445     0.0.0.0 0       LISTENING       4       System  -
0x7d7e7690      TCPv6   ::      445     ::      0       LISTENING       4       System  -
0x7d7f44f0      TCPv4   0.0.0.0 49157   0.0.0.0 0       LISTENING       480     services.exe    -
0x7d7f44f0      TCPv6   ::      49157   ::      0       LISTENING       480     services.exe    -
0x7d8199c0      TCPv4   0.0.0.0 49155   0.0.0.0 0       LISTENING       936     svchost.exe     -
0x7d8199c0      TCPv6   ::      49155   ::      0       LISTENING       936     svchost.exe     -
0x7d819ee0      TCPv4   0.0.0.0 49155   0.0.0.0 0       LISTENING       936     svchost.exe     -
0x7d96b280      TCPv4   127.0.0.1       23401   0.0.0.0 0       LISTENING       1104    NvBackend.exe   -
0x7da9d010      UDPv4   0.0.0.0 5355    *       0               472     svchost.exe     2023-11-02 05:50:37.000000
```

Fig. 7.212: Netscan Results tab in ForensicVM Introspection

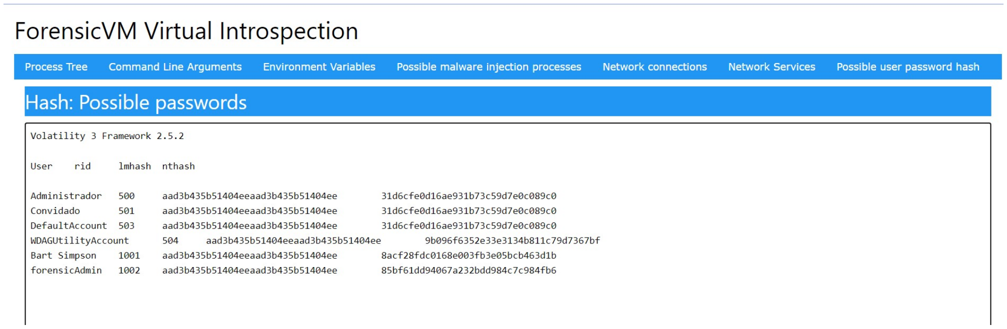


```
Volatility 3 Framework 2.5.2

Offset  Proto   LocalAddr       LocalPort       ForeignAddr     ForeignPort     State   PID     Owner   Created

0xfa8002fce010  TCPv4   0.0.0.0 135     0.0.0.0 0       LISTENING       744     svchost.exe     -
0xfa8002fce010  TCPv6   ::      135     ::      0       LISTENING       744     svchost.exe     -
0xfa8002fe1b80  TCPv4   0.0.0.0 135     0.0.0.0 0       LISTENING       744     svchost.exe     -
0xfa8003810b80  TCPv4   169.254.82.9    139     0.0.0.0 0       LISTENING       4       System  -
0xfa80041e7690  TCPv4   0.0.0.0 445     0.0.0.0 0       LISTENING       4       System  -
0xfa80041e7690  TCPv6   ::      445     ::      0       LISTENING       4       System  -
0xfa8001a959c0  TCPv4   0.0.0.0 554     0.0.0.0 0       LISTENING       2500    wmpnetwk.exe    -
0xfa8001a959c0  TCPv6   ::      554     ::      0       LISTENING       2500    wmpnetwk.exe    -
0xfa80019846b0  TCPv4   0.0.0.0 554     0.0.0.0 0       LISTENING       2500    wmpnetwk.exe    -
0xfa8001c02b10  TCPv4   0.0.0.0 2869    0.0.0.0 0       LISTENING       4       System  -
0xfa8001c02b10  TCPv6   ::      2869    ::      0       LISTENING       4       System  -
0xfa800431f010  TCPv4   0.0.0.0 2968    0.0.0.0 0       LISTENING       2788    EEventManager.  -
0xfa80043bd9a0  TCPv4   0.0.0.0 10243   0.0.0.0 0       LISTENING       4       System  -
0xfa80043bd9a0  TCPv6   ::      10243   ::      0       LISTENING       4       System  -
0xfa8003f6b280  TCPv4   127.0.0.1       23401   0.0.0.0 0       LISTENING       1104    NvBackend.exe   -
0xfa8003d6dcd0  TCPv6   ::1     27275   ::      0       LISTENING       1064    AvastSvc.exe    -
0xfa8003cf9ee0  TCPv4   127.0.0.1       27275   0.0.0.0 0       LISTENING       1064    AvastSvc.exe    -
0xfa800302e8c0  TCPv4   0.0.0.0 49152   0.0.0.0 0       LISTENING       396     wininit.exe     -
0xfa800302e8c0  TCPv6   ::      49152   ::      0       LISTENING       396     wininit.exe     -
0xfa800302ede0  TCPv4   0.0.0.0 49152   0.0.0.0 0       LISTENING       396     wininit.exe     -
```

Fig. 7.213: Netstat tab in ForensicVM Introspection

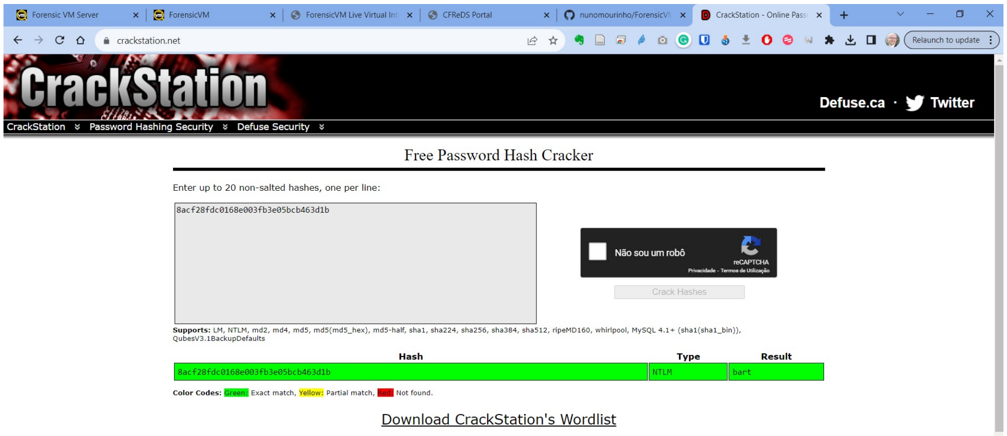
7) **Possible User Password Hashes:** Displays password hashes found in memory. These hashes can be analyzed further on external platforms like crackstation.com to potentially uncover user passwords.

Example Case: An example is provided where the Bart Simpson hash is decoded to reveal the original password, "bart."



```
Volatility 3 Framework 2.5.2

User    rid     lmhash  nthash

Administrador   500     aad3b435b51404eeaad3b435b51404ee        31d6cfe0d16ae931b73c59d7e0c089c0
Convidado       501     aad3b435b51404eeaad3b435b51404ee        31d6cfe0d16ae931b73c59d7e0c089c0
DefaultAccount  503     aad3b435b51404eeaad3b435b51404ee        31d6cfe0d16ae931b73c59d7e0c089c0
WDAGUtilityAccount      504     aad3b435b51404eeaad3b435b51404ee        9b096f6352e33e3134b811c79d7367bf
Bart Simpson    1001    aad3b435b51404eeaad3b435b51404ee        8acf28fdc0168e003fb3e05bcb463d1b
forensicAdmin   1002    aad3b435b51404eeaad3b435b51404ee        85bf61dd94067a232bdd984c7c984fb6
```

Fig. 7.214: Possible User Password Hashes tab in ForensicVM Introspection



Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
8acf28fdc0168e003fb3e05bcb463d1b
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
8acf28fdc0168e003fb3e05bcb463d1b	NTLM	bart

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Download CrackStation's Wordlist

Fig. 7.215: Example of password hash decoding in ForensicVM

7.19 Fine-Tuning ForensicVM

The conversion of a forensic image into a ForensicVM generates a configuration file in the background. This file encompasses various configuration parameters for the forensic virtual machine, such as memory size, attached disks, UEFI boot options, and more. The “Fine-Tuning” section within the Autopsy ForensicVM Client interface facilitates adjustments to certain parameters—currently, the ForensicVM’s memory size and its start date & time.

Modifying Memory Size:

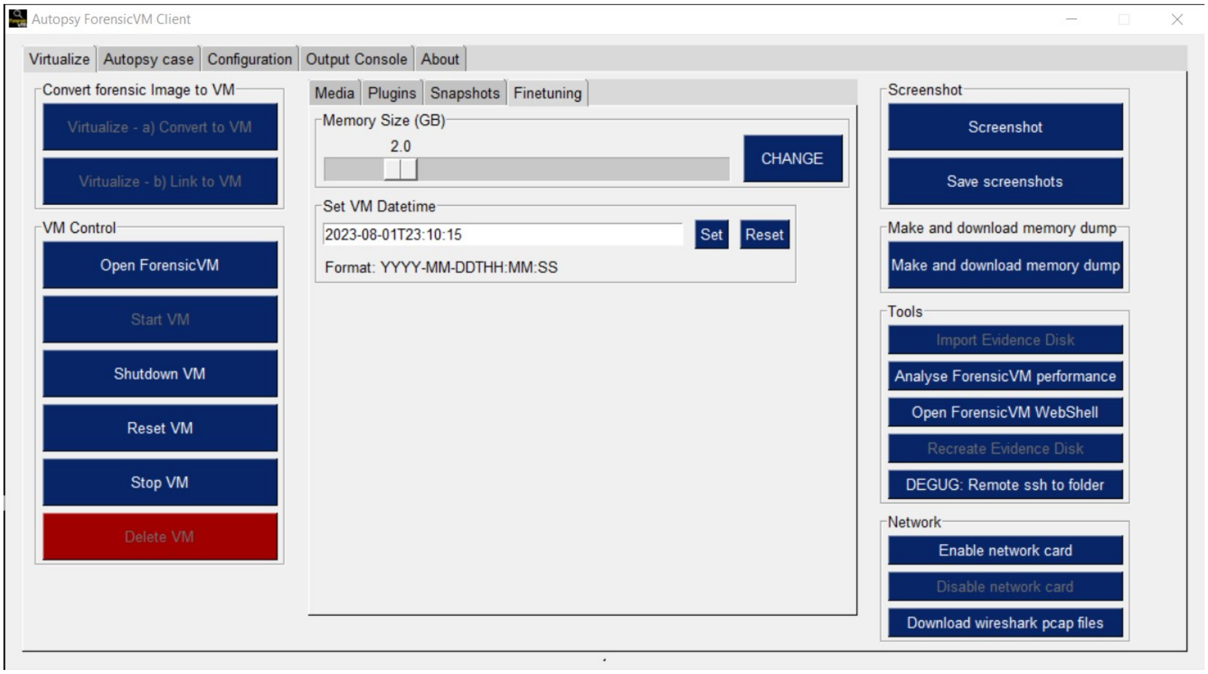
1. Navigate to the “Fine-Tuning” section in the interface.
2. Use the slider to adjust the memory size as desired.
3. Click the “Change” button to save your selection.
4. For the changes to take effect, shut down the ForensicVM and then start it again.

Note: Merely restarting the VM will not apply the memory adjustments. It’s imperative to shut down and then start the VM afresh.

Setting the VM Date & Time:

1. Enter the desired date and time in the format YYYY-MM-DD **T** HH:MM:SS. Note the **T** divider between the date and time components.
2. Press the "Set" button to save the new start date & time for the VM.
3. Again, to apply this change, shut down and then start the ForensicVM.

Below is an illustration showcasing both the memory size adjustment slider and the VM date & time setting option:



Memory Size (GB): 2.0

Set VM Datetime: 2023-08-01T23:10:15

Format: YYYY-MM-DDTHH:MM:SS

Fig. 7.216: Fine-Tuning memory size and setting ForensicVM start date & time

7.20 WebShell for Remote Administration

For enhanced remote server administration, a webshell has been crafted based on the *shellinabox* project which has been adapted into a Django application. This allows secure root access to the server, making it an invaluable tool for troubleshooting and remote server management tasks.

Accessing the WebShell:

There are two primary methods to access the WebShell:

1. **Through the Autopsy** ForensicVM Client Plugin:
   - Within the plugin interface, click on the *Open ForensicVM WebShell* button. This action will open the WebShell in your default browser.

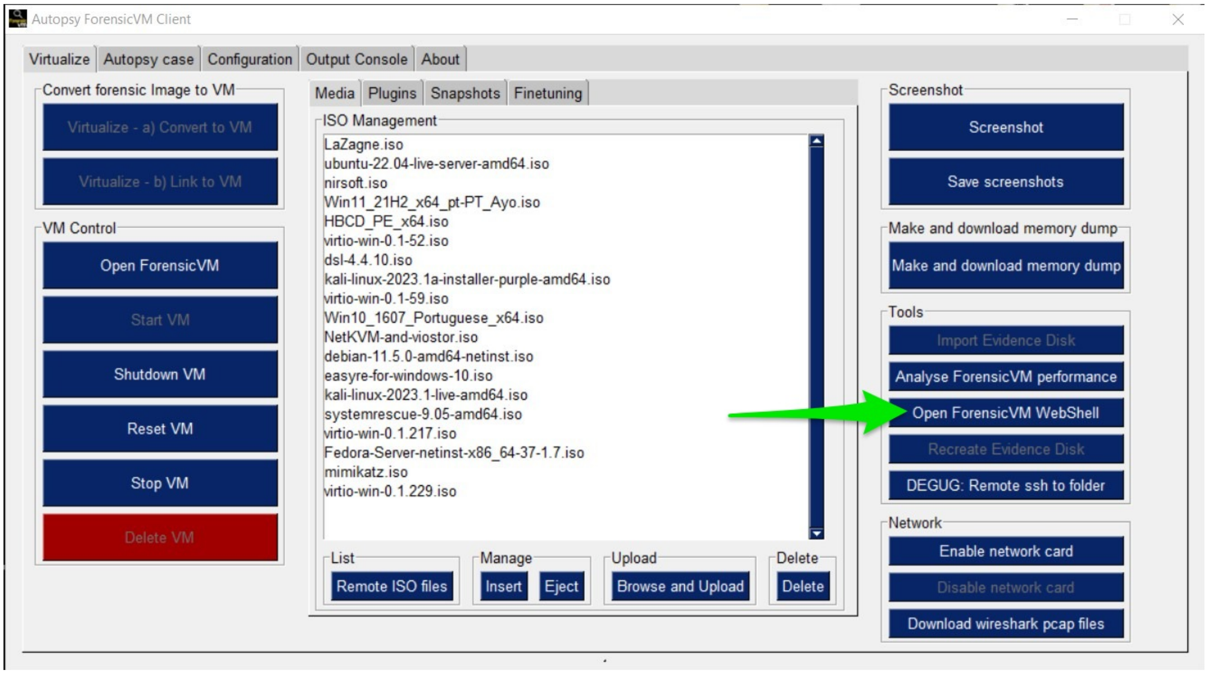
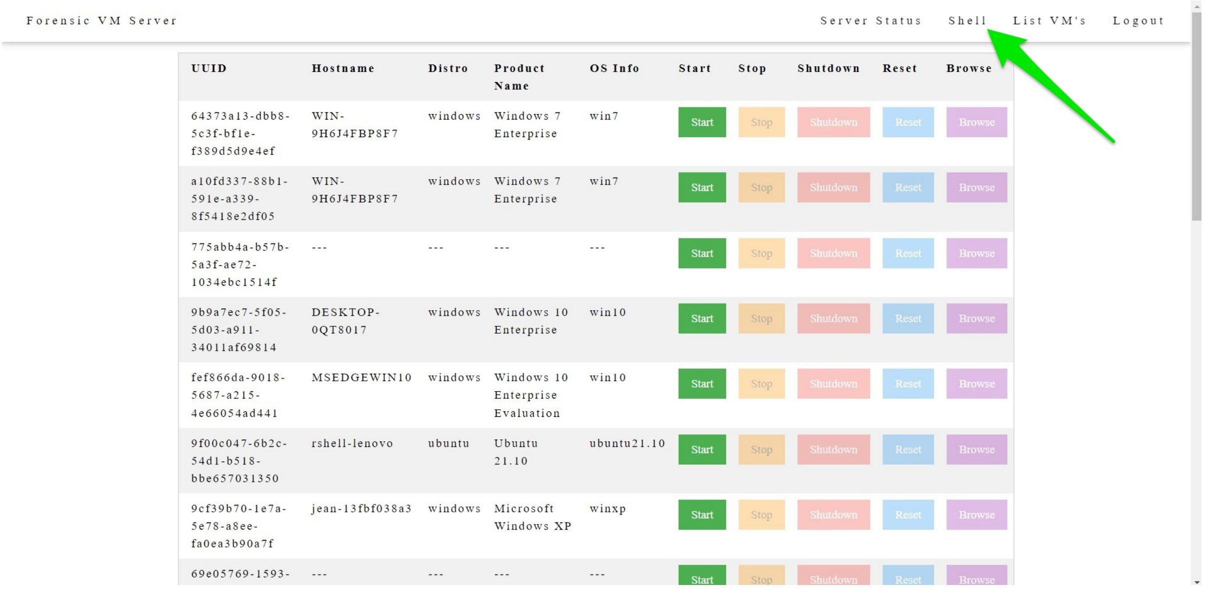


Fig. 7.217: WebShell accessed via Autopsy ForensicVM Client Plugin

2. **Via the ForensicVM** Main Web Interface:
   - Navigate to the main interface and click on the *Shell* link to access the WebShell.



UUID	Hostname	Distro	Product Name	OS Info	Start	Stop	Shutdown	Reset	Browse
64373a13-dbb8-5c3f-bf1e-f389d5d9e4ef	WIN-9H6J4FBP8F7	windows	Windows 7 Enterprise	win7	Start	Stop	Shutdown	Reset	Browse
a10fd337-88b1-591e-a339-8f5418e2df05	WIN-9H6J4FBP8F7	windows	Windows 7 Enterprise	win7	Start	Stop	Shutdown	Reset	Browse
775abb4a-b57b-5a3f-ae72-1034ebc1514f	---	---	---	---	Start	Stop	Shutdown	Reset	Browse
9b9a7ec7-5f05-5d03-a911-34011af69814	DESKTOP-0QT8017	windows	Windows 10 Enterprise	win10	Start	Stop	Shutdown	Reset	Browse
fef866da-9018-5687-a215-4e66054ad441	MSEDGEWIN10	windows	Windows 10 Enterprise Evaluation	win10	Start	Stop	Shutdown	Reset	Browse
9f00c047-6b2c-54d1-b518-bbe657031350	rshell-lenovo	ubuntu	Ubuntu 21.10	ubuntu21.10	Start	Stop	Shutdown	Reset	Browse
9cf39b70-1e7a-5e78-a8ee-fa0ea3b90a7f	jean-13fbf038a3	windows	Microsoft Windows XP	winxp	Start	Stop	Shutdown	Reset	Browse
69e05769-1593-	---	---	---	---	Start	Stop	Shutdown	Reset	Browse

Fig. 7.218: WebShell accessed via ForensicVM Main Web Interface

WebShell Interface:

Upon accessing the WebShell, users will encounter an interface resembling the following:

```
v2v-forensicVM login: 
```

ForensicVM WebShell Interface

Note: The WebShell provides a direct and secure interface to the server. However, ensure to logout after your session to maintain security.

7.21 Netdata on ForensicVM Server

7.21.1 Introduction

Netdata is a tool that helps watch over servers and apps in real-time. With ForensicVM Server, Netdata shows how the server is doing and makes sure everything runs smoothly.

7.21.2 Key Points

- Real-time Look: Netdata updates every second, helping catch issues fast.
- **Sees Everything**: It checks everything - like how the CPU is used, memory use, disk activity, and how the network is doing.
- **Alerts**: Get warnings if something goes beyond normal levels.
- **Easy-to-Read Charts**: A simple dashboard shows all the info in clear charts.

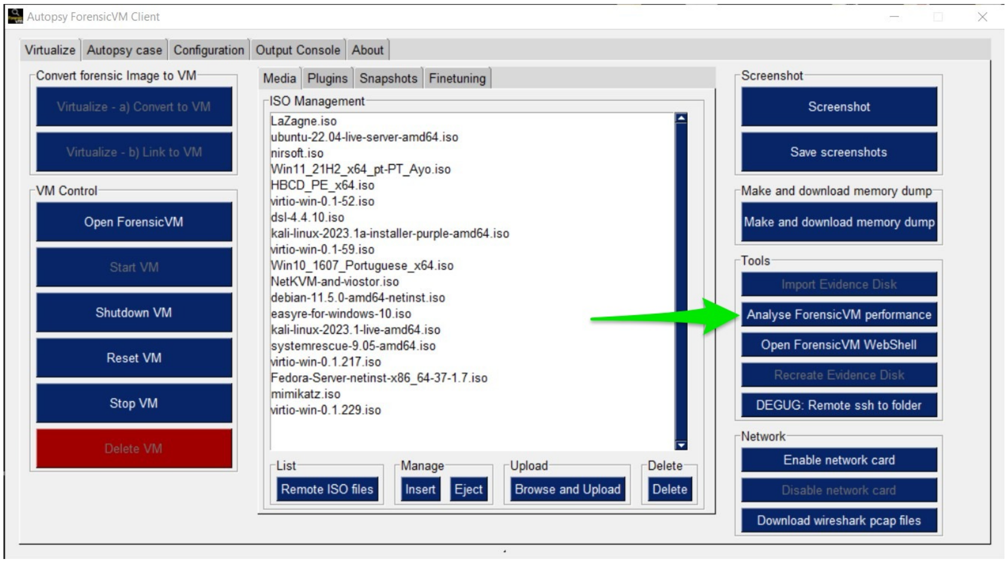
7.21.3 How to Start with Netdata on ForensicVM Server

Installation:

Netdata is already installed on ForensicVM Server.

How to Use the Netdata **Dashboard**:

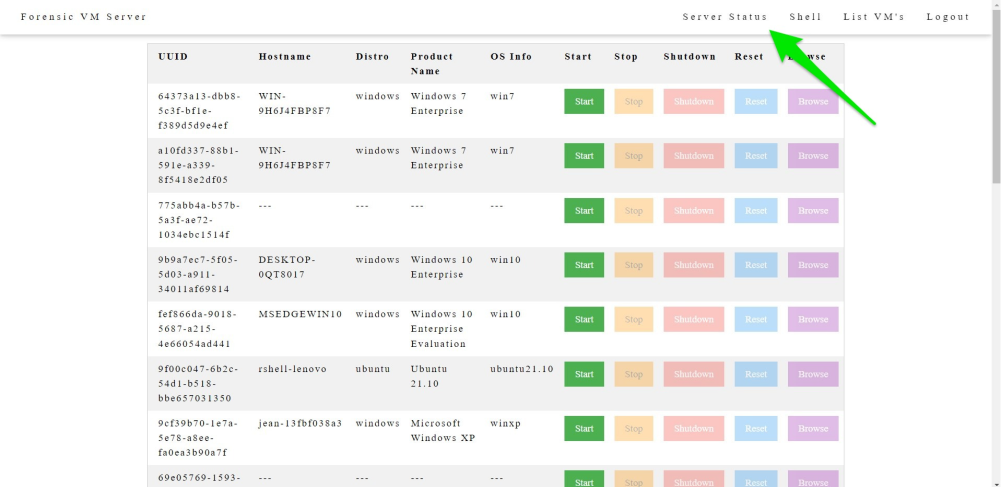
You can open it from the Autopsy ForensicVM Client Plugin:



LaZagne.iso
ubuntu-22.04-live-server-amd64.iso
nirsoft.iso
Win11_21H2_x64_pt-PT_Ayo.iso
HBCD_PE_x64.iso
virtio-win-0.1-52.iso
dsl-4.4.10.iso
kali-linux-2023.1a-installer-purple-amd64.iso
virtio-win-0.1-59.iso
Win10_1607_Portuguese_x64.iso
NetKVM-and-viostor.iso
debian-11.5.0-amd64-netinst.iso
easyre-for-windows-10.iso
kali-linux-2023.1-live-amd64.iso
systemrescue-9.05-amd64.iso
virtio-win-0.1.217.iso
Fedora-Server-netinst-x86_64-37-1.7.iso
mimikatz.iso
virtio-win-0.1.229.iso

Fig. 7.219: Opening Netdata through Autopsy

Or, use the ForensicVM main web page:

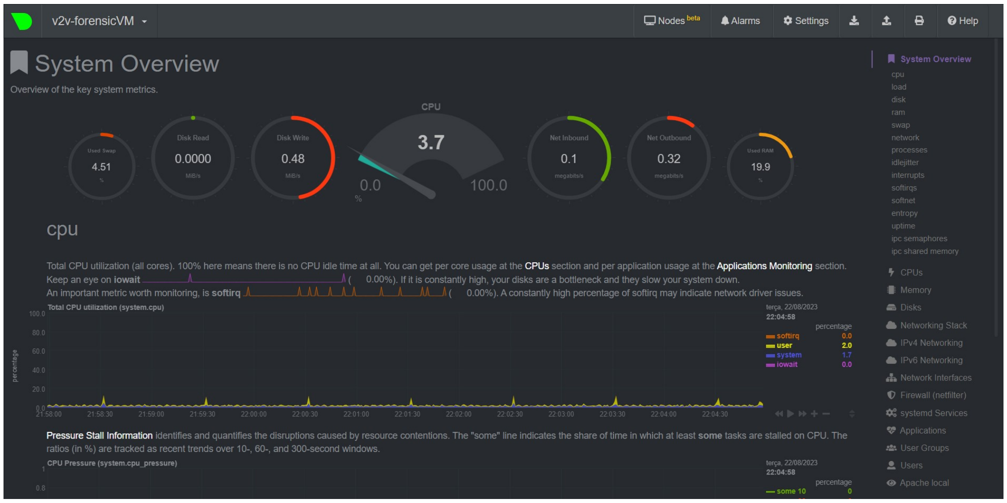


UUID	Hostname	Distro	Product Name	OS Info	Start	Stop	Shutdown	Reset	Browse
64373a13-dbb8-5c3f-bf1e-f389d5d9e4ef	WIN-9H6J4FBP8F7	windows	Windows 7 Enterprise	win7	Start	Stop	Shutdown	Reset	Browse
a10fd337-88b1-591e-a339-8f5418e2df05	WIN-9H6J4FBP8F7	windows	Windows 7 Enterprise	win7	Start	Stop	Shutdown	Reset	Browse
775abb4a-b57b-5a3f-ae72-1034ebc1514f	---	---	---	---	Start	Stop	Shutdown	Reset	Browse
9b9a7ec7-5f05-5d03-a911-34011af69814	DESKTOP-0QT8017	windows	Windows 10 Enterprise	win10	Start	Stop	Shutdown	Reset	Browse
fef866da-9018-5687-a215-4e66054ad441	MSEDGEWIN10	windows	Windows 10 Enterprise Evaluation	win10	Start	Stop	Shutdown	Reset	Browse
9f00c047-6b2c-54d1-b518-bbe657031350	rshell-lenovo	ubuntu	Ubuntu 21.10	ubuntu21.10	Start	Stop	Shutdown	Reset	Browse
9cf39b70-1e7a-5e78-a8ee-fa0ea3b90a7f	jean-13fbf038a3	windows	Microsoft Windows XP	winxp	Start	Stop	Shutdown	Reset	Browse
69e05769-1593-	---	---	---	---	Start	Stop	Shutdown	Reset	Browse

Fig. 7.220: Opening Netdata from the main page

7.21.4 How Netdata Helps with ForensicVM Server

Example of what you see:



Overview of the key system metrics.

Total CPU utilization (all cores). 100% here means there is no CPU idle time at all. You can get per core usage at the **CPUs** section and per application usage at the **Applications Monitoring** section.
Keep an eye on **iowait** (0.00%). If it is constantly high, your disks are a bottleneck and they slow your system down.
An important metric worth monitoring, is **softirq** (0.00%). A constantly high percentage of softirq may indicate network driver issues.

Pressure Stall Information identifies and quantifies the disruptions caused by resource contentions. The "some" line indicates the share of time in which at least **some** tasks are stalled on CPU. The ratios (in %) are tracked as recent trends over 10-, 60-, and 300-second windows.

Fig. 7.221: Netdata Dashboard view

- **CPU**: See how much CPU is being used. If it's too much, maybe add more resources.
- **Memory**: Make sure there's enough RAM for all the tasks.
- Disk Activity: Make sure the disk isn't too busy. If it is, tasks might slow down.
- **Network**: Keep an eye on data coming in and out, especially with big files.
- **Alerts**: Set warnings for important things, like if RAM use is very high.

7.21.5 Making Netdata Work for You

- Set Your Alarms: Set warnings for things that matter to you.
- **Your Dashboard**: Make a dashboard that shows what's important for your tasks.
- Connect with Other Tools: Netdata can send alerts to places like Slack, Twilio, or email.

Netdata is a great helper for those using ForensicVM Server. It watches over things and makes sure all is good. For admins, it's a must-have tool.

Note: To learn more about Netdata, visit the [Netdata website](https://learn.netdata.cloud/).

7.22 ForensicVM Case Study - Bart the hacker

7.22.1 Challenge Description

This appendix details the ForensicVM Case Study and Challenge, which is designed to highlight the differences between the evidence collected by dead-box forensics and live-forensics in a virtualized environment. The data set was created with VirtualBox and features a Windows 11 Pro environment equipped with various local and cloud applications. The image was captured using the FTK Imager in Expert Witness Format (EWF).

- Virtualisation is required to extract vital evidence.
- Bypassing the 'Bart' password is necessary to access the applications.
- Existing passwords within the data set must remain unchanged to maintain the integrity of the challenge.
- The Bart windows password is simple, but the challenge encourages ethical hacking skills to bypass or decrypt it.

7.22.2 Steps to Solve the Challenge

The following steps provide a structured approach to tackle the ForensicVM challenge:

1. Utilise dead box forensics techniques in autopsy software to attempt full data retrieval from cloud applications and local applications. Document all findings.
2. Virtualize the forensic image using the autopsy ForensicVM plugin.
3. Attempt to identify and bypass the Bart password to gain access to the applications.
4. Run the ForensicVM
5. Without internet access, systematically extract information from each application cloud and local application. Document all findings.
6. Enable internet access and repeat the information extraction process, noting any differences.
7. Record any additional information obtained after establishing an Internet connection.
8. Identify and document information related to the two financial applications present in the environment.
9. Extract and analyse data related to cryptocurrency.
10. Create a comprehensive chain of custody for all investigative actions taken.
11. Conduct and document a memory dump and network traffic dump.

12. Capture all investigative actions via video and take screenshots for evidence support.

For further information, refer to the ForensicVM Autopsy Plugin User Manual available at:

ForensicVM Autopsy Plugin User Manual

The complete dataset can be accessed via the following links:

- Google Drive Dataset
- Zenodo Dataset
- NIST CFReDS Dataset

7.23 Challenge Solution

7.23.1 Dead box forensics

The resolution of the digital forensic challenge began with the establishment of a new case within the forensic autopsy software. The initial phase involved the creation of a case as captured in Figure Fig. 7.222.

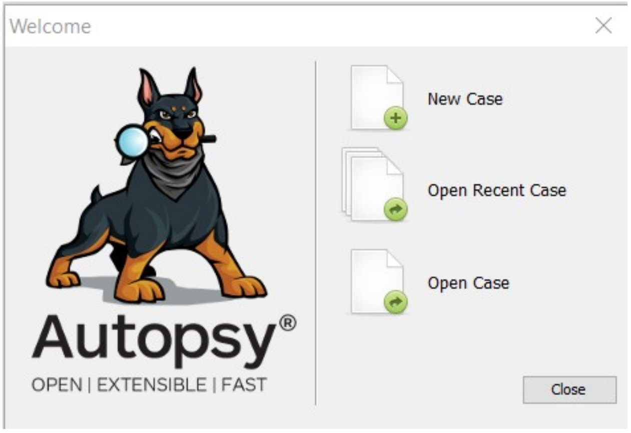
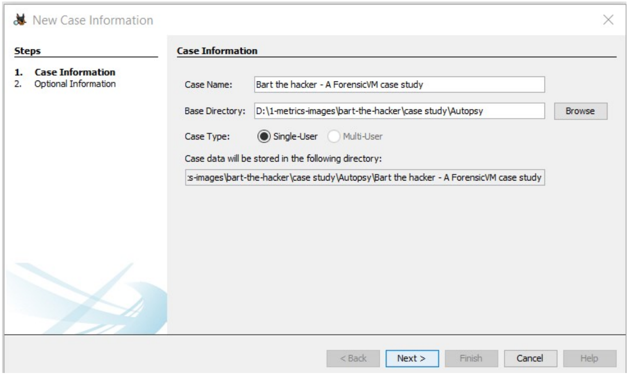


Fig. 7.222: Creation of a New Case

Subsequently, the case details were entered as demonstrated in Figure Fig. 7.223, ensuring that all pertinent information was correctly documented.



Case Name: Bart the hacker - A ForensicVM case study

Base Directory: D:\1-metrics-images\bart-the-hacker\case study\Autopsy

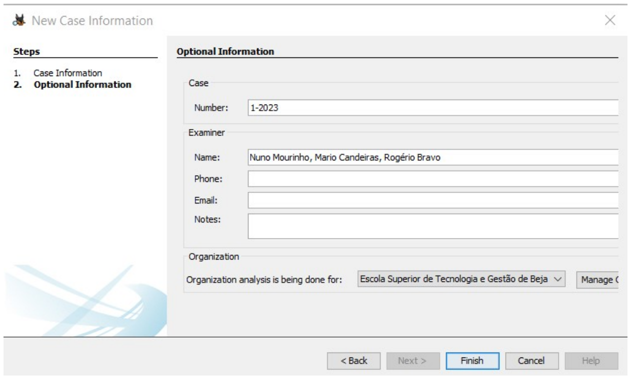
Case Type: ● Single-User ○ Multi-User

Case data will be stored in the following directory:

:s-images\bart-the-hacker\case study\Autopsy\Bart the hacker - A ForensicVM case study

Fig. 7.223: Entering Case Information

Optional case information was also provided to provide additional context and metadata for the investigation, as shown in Figure Fig. 7.224.



Steps

1. Case Information
2. **Optional Information**

Optional Information

Case

Number: 1-2023

Examiner

Name: Nuno Mourinho, Mario Candeiras, Rogério Bravo

Phone:

Email:

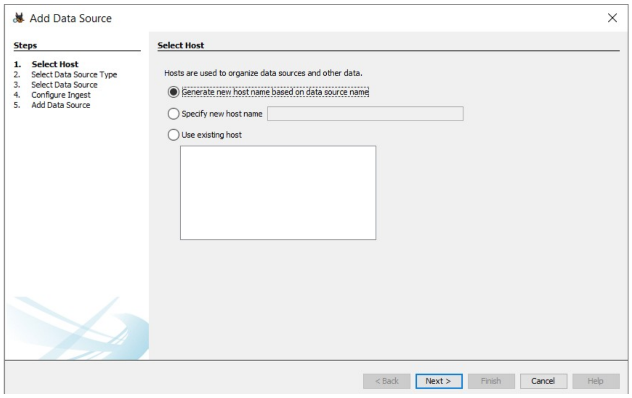
Notes:

Organization

Organization analysis is being done for: Escola Superior de Tecnologia e Gestão de Beja

Fig. 7.224: Providing Optional Case Information

To facilitate analysis, host information was generated as shown in Figure Fig. 7.225, which helps align the investigative environment with the specifics of the case.



Steps

1. **Select Host**
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source

Select Host

Hosts are used to organize data sources and other data.

● Generate new host name based on data source name

○ Specify new host name

○ Use existing host

Fig. 7.225: Generating Host Information

The subsequent step was to select the disk image or VM file that contained the forensic evidence, ensuring that the correct data source was incorporated into the investigation (Figure Fig. 7.226).

The timezone configuration is critical for accurate timestamp analysis; therefore, the forensic image path was established and the timezone was adjusted to Europe/Lisbon as part of the configuration process (Figure Fig. 7.227).

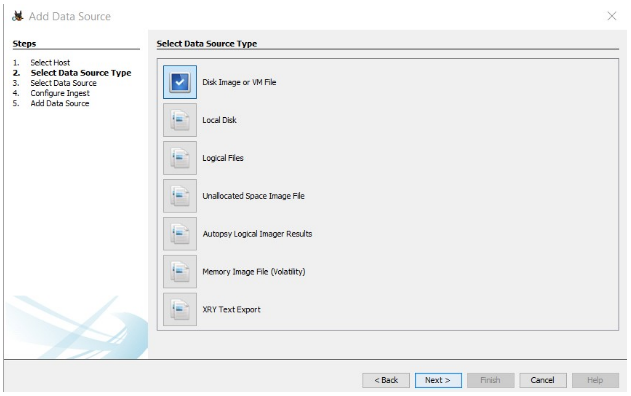
For initial data processing, ingest plugins were selected, specifically 'Recent Activity' and 'Picture Analyser', to extract relevant user activities and image-related evidence (Figure Fig. 7.228).

The investigator then waited for the completion of the addition of the data source, monitoring the progress to ensure successful incorporation into the case (Figure Fig. 7.229).

Upon successful addition of the data source, as confirmed by the software, the evidence was ready for a thorough examination (Figure Fig. 7.230).

Exploration within the "Os accounts" section yielded security answers that were potential avenues for password bypass efforts, with all answers being "textbf{bart}", which could provide a breakthrough in the case (Figure Fig. 7.231).

In the process of forensic analysis, the discovery of the password 'textbf{Lisa@Springfield}' via the Autofill feature in the Autopsy Web form represents a pivotal development. This password is a critical piece of evidence for the case, as it could potentially grant access to restricted areas that may contain further information or clues. The uncovering of this



Add Data Source

Steps

1. Select Host
2. **Select Data Source Type**
3. Select Data Source
4. Configure Ingest
5. Add Data Source

Select Data Source Type

☑ Disk Image or VM File

Local Disk

Logical Files

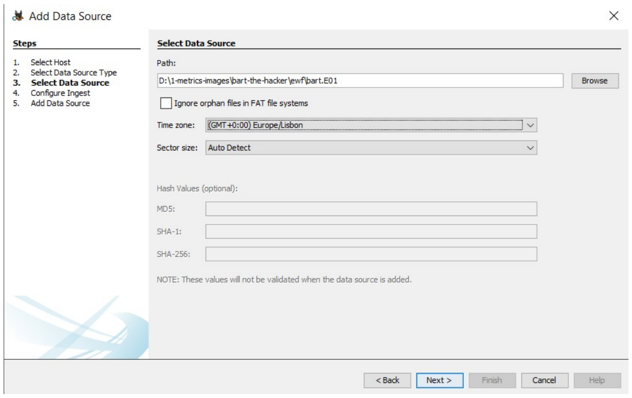
Unallocated Space Image File

Autopsy Logical Imager Results

Memory Image File (Volatility)

XRY Text Export

Fig. 7.226: Disk Image or VM File Selection



Add Data Source

Steps

1. Select Host
2. Select Data Source Type
3. **Select Data Source**
4. Configure Ingest
5. Add Data Source

Select Data Source

Path: D:\1-metrics-images\bart-the-hacker\ewf\bart.E01

□ Ignore orphan files in FAT file systems

Time zone: (GMT+0:00) Europe/Lisbon

Sector size: Auto Detect

Hash Values (optional):

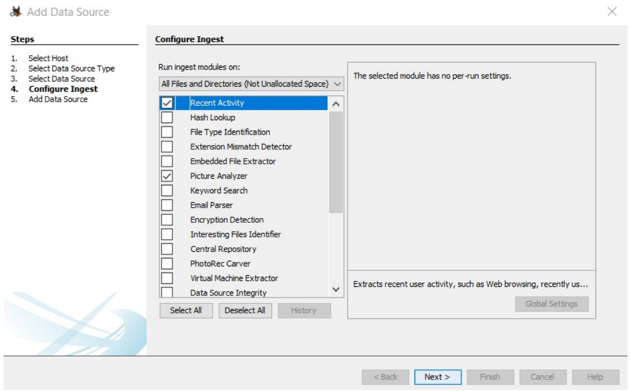
MD5:

SHA-1:

SHA-256:

NOTE: These values will not be validated when the data source is added.

Fig. 7.227: Configuring the Forensic Image Path and Timezone :label: fig:autopsy_0006



Add Data Source

Steps

1. Select Host
2. Select Data Source Type
3. Select Data Source
4. **Configure Ingest**
5. Add Data Source

Configure Ingest

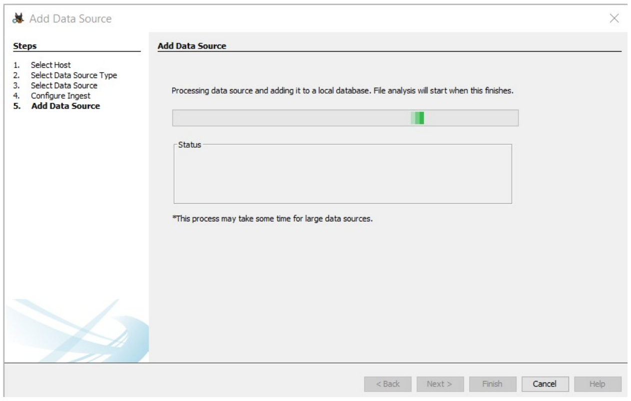
Run ingest modules on: All Files and Directories (Not Unallocated Space)

☑ Recent Activity
□ Hash Lookup
□ File Type Identification
□ Extension Mismatch Detector
□ Embedded File Extractor
☑ Picture Analyzer
□ Keyword Search
□ Email Parser
□ Encryption Detection
□ Interesting Files Identifier
□ Central Repository
□ PhotoRec Carver
□ Virtual Machine Extractor
□ Data Source Integrity

The selected module has no per-run settings.

Extracts recent user activity, such as Web browsing, recently us...

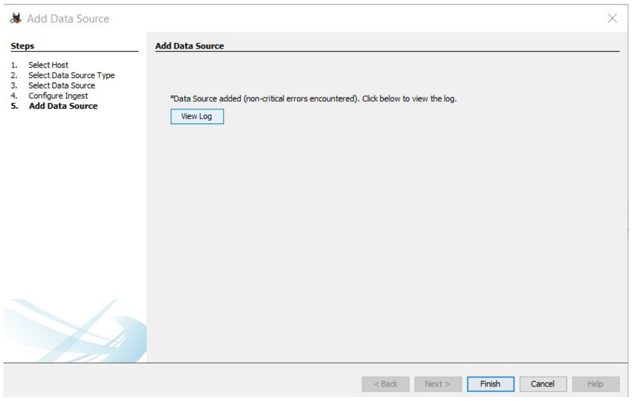
Fig. 7.228: Selection of Initial Ingest Plugins



Processing data source and adding it to a local database. File analysis will start when this finishes.

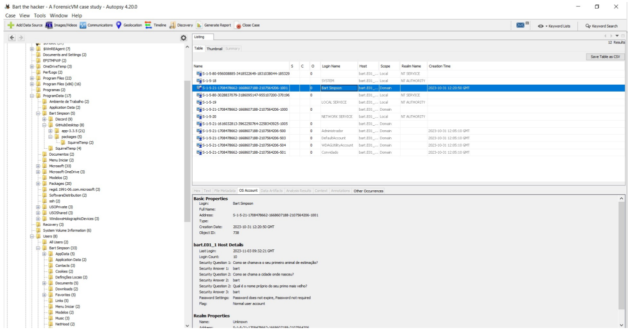
*This process may take some time for large data sources.

Fig. 7.229: Monitoring Data Source Addition



*Data Source added (non-critical errors encountered). Click below to view the log.

Fig. 7.230: Confirmation of Data Source Addition

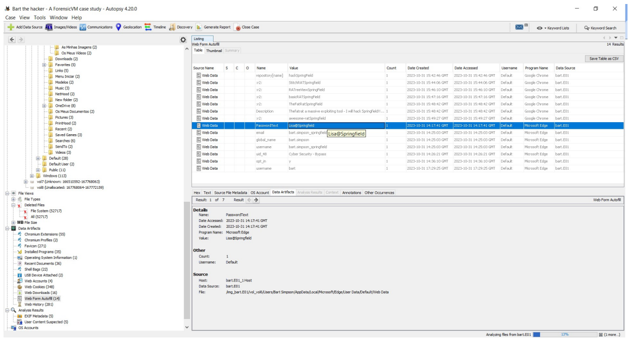


Name	S	C	O	Login Name	Host	Scope	Realm Name	Creation Time
S-1-5-80-956008885-3418522649-1831038044-185329			0		bart.E01_...	Local	NT SERVICE	
S-1-5-18				SYSTEM	bart.E01_...	Local	NT AUTHORITY	
S-1-5-21-1708478662-1668607188-2107564206-1001			0	Bart Simpson	bart.E01_...	Domain		2023-10-31 12:20:50 GMT
S-1-5-80-3028837079-3186095147-955107200-370196			0		bart.E01_...	Local	NT SERVICE	
S-1-5-19				LOCAL SERVICE	bart.E01_...	Local	NT AUTHORITY	
S-1-5-21-1708478662-1668607188-2107564206-1000			0		bart.E01_...	Domain		
S-1-5-20				NETWORK SERVICE	bart.E01_...	Local	NT AUTHORITY	
S-1-5-21-1616032813-3962250764-2258343925-1005			0		bart.E01_...	Domain		
S-1-5-21-1708478662-1668607188-2107564206-500			0	Administrador	bart.E01_...	Domain		2023-10-31 12:05:10 GMT
S-1-5-21-1708478662-1668607188-2107564206-503			0	DefaultAccount	bart.E01_...	Domain		2023-10-31 12:05:10 GMT
S-1-5-21-1708478662-1668607188-2107564206-504			0	WDAGUtilityAccount	bart.E01_...	Domain		2023-10-31 12:05:10 GMT
S-1-5-21-1708478662-1668607188-2107564206-501			0	Convidado	bart.E01_...	Domain		2023-10-31 12:05:10 GMT

```
Basic Properties
    Login:               Bart Simpson
    Full Name:
    Address:             S-1-5-21-1708478662-1668607188-2107564206-1001
    Type:
    Creation Date:       2023-10-31 12:20:50 GMT
    Object ID:           738

bart.E01_1 Host Details
    Last Login:          2023-11-03 09:32:21 GMT
    Login Count:         10
    Security Question 1: Como se chamava o seu primeiro animal de estimação?
    Security Answer 1:   bart
    Security Question 2: Como se chama a cidade onde nasceu?
    Security Answer 2:   bart
    Security Question 2: Qual é o nome próprio do seu primo mais velho?
    Security Answer 3:   bart
    Password Settings:   Password does not expire, Password not required
    Flag:                Normal user account

Realm Properties
    Name:                Unknown
    Address:             S-1-5-21-1708478662-1668607188-2107564206
```

Fig. 7.231: OS Accounts and Security Answers

password, as displayed in Figure Fig. 7.232, underscores the importance of thorough examination of digital artefacts which may hold vital information within a forensic investigation.



Source Name	S	C	O	Name	Value	Count	Date Created	Date Accessed	Username	Program Name	Data Source
Web Data				repository[name]	hackSpringField	1	2023-10-31 15:42:46 GMT	2023-10-31 15:42:46 GMT	Default	Google Chrome	bart.E01
Web Data				:r2:	StitchRATSpringfield	1	2023-10-31 15:44:06 GMT	2023-10-31 15:44:06 GMT	Default	Google Chrome	bart.E01
Web Data				:r2:	RATreeViewSpringField	1	2023-10-31 15:46:10 GMT	2023-10-31 15:46:10 GMT	Default	Google Chrome	bart.E01
Web Data				:r2:	basicRATSpringField	1	2023-10-31 15:47:16 GMT	2023-10-31 15:47:16 GMT	Default	Google Chrome	bart.E01
Web Data				:r2:	TheFatRatSpringField	1	2023-10-31 15:48:42 GMT	2023-10-31 15:48:42 GMT	Default	Google Chrome	bart.E01
Web Data				Description	Thefatrat a massive exploiting tool - I will hack Springfield!!...	1	2023-10-31 15:48:42 GMT	2023-10-31 15:48:42 GMT	Default	Google Chrome	bart.E01
Web Data				:r2:	awesome-ratSpringfield	1	2023-10-31 15:49:27 GMT	2023-10-31 15:49:27 GMT	Default	Google Chrome	bart.E01
Web Data				PasswordText	Lisa@Springfield	1	2023-10-31 14:17:41 GMT	2023-10-31 14:17:41 GMT	Default	Microsoft Edge	bart.E01
Web Data				email	bart.simpson_springfield	1	2023-10-31 14:25:03 GMT	2023-10-31 14:25:03 GMT	Default	Microsoft Edge	bart.E01
Web Data				global_name	bart.simpson	1	2023-10-31 14:25:03 GMT	2023-10-31 14:25:03 GMT	Default	Microsoft Edge	bart.E01
Web Data				username	bart.simpson_springfield	1	2023-10-31 14:25:03 GMT	2023-10-31 14:25:03 GMT	Default	Microsoft Edge	bart.E01
Web Data				uid_48	Cyber Security - Bypass	1	2023-10-31 14:26:21 GMT	2023-10-31 14:26:21 GMT	Default	Microsoft Edge	bart.E01
Web Data				opt_in	y	1	2023-10-31 14:36:10 GMT	2023-10-31 14:36:10 GMT	Default	Microsoft Edge	bart.E01
Web Data				username	bart	1	2023-10-31 17:29:25 GMT	2023-10-31 17:29:25 GMT	Default	Microsoft Edge	bart.E01

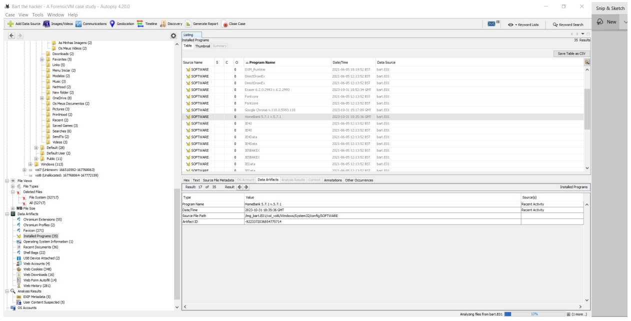
Details
Name: PasswordText
Date Accessed: 2023-10-31 14:17:41 GMT
Date Created: 2023-10-31 14:17:41 GMT
Program Name: Microsoft Edge
Value: Lisa@Springfield

Other
Count: 1
Username: Default

Source
Host: bart.E01_1 Host
Data Source: bart.E01
File: /img_bart.E01/vol_vol6/Users/Bart Simpson/AppData/Local/Microsoft/Edge/User Data/Default/Web Data

Fig. 7.232: Discovery of a Password via Web Form Autofill

Moreover, the identification of specific applications such as Eraser 6.2.0.2993, which is designed for secure file deletion, and HomeBank 5.7.1, a personal finance application, can offer valuable insights into the suspect's actions and intents. As depicted in Figure Fig. 7.233, the presence of these applications may suggest attempts to conceal activities or manage finances in a way that is pertinent to the investigation.

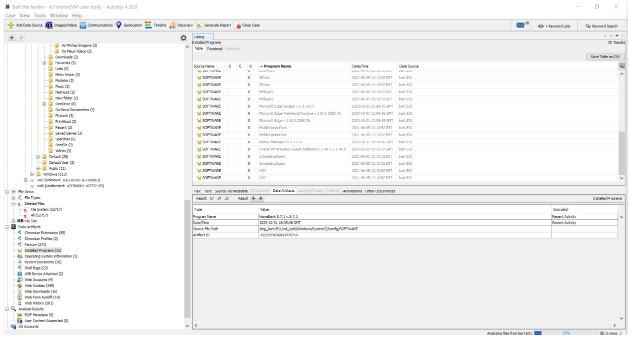


Source Name	S	C	O	Program Name	Date/Time	Data Source
SOFTWARE			0	DXM_Runtime	2021-06-05 18:19:52 BST	bart.E01
SOFTWARE			0	DirectDrawEx	2021-06-05 12:13:52 BST	bart.E01
SOFTWARE			0	DirectDrawEx	2021-06-05 12:13:52 BST	bart.E01
SOFTWARE			0	Eraser 6.2.0.2993 v.6.2.2993	2023-10-31 18:52:34 GMT	bart.E01
SOFTWARE			0	Fontcore	2021-06-05 12:13:52 BST	bart.E01
SOFTWARE			0	Fontcore	2021-06-05 12:13:52 BST	bart.E01
SOFTWARE			0	Google Chrome v.118.0.5993.118	2023-10-31 15:17:09 GMT	bart.E01
SOFTWARE			0	HomeBank 5.7.1 v.5.7.1	2023-10-31 18:35:36 GMT	bart.E01
SOFTWARE			0	IE40	2021-06-05 12:13:52 BST	bart.E01
SOFTWARE			0	IE40	2021-06-05 12:13:52 BST	bart.E01
SOFTWARE			0	IE4Data	2021-06-05 12:13:52 BST	bart.E01
SOFTWARE			0	IE4Data	2021-06-05 12:13:52 BST	bart.E01
SOFTWARE			0	IE5BAKEX	2021-06-05 12:13:52 BST	bart.E01
SOFTWARE			0	IE5BAKEX	2021-06-05 12:13:52 BST	bart.E01
SOFTWARE			0	IEData	2021-06-05 12:13:52 BST	bart.E01
SOFTWARE			0	IEData	2021-06-05 12:13:52 BST	bart.E01

Type	Value	Source(s)
Program Name	HomeBank 5.7.1 v.5.7.1	Recent Activity
Date/Time	2023-10-31 18:35:36 GMT	Recent Activity
Source File Path	/img_bart.E01/vol_vol6/Windows/System32/config/SOFTWARE	
Artifact ID	-9223372036854775714	

Fig. 7.233: Applications of Interest Including Secure File Deletion and Personal Finance Management Tools

The further discovery of Money Manager Ex v.1.6.4, another financial management tool, as indicated in Figure Fig. 7.234, reinforces the financial angle of the user's activity profile. This could be integral to constructing a narrative regarding the suspect's financial dealings or motivations.

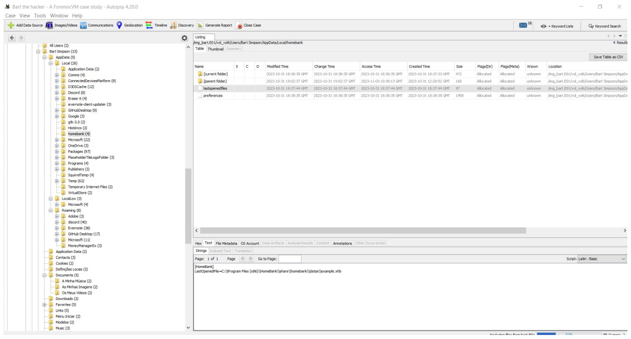


Source Name	S	C	O	Program Name	Date/Time	Data Source
SOFTWARE			0	IEData	2021-06-05 12:13:52 BST	bart.E01
SOFTWARE			0	IEData	2021-06-05 12:13:52 BST	bart.E01
SOFTWARE			0	MPlayer2	2021-06-05 18:19:52 BST	bart.E01
SOFTWARE			0	MPlayer2	2021-06-05 18:19:52 BST	bart.E01
SOFTWARE			0	Microsoft Edge Update v.1.3.181.5	2023-10-31 12:04:15 GMT	bart.E01
SOFTWARE			0	Microsoft Edge WebView2 Runtime v.118.0.2088.76	2023-10-31 12:09:46 GMT	bart.E01
SOFTWARE			0	Microsoft Edge v.118.0.2088.76	2023-10-31 12:08:45 GMT	bart.E01
SOFTWARE			0	MobileOptionPack	2021-06-05 12:13:52 BST	bart.E01
SOFTWARE			0	MobileOptionPack	2021-06-05 12:13:52 BST	bart.E01
SOFTWARE			0	Money Manager EX v.1.6.4	2023-10-31 18:34:06 GMT	bart.E01
SOFTWARE			0	Oracle VM VirtualBox Guest Additions 6.1.40 v.6.1.40.0	2023-10-31 19:33:37 GMT	bart.E01
SOFTWARE			0	SchedulingAgent	2021-06-05 12:13:52 BST	bart.E01
SOFTWARE			0	SchedulingAgent	2021-06-05 12:13:52 BST	bart.E01
SOFTWARE			0	WIC	2021-06-05 12:13:52 BST	bart.E01
SOFTWARE			0	WIC	2021-06-05 12:13:52 BST	bart.E01

Type	Value	Source(s)
Program Name	HomeBank 5.7.1 v.5.7.1	Recent Activity
Date/Time	2023-10-31 18:35:36 GMT	Recent Activity
Source File Path	/img_bart.E01/vol_vol6/Windows/System32/config/SOFTWARE	
Artifact ID	-9223372036854775714	

Fig. 7.234: Additional Financial Application Money Manager Ex Indicating In-Depth Financial Activities

Lastly, the opening of a financial database named example.xhb from the HomeBank files, as shown in Figure Fig. 7.235, further corroborates the financial dimension of the investigation. This particular file may contain transaction records, budgets, or other financial data which could be analysed to provide a clearer understanding of the suspect's financial behaviour or potential illicit activities.



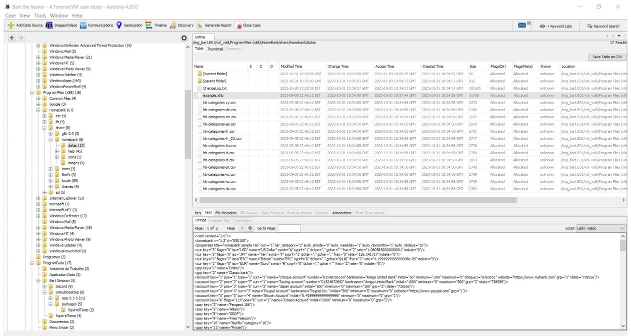
/img_bart.E01/vol_vol6/Users/Bart Simpson/AppData/Local/homebank

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
[current folder]				2023-10-31 18:38:35 GMT	2023-10-31 18:38:35 GMT	2023-10-31 18:38:35 GMT	2023-10-31 18:37:33 GMT	472	Allocated	Allocated	unknown	/img_bart.E01/vol_vol6/Users/Bart Simpson/AppDa
[parent folder]				2023-10-31 19:02:37 GMT	2023-10-31 19:02:37 GMT	2023-11-03 10:38:13 GMT	2023-10-31 12:20:52 GMT	168	Allocated	Allocated	unknown	/img_bart.E01/vol_vol6/Users/Bart Simpson/AppDa
lastopenedfiles				2023-10-31 18:37:44 GMT	2023-10-31 18:37:44 GMT	2023-10-31 18:37:44 GMT	2023-10-31 18:37:44 GMT	97	Allocated	Allocated	unknown	/img_bart.E01/vol_vol6/Users/Bart Simpson/AppDa
preferences				2023-10-31 18:38:35 GMT	2023-10-31 18:38:35 GMT	2023-10-31 18:38:35 GMT	2023-10-31 18:38:35 GMT	1958	Allocated	Allocated	unknown	/img_bart.E01/vol_vol6/Users/Bart Simpson/AppDa

```
[HomeBank]
LastOpenedFile=C:\\Program Files (x86)\\HomeBank\\share\\homebank\\datas\\example.xhb
```

Fig. 7.235: Opened Financial Database example.xhb Revealing Recent User Activities with Financial Data

The discovery of the example.xhb database in XML format, as depicted in Figure Fig. 7.236, adds a layer of complexity due to the proprietary structure of the file. This could imply that special attention must be paid to decipher the data structure to interpret the financial information contained within. The proprietary nature of the format might necessitate the use of specific tools or methods to extract and analyse the data accurately.



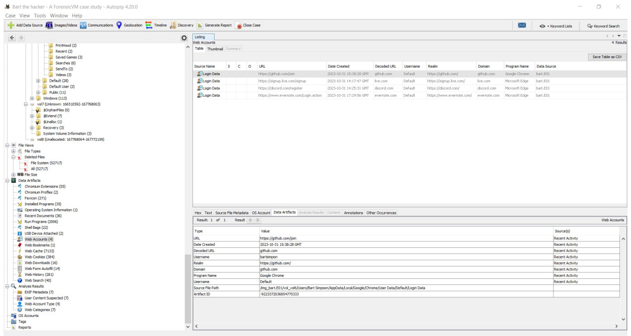
/img_bart.E01/vol_vol6/Program Files (x86)/HomeBank/share/homebank/datas

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
[current folder]				2023-10-31 18:34:58 GMT	2023-10-31 18:34:58 GMT	2023-11-03 10:05:35 GMT	2023-10-31 18:34:57 GMT	56	Allocated	Allocated	unknown	/img_bart.E01/vol_vol6/Program Files (x86
[parent folder]				2023-10-31 18:35:03 GMT	2023-10-31 18:35:03 GMT	2023-11-03 10:04:33 GMT	2023-10-31 18:34:57 GMT	432	Allocated	Allocated	unknown	/img_bart.E01/vol_vol6/Program Files (x86
ChangeLog.txt				2023-10-08 13:28:58 BST	2023-10-31 18:34:57 GMT	2023-10-31 18:34:57 GMT	2023-10-31 18:34:57 GMT	101685	Allocated	Allocated	unknown	/img_bart.E01/vol_vol6/Program Files (x86
example.xhb				2023-09-05 22:46:12 BST	2023-10-31 18:34:58 GMT	2023-10-31 18:37:44 GMT	2023-10-31 18:34:58 GMT	31766	Allocated	Allocated	unknown	/img_bart.E01/vol_vol6/Program Files (x86
hb-categories-cy.csv				2023-09-05 22:46:12 BST	2023-10-31 18:34:58 GMT	2023-10-31 18:34:58 GMT	2023-10-31 18:34:58 GMT	2273	Allocated	Allocated	unknown	/img_bart.E01/vol_vol6/Program Files (x86
hb-categories-de.csv				2023-09-05 22:46:12 BST	2023-10-31 18:34:58 GMT	2023-10-31 18:34:58 GMT	2023-10-31 18:34:58 GMT	2480	Allocated	Allocated	unknown	/img_bart.E01/vol_vol6/Program Files (x86
hb-categories-en.csv				2023-09-05 22:46:12 BST	2023-10-31 18:34:58 GMT	2023-10-31 18:34:58 GMT	2023-10-31 18:34:58 GMT	2242	Allocated	Allocated	unknown	/img_bart.E01/vol_vol6/Program Files (x86
hb-categories-es.csv				2023-09-05 22:46:12 BST	2023-10-31 18:34:58 GMT	2023-10-31 18:34:58 GMT	2023-10-31 18:34:58 GMT	2938	Allocated	Allocated	unknown	/img_bart.E01/vol_vol6/Program Files (x86
hb-categories-fr.csv				2023-09-05 22:46:12 BST	2023-10-31 18:34:58 GMT	2023-10-31 18:34:58 GMT	2023-10-31 18:34:58 GMT	2711	Allocated	Allocated	unknown	/img_bart.E01/vol_vol6/Program Files (x86
hb-categories-fr_CA.csv				2023-09-05 22:46:12 BST	2023-10-31 18:34:58 GMT	2023-10-31 18:34:58 GMT	2023-10-31 18:34:58 GMT	2717	Allocated	Allocated	unknown	/img_bart.E01/vol_vol6/Program Files (x86
hb-categories-hu.csv				2023-09-05 22:46:12 BST	2023-10-31 18:34:58 GMT	2023-10-31 18:34:58 GMT	2023-10-31 18:34:58 GMT	2790	Allocated	Allocated	unknown	/img_bart.E01/vol_vol6/Program Files (x86
hb-categories-it.csv				2023-09-05 22:46:12 BST	2023-10-31 18:34:58 GMT	2023-10-31 18:34:58 GMT	2023-10-31 18:34:58 GMT	2750	Allocated	Allocated	unknown	/img_bart.E01/vol_vol6/Program Files (x86
hb-categories-lt.csv				2023-09-05 22:46:12 BST	2023-10-31 18:34:58 GMT	2023-10-31 18:34:58 GMT	2023-10-31 18:34:58 GMT	2053	Allocated	Allocated	unknown	/img_bart.E01/vol_vol6/Program Files (x86
hb-categories-pt.csv				2023-09-05 22:46:12 BST	2023-10-31 18:34:58 GMT	2023-10-31 18:34:58 GMT	2023-10-31 18:34:58 GMT	2740	Allocated	Allocated	unknown	/img_bart.E01/vol_vol6/Program Files (x86
hb-categories-ro.csv				2023-09-05 22:46:12 BST	2023-10-31 18:34:58 GMT	2023-10-31 18:34:58 GMT	2023-10-31 18:34:58 GMT	2799	Allocated	Allocated	unknown	/img_bart.E01/vol_vol6/Program Files (x86
hb-categories-ru.csv				2023-09-05 22:46:12 BST	2023-10-31 18:34:58 GMT	2023-10-31 18:34:58 GMT	2023-10-31 18:34:58 GMT	4749	Allocated	Allocated	unknown	/img_bart.E01/vol_vol6/Program Files (x86
hb-categories-sk.csv				2023-09-05 22:46:12 BST	2023-10-31 18:34:58 GMT	2023-10-31 18:34:58 GMT	2023-10-31 18:34:58 GMT	2304	Allocated	Allocated	unknown	/img_bart.E01/vol_vol6/Program Files (x86

```
<?xml version="1.0"?>
<homebank v="1.3" d="050100">
<properties title="HomeBank Sample File" curr="1" car_category="2" auto_smode="0" auto_weekday="1" auto_nbmonths="1" auto_nbdays="10"/>
<cur key="3" flags="0" iso="USD" name="US Dollar" symb="$" syprf="1" dchar="," gchar=" " frac="2" rate="1.0805830000000001" mdate="0"/>
<cur key="2" flags="0" iso="JPY" name="Yen" symb="¥" syprf="1" dchar="." gchar="," frac="0" rate="158.141717" mdate="0"/>
<cur key="4" flags="2" iso="BTC" name="Bitcoin" symb="BTC" syprf="0" dchar="." gchar="(null)" frac="2" rate="4.1999999999999998e-05" mdate="0"/>
<cur key="1" flags="0" iso="EUR" name="Euro" symb="€" syprf="0" dchar="," gchar=" " frac="2" rate="0" mdate="0"/>
<grp key="1" name="Online"/>
<grp key="2" name="Classic bank"/>
<account key="1" pos="1" type="1" curr="1" name="Cheque account" number="01548726554" bankname="Amiga United Bank" initial="50" minimum="-200" maximum="0" cheque1="8760951" website="https://www.mybank.com" grp="2" rdate="738556"/>
<account key="2" pos="2" type="7" curr="1" name="Saving account" number="01524872652" bankname="Amiga United Bank" initial="1000" minimum="0" maximum="500" grp="2" rdate="738556"/>
<account key="3" pos="3" type="6" curr="2" name="Japan account" initial="500" minimum="0" maximum="100" grp="2" rdate="738556"/>
<account key="4" pos="4" curr="3" name="Paypal Account" bankname="Paypal Inc." initial="500" minimum="0" maximum="0" website="https://www.paypal.com" grp="1"/>
<account key="5" pos="5" curr="4" name="Bitcoin Account" initial="0.41999999999999998" minimum="0" maximum="0" grp="1"/>
<account key="6" flags="114" pos="6" curr="1" name="Closed Account" initial="2000" minimum="0" maximum="0" grp="2"/>
<pay key="3" name="Peugeot 106"/>
<pay key="5" name="Allianz"/>
<pay key="8" name="GRDF"/>
<pay key="9" name="Free Telecom"/>
<pay key="10" name="Netflix" category="10"/>
<pay key="11" name="Prixtel"/>
```

Fig. 7.236: Proprietary XML Structure of the example.xhb Database

The identification of cloud applications in the forensic investigation is critical as it may provide insight into data that is not stored locally on the device. The accounts discovered through the Autopsy software, including GitHub, live.com, discord.com, and evernote.com, extend the potential for finding evidence to the cloud. The presence of these services as shown in Figure Fig. 7.237, suggests a broad range of user activity, from software development and project management to personal communication and note-taking, which could be relevant to the case.



Web Accounts

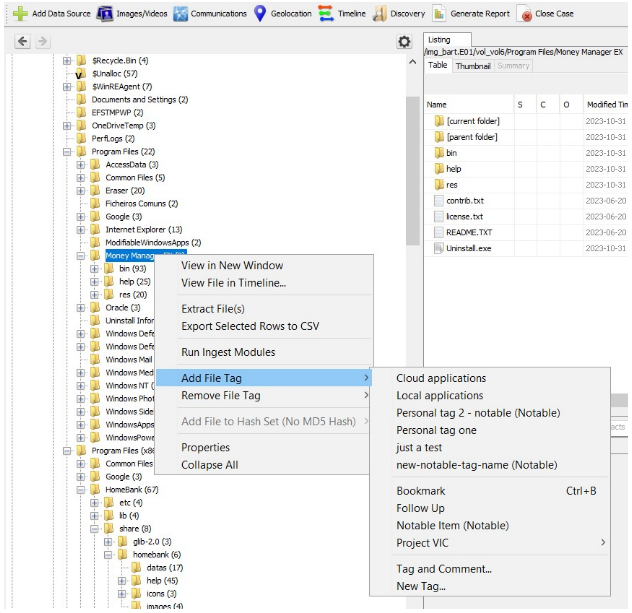
Source Name	S	C	O	URL	Date Created	Decoded URL	Username	Realm	Domain	Program Name	Data Source
Login Data				https://github.com/join	2023-10-31 15:38:28 GMT	github.com	Default	https://github.com/	github.com	Google Chrome	bart.E01
Login Data				https://signup.live.com/signup	2023-10-31 14:17:47 GMT	live.com	Default	https://signup.live.com/	live.com	Microsoft Edge	bart.E01
Login Data				https://discord.com/register	2023-10-31 14:25:31 GMT	discord.com	Default	https://discord.com/	discord.com	Microsoft Edge	bart.E01
Login Data				https://www.evernote.com/Login.action	2023-10-31 17:29:56 GMT	evernote.com	Default	https://www.evernote.com/	evernote.com	Microsoft Edge	bart.E01

Result: 1 of 1 Result — Web Accounts

Type	Value	Source(s)
URL	https://github.com/join	Recent Activity
Date Created	2023-10-31 15:38:28 GMT	Recent Activity
Decoded URL	github.com	Recent Activity
Username	bartsimpon	Recent Activity
Realm	https://github.com/	Recent Activity
Domain	github.com	Recent Activity
Program Name	Google Chrome	Recent Activity
Username	Default	Recent Activity
Source File Path	/img_bart.E01/vol_vol6/Users/Bart Simpson/AppData/Local/Google/Chrome/User Data/Default/Login Data	
Artifact ID	-9223372036854775333	

Fig. 7.237: Overview of Cloud Applications Uncovered in Autopsy

Tagging folders related to financial applications within Autopsy helps in organising evidence and highlights the importance of financial data in the investigation. As illustrated in Figure Fig. 7.238, tagging these folders ensures that relevant information is easily accessible and distinguishable from other unrelated data, facilitating a more efficient investigation process.

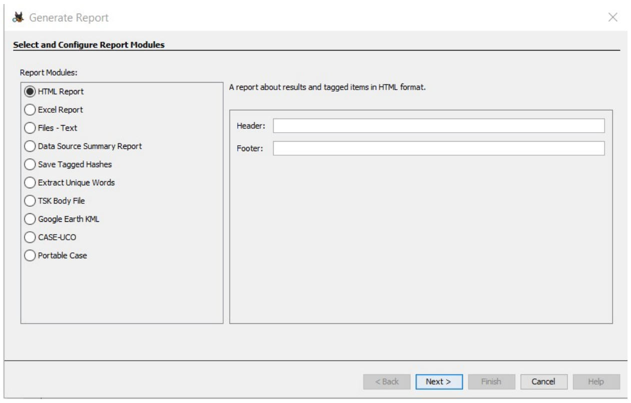


/img_bart.E01/vol_vol6/Program Files/Money Manager EX

Name	S	C	O	Modified Tim
[current folder]				2023-10-31
[parent folder]				2023-10-31
bin				2023-10-31
help				2023-10-31
res				2023-10-31
contrib.txt				2023-06-20
license.txt				2023-06-20
README.TXT				2023-06-20
Uninstall.exe				2023-10-31

Fig. 7.238: Tagging of Folders Pertaining to Financial Applications

The creation of an Autopsy HTML report is a critical step for documenting the investigation, offering a comprehensive and accessible format for presenting the findings. The series of figures, from Figure Fig. 7.239 to Figure Fig. 7.243, encapsulate various aspects of the report, from the general overview to specific details regarding data sources and tagged items.



● HTML Report
○ Excel Report
○ Files - Text
○ Data Source Summary Report
○ Save Tagged Hashes
○ Extract Unique Words
○ TSK Body File
○ Google Earth KML
○ CASE-UCO
○ Portable Case

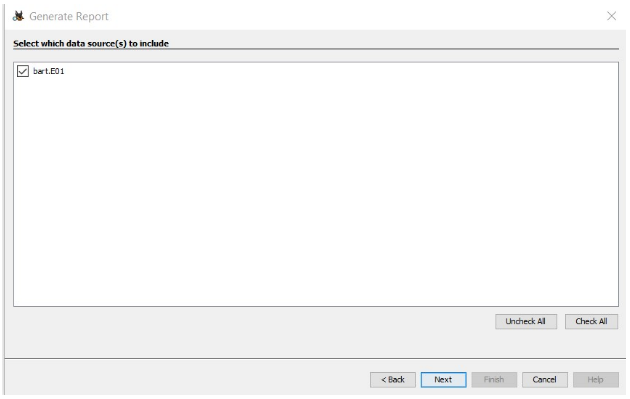
A report about results and tagged items in HTML format.

Header:

Footer:

Fig. 7.239: Snapshot of the Autopsy HTML Report Interface

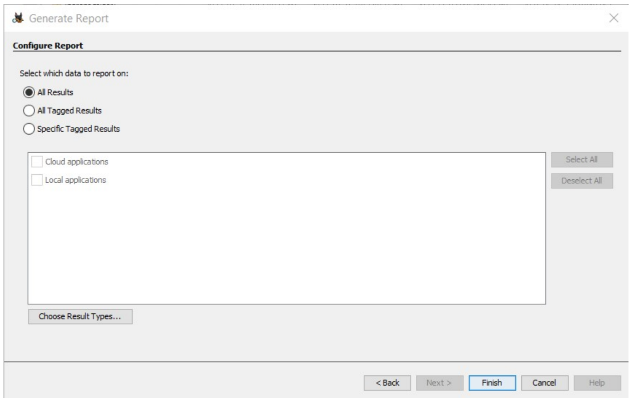
Local applications and those identified as relevant through tagging were systematically documented within the Autopsy report as well. This incorporation of tagged local and cloud applications allows for a more comprehensive review of the software environment of the system under investigation (Figure Fig. 7.244).



Select which data source(s) to include

☑ bart.E01

Fig. 7.240: Detailing the Data Source 'bart.E01' within the HTML Report



Configure Report

Select which data to report on:

● All Results

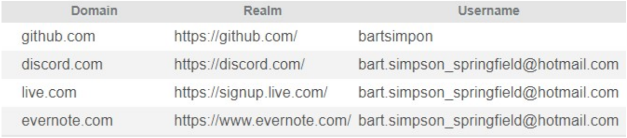
○ All Tagged Results

○ Specific Tagged Results

□ Cloud applications

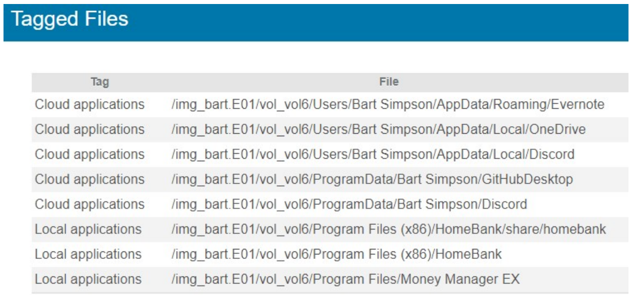
□ Local applications

Fig. 7.241: Autopsy HTML Report Showing Tagged Items and Analysis Results



Domain	Realm	Username
github.com	https://github.com/	bartsimpon
discord.com	https://discord.com/	bart.simpson_springfield@hotmail.com
live.com	https://signup.live.com/	bart.simpson_springfield@hotmail.com
evernote.com	https://www.evernote.com/	bart.simpson_springfield@hotmail.com

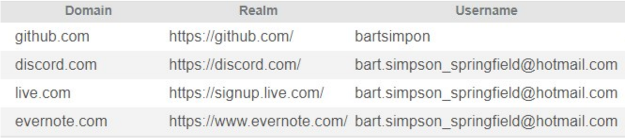
Fig. 7.242: Compilation of All Results in the Autopsy HTML Report



Tagged Files

Tag	File
Cloud applications	/img_bart.E01/vol_vol6/Users/Bart Simpson/AppData/Roaming/Evernote
Cloud applications	/img_bart.E01/vol_vol6/Users/Bart Simpson/AppData/Local/OneDrive
Cloud applications	/img_bart.E01/vol_vol6/Users/Bart Simpson/AppData/Local/Discord
Cloud applications	/img_bart.E01/vol_vol6/ProgramData/Bart Simpson/GitHubDesktop
Cloud applications	/img_bart.E01/vol_vol6/ProgramData/Bart Simpson/Discord
Local applications	/img_bart.E01/vol_vol6/Program Files (x86)/HomeBank/share/homebank
Local applications	/img_bart.E01/vol_vol6/Program Files (x86)/HomeBank
Local applications	/img_bart.E01/vol_vol6/Program Files/Money Manager EX

Fig. 7.243: Report Detailing Found Cloud Applications and Associated Usernames



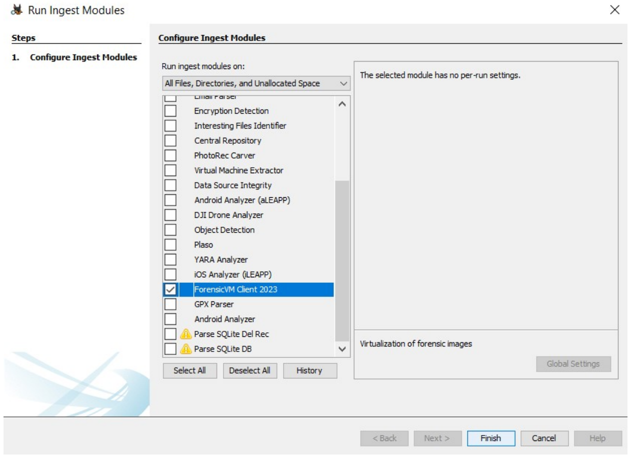
Domain	Realm	Username
github.com	https://github.com/	bartsimpon
discord.com	https://discord.com/	bart.simpson_springfield@hotmail.com
live.com	https://signup.live.com/	bart.simpson_springfield@hotmail.com
evernote.com	https://www.evernote.com/	bart.simpson_springfield@hotmail.com

Fig. 7.244: Tagged files depicting local and cloud applications within Autopsy

7.23.2 Live forensic with ForensicVM - Phase 1: Network disabled

The commencement of live forensics entails the virtualization of the forensic image, utilizing the capabilities of the ForensicVM server and client infrastructure.

The initial step involves initiating the ForensicVM client ingest module via Autopsy, as illustrated in Figure Fig. 7.245.



Run ingest modules on: All Files, Directories, and Unallocated Space

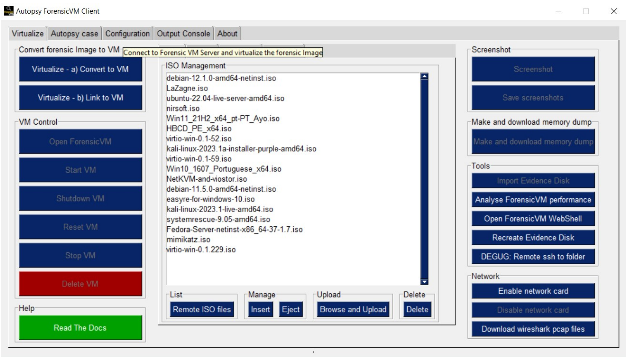
☐ Email Parser
☐ Encryption Detection
☐ Interesting Files Identifier
☐ Central Repository
☐ PhotoRec Carver
☐ Virtual Machine Extractor
☐ Data Source Integrity
☐ Android Analyzer (aLEAPP)
☐ DJI Drone Analyzer
☐ Object Detection
☐ Plaso
☐ YARA Analyzer
☐ iOS Analyzer (iLEAPP)
☑ ForensicVM Client 2023
☐ GPX Parser
☐ Android Analyzer
☐ Parse SQLite Del Rec
☐ Parse SQLite DB

The selected module has no per-run settings.

Virtualization of forensic images

Fig. 7.245: Run ingest modules: ForensicVM Client

Subsequently, a comprehensive virtualization of the image was executed. Utilizing the command textbf{Virtualize - a) Convert to VM}, a duplicate of the forensic image is created. This process entails altering the hardware abstraction layer by incorporating virtio optimized drivers, culminating in the creation of a ForensicVM, as depicted in Figure Fig. 7.246, Figure Fig. 7.247, and Figure Fig. 7.248.

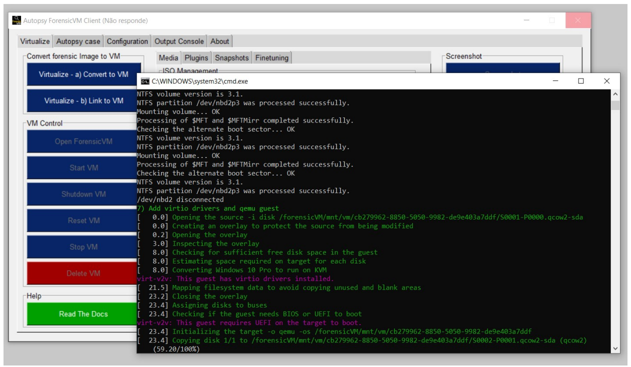


Connect to Forensic VM Server and virtualize the forensic Image

debian-12.1.0-amd64-netinst.iso
LaZagne.iso
ubuntu-22.04-live-server-amd64.iso
nirsoft.iso
Win11_21H2_x64_pt-PT_Ayo.iso
HBCD_PE_x64.iso
virtio-win-0.1-52.iso
kali-linux-2023.1a-installer-purple-amd64.iso
virtio-win-0.1-59.iso
Win10_1607_Portuguese_x64.iso
NetKVM-and-viostor.iso
debian-11.5.0-amd64-netinst.iso
easyre-for-windows-10.iso
kali-linux-2023.1-live-amd64.iso
systemrescue-9.05-amd64.iso
Fedora-Server-netinst-x86_64-37-1.7.iso
mimikatz.iso
virtio-win-0.1.229.iso

Fig. 7.246: ForensicVM client main form

The recovery questions were noted to be identical (textbf{bart}), prompting an attempt to use them as the password. This strategy proved effective due to the recovery questions being set identically to the password, as shown in Figure



```
NTFS volume version is 3.1.
NTFS partition /dev/nbd2p3 was processed successfully.
Mounting volume... OK
Processing of $MFT and $MFTMirr completed successfully.
Checking the alternate boot sector... OK
NTFS volume version is 3.1.
NTFS partition /dev/nbd2p3 was processed successfully.
Mounting volume... OK
Processing of $MFT and $MFTMirr completed successfully.
Checking the alternate boot sector... OK
NTFS volume version is 3.1.
NTFS partition /dev/nbd2p3 was processed successfully.
/dev/nbd2 disconnected
7) Add virtio drivers and qemu guest
[   0.0] Opening the source -i disk /forensicVM/mnt/vm/cb279962-8850-5050-9982-de9e403a7ddf/S0001-P0000.qcow2-sda
[   0.0] Creating an overlay to protect the source from being modified
[   0.2] Opening the overlay
[   3.0] Inspecting the overlay
[   8.0] Checking for sufficient free disk space in the guest
[   8.0] Estimating space required on target for each disk
[   8.0] Converting Windows 10 Pro to run on KVM
virt-v2v: This guest has virtio drivers installed.
[  21.5] Mapping filesystem data to avoid copying unused and blank areas
[  23.2] Closing the overlay
[  23.4] Assigning disks to buses
[  23.4] Checking if the guest needs BIOS or UEFI to boot
virt-v2v: This guest requires UEFI on the target to boot.
[  23.4] Initializing the target -o qemu -os /forensicVM/mnt/vm/cb279962-8850-5050-9982-de9e403a7ddf
[  23.4] Copying disk 1/1 to /forensicVM/mnt/vm/cb279962-8850-5050-9982-de9e403a7ddf/S0002-P0001.qcow2-sda (qcow2)
   (59.20/100%)
```

Fig. 7.247: Forensic image to forensicVM Conversion progress

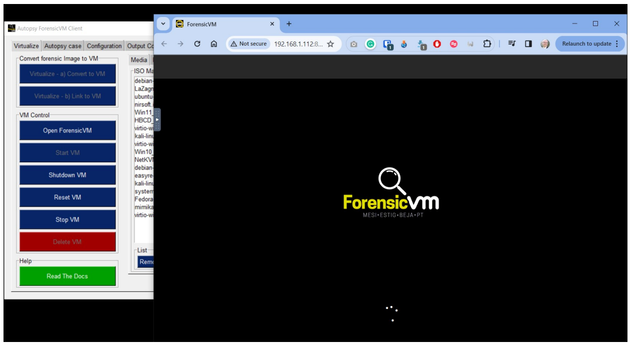


Fig. 7.248: ForensicVM First execution

Fig. 7.249.

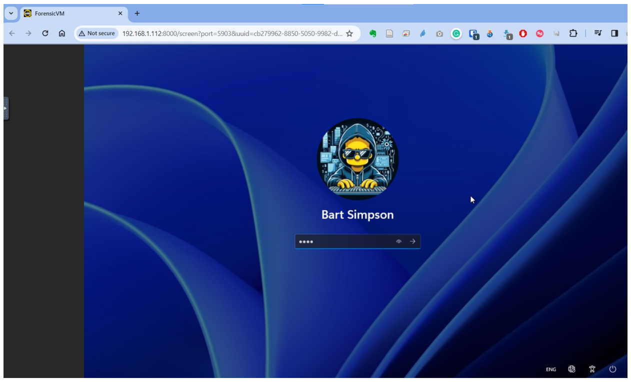

ForensicVM
Not secure
192.168.1.112:8000/screen?port=5903&uuid=cb279962-8850-5050-9982-d...
Bart Simpson
••••
ENG

Fig. 7.249: Password recovery utilizing identical security questions

Access was successfully gained to the Bart desktop, which featured a wallpaper indicating potential malicious intent with the message "I will hack Springfield…," as seen in Figure Fig. 7.250.

The desktop was populated with numerous icons, one of which was for the Evernote cloud application. Activating this icon initiated Evernote, within which several recent notes were apparent: Extra images, Secret nuclear plants, Bart Simpson Passwords, and My pass, as illustrated in Figure Fig. 7.251.

In the forensic investigation within the Evernote application, a notebook titled textbf{Bart secret plans} containing three notes was identified. The procedure to export these notes to the forensicVM evidence drive is crucial, as illustrated in Figure Fig. 7.252.

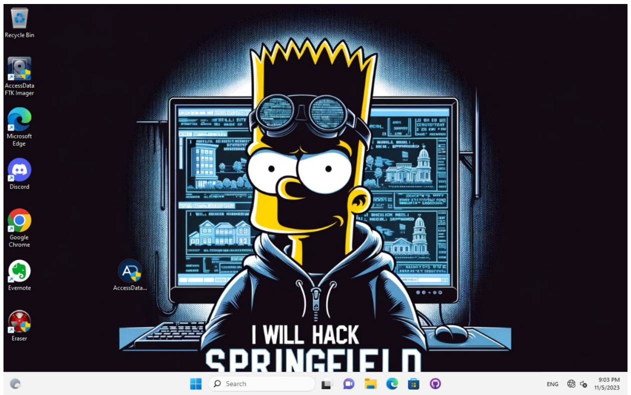
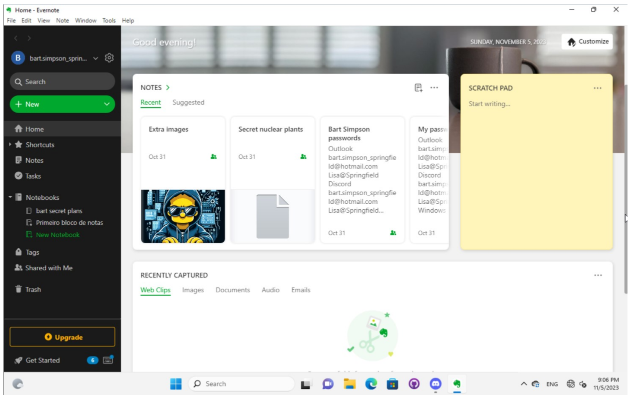


Fig. 7.250: Bart desktop with indicative wallpaper message

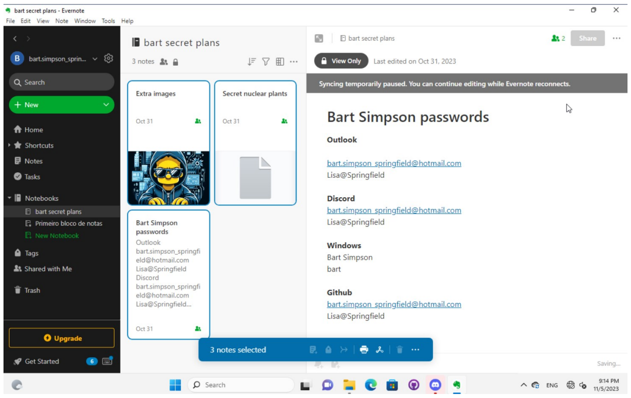


Extra images
Oct 31

Secret nuclear plants
Oct 31

Bart Simpson passwords
Outlook
bart.simpson_springfield@hotmail.com
Lisa@Springfield
Discord
bart.simpson_springfield@hotmail.com
Lisa@Springfield...
Oct 31

Fig. 7.251: Evernote application with recent notes



Last edited on Oct 31, 2023

Syncing temporarily paused. You can continue editing while Evernote reconnects.

Bart Simpson passwords

Outlook

bart.simpson_springfield@hotmail.com
Lisa@Springfield

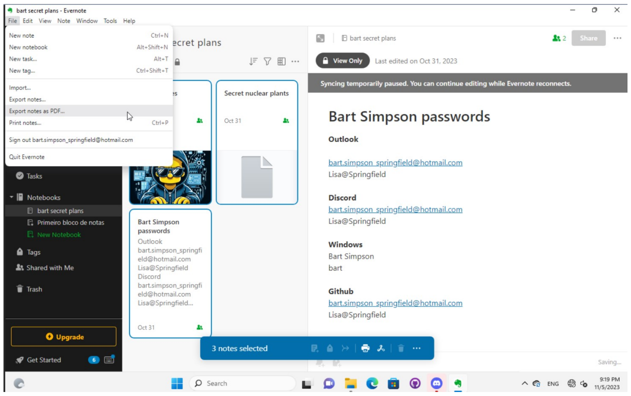
Discord
bart.simpson_springfield@hotmail.com
Lisa@Springfield

Windows
Bart Simpson
bart

Github
bart.simpson_springfield@hotmail.com
Lisa@Springfield

Fig. 7.252: Evernote notebook 'Bart secret plans'

To commence the note export process, the notes were first converted into PDF format as shown in Figure Fig. 7.253.



Last edited on Oct 31, 2023

Syncing temporarily paused. You can continue editing while Evernote reconnects.

Bart Simpson passwords

Outlook

bart.simpson_springfield@hotmail.com
Lisa@Springfield

Discord
bart.simpson_springfield@hotmail.com
Lisa@Springfield

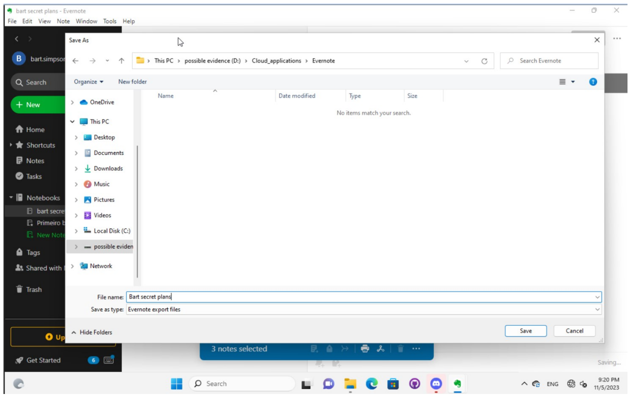
Windows
Bart Simpson
bart

Github
bart.simpson_springfield@hotmail.com
Lisa@Springfield

Bart Simpson passwords
Outlook
bart.simpson_springfield@hotmail.com
Lisa@Springfield
Discord
bart.simpson_springfield@hotmail.com
Lisa@Springfield...

Fig. 7.253: Exporting notes as PDF

The notes were then methodically stored in a subfolder named Evernote, located within the Cloud_applications tag in Autopsy. The textbf{Bart secret plans} file was exported to this specific folder, detailed in Figure Fig. 7.254.



This PC › possible evidence (D:) › Cloud_applications › Evernote

No items match your search.

File name: Bart secret plans
Save as type: Evernote export files

Fig. 7.254: PDF export destination folder structure

A verification step was conducted to ensure that the exported PDFs contained all potential evidence, as confirmed in Figure Fig. 7.255.

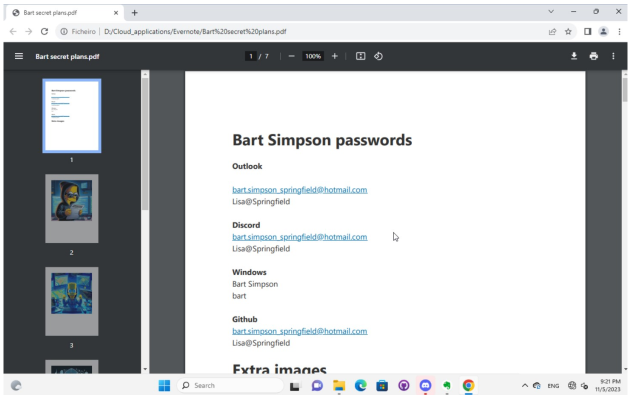
The export procedure was repeated for another notebook titled textbf{Primeiro bloco de notas}, which was also moved to the Evernote folder on the evidence disk, as depicted in Figure Fig. 7.256.

Investigation revealed that the **bart secret plans** notebook was shared by a user named **Nuno Mourinho**, which may indicate collaborative or shared use of the contents, as evidenced by Figures Fig. 7.257 and Fig. 7.258.

Additionally, the Evernote trash was scrutinized, and it was confirmed that no notes had been deleted, as shown in Figure Fig. 7.259. The absence of deleted notes might suggest that the user did not attempt to remove evidence or considered the contents of the notes to be non-incriminating.

The forensic analysis included the observation of software behavior in a controlled environment. The Discord application displayed a notification for an update, which could not be completed due to a lack of internet connectivity, leaving the application in a state of limbo as depicted in Figure Fig. 7.260.

Subsequently, GitHub Desktop was launched, which is a graphical client interface for interacting with GitHub repositories. It attempted to locate a repository named hackSpringField, but without internet access, the search was unsuccessful, as demonstrated in Figure Fig. 7.261.



Bart Simpson passwords

Outlook

bart.simpson_springfield@hotmail.com
Lisa@Springfield

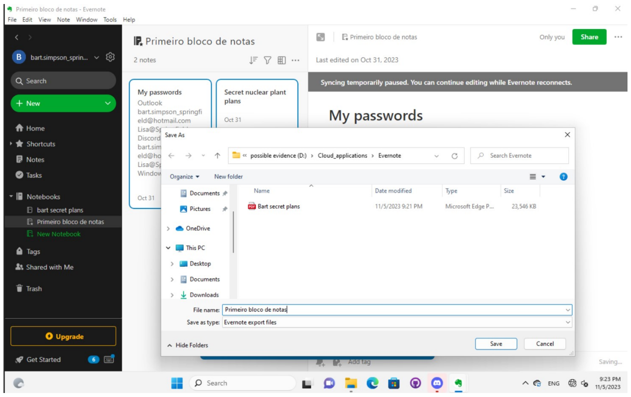
Discord
bart.simpson_springfield@hotmail.com
Lisa@Springfield

Windows
Bart Simpson
bart

Github
bart.simpson_springfield@hotmail.com
Lisa@Springfield

Extra images

Fig. 7.255: Verification of exported PDF content



Last edited on Oct 31, 2023

Syncing temporarily paused. You can continue editing while Evernote reconnects.

My passwords
Outlook
bart.simpson_springfield@hotmail.com
Lisa@Sp
Discord
bart.sim
eld@ho
Lisa@Sp
Window
Oct 31

Secret nuclear plant plans
Oct 31

My passwords

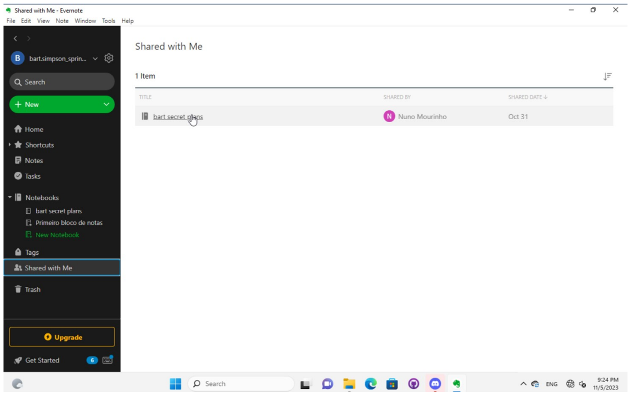
« possible evidence (D:) › Cloud_applications › Evernote

Name	Date modified	Type	Size
Bart secret plans	11/5/2023 9:21 PM	Microsoft Edge P...	23,546 KB

File name: Primeiro bloco de notas

Save as type: Evernote export files

Fig. 7.256: Exporting 'Primeiro bloco de notas' from Evernote

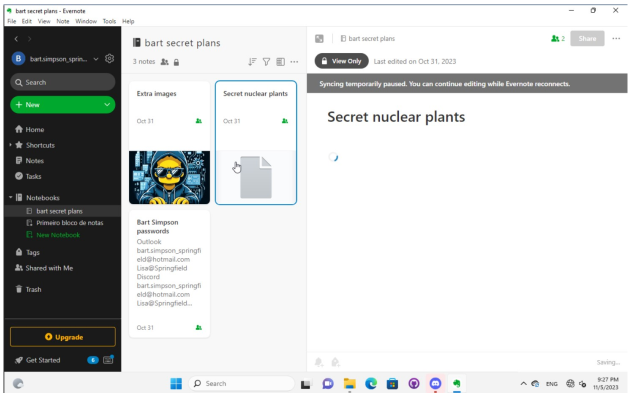


Shared with Me

1 Item

TITLE	SHARED BY	SHARED DATE ↓
bart secret plans	N Nuno Mourinho	Oct 31

Fig. 7.257: Shared user detail for 'bart secret plans' notebook



Last edited on Oct 31, 2023

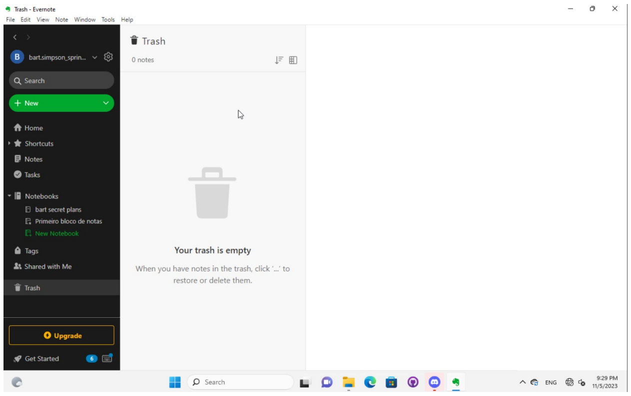
Syncing temporarily paused. You can continue editing while Evernote reconnects.

Secret nuclear plants

Bart Simpson passwords
Outlook
bart.simpson_springfield@hotmail.com
Lisa@Springfield
Discord
bart.simpson_springfield@hotmail.com
Lisa@Springfield...

Saving...

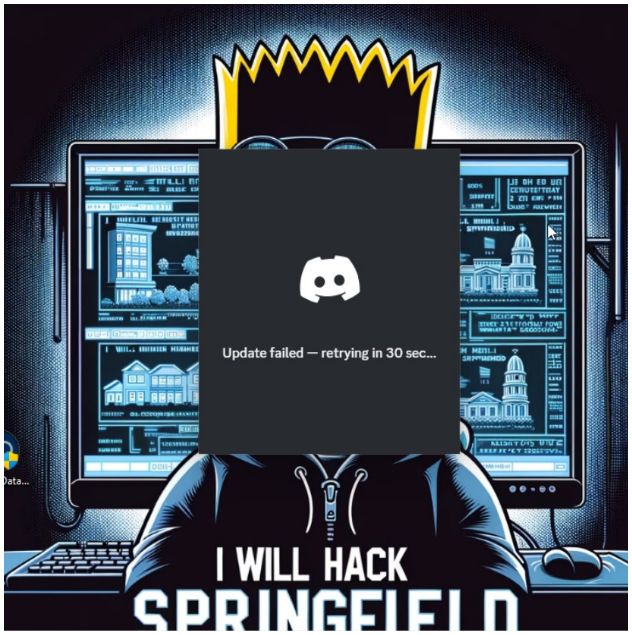
Fig. 7.258: Notebook sharing information indicating ‘Nuno Mourinho’



Your trash is empty

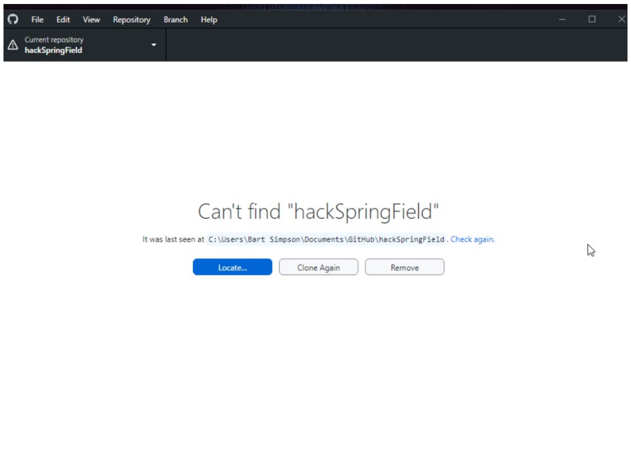
When you have notes in the trash, click '...' to restore or delete them.

Fig. 7.259: Checking Evernote trash for deleted notes



Update failed — retrying in 30 sec...

Fig. 7.260: Discord application unable to update without internet connection

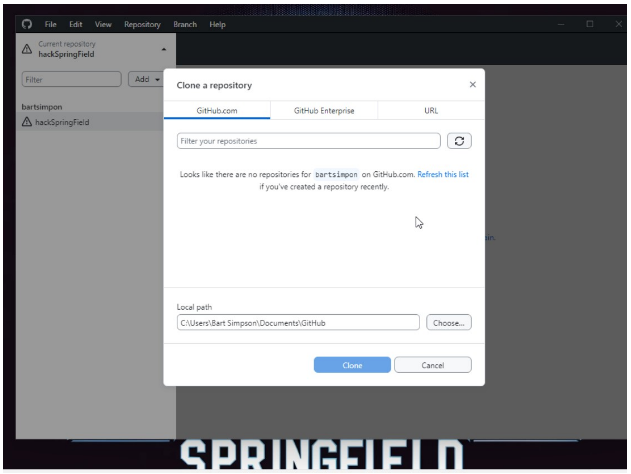


Can't find "hackSpringField"

It was last seen at `C:\Users\Bart Simpson\Documents\GitHub\hackSpringField`. Check again.

Fig. 7.261: GitHub Desktop failing to find the 'hackSpringField' repository

Due to the absence of an internet or local network connection, the content within the GitHub repository could not be retrieved or reviewed, which is an essential aspect to consider for future investigative steps. This scenario is highlighted in Figure Fig. 7.262.



Clone a repository

Filter your repositories

Looks like there are no repositories for `bartsimpon` on GitHub.com. Refresh this list if you've created a repository recently.

Local path: C:\Users\Bart Simpson\Documents\GitHub

Fig. 7.262: Unreachable GitHub repository contents due to lack of network connectivity

The investigation then moved to financial applications, with a specific focus on Homebank. An attempt to launch this application was made as indicated by the presence of its icon, and this is captured in Figure Fig. 7.263.

Upon accessing Homebank, the last opened file named example.xhb was identified, suggesting a possible area of interest for the investigation. The examination of this file is depicted in Figure Fig. 7.264.

Within the example.xhb file, the existence of a Bitcoin account was noted. Even though the file bore the name 'example', it was considered worthy of detailed examination to discern any potential financial improprieties or to trace financial transactions, as shown in Figure Fig. 7.265.

So far, this analysis underscores the complexity of digital forensics, particularly when dealing with cloud-based services and financial software, where access to the content is often restricted without proper connectivity or credentials.

Upon uncovering Bitcoin-related transaction data within the Homebank application, steps were taken to document this information. The transactions were exported to a PDF file for ease of analysis and future reference, a process captured in Figures Fig. 7.266 and Fig. 7.267.

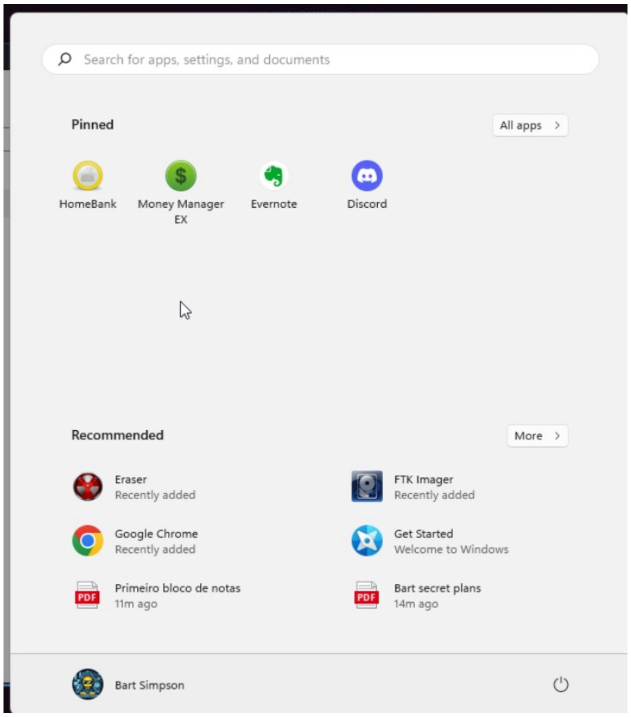


Fig. 7.263: Locating the Homebank application

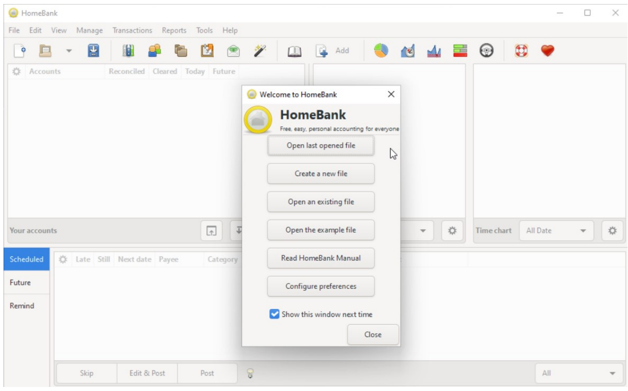
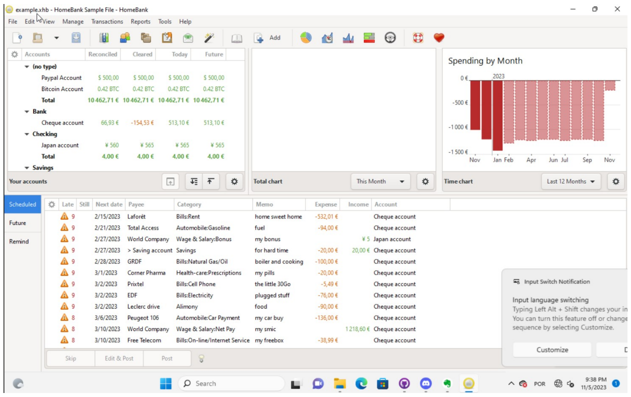


Fig. 7.264: Opening the last accessed file in Homebank


example.xhb - HomeBank Sample File - HomeBank
File Edit View Manage Transactions Reports Tools Help
Add

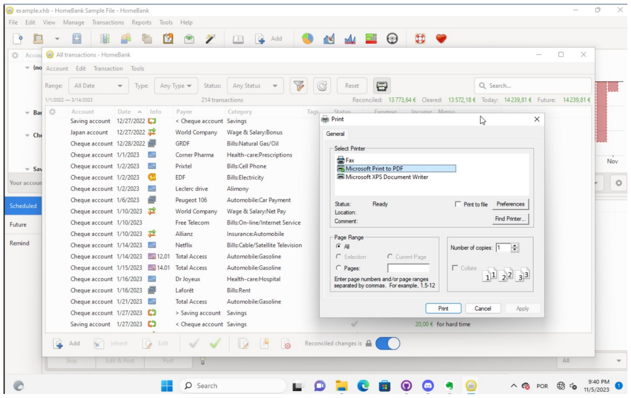
Accounts	Reconciled	Cleared	Today	Future
(no type)				
Paypal Account	$ 500,00	$ 500,00	$ 500,00	$ 500,00
Bitcoin Account	0.42 BTC	0.42 BTC	0.42 BTC	0.42 BTC
Total	10 462,71 €	10 462,71 €	10 462,71 €	10 462,71 €
Bank				
Cheque account	66,93 €	-154,53 €	513,10 €	513,10 €
Checking				
Japan account	¥ 560	¥ 565	¥ 565	¥ 565
Total	4,00 €	4,00 €	4,00 €	4,00 €
Savings				

Late	Still	Next date	Payee	Category	Memo	Expense	Income	Account
⚠ 9		2/15/2023	Laforêt	Bills:Rent	home sweet home	-532,01 €		Cheque account
⚠ 9		2/21/2023	Total Access	Automobile:Gasoline	fuel	-94,00 €		Cheque account
⚠ 9		2/27/2023	World Company	Wage & Salary:Bonus	my bonus		¥ 5	Japan account
⚠ 9		2/27/2023	> Saving account	Savings	for hard time	-20,00 €	20,00 €	Cheque account
⚠ 9		2/28/2023	GRDF	Bills:Natural Gas/Oil	boiler and cooking	-100,00 €		Cheque account
⚠ 9		3/1/2023	Corner Pharma	Health-care:Prescriptions	my pills	-20,00 €		Cheque account
⚠ 9		3/2/2023	Prixtel	Bills:Cell Phone	the little 30Go	-5,49 €		Cheque account
⚠ 9		3/2/2023	EDF	Bills:Electricity	plugged stuff	-76,00 €		Cheque account
⚠ 9		3/2/2023	Leclerc drive	Alimony	food	-90,00 €		Cheque account
⚠ 8		3/6/2023	Peugeot 106	Automobile:Car Payment	my car buy	-136,00 €		Cheque account
⚠ 8		3/10/2023	World Company	Wage & Salary:Net Pay	my smic		1 218,60 €	Cheque account
⚠ 8		3/10/2023	Free Telecom	Bills:On-line/Internet Service	my freebox	-38,99 €		Cheque account

Input Switch Notification

Input language switching
Typing Left Alt + Shift changes your in
You can turn this feature off or change
sequence by selecting Customize.

Fig. 7.265: Evidence of a Bitcoin account in the Homebank file ‘example.xhb’



example.xhb - HomeBank Sample File - HomeBank
File Edit View Manage Transactions Reports Tools Help
All transactions - HomeBank
Account Edit Transaction Tools
Range: All Date
Type: Any Type
Status: Any Status
Reset
Search...
Scheduled
Future
Remind
Add
Inherit
Edit
Skip
Edit & Post
Post
Reconciled changes is
Search

1/1/2022 — 3/14/2023 214 transactions

Reconciled: 13 773,64 € Cleared: 13 572,18 € Today: 14 239,81 € Future: 14 239,81 €

Account	Date	Info	Payee	Category
Saving account	12/27/2022		< Cheque account	Savings
Japan account	12/27/2022		World Company	Wage & Salary:Bonus
Cheque account	12/28/2022		GRDF	Bills:Natural Gas/Oil
Cheque account	1/1/2023		Corner Pharma	Health-care:Prescriptions
Cheque account	1/2/2023		Prixtel	Bills:Cell Phone
Cheque account	1/2/2023		EDF	Bills:Electricity
Cheque account	1/2/2023		Leclerc drive	Alimony
Cheque account	1/6/2023		Peugeot 106	Automobile:Car Payment
Cheque account	1/10/2023		World Company	Wage & Salary:Net Pay
Cheque account	1/10/2023		Free Telecom	Bills:On-line/Internet Service
Cheque account	1/10/2023		Allianz	Insurance:Automobile
Cheque account	1/14/2023		Netflix	Bills:Cable/Satellite Television
Cheque account	1/14/2023	12.01	Total Access	Automobile:Gasoline
Cheque account	1/15/2023	14.01	Total Access	Automobile:Gasoline
Cheque account	1/16/2023		Dr Joyeux	Health-care:Hospital
Cheque account	1/16/2023		Laforêt	Bills:Rent
Cheque account	1/21/2023		Total Access	Automobile:Gasoline
Cheque account	1/27/2023		> Saving account	Savings
Saving account	1/27/2023		< Cheque account	Savings

20,00 € for hard time

Print

General

Select Printer

- Fax
- Microsoft Print to PDF
- Microsoft XPS Document Writer

Status: Ready

Location:

Comment:

□ Print to file

Preferences

Find Printer...

Page Range

● All

○ Selection ○ Current Page

○ Pages:

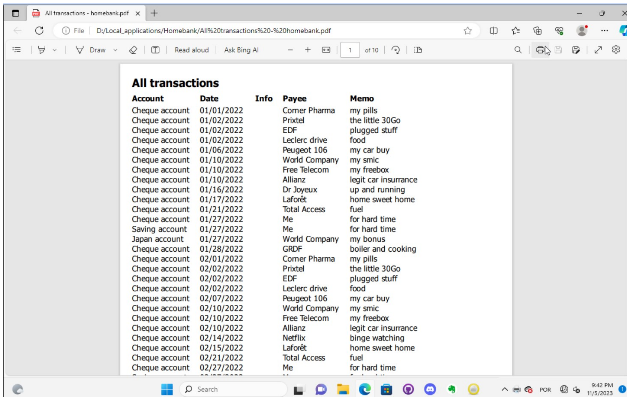
Enter page numbers and/or page ranges separated by commas. For example, 1,5-12

Number of copies: 1

□ Collate

Print Cancel Apply

Fig. 7.266: Exporting Bitcoin transaction data to PDF



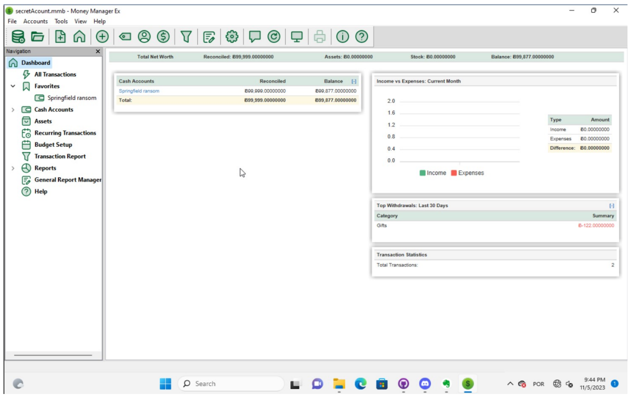
File D:/Local_applications/Homebank/All%20transactions%20-%20homebank.pdf

All transactions

Account	Date	Info	Payee	Memo
Cheque account	01/01/2022		Corner Pharma	my pills
Cheque account	01/02/2022		Prixtel	the little 30Go
Cheque account	01/02/2022		EDF	plugged stuff
Cheque account	01/02/2022		Leclerc drive	food
Cheque account	01/06/2022		Peugeot 106	my car buy
Cheque account	01/10/2022		World Company	my smic
Cheque account	01/10/2022		Free Telecom	my freebox
Cheque account	01/10/2022		Allianz	legit car insurrance
Cheque account	01/16/2022		Dr Joyeux	up and running
Cheque account	01/17/2022		Laforêt	home sweet home
Cheque account	01/21/2022		Total Access	fuel
Cheque account	01/27/2022		Me	for hard time
Saving account	01/27/2022		Me	for hard time
Japan account	01/27/2022		World Company	my bonus
Cheque account	01/28/2022		GRDF	boiler and cooking
Cheque account	02/01/2022		Corner Pharma	my pills
Cheque account	02/02/2022		Prixtel	the little 30Go
Cheque account	02/02/2022		EDF	plugged stuff
Cheque account	02/02/2022		Leclerc drive	food
Cheque account	02/07/2022		Peugeot 106	my car buy
Cheque account	02/10/2022		World Company	my smic
Cheque account	02/10/2022		Free Telecom	my freebox
Cheque account	02/10/2022		Allianz	legit car insurrance
Cheque account	02/14/2022		Netflix	binge watching
Cheque account	02/15/2022		Laforêt	home sweet home
Cheque account	02/21/2022		Total Access	fuel
Cheque account	02/27/2022		Me	for hard time

Fig. 7.267: The process of printing transaction data to a PDF file

The forensic examination then proceeded to another financial application, Money Manager Ex. Upon initiation, the application's dashboard revealed an account with the noteworthy title 'Springfield ransom', as displayed in Figure Fig. 7.268.



Total Net Worth Reconciled: ฿99,999.00000000 Assets: ฿0.00000000 Stock: ฿0.00000000 Balance: ฿99,877.00000000

Cash Accounts	Reconciled	Balance
Springfield ransom	฿99,999.00000000	฿99,877.00000000
Total:	฿99,999.00000000	฿99,877.00000000

Type	Amount
Income	฿0.00000000
Expenses	฿0.00000000
Difference:	฿0.00000000

Top Withdrawals: Last 30 Days

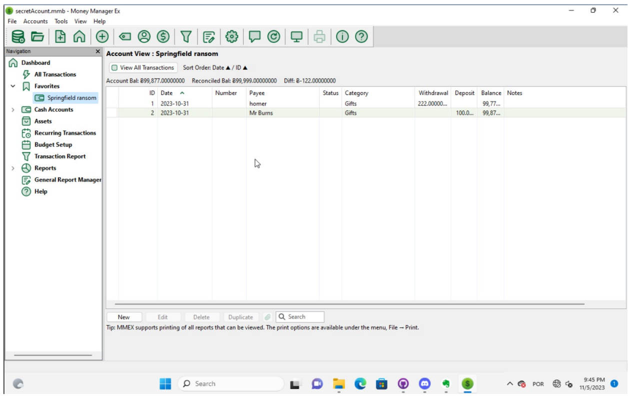
Category	Summary
Gifts	฿-122.00000000

Transaction Statistics

Total Transactions: 2

Fig. 7.268: Dashboard of Money Manager Ex showing the 'Springfield ransom' account

Within this application, two significant transactions were identified: a withdrawal of 222 million by a user named Homer, and a deposit of 100 million to a Mr. Burns. These transactions, detailed in Figure Fig. 7.269, could suggest a flow of funds that may be pertinent to the investigation.



Account View : Springfield ransom

□ View All Transactions Sort Order: Date ▲ / ID ▲

Account Bal: ฿99,877.00000000 Reconciled Bal: ฿99,999.00000000 Diff: ฿-122.00000000

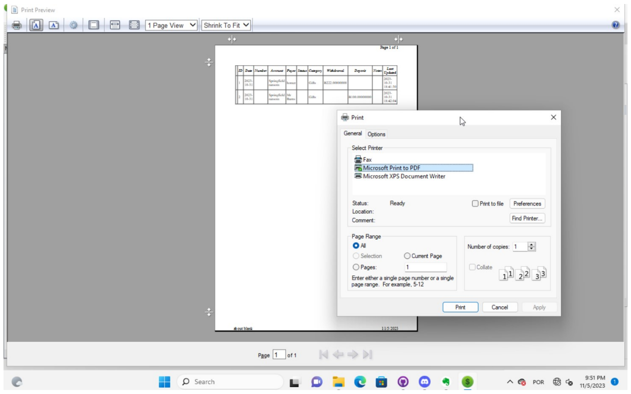
ID	Date	Number	Payee	Status	Category	Withdrawal	Deposit	Balance	Notes
1	2023-10-31		homer		Gifts	222.00000...		99,77...	
2	2023-10-31		Mr Burns		Gifts		100.0...	99,87...	

Tip: MMEX supports printing of all reports that can be viewed. The print options are available under the menu, File → Print.

Fig. 7.269: Transactions in Money Manager Ex involving significant sums of money

To collate the findings, a PDF document was created and stored on an evidence drive, ensuring the preservation of the data uncovered during the investigation. This step is illustrated in Figures Fig. 7.270 and ref{fig:autopsy_0056}.

Finally, verification was carried out to ensure that the PDF created indeed contained the exported transaction data, as can be affirmed by Figure Fig. 7.272.



Select Printer
Fax
Microsoft Print to PDF
Microsoft XPS Document Writer

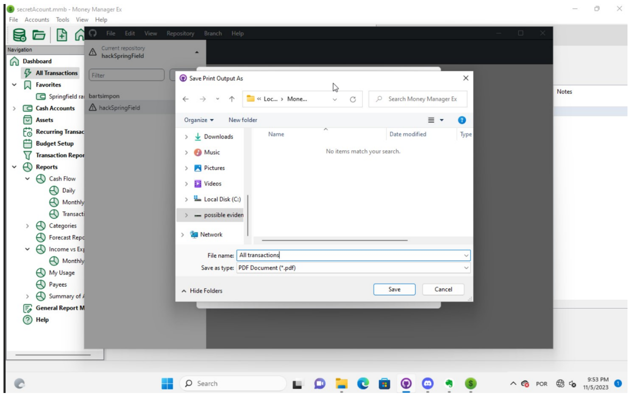
Status: Ready

Page Range
● All
○ Selection
○ Current Page
○ Pages: 1

Enter either a single page number or a single page range. For example, 5-12

Number of copies: 1

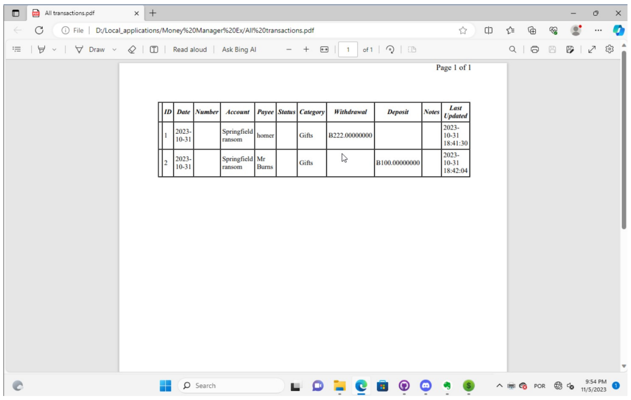
Fig. 7.270: Compiling findings into a PDF document



File name: All transactions

Save as type: PDF Document (*.pdf)

Fig. 7.271: Saving the PDF document to the evidence drive



D:/Local_applications/Money%20Manager%20Ex/All%20transactions.pdf

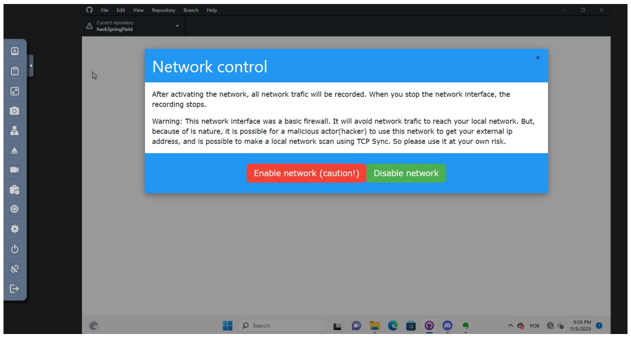
Page 1 of 1

	ID	Date	Number	Account	Payee	Status	Category	Withdrawal	Deposit	Notes	Last Updated
	1	2023-10-31		Springfield ransom	homer		Gifts	B222.00000000			2023-10-31 18:41:30
	2	2023-10-31		Springfield ransom	Mr Burns		Gifts		B100.00000000		2023-10-31 18:42:04

Fig. 7.272: Confirmation of the exported transaction data within the PDF document

7.23.3 Live forensic with ForensicVM - Phase 2: Network enabled

In the continuation of the live forensic analysis using ForensicVM, the investigation progressed to include cloud-based evidence following the activation of the network interface. This crucial step is depicted in Figure Fig. 7.273.


Network control

After activating the network, all network trafic will be recorded. When you stop the network interface, the recording stops.

Warning: This network interface was a basic firewall. It will avoid network trafic to reach your local network. But, because of is nature, it is possible for a malicious actor(hacker) to use this network to get your external ip address, and is possible to make a local network scan using TCP Sync. So please use it at your own risk.

Fig. 7.273: Enabling the network interface on the ForensicVM webscreen

One of the primary cloud applications scrutinised was GitHub Desktop. This application was of particular interest as it may contain repositories that could provide evidence of illicit activity if the computer in question belonged to a potential hacker. The repository named **hackSpringField** was cloned as an initial step, a process illustrated in Figure Fig. 7.274.

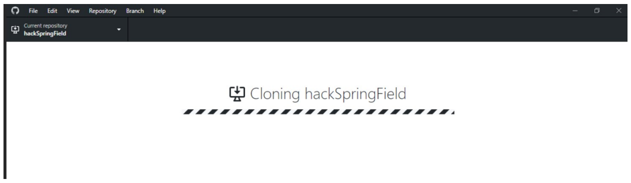


Fig. 7.274: Cloning the deleted repository ‘hackSpringField’ using GitHub Desktop

Within the cloned repository, a README file disclosed Bart’s likely malicious intent, containing the message “I will hack Springfield Buhahahahahaha!”, as seen in Figure Fig. 7.275.

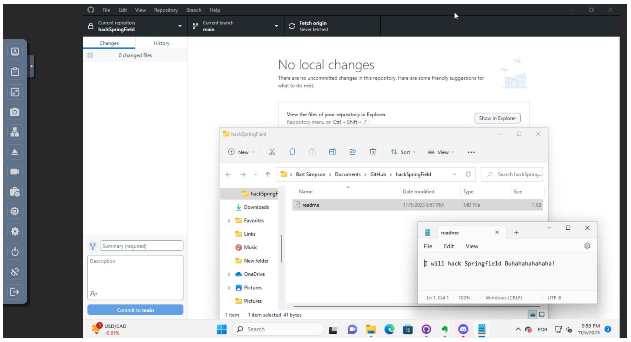

```
I will hack Springfield Buhahahahahaha!
```

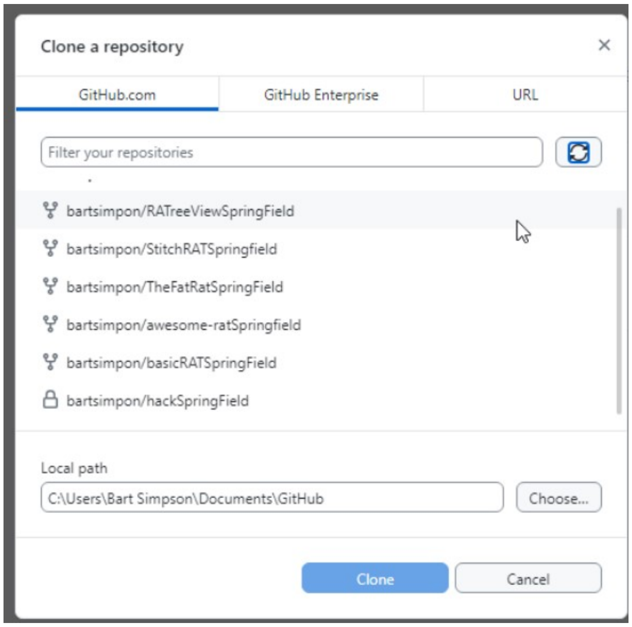
Fig. 7.275: The README file within the ‘hackSpringField’ repository indicating potential malevolent intentions

The exploration of Bart’s GitHub repositories revealed several with names that suggest they could be tools for malicious purposes:

- RATreeViewSpringField
- StichRATSpringfield
- TheFatRatSpringField

- awesome-ratSpringField
- basicRATSpringField

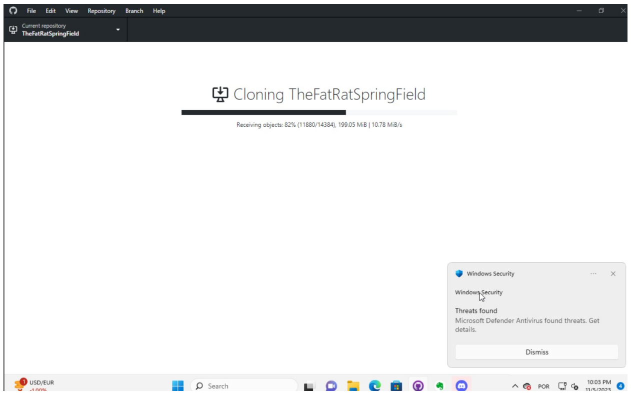
These repositories were cloned as part of the investigatory process, as documented in Figures Fig. 7.276, Fig. 7.277, and Fig. 7.278.


Clone a repository

bartsimpon/RATreeViewSpringField
bartsimpon/StitchRATSpringfield
bartsimpon/TheFatRatSpringField
bartsimpon/awesome-ratSpringfield
bartsimpon/basicRATSpringField
bartsimpon/hackSpringField

Local path: C:\Users\Bart Simpson\Documents\GitHub

Fig. 7.276: Cloning of repositories suspected to be associated with malicious activities



Current repository
TheFatRatSpringField

Cloning TheFatRatSpringField

Receiving objects: 82% (11880/14384), 199.05 MiB | 10.78 MiB/s

Windows Security

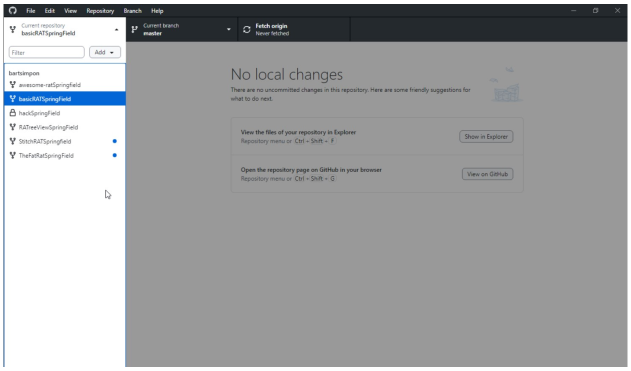
Windows Security

Threats found
Microsoft Defender Antivirus found threats. Get details.

Fig. 7.277: Acquiring repository content for further forensic analysis

Subsequently, the cloned repositories were transferred to a specifically labelled folder ‘Github-Internet On’ within the cloud_applications autopsy tag folder, with the process captured in Figures Fig. 7.279, Fig. 7.280, and Fig. 7.281.

The shared notebook named **bart secret plans** now has 14 notes, an increase of 11 notes from when the system was examined in offline mode. This surge in content could indicate active use or automated synchronization once the network was enabled. Among these notes, several are titled with ‘Command and Control (C2C)’, each followed by a sequence number, which suggests a structured approach to potentially illicit command sequences. Furthermore, the presence of Evernote Cloud API python guide notes could imply an intention to leverage Evernote as a platform for issuing commands to compromised systems or for managing a network of controlled devices. An illustrative note contains the command *sdelete -z c:*, which is known to overwrite free space on a drive with zeros, typically a method to



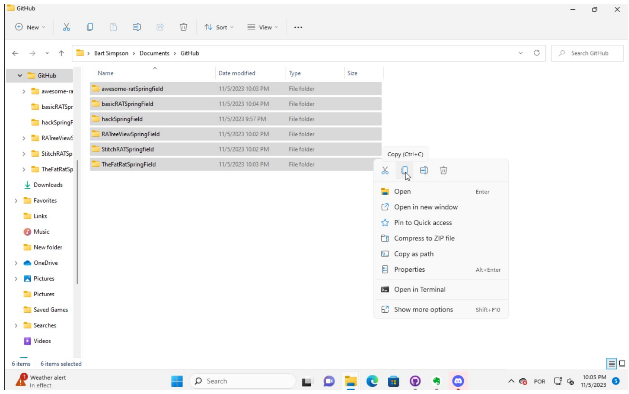
No local changes

There are no uncommitted changes in this repository. Here are some friendly suggestions for what to do next.

View the files of your repository in Explorer
Repository menu or Ctrl + Shift + F

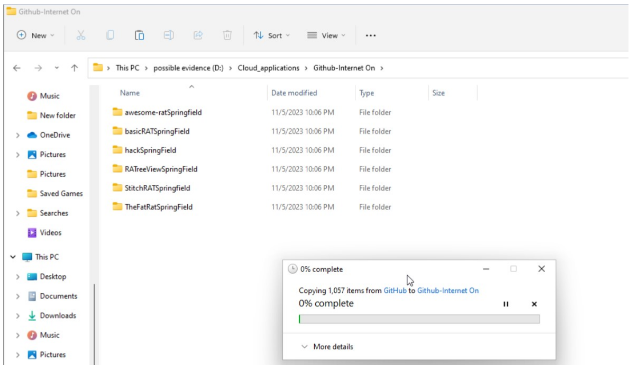
Open the repository page on GitHub in your browser
Repository menu or Ctrl + Shift + G

Fig. 7.278: Documentation of the cloned repositories from the suspected hacker's GitHub account



Name	Date modified	Type	Size
awesome-ratSpringfield	11/5/2023 10:03 PM	File folder	
basicRATSpringField	11/5/2023 10:04 PM	File folder	
hackSpringField	11/5/2023 9:57 PM	File folder	
RATreeViewSpringField	11/5/2023 10:02 PM	File folder	
StitchRATSpringfield	11/5/2023 10:02 PM	File folder	
TheFatRatSpringField	11/5/2023 10:03 PM	File folder	

Fig. 7.279: Copying cloned repositories to the designated forensic analysis folder



Name	Date modified	Type	Size
awesome-ratSpringfield	11/5/2023 10:06 PM	File folder	
basicRATSpringField	11/5/2023 10:06 PM	File folder	
hackSpringField	11/5/2023 10:06 PM	File folder	
RATreeViewSpringField	11/5/2023 10:06 PM	File folder	
StitchRATSpringfield	11/5/2023 10:06 PM	File folder	
TheFatRatSpringField	11/5/2023 10:06 PM	File folder	

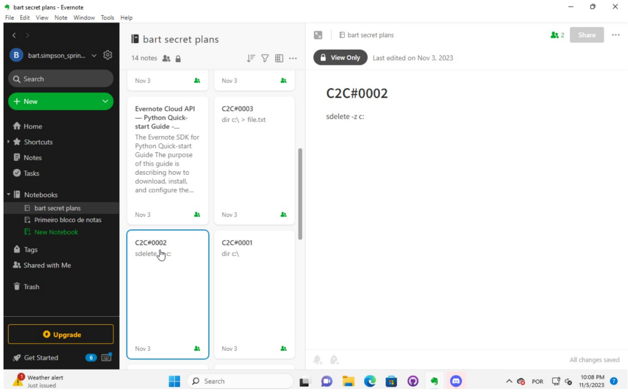
0% complete

Copying 1,057 items from GitHub to Github-Internet On

0% complete

Fig. 7.280: Organising the collected repositories in the 'Github-Internet On' folder for detailed examination

prevent data recovery – a concerning find, possibly indicative of attempts to obfuscate or destroy evidence. This detail is depicted in Figure Fig. 7.281.



Evernote Cloud API — Python Quick-start Guide -... The Evernote SDK for Python Quick-start Guide The purpose of this guide is describing how to download, install, and configure the...

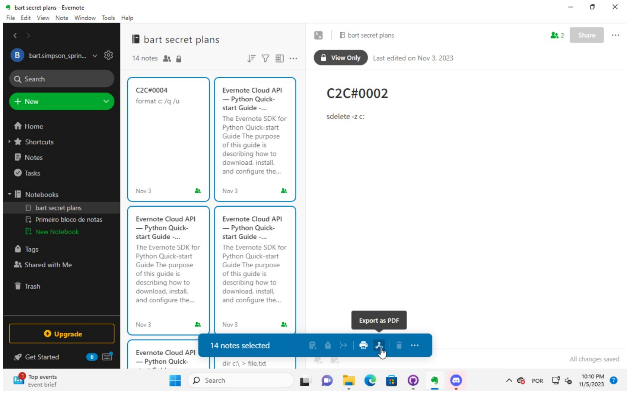
C2C#0003
dir c:\ > file.txt

C2C#0002
sdelete -z c:

C2C#0001
dir c:\

Fig. 7.281: Screenshot illustrating the use of 'sdelete' command within a note from the 'bart secret plans' notebook

In a detailed examination, all notes from the **bart secret plans** notebook were exported as multiple webpages to be preserved as evidence, as shown in Figures Fig. 7.282 and Fig. 7.283.



C2C#0004
format c: /q /u

C2C#0002
sdelete -z c:

Fig. 7.282: Exporting the contents of 'bart secret plans' to webpages, part 1

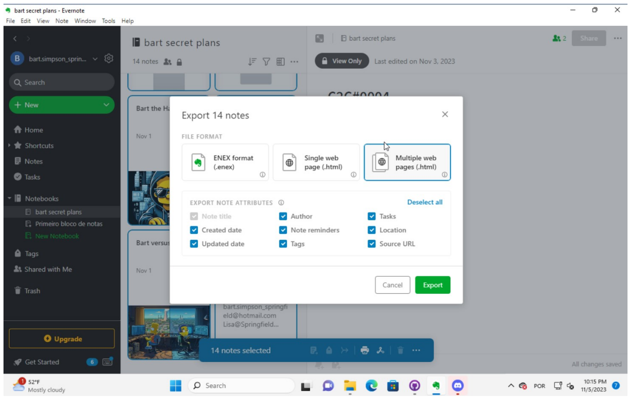
Similarly, the *Primeiro bloco de notas* (First Notebook) was exported, revealing an additional note not previously visible in offline mode. The findings are presented in Figure Fig. 7.284.

Upon inspecting the Discord application, which was set to the Portuguese language, we accessed the user bart.simpson's server. The server's activity log, accessed via the bart.simpson_springfield login, can be observed in Figure Fig. 7.285.

Further investigation within the server revealed a channel named 'Servidor de bart.simpson' (bart.simpson's server), which contained an announcement seemingly related to the sale of data on the dark web, as captured in Figure Fig. 7.287 after opening the server shown in Figure Fig. 7.286.

Within the Discord channel named cyber-security-bypass, the user 'bart' claimed to have *ex-filtrated data from the Springfield Nuclear Plant*. Evidence of such a breach was showcased in an Excel format, which was presented as a sample of the exfiltrated data. Additionally, 'bart' stipulated a ransom demand of 1000 dollars for the recovery of the data, directing the payment to be made to a specified Bitcoin wallet. This incriminating interaction, including the digital ransom note and the proof of the stolen data, is captured in Figure Fig. 7.288.

Subsequent to the discovery of the Discord communication, efforts were made to download the chain of custody report utilizing the ForensicVM webscreen interface. This procedure is critical for maintaining the integrity of the digital evidence and ensuring that all investigative actions are properly documented. The process of downloading this report is depicted in Figures Fig. 7.289 and Fig. 7.290.



Export 14 notes

FILE FORMAT

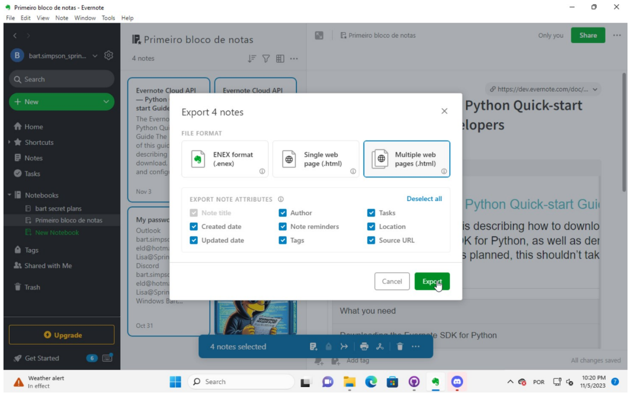
ENEX format (.enex) | Single web page (.html) | Multiple web pages (.html)

EXPORT NOTE ATTRIBUTES — Deselect all

☑ Note title ☑ Author ☑ Tasks
☑ Created date ☑ Note reminders ☑ Location
☑ Updated date ☑ Tags ☑ Source URL

Cancel | Export

Fig. 7.283: Exporting the contents of ‘bart secret plans’ to webpages, part 2



Export 4 notes

FILE FORMAT

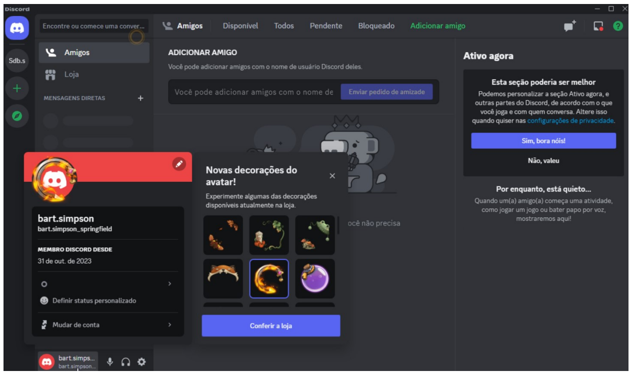
ENEX format (.enex) | Single web page (.html) | Multiple web pages (.html)

EXPORT NOTE ATTRIBUTES — Deselect all

☑ Note title ☑ Author ☑ Tasks
☑ Created date ☑ Note reminders ☑ Location
☑ Updated date ☑ Tags ☑ Source URL

Cancel | Export

Fig. 7.284: The export process of the ‘Primeiro bloco de notas’ indicating the presence of an additional note



ADICIONAR AMIGO

Você pode adicionar amigos com o nome de usuário Discord deles.

Você pode adicionar amigos com o nome de | Enviar pedido de amizade

Ativo agora

Esta seção poderia ser melhor

Podemos personalizar a seção Ativo agora, e outras partes do Discord, de acordo com o que você joga e com quem conversa. Altere isso quando quiser nas configurações de privacidade.

Sim, bora nóis! | Não, valeu

Por enquanto, está quieto...

Quando um(a) amigo(a) começa uma atividade, como jogar um jogo ou bater papo por voz, mostraremos aqui!

bart.simpson
bart.simpson_springfield

MEMBRO DISCORD DESDE
31 de out. de 2023

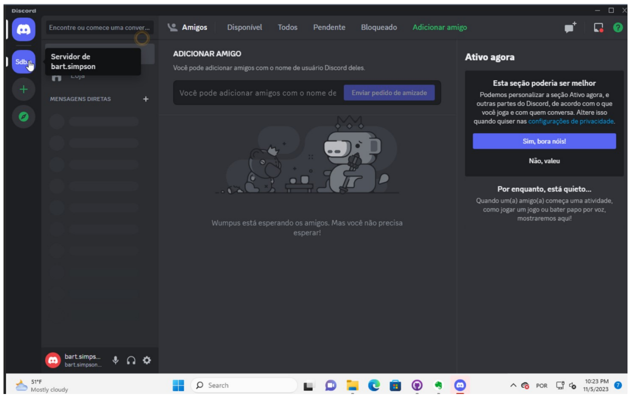
Definir status personalizado
Mudar de conta

Novas decorações do avatar!

Experimente algumas das decorações disponíveis atualmente na loja.

Conferir a loja

Fig. 7.285: Accessing Discord server with bart.simpson_springfield user credentials



ADICIONAR AMIGO

Você pode adicionar amigos com o nome de usuário Discord deles.

Você pode adicionar amigos com o nome de

Wumpus está esperando os amigos. Mas você não precisa esperar!

Ativo agora

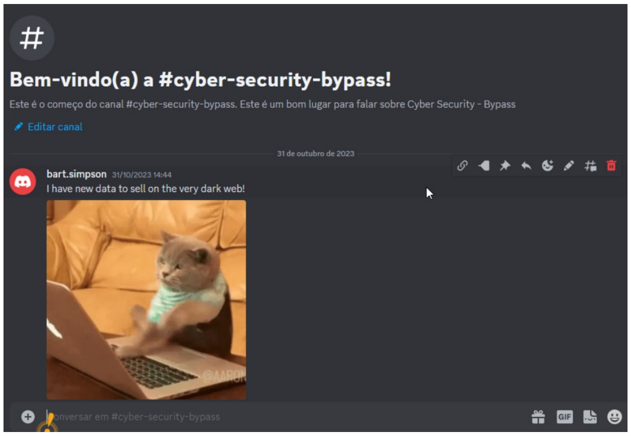
Esta seção poderia ser melhor

Podemos personalizar a seção Ativo agora, e outras partes do Discord, de acordo com o que você joga e com quem conversa. Altere isso quando quiser nas configurações de privacidade.

Por enquanto, está quieto...

Quando um(a) amigo(a) começa uma atividade, como jogar um jogo ou bater papo por voz, mostraremos aqui!

Fig. 7.286: The Discord server 'Servidor de bart.simpson' accessed for investigation



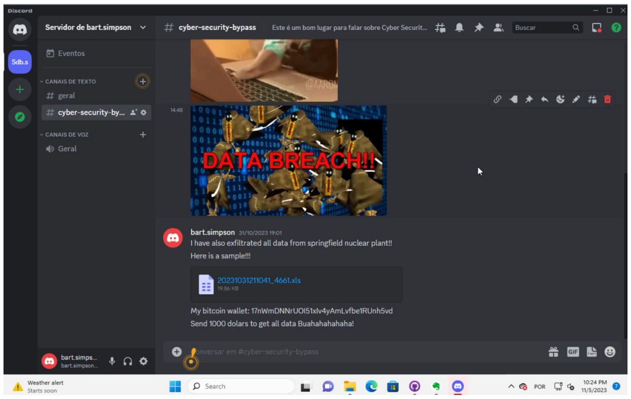
Bem-vindo(a) a #cyber-security-bypass!

Este é o começo do canal #cyber-security-bypass. Este é um bom lugar para falar sobre Cyber Security - Bypass

31 de outubro de 2023

bart.simpson 31/10/2023 14:44
I have new data to sell on the very dark web!

Fig. 7.287: Announcement on 'Servidor de bart.simpson' revealing intentions to sell data on the dark web



Este é um bom lugar para falar sobre Cyber Securit...

bart.simpson 31/10/2023 19:01
I have also exfiltrated all data from springfield nuclear plant!!
Here is a sample!!!

20231031211041_4661.xls
19.86 KB

My bitcoin wallet: 17nWmDNNrUOI51xlv4yAmLvfbe1RUnh5vd
Send 1000 dolars to get all data Buahahahahaha!

conversar em #cyber-security-bypass

Fig. 7.288: Screenshot displaying the ransom demand and sample of exfiltrated data from Springfield Nuclear Plant on Discord

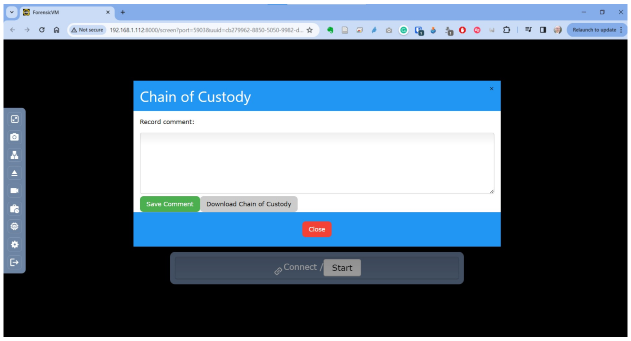
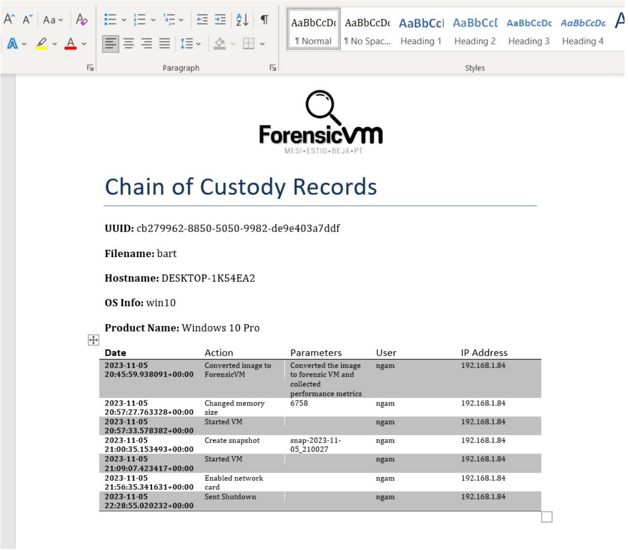


Fig. 7.289: Downloading the chain of custody report via the ForensicVM webscreen interface, part 1



Chain of Custody Records

UUID: cb279962-8850-5050-9982-de9e403a7ddf

Filename: bart

Hostname: DESKTOP-1K54EA2

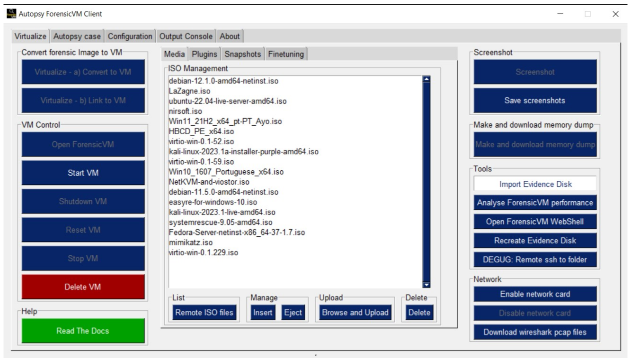
OS Info: win10

Product Name: Windows 10 Pro

Date	Action	Parameters	User	IP Address
2023-11-05 20:45:59.938091+00:00	Converted image to ForensicVM	Converted the image to forensic VM and collected performance metrics	ngam	192.168.1.84
2023-11-05 20:57:27.763328+00:00	Changed memory size	6758	ngam	192.168.1.84
2023-11-05 20:57:33.578382+00:00	Started VM		ngam	192.168.1.84
2023-11-05 21:00:35.153493+00:00	Create snapshot	snap-2023-11-05_210027	ngam	192.168.1.84
2023-11-05 21:09:07.423417+00:00	Started VM		ngam	192.168.1.84
2023-11-05 21:56:35.341631+00:00	Enabled network card		ngam	192.168.1.84
2023-11-05 22:28:55.020232+00:00	Sent Shutdown		ngam	192.168.1.84

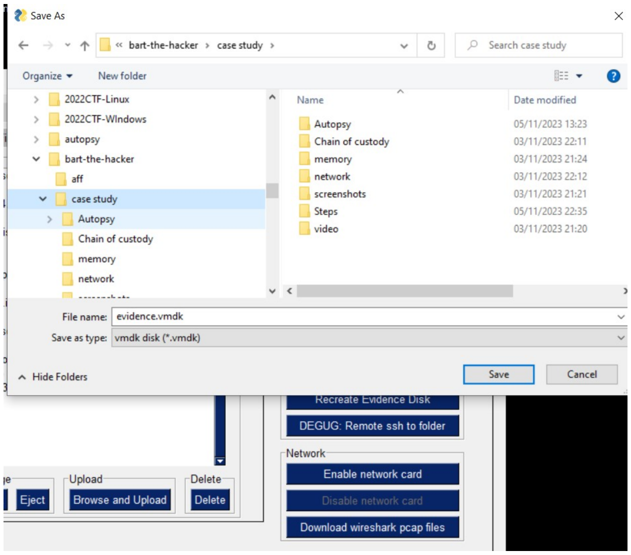
Fig. 7.290: Downloading the chain of custody report via the ForensicVM webscreen interface, part 2

The next phase in the investigative process involves exporting the ForensicVM evidence disk in the virtual machine disk (VMDK) format. This step is necessary to facilitate the importation of the disk into the Autopsy analysis tool for a comprehensive examination. The sequence of actions taken to halt the ForensicVM, followed by the initiation of the 'Import Evidence Disk' process, is sequentially illustrated in Figures Fig. 7.291 through Fig. 7.294.



debian-12.1.0-amd64-netinst.iso
LaZagne.iso
ubuntu-22.04-live-server-amd64.iso
nirsoft.iso
Win11_21H2_x64_pt-PT_Ayo.iso
HBCD_PE_x64.iso
virtio-win-0.1-52.iso
kali-linux-2023.1a-installer-purple-amd64.iso
virtio-win-0.1-59.iso
Win10_1607_Portuguese_x64.iso
NetKVM-and-viostor.iso
debian-11.5.0-amd64-netinst.iso
easyre-for-windows-10.iso
kali-linux-2023.1-live-amd64.iso
systemrescue-9.05-amd64.iso
Fedora-Server-netinst-x86_64-37-1.7.iso
mimikatz.iso
virtio-win-0.1.229.iso

Fig. 7.291: Initiating the export of ForensicVM evidence disk from the Autopsy Forensic Client main interface



Name	Date modified
Autopsy	05/11/2023 13:23
Chain of custody	03/11/2023 22:11
memory	03/11/2023 21:24
network	03/11/2023 22:12
screenshots	03/11/2023 21:21
Steps	05/11/2023 22:35
video	03/11/2023 21:20

File name: evidence.vmdk
Save as type: vmdk disk (*.vmdk)

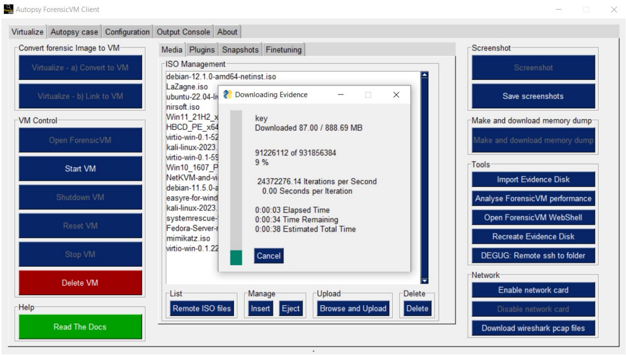
Fig. 7.292: Stopping the ForensicVM in preparation for exporting the evidence disk

In the final step of the digital forensic analysis, a new data source was added to the Autopsy forensic software. This new data source was the VMDK disk which contained the evidence that had been previously gathered from ForensicVM. This action is paramount for enabling a detailed examination and analysis within the Autopsy environment. The step-by-step process of adding this new evidence source is captured in Figures Fig. 7.295 through Fig. 7.300.

Post-importation of the meticulously crafted evidence disk into Autopsy, the investigation is poised to enter a detailed examination phase. The evidence disk, structured with folders mirroring the tags utilized within Autopsy, allows for an organized and efficient review process. The subsequent investigative steps will leverage the logical structure and tagging system to ensure a comprehensive analysis of the data.

The primary step involves the cataloging and verification of the imported data against the original evidence tags. This ensures that the transfer has been successful and that the integrity of the data has been maintained during the process. The alignment of folders with Autopsy tags streamlines the verification process, allowing investigators to swiftly confirm the presence and accuracy of all tagged items.

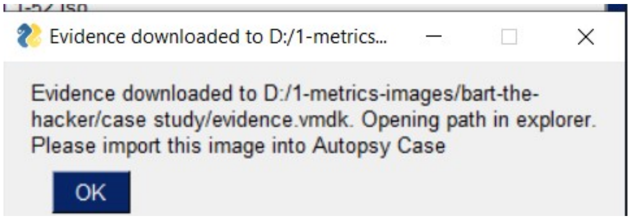
Following this, a thorough content analysis within each tagged folder will be undertaken. Since these folders are orga-



debian-12.1.0-amd64-netinst.iso
LaZagne.iso
ubuntu-22.04-li
nirsoft.iso
Win11_21H2_x
HBCD_PE_x64
virtio-win-0.1-52
kali-linux-2023.
virtio-win-0.1-59
Win10_1607_P
NetKVM-and-vi
debian-11.5.0-a
easyre-for-wind
kali-linux-2023.
systemrescue-
Fedora-Server-
mimikatz.iso
virtio-win-0.1.22

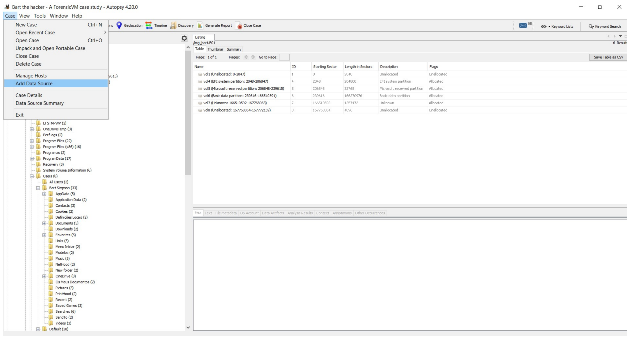
```
key
Downloaded 87.00 / 888.69 MB

91226112 of 931856384
9 %

 24372276.14 Iterations per Second
   0.00 Seconds per Iteration

0:00:03 Elapsed Time
0:00:34 Time Remaining
0:00:38 Estimated Total Time
```

Fig. 7.293: Selection of the 'Import Evidence Disk' option in the Autopsy Forensic Client



Evidence downloaded to D:/1-metrics-images/bart-the-hacker/case study/evidence.vmdk. Opening path in explorer. Please import this image into Autopsy Case

Fig. 7.294: Finalization of the ForensicVM evidence disk export in VMDK format.

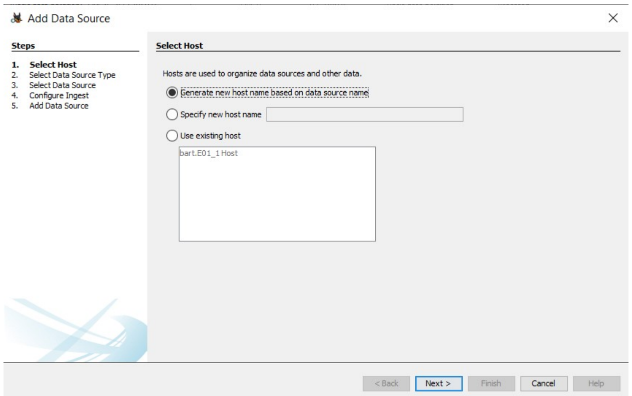


/img_bart.E01

Page: 1 of 1 Pages: Go to Page:

Name	ID	Starting Sector	Length in Sectors	Description	Flags
vol1 (Unallocated: 0-2047)	1	0	2048	Unallocated	Unallocated
vol4 (EFI system partition: 2048-206847)	4	2048	204800	EFI system partition	Allocated
vol5 (Microsoft reserved partition: 206848-239615)	5	206848	32768	Microsoft reserved partition	Allocated
vol6 (Basic data partition: 239616-166510591)	6	239616	166270976	Basic data partition	Allocated
vol7 (Unknown: 166510592-167768063)	7	166510592	1257472	Unknown	Allocated
vol8 (Unallocated: 167768064-167772159)	8	167768064	4096	Unallocated	Unallocated

Fig. 7.295: Initiating the addition of a new data source in Autopsy.



Hosts are used to organize data sources and other data.

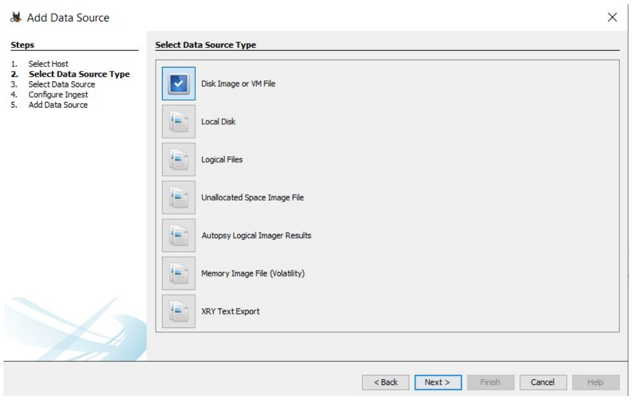
● Generate new host name based on data source name

○ Specify new host name

○ Use existing host

bart.E01_1 Host

Fig. 7.296: Selecting the evidence disk for the new data source.



Add Data Source

Steps

1. Select Host
2. **Select Data Source Type**
3. Select Data Source
4. Configure Ingest
5. Add Data Source

Select Data Source Type

☑ Disk Image or VM File

Local Disk

Logical Files

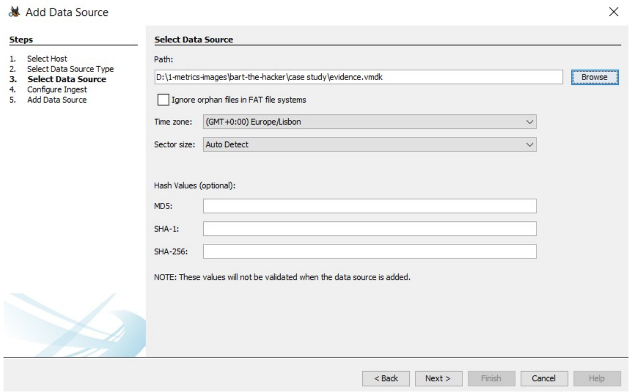
Unallocated Space Image File

Autopsy Logical Imager Results

Memory Image File (Volatility)

XRY Text Export

Fig. 7.297: Confirming the selection of the VMDK disk file.



Add Data Source

Steps

1. Select Host
2. Select Data Source Type
3. **Select Data Source**
4. Configure Ingest
5. Add Data Source

Select Data Source

Path:

D:\1-metrics-images\bart-the-hacker\case study\evidence.vmdk

□ Ignore orphan files in FAT file systems

Time zone: (GMT+0:00) Europe/Lisbon

Sector size: Auto Detect

Hash Values (optional):

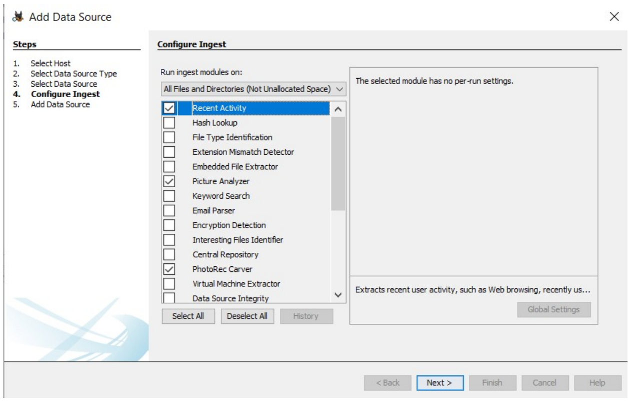
MD5:

SHA-1:

SHA-256:

NOTE: These values will not be validated when the data source is added.

Fig. 7.298: Setting up the data source parameters in Autopsy.



Add Data Source

Steps

1. Select Host
2. Select Data Source Type
3. Select Data Source
4. **Configure Ingest**
5. Add Data Source

Configure Ingest

Run ingest modules on:

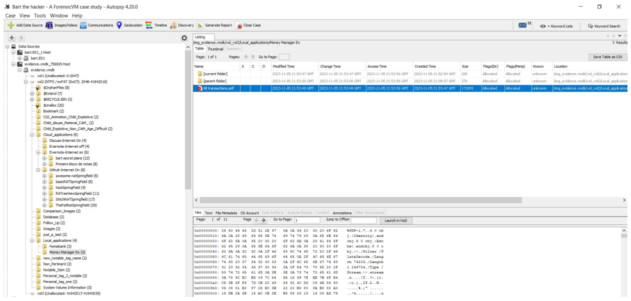
All Files and Directories (Not Unallocated Space)

☑ Recent Activity
□ Hash Lookup
□ File Type Identification
□ Extension Mismatch Detector
□ Embedded File Extractor
☑ Picture Analyzer
□ Keyword Search
□ Email Parser
□ Encryption Detection
□ Interesting Files Identifier
□ Central Repository
☑ PhotoRec Carver
□ Virtual Machine Extractor
□ Data Source Integrity

The selected module has no per-run settings.

Extracts recent user activity, such as Web browsing, recently us...

Fig. 7.299: Progression of the data source addition process.



/img_evidence.vmdk/vol_vol2/Local_applications/Money Manager Ex

3 Results

Page: 1 of 1 Pages: Go to Page:

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
[current folder]				2023-11-05 21:53:47 GMT	2023-11-05 21:53:47 GMT	2023-11-05 21:53:56 GMT	2023-11-05 21:52:54 GMT	288	Allocated	Allocated	unknown	/img_evidence.vmdk/vol_vol2/Local_application
[parent folder]				2023-11-05 21:53:00 GMT	2023-11-05 21:53:00 GMT	2023-11-05 21:53:56 GMT	2023-11-05 21:08:57 GMT	376	Allocated	Allocated	unknown	/img_evidence.vmdk/vol_vol2/Local_application
All transactions.pdf				2023-11-05 21:53:48 GMT	2023-11-05 21:53:48 GMT	2023-11-05 21:53:56 GMT	2023-11-05 21:53:47 GMT	172893	Allocated	Allocated	unknown	/img_evidence.vmdk/vol_vol2/Local_application

Page: 1 of 11 Page Go to Page: 1 Jump to Offset

```
0x00000000: 25 50 44 46  2D 31 2E 37   0A 0A 34 20  30 20 6F 62   %PDF-1.7..4 0 ob
0x00000010: 6A 0A 28 49  64 65 6E 74   69 74 79 29  0A 65 6E 64   j.(Identity).end
0x00000020: 6F 62 6A 0A  35 20 30 20   6F 62 6A 0A  28 41 64 6F   obj.5 0 obj.(Ado
0x00000030: 62 65 29 0A  65 6E 64 6F   62 6A 0A 38  20 30 20 6F   be).endobj.8 0 o
0x00000040: 62 6A 0A 3C  3C 0A 2F 46   69 6C 74 65  72 20 2F 46   bj.<<./Filter /F
0x00000050: 6C 61 74 65  44 65 63 6F   64 65 0A 2F  4C 65 6E 67   lateDecode./Leng
0x00000060: 74 68 20 37  34 32 30 33   0A 2F 4C 65  6E 67 74 68   th 74203./Length
0x00000070: 31 20 32 34  36 37 30 34   0A 2F 54 79  70 65 20 2F   1 246704./Type /
0x00000080: 53 74 72 65  61 6D 0A 3E   3E 0A 73 74  72 65 61 6D   Stream.>>.stream
0x00000090: 0A 78 9C EC  BD 09 7C 54   D5 15 3F 7E  EE 7B 6F E6   .x....|T..?~.{o.
0x000000a0: CD 3E 6F F6  7D CB 2C 49   66 92 4C D6  C9 4E 86 90   .>o.}.,If.L..N..
0x000000b0: 05 08 81 B0  87 25 EC 3B   22 20 B8 80  0A B8 82 A0   .....%.;" ......
0x000000c0: 15 DB 2A 6E  15 AC 0B 2E   B5 86 28 18  16 05 AD 75   ..*n......(....u
```

Fig. 7.300: Completion of the new data source addition in Autopsy.

nized based on the categorization relevant to the investigation, the analysis can be targeted and specific. Investigators will parse through each category, looking for suspicious patterns or incriminating evidence that correlates with the activities under investigation.

Subsequently, cross-referencing the extracted evidence with the case timeline will be imperative. The analysis will involve correlating timestamps of file creation, modification, and deletion with the case events. Such a timeline analysis can often unearth critical insights into the suspect's behavior and modus operandi.

The investigation will also include a thorough review of any executable files and scripts that were used or potentially created as part of the suspect's activities. The scripts found in the 'C2C' (Command and Control) folders, for example, will be scrutinized to understand the nature of the commands issued, their targets, and the extent of control exerted over compromised systems.

A meticulous examination of communication logs and metadata is also essential. This includes not only traditional system logs but also any extracted communication from applications such as Discord, as indicated by the presence of specific tags and folders. Insights gleaned from these sources can be invaluable in establishing the suspect's network of contacts and the breadth of the cyber-security breach.

In addition, a deep-dive analysis into the files marked for deletion or those found within the unallocated space of the file system will be conducted. Using file carving techniques, investigators aim to recover and reconstruct such files, as they may hold critical evidence that the suspect attempted to obscure or erase.

Finally, the entire investigation will be supported by a robust documentation process. Each step, discovery, and piece of evidence will be recorded with exacting detail. This ensures that the chain of custody is preserved and that all the investigative actions can withstand the rigorous scrutiny of legal proceedings.

CHAPTER

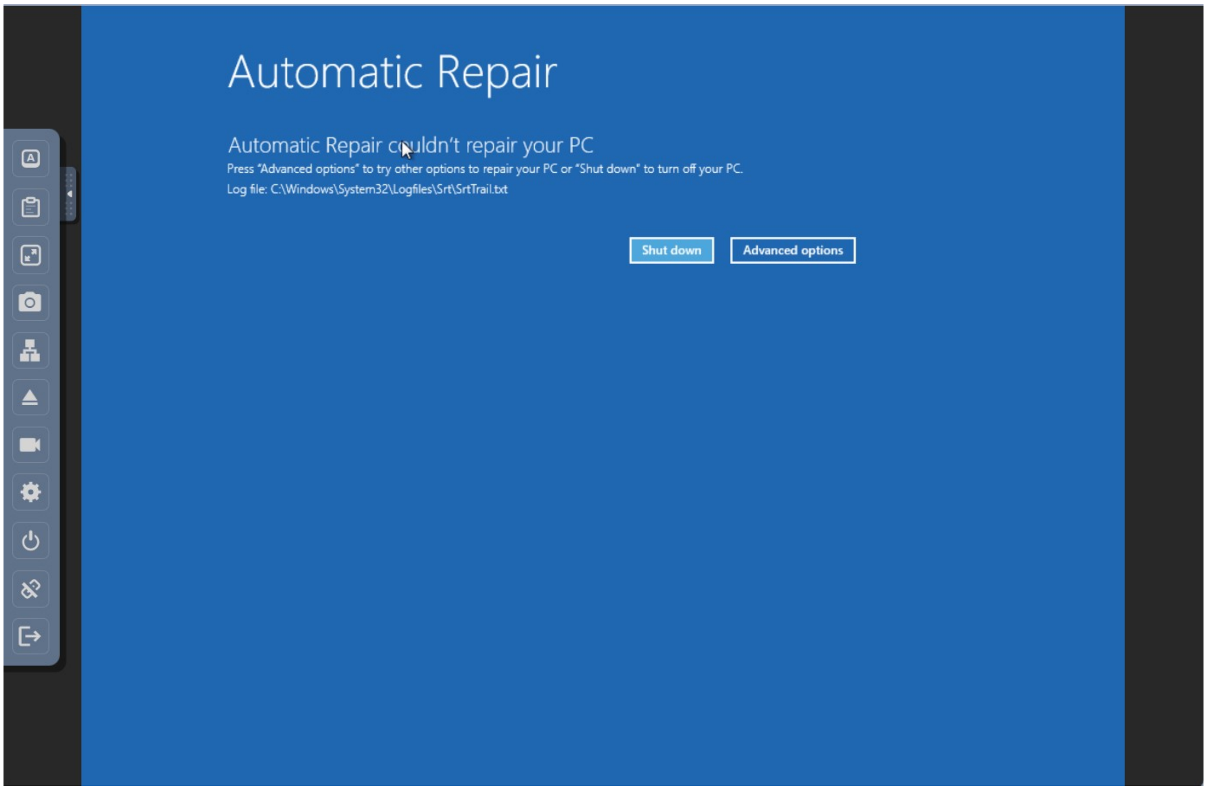
EIGHT

TROUBLESHOOTING

8.1 Booting without signed drivers

If your machine cannot boot due to the virtio drivers installed during the automatic driver installation in the virtualization phase being unsigned or having an invalid signature for your operating system, the machine may enter a recovery boot loop. To address this issue, follow these steps:

- **1. Advanced options in the Automatic Repair boot screen**: Press the "Advanced options" button.



Automatic Repair

Automatic Repair couldn't repair your PC

Press "Advanced options" to try other options to repair your PC or "Shut down" to turn off your PC.

Log file: C:\Windows\System32\Logfiles\Srt\SrtTrail.txt

Fig. 8.1: Advanced options in the Automatic Repair boot screen

- **2. Troubleshoot**: Select the "Troubleshoot" option.

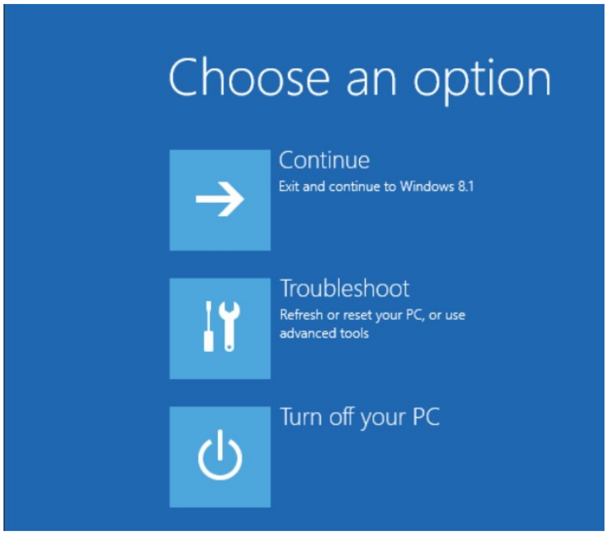

Choose an option
Continue
Exit and continue to Windows 8.1
Troubleshoot
Refresh or reset your PC, or use advanced tools
Turn off your PC

Fig. 8.2: Troubleshoot option

- **3. Advanced options**: Choose the "Advanced options".

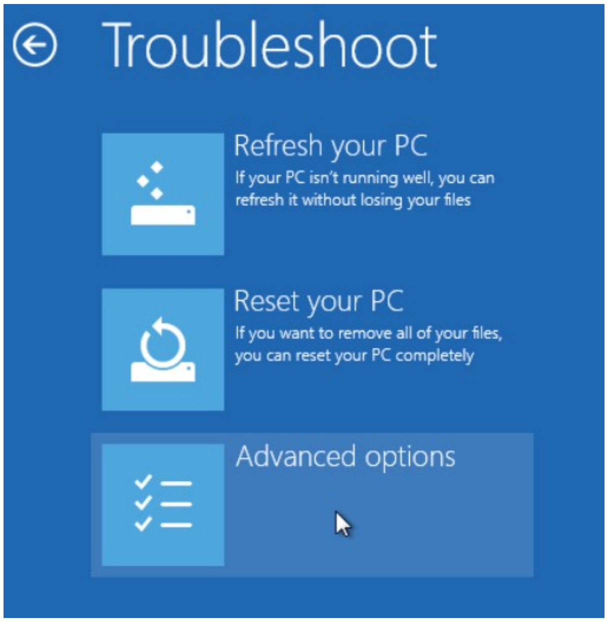
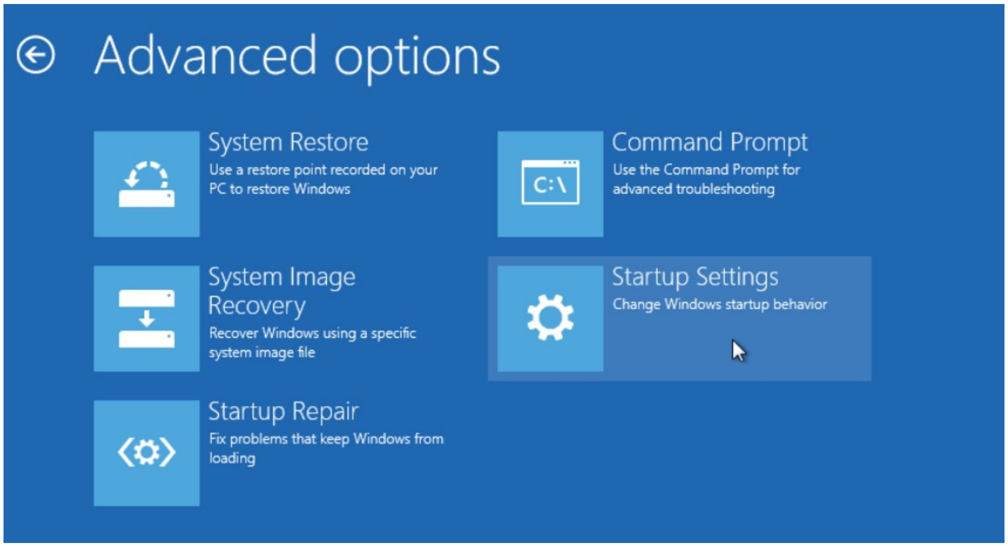

Troubleshoot
Refresh your PC
If your PC isn't running well, you can refresh it without losing your files
Reset your PC
If you want to remove all of your files, you can reset your PC completely
Advanced options

Fig. 8.3: Choosing Advanced options

- **4. Startup Settings**: Within the Advanced options, select the "Startup Settings" to change Windows startup behavior.



Advanced options

System Restore
Use a restore point recorded on your PC to restore Windows

Command Prompt
Use the Command Prompt for advanced troubleshooting

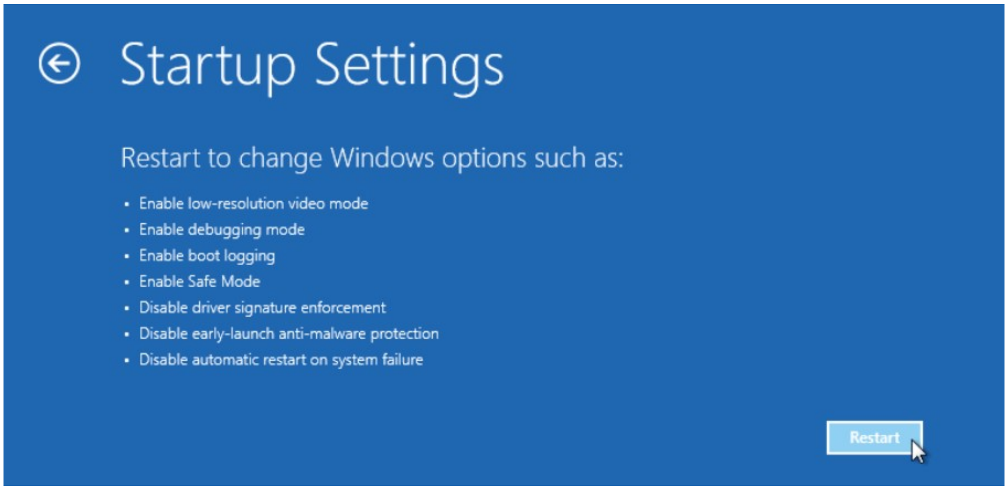
System Image Recovery
Recover Windows using a specific system image file

Startup Settings
Change Windows startup behavior

Startup Repair
Fix problems that keep Windows from loading

Fig. 8.4: Startup Settings option

- **5. Restart**: Press the "Restart" button and await the system restart.



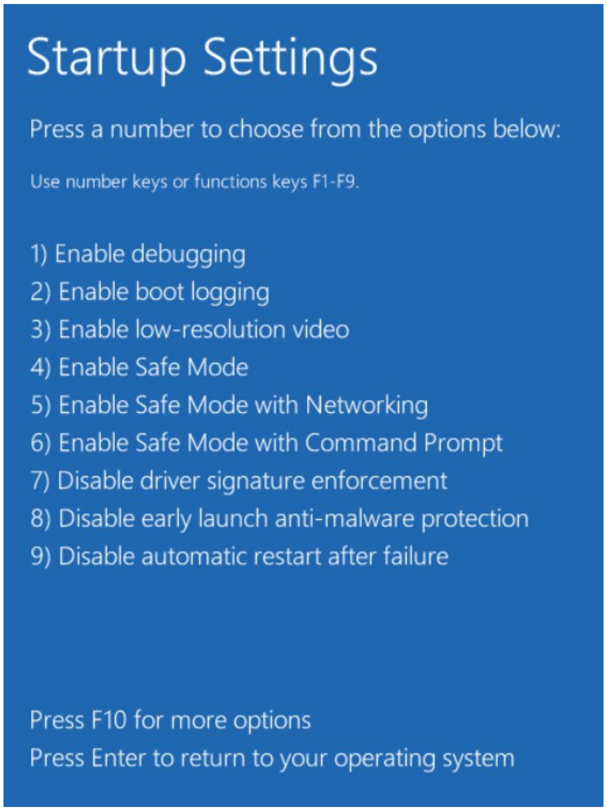
Startup Settings

Restart to change Windows options such as:

- Enable low-resolution video mode
- Enable debugging mode
- Enable boot logging
- Enable Safe Mode
- Disable driver signature enforcement
- Disable early-launch anti-malware protection
- Disable automatic restart on system failure

Fig. 8.5: Restart option

- **6. Press F7**: Once the system restarts, press the **F7** key to choose "Disable driver signature enforcement".



Startup Settings

Press a number to choose from the options below:

Use number keys or functions keys F1-F9.

1) Enable debugging
2) Enable boot logging
3) Enable low-resolution video
4) Enable Safe Mode
5) Enable Safe Mode with Networking
6) Enable Safe Mode with Command Prompt
7) Disable driver signature enforcement
8) Disable early launch anti-malware protection
9) Disable automatic restart after failure

Press F10 for more options
Press Enter to return to your operating system

Fig. 8.6: Pressing F7 for Disable driver signature enforcement

- **7. Windows normal boot**: Your Windows should now boot normally.

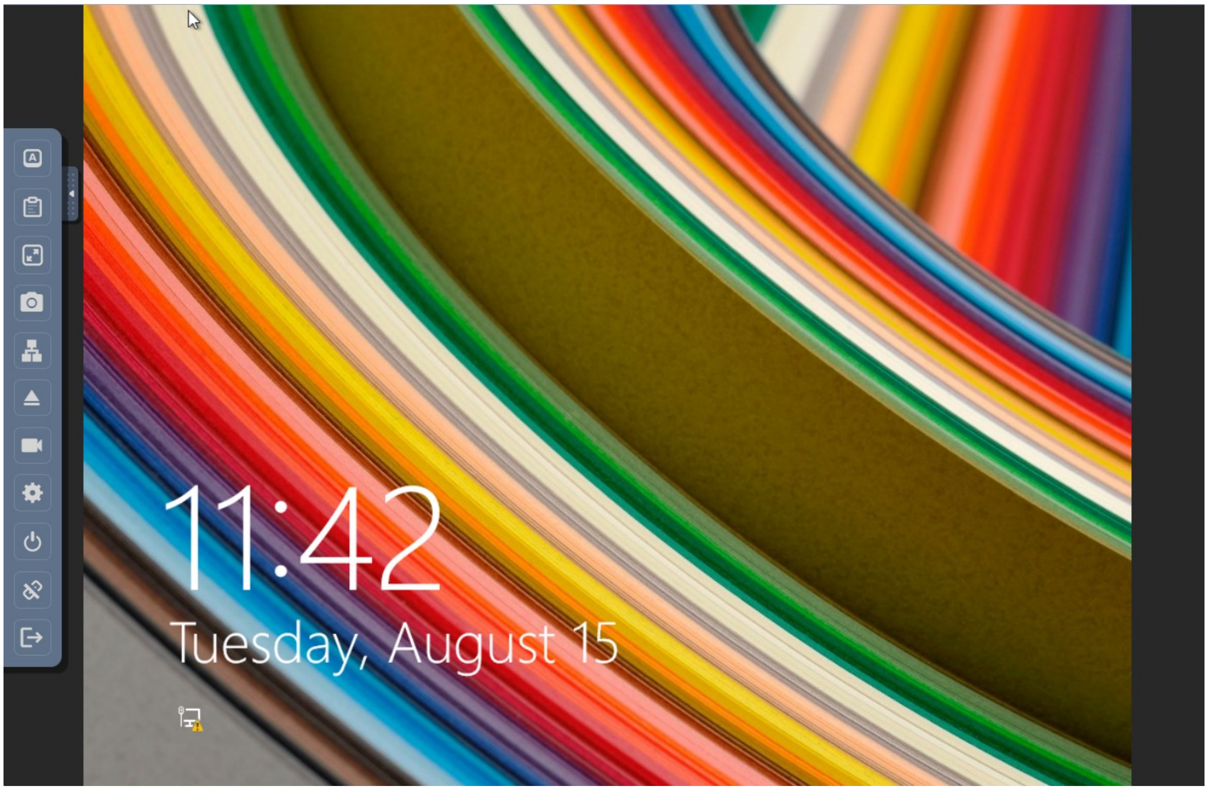


Fig. 8.7: Windows booting normally

Note: This behavior has been observed in older Windows versions, such as Windows 8.1. Mismatches or odd dates in the driver certificate can lead to this issue.

8.2 DEBUG: Remote ssh to folder

If you encounter issues with the forensicVM, you might need to directly edit its configuration files or control its state (start/stop). Below is a step-by-step guide on how to perform these actions:

1. In the Autopsy ForensicVM Client Plugin, select **DEBUG: Remote ssh to folder**.

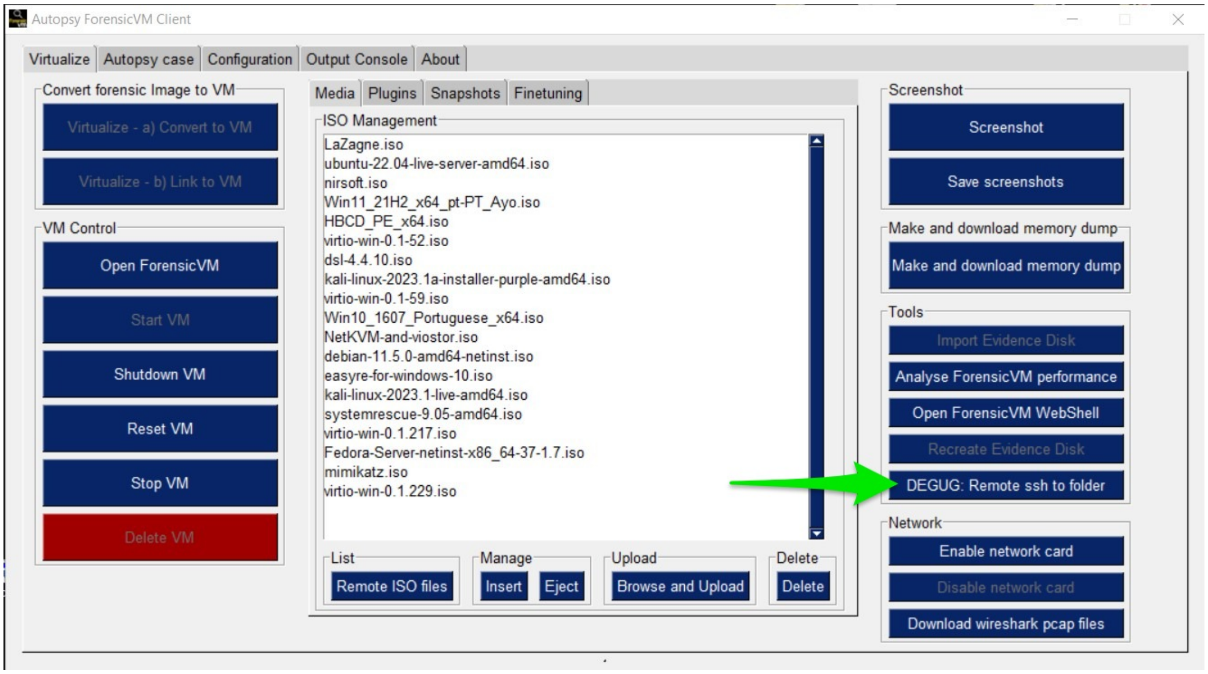
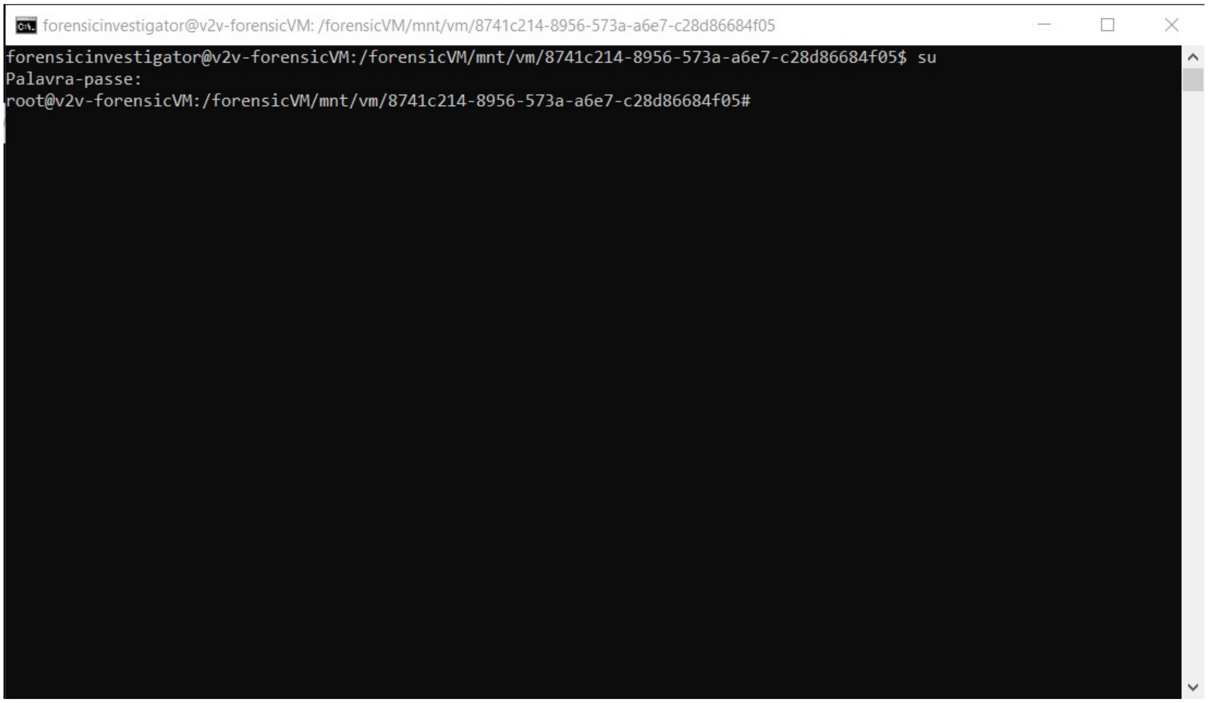


Fig. 8.8: DEBUG: Remote ssh to folder option in the Autopsy ForensicVM Client Plugin.

2. Elevate to root permissions. Enter the *su* command and provide the root password when prompted.



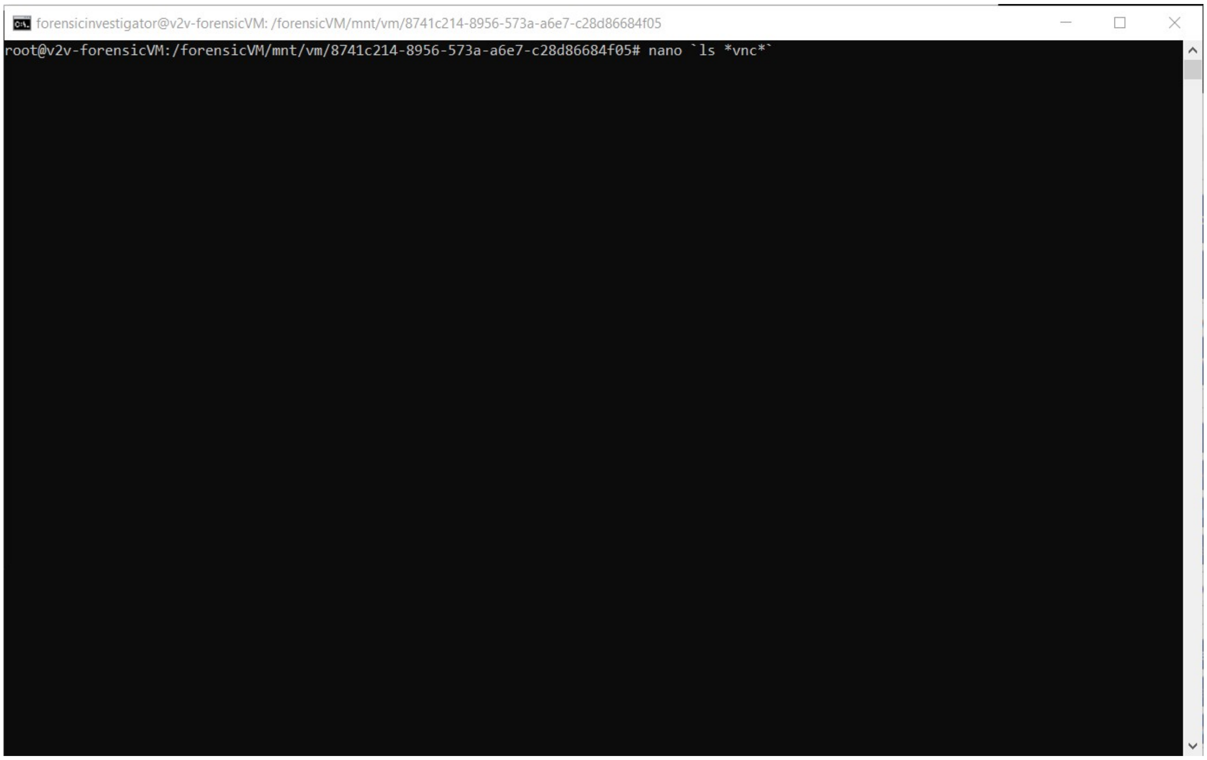
forensicinvestigator@v2v-forensicVM: /forensicVM/mnt/vm/8741c214-8956-573a-a6e7-c28d86684f05

```
forensicinvestigator@v2v-forensicVM:/forensicVM/mnt/vm/8741c214-8956-573a-a6e7-c28d86684f05$ su
Palavra-passe:
root@v2v-forensicVM:/forensicVM/mnt/vm/8741c214-8956-573a-a6e7-c28d86684f05#
```

Fig. 8.9: Elevating to root using the su command.

3. Input the following command to edit the configuration file associated with the forensicVM:

```
nano `ls *vnc*`
```

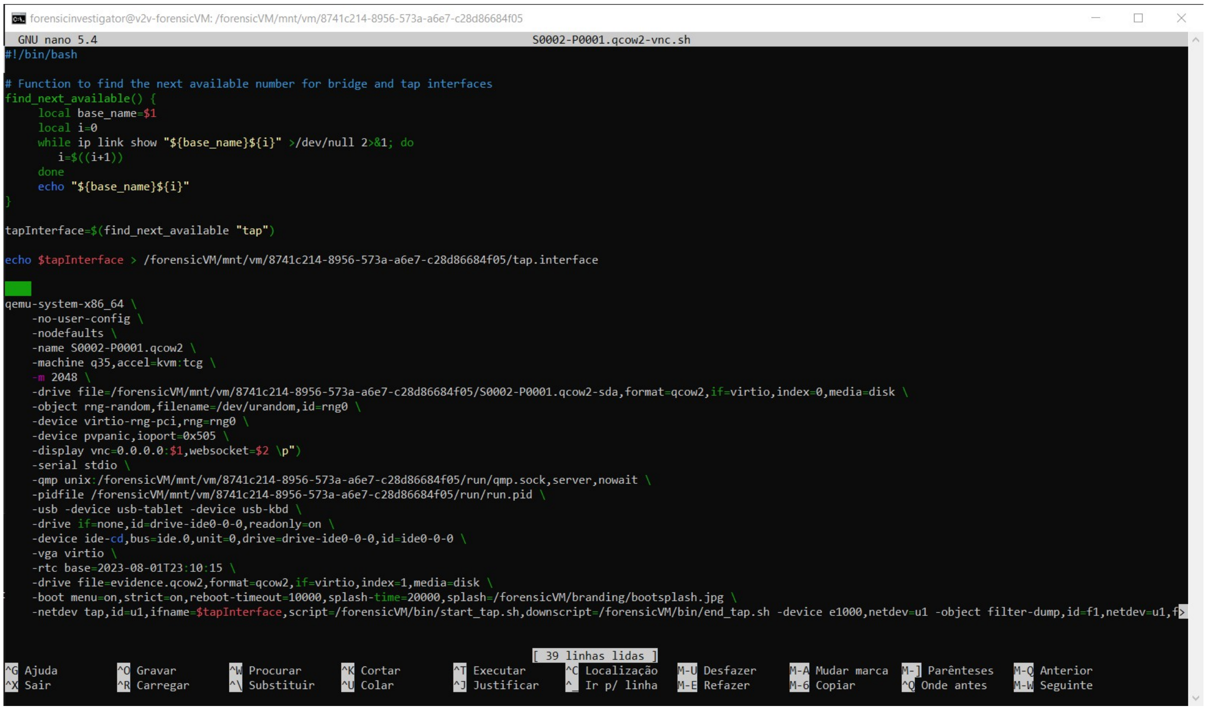


forensicinvestigator@v2v-forensicVM: /forensicVM/mnt/vm/8741c214-8956-573a-a6e7-c28d86684f05

```
root@v2v-forensicVM:/forensicVM/mnt/vm/8741c214-8956-573a-a6e7-c28d86684f05# nano `ls *vnc*`
```

Fig. 8.10: Editing the forensicVM configuration file with nano.

4. Inside the editor, modify the configuration file as needed. Adjust the relevant parameters to your requirements.



forensicinvestigator@v2v-forensicVM: /forensicVM/mnt/vm/8741c214-8956-573a-a6e7-c28d86684f05

```
  GNU nano 5.4                                                S0002-P0001.qcow2-vnc.sh
#!/bin/bash

# Function to find the next available number for bridge and tap interfaces
find_next_available() {
     local base_name=$1
     local i=0
     while ip link show "${base_name}${i}" >/dev/null 2>&1; do
        i=$((i+1))
     done
     echo "${base_name}${i}"
}

tapInterface=$(find_next_available "tap")

echo $tapInterface > /forensicVM/mnt/vm/8741c214-8956-573a-a6e7-c28d86684f05/tap.interface


qemu-system-x86_64 \
    -no-user-config \
    -nodefaults \
    -name S0002-P0001.qcow2 \
    -machine q35,accel=kvm:tcg \
    -m 2048 \
    -drive file=/forensicVM/mnt/vm/8741c214-8956-573a-a6e7-c28d86684f05/S0002-P0001.qcow2-sda,format=qcow2,if=virtio,index=0,media=disk \
    -object rng-random,filename=/dev/urandom,id=rng0 \
    -device virtio-rng-pci,rng=rng0 \
    -device pvpanic,ioport=0x505 \
    -display vnc=0.0.0.0:$1,websocket=$2 \p")
    -serial stdio \
    -qmp unix:/forensicVM/mnt/vm/8741c214-8956-573a-a6e7-c28d86684f05/run/qmp.sock,server,nowait \
    -pidfile /forensicVM/mnt/vm/8741c214-8956-573a-a6e7-c28d86684f05/run/run.pid \
    -usb -device usb-tablet -device usb-kbd \
    -drive if=none,id=drive-ide0-0-0,readonly=on \
    -device ide-cd,bus=ide.0,unit=0,drive=drive-ide0-0-0,id=ide0-0-0 \
    -vga virtio \
    -rtc base=2023-08-01T23:10:15 \
    -drive file=evidence.qcow2,format=qcow2,if=virtio,index=1,media=disk \
    -boot menu=on,strict=on,reboot-timeout=10000,splash-time=20000,splash=/forensicVM/branding/bootsplash.jpg \
    -netdev tap,id=u1,ifname=$tapInterface,script=/forensicVM/bin/start_tap.sh,downscript=/forensicVM/bin/end_tap.sh -device e1000,netdev=u1 -object filter-dump,id=f1,netdev=u1,f>

                                                       [ 39 linhas lidas ]
^G Ajuda        ^O Gravar       ^W Procurar     ^K Cortar       ^T Executar     ^C Localização  M-U Desfazer    M-A Mudar marca M-] Parênteses  M-Q Anterior
^X Sair         ^R Carregar     ^\ Substituir   ^U Colar        ^J Justificar   ^_ Ir p/ linha  M-E Refazer     M-6 Copiar      ^Q Onde antes   M-W Seguinte
```

Fig. 8.11: The configuration file open in nano for editing.

5. Once done, exit the remote shell. Now, you can start the forensicVM as you typically would.

Note: It's essential to ensure that the configurations are correct to prevent any unexpected behaviors.

For advanced techniques and in-depth configurations for the forensicVM, consider referring to the official QEMU documentation: QEMU Documentation.

CHAPTER NINE

GLOSSARY

1980x1080 resolution

A specific pixel count for display screens. This resolution is recommended to ensure a clear and detailed view of the ForensicVM interface.

64-bit multi-core processor

A processor with multiple cores capable of handling 64-bit data chunks simultaneously. It's essential for ForensicVM to achieve optimal performance, especially during intricate tasks.

7-zip

A free and open-source file archiver, commonly used for compressing and decompressing files.

Access the Project Repository

The hosted project on GitHub where you can view, clone, or fork the ForensicVM Plugins repository.

Accessing the WebShell

Refers to the methods available for users to access the WebShell for remote administration.

Add Linux Forensic Admin

A plugin to create a new Linux user with 'sudo' permissions.

Add Windows Forensic Admin

A plugin that creates a new Windows admin user with specific credentials. The user belongs to the "Administrator" group.

Additional Security Bypass Features

Plugins designed to bypass other security measures apart from authentication.

Adjusting Screen Scaling: Local Scaling

Steps to optimize the viewing experience within the webscreen console.

Advanced options

A deeper layer of settings, usually accessed after selecting "Troubleshoot", that offers more specific ways to address boot issues.

Advanced options in the Automatic Repair boot screen

An option in the boot screen that provides advanced repair capabilities when facing boot-related issues.

Alerts

Notifications triggered when certain parameters exceed predefined limits.

API key

A code passed in by computer programs to identify the calling program. It grants access to a service, in this case, the ForensicVM server.

Authentication Bypass Features

A suite of plugins designed specifically to bypass various authentication measures.

Autopsy

An open-source digital forensics platform designed for analyzing, managing, reporting, and conducting digital investigations. It is used for disk forensics, post-mortem analysis, and handling forensic data. The platform also provides a user interface to manage various functionalities, including the ForensicVM. ForensicVM requires compatibility with at least Autopsy version 4.20.

Autopsy Case

Displays Autopsy case details, including existing case tags and the generated unique UUID.

Autopsy ForensicVM Client Plugin

An extension for the Autopsy framework, this plugin facilitates interaction with the ForensicVM environment. Through this interface, forensic investigators can access and manage various functionalities, including snapshot, ISO, and tools management like WebShell and Netdata. It is also tailored for managing and analyzing virtual forensic machines.

Autopsy ForensicVM Client Plugin: A Comprehensive Interface Guide

A detailed guide describing the functionalities and operations of the Autopsy ForensicVM Client Plugin.

Autopsy framework

A subset of the Autopsy platform focused on tools and functionalities used for conducting investigations, such as analyzing disk images or VM files, and post-mortem analysis.

Autopsy Plugin

Extensions or tools within the Autopsy platform designed to enhance its forensic investigation capabilities. These plugins extend the core functionality of the Autopsy platform. The ForensicVM Client Plugin is a notable example.

Autopsy Tags

Markers or labels within the Autopsy platform that aid in organizing and categorizing evidence. They are represented as directories or folders on the evidence disk.

Bare metal server

A physical server dedicated to a single tenant or purpose.

Base Snapshot

Often referred to as the ‘first snapshot,’ this represents the initial state of a system or piece of evidence, functioning as an untouched reference point.

Belkasoft Evidence Center

A software solution that includes the ability to analyze computer memory.

BIOS

Basic Input/Output System, a software that is built into the PC, and is the first code run by a PC when powered on.

BitLocker Drive

A drive encryption feature integrated into the Microsoft Windows operating system. In the provided context, the entire encrypted BitLocker drive is showcased being transferred for forensic analysis.

Blue Screen of Death

A colloquial term for a Windows system crash.

Boot Manager

A software process that starts the operating system when the computer is powered on.

Bootable Media

Digital storage media, like an ISO, that contains a boot sector, allowing a computer to start up from it. It provides details about booting from an ISO or CD-ROM for specific forensic tasks.

BOOTFIX: Disable Driver Enforcement

A utility that addresses challenges related to driver signatures.

Booting without signed drivers
Refers to the potential issue of a machine not booting when certain drivers, such as virtio drivers, are unsigned or possess an invalid signature for a given operating system.

Browse and Upload ISO
The process to navigate the interface and upload essential ISO files to the ForensicVM environment.

Browse ForensicVM
Accessing and navigating the forensic virtual machine using interfaces like web browsers.

Browsing Available Plugins
A process to view, manage, and deploy available plugins for ForensicVM using the Autopsy ForensicVM Client.

Bypass Windows Password
A plugin that patches the "ntlmshared.dll" file, allowing for the bypass of Windows authentication.

C2C (Command and Control) client
A centralized computer that issues commands to a botnet (a group of private computers infected with malicious software) and receives reports back.

Case
A specific digital forensic investigation project in Autopsy that may contain one or more data sources.

Case Information
Metadata associated with a case, including its name and other optional details.

Chain of Custody
The chronological documentation or paper trail, showing the seizure, custody, control, transfer, analysis, and disposition of physical or electronic evidence.

Client
Provides a user-friendly interface for managing forensic images. It allows users to create, run, and decommission instances as per their needs.

Cloud Services
Platforms and applications that provide data and services over the internet, often requiring network access to retrieve data.

Command Line Window
A windowed interface for command-line interactions.

Community Plugins Project
An open initiative aiming to enhance ForensicVM functionalities through community contributions.

Configuration File
A file that stores settings and parameters that define how a software or system behaves, and contains various parameters for the forensic virtual machine, such as memory size, attached disks, UEFI boot options, and more.

Confirmation Dialog
A prompt or interface that seeks affirmation from a user for a potentially critical action.

Confirmation Popup
A user interface element that appears to ensure that the user wants to proceed with an action, in this case, the deletion of the ForensicVM.

Connect with Other Tools
Refers to Netdata's integration capabilities, where it can relay alerts to other platforms such as Slack or Twilio.

Contributing Code
Steps to contribute developed plugins or improvements to existing ones.

Control

A UI element, such as a button, that provides management capabilities (e.g., “Start,” “Stop,” “Reset”) for the forensicVM.

Control Bar icon

An icon that reveals the tool panel in the ForensicVM’s web interface.

Convert Forensic Image to VM

Options that facilitate transforming the forensic image into a forensic virtual machine.

CPU

Central Processing Unit, a primary indicator of a server’s processing capability. Netdata provides insights into its utilization.

Danger Zone

A section within the ForensicVM client interface dedicated to critical or potentially irreversible operations, such as deleting snapshots.

Data Extraction and Analysis

Tools or functionalities that help to extract and analyze data from a forensic image.

Data Overload

A situation where the amount of captured data is so vast that it becomes challenging to identify essential and relevant information.

Data Source

An entity from which digital evidence is extracted. This can refer to a repository, location, specific input, or reference. In the context of Autopsy, it encompasses evidence such as disk images, VM files, or any origin of forensic data. It is used as a connection or reference to gather, analyze, and acquire evidence within the forensic tool.

Data Source Processing Progress

A visual representation, usually a progress bar, showing the ongoing processing of a data source.

Deactivate

The process or act of shutting down or turning off a virtual machine or forensicVM, making it inactive or non-operational.

Debian 11 (Bullseye)

A specific version of the Debian operating system, also known as Bullseye. Recommended for installing the ForensicVM server and supported by ForensicVM.

DEBUG: Remote ssh to folder

A feature that provides a direct remote connection to the forensicVM, facilitating the editing of configuration files or control over its state.

Decoding Protocols

The process of translating network data from a machine-based protocol into a format that is human-readable.

Delete

The action of permanently removing an item, in this context, an ISO file, from storage or memory.

Delete ISO

Instructions to remove unwanted ISO files.

Delete VM Button

A designated button within the ForensicVM interface or related software used to initiate the deletion process of the virtual machine.

Digital Evidence

Information stored or transmitted in binary form that might be relied upon in court.

Direct Copy to Server
A method that duplicates the forensic image, creating a new forensic virtual machine on the server.

Disable driver signature enforcement
A startup option that allows Windows to bypass driver signature checks during boot, potentially enabling problematic or unsigned drivers to load.

Disable Network Card
The action of turning off the network card to halt all network communications for the forensicVM.

Disable Windows Defender and Firewall
A plugin that disables both Windows Defender and the firewall.

Disk Activity
Indicates how actively a disk is being read or written to, monitored by Netdata.

Disk Image or VM File
A digital copy or replica of a physical disk, also known as a bit-by-bit copy, often used in digital forensics to preserve the state of a drive. In the context of ForensicVM, a forensic image is used as a source for virtualization. As a data source, it represents either a snapshot of a disk or a virtual machine image.

Django
A high-level Python web framework that promotes rapid development and pragmatic, clean design. Allows for rapid web development.

Documentation and Chain of Custody
A process to ensure that the evidence is genuine and reliable, maintained through a documented and unbroken sequence of possession or control.

Download Progress
An indicator that displays the current status of a download operation.

Eject ISO / Web Eject CD-ROM
Guidance on ejecting a mounted ISO file or CD-ROM.

Elevate to root permissions
The act of gaining elevated system access rights, commonly achieved using the “su” command in Unix-like systems.

Evidence Collection
The process of gathering evidence, often digital, to support investigations and potentially use in court.

Evidence Disk
A disk or drive that serves multiple functions. It contains all tags from Autopsy Software and is automatically generated during the conversion of a forensic image to a ForensicVM. The disk contains directories named after Autopsy tags and serves as a container for evidence related to each tag. Additionally, it is the specific storage area where collected forensic evidence is saved and is often labeled as “possible evidence”.

Evidence Preservation
The safeguarding of the original state of evidence, reducing risks of contamination or alteration.

evidence.vmdk disk
A specific format of a virtual disk image used to store forensic evidence in the context of Autopsy and VMs.

Executing Plugins
The process of running plugins on the ForensicVM.

Fallback Conversion
A backup method of conversion for unidentified OS.

Feature Suggestions and Plugin Requests
A method to contribute ideas for new plugins, features, or improvements without coding them.

Fiber Optics
A type of high-speed internet connection.

File Explorer
A graphical user interface (GUI) component that lets users manage and view files. It is used to navigate and identify the evidence disk.

Fine-Tuning ForensicVM
The process of making adjustments to various configuration parameters of a ForensicVM. This is done via a configuration file that is generated when a forensic image is converted into a ForensicVM.

Firewall
A network security system or component that monitors and controls incoming and outgoing network traffic based on predetermined security policies. Designed to block unauthorized access, it allows only permitted communications to pass.

Forensic Administrator User
A user profile with elevated privileges, potentially created for the purpose of a forensic investigation, to ensure unrestricted access to required data.

Forensic Analysis
Using memory dumps in digital forensics to reconstruct events, recover data, and analyze user and system interactions.

Forensic Image
A digital representation, snapshot, or copy of a storage device or data from a device. It preserves both the structure and content and is used for the purpose of analysis and investigation in digital forensics. Crucial for digital forensic investigations.

Forensic SSH Server Redirection
A method used by ForensicVM to safely access Windows shared folders over the internet via a reverse SSH connection.

Forensic Virtual Machine (VM)
A digital environment replicated from a forensic image that serves as a snapshot of a system at a specific point in time.

ForensicVM / forensicVM
A specialized or comprehensive virtual machine environment tailored for forensic investigations. It operates on a hypervisor and is derived from a forensic image. The operating system is detected, and necessary drivers are installed to replicate the functionality of the original system. An initial snapshot is created to preserve the original state. The ForensicVM allows detailed examination within a safe and controlled environment, without risk to other systems or compromising the original data. It often has a network card disabled by default for security reasons and offers tools and functionalities essential for digital forensic investigations. Designed to assist forensic investigators in the virtualization, management, and analysis of forensic images, it's essential to manage its operations correctly to preserve the integrity of the evidence.

ForensicVM Client Plugin
A specialized Autopsy plugin that forms one of the two primary components of the ForensicVM project. It is the main program interface running in Autopsy Software and is designed to assist in the processing, converting, and forensic analysis of virtual machines and forensic images. Tailored for managing and interacting with Forensic Virtual Machines (VM), it facilitates the analysis of VM images.

ForensicVM Loader
A component that is part of the ForensicVM toolset and plugin, responsible for initializing and setting up the forensic analysis environment for VM analysis.

ForensicVM Main Screen
The primary interface of the forensic virtual machine when accessed via the web.

ForensicVM Main Web Interface or web page
The primary interface of the ForensicVM, where users can navigate to various tools and features, including the WebShell and Netdata.

ForensicVM Server
The main backbone of the ForensicVM system, developed using Django and Python, it facilitates the functionalities of the ForensicVM.

ForensicVM Server Remote Web Screen/Console Control Interface
A web-based interface designed for remote forensic investigators to collaborate and control the ForensicVM. It lets users interact with the forensicVM directly and provides an interactive console for access to the virtual screen of the remote ForensicVM. It serves as a display of the forensicVM as seen when accessed remotely, especially through web interfaces.

ForensicVM Webscreen Console Control Toolbar
A detailed overview of the Control Toolbar in the ForensicVM Webscreen Console.

ForensicVM.exe
The setup file responsible for installing the AutopsyVM client plugin on a user's system.

FTK Imager
A product by AccessData, used for capturing and analyzing memory dumps.

Gigabit connection
A network connection that offers speeds of up to 1 gigabit per second.

GRR (Google Rapid Response)
An incident response framework that includes memory analysis capabilities.

Halt
The act of temporarily pausing or stopping the operations of the forensicVM without fully shutting it down.

Hash Dump File
A file that contains hashed representations of data. In the context, it is identified as potential evidence.

Hibernate File Management
Tools or methods to manage or remove hibernation files.

Hibernation
A power-saving mode for computers. In Windows, when the system goes into hibernation, it saves the current state of the system (including open applications and documents) into the hibernation file and shuts down, allowing for a faster start-up later.

Host
In the context of Autopsy, refers to a machine or system from which data is being collected or investigated.

Host configuration
The settings that determine how the data source is treated or processed within a forensic analysis environment.

HP ILO
Integrated Lights-Out. A remote management tool used for server administration.

Hypervisor
A piece of software, firmware, or hardware that creates and manages virtual machines (VMs). Also known as a virtual machine monitor (VMM), it is responsible for the execution of virtualized forensic images, manages resources, and ensures isolation between different instances.

ifconfig
A system administration utility in Unix-like operating systems to configure, control, and query TCP/IP network interface parameters.

Immediate Reboot
A rapid restart of the forensicVM without fully shutting it down. This is especially useful in scenarios requiring quick troubleshooting, testing, or managing different VM states.

Immutable Record
Non-alterable and chronological documentation, especially in the form of a video, captures every action and finding during an investigation.

Import
The act of bringing data into a software platform (like Autopsy) from an external source.

Import Evidence Disk
A function or feature that allows users to introduce an evidence disk into the analysis environment.

Ingest Modules
Modules in Autopsy that perform data extraction, analysis, and organization tasks automatically for the investigator.

Ingest Plugins
Plugins or modules in forensic software that are used to process and analyze specific types of data or evidence.

Insert ISO / Web Insert CD-ROM
Procedure to virtually insert an ISO file or CD-ROM for access within the ForensicVM environment.

Installation / Installation and Setup
The process of setting up various components, such as Netdata on a system. For ForensicVM Server, Netdata comes pre-installed. It also involves the steps necessary to install and prepare ForensicVM for use.

Interface
The user-friendly platform of ForensicVM that presents various features and tools systematically.

IP Conflict
Occurs when two or more devices or components on the same local network claim to have the same IP address, leading to network malfunctions.

ISO / ISO files
ISO 9660, also known as ECMA-119, is a file system for optical disc media standardized by the International Organization for Standardization (ISO). It is an optical disc image containing the content from a CD, DVD, or Blu-ray Disc that can be used to reproduce the content of these media. In the context of forensic tools, ISO files are encapsulations of entire file systems used to house specialized forensic tools. (Reference: ISO 9660 on Wikipedia)

ISO Management
The handling of ISO files, which are typically used for optical disk images.

Kali Linux Forensic Tools
A set of forensic tools provided by the Kali Linux distribution.

KVM / Kernel-based Virtual Machine
A virtualization infrastructure for the Linux kernel that allows the kernel to function as a hypervisor.

KVM drivers
Drivers optimized for KVM virtualization.

Legal Compliance
Adhering to standards and requirements established by legal authorities, ensuring the chain of custody is maintained.

Legal Evidence
In legal proceedings, memory dumps might provide evidence related to computer usage, unauthorized access, and intellectual property theft.

Link Creation
A method where a link is established between the local forensic image and a new VM on the server.

Link Mode
A specific mode in which a forensic image is linked, rather than copied, to the forensicVM.

Linux Terminal
A command-line interface in Linux-based operating systems for executing commands.

List Remote ISO Files
An overview of ISO files stored remotely on the ForensicVM server.

List Remote Snapshots
A feature that allows users to manually fetch and view the list of all snapshots associated with a ForensicVM from a remote server.

Logical Files
A type of data source in Autopsy representing non-physical files, often used for importing various types of digital data.

Login Button
A button clicked after entering username and password to gain access to the web interface.

Magnet RAM Capture
A free tool designed to capture physical RAM.

Main Panel Overview
A detailed breakdown of the main display area based on the selected tab option.

Main Plugin Interface
The primary user interface within a specific framework, such as Autopsy, from where the forensicVM can be initiated, managed, and controlled. It also offers options to shut down the forensicVM.

Main Toolbar Overview
A description of the primary toolbar on the Autopsy ForensicVM Client Plugin.

Main Web Interface
The primary browser-based interface for managing and interacting with the forensicVM.

Media Control Modal Box
An interface component used in the process of inserting or ejecting ISOs via the web interface.

Media Control Modal Panel
A specific part of the web screen interface that provides controls for media management.

Media Management in ForensicVM
The procedure to navigate, upload, select, insert, eject, delete, and boot from ISO files within ForensicVM.

Media Panel
An interface section within the Autopsy ForensicVM Client Plugin used to manage different media files, including ISOs.

Media Panel Separator
A component in the ForensicVM Client Plugin to access the Media Panel.

Memory
RAM (Random Access Memory) usage and availability, tracked by Netdata.

Memory Dump
A snapshot or the recorded state of the working memory (RAM) of a computer program or system at a specific time. Used in forensic analysis to review the state of the system and includes tools to engage with the active memory data of the forensic virtual machine.

Meterpreter

A type of payload in the Metasploit framework that provides an investigator with a command line interface to the targeted system. In the context, its deployment is considered as potential evidence.

Modifying Memory Size

The process of adjusting the ForensicVM's memory size within the "Fine-Tuning" section of the Autopsy ForensicVM Client interface.

MoonSols DumpIt

A tool for creating memory dumps from Windows systems.

MS-DOS Command Window

A command-line interface available in older versions of Windows.

Netdata

A real-time health monitoring and performance troubleshooting tool for systems. It offers insights into server and application performance.

Network

Options to manage network settings and operations for the ForensicVM.

Network Card

A hardware component or a virtual representation that connects a computer to a network.

Network Isolation

A safety measure that eliminates the need for network connectivity to mitigate associated risks.

Network Troubleshooter

A built-in Windows tool designed to diagnose and fix common network issues.

Notable Item Tag

A label or marker in Autopsy, used to identify and categorize significant pieces of evidence or data points during forensic analysis.

Notification Area

A designated area on the interface for system notifications, warnings, and error messages.

NVMe

Non-Volatile Memory Express. A modern protocol developed for SSDs to exploit the full potential of high-speed PCI Express storage devices.

Open ForensicVM

An action or option to access and interact with the forensicVM's main display, either through the Autopsy plugin or web interface. This can be initiated through various means such as a button within the Autopsy ForensicVM Client Plugin that allows users to launch the WebShell in their default browser.

Output Console

A console that captures all system messages and is instrumental for debugging.

Panel Opener

An interface element within the forensicVM used to reveal various options or configurations.

Password Administration

Tools or methods to reset forgotten passwords or generate new administrator accounts.

Patch Accessibility

A strategic patch enabling the invocation of a system-level cmd.exe prompt by pressing the shift key five times on the Windows login screen.

pcap Directory

The directory or folder where pcap files, often extracted from the pcap.zip, are stored for analysis.

pcap.zip

A compressed file containing Wireshark pcap files collected during the network card activity periods.

Picture Analyser Plugin

A plugin in Autopsy used to analyze and manage pictures or images.

Plugin Architecture

A method by which external additions can be made to extend a software's capabilities.

Plugin Interface

The user interface provided by a software plugin, such as the one in Autopsy for the forensicVM.

Plugin Location

The directory or file path where the AutopsyVM client plugin will be installed on your computer.

Plugin/Plugins

Modular software components that add specific features to an existing computer program. Within the context of ForensicVM and Autopsy, the plugin architecture fosters community involvement and functionality expansion. They enhance or extend functionality and provide forensic investigators with capabilities to bypass protections in locked forensicVM machines. They may also help in functions such as creating new user credentials or resetting existing ones.

Possible Evidence virtual drive

A dedicated virtual drive within ForensicVM designed to store potential pieces of evidence without contaminating the original data.

Power Off/Log Out Option

An option in operating systems (like Ubuntu 22.10) that allows users to either shut down or log out of their accounts. Proper shutdown is recommended to ensure the integrity of collected evidence.

Pre-plugin Execution Recommendation

A cautionary advice to capture a snapshot of the machine's state before initiating any plugin.

Protective Shield

The protection provided by ForensicVM's virtual environment to the host system against potential threats.

Python

A high-level programming language known for its clear syntax and readability.

ython Ingest Plugin A plugin in Autopsy written in Python, used to automate the ingestion of data from a data source.

qcow2

A disk file format commonly used in QEMU and KVM virtualization. It is a free and open-source hardware virtualization solution.

QEMU

Quick Emulator. An open-source machine emulator, virtualizer, and hypervisor that performs hardware virtualization. ForensicVM uses QEMU to create a new forensic hypervisor server.

RAID 10

A type of RAID (Redundant Array of Independent Disks) configuration that combines mirroring and striping to protect data. It's recommended for storing forensic images in ForensicVM.

RAM

Random Access Memory. A type of computer memory used for temporary storage and quick access. ForensicVM requires a minimum of 16 GB RAM for efficient operation, although 32 GB or more is recommended for efficient virtualization of forensic images. The Autopsy documentation suggests that the software can use up to 4GB of RAM, not including the additional memory the Solr text indexing server might use.

Readonly windows shares

Network-shared folders in the Windows operating system that do not allow modifications to the shared files. The ForensicVM plugin may create such shares and therefore requires specific permissions.

Real-time Look

Refers to Netdata's capability to update its insights every second.

Recreate Evidence Disk

An action that leads to the deletion and fresh generation of the evidence disk within the Autopsy environment.

Redline

A tool provided by FireEye offering advanced memory and file analysis capabilities.

Rekall

A memory forensics toolkit.

Reset

The act of immediately rebooting the forensicVM, similar to a hard restart. It brings the machine back to its initial or default state without shutting it down completely.

Reset Button

A user interface control designed to immediately reboot the forensicVM, bringing it to its default or initial state.

Reset Windows 2003 or XP Activation

A plugin that resets activation for Windows 2003 or XP.

Reverse SSH connection

A technique where an SSH connection is initiated from a remote machine to the user's machine, essentially reversing the typical connection direction.

Rollback

The process of reverting the state of the ForensicVM to a previously taken snapshot.

Root privileges

The highest level of access rights on a system, allowing full control over all functions and files.

Samba CIFS share

A type of shared resource that can be accessed by other computers. Known as Windows share.

Screenshot

A digital image that captures the contents of a computer screen, often used for documentation, analysis, or reporting purposes.

Screenshot Management

Tools to capture and manage screenshots during forensic investigations.

Sector Size

A fundamental unit of data storage on a disk, usually specified in bytes (e.g., 512 bytes). It is the smallest addressable unit on a disk.

Security Analysis

In cybersecurity, it involves using memory dumps to uncover malware behavior, detect hidden processes, analyze injected codes, and assess user credentials.

Session Cookies

Small pieces of data stored on a user's computer during a browsing session, often containing information about user preferences or authentication status.

Set Your Alarms

A feature in Netdata that allows users to customize alert thresholds based on their needs.

Setting the VM Date & Time

A function that allows users to define the start date & time for the ForensicVM.

Shellinabox project

An open-source project that enables users to access remote servers from a web browser using a web-based terminal emulator.

Shutdown

- **Shut Down VM on the Web Interface**: The method of deactivating the forensicVM directly from the web-based interface.
- **Shut Down VM on the Web Remote Screen**: The method of shutting down the forensicVM when accessed remotely via the web.
- **Shutdown Button**: A user interface control designed to initiate the process to deactivate and shut down the forensicVM. This button is present in the Autopsy Plugin and various other interfaces.
- **Shutdown Icon**: A graphical representation or symbol indicating the control to shut down the forensicVM.

Snapshot

A saved state of a virtualized resource, such as a VM or forensic image.

Snapshot Deletion Interface

An interface or prompt within the ForensicVM client that facilitates the process of deleting a snapshot.

Snapshot Management

- **Snapshot Management**: The control and management of VM snapshots.
- **Snapshot Management in ForensicVM**: A section or functionality within the ForensicVM or its client interface, where snapshots are created, viewed, and managed.

Snapshots

A feature in ForensicVM that captures and preserves the state of the system or evidence at a specific point in time.

SSD

- **SSD (Solid State Drive)**: A storage device that uses integrated circuit assemblies to store data persistently, typically using flash memory.
- **SSD for Acquisition**: A faster type of storage device compared to traditional HDDs, beneficial for speeding up acquisition processes.

SSH

- **SSH (Secure Shell)**: A cryptographic network protocol used for secure data communication and server administration.
- **SSH for Network Services**: Used for operating network services securely over an unsecured network.
- **SSH Connection**: Refers to a Secure Shell connection, which utilizes the cryptographic network protocol for secure data communication.

Start Button

A button used to initiate the forensicVM.

Startup Settings

An option within the "Advanced options" which allows changing the behavior of Windows during startup.

Stop Button

- **Stop Button in Autopsy Plugin**: A button within the Autopsy Plugin interface specifically used to halt the forensicVM.
- **UI Control for Halting**: A user interface control designed to initiate the process to halt and stop the forensicVM.

Tag

A label or marker within Autopsy used to identify and categorize data points or items of interest during forensic analysis.

Tagging

- **Tagging Action**: The act of marking or labeling a specific item (like a screenshot) for identification, organization, or further analysis.
- **Tagging in Forensic Context**: The process of marking or labeling a piece of evidence or finding with a specific tag or label to easily categorize, search, or identify it later.

Tampered Data

Information that has been intentionally altered or falsified to mislead or deceive.

Third-Party Tools

Software or utilities that are not part of the original package or platform but can be integrated or used alongside it for additional functionalities.

Time Zone

A region that observes a uniform standard time for legal, commercial, and social purposes.

Timestamps

Digital records of specific times at which events occurred.

Tools

Additional utilities for forensic operations within the ForensicVM interface.

Traffic Analysis

The process of intercepting and examining messages to deduce information from patterns in communication, endpoints, and more.

Transparency and Accountability

The assurance that the forensic process is done ethically and without tampering, as demonstrated by a detailed log such as a video recording.

Troubleshoot

A selection available during boot-up that aids in diagnosing and fixing issues that prevent the system from starting.

TTPs (Tactics, Techniques, and Procedures)

Patterns of activities or methods associated with a specific threat actor or group of threat actors.

Ubuntu 22.10

A version of the Ubuntu operating system. Ubuntu is an open-source software platform that runs everywhere from the PC to the server and the cloud.

UEFI

Unified Extensible Firmware Interface, a specification for the software program that connects a computer's firmware to its operating system.

UEFI QEMU DVD-ROM

A UEFI-compatible DVD-ROM virtual device provided by QEMU, a hosted virtual machine monitor.

UUID (Universally Unique Identifier)

A 128-bit number used to uniquely identify some object or entity on the Internet. In this context, it identifies the specific ForensicVM instance that was deleted.

Virtual CD-ROM Drive

A simulated or software representation of a CD-ROM drive that allows the mounting and reading of ISO files as if they were physical discs.

Virtualization

The creation and management of virtualized instances of certain resources, in this context, forensic images.

Virtualize Tab
The main tab within the toolbar that provides access to core ForensicVM operations.

VM
Virtual machine - In computing, a virtual machine (VM) is the virtualization or emulation of a computer system. Virtual machines are based on computer architectures and provide the functionality of a physical computer. Their implementations may involve specialized hardware, software, or a combination of the two. Virtual machines differ and are organized by their function, shown here: System virtual machines (also called full virtualization VMs) provide a substitute for a real machine. They provide the functionality needed to execute entire operating systems. A hypervisor uses native execution to share and manage hardware, allowing for multiple environments that are isolated from one another yet exist on the same physical machine. Modern hypervisors use hardware-assisted virtualization, with virtualization-specific hardware features on the host CPUs providing assistance to hypervisors. (Reference: https://en.wikipedia.org/wiki/Virtual_machine)

VM Control
Options to manage the basic operations of the forensic virtual machine.

VM File (Virtual Machine File)
A file representing a virtual machine, which contains an OS, applications, and data, and can be executed on a hypervisor.

VM Image
A virtual disk image, which contains a virtual system's disk data, used for creating replicas of or taking snapshots of original virtual disks.

vmdk
A disk file format used for virtual appliances developed for VMware products.

Volatility
An open-source memory forensics framework.

Web Interface
An interface accessible via a web browser where users can control the forensicVM.

Web Interface

- **Web Interface for Managing ForensicVM**: A web-based platform from which users can manage and control the forensicVM. It offers different functionalities, including shutting down or stopping the machine.
- **Web Interface for Controlling ForensicVM**: A web-based platform through which users can manage, control, and reset the forensicVM. It is accessible through a browser and might be preferable for remote operations or specific service interfaces.

Web Interface URL
The web address used to access the forensicVM's browser-based interface.

Web Remote Screen / Web Remote Screen (Shutdown)

- **Web Remote Screen**: A specific section of the web interface tailored for remote access. It allows users to remotely control and manage the forensicVM, providing options like shutting down the machine.
- **Web Remote Screen (Shutdown)**: A method to shut down the forensicVM when accessed remotely, offering flexibility for those working from distant locations or specific service interfaces.

Web Remote Screen Interface
A web-based interface allowing users to remotely control and manage the forensicVM. It can be accessed after logging in. It provides options to reset the machine, among other functionalities.

Web Screen Interface

- **Web Screen Interface**: A web-based platform through which users can interact with and manage the forensicVM.

- **Web Screen Interface**: An interface within the forensicVM that provides access to various settings including network configurations.
- **Web Screen Interface**: A web-based interface that provides access to various functionalities, including the ability to eject and manage media within the ForensicVM.

Webscreen Console Main Area
A description of the main area in the ForensicVM Webscreen Console.

WebShell
A script that can be uploaded to a web server to enable remote administration of the machine.

WebShell for Remote Administration
A tool based on the shellinabox project adapted into a Django application that facilitates enhanced remote server administration, offering secure root access to the server.

WebShell Interface
The user interface that is presented upon accessing the WebShell, providing a direct and secure interaction with the server.

What-If Analysis
A series of hypothetical scenarios in forensic investigations, where investigators simulate actions to test different hypotheses.

WinDbg
Microsoft's debugger used for debugging Windows applications and analyzing memory dumps.

Windows 10 or later
A version of the Microsoft Windows operating system. ForensicVM supports Windows 10 and its successors for running the Autopsy plugin.

Windows Explorer
The default file manager in Microsoft Windows operating systems that provides a graphical user interface for accessing the file system.

Windows Share
A feature in the Windows operating system that allows files and folders to be shared over a network.

Wireshark
A network protocol analyzer tool that captures network packets in real-time and displays them in a human-readable format for detailed analysis.

Wireshark pcap
A specific file format used to capture and store network packets for later analysis using tools like Wireshark. It is commonly used to capture and save network traffic data.

Wizard Interface
A user-friendly interface in software that guides users through a process step by step.

X-Ways Forensics
A commercial forensic software with strong memory analysis features.

ZIP File
A file format that allows for lossless data compression. It can contain multiple files or folders compressed into a single file.

CHAPTER

TEN

LIST OF FIGURES

LIST OF FIGURES

INDEX