

**GROUP ASSIGNMENT**

**CT046-3-1-ISFT**

**INTRODUCTION TO SECURITY AND FORENSIC TECHNOLOGIES**

**APD1FCS(CYB) / APU1FCS(CYB)**

**------------------------------------------------------------------------------------------------**

**HAND OUT DATE: 2 February 2024**

**HAND IN DATE: 29 JUNE 2024**

|  |  |
| --- | --- |
| **TP number** | **Name** |
| TP078221 | Abdur Rehman Mohmmed Firasath (Leader) |
| TP077667 | Talla Elrashed Ahmed Suliman |
| TP077473 | Lim Tze Ern |
| TP077401 | Anas Waddah Mohammed Qaid |
| TP076879 | Ahmed Mohamed Sadiq |

Table of Contents

[Introduction 3](#_Toc170427368)

[Forensic Tools Used 4](#_Toc170427369)

[Data Acquisition: RAM & HDD 8](#_Toc170427370)

[Analysis: RAM & HDD Image Analysis 14](#_Toc170427371)

[4.1 RAM Image Analysis 14](#_Toc170427372)

[4.2 HDD Image Analysis 17](#_Toc170427373)

[5.0 Technical Report 32](#_Toc170427374)

[6.0 Conclusion 32](#_Toc170427375)

[7.0 Workload Matrix 34](#_Toc170427376)

[8.0 References 35](#_Toc170427377)

# **Introduction**

Forensic investigations play a crucial role in cybersecurity by comprehending and reducing threats of malware and other types of malicious activity. This research will cover forensic procedures of data acquisition, analysis and reporting on a compromised windows 10 virtual system, placing us right in the centre of these kinds of investigations.

Our primary objective is to find and record evidence of harmful activities on the provided system. This call for a thorough root cause analysis to find and examine any possible danger.

We will work together to do extensive investigative tasks in order to determine the type and extent of the security breach.

# **Forensic Tools Used**

1. **Volatility**

Volatility is an important memory forensic framework designed to analyse memory dumps from windows, macOS and Linux. In the context of a window 10 forensic investigation, volatility is particularly valuable for retrieving crucial data that might not be accessible through commonly used disk-based forensics.

Forensic investigators typically use it early in investigation to capture and examine data by identifying live and active threats, and by understanding the state of the system at the time of memory capture. Volatility allows analysts to develop or utilize plugins specific to investigation needs.

**key characteristics:**

1. Process analysis

provides detailed insights into running processes including process IDs, command line arguments, and loaded modules. This helps in identifying suspicious activities and detecting malware injection.

1. Network analysis

Reveals active network connections, open ports and associated processes during memory capture. Aiding to understand communication patterns and identify malware command and control channels

1. Registry analysis

Extracts window registry hives from memory dumps, recovering keys, values, and timestamps. This is essential for understanding system configuration, user activity and the effects of malware.

1. File system analysis

Identify open file and directory in memory dumps by assisting in understanding file access patterns and detecting files effected by malware.

1. **FTK imager**

Developed by AccessData, FTK imager is a versatile tool used for disk imaging and analysis. It is essential for acquiring images of storage devices in a forensic sound matter.

It is used during acquisition phase because it allows investigators to capture 9a pristine copy of digital evidence without altering source data

**key characteristics:**

1. Disk imaging

FTK imager allows forensic analysts to create bit-for-bit copies of hard drives, SSDs, USB drives and other storage media, ensuring data integrity through hashing (MD5, SHA-1, SHA-256) enabling verification of acquired images.

1. File analysis

FTK imager examines file metadata such as timestamps, file paths and permissions. Analysts can recover deleted files and analyse file content for digital evidence.

1. Forensic integrity

The tool adheres to forensics best practices, ensuring that images retrieved maintain integrity and can be presented as admissible evidence in legal proceedings, supporting various image formats and offers tools for viewing and verifying content.

1. **Autopsy**

Is a digital forensic platform developed by basis technology, providing a graphical interface for analysing disk images, filesystems, and other forms of digital evidence.

It is mainly used for its ability to handle large volumes of data & streamline analysis tasks. Its intuitive interface and comprehensive features enable analysts to conduct through examinations, generated detailed reports, and present findings effectively.

**key characteristics:**

1. Automated analysis

The platform incorporates automated analysis module to scan disk images for potential evidence automatically. This include identifying file types such as document, images or email, highlighting and flagging suspicious activity.

1. Keyword search

Investigators can perform keyword searches across disk images and file contents, enabling targeted searches for specific terms or indicators related to malicious activity, targeting & locating relevant information quickly in a vast amount of data

1. Timeline analysis

Supporting timeline creation based on file timestamps, user activity and system

events, identifying correlations and establishing timelines of incidents/activities.

1. Hash filtering.

The platform integrates hash sets to filter out known good files or identify files matching known malware signature. this assist in prioritizing analysis efforts and focusing on potential malicious files within the examination scope.

1. **VirusTotal**

Owned by Google, VirusTotal is an online service launched in 2004 that analyse files and URLs to detect viruses, worm, trojans, and other kinds of malicious attacks.

VirusTotal works by aggregating many antivirus products and online scan engines to provide a detailed analysis of submitted files or URLs.

**key characteristics:**

1. File analysis

Users can upload multiple files to the service for scanning, supporting a big range of file formats & sizes while generating a detailed reports that include detection names from each scanning engine and additional metadata.

The reports help users understand the type of threat they may face and its potential impact

1. URL analysis

VirusTotal allows users to submit URLs for scanning, it checks these URLs against multiple databases to detect attacks such as phishing and malware.

This URL service makes VirusTotal a user-friendly website, making it easy investigators to submit URLs for scanning and to interpret the results.

1. Hash search

Similar to FTK imager, Users can search files using hashes such as MD5, SHA-1, and SHA-256. This feature allows investigators to conclude if a file has been previously analysed and access the existing reports.

1. Integration with other tools

VirusTotal enhancing its utility in broader security and forensic workflows by integrating seamlessly with various security tools

Below is a list of some forensic tools that VirusTotal can integrate with:

|  |  |  |  |
| --- | --- | --- | --- |
| **NO.** |  | **Forensic Tools** |  |
| 1 | Autopsy | 6 | Prodiscover |
| 2 | Encase | 7 | Cellebrite |
| 3 | OS forensics | 8 | Helix3 |
| 4 | FTK imager | 9 | The sleuth kit |
| 5 | Volatility | 10 | X-ways forensic |

# **Data Acquisition: RAM & HDD**

In the field of digital forensics, evidence collection is a critical step in understanding the nature and extent of a cyber incident. Two primary sources of digital evidence are hard disk drives (HDDs) and random-access memory (RAM). Each offers distinct insights into the state of a system at a specific time and requires tailored acquisition techniques due to their differing characteristics and volatility.

Let's proceed into the details of how data is acquired from these sources and why this process is so crucial for a thorough forensic investigation.

**Random Access Memory (RAM) Acquisition**

RAM is like the short-term memory of a computer. It only holds data while the computer is on. When we acquire data from RAM, we're getting a snapshot of what was happening at that moment: what programs were running, what websites were open, etc.

These are the steps to capture memory within a virtual machine (VM) using FTK Imager and save it to an external USB drive:

**Prerequisites:**

* **FTK Imager:** Ensure you have FTK Imager installed within your virtual machine. You can download it from the AccessData website if needed.
* **External USB Drive:** Have a formatted USB drive with sufficient space to store the captured memory image.

A screenshot of a computer

Description automatically generated**Steps:**

1. **Connect the USB Drive:** Insert the USB drive into the physical host machine (the computer running the virtual machine software).
2. **Make USB Accessible to VM:** In your VM software's settings (e.g., VirtualBox, VMware), configure the USB drive to be accessible within the VM settings, find the A screenshot of a computer

   Description automatically generatedUSB section, and selecting your USB drive from the list of available devices.
3. **Open FTK Imager in VM:** Launch FTK Imager within the virtual machine.
4. **Capture Memory:**

Go to **File** > **Capture Memory**.

A screenshot of a computer

Description automatically generated

1. **In the dialog box:** Choose the destination for the memory image. Browse to the mounted USB drive and select a location to save the file.

(Optional) Enable the "Include Page file" option to capture data from the VM's page file (virtual memory). Click **Capture** Memory

1. **A screenshot of a computer

   Description automatically generatedMonitor the Capture:** FTK Imager will display the progress of the memory capture. This might take some time, depending on the size of the VM's memory
2. **Complete Capture:** Once the capture is finished, FTK Imager will confirm the successful creation of the memory image on the USB drive.

A computer screen shot of a computer screen

Description automatically generated

1. **Confirm The Captured Memory:** Proceed to the directory of the USB Drive to check The Captured Memory
2. **Safely Remove USB Drive:** In your VM software, ensure you safely remove the USB drive from the VM before physically disconnecting it. Then, eject the USB drive from your host machine.

**Hard Disk Drive (HDD) Acquisition**

HDDs are like the long-term storage of a computer. Even when the computer is off, the data stays on the HDD. When we acquire data from an HDD, we're essentially making an exact copy of everything on it, even stuff that's been deleted. This copy is called a forensic image, and it's super important because it lets us analyse the data without messing with the original evidence.

This is how to perform HDD acquisition from a VMDK file using FTK Imager to create an E01 forensic image:

**Prerequisites:**

* **FTK Imager Software:** Download and install the latest version of FTK Imager on your forensic workstation.
* **VMDK File:** Ensure you have the VMDK file of the infected windows
* **Destination Drive:** A drive with enough storage capacity to hold the forensic image and additional metadata.

**Steps:**

1. **Open FTK Imager:**

* Launch FTK Imager with administrative privileges.

1. **Create a New Case:**

* Click on "File" > "Create New Case".
* Provide a case number, evidence number, unique description, and examiner notes (optional).
* Click "Next" to proceed.

Add Evidence Item: Choose "Image File" as the evidence source type.

A screenshot of a computer

Description automatically generated

Select the **VMDK file** from your system. If prompted, also select the associated VMDK descriptor file.**A screenshot of a computer

Description automatically generated**A screenshot of a computer

Description automatically generated Click "Finish" to add the evidence item.

**Verify Image Details:** Double-check the image details displayed in FTK Imager to ensure you are working with the correct VMDK file. Note the original virtual disk's size and any other relevant information.

A screenshot of a computer

Description automatically generated**Image Creation:**

Click on the "Image Creation" tab.

Choose "Add Evidence Item" and select the previously added VMDK image file.

A screenshot of a computer

Description automatically generatedSelect "E01" as the image format.

Set the desired compression level (if any).

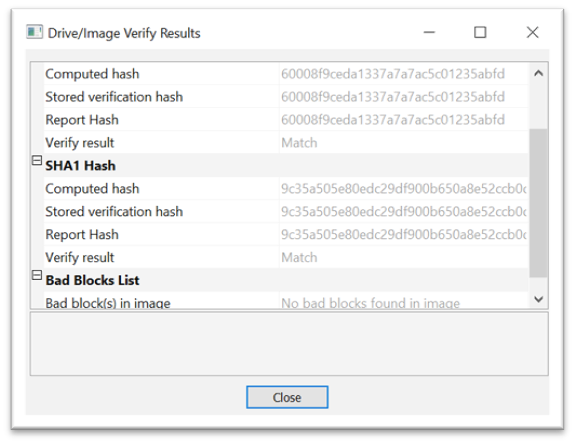
Choose a destination path for the image file and provide a suitable file name.

Enable "Verify images after they are created" to ensure data integrity. Click "Start" to begin the imaging process

A screenshot of a computer

Description automatically generated

**Monitor Progress:** FTK Imager will display the progress of the imaging process, including the elapsed time and estimated remaining time.

**Verification:** Once the imaging is complete, FTK Imager will automatically verify the created image against the source VMDK file (if enabled).

**Verify the MD5 and SHA1** hashes of the image against the values reported by FTK Imager.

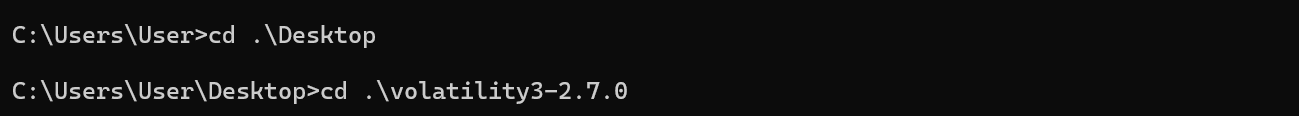
**Securely Store Image:** Store the E01 image file and the associated image info (.txt) file in a secure and known location.

# **Analysis: RAM & HDD Image Analysis**

Volatility is used for the RAM image analysis, while Autopsy is used for the HDD image analysis. VirusTotal is used to identify the malwares.

## **4.1 RAM Image Analysis**

Step 1: Open Volatility from Command Prompt

 *commands to open Volatility*

Step 2: Run the pslist, psscan, pstree, malfind command

A screenshot of a computer screen

Description automatically generated*pslist command with some outputs*

A screenshot of a computer

Description automatically generated *psscan command with some outputs*

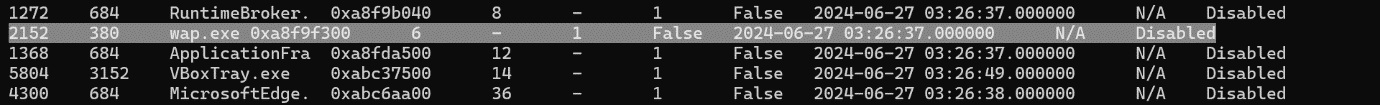
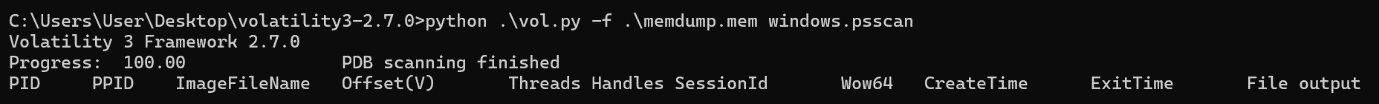
*A screen shot of a computer

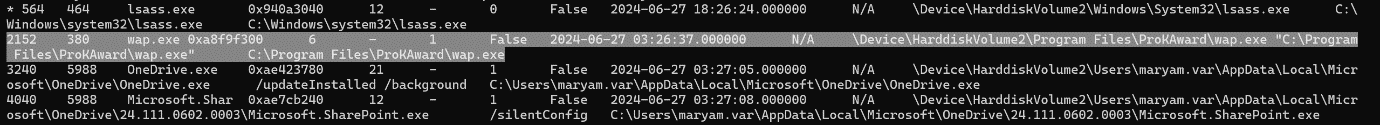
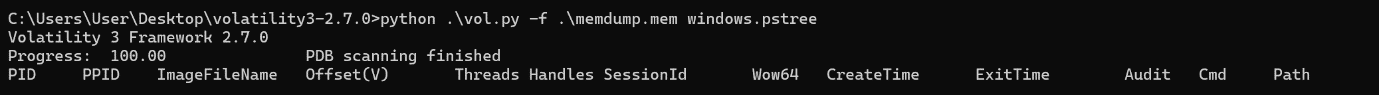
Description automatically generated pstree command with some outputs*

A screenshot of a computer

Description automatically generated *malfind command with some outputs*

Step 3: Analyse the output of the command

 *psscan-wap.exe*

*pstree-wap.exe*

The wap.exe is suspicious after running psscan and pstree, because it is in the ‘ProKAward’ directory, which is not a standard directory.

A black screen with white text

Description automatically generatedA black screen with white text

Description automatically generated*malfind-MsMpEng.exe & SearchUI.exe*

Both MsMpEng.exe & SearchUI.exe files are suspicious, since they have PAGE\_EXECUTE\_READWRITE pages. This is suspicious as it is a common technique used by malware. But it can be false positive.

## **4.2 HDD Image Analysis**

Step 1: Launch Autopsy and choose ‘New Case’.

A screenshot of a computer

Description automatically generated

Step 2: Enter the case information.

A screenshot of a computer

Description automatically generated

Step 3: Select host.

A screenshot of a computer

Description automatically generated

Step 4: Select data source type as Disk Image or VM File.

A screenshot of a computer

Description automatically generated

Step 5: Select data source.

A screenshot of a computer

Description automatically generated

Step 6: Configure Ingest. Select the ingest modules needed.

A screenshot of a computer

Description automatically generated

Step 6: Add Data Source and wait for the analysis to complete.

A screenshot of a computer

Description automatically generated

Step 7: After the analysis completed, check the hash number in VirusTotal to identify the malwares.

Malware 1: win10drivetest (Demo).exe

A screenshot of a computer

Description automatically generated *Autopsy-Metadata of win10drivetest (Demo).exe*

A screenshot of a computer program

Description automatically generated*VirusTotal-Result of win10drivetest (Demo).exe*

Since 61/74 security vendors and no sandboxes flagged this as malicious, it has high potential to be a malware.

Malware 2:

A screenshot of a computer

Description automatically generated*Autopsy-Metadata of filedat.dat*

A screenshot of a computer

Description automatically generated*VirusTotal-Result of filedat.dat*

Since 57/71 security vendors and no sandboxes flagged this as malicious, it has high potential to be a malware.

Malware 3:

A screenshot of a computer

Description automatically generated*Autopsy-Metadata of wap.exe*

A screenshot of a computer

Description automatically generated *VirusTotal-Result of wap.exe*

Since 42/74 security vendors and no sandboxes flagged this as malicious, it has high potential to be a malware.

Malware 4:

A screenshot of a computer

Description automatically generated*Autopsy-Metadata of KMSAuto Net.exe*

A screenshot of a computer

Description automatically generated *VirusTotal-Result of KMSAuto Net.exe*

Since 54/74 security vendors and no sandboxes flagged this as malicious, it has high potential to be a malware.

Malware 5:

A screenshot of a computer

Description automatically generated *Autopsy-Metadata of KMSCleaner.exe*

A screenshot of a computer

Description automatically generated *VirusTotal-Result of KMSCleaner.exe*

Since 44/74 security vendors and no sandboxes flagged this as malicious, it has high potential to be a malware.

Malware 6:

A screenshot of a computer

Description automatically generated*Autopsy-Metadata of wap.dll*

A screenshot of a computer

Description automatically generated*VirusTotal-Result of wap.dll*

Even there is only 7/72 security vendors and no sandboxes flagged this as malicious, it has the potential to be a malware.

Malware 7:

A screenshot of a computer

Description automatically generated *Autopsy-Metadata of wrar56b4.exe*

A screenshot of a computer

Description automatically generated*VirusTotal-Result of wrar56b4.exe*

Even there is only 2/72 security vendors and no sandboxes flagged this as malicious, it has the potential to be a malware.

Malware 8:

A screenshot of a computer

Description automatically generated*Autopsy-Metadata of DW20.exe*

A screenshot of a computer

Description automatically generated*VirusTotal-Result of DW20.exe*

Even there is only 2/66 security vendors and no sandboxes flagged this as malicious, it has the potential to be a malware.

Malware 9:

A screenshot of a computer

Description automatically generated*Autopsy-Metadata of UW.exe*

A screenshot of a computer program

Description automatically generated*VirusTotal-Result of UW.exe*

Even there is only 2/71 security vendors and no sandboxes flagged this as malicious, it has the potential to be a malware.

Malware 9:

A screenshot of a computer

Description automatically generated*Autopsy-Metadata of Builder.exe*

A screenshot of a computer

Description automatically generated*VirusTotal-Result of Builder.exe*

Even there is only 2/71 security vendors and no sandboxes flagged this as malicious, it has the potential to be a malware.

Malware 10:

A screenshot of a computer

Description automatically generated*Autopsy-Metadata of RarExt.dll*

A screenshot of a computer

Description automatically generated*VirusTotal-Result of RarExt.dll*

Even there is only 2/74 security vendors and no sandboxes flagged this as malicious, it has the potential to be a malware.

# **Technical Report:**

Forensic Investigation of an Infected Windows 10 System

**Introduction**

This forensic investigation aims to identify and document evidence of malicious activity on an Infected Windows 10 virtual system. The primary objective is to conduct a root cause analysis to determine the nature and extent of the Malware. The investigation involves data acquisition from both RAM and HDD, followed by a thorough analysis using specialized forensic tools.

**Forensic Tools Used**

1. **Volatility:** A memory forensic framework used for analyzing RAM dumps. It aids in identifying active processes, network connections, registry modifications, and file system interactions.
2. **FTK Imager:** A disk imaging tool used to create forensically sound copies of storage devices. It ensures data integrity and provides a platform for file analysis and recovery.
3. **Autopsy:** A digital forensic platform that offers a graphical interface for analyzing disk images and various types of digital evidence. It automates analysis, facilitates keyword searches, timeline creation, and hash filtering.
4. **VirusTotal:** An online service that analyzes files and URLs to detect malware. It aggregates results from multiple antivirus engines and provides detailed reports.

**Data Acquisition**

* **RAM Acquisition:** RAM data was acquired to capture a snapshot of the system's state at the time of compromise. Volatility was used to analyze the RAM image, revealing suspicious processes and potential malware activity.
* **HDD Acquisition:** An E01 forensic image was created from the VMDK file using FTK Imager. This image preserves the integrity of the original data and serves as a basis for further analysis.

**Analysis**

* **RAM Image Analysis:** Volatility commands like pslist, psscan, pstree, and malfind were used to analyze the RAM image. Suspicious processes like wap.exe, located in a non-standard directory, and MsMpEng.exe and SearchUI.exe, exhibiting PAGE\_EXECUTE\_READWRITE pages, were identified.
* **HDD Image Analysis:** Autopsy was used to analyze the E01 image. Multiple malware files were identified by their hash values and verified using VirusTotal. These include win10drivetest(Demo).exe, filedat.dat, wap.exe, KMSAuto Net.exe, KMSCleaner.exe, wap.dll, wrar56b4.exe, DW20.exe, UW.exe, Builder.exe, and RarExt.dll.

**Conclusion:**

The forensic investigation successfully identified multiple malware infections on the Infected Windows 10 virtual system. The analysis of both RAM and HDD images, along with the use of specialized forensic tools, provided valuable insights into the nature and extent of the compromise. The findings can be used to remediate the system, strengthen security measures.

**Workload Matrix:**

|  |  |
| --- | --- |
| **Work assigned** | **Name & TP number** |
| 1)Forensic Tools Used | Talla Elrashed Ahmed Suliman (TP077667) |
| 2) Data Acquisition: RAM & HDD | Abdur Rehman Mohmmed Firasath  (TP078221)-Leader |
| 3) Analysis: RAM & HDD Image Analysis | Lim Tze Ern (TP077473) |
| 4) Technical Report Conclusion | Anas Waddah Mohammed Qaid (TP077401) |
| 5) Technical Report Conclusion | Ahmed Mohamed Sadiq (TP076879) |

# **References**

1. **Volatility Workbench - A GUI for Volatility memory forensics. (n.d.). Www.osforensics.com.** [**https://www.osforensics.com/tools/volatility-workbench.html**](https://www.osforensics.com/tools/volatility-workbench.html)
2. **Fox, N. (2022, April 12). How to Use Volatility for Memory Forensics and Analysis | Varonis. Www.varonis.com.** [**https://www.varonis.com/blog/how-to-use-volatility**](https://www.varonis.com/blog/how-to-use-volatility)
3. **Menezes, H. (2024, March 7). How to Use FTK Imager: A Step-by-Step Guide. Medium.** [**https://medium.com/@herschel-menezes/how-to-use-ftk-imager-a-step-by-step-guide-7413623c471e**](https://medium.com/@herschel-menezes/how-to-use-ftk-imager-a-step-by-step-guide-7413623c471e)
4. **FTK Imager - Forensic Data Imaging and Preview Solution. (n.d.). Exterro.** [**https://www.exterro.com/digital-forensics-software/ftk-imager#:~:text=Quickly%20assess%20electronic%20evidence%2C%20create%20forensic%20images%2C%20and**](https://www.exterro.com/digital-forensics-software/ftk-imager#:~:text=Quickly%20assess%20electronic%20evidence%2C%20create%20forensic%20images%2C%20and)
5. **Autopsy. (n.d.). Sleuthkit.org.** [**https://sleuthkit.org/autopsy/#:~:text=Autopsy%C2%AE%20is%20a%20digital%20forensics%20platform%20and%20graphical**](https://sleuthkit.org/autopsy/#:~:text=Autopsy%C2%AE%20is%20a%20digital%20forensics%20platform%20and%20graphical)
6. **Tetik, E. (2023, August 4). Introduction to Autopsy — An Open-Source Digital Forensics Tool. Medium.** [**https://medium.com/@edatetkk/introduction-to-autopsy-an-open-source-digital-forensics-tool-fa19cc94cb3f**](https://medium.com/@edatetkk/introduction-to-autopsy-an-open-source-digital-forensics-tool-fa19cc94cb3f)
7. **De Alwis, C. (2018, March 2). Evidence Acquisition Using Accessdata FTK Imager. Forensic Focus.** [**https://www.forensicfocus.com/articles/evidence-acquisition-using-accessdata-ftk-imager/**](https://www.forensicfocus.com/articles/evidence-acquisition-using-accessdata-ftk-imager/)
8. **Thakur, V. (2020, February 10). Forensic Report Sample: Volatile Memory Acquisition using FTK Imager Lite. Medium.** [**https://vishaltk.medium.com/forensic-report-sample-volatile-memory-acquisition-using-ftk-imager-lite-bfd083d9d517**](https://vishaltk.medium.com/forensic-report-sample-volatile-memory-acquisition-using-ftk-imager-lite-bfd083d9d517)
9. **Cawley, C. (2023, August 17). 3 Ways to Transfer Files Between a Virtual Machine and PC on VMware and VirtualBox. MakeUseOf.** [**https://www.makeuseof.com/tag/transfer-files-virtual-machine-guest-host-pc/**](https://www.makeuseof.com/tag/transfer-files-virtual-machine-guest-host-pc/)
10. **DFIRScience. (2022, February 8). Starting a New Digital Forensic Investigation Case in Autopsy 4.19+ [Video]. YouTube.** [**https://www.youtube.com/watch?v=fEqx0MeCCHg**](https://www.youtube.com/watch?v=fEqx0MeCCHg)
11. **Menezes,H. (2024,May 7). How to Use FTK Imager: A Step-by-Step Guide**

[**https://medium.com/@herschel-menezes/how-to-use-ftk-imager-a-step-by-step-guide-7413623c471e**](https://medium.com/@herschel-menezes/how-to-use-ftk-imager-a-step-by-step-guide-7413623c471e)

‌

‌

‌

‌

‌

‌