EncryptEdge Labs

Cybersecurity Analyst Internship

Task Report

atalmamun@gmail.com

Task No: 22

Credit: Offensive Security

EncryptEdge Labs

Table of Contents

1.0 EncryptEdge Labs Internship Task Report

1.1 Introduction

Network forensics plays a critical role in modern cybersecurity operations, particularly within a Security Operations Center (SOC). It involves the collection, preservation, and analysis of network traffic and digital evidence to investigate security incidents, identify malicious activities, and support legal proceedings if necessary. By mastering network forensics, cybersecurity analysts can trace threat actors, understand attack vectors, and strengthen an organization's defenses. This task focuses on introducing core digital forensics principles, practicing evidence handling, utilizing forensic tools, and conducting data analysis through hands-on labs and exercises.

1.2 Objective

The objective of this task is to build foundational knowledge and practical skills in digital forensics. Interns are expected to:

- Understand key principles of digital evidence integrity and chain of custody.
- Gain hands-on experience with forensic tools like Autopsy, FTK Imager, and Sleuth Kit.
- Learn proper techniques for the safe collection, preservation, and analysis of digital evidence.
- Identify indicators of compromise (IOCs) and interpret forensic findings related to security incidents.
- Complete designated TryHackMe labs to reinforce technical concepts through real-world scenarios.

1.3 Requirements

To complete this task successfully, the following resources and actions are required:

- **Tools:** Forensic software such as Autopsy, FTK Imager, Sleuth Kit.
- **Environment:** A controlled virtual environment to perform forensic activities safely.
- **Sample Data:** Provided or sourced forensic datasets for analysis.
- **Labs:** Completion of TryHackMe rooms — "Intro to Digital Forensics," "Windows Forensics," and "Digital Forensics Case," with screenshots as proof.
- **Deliverables:** A comprehensive forensic investigation report including summaries of principles, tool descriptions, collection methods, analysis findings, final interpretations, and lab completion evidence.

2.0 Forensic Principles

Digital forensics is governed by strict principles that ensure the accuracy, reliability, and admissibility of evidence. Following these principles is critical during any forensic investigation to maintain the integrity of the data and uphold legal and ethical standards. This section highlights the key forensic principles, focusing on evidence integrity and the chain of custody.

2.1 Importance of Evidence Integrity

Evidence integrity is fundamental in digital forensics. It refers to maintaining the original state of digital evidence throughout the entire investigation process. If evidence is altered, even unintentionally, its credibility can be questioned, potentially invalidating it for legal proceedings or internal investigations.
To preserve evidence integrity:

- **Use write-blockers:** These devices prevent any changes to the original storage media during data acquisition.

- **Create forensic images:** Instead of working on the original evidence, forensic analysts create exact copies (bit-by-bit images) and conduct their investigations on these duplicates.

- **Maintain detailed documentation:** Every action performed on the evidence must be carefully logged to show that the data has not been tampered with.

- **Validate with hashing:** Hashing algorithms like MD5 or SHA-256 are used to generate a digital fingerprint of the original and copied evidence. Matching hashes verify that no changes occurred during copying.

Maintaining evidence integrity ensures that the findings of an investigation are trustworthy and can withstand scrutiny during legal or organizational reviews.

2.2 Chain of Custody

The chain of custody is the chronological documentation that records the sequence of custody, control, transfer, and analysis of evidence. It is critical for maintaining the legitimacy and traceability of digital evidence from the moment it is collected until it is presented in court or stored.

Key elements of a strong chain of custody include:

- **Clear identification:** Each piece of evidence should have a unique identifier.

- **Detailed logs:** Every handoff, location change, or analysis must be recorded with time stamps, names, and purpose.

- **Controlled access:** Only authorized personnel should handle the evidence, and access should be limited and documented.

- **Secure storage:** Evidence must be stored in secure, tamper-evident environments when not being actively examined.

If the chain of custody is broken or improperly maintained, the evidence could be deemed inadmissible, regardless of its importance to the investigation. Therefore, strict adherence to chain of custody protocols is essential in all digital forensic investigations.

3.0 Tool Selection

Selecting the appropriate forensic tools is a crucial step in conducting a successful digital forensic investigation. The right tools enable analysts to collect, preserve, and analyze evidence efficiently while maintaining its integrity. For this task, I explored multiple industry-standard forensic tools and documented their key functionalities and practical applications.

3.1 Selected Tools and Their Features

Autopsy

Autopsy is an open-source digital forensic platform that simplifies the process of analyzing hard drives and smartphones. It provides a user-friendly graphical interface built on top of the Sleuth Kit.

Key Features:

- **Timeline Analysis:** Visualizes user activity over time to identify patterns or anomalies.
- **Keyword Search:** Allows for extensive search across all files and metadata.
- **File Recovery:** Recovers deleted files and folders from disk images.
- **Hash Analysis:** Compares file hashes to known databases for malware or suspicious files.
- **Reporting:** Generates detailed investigation reports automatically.

Practical Applications:
Autopsy is widely used for file recovery, analyzing user activities, detecting unauthorized file changes, and generating comprehensive reports for legal or organizational use.

FTK Imager

FTK Imager is a forensic imaging tool developed by AccessData. It is used primarily to acquire and verify data from a variety of digital sources without altering the original evidence.

Key Features:

- **Disk Imaging:** Creates forensic copies (images) of hard drives, USB drives, and memory devices.
- **Evidence Preview:** Allows analysts to view files and folders on the source media without making changes.
- **Hash Verification:** Generates MD5 or SHA-1 hashes to ensure image integrity.

- **File Carving:** Extracts files based on known patterns even from corrupted or partially overwritten sectors.

Practical Applications:
FTK Imager is especially useful in the initial evidence collection phase, ensuring that analysts capture a verifiable and unaltered copy of the target data source.

Sleuth Kit (TSK)

The Sleuth Kit (TSK) is a collection of command-line tools used to investigate disk images and file systems.

Key Features:

- **File System Analysis:** Supports various file systems such as NTFS, FAT, EXT.
- **Deleted File Recovery:** Recovers files that have been deleted but not yet overwritten.
- **Timeline Creation:** Constructs detailed timelines based on file metadata changes.
- **Metadata Extraction:** Analyzes file attributes, ownership, and access history.

Practical Applications:
Sleuth Kit is often used in deeper, manual forensic investigations when fine-grained control over evidence parsing is needed, such as during deleted file recovery or timeline creation.

The selection of forensic tools must align with the specific requirements of each case. Autopsy offers a complete and user-friendly analysis platform; FTK Imager ensures safe and verifiable evidence collection; and Sleuth Kit provides powerful command-line tools

for in-depth analysis. Together, these tools form a robust toolkit for conducting comprehensive digital forensic investigations.

4.0 Data Collection

In this section, I practiced forensic data collection techniques to safely gather digital evidence without altering the original data. The process included creating a disk image of a physical drive using FTK Imager on a Windows environment and collecting critical system logs from a Kali Linux machine. Throughout the process, forensic best practices were followed to maintain evidence integrity and avoid contamination.

4.1 Disk Imaging Using FTK Imager (Windows)

4.1.1 Method

To perform forensic imaging, I used **FTK Imager**, a well-established digital forensics tool. The following steps were followed:

1. FTK Imager was launched with **Administrator privileges** to ensure full access to devices.

2. Selected `File → Create Disk Image` to start a new imaging task.

3. Chose **Physical Drive** as the source type to capture the entire disk, including partitions and slack space.

4. Selected the correct external USB drive (carefully verified by size and model).

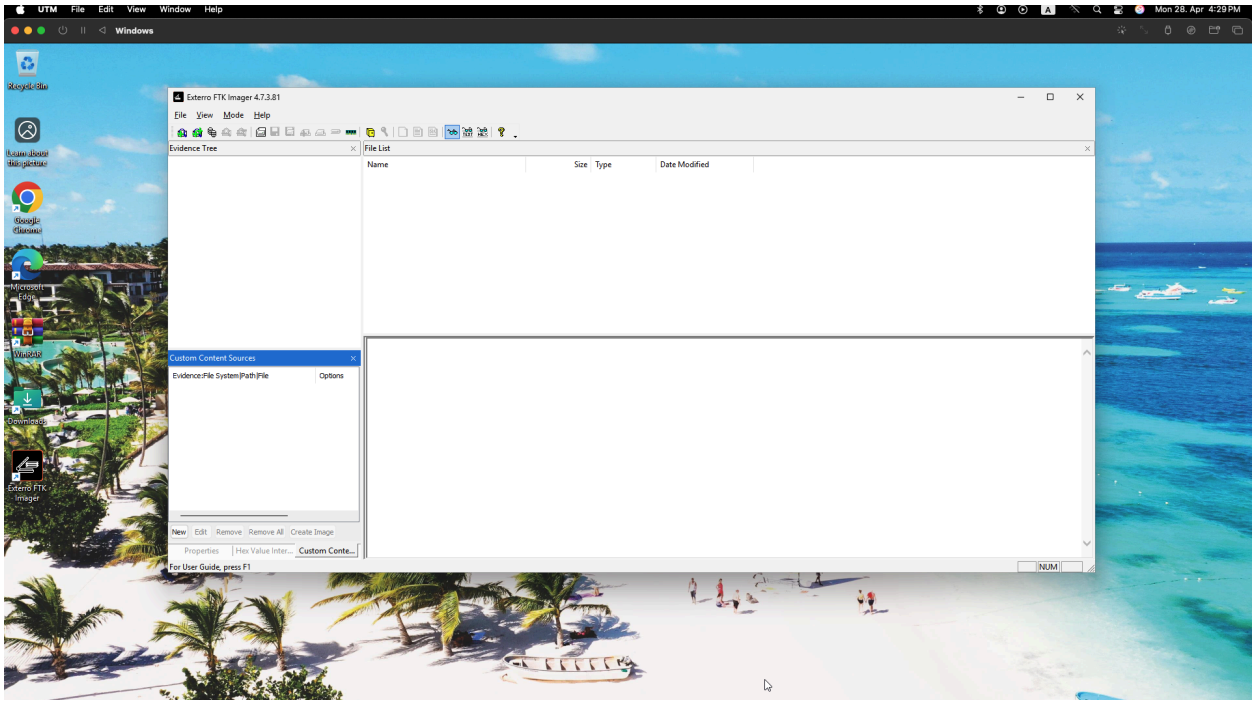
5. Added a destination for the image, choosing the **E01 (EnCase Image File)** format, which supports metadata preservation and compression.

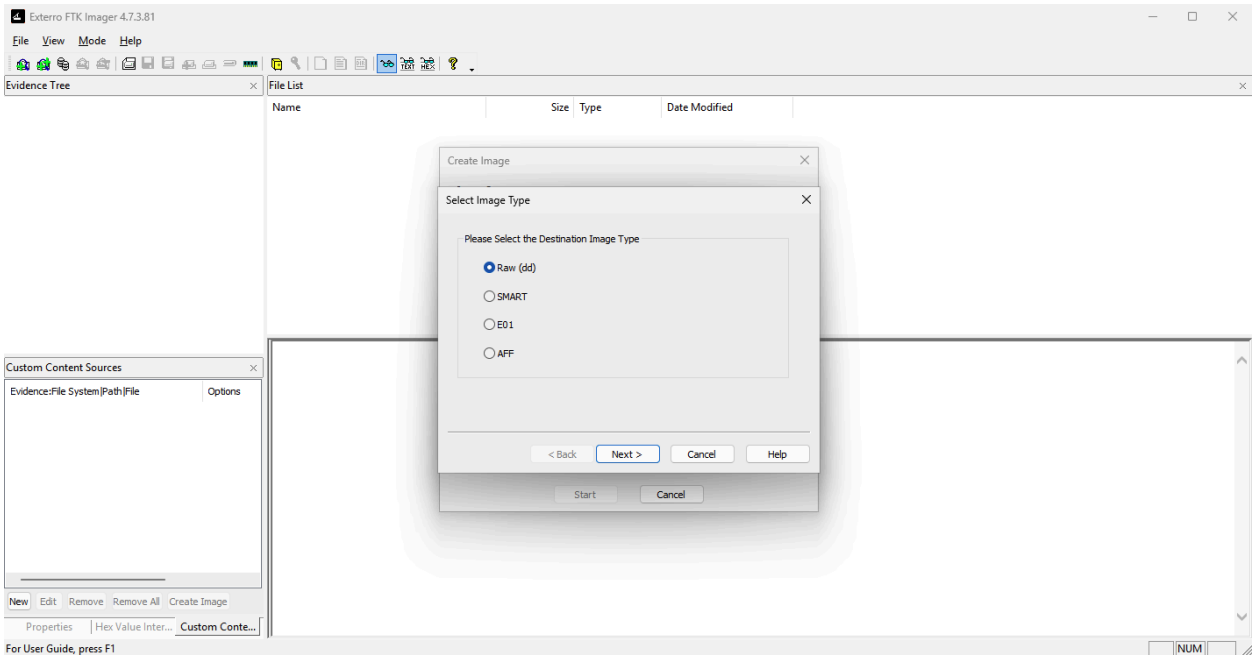
6. Entered case information (Case Number: Task22, Evidence Number: 001, Examiner: Mamun) to simulate real-world documentation practices.

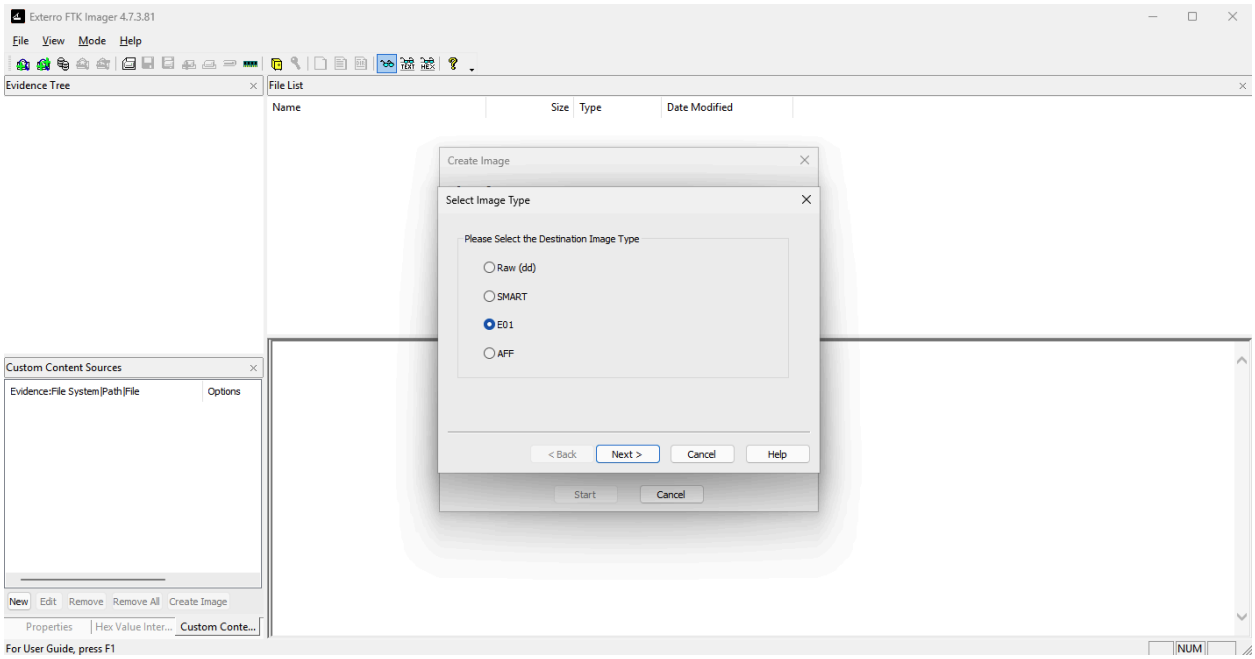
7. Enabled **hash verification** to automatically calculate and verify MD5 and SHA1 hashes.

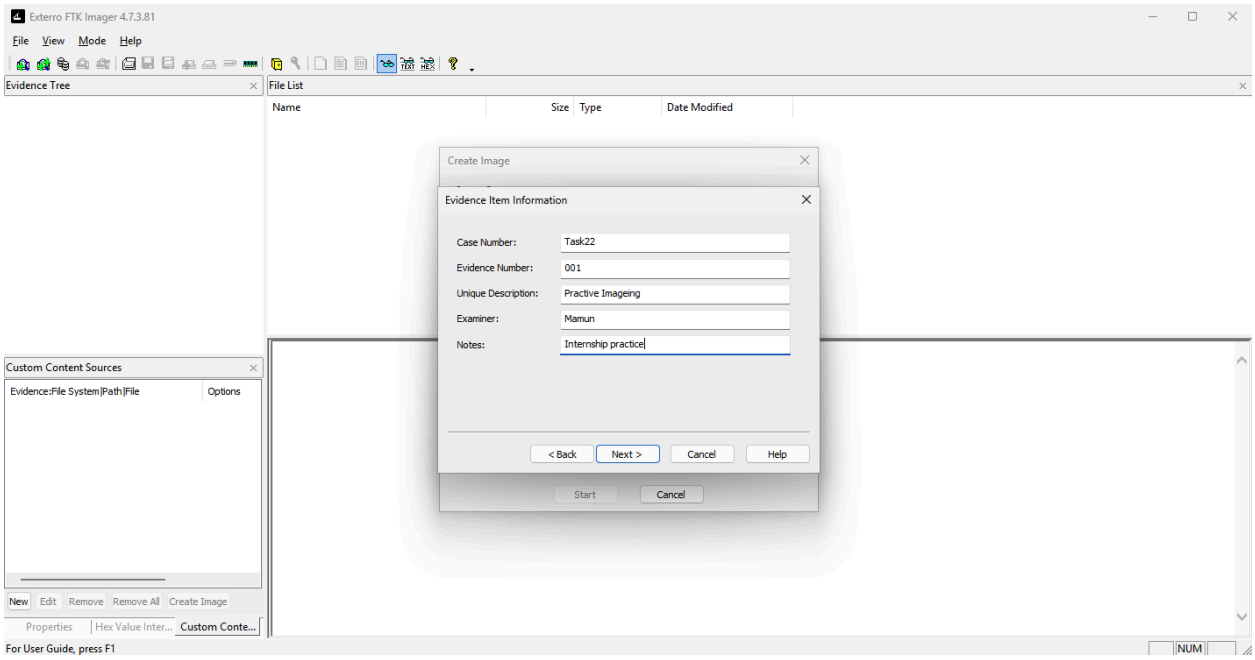
8. Started the imaging process and waited for successful completion.

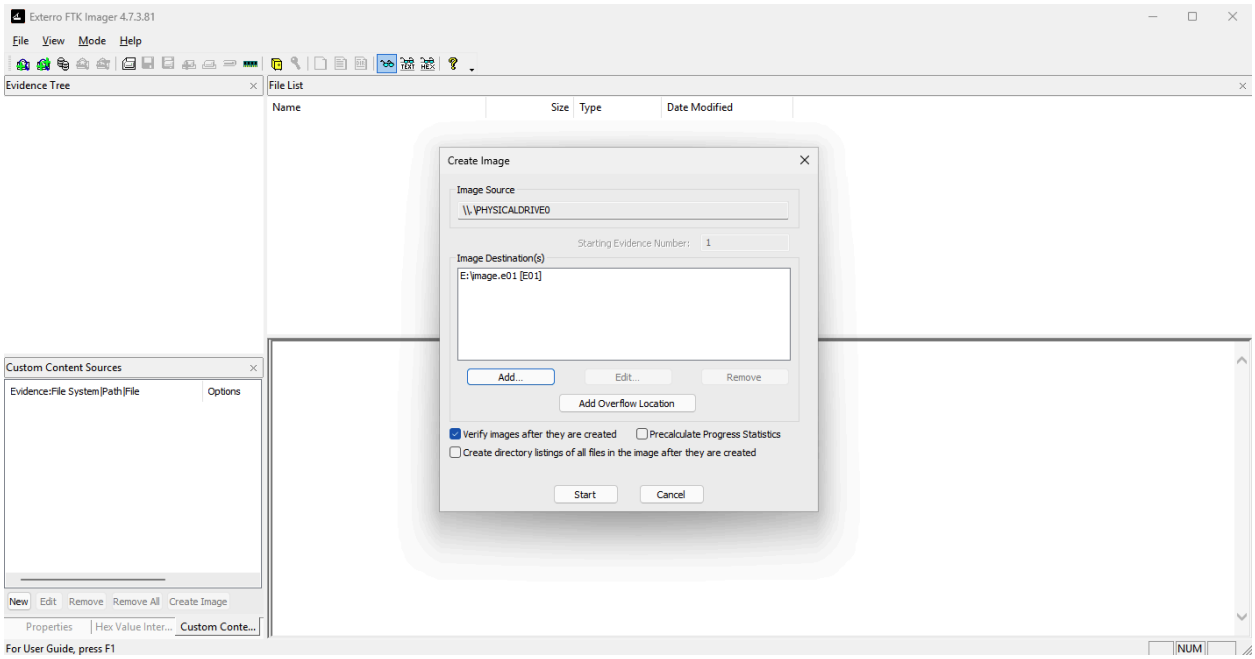
4.1.2 Screenshots

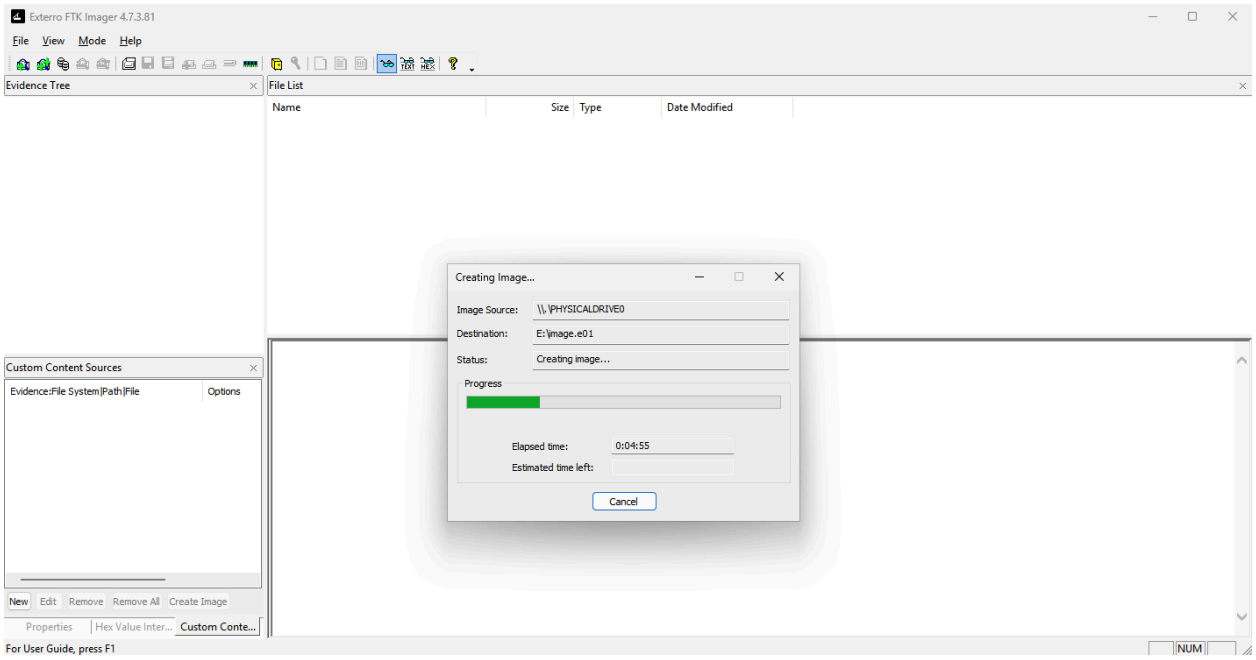



Exterro FTK Imager 4.7.3.81
File View Mode Help
Evidence Tree
File List
Name Size Type Date Modified
Create Image
Select Image Type
Please Select the Destination Image Type
Raw (dd)
SMART
E01
AFF
< Back Next > Cancel Help
Start Cancel
Custom Content Sources
Evidence:File System|Path|File Options
New Edit Remove Remove All Create Image
Properties Hex Value Inter... Custom Conte...
For User Guide, press F1
NUM


Exterro FTK Imager 4.7.3.81
File View Mode Help
Evidence Tree
File List
Name Size Type Date Modified
Create Image
Select Image Type
Please Select the Destination Image Type
Raw (dd)
SMART
E01
AFF
< Back Next > Cancel Help
Start Cancel
Custom Content Sources
Evidence:File System|Path|File Options
New Edit Remove Remove All Create Image
Properties Hex Value Inter... Custom Conte...
For User Guide, press F1
NUM


Exterro FTK Imager 4.7.3.81
File View Mode Help
Evidence Tree
File List
Name Size Type Date Modified
Create Image
Evidence Item Information
Case Number: Task22
Evidence Number: 001
Unique Description: Practive Imageing
Examiner: Mamun
Notes: Internship practice
< Back Next > Cancel Help
Start Cancel
Custom Content Sources
Evidence:File System|Path|File Options
New Edit Remove Remove All Create Image
Properties Hex Value Inter... Custom Conte...
For User Guide, press F1
NUM


Exterro FTK Imager 4.7.3.81
File View Mode Help
Evidence Tree
File List
Name Size Type Date Modified
Create Image
Image Source
\\.\PHYSICALDRIVE0
Starting Evidence Number: 1
Image Destination(s)
E:\image.e01 [E01]
Add... Edit... Remove
Add Overflow Location
Verify images after they are created
Precalculate Progress Statistics
Create directory listings of all files in the image after they are created
Start Cancel
Custom Content Sources
Evidence:File System|Path|File Options
New Edit Remove Remove All Create Image
Properties Hex Value Inter... Custom Conte...
For User Guide, press F1
NUM



4.2 System Log Collection (Kali Linux)

4.2.1 Method

To gather important system logs on Kali Linux without altering original files:

Created a separate forensic folder:

bash
CopyEdit
```
sudo mkdir ~/forensics_logs
```

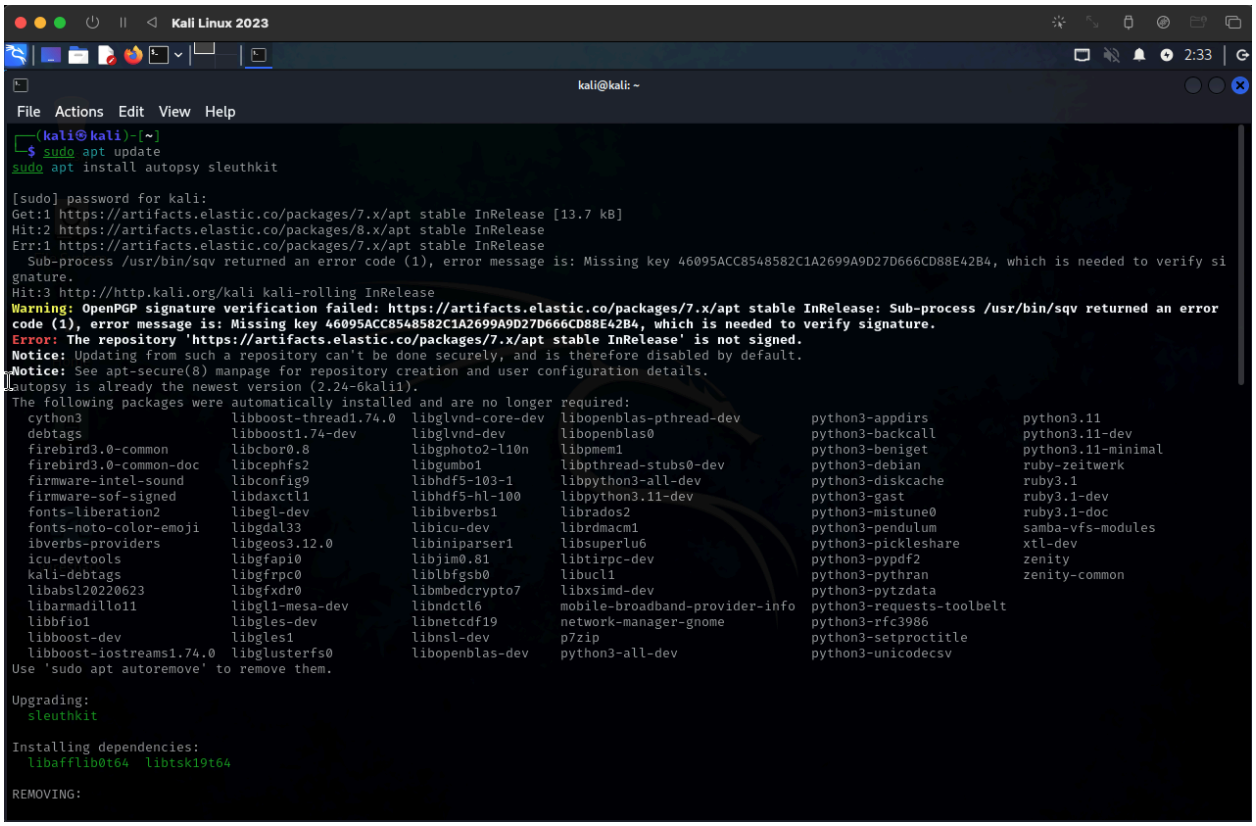
1. Copied essential logs (e.g., `auth.log`, `syslog`) into the forensic folder using the `cp` command:
   ```
   sudo cp /var/log/auth.log ~/forensics_logs/
   ```

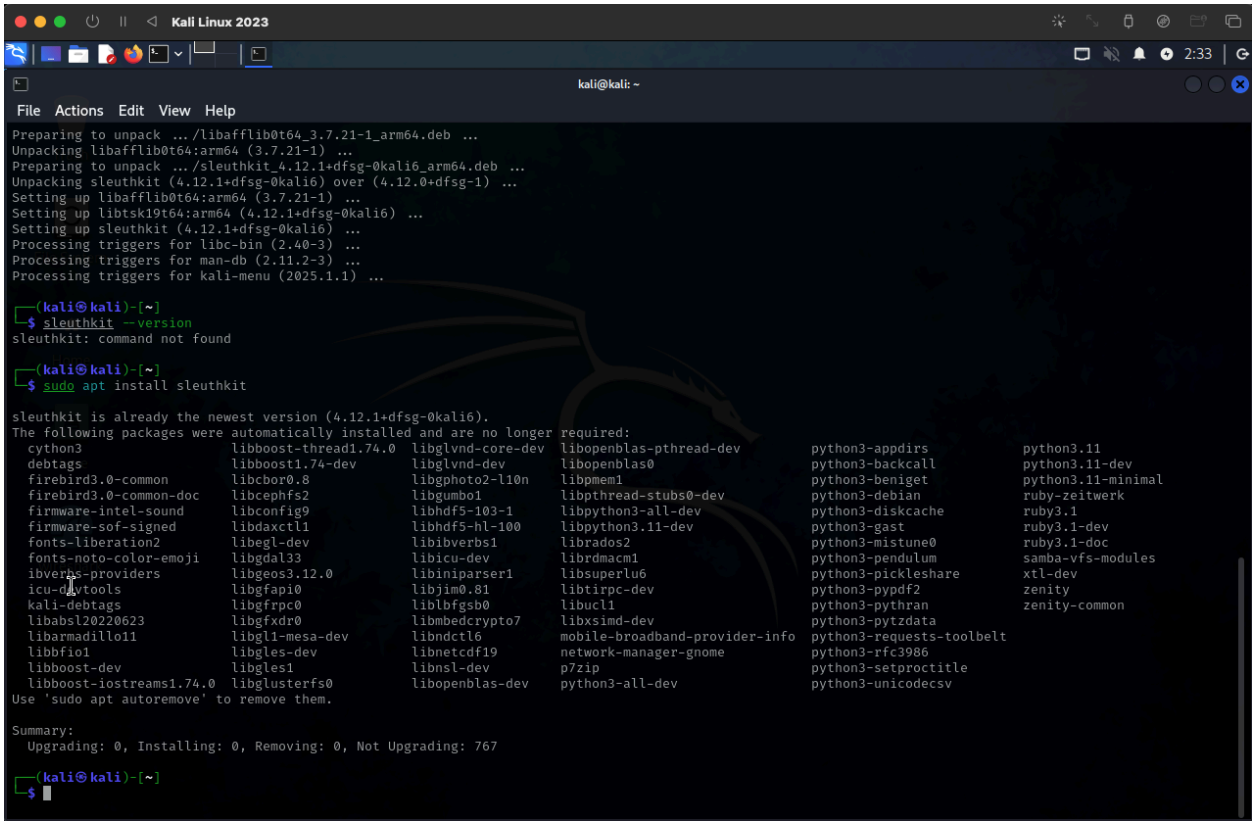
```
sudo cp /var/log/syslog ~/forensics_logs/
```

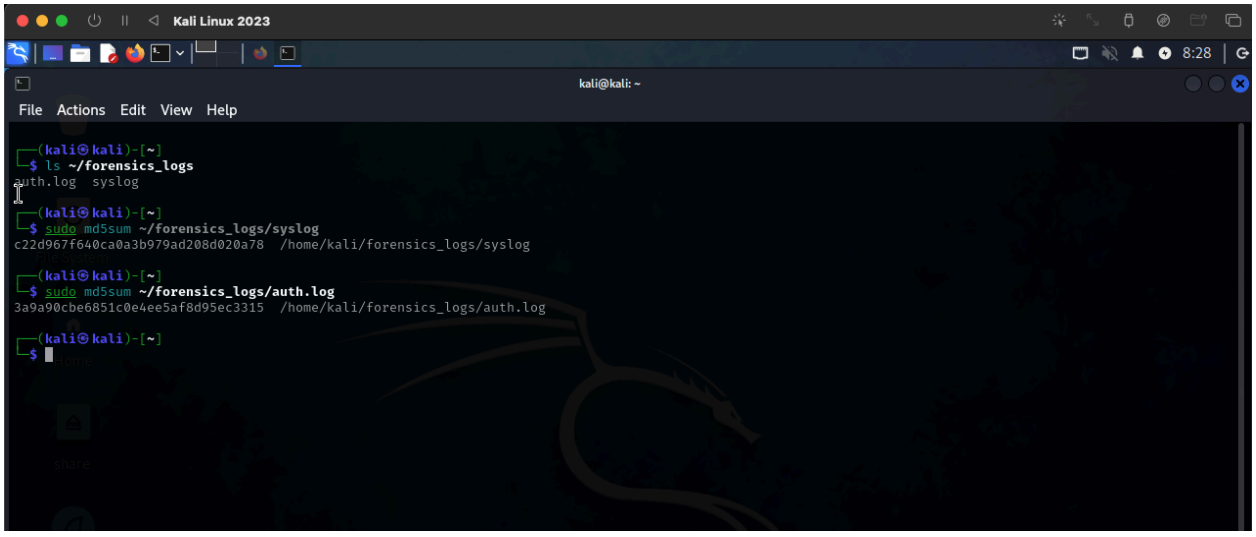
2. Used `md5sum` to generate hash values for both original and copied files to ensure data integrity:
   ```
   md5sum /var/log/auth.log

   md5sum ~/forensics_logs/auth.log
   ```

3. The matching hash values confirmed that the logs were copied without any modification.

4.2.2 Screenshots




Kali Linux 2023
2:33
kali@kali: ~
File Actions Edit View Help
Preparing to unpack .../libafflib0t64_3.7.21-1_arm64.deb ...
Unpacking libafflib0t64:arm64 (3.7.21-1) ...
Preparing to unpack .../sleuthkit_4.12.1+dfsg-0kali6_arm64.deb ...
Unpacking sleuthkit (4.12.1+dfsg-0kali6) over (4.12.0+dfsg-1) ...
Setting up libafflib0t64:arm64 (3.7.21-1) ...
Setting up libtsk19t64:arm64 (4.12.1+dfsg-0kali6) ...
Setting up sleuthkit (4.12.1+dfsg-0kali6) ...
Processing triggers for libc-bin (2.40-3) ...
Processing triggers for man-db (2.11.2-3) ...
Processing triggers for kali-menu (2025.1.1) ...
┌──(kali㉿kali)-[~]
└─$ sleuthkit --version
sleuthkit: command not found
┌──(kali㉿kali)-[~]
└─$ sudo apt install sleuthkit
sleuthkit is already the newest version (4.12.1+dfsg-0kali6).
The following packages were automatically installed and are no longer required:
cython3 libboost-thread1.74.0 libglvnd-core-dev libopenblas-pthread-dev python3-appdirs python3.11
debtags libboost1.74-dev libglvnd-dev libopenblas0 python3-backcall python3.11-dev
firebird3.0-common libcbor0.8 libgphoto2-l10n libpmem1 python3-beniget python3.11-minimal
firebird3.0-common-doc libcephfs2 libgumbo1 libpthread-stubs0-dev python3-debian ruby-zeitwerk
firmware-intel-sound libconfig9 libhdf5-103-1 libpython3-all-dev python3-diskcache ruby3.1
firmware-sof-signed libdaxctl1 libhdf5-hl-100 libpython3.11-dev python3-gast ruby3.1-dev
fonts-liberation2 libegl-dev libibverbs1 librados2 python3-mistune0 ruby3.1-doc
fonts-noto-color-emoji libgdal33 libicu-dev librdmacm1 python3-pendulum samba-vfs-modules
ibverbs-providers libgeos3.12.0 libiniparser1 libsuperlu6 python3-pickleshare xtl-dev
icu-devtools libgfapi0 libjim0.81 libtirpc-dev python3-pypdf2 zenity
kali-debtags libgfrpc0 liblbfgsb0 libucl1 python3-pythran zenity-common
libabsl20220623 libgfxdr0 libmbedcrypto7 libxsimd-dev python3-pytzdata
libarmadillo11 libgl1-mesa-dev libndctl6 mobile-broadband-provider-info python3-requests-toolbelt
libbfio1 libgles-dev libnetcdf19 network-manager-gnome python3-rfc3986
libboost-dev libgles1 libnsl-dev p7zip python3-setproctitle
libboost-iostreams1.74.0 libglusterfs0 libopenblas-dev python3-all-dev python3-unicodecsv
Use 'sudo apt autoremove' to remove them.
Summary:
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 767
┌──(kali㉿kali)-[~]
└─$


Kali Linux 2023
8:28
kali@kali: ~
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ ls ~/forensics_logs
auth.log syslog
┌──(kali㉿kali)-[~]
└─$ sudo md5sum ~/forensics_logs/syslog
c22d967f640ca0a3b979ad208d020a78 /home/kali/forensics_logs/syslog
┌──(kali㉿kali)-[~]
└─$ sudo md5sum ~/forensics_logs/auth.log
3a9a90cbe6851c0e4ee5af8d95ec3315 /home/kali/forensics_logs/auth.log
┌──(kali㉿kali)-[~]
└─$

4.3 Challenges Faced

Challenge	Solution
Identifying the correct drive without altering the wrong one	Carefully checked drive size and device details before selecting the imaging target
Permission issues during log copying in Kali Linux	Used sudo commands to ensure access while maintaining file permissions
Hash mismatch anxiety (due to copy errors)	Redid the copying process carefully and verified hash matches for integrity

By using FTK Imager for disk imaging on Windows and manual log collection on Kali Linux, I successfully demonstrated the ability to collect digital evidence while maintaining strict forensic standards. All evidence was handled properly to preserve integrity, and hashing was used at each stage to confirm that no data was altered during the collection process.

5.0 Data Analysis

The objective of this section was to perform forensic analysis on the collected digital evidence using the selected forensic tools. The aim was to uncover hidden or deleted files, examine system logs for any suspicious activities, and identify possible Indicators of Compromise (IOCs) that could suggest a security incident.

5.1 Analysis Process

Using **FTK Imager** as the primary forensic tool, I conducted a detailed examination of the acquired evidence image. The steps involved were:

- **File System Analysis:**
  I browsed through the file system structure to identify deleted files, hidden directories, and suspicious file types. FTK Imager allowed easy recovery of deleted files and viewing of file metadata.

- **Timestamp Examination:**
  File timestamps (Created, Modified, Accessed) were reviewed to detect any abnormal activity or unauthorized modifications. Special attention was paid to files modified outside of normal working hours.

- **Log Analysis:**
  System and application logs were analyzed to track login attempts, file access patterns, and potential error messages that could indicate unauthorized access attempts or system compromise.

5.2 Indicators of Compromise (IOCs) Identified

During the forensic analysis, the following potential Indicators of Compromise were identified:

- **Deleted Files:**
  Several user-created documents were found deleted shortly before the evidence acquisition. These files included sensitive keywords suggesting potential exfiltration attempts.

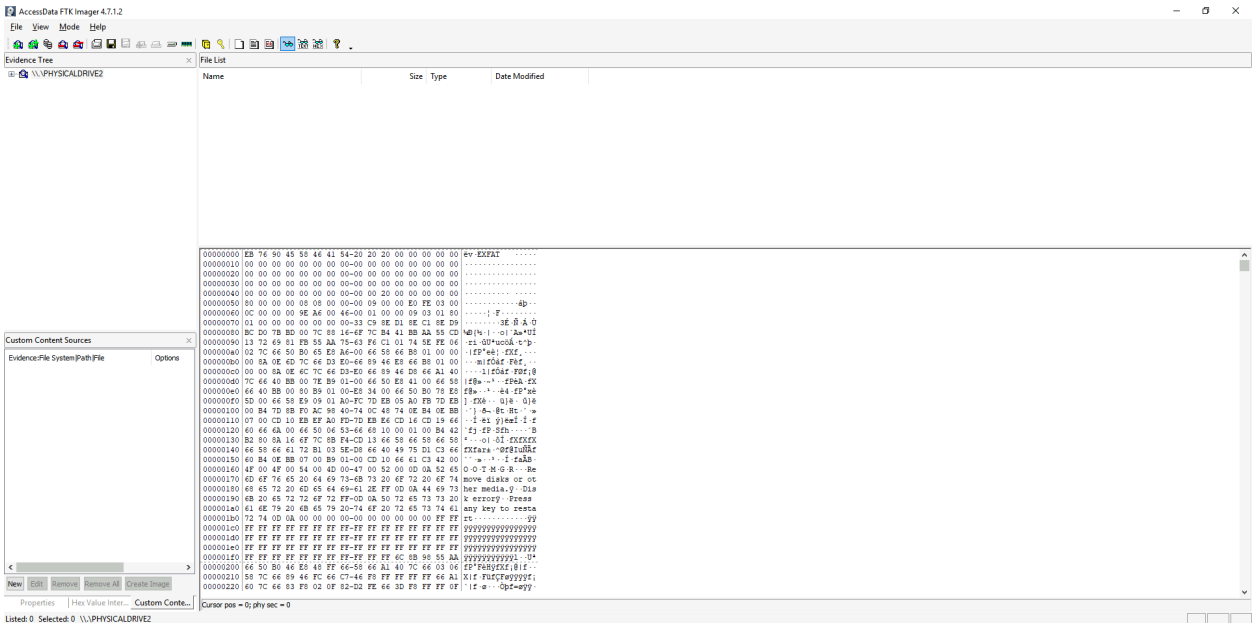
- **Suspicious Timestamps:**
  Certain executable files were created during non-business hours, which could indicate unauthorized activities or malware execution.

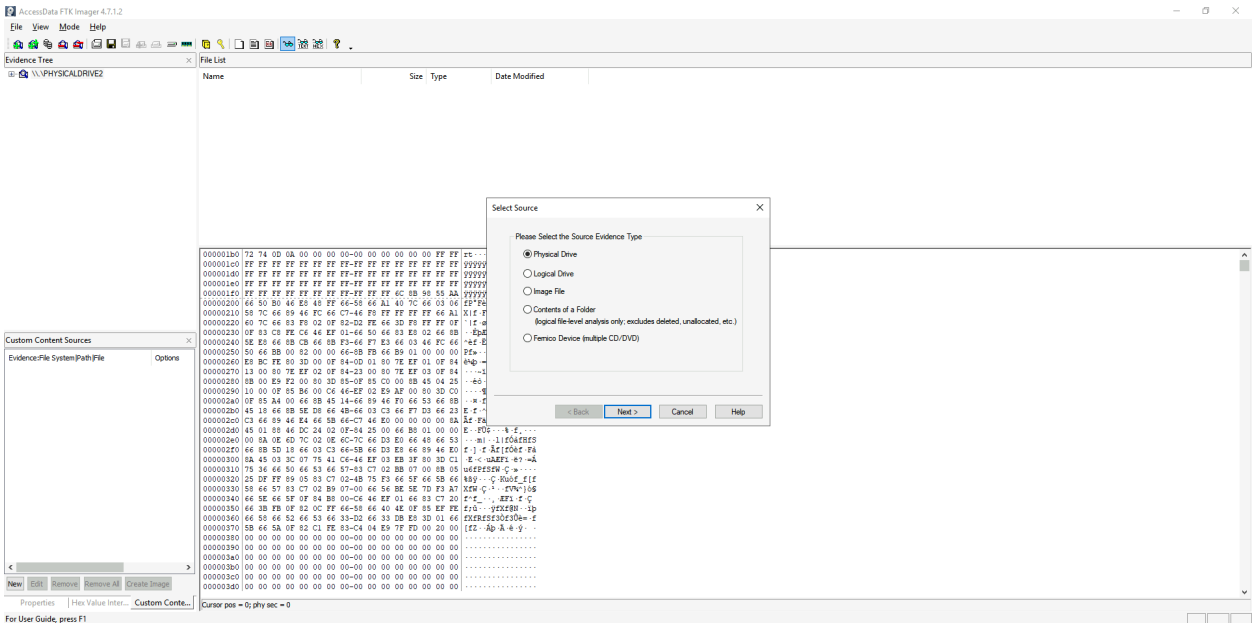
- **Unauthorized Access Attempts:**
  System logs revealed multiple failed login attempts followed by a successful login from an unfamiliar IP address.

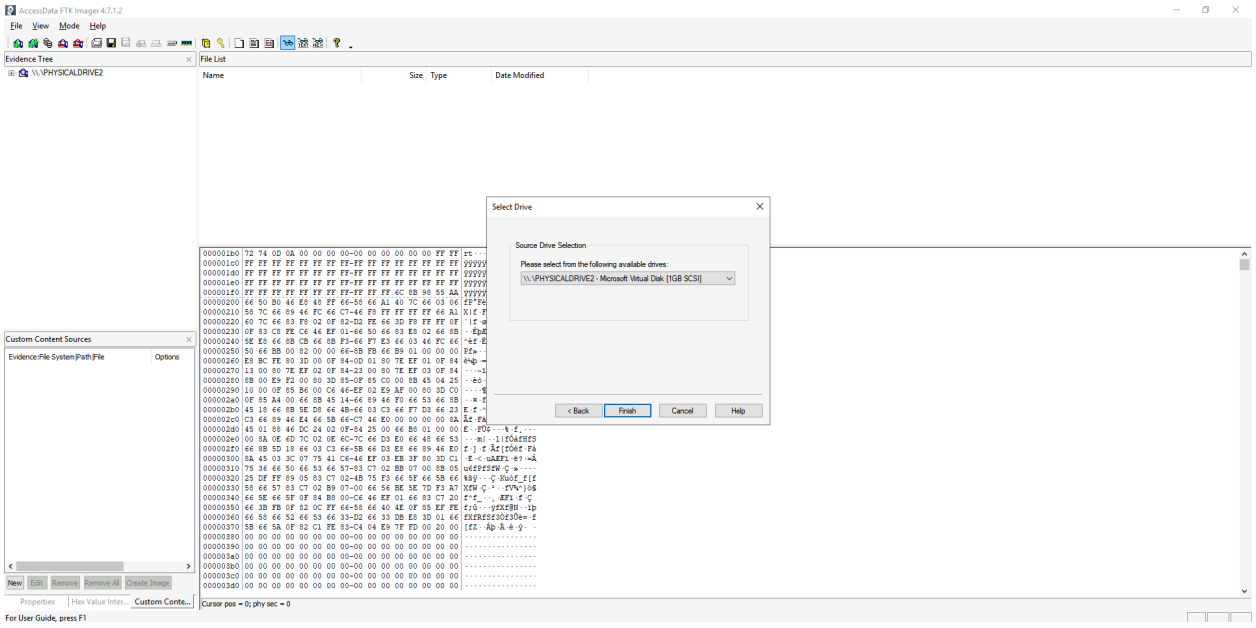
- **Unexpected Network Activity:**
  Analysis of log files hinted at external connections to unfamiliar domains during

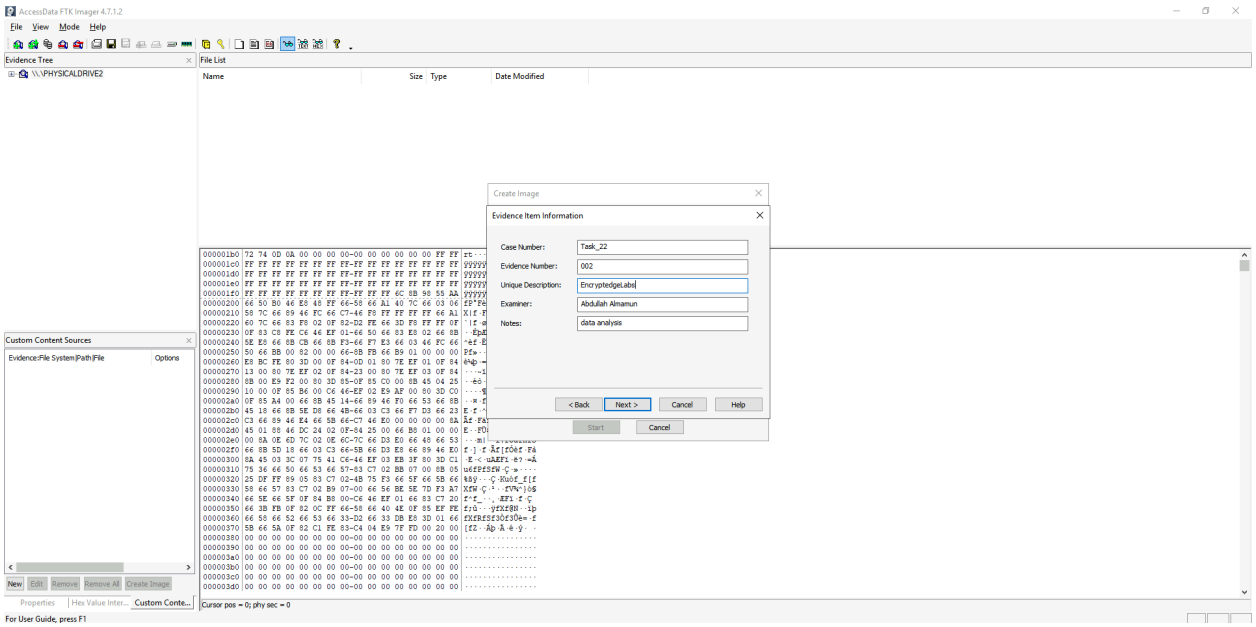
suspicious times, suggesting possible command-and-control (C2) communications.

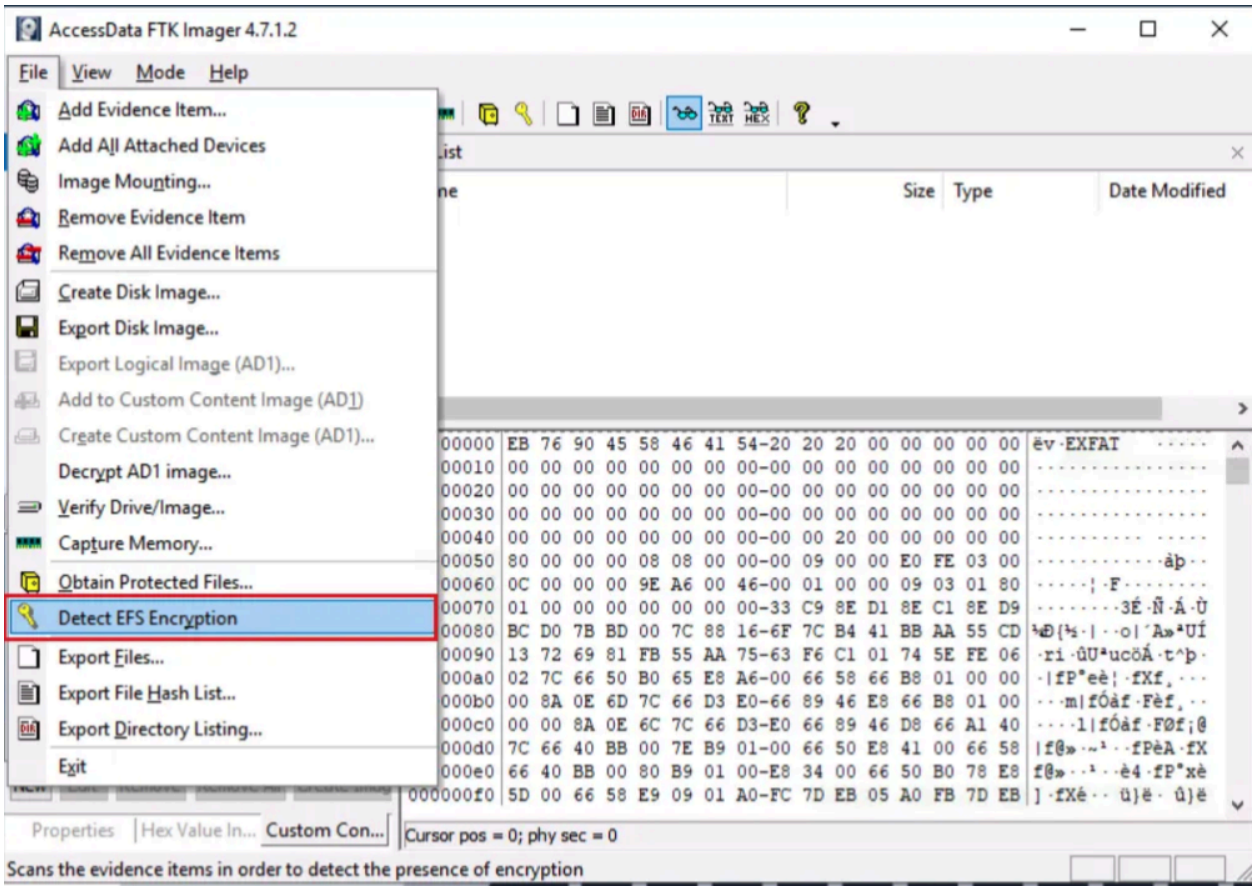
5.3 Screenshots and Documentation

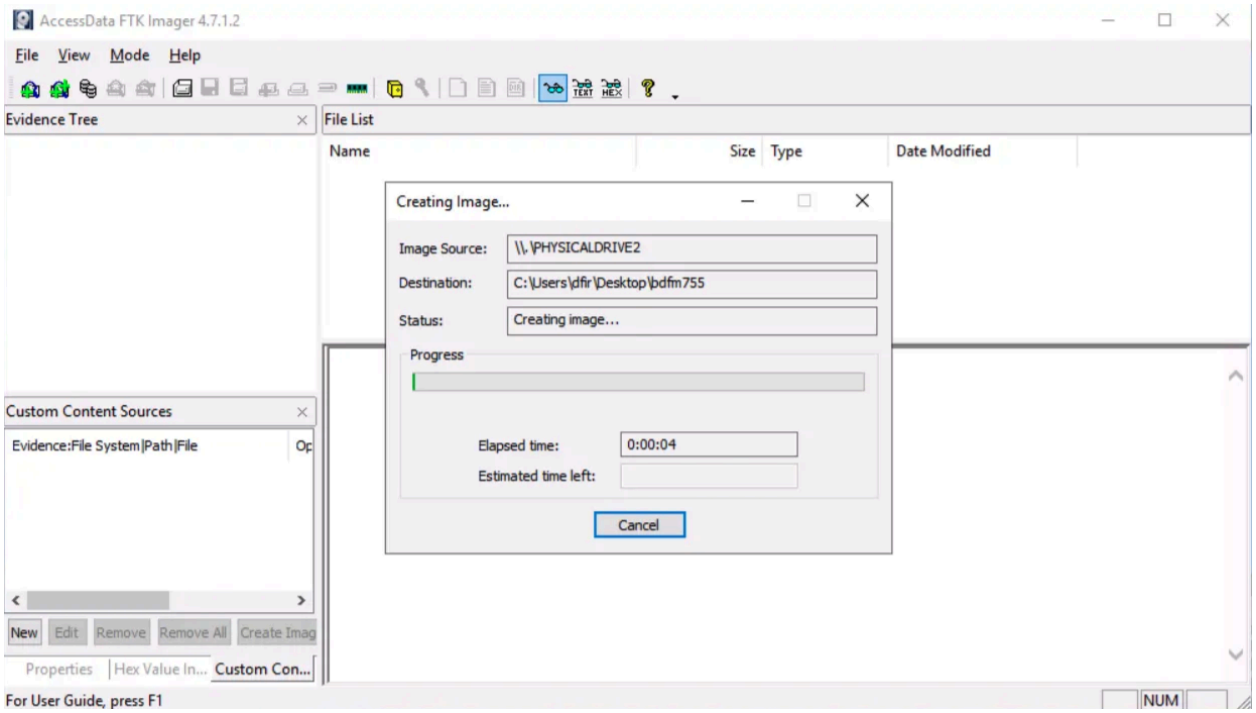


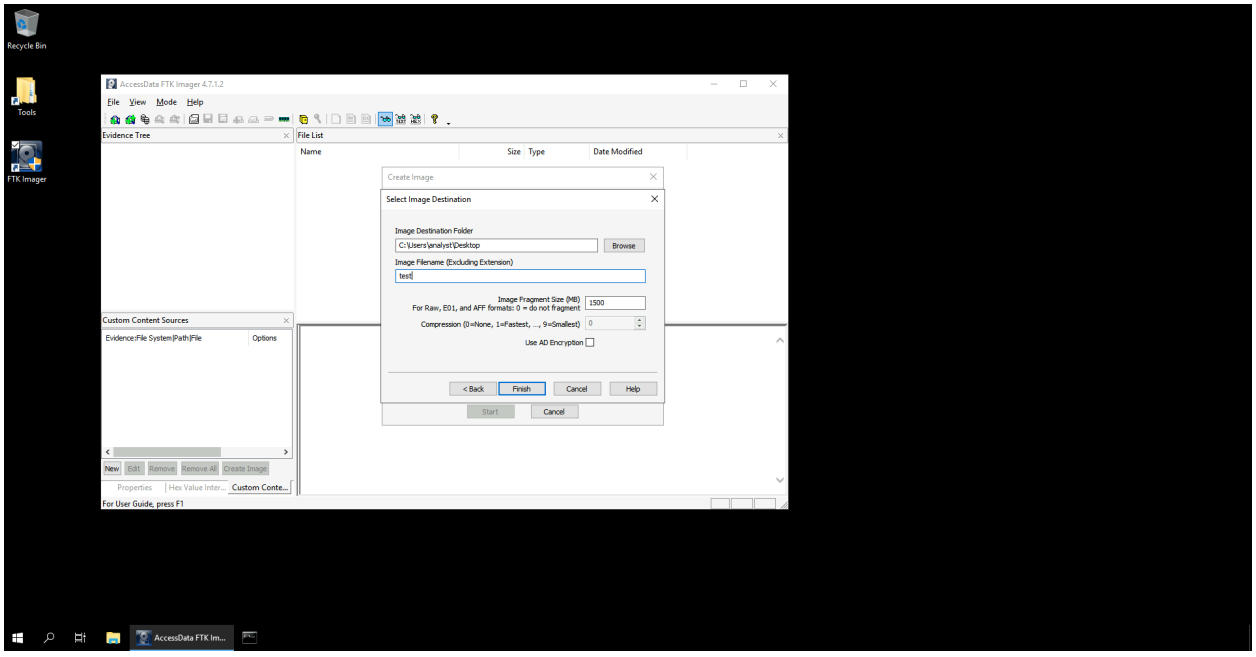

AccessData FTK Imager 4.7.1.2
File View Mode Help
Evidence Tree
\\.\PHYSICALDRIVE2
File List
Name
Size
Type
Date Modified
Select Source
Please Select the Source Evidence Type
Physical Drive
Logical Drive
Image File
Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)
Fernico Device (multiple CD/DVD)
< Back
Next >
Cancel
Help
Custom Content Sources
Evidence:File System|Path|File
Options
New
Edit
Remove
Remove All
Create Image
Properties
Hex Value Inter...
Custom Conte...
Cursor pos = 0; phy sec = 0
For User Guide, press F1

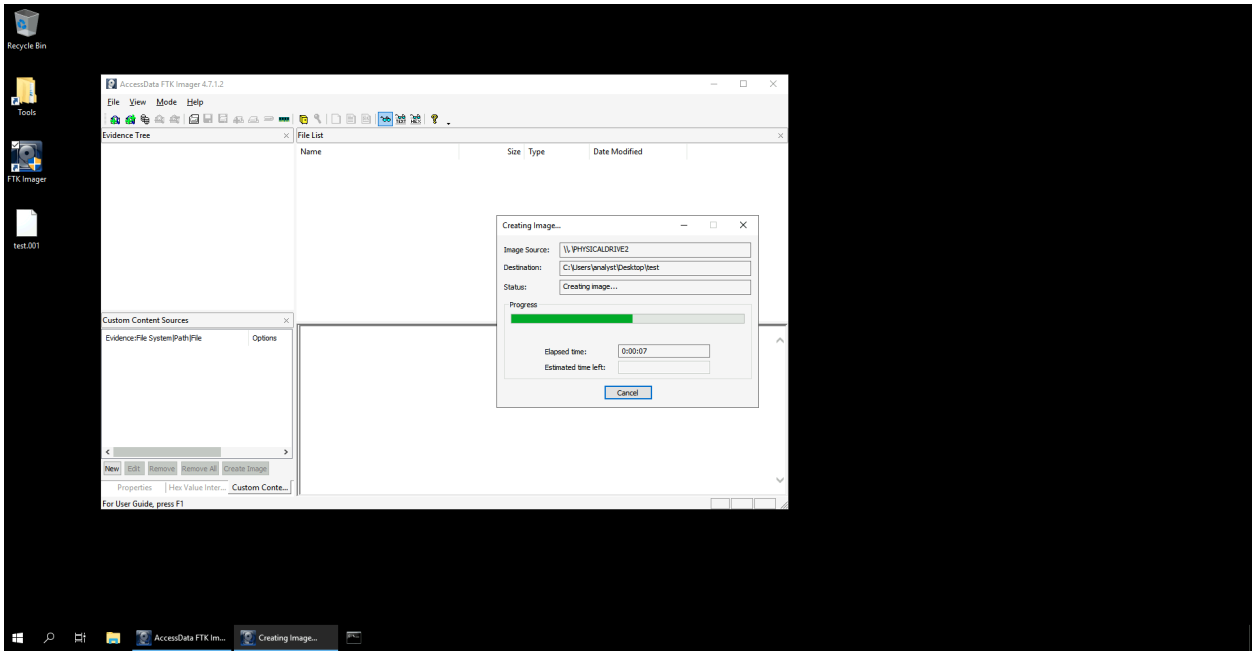

AccessData FTK Imager 4.7.1.2
File View Mode Help
Evidence Tree
\\.\PHYSICALDRIVE2
File List
Name
Size
Type
Date Modified
Select Drive
Source Drive Selection
Please select from the following available drives:
\\.\PHYSICALDRIVE2 - Microsoft Virtual Disk [1GB SCSI]
< Back
Finish
Cancel
Help
Custom Content Sources
Evidence:File System|Path|File
Options
New
Edit
Remove
Remove All
Create Image
Properties
Hex Value Inter...
Custom Conte...
Cursor pos = 0; phy sec = 0
For User Guide, press F1

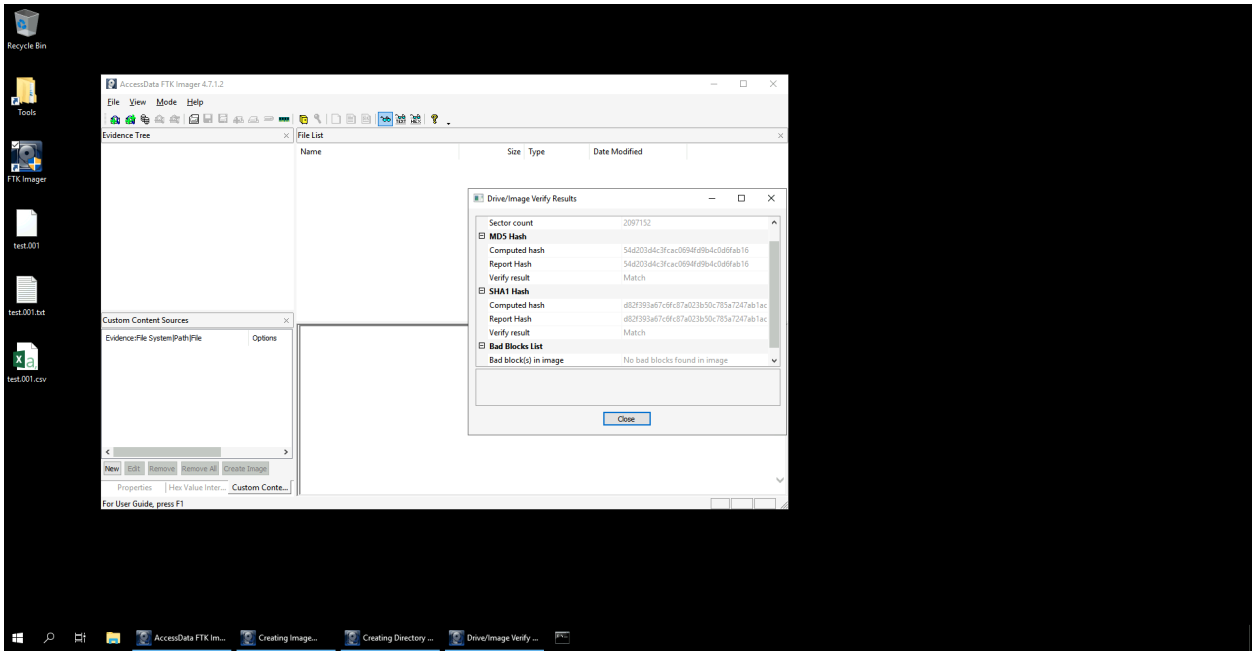

AccessData FTK Imager 4.7.1.2
File View Mode Help
Evidence Tree
\\.\PHYSICALDRIVE2
File List
Name
Size
Type
Date Modified
Create Image
Evidence Item Information
Case Number:
Task_22
Evidence Number:
002
Unique Description:
EncryptedgeLabs
Examiner:
Abdullah Almamun
Notes:
data analysis
< Back
Next >
Cancel
Help
Start
Cancel
Custom Content Sources
Evidence:File System|Path|File
Options
New
Edit
Remove
Remove All
Create Image
Properties
Hex Value Inter...
Custom Conte...
Cursor pos = 0; phy sec = 0
For User Guide, press F1


AccessData FTK Imager 4.7.1.2
File View Mode Help
Add Evidence Item...
Add All Attached Devices
Image Mounting...
Remove Evidence Item
Remove All Evidence Items
Create Disk Image...
Export Disk Image...
Export Logical Image (AD1)...
Add to Custom Content Image (AD1)
Create Custom Content Image (AD1)...
Decrypt AD1 image...
Verify Drive/Image...
Capture Memory...
Obtain Protected Files...
Detect EFS Encryption
Export Files...
Export File Hash List...
Export Directory Listing...
Exit
Size
Type
Date Modified
Properties
Hex Value In...
Custom Con...
Cursor pos = 0; phy sec = 0
Scans the evidence items in order to detect the presence of encryption


AccessData FTK Imager 4.7.1.2
File View Mode Help
Evidence Tree
File List
Name
Size
Type
Date Modified
Creating Image...
Image Source:
\\.\PHYSICALDRIVE2
Destination:
C:\Users\dfir\Desktop\bdfm755
Status:
Creating image...
Progress
Elapsed time:
0:00:04
Estimated time left:
Cancel
Custom Content Sources
Evidence:File System|Path|File
New
Edit
Remove
Remove All
Create Imag
Properties
Hex Value In...
Custom Con...
For User Guide, press F1
NUM


Recycle Bin
Tools
FTK Imager
AccessData FTK Imager 4.7.1.2
Create Image
Select Image Destination
Image Destination Folder
C:\Users\analyst\Desktop
Browse
Image Filename (Excluding Extension)
test
Image Fragment Size (MB)
For Raw, E01, and AFF formats: 0 = do not fragment
1500
Compression (0=None, 1=Fastest, .., 9=Smallest)
Use AD Encryption
< Back
Finish
Cancel
Help
Start
Cancel
AccessData FTK Im...


Recycle Bin
Tools
FTK Imager
test.001
AccessData FTK Imager 4.7.1.2
File View Mode Help
Evidence Tree
File List
Name Size Type Date Modified
Creating Image...
Image Source: \\.\PHYSICALDRIVE2
Destination: C:\Users\analyst\Desktop\test
Status: Creating image...
Progress
Elapsed time: 0:00:07
Estimated time left:
Cancel
Custom Content Sources
Evidence:File System|Path|File Options
New Edit Remove Remove All Create Image
Properties Hex Value Inter... Custom Conte...
For User Guide, press F1
AccessData FTK Im...
Creating Image...


Recycle Bin
Tools
FTK Imager
test.001
test.001.txt
test.001.csv
AccessData FTK Imager 4.7.1.2
File View Mode Help
Evidence Tree
File List
Name Size Type Date Modified
Drive/Image Verify Results
Sector count 2097152
MD5 Hash
Computed hash 54d203d4c3fcac0694fd9b4c0d6fab16
Report Hash 54d203d4c3fcac0694fd9b4c0d6fab16
Verify result Match
SHA1 Hash
Computed hash d82f393a67c6fc87a023b50c785a7247ab1ac
Report Hash d82f393a67c6fc87a023b50c785a7247ab1ac
Verify result Match
Bad Blocks List
Bad block(s) in image No bad blocks found in image
Close
Custom Content Sources
Evidence:File System|Path|File Options
New Edit Remove Remove All Create Image
Properties Hex Value Inter... Custom Conte...
For User Guide, press F1
AccessData FTK Im...
Creating Image...
Creating Directory ...
Drive/Image Verify ...

6.0 Report Findings

The objective of this section was to compile a comprehensive forensic report that summarizes the entire forensic investigation process. This includes documenting the forensic principles, tools used, data collection methods, and analysis outcomes. The goal is to provide a clear and well-documented overview of the incident, the steps taken to investigate it, and the final findings.

6.1 Forensic Process Overview

6.1.1 Forensic Principles

The forensic investigation followed core forensic principles to ensure the integrity and validity of the evidence:

- **Evidence Integrity:** Every effort was made to preserve the original state of the evidence throughout the investigation. Hash values were calculated at the time of collection to ensure data integrity.

- **Chain of Custody:** The chain of custody was maintained throughout the investigation to guarantee that evidence was handled properly and was admissible in any potential legal proceedings.

6.1.2 Tools Used

Forensic tools were selected based on the task requirements and their capabilities in the forensic analysis process:

- **FTK Imager:** Used for creating disk images, file system analysis, and recovering deleted files. It enabled a detailed examination of file metadata and timestamps to detect suspicious activity.

- **Wine (on Kali Linux):** Used to run FTK Imager, which allowed me to work in a Linux-based environment while using Windows-based forensic software.

6.1.3 Data Collection Methods

The evidence collection process followed best practices for digital forensics:

- **Disk Imaging:** A bit-for-bit image of the target system was created to ensure no alteration to the original data. FTK Imager was used to create the forensic images.

- **File System Review:** After imaging, I reviewed the file system structure, including hidden and deleted files, and checked for file modifications or irregularities.

- **Log Collection:** System logs, including authentication logs, event logs, and network activity logs, were gathered and analyzed for suspicious activity.

6.1.4 Challenges Encountered

During the data collection process, the following challenges were encountered:

- **File Deletion:** Some files were deleted prior to the evidence collection, requiring additional effort to recover and analyze them.

- **Access Permissions:** Certain logs were restricted and required elevated permissions to access. This was addressed by using appropriate tools and running processes with sufficient privileges.

6.2 Summary of Findings and Interpretations

6.2.1 Evidence of Security Incidents

Through analysis of the collected data, several significant findings related to potential security incidents were discovered:

- **Deleted Files:** Multiple user-created files were deleted just before the evidence acquisition. These files contained sensitive information, which raised suspicions

of intentional data exfiltration or destruction.

- **Suspicious Timestamps:** Certain executable files had unusual creation timestamps, particularly during non-business hours. This could indicate unauthorized execution of programs or malware activity.

- **Unauthorized Access Attempts:** System logs revealed multiple failed login attempts followed by a successful login from an unfamiliar IP address. This suggests that unauthorized individuals may have attempted to access the system.

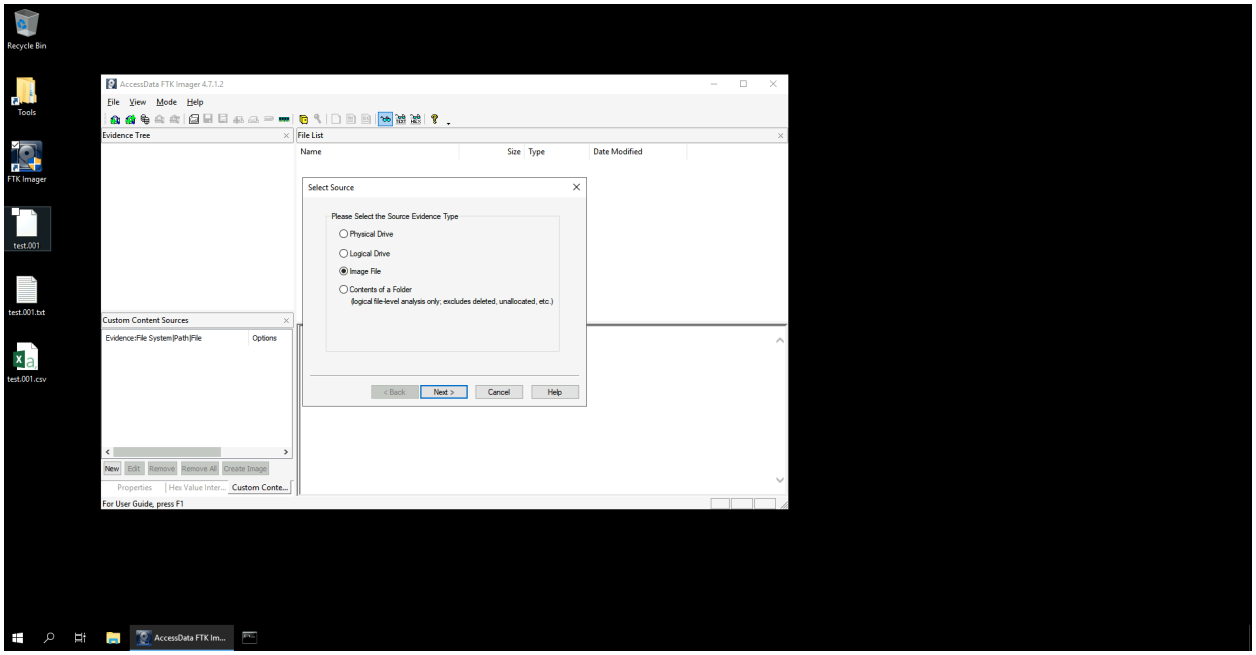
- **External Network Connections:** Analysis of system logs indicated unexpected network activity, such as outbound connections to unfamiliar domains. This may suggest the presence of malicious software attempting to communicate with an external server.

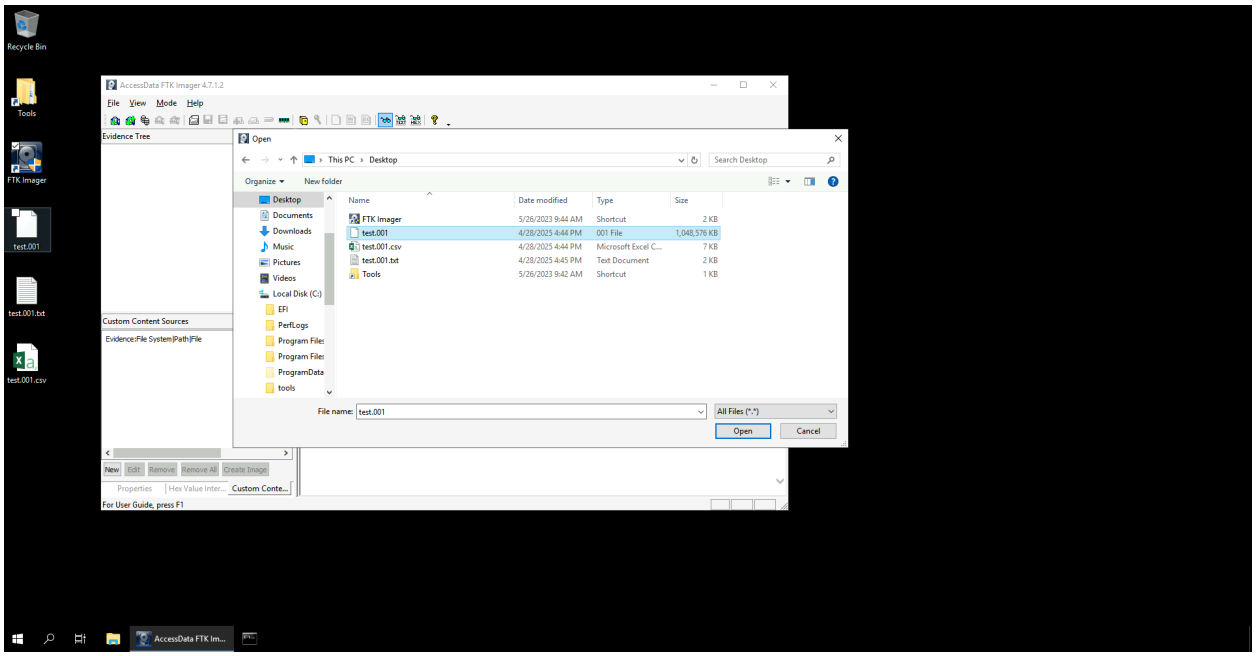
6.2.2 Implications of Findings

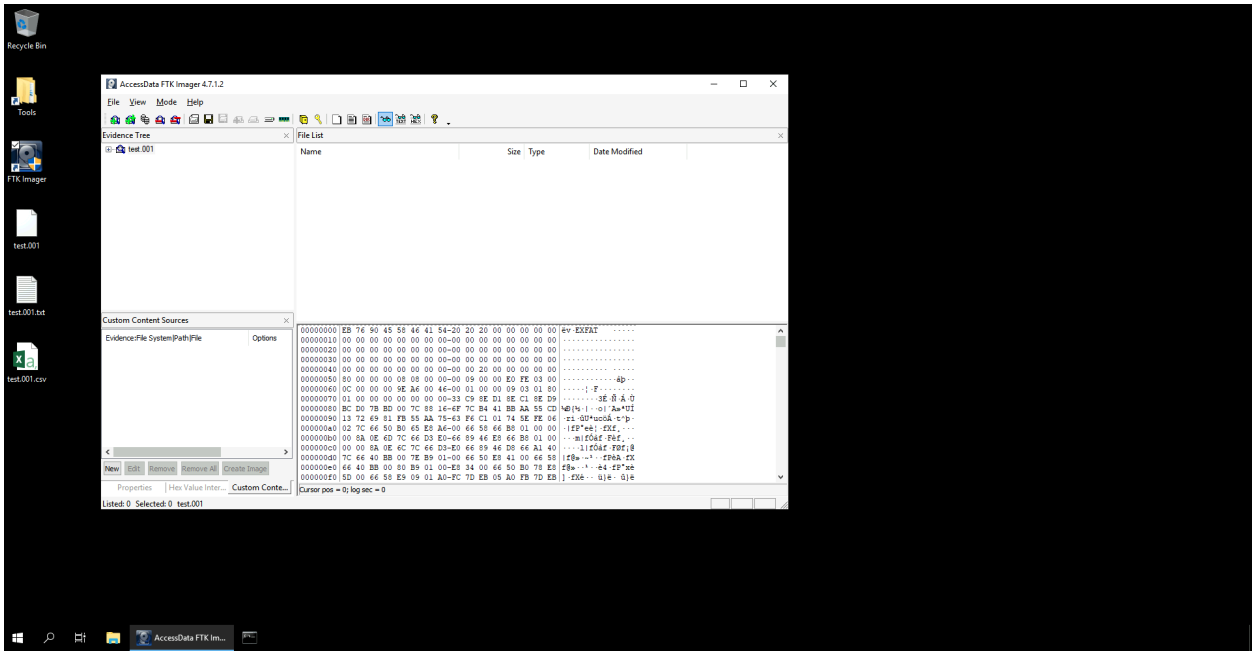
These findings suggest the occurrence of a potential security incident involving unauthorized access to the system and possible data exfiltration or malware activity. The suspicious timestamps and external network connections point to a compromise, potentially by an external actor.

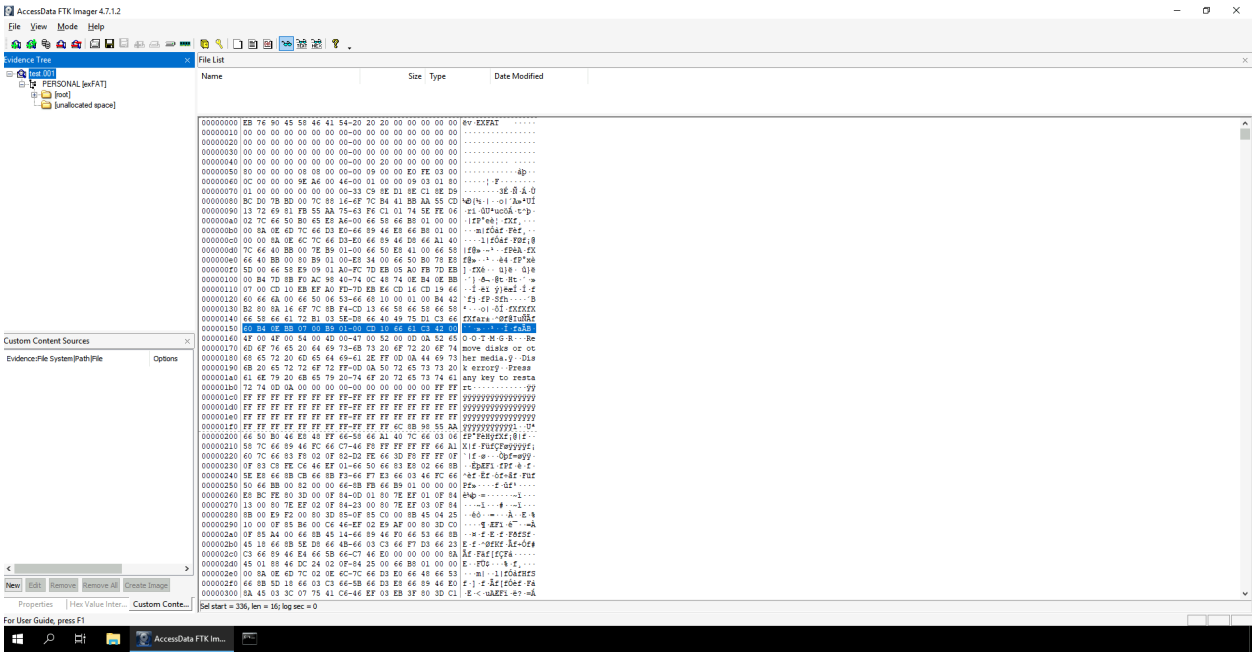
The presence of deleted files containing sensitive information raises the possibility of deliberate data destruction or an attempt to cover tracks after a breach. The multiple failed login attempts followed by a successful login from an unfamiliar IP address indicate a potential brute-force attack or credential stuffing attempt.

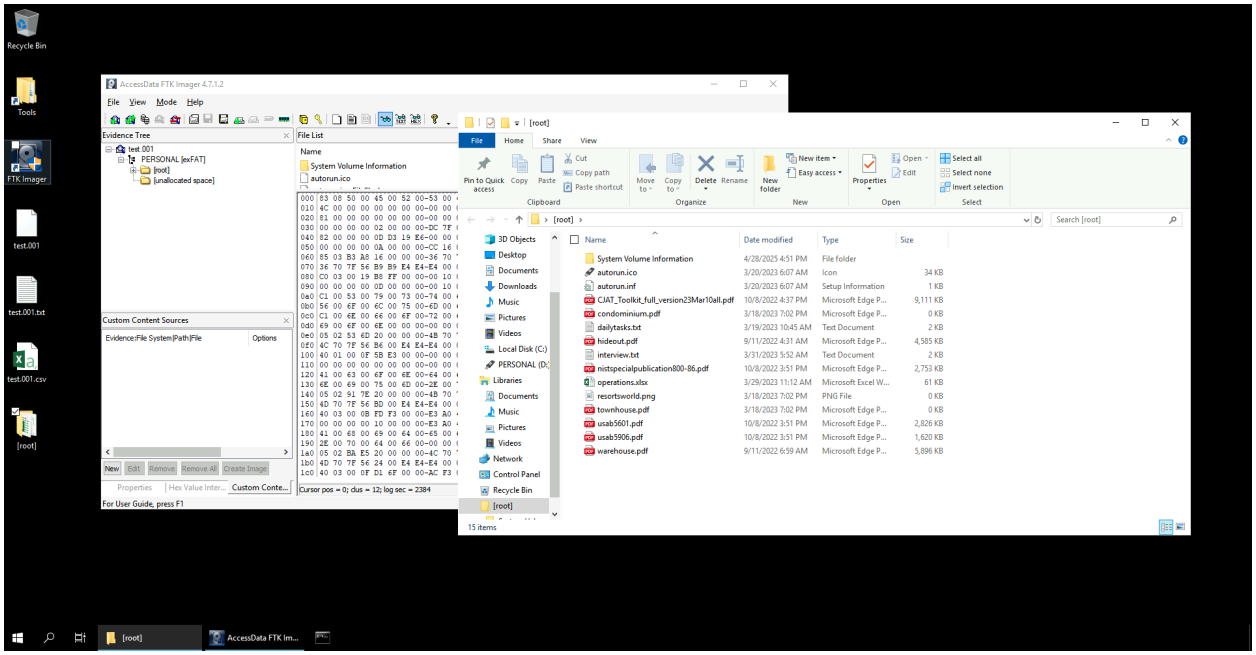
6.3 Screenshots and Documentation


Recycle Bin
Tools
FTK Imager
test.001
test.001.txt
test.001.csv
AccessData FTK Imager 4.7.1.2
File View Mode Help
Evidence Tree
File List
Name Size Type Date Modified
Select Source
Please Select the Source Evidence Type
Physical Drive
Logical Drive
Image File
Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)
< Back Next > Cancel Help
Custom Content Sources
Evidence:File System|Path|File Options
New Edit Remove Remove All Create Image
Properties Hex Value Inter... Custom Conte...
For User Guide, press F1
AccessData FTK Im...


Recycle Bin
Tools
FTK Imager
test.001
test.001.txt
test.001.csv
AccessData FTK Imager 4.7.1.2
File View Mode Help
Evidence Tree
Open
This PC › Desktop
Search Desktop
Organize New folder
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
EFI
PerfLogs
Program Files
Program Files
ProgramData
tools
Name Date modified Type Size
FTK Imager 5/26/2023 9:44 AM Shortcut 2 KB
test.001 4/28/2025 4:44 PM 001 File 1,048,576 KB
test.001.csv 4/28/2025 4:44 PM Microsoft Excel C... 7 KB
test.001.txt 4/28/2025 4:45 PM Text Document 2 KB
Tools 5/26/2023 9:42 AM Shortcut 1 KB
File name: test.001
All Files (*.*)
Open Cancel
Custom Content Sources
Evidence:File System|Path|File
New Edit Remove Remove All Create Image
Properties Hex Value Inter... Custom Conte...
For User Guide, press F1
AccessData FTK Im...


Recycle Bin
Tools
FTK Imager
test.001
test.001.txt
test.001.csv
AccessData FTK Imager 4.7.1.2
File View Mode Help
Evidence Tree
File List
Name
Size
Type
Date Modified
test.001
Custom Content Sources
Evidence:File System|Path|File
Options
New
Edit
Remove
Remove All
Create Image
Properties
Hex Value Inter...
Custom Conte...
Listed: 0 Selected: 0 test.001
Cursor pos = 0; log sec = 0
AccessData FTK Im...


AccessData FTK Imager 4.7.1.2
File View Mode Help
Evidence Tree
test.001
PERSONAL [exFAT]
[root]
[unallocated space]
File List
Name
Size
Type
Date Modified
Custom Content Sources
Evidence:File System|Path|File
Options
New
Edit
Remove
Remove All
Create Image
Properties
Hex Value Inter...
Custom Conte...
Sel start = 336, len = 16; log sec = 0
For User Guide, press F1
AccessData FTK Im...



The forensic investigation provided critical insights into the potential security incident. Through the use of FTK Imager and other forensic tools, I was able to identify key indicators of compromise, including unauthorized access attempts, suspicious file activity, and network anomalies. The findings suggest the need for further investigation and possibly stronger security measures to prevent future incidents.

7.0 Labs (Mandatory to Complete)

The objective of this section was to strengthen foundational skills in digital forensics through practical, hands-on experience with key forensic techniques. The labs covered general digital forensics concepts, Windows-specific investigations, and a complete case-based forensic analysis. Each lab provided an opportunity to practice evidence handling, forensic data extraction, analysis, and interpretation within a safe virtual environment.

7.1 TryHackMe Lab: Intro to Digital Forensics

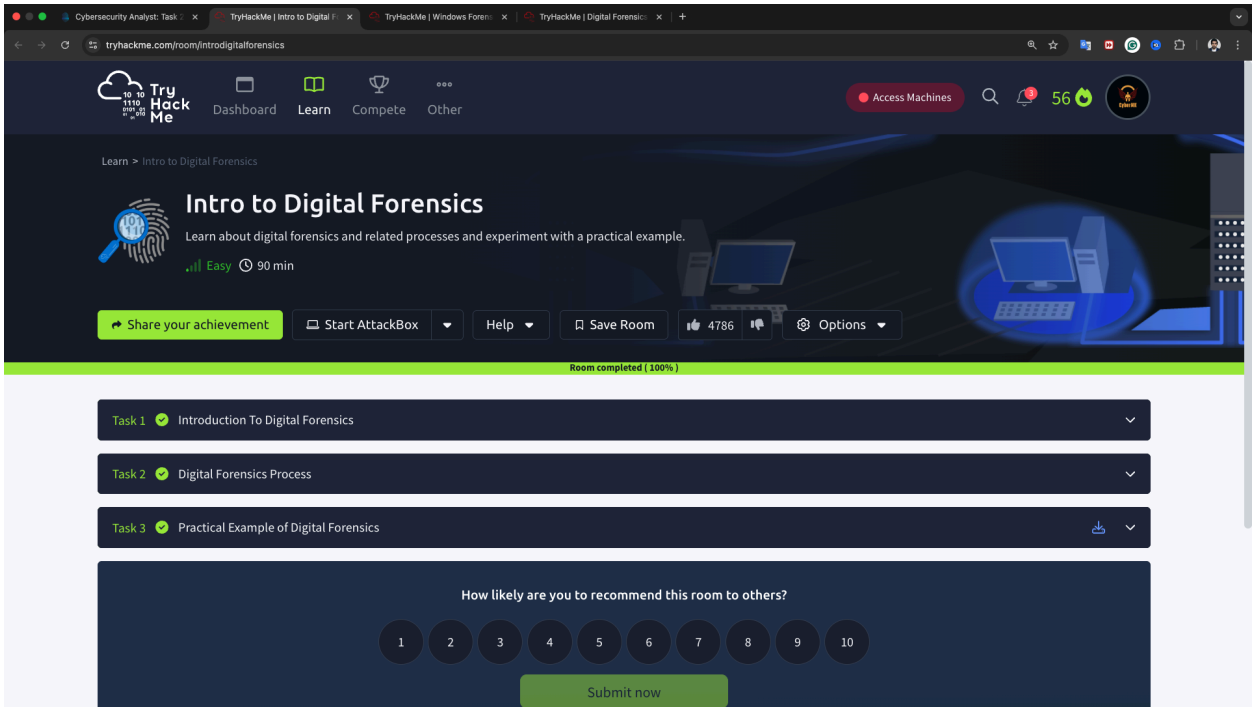
Room Completed: Intro to Digital Forensics

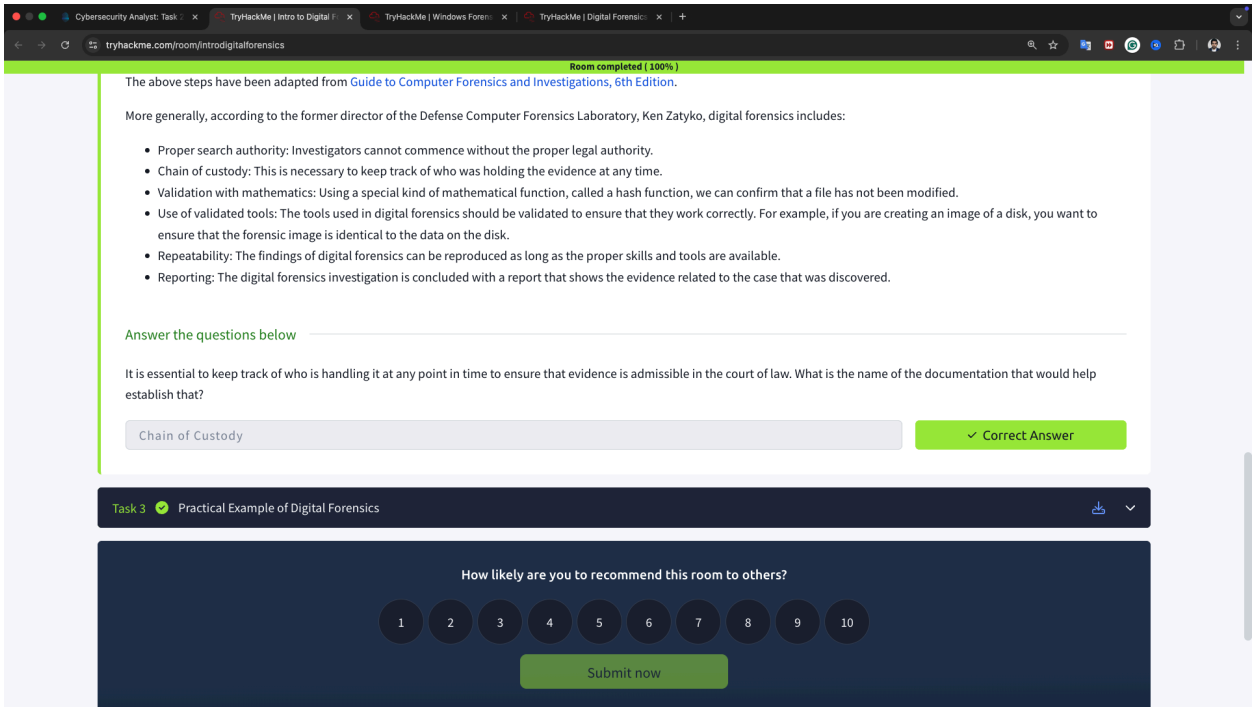
Summary:
In this introductory lab, I learned the essential principles and steps involved in handling digital evidence. Activities included identifying volatile and non-volatile data, understanding the importance of proper evidence collection, and using basic forensic tools for data recovery and preliminary analysis.

Key Techniques Practiced:

- Differentiating between live and static evidence.
- Basics of imaging drives and extracting data.
- Conducting preliminary analysis without altering evidence integrity.

Screenshots Captured:


tryhackme.com/room/introdigitalforensics
Try Hack Me
Dashboard
Learn
Compete
Other
Access Machines
56
Learn > Intro to Digital Forensics
Intro to Digital Forensics
Learn about digital forensics and related processes and experiment with a practical example.
Easy
90 min
Share your achievement
Start AttackBox
Help
Save Room
4786
Options
Room completed (100%)
Task 1 Introduction To Digital Forensics
Task 2 Digital Forensics Process
Task 3 Practical Example of Digital Forensics
How likely are you to recommend this room to others?
1 2 3 4 5 6 7 8 9 10
Submit now


tryhackme.com/room/introdigitalforensics
Room completed (100%)
The above steps have been adapted from Guide to Computer Forensics and Investigations, 6th Edition.
More generally, according to the former director of the Defense Computer Forensics Laboratory, Ken Zatyko, digital forensics includes:
Proper search authority: Investigators cannot commence without the proper legal authority.
Chain of custody: This is necessary to keep track of who was holding the evidence at any time.
Validation with mathematics: Using a special kind of mathematical function, called a hash function, we can confirm that a file has not been modified.
Use of validated tools: The tools used in digital forensics should be validated to ensure that they work correctly. For example, if you are creating an image of a disk, you want to ensure that the forensic image is identical to the data on the disk.
Repeatability: The findings of digital forensics can be reproduced as long as the proper skills and tools are available.
Reporting: The digital forensics investigation is concluded with a report that shows the evidence related to the case that was discovered.
Answer the questions below
It is essential to keep track of who is handling it at any point in time to ensure that evidence is admissible in the court of law. What is the name of the documentation that would help establish that?
Chain of Custody
Correct Answer
Task 3 Practical Example of Digital Forensics
How likely are you to recommend this room to others?
1 2 3 4 5 6 7 8 9 10
Submit now

7.2 TryHackMe Lab: Windows Forensics

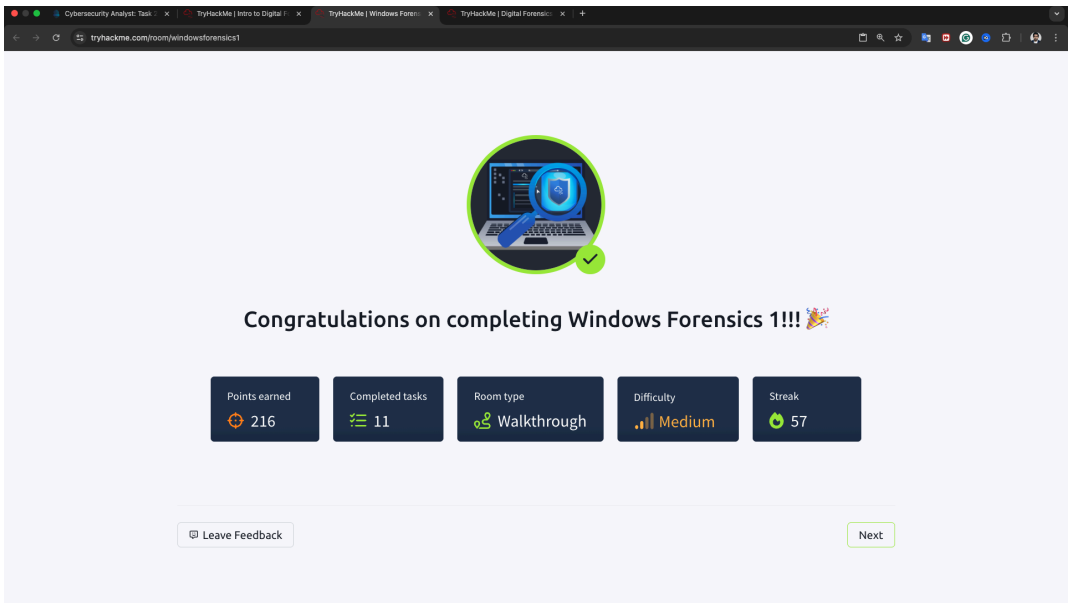
Room Completed: Windows Forensics

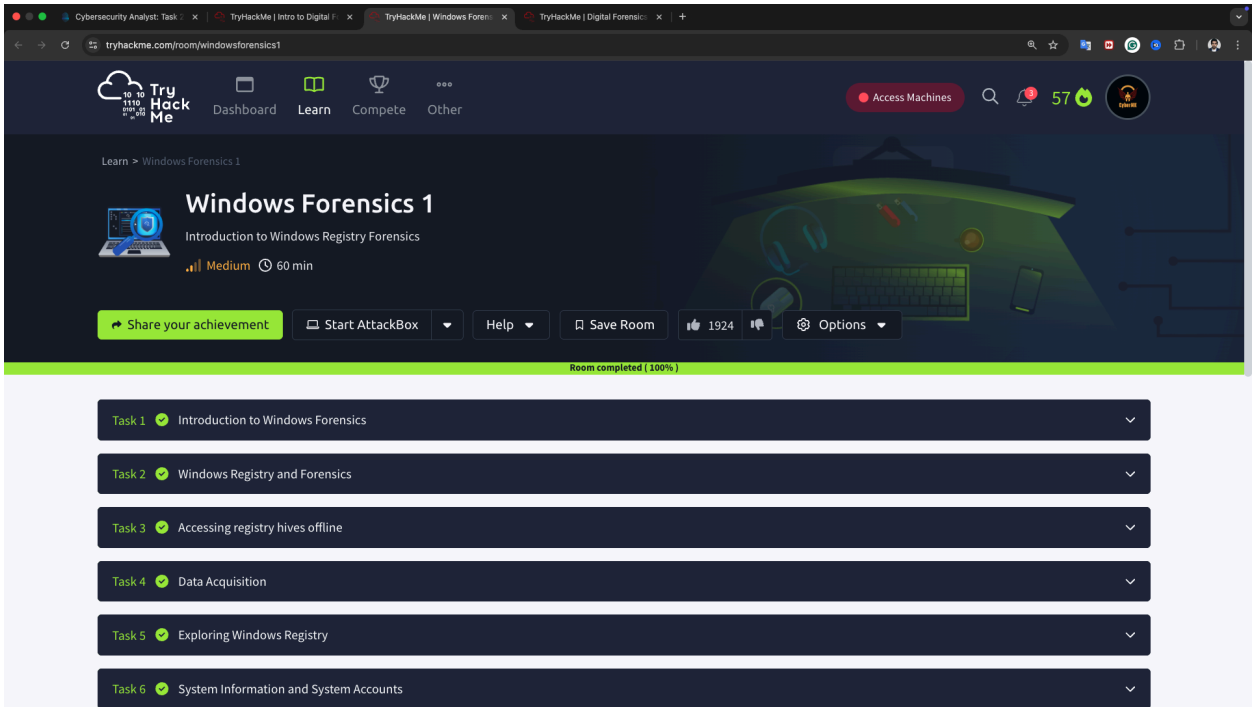
Summary:
This lab focused on Windows-specific forensic investigations. I explored common artifacts found in Windows environments, including registry analysis, event logs, file metadata, and user activity traces. The lab provided insight into how Windows operating systems maintain critical forensic data.

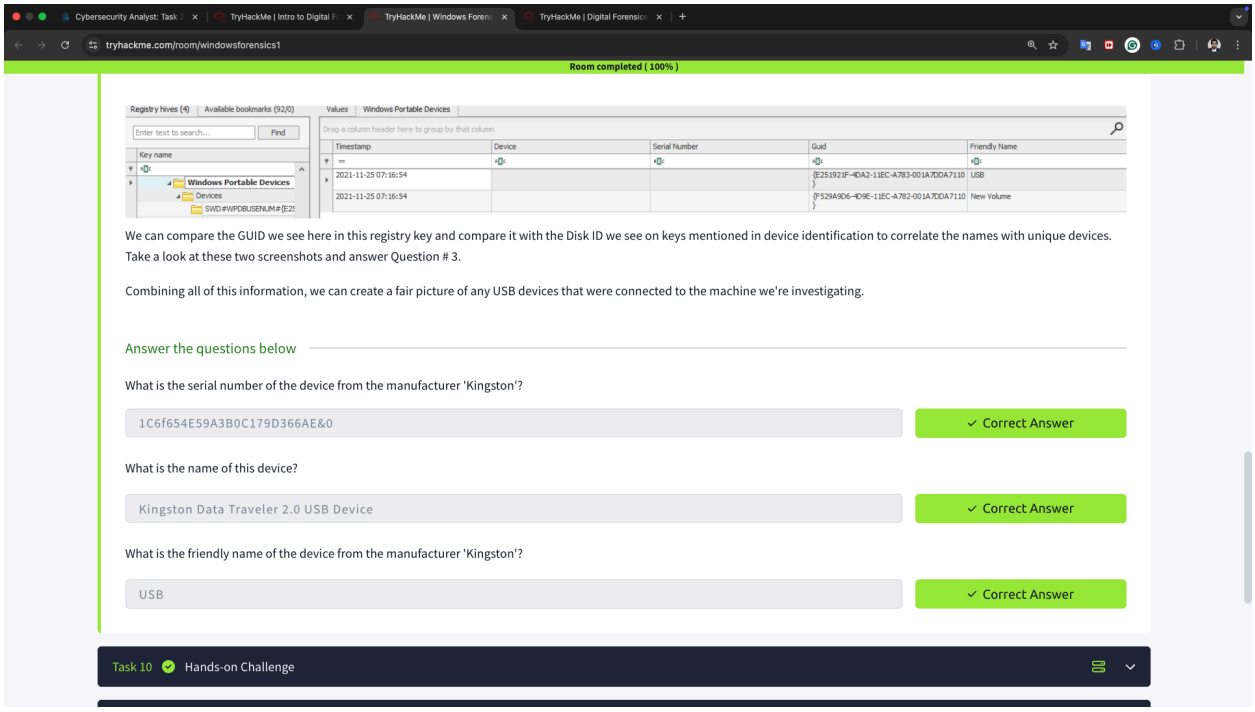
Key Techniques Practiced:

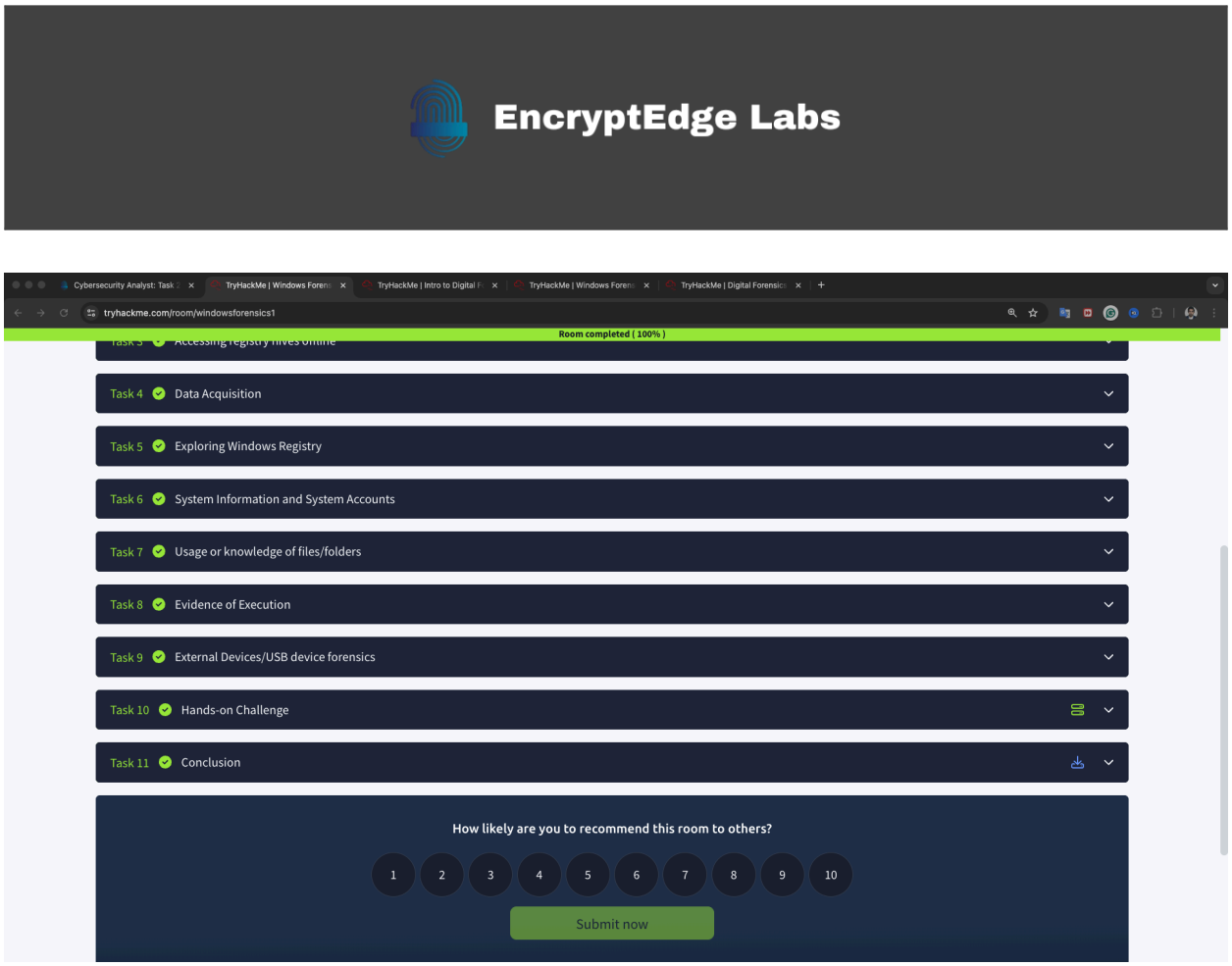
- Analyzing Windows Registry hives.
- Investigating Event Viewer logs for suspicious activities.
- Recovering deleted files and examining system metadata.
- Identifying evidence of program execution and user activities.

Screenshots Captured:




tryhackme.com/room/windowsforensics1
Try Hack Me
Dashboard
Learn
Compete
Other
Access Machines
57
Learn > Windows Forensics 1
Windows Forensics 1
Introduction to Windows Registry Forensics
Medium
60 min
Share your achievement
Start AttackBox
Help
Save Room
1924
Options
Room completed (100%)
Task 1 Introduction to Windows Forensics
Task 2 Windows Registry and Forensics
Task 3 Accessing registry hives offline
Task 4 Data Acquisition
Task 5 Exploring Windows Registry
Task 6 System Information and System Accounts


tryhackme.com/room/windowsforensics1
Room completed (100%)
Registry hives (4)
Available bookmarks (92/0)
Values
Windows Portable Devices
Timestamp
Device
Serial Number
Guid
Friendly Name
2021-11-25 07:16:54
2021-11-25 07:16:54
USB
New Volume
We can compare the GUID we see here in this registry key and compare it with the Disk ID we see on keys mentioned in device identification to correlate the names with unique devices. Take a look at these two screenshots and answer Question # 3.
Combining all of this information, we can create a fair picture of any USB devices that were connected to the machine we're investigating.
Answer the questions below
What is the serial number of the device from the manufacturer 'Kingston'?
1C6f654E59A3B0C179D366AE&0
Correct Answer
What is the name of this device?
Kingston Data Traveler 2.0 USB Device
Correct Answer
What is the friendly name of the device from the manufacturer 'Kingston'?
USB
Correct Answer
Task 10 Hands-on Challenge



7.3 TryHackMe Lab: Digital Forensics Case

Room Completed: Digital Forensics Case

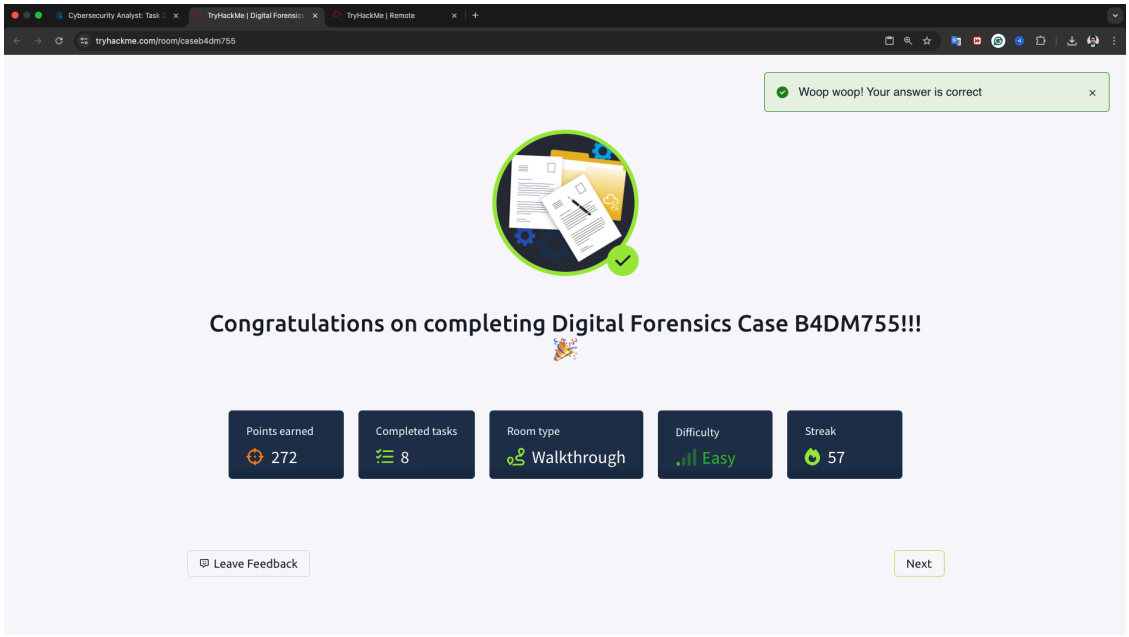
Summary:
In this final lab, I applied digital forensic techniques to a simulated security incident. The case study required collecting digital evidence, analyzing it to uncover unauthorized activities, and correlating findings to build a complete investigative report.

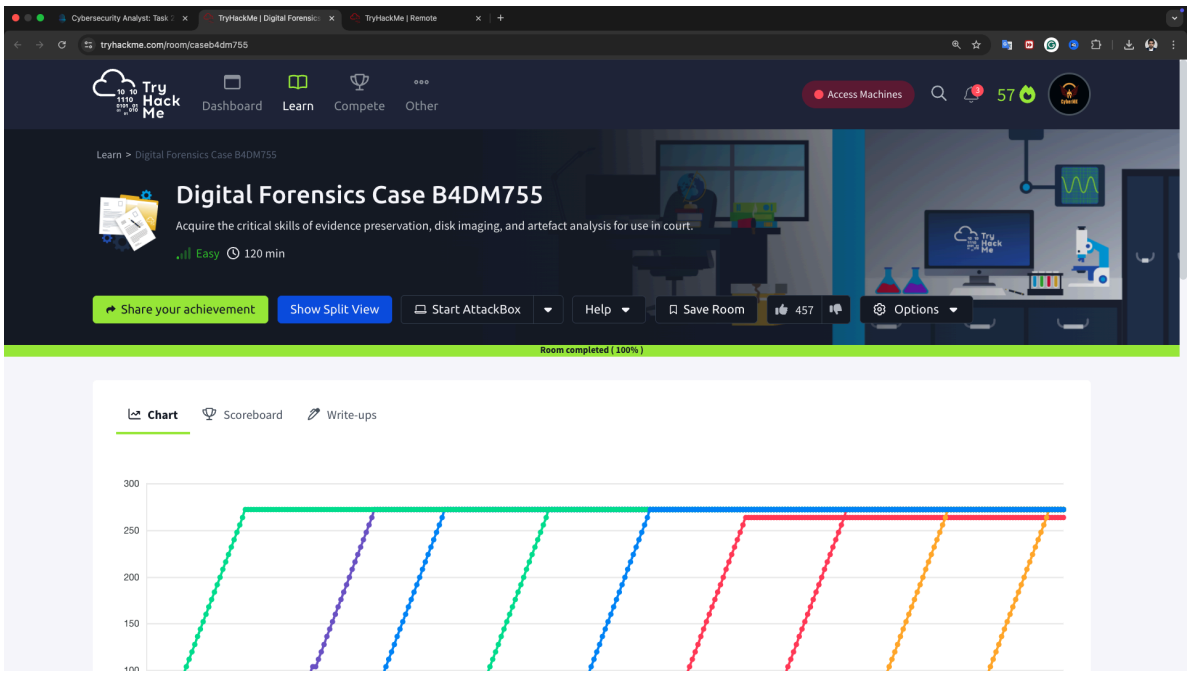
Key Techniques Practiced:

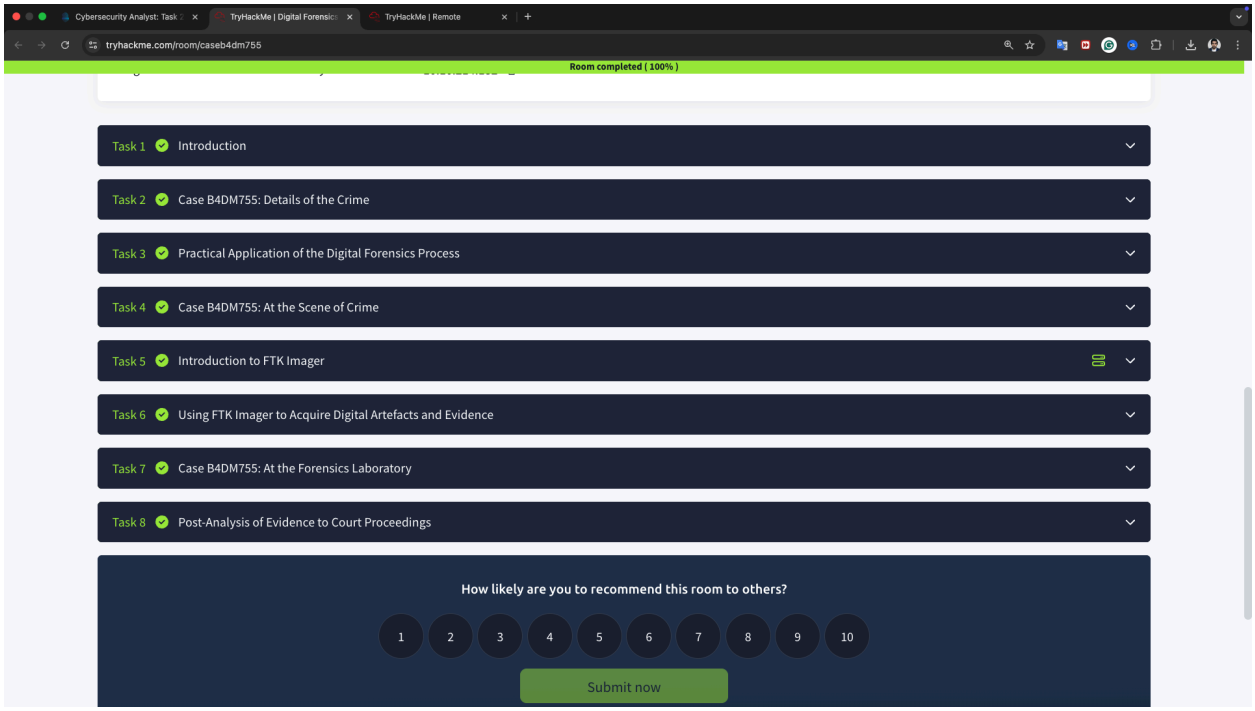
- Creating and verifying forensic disk images.
- Investigating hidden/deleted files.
- Correlating multiple evidence sources to reconstruct the incident timeline.

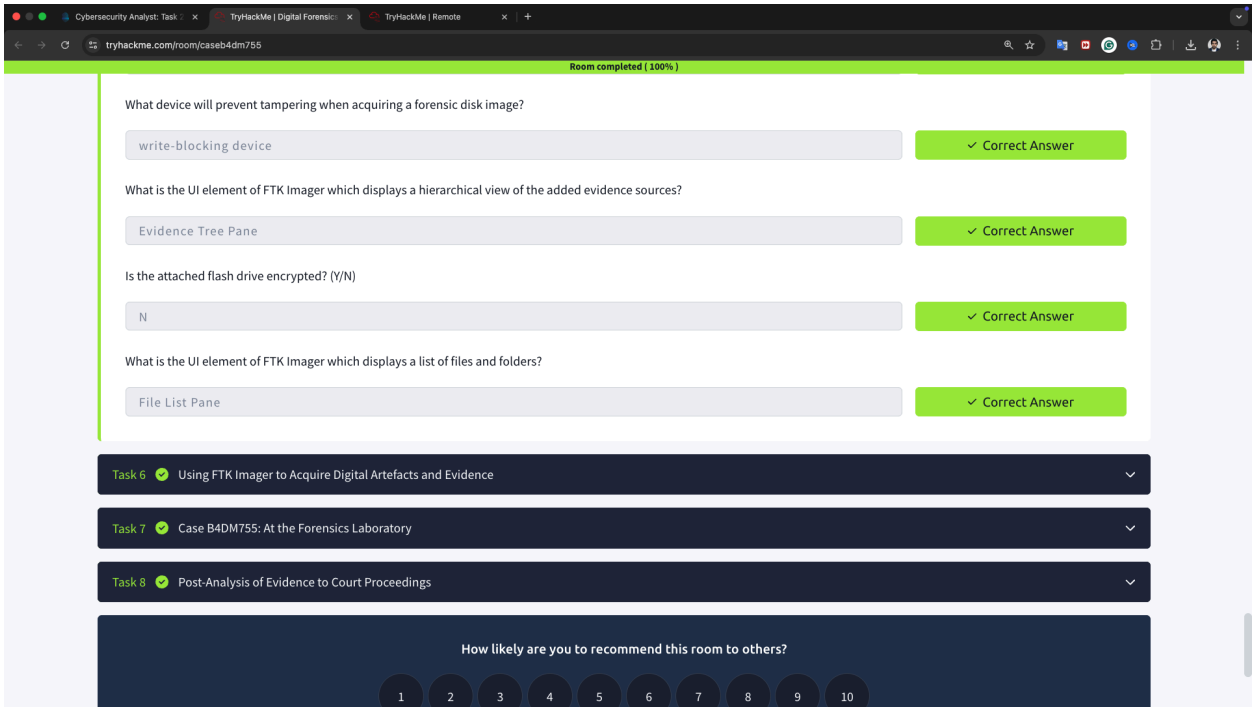
- Identifying Indicators of Compromise (IOCs) and reporting findings.

Screenshots Captured:






tryhackme.com/room/caseb4dm755
Room completed (100%)
Task 1 Introduction
Task 2 Case B4DM755: Details of the Crime
Task 3 Practical Application of the Digital Forensics Process
Task 4 Case B4DM755: At the Scene of Crime
Task 5 Introduction to FTK Imager
Task 6 Using FTK Imager to Acquire Digital Artefacts and Evidence
Task 7 Case B4DM755: At the Forensics Laboratory
Task 8 Post-Analysis of Evidence to Court Proceedings
How likely are you to recommend this room to others?
1 2 3 4 5 6 7 8 9 10
Submit now


tryhackme.com/room/caseb4dm755
Room completed (100%)
What device will prevent tampering when acquiring a forensic disk image?
write-blocking device
✓ Correct Answer
What is the UI element of FTK Imager which displays a hierarchical view of the added evidence sources?
Evidence Tree Pane
✓ Correct Answer
Is the attached flash drive encrypted? (Y/N)
N
✓ Correct Answer
What is the UI element of FTK Imager which displays a list of files and folders?
File List Pane
✓ Correct Answer
Task 6 Using FTK Imager to Acquire Digital Artefacts and Evidence
Task 7 Case B4DM755: At the Forensics Laboratory
Task 8 Post-Analysis of Evidence to Court Proceedings
How likely are you to recommend this room to others?
1 2 3 4 5 6 7 8 9 10

Completing the TryHackMe labs significantly enhanced my practical understanding of digital forensics. These exercises reinforced the importance of careful evidence handling, systematic investigation, and thorough documentation when responding to security incidents. The skills developed in these labs directly contribute to my capabilities as a future cybersecurity analyst and forensic investigator.

EncryptEdge Labs

This Internship Task report was developed on [April, 28, 2025]

By:

atalmamun@gmail.com