# Industry Project Report

## On

# Forensic Analysis of Digital Devices

**Developed By: -**

Atharva Deshpande (21162171003)

**Guided By:-**

Prof. Tejas Kadiya (Internal)

Ms. Janvi Sharma (External)

## Submitted to
## Faculty of Engineering and Technology
## Institute of Computer Technology
## Ganpat University

**Year - 2025**

Ganpat University

॥ विद्या समाजोत्कर्षः ॥

Institute of Computer Technology

# CERTIFICATE

This is to attest that the **Industry** Project work entitled **“Forensic Analysis of Digital Devices”** by Atharva Deshpande (Enrolment No.21162171003 of Ganpat University, towards the partial fulfillment of requirements of the degree of Bachelor of Technology – Computer Science and Engineering, carried out by him in the CSE(CS) Department at Heritage Cyber world LLP. No University or Institute has accepted the outcomes or findings of this project in whole or in part for the fulfillment of any degree or diploma.

Name & Sign. of Internal Guide

Name & Sign. of Head

**Place: ICT - GUNI**

**Date: May 09 2025**

# ACKNOWLEDGEMENT

An excellent opportunity for education and personal growth is the Industry Internship project. Having so many amazing people guide me through the completion of this endeavour makes me feel really fortunate and humbled. First and foremost, I would like to thank Dr. Rohit Patel, Principal, ICT, and Prof. Dharmesh Darji, Head, ICT who gave us an opportunity to undertake this project. Despite their extremely hectic academic schedules, Prof. Tejas Kadiya and Ms. Janvi Sharma (Internal & External Guides) took the time to listen to us, offer advice, and steer us in the right direction during our project work on Digital Forensic Analysis of Evidences. Without his or her assistance, we are unsure of where we might have ended up. The CSE department organized all the facilities to make living easy and kept an eye on our development. We would want to use this opportunity to express our gratitude for their generosity.

**ATHARVA DESHPANDE (Enrollment No:21162171003)**

# ABSTRACT

The widespread adoption of computers, smartphones, and other connected technologies in today's advanced society has introduced both unprecedented opportunities and challenging issues. The rapid expansion of digital platforms and mobile apps has heightened the chances of cyberattacks, data breaches, and privacy infringements. To effectively address these problems, there is an increasing need for skilled professionals with education in digital forensics.

The purpose of Forensic Analysis of Digital Devices is to provide individuals with the knowledge and practical skills necessary to investigate and assess digital evidence. For legal and investigative purposes, this entails the systematic examination of digital devices such as computers, tablets, and smartphones to retrieve, analyze and preserve crucial information. Through this Internship, I acquired skills in utilizing forensic methods and instruments to learn about cybercrime evidence, detect anomalies, and reconstruct events. In today’s world, this knowledge is essential for supporting cybersecurity efforts, law enforcement actions, and judicial processes.

# INDEX

**Title** **PageNo**

# CHAPTER: 1 INTRODUCTION

# CHAPTER 1 INTRODUCTION

The growing reliance on computers, smartphones, and interconnected technologies in modern society has brought about both transformative benefits and significant security concerns. With the rapid rise of digital platforms and mobile applications, the threat landscape has expanded, increasing the frequency and complexity of cyberattacks, data breaches, and privacy violations. Addressing these challenges requires trained professionals equipped with specialized knowledge in digital forensics.

This Internship empowered me with both theoretical understanding and hands-on experience in analyzing digital evidence. The training focused on the structured examination of digital devices—including computers, tablets, and smartphones—to extract, interpret, and securely preserve critical data for investigative and legal purposes. It provides a solid foundation in the core principles of digital forensics, including chain of custody, data recovery, and evidence handling.

I gained proficiency in advanced forensic tools and techniques to uncover traces of cybercrime, detect anomalies, and reconstruct digital events. These skills are essential for supporting cybersecurity operations, assisting law enforcement agencies, and contributing to judicial proceedings. In an era where digital threats continue to evolve, Forensic Analysis of Digital Devices plays a vital role in preparing professionals to respond effectively and ethically.

# CHAPTER: 2 PROJECT SCOPE

# CHAPTER 2 PROJECT SCOPE

The scope of project includes investigating cybercrimes, recovering lost or deleted data, identifying security vulnerabilities, and analyzing digital evidence to support legal and investigative processes. It also extends to developing predictive models for assessing risks and enhancing the security of digital ecosystems.

# CHAPTER: 3 SOFTWARE AND HARDWARE REQUIREMENTS

# CHAPTER 3 SOFTWARE AND HARDWARE REQUIREMENTS

## Minimum Hardware Requirements

| | |
|---|---|
| **Processor** | 2.0 GHz |
| **RAM** | 8GB |
| **HDD** | 40GB |

*Table 3.1 Minimum Hardware Requirements*

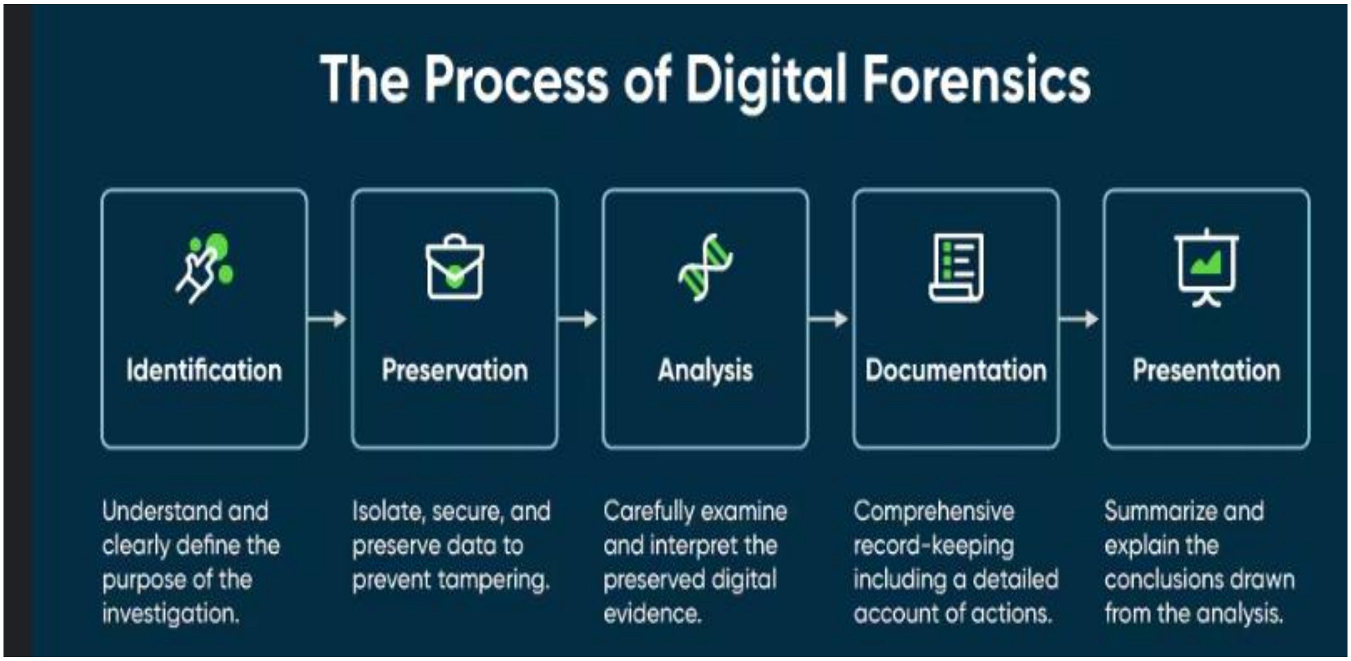
## Minimum Software Requirements

| | |
|---|---|
| **Operating System** | Any operating system which can support an internet browser. |
| **Programming language** | - |
| **Other tools & tech** | FTK Imager, Autopsy, Encase and Wireshark |

*Table 3.2 Minimum Software Requirements*

# CHAPTER: 4 PROCESS MODEL

# CHAPTER 4 PROCESS MODEL



The Process of Digital Forensics

Understand and clearly define the purpose of the investigation.

Isolate, secure, and preserve data to prevent tampering.

Carefully examine and interpret the preserved digital evidence.

Comprehensive record-keeping including a detailed account of actions.

Summarize and explain the conclusions drawn from the analysis.

*Figure 4.1 Process Model of Project*

# CHAPTER: 5 PROJECT PLAN

# CHAPTER 5 PROJECT PLAN

## 5.1 List of Major Activities

1. Task: - 1 Identification: Clearly define the purpose of the investigation, focusing on the specific digital devices and data to be analyzed.
2. Task: - 2 Preservation: Isolate, secure, and preserve the data from the digital devices to prevent tampering or loss of critical evidence.
3. Task: - 3 Analysis: Carefully examine and interpret the preserved digital evidence to uncover insights, patterns, or anomalies related to the investigation.
4. Task: - 4 Documentation: Maintain comprehensive records of all actions taken during the forensic process, ensuring transparency and accountability.
5. Task: - 5 Presentation: Summarize and explain the findings and conclusions drawn from the analysis in a clear and concise manner for legal or investigative purposes.

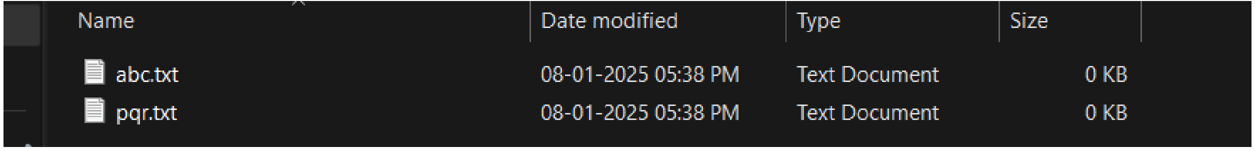
# CHAPTER: 6 IMPLEMENTATION DETAILS

## 6.1 UNDERSTANDING THE CONCEPTS OF HASH VALUES.

In this section we are going to learn about the working of Hash values and different scenarios of their working.

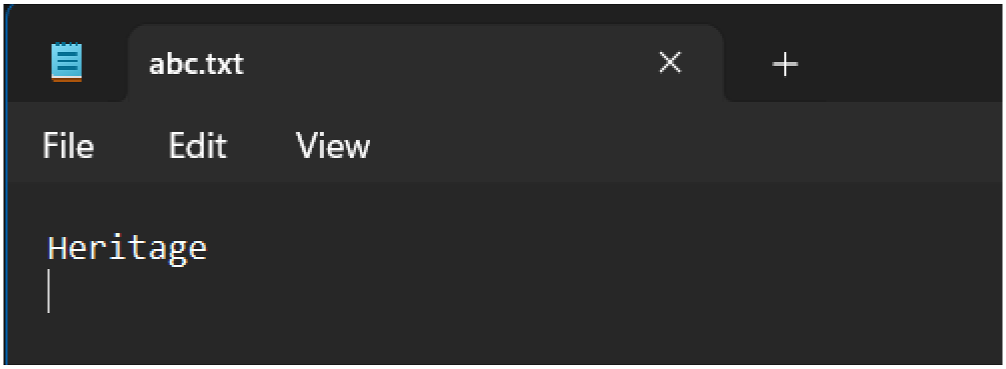
### 6.1.1 Compare hash values of 2 files after changing their extension.

We have 2 files abc.txt and pqr.txt.



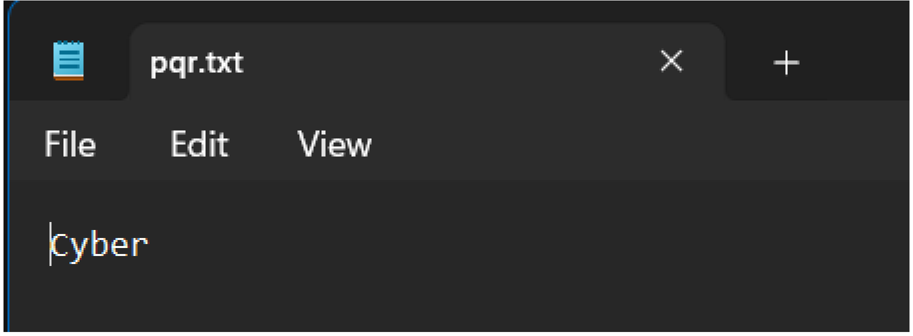
| Name | Date modified | Type | Size |
|---|---|---|---|
| abc.txt | 08-01-2025 05:38 PM | Text Document | 0 KB |
| pqr.txt | 08-01-2025 05:38 PM | Text Document | 0 KB |

Their contents are as below.
abc.txt



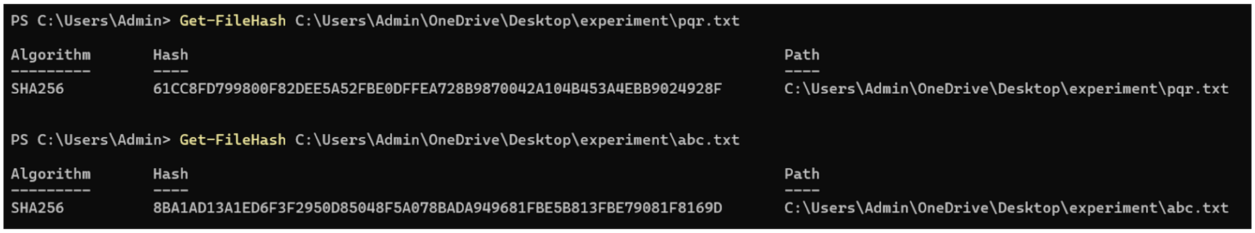
Heritage

pqr.txt



Cyber

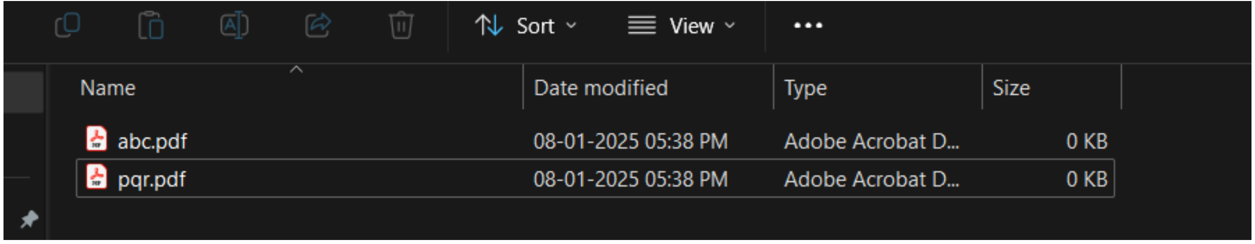
Their hash values are as below



```
PS C:\Users\Admin> Get-FileHash C:\Users\Admin\OneDrive\Desktop\experiment\pqr.txt

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA256          61CC8FD799800F82DEE5A52FBE0DFFEA728B98700042A104B453A4EBB9024928F       C:\Users\Admin\OneDrive\Desktop\experiment\pqr.txt

PS C:\Users\Admin> Get-FileHash C:\Users\Admin\OneDrive\Desktop\experiment\abc.txt

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA256          8BA1AD13A1ED6F3F2950D85048F5A078BADA949681FBE5B813FBE79081F8169D       C:\Users\Admin\OneDrive\Desktop\experiment\abc.txt
```

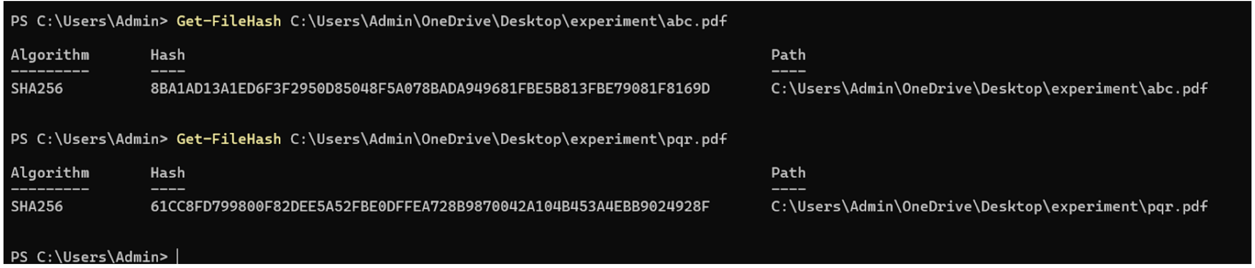
Hash values did not change.

Now, let’s change their file formats.



| Name | Date modified | Type | Size |
|---|---|---|---|
| abc.pdf | 08-01-2025 05:38 PM | Adobe Acrobat D... | 0 KB |
| pqr.pdf | 08-01-2025 05:38 PM | Adobe Acrobat D... | 0 KB |

Now let’s check their hash values again.

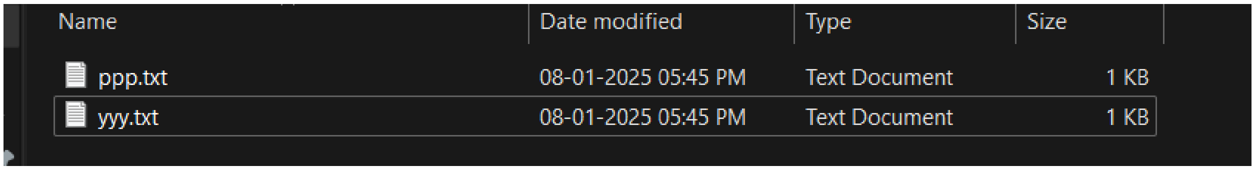


```
PS C:\Users\Admin> Get-FileHash C:\Users\Admin\OneDrive\Desktop\experiment\abc.pdf

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA256          8BA1AD13A1ED6F3F2950D85048F5A078BADA949681FBE5B813FBE79081F8169D       C:\Users\Admin\OneDrive\Desktop\experiment\abc.pdf


PS C:\Users\Admin> Get-FileHash C:\Users\Admin\OneDrive\Desktop\experiment\pqr.pdf

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA256          61CC8FD799800F82DEE5A52FBE0DFFEA728B9870042A104B453A4EBB9024928F       C:\Users\Admin\OneDrive\Desktop\experiment\pqr.pdf


PS C:\Users\Admin> |
```

We see that their hash values did not change and remained the same.

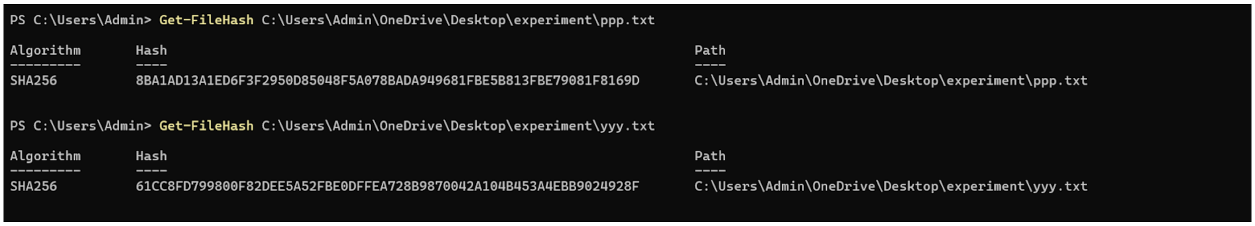
### 6.1.2 Compare hash values of 2 files with the same content after changing their file name.

We will change abc.txt to ppp.txt and pqr.txt to yyy.txt.



| Name | Date modified | Type | Size |
|---|---|---|---|
| ppp.txt | 08-01-2025 05:45 PM | Text Document | 1 KB |
| yyy.txt | 08-01-2025 05:45 PM | Text Document | 1 KB |

Now let’s check the hash values.

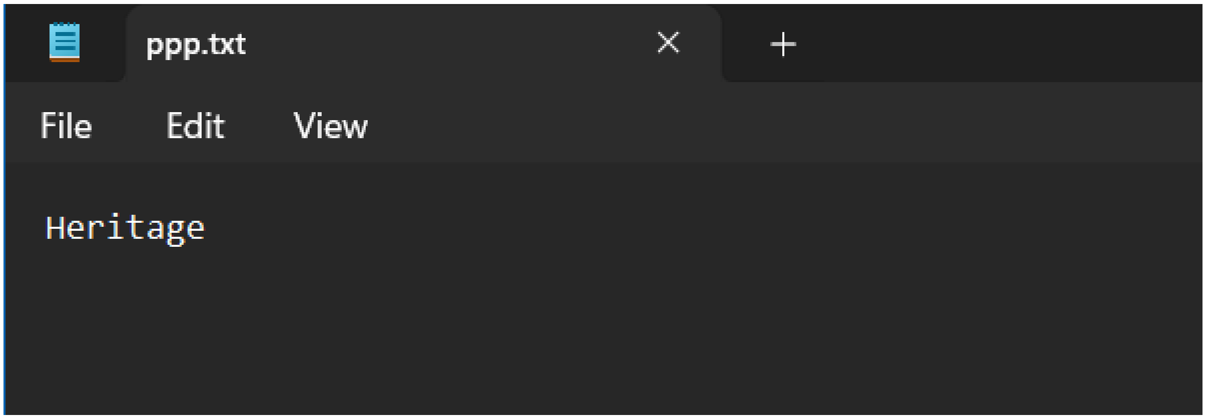


```
PS C:\Users\Admin> Get-FileHash C:\Users\Admin\OneDrive\Desktop\experiment\ppp.txt

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA256          8BA1AD13A1ED6F3F2950D85048F5A078BADA949681FBE5B813FBE79081F8169D       C:\Users\Admin\OneDrive\Desktop\experiment\ppp.txt


PS C:\Users\Admin> Get-FileHash C:\Users\Admin\OneDrive\Desktop\experiment\yyy.txt

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA256          61CC8FD799800F82DEE5A52FBE0DFFEA728B9870042A104B453A4EBB9024928F       C:\Users\Admin\OneDrive\Desktop\experiment\yyy.txt
```

We see that their hash values did not change in spite of changing the file name.

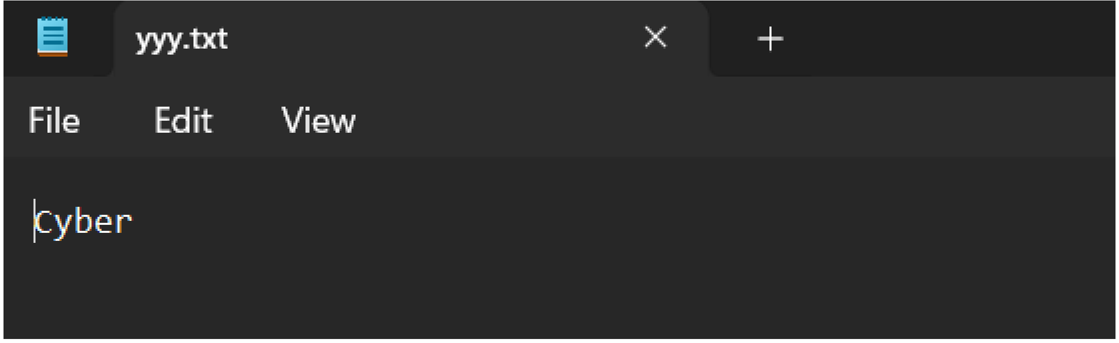
### 6.13. Compare hash values of 2  different file names with changed content.

Content of ppp.txt



```
Heritage
```

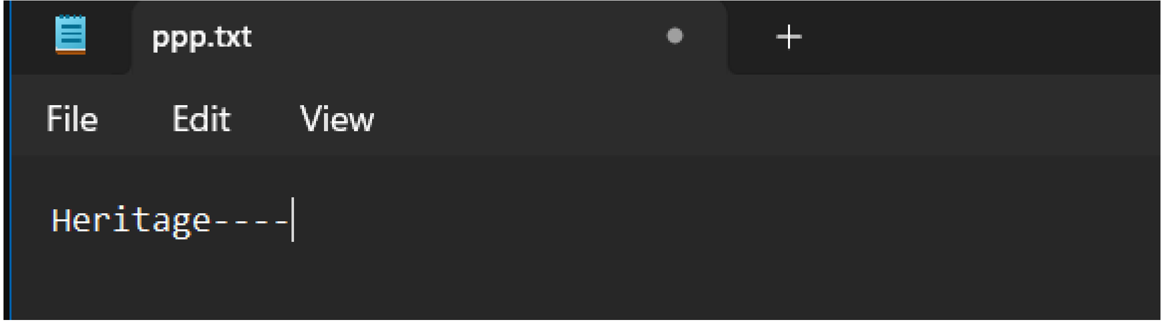
Content of yyy.txt



```
Cyber
```

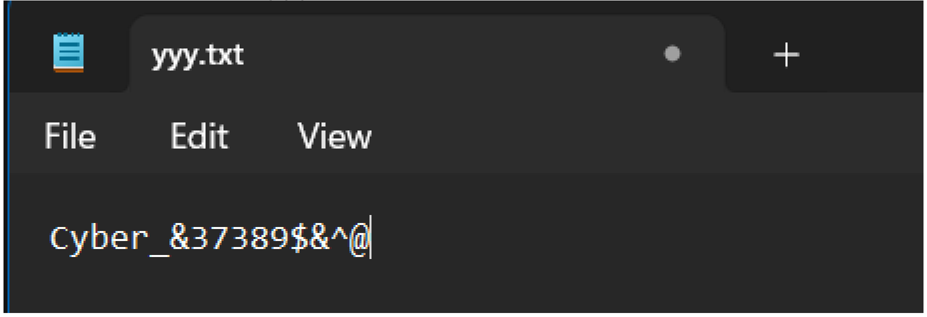
Now let’s modify the content.

Modified content of ppp.txt



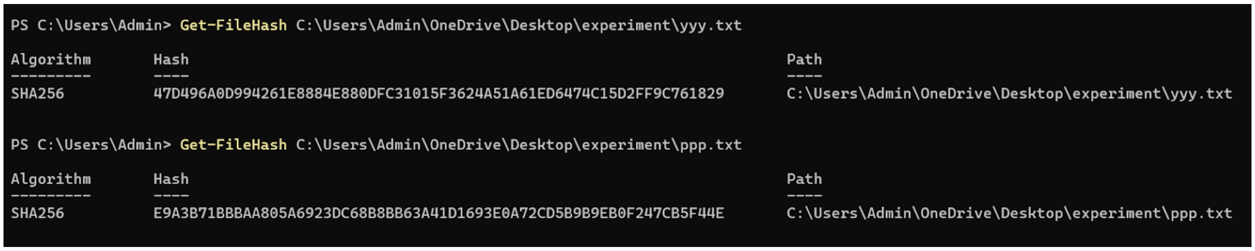
```
Heritage----
```

Modified content of yyy.txt



```
Cyber_&37389$&^@
```

Now let’s check  their hash values.



```
PS C:\Users\Admin> Get-FileHash C:\Users\Admin\OneDrive\Desktop\experiment\yyy.txt

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA256          47D496A0D994261E8884E880DFC31015F3624A51A61ED6474C15D2FF9C761829       C:\Users\Admin\OneDrive\Desktop\experiment\yyy.txt

PS C:\Users\Admin> Get-FileHash C:\Users\Admin\OneDrive\Desktop\experiment\ppp.txt

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA256          E9A3B71BBBAA805A6923DC68B8BB63A41D1693E0A72CD5B9B9EB0F247CB5F44E       C:\Users\Admin\OneDrive\Desktop\experiment\ppp.txt
```

Their hash values are different!!

Conclusion

From three scenarios, we conclude that hash value changes when content of 2 files are changed.

## 6.2 WORKING OF BOOTING PROCESS

### 6.2.1. Windows Booting Process

Step 1: Power-On Self-Test (POST)

When the system is powered on, the BIOS (Basic Input Output System) or UEFI (Unified Extensible Firmware Interface) firmware initializes the hardware components. It performs a hardware check (POST) to verify that essential components like CPU, RAM, and storage devices are functioning correctly.

Step 2: Boot Manager

The BIOS/UEFI locates the Master Boot Record (MBR) or GUID Partition Table (GPT) on the primary boot device. It  loads the Windows Boot Manager (bootmgr) from the EFI System Partition (ESP) for UEFI or from the boot sector for legacy BIOS systems.

Step 3: Boot Configuration Data (BCD)

The Boot Manager reads the Boot Configuration Data (BCD) file to determine the location of the Windows loader and other boot parameters.

Step 4: Windows Loader

The Windows Loader (winload.exe) is executed. It:

- Loads essential drivers.
- Loads the ntoskrnl.exe (Windows Kernel).
- Loads the HAL (Hardware Abstraction Layer).

Step 5: Kernel Initialization

The kernel initializes system processes and threads.

The Session Manager Subsystem (smss.exe) is launched, which starts critical system processes, including csrss.exe (Client-Server Runtime Subsystem) and wininit.exe.

Step 6: User Mode Initialization

The winlogon.exe process is started, which handles user authentication. The Graphical User Interface (GUI) is initialized, and the login screen is displayed.

Step 7: User Login

After successful login, user-specific settings are loaded from the registry, and the desktop environment is displayed.

### 6.2.2 Linux Booting Process

Step 1: BIOS/UEFI Initialization

Similar to Windows, the system starts with POST to check hardware functionality. The BIOS/UEFI firmware identifies the bootable device and loads the bootloader from the MBR or GPT.

Step 2: Bootloader

Common bootloaders include GRUB (GNU GRUB) or LILO (Linux Loader). The bootloader displays a menu allowing the user to select the kernel or operating system to boot. It loads the selected kernel and an initial RAM disk (initramfs or initrd).

Step 3: Kernel Initialization

The kernel is loaded into memory and begins execution.It initializes hardware drivers and mounts the root files System. The initramfs or initrd provides temporary access to necessary files until the root files ystem is ready.

Step 4: Init/Systemd Process

The first process started by the kernel is init (in older systems) or systemd (modern systems). systemd is the most common initialization system in modern Linux distributions. It organizes system processes into units for efficient management. init uses run levels (0 to 6) to manage system states.

Step 5: Services and Daemons

Essential services and background processes (daemons) are started according to the run level or systemd target (e.g., graphical .target for GUI-based systems).

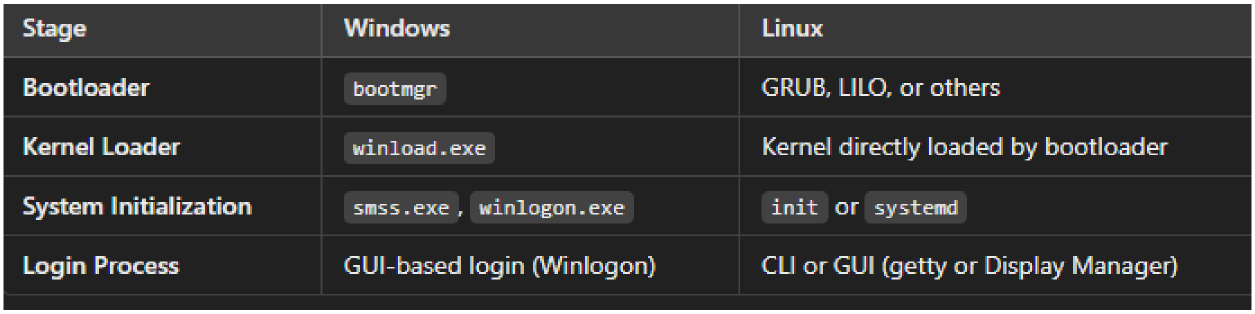
Step 6: User Login

The login manager (e.g., getty for text-based login or a display manager like gdm, lightdm, etc., for GUI) prompts the user for credentials. After successful authentication, the user shell or desktop environment is launched.

**Screenshot**

Screenshot : Not available as can’t capture screenshot on Company system

**Comparison of Key Components**



| Stage | Windows | Linux |
|---|---|---|
| Bootloader | `bootmgr` | GRUB, LILO, or others |
| Kernel Loader | `winload.exe` | Kernel directly loaded by bootloader |
| System Initialization | `smss.exe`, `winlogon.exe` | `init` or `systemd` |
| Login Process | GUI-based login (Winlogon) | CLI or GUI (getty or Display Manager) |

**Overall Conclusion**

Both systems aim to efficiently load the OS, initialize the hardware, and provide an environment for user interaction, though their architectures and tools differ significantly.

**Screenshot**

Not available as can’t capture screenshot on Company system

## 6.3 CHAIN OF CUSTODY

In the context of **Digital Forensics (DF)**, the **chain of custody** refers to the documented and unbroken process of collecting, preserving, transferring, analyzing, and presenting digital evidence. This ensures that the evidence is handled properly and remains admissible in court, maintaining its integrity throughout the investigation.

**Key Elements of the Chain of Custody**

### 6.3.1 General Flow in Chain of Custody

**Collection of Evidence**

1.Identify and document the digital evidence at the scene (e.g., hard drives, USBs, computers, mobile devices).
Label the evidence with a unique identifier (e.g., serial numbers, case IDs).

- Use forensic tools (e.g., write-blockers) to prevent accidental alteration while acquiring the data.

2. **Documentation**
   - Record every detail of the evidence, including:
     - Who collected it.
     - When and where it was collected.

        - What the evidence contains (a brief description).
        - How it was collected (e.g., tools used, method followed).
    - Include photos, screenshots, or sketches for clarity.

3. **Storage and Preservation**
    - Store the evidence in a secure, tamper-proof environment (e.g., locked storage, sealed evidence bags).
    - Ensure digital data is not altered or damaged during storage.
    - Maintain backups in case of accidental corruption.
4. **Transfer of Evidence**
    - Document every handover of the evidence between individuals, including:
        - The date and time of transfer.
        - The names of the sender and recipient.
        - The reason for transfer.
    - Ensure the evidence is securely transported (e.g., encrypted containers for digital files).
5. **Analysis**
    - Use forensically sound tools and methods for analysis to ensure evidence integrity (e.g., EnCase, FTK, or Autopsy).
    - Maintain logs of all actions performed on the evidence during analysis (e.g., hash value verification).
6. **Presentation**
    - Present the evidence in court or to relevant authorities.
    - Ensure that the evidence's chain of custody is well-documented to establish its authenticity and admissibility.
    - Expert witnesses may testify to validate the processes followed.

### 6.3.2 Importance of Chain of Custody in Digital Forensics

1. **Evidence Integrity:**
    - Ensures the evidence is not altered, tampered with, or corrupted during the investigation process.
2. **Admissibility in Court:**
    - Without a proper chain of custody, the evidence may be deemed inadmissible, as its authenticity can be questioned.
3. **Accountability:**
    - Assigns responsibility for handling and securing the evidence at every stage.
4. **Transparency:**
    - Provides a clear and documented trail of how the evidence was managed from collection to presentation.

## 6.4 FILE SYSTEM ARCHITECTURE

File system architecture defines the way data is stored, organized, retrieved, and managed on storage devices. Common file systems include FAT, NTFS, exFAT, ext, and others, each designed with different features, limitations, and use cases.

### 6.4.1 FAT (File Allocation Table)

- Types: FAT12, FAT16, FAT32
- Developer: Microsoft
- Common Use: USB drives, memory cards, and legacy systems

Key Features:

- Simple structure, highly compatible across OSes
- FAT32 supports partitions up to 2 TB (Windows supports up to 32 GB)
- Maximum file size: 4 GB

Limitations:

- No journaling support
- No file permissions or security features
- Prone to fragmentation and corruption

### 6.4.2 NTFS (New Technology File System)

- Developer: Microsoft
- Common Use: Default file system for modern Windows OS

Key Features:

- Supports very large file and partition sizes (up to 16 EB theoretical)
- Journaling for improved reliability
- File-level security via Access Control Lists (ACLs)
- Built-in compression, encryption (EFS), and disk quotas

Limitations:

- Limited support in macOS and Linux (read-only access by default)
- More complex structure compared to FAT

### 6.4.3 exFAT (Extended File Allocation Table)

- Developer: Microsoft
- Common Use: USB drives and SD cards for large file transfers

Key Features:

- Removes FAT32's 4 GB file size limit

- Lightweight with better performance for flash media
- Compatible with Windows, macOS, and Linux (with drivers)

Limitations:

- No journaling or advanced security
- Less robust than NTFS for critical storage

### 6.4.4 ext (Extended File System)

- Versions: ext2, ext3, ext4
- Developer: Linux community
- Common Use: Default file system in many Linux distributions

Key Features (ext4):

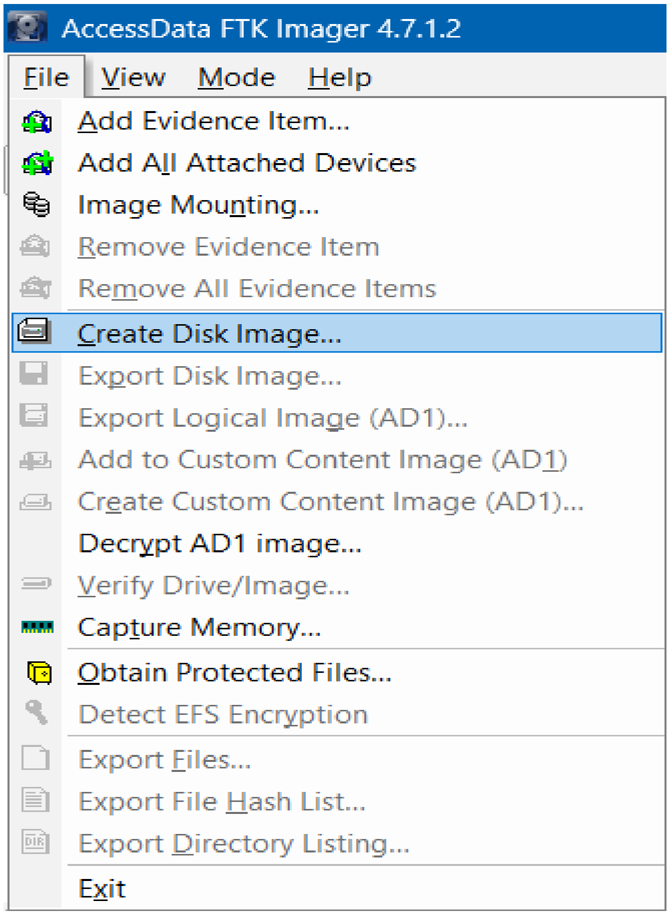
- Journaling and backward compatibility with ext2/ext3
- Maximum file size: 16 TB; maximum volume size: 1 EB
- Supports extents, delayed allocation, and reduced fragmentation

Limitations:

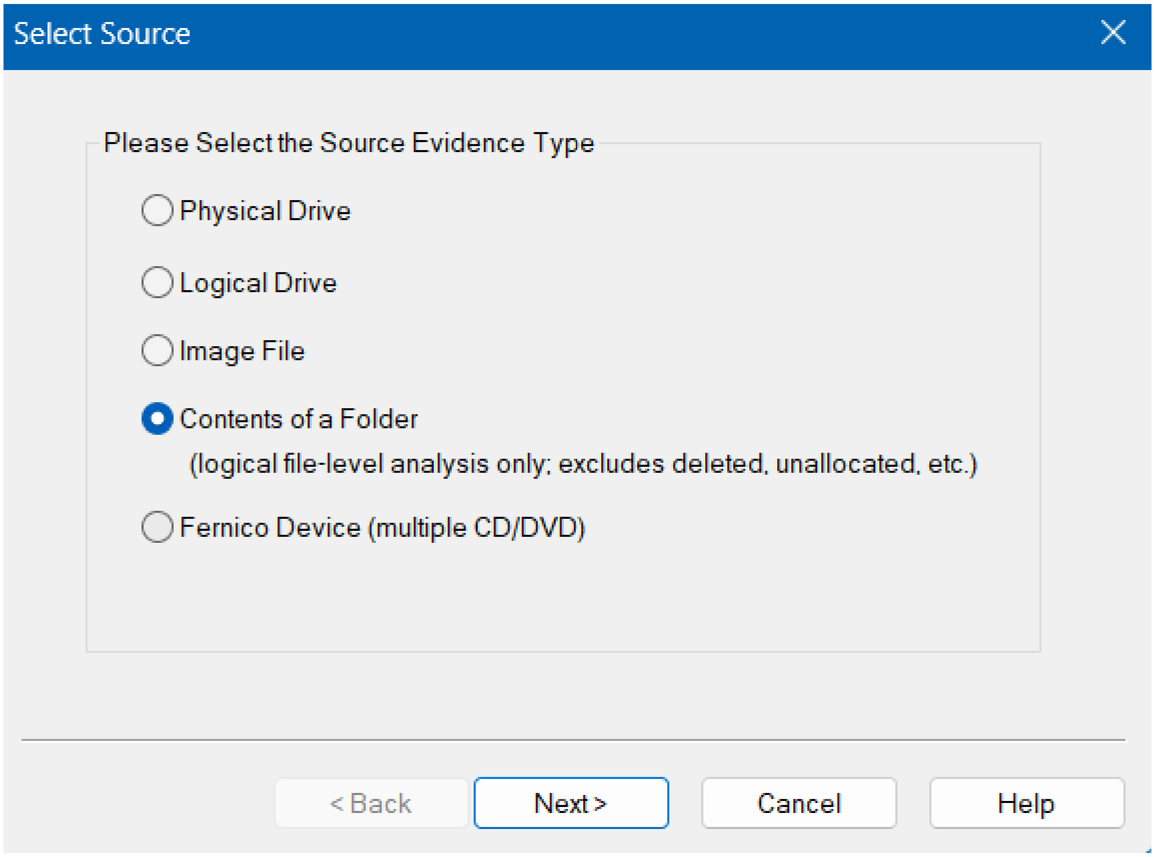
- Native support limited to Linux; third-party tools needed for Windows/macOS

## 6.5 IMAGING : CREATING AN IMAGE OF A FOLDER USING FTK IMAGER

1. Open ftk imager. Go to create a disk image.



2. Next select contents of a folder option to create an image (selecting this option as it will take less time)



Please Select the Source Evidence Type

○ Physical Drive

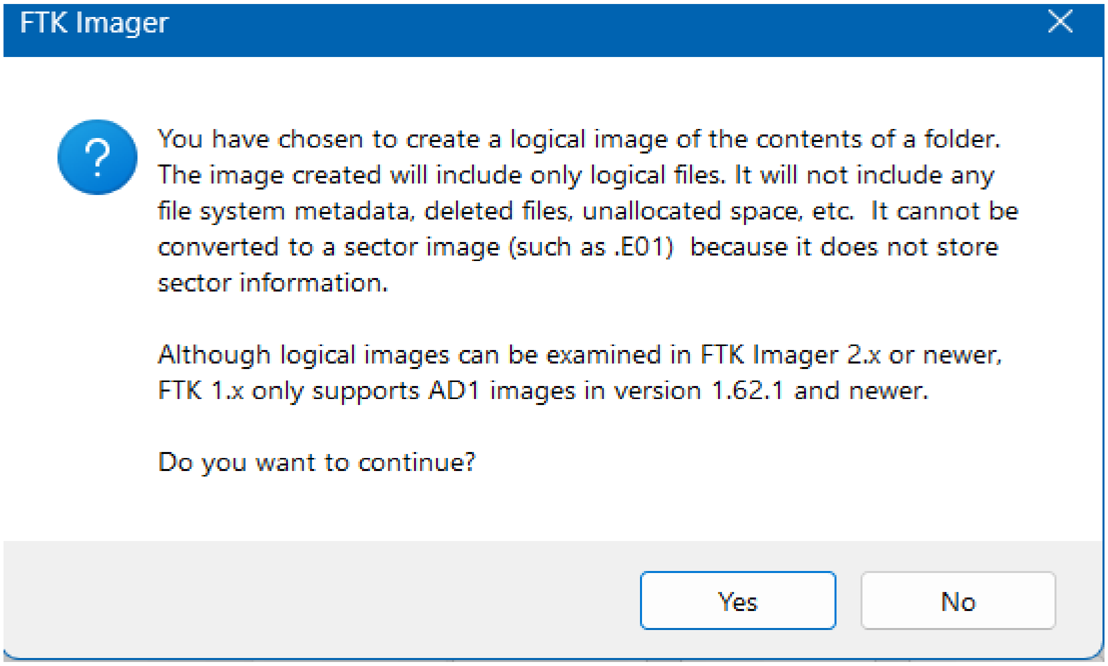
○ Logical Drive

○ Image File

● Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)

○ Fernico Device (multiple CD/DVD)

3. Click ok.

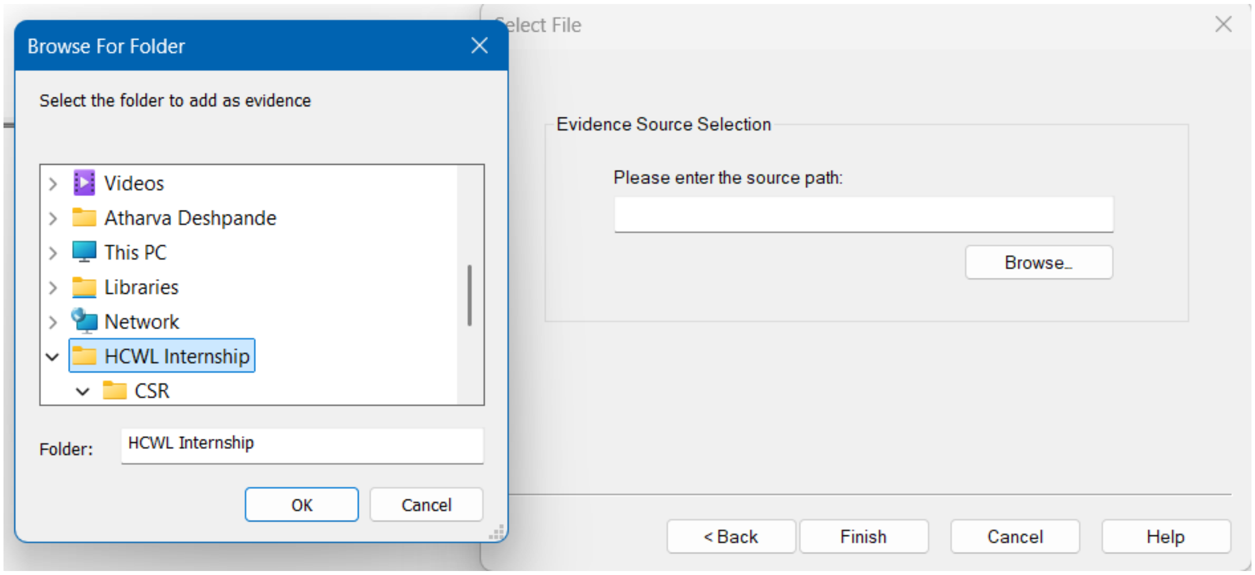


You have chosen to create a logical image of the contents of a folder. The image created will include only logical files. It will not include any file system metadata, deleted files, unallocated space, etc. It cannot be converted to a sector image (such as .E01) because it does not store sector information.

Although logical images can be examined in FTK Imager 2.x or newer, FTK 1.x only supports AD1 images in version 1.62.1 and newer.

Do you want to continue?

4. I am selecting this folder. (This folder contains internship related data).

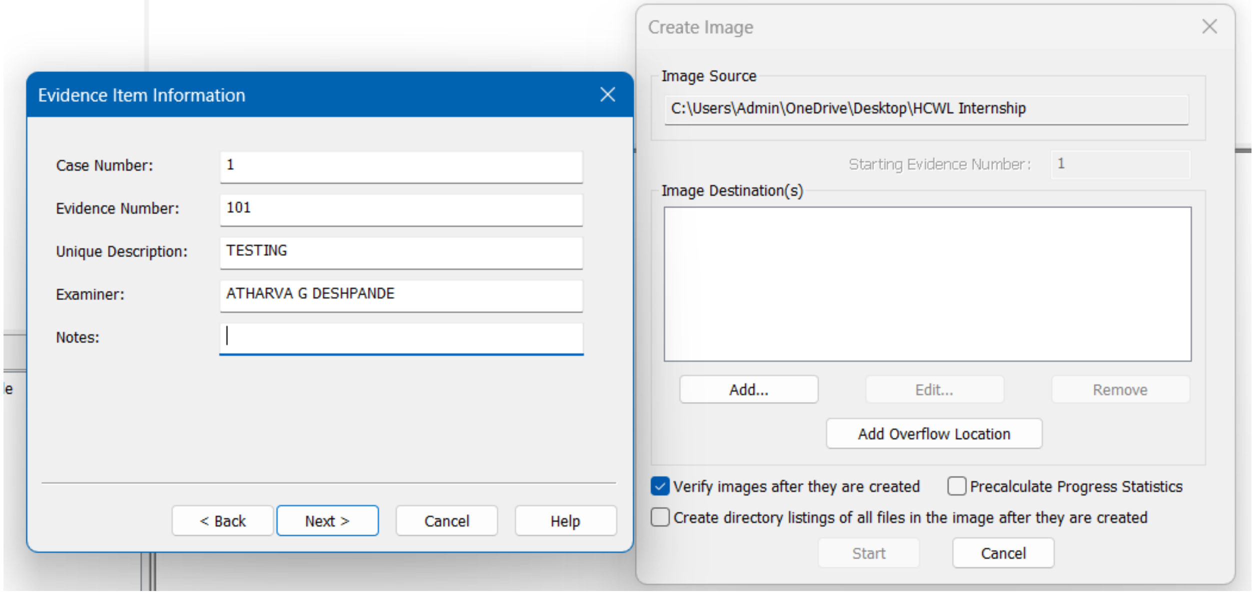


Select the folder to add as evidence

- Videos
- Atharva Deshpande
- This PC
- Libraries
- Network
- HCWL Internship
  - CSR

Folder: HCWL Internship

5. Fill in these details properly.



| | |
|---|---|
| Case Number: | 1 |
| Evidence Number: | 101 |
| Unique Description: | TESTING |
| Examiner: | ATHARVA G DESHPANDE |
| Notes: | |

Image Source: C:\Users\Admin\OneDrive\Desktop\HCWL Internship

Starting Evidence Number: 1

☑ Verify images after they are created ☐ Precalculate Progress Statistics

☐ Create directory listings of all files in the image after they are created

6. Enter image destination folder details

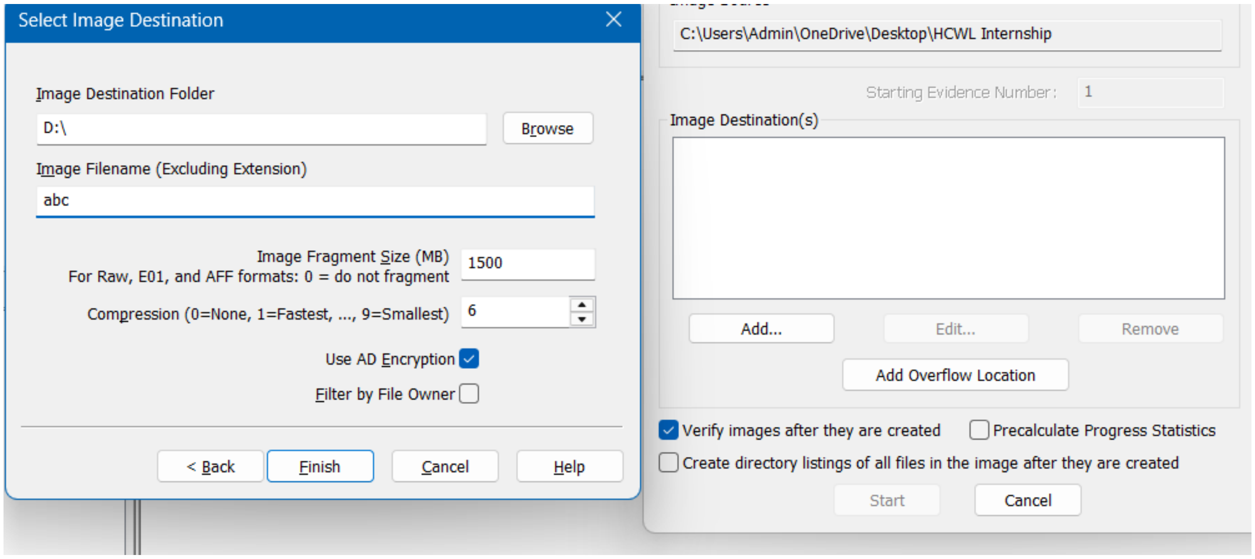


Image Destination Folder: D:\

Image Filename (Excluding Extension): abc

Image Fragment Size (MB)
For Raw, E01, and AFF formats: 0 = do not fragment: 1500

Compression (0=None, 1=Fastest, ..., 9=Smallest): 6

Use AD Encryption ☑

Filter by File Owner □

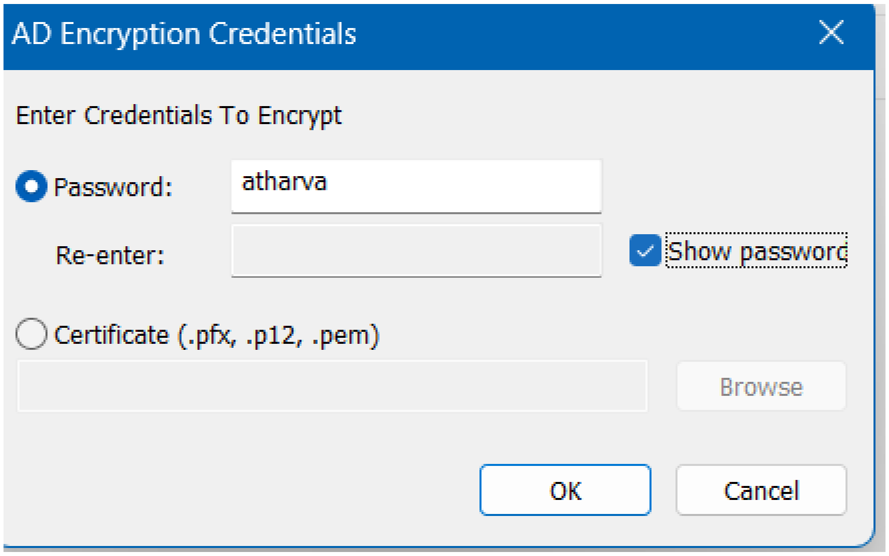
C:\Users\Admin\OneDrive\Desktop\HCWL Internship

Starting Evidence Number: 1

☑ Verify images after they are created □ Precalculate Progress Statistics

□ Create directory listings of all files in the image after they are created

7. Enter the AD image encryption details (As earlier we selected this option for encryption).



Enter Credentials To Encrypt

● Password: atharva

Re-enter: ☑ Show password

○ Certificate (.pfx, .p12, .pem)

8. Click on the Start button to start the image creation.

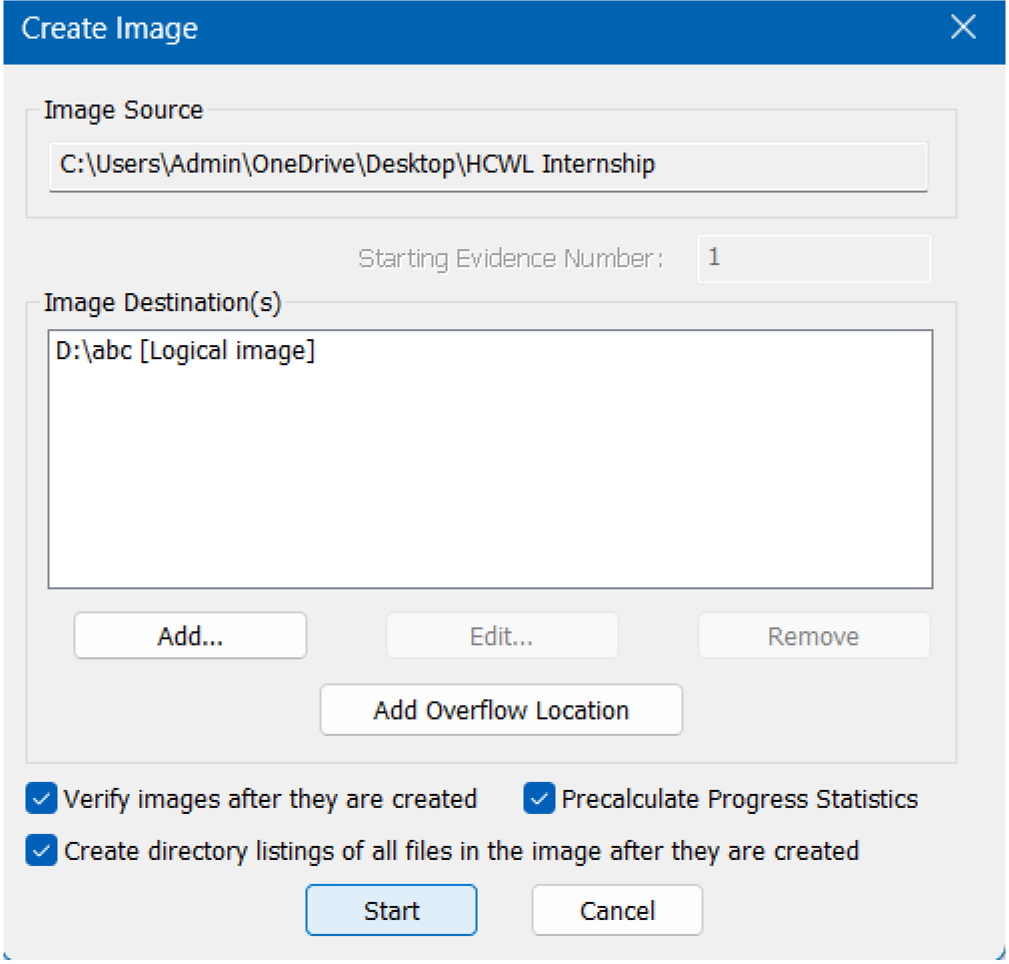

Create Image

Image Source

C:\Users\Admin\OneDrive\Desktop\HCWL Internship

Starting Evidence Number: 1

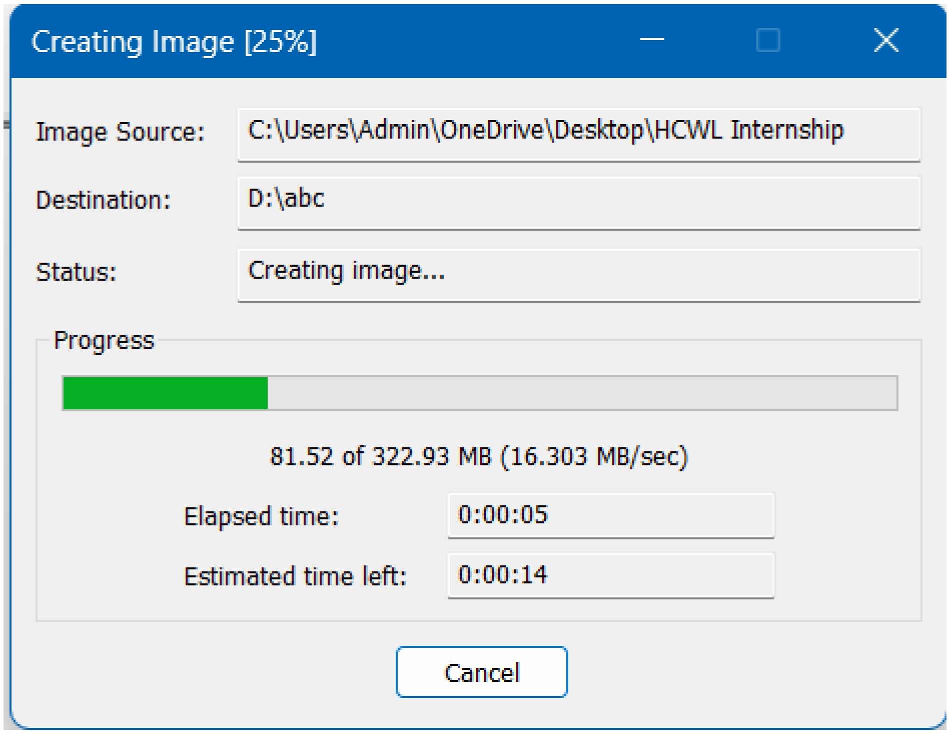
Image Destination(s)

D:\abc [Logical image]

☑ Verify images after they are created ☑ Precalculate Progress Statistics

☑ Create directory listings of all files in the image after they are created

9. Image creation is in Progress.



Creating Image [25%]

Image Source: C:\Users\Admin\OneDrive\Desktop\HCWL Internship

Destination: D:\abc

Status: Creating image...

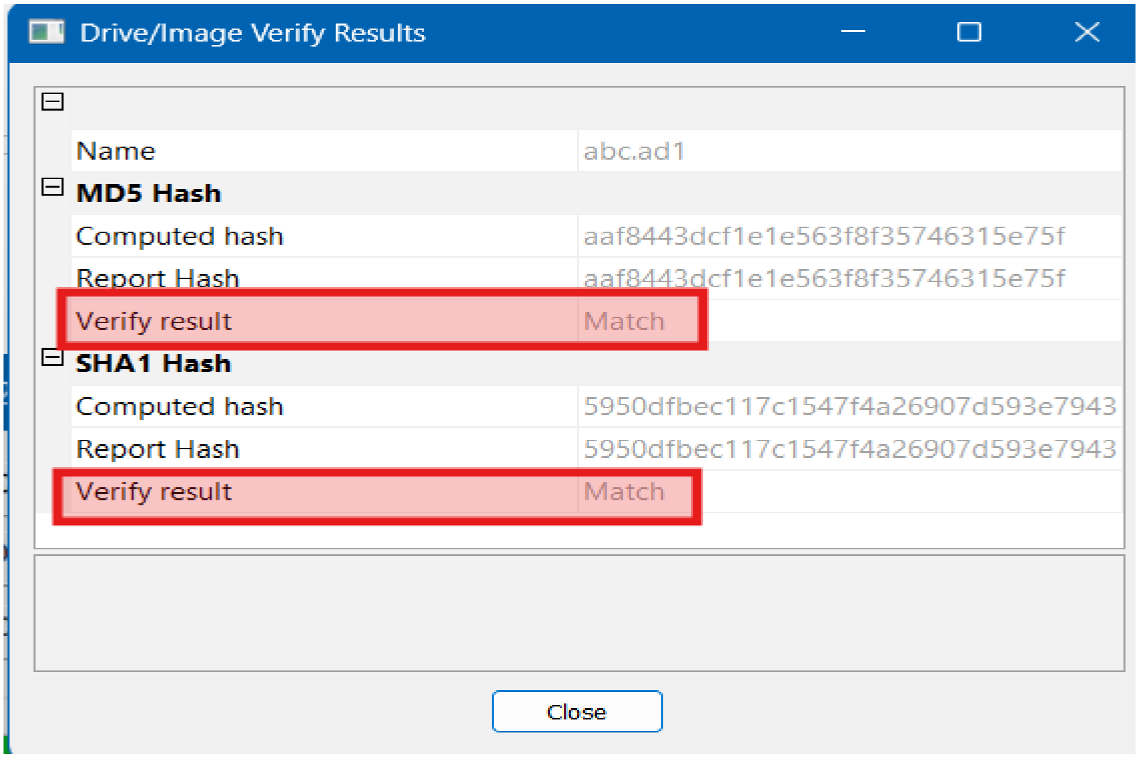
Progress

81.52 of 322.93 MB (16.303 MB/sec)

Elapsed time: 0:00:05

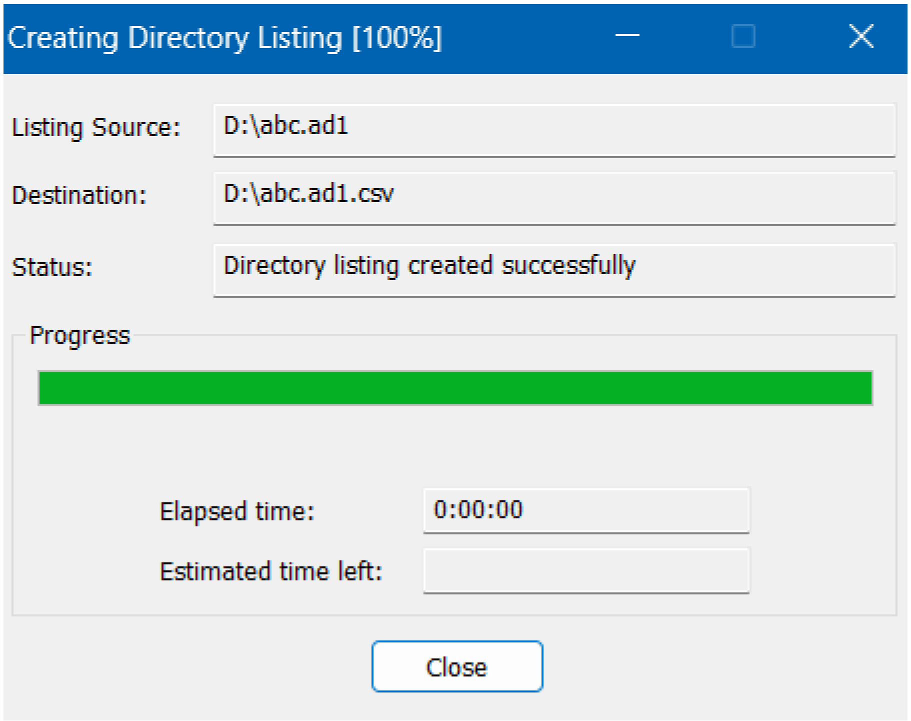
Estimated time left: 0:00:14

10. Result verification has been successful.



Drive/Image Verify Results

|  |  |
|---|---|
| Name | abc.ad1 |
| **MD5 Hash** |  |
| Computed hash | aaf8443dcf1e1e563f8f35746315e75f |
| Report Hash | aaf8443dcf1e1e563f8f35746315e75f |
| Verify result | Match |
| **SHA1 Hash** |  |
| Computed hash | 5950dfbec117c1547f4a26907d593e7943 |
| Report Hash | 5950dfbec117c1547f4a26907d593e7943 |
| Verify result | Match |



Creating Directory Listing [100%]

Listing Source: D:\abc.ad1

Destination: D:\abc.ad1.csv

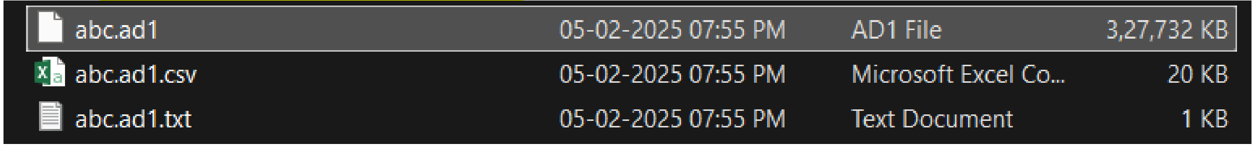
Status: Directory listing created successfully

Progress

Elapsed time: 0:00:00

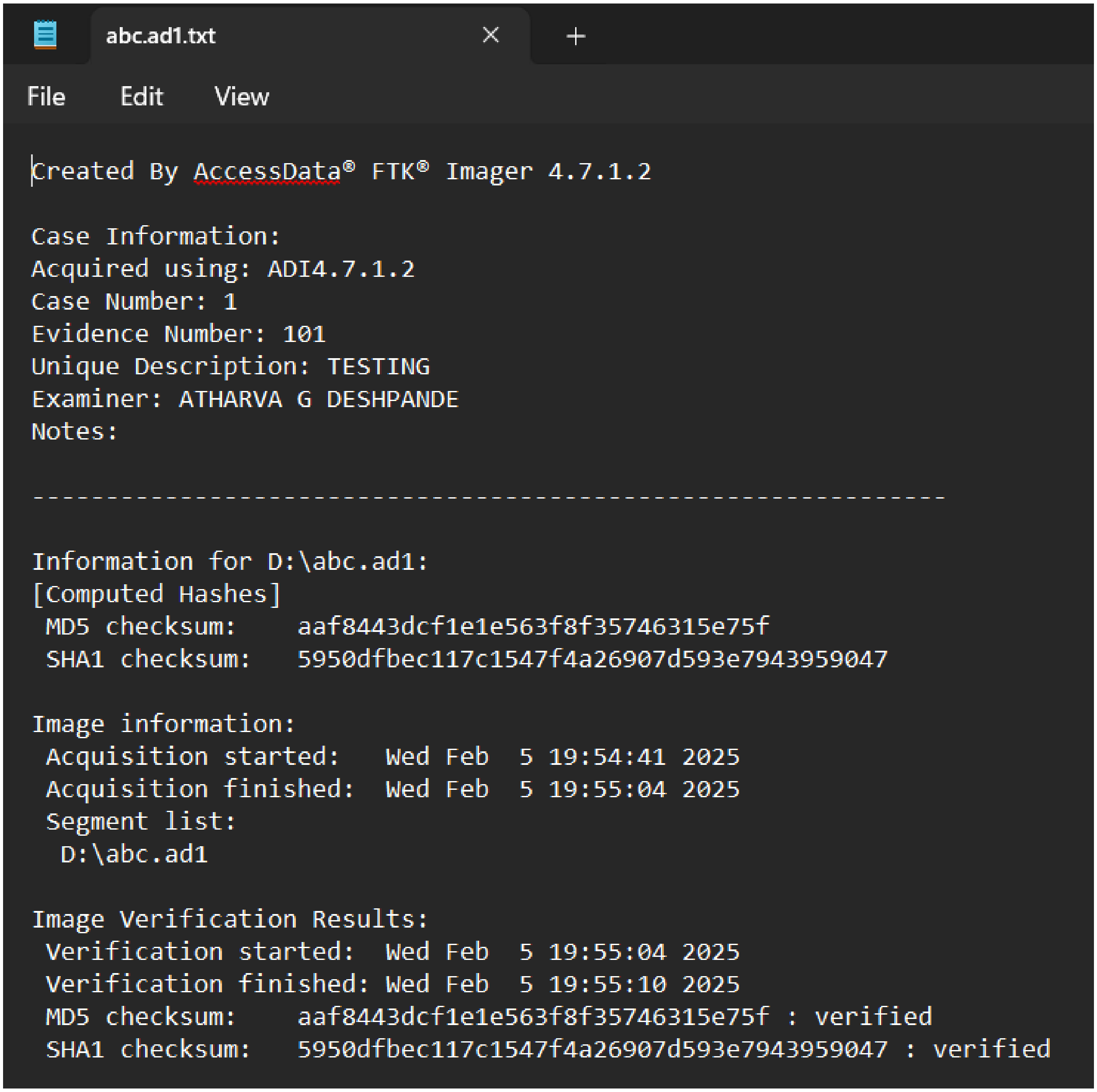
Estimated time left:

11. Final output of the image created.



```
abc.ad1        05-02-2025 07:55 PM   AD1 File               3,27,732 KB
abc.ad1.csv    05-02-2025 07:55 PM   Microsoft Excel Co...      20 KB
abc.ad1.txt    05-02-2025 07:55 PM   Text Document               1 KB
```

12. Summarization



```
Created By AccessData® FTK® Imager 4.7.1.2

Case Information:
Acquired using: ADI4.7.1.2
Case Number: 1
Evidence Number: 101
Unique Description: TESTING
Examiner: ATHARVA G DESHPANDE
Notes:

--------------------------------------------------------------

Information for D:\abc.ad1:
[Computed Hashes]
 MD5 checksum:    aaf8443dcf1e1e563f8f35746315e75f
 SHA1 checksum:   5950dfbec117c1547f4a26907d593e7943959047

Image information:
 Acquisition started:   Wed Feb  5 19:54:41 2025
 Acquisition finished:  Wed Feb  5 19:55:04 2025
 Segment list:
  D:\abc.ad1

Image Verification Results:
 Verification started:  Wed Feb  5 19:55:04 2025
 Verification finished: Wed Feb  5 19:55:10 2025
 MD5 checksum:    aaf8443dcf1e1e563f8f35746315e75f : verified
 SHA1 checksum:   5950dfbec117c1547f4a26907d593e7943959047 : verified
```

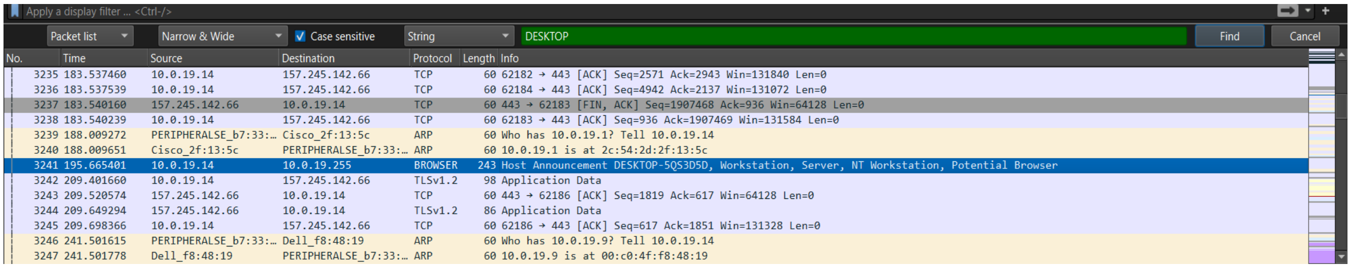
**Conclusion : Image verification is successful**

## 6.6 WIRESHARK ANALYSIS: TASK TO ANALYZE SUSPICIOUS FILE.

In this section, we will analyze a suspicious pcap file and try to look for any malicious content in it.

### 6.6.1 Install Wireshark and open the file.

Upon opening the packet we see the following interface with it's user details.



Packet list ▾ Narrow & Wide ▾ ☑ Case sensitive String ▾ DESKTOP

```
No.   Time       Source             Destination        Protocol Length Info
 3235 183.537460 10.0.19.14         157.245.142.66     TCP       60 62182 → 443 [ACK] Seq=2571 Ack=2943 Win=131840 Len=0
 3236 183.537539 10.0.19.14         157.245.142.66     TCP       60 62184 → 443 [ACK] Seq=4942 Ack=2137 Win=131072 Len=0
 3237 183.540160 157.245.142.66     10.0.19.14         TCP       60 443 → 62183 [FIN, ACK] Seq=1907468 Ack=936 Win=64128 Len=0
 3238 183.540239 10.0.19.14         157.245.142.66     TCP       60 62183 → 443 [ACK] Seq=936 Ack=1907469 Win=131584 Len=0
 3239 188.009272 PERIPHERALSE_b7:33:… Cisco_2f:13:5c   ARP       60 Who has 10.0.19.1? Tell 10.0.19.14
 3240 188.009651 Cisco_2f:13:5c     PERIPHERALSE_b7:33:… ARP     60 10.0.19.1 is at 2c:54:2d:2f:13:5c
 3241 195.665401 10.0.19.14         10.0.19.255        BROWSER  243 Host Announcement DESKTOP-5QS3D5D, Workstation, Server, NT Workstation, Potential Browser
 3242 209.401660 10.0.19.14         157.245.142.66     TLSv1.2   98 Application Data
 3243 209.520574 157.245.142.66     10.0.19.14         TCP       60 443 → 62186 [ACK] Seq=1819 Ack=617 Win=64128 Len=0
 3244 209.649294 157.245.142.66     10.0.19.14         TLSv1.2   86 Application Data
 3245 209.698366 10.0.19.14         157.245.142.66     TCP       60 62186 → 443 [ACK] Seq=617 Ack=1851 Win=131328 Len=0
 3246 241.501615 PERIPHERALSE_b7:33:… Dell_f8:48:19    ARP       60 Who has 10.0.19.9? Tell 10.0.19.14
 3247 241.501778 Dell_f8:48:19      PERIPHERALSE_b7:33:… ARP     60 10.0.19.9 is at 00:c0:4f:f8:48:19
```

We got the following details. This is the user of the system.

User : Patrick Zimmerman

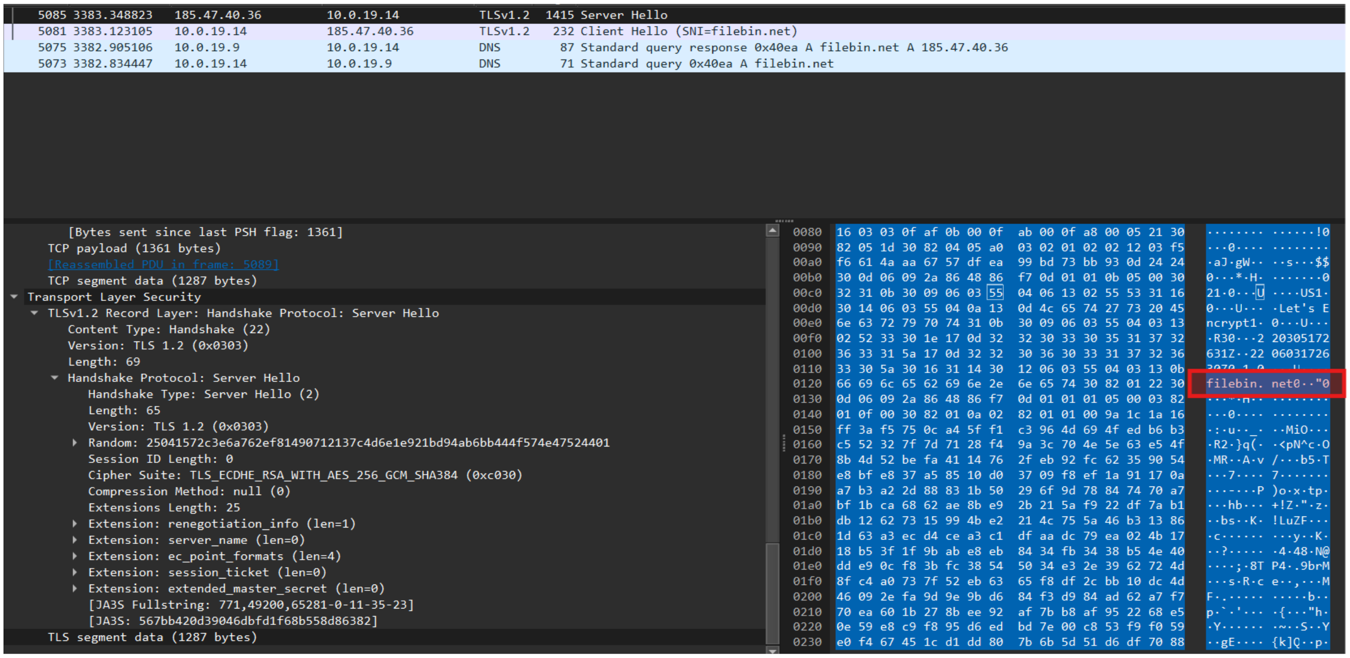
IP Address : 10.0.19.14

Device : DESKTOP-5QS3D5D

MAC Address : 00:60:52:b7:33:0f

### 6.6.2 Scanning for IOC's in the packet.

Upon examining the stream, we came across with a suspicious and unusual IP and domain name 'filebin.net'.

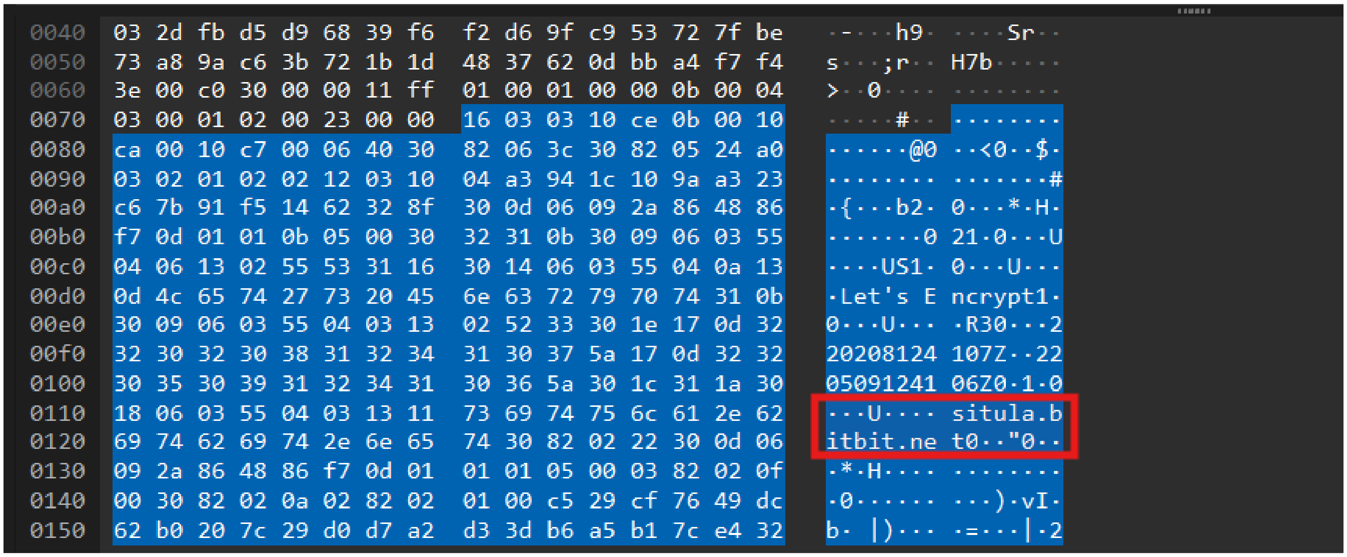


```
5085 3383.348823   185.47.40.36     10.0.19.14       TLSv1.2  1415 Server Hello
5081 3383.123105   10.0.19.14       185.47.40.36     TLSv1.2   232 Client Hello (SNI=filebin.net)
5075 3382.905106   10.0.19.9        10.0.19.14       DNS        87 Standard query response 0x40ea A filebin.net A 185.47.40.36
5073 3382.834447   10.0.19.14       10.0.19.9        DNS        71 Standard query 0x40ea A filebin.net
```

```
      [Bytes sent since last PSH flag: 1361]
    TCP payload (1361 bytes)
    [Reassembled PDU in frame: 5089]
    TCP segment data (1287 bytes)
▾ Transport Layer Security
  ▾ TLSv1.2 Record Layer: Handshake Protocol: Server Hello
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 69
    ▾ Handshake Protocol: Server Hello
        Handshake Type: Server Hello (2)
        Length: 65
        Version: TLS 1.2 (0x0303)
      ▸ Random: 25041572c3e6a762ef81490712137c4d6e1e921bd94ab6bb444f574e47524401
        Session ID Length: 0
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
        Compression Method: null (0)
        Extensions Length: 25
      ▸ Extension: renegotiation_info (len=1)
      ▸ Extension: server_name (len=0)
      ▸ Extension: ec_point_formats (len=4)
      ▸ Extension: session_ticket (len=0)
      ▸ Extension: extended_master_secret (len=0)
        [JA3S Fullstring: 771,49200,65281-0-11-35-23]
        [JA3S: 567bb420d39046dbfd1f68b558d86382]
    TLS segment data (1287 bytes)
```

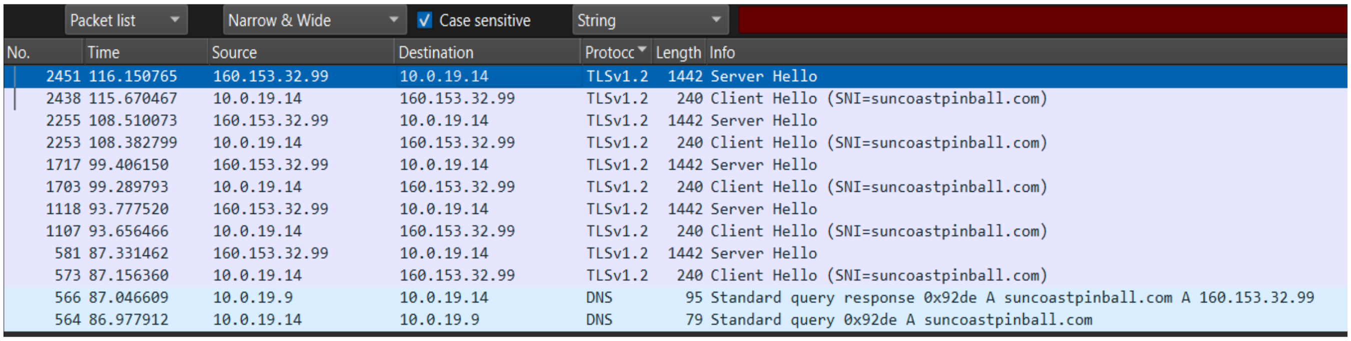
```
0080  16 03 03 0f af 0b 00 0f  ab 00 0f a8 00 05 21 30   ········ ······!0
0090  82 05 1d 30 82 04 05 a0  03 02 01 02 02 12 03 f5   ···0···· ········
00a0  f6 61 4a aa 67 57 df ea  99 bd 73 bb 93 0d 24 24   ·aJ·gW·· ··s···$$
00b0  30 0d 06 09 2a 86 48 86  f7 0d 01 01 0b 05 00 30   0···*·H· ·······0
00c0  32 31 0b 30 09 06 03 55  04 06 13 02 55 53 31 16   21·0···U ····US1·
00d0  30 14 06 03 55 04 0a 13  0d 4c 65 74 27 73 20 45   0···U··· ·Let's E
00e0  6e 63 72 79 70 74 31 0b  30 09 06 03 55 04 03 13   ncrypt1· 0···U···
00f0  02 52 33 30 1e 17 0d 32  32 30 33 30 35 31 37 32   ·R30···2 20305172
0100  36 33 31 5a 17 0d 32 32  30 36 30 33 31 37 32 36   631Z··22 06031726
0110  33 30 5a 30 16 31 14 30  12 06 03 55 04 03 13 0b   30Z0·1·0 ···U····
0120  66 69 6c 65 62 69 6e 2e  6e 65 74 30 82 01 22 30   filebin. net0··"0
0130  0d 06 09 2a 86 48 86 f7  0d 01 01 01 05 00 03 82   ···*·H·· ········
0140  01 0f 00 30 82 01 0a 02  82 01 01 00 9a 1c 1a 16   ···0···· ········
0150  ff 3a f5 75 0c a4 5f f1  c3 96 4d 69 4f ed b6 b3   ·:·u··_· ··MiO···
0160  c5 52 32 7f 7d 71 28 f4  9a 3c 70 4e 5e 63 e5 4f   ·R2·}q(· ·<pN^c·O
0170  8b 4d 52 be fa 41 14 76  2f eb 92 fc 62 35 90 54   ·MR··A·v /···b5·T
0180  e8 bf e8 37 a5 85 10 d0  37 09 f8 ef 1a 91 17 0a   ···7···· 7·······
0190  a7 b3 a2 2d 88 83 1b 50  29 6f 9d 78 84 74 70 a7   ···-···P )o·x·tp·
01a0  bf 1b ca 68 62 ae 8b e9  2b 21 5a f9 22 df 7a b1   ···hb··· +!Z·"·z·
01b0  db 12 62 73 15 99 4b e2  21 4c 75 5a 46 b3 13 86   ··bs··K· !LuZF···
01c0  1d 63 a3 ec d4 ce a3 c1  df aa dc 79 ea 02 4b 17   ·c······ ···y··K·
01d0  18 b5 3f 1f 9b ab e8 eb  84 34 fb 34 38 b5 4e 40   ··?····· ·4·48·N@
01e0  dd e9 0c f8 3b fc 38 54  50 34 e3 2e 39 62 72 4d   ····;·8T P4·.9brM
01f0  8f c4 a0 73 7f 52 eb 63  65 f8 df 2c bb 10 dc 4d   ···s·R·c e··,···M
0200  46 09 2e fa 9d 9e 9b d6  84 f3 d9 84 ad 62 a7 f7   F·.····· ·····b··
0210  70 ea 60 1b 27 8b ee 92  af 7b b8 af 95 22 68 e5   p·`·'··· ·{···"h·
0220  0e 59 e8 c9 f8 95 d6 ed  bd 7e 00 c8 53 f9 f0 59   ·Y······ ·~··S··Y
0230  e0 f4 67 45 1c d1 dd 80  7b 6b 5d 51 d6 df 70 88   ··gE···· {k]Q··p·
```

Again on deep inspection of messages and data exchanged, we observe data is being sent to suspicious domain ‘situla.bitbit.net’.



```
0040  03 2d fb d5 d9 68 39 f6  f2 d6 9f c9 53 72 7f be   ·-···h9· ····Sr··
0050  73 a8 9a c6 3b 72 1b 1d  48 37 62 0d bb a4 f7 f4   s···;r·· H7b·····
0060  3e 00 c0 30 00 00 11 ff  01 00 01 00 00 0b 00 04   >··0···· ········
0070  03 00 01 02 00 23 00 00  16 03 03 10 ce 0b 00 10   ·····#·· ········
0080  ca 00 10 c7 00 06 40 30  82 06 3c 30 82 05 24 a0   ······@0 ··<0··$·
0090  03 02 01 02 02 12 03 10  04 a3 94 1c 10 9a a3 23   ········ ·······#
00a0  c6 7b 91 f5 14 62 32 8f  30 0d 06 09 2a 86 48 86   ·{···b2· 0···*·H·
00b0  f7 0d 01 01 0b 05 00 30  32 31 0b 30 09 06 03 55   ·······0 21·0···U
00c0  04 06 13 02 55 53 31 16  30 14 06 03 55 04 0a 13   ····US1· 0···U···
00d0  0d 4c 65 74 27 73 20 45  6e 63 72 79 70 74 31 0b   ·Let's E ncrypt1·
00e0  30 09 06 03 55 04 03 13  02 52 33 30 1e 17 0d 32   0···U··· ·R30···2
00f0  32 30 32 30 38 31 32 34  31 30 37 5a 17 0d 32 32   20208124 107Z··22
0100  30 35 30 39 31 32 34 31  30 36 5a 30 1c 31 1a 30   05091241 06Z0·1·0
0110  18 06 03 55 04 03 13 11  73 69 74 75 6c 61 2e 62   ···U···· situla.b
0120  69 74 62 69 74 2e 6e 65  74 30 82 02 22 30 0d 06   itbit.ne t0··"0··
0130  09 2a 86 48 86 f7 0d 01  01 01 05 00 03 82 02 0f   ·*·H···· ········
0140  00 30 82 02 0a 02 82 02  01 00 c5 29 cf 76 49 dc   ·0······ ···)·vI·
0150  62 b0 20 7c 29 d0 d7 a2  d3 3d b6 a5 b1 7c e4 32   b· |)··· ·=···|·2
```

Lastly, we observe malicious interaction with DNS server ‘suncoastpinball.net’. The Server IP and Port Number looks suspicious as well.



```
No.   Time        Source         Destination    Protocc Length Info
 2451 116.150765  160.153.32.99  10.0.19.14     TLSv1.2  1442 Server Hello
 2438 115.670467  10.0.19.14     160.153.32.99  TLSv1.2   240 Client Hello (SNI=suncoastpinball.com)
 2255 108.510073  160.153.32.99  10.0.19.14     TLSv1.2  1442 Server Hello
 2253 108.382799  10.0.19.14     160.153.32.99  TLSv1.2   240 Client Hello (SNI=suncoastpinball.com)
 1717 99.406150   160.153.32.99  10.0.19.14     TLSv1.2  1442 Server Hello
 1703 99.289793   10.0.19.14     160.153.32.99  TLSv1.2   240 Client Hello (SNI=suncoastpinball.com)
 1118 93.777520   160.153.32.99  10.0.19.14     TLSv1.2  1442 Server Hello
 1107 93.656466   10.0.19.14     160.153.32.99  TLSv1.2   240 Client Hello (SNI=suncoastpinball.com)
  581 87.331462   160.153.32.99  10.0.19.14     TLSv1.2  1442 Server Hello
  573 87.156360   10.0.19.14     160.153.32.99  TLSv1.2   240 Client Hello (SNI=suncoastpinball.com)
  566 87.046609   10.0.19.9      10.0.19.14     DNS        95 Standard query response 0x92de A suncoastpinball.com A 160.153.32.99
  564 86.977912   10.0.19.14     10.0.19.9      DNS        79 Standard query 0x92de A suncoastpinball.com
```

Conclusion

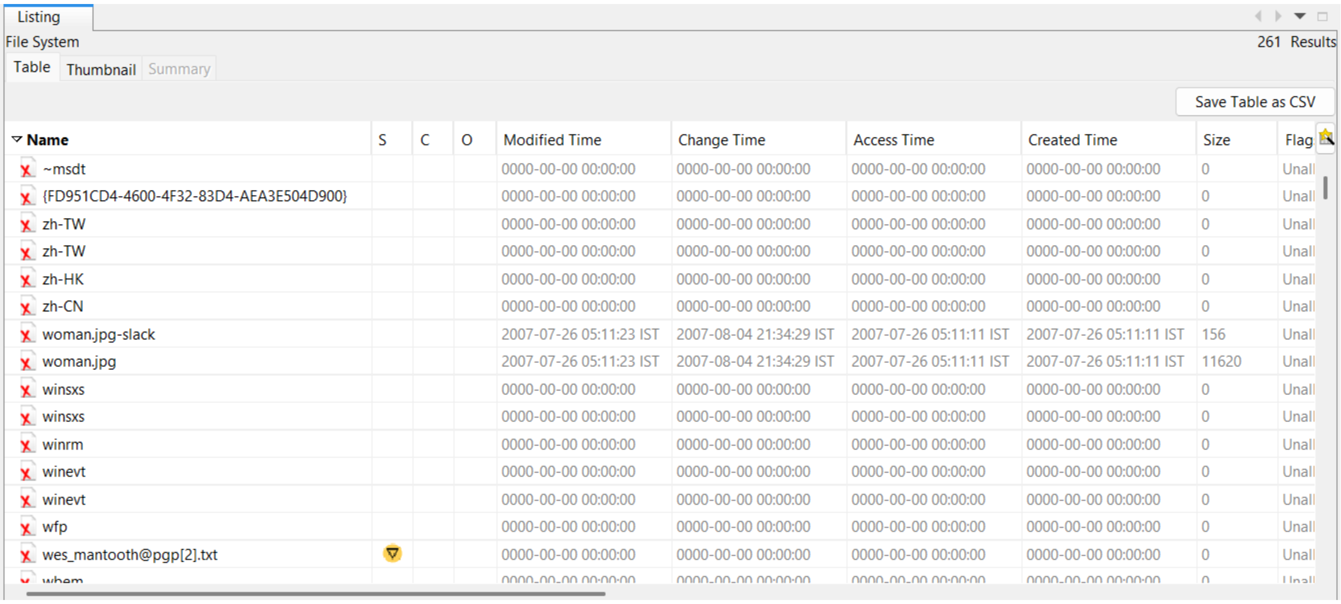
From the packet analysis, I have found a total of 3 IOC’s with their details explained above. The IOC’s are malicious domains by which a cyber- attack might have been performed on the user.

## 6.7 ANALYZING FORENSIC IMAGE OF DISC DRIVE

### 6.7.1 Load the image in Autopsy (A software for analyzing disc images).

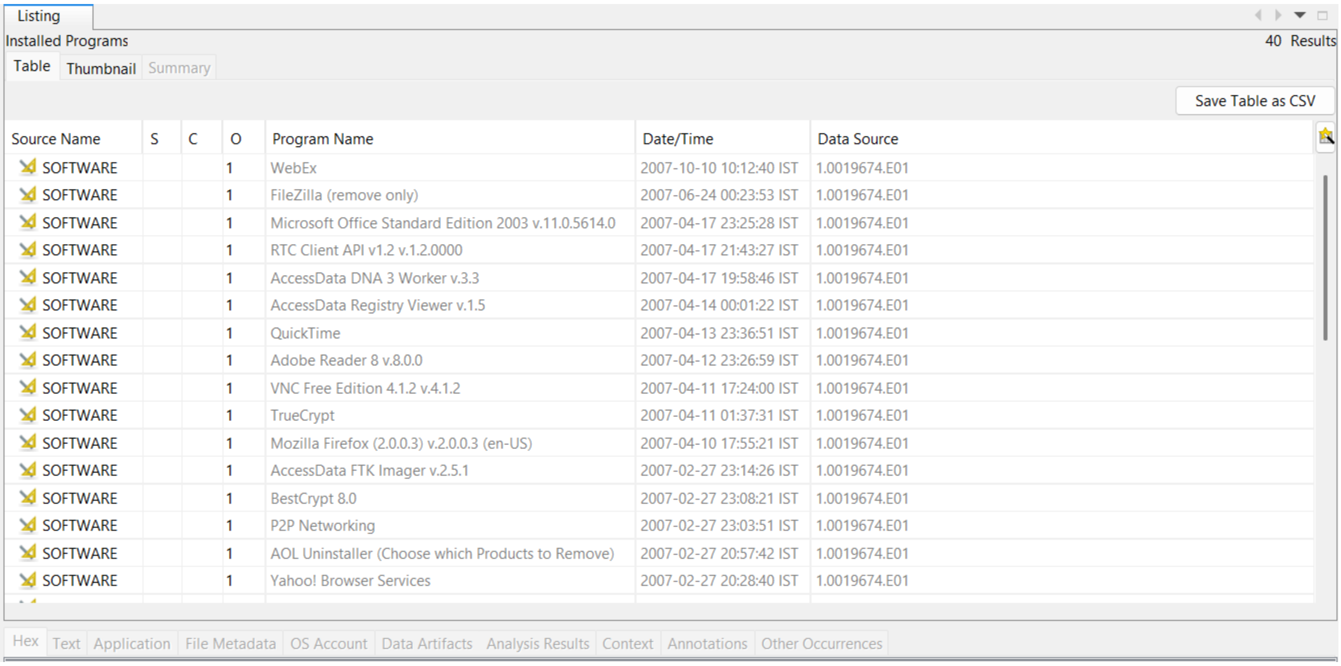
Autopsy accepts E.01 File Formats images. In this case, we will analyze an E.01 image file generated from evidence master copy.

### 6.7.2 List of Deleted Files



| Name | S | C | O | Modified Time | Change Time | Access Time | Created Time | Size | Flag |
|---|---|---|---|---|---|---|---|---|---|
| ~msdt | | | | 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 | Unall |
| {FD951CD4-4600-4F32-83D4-AEA3E504D900} | | | | 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 | Unall |
| zh-TW | | | | 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 | Unall |
| zh-TW | | | | 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 | Unall |
| zh-HK | | | | 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 | Unall |
| zh-CN | | | | 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 | Unall |
| woman.jpg-slack | | | | 2007-07-26 05:11:23 IST | 2007-08-04 21:34:29 IST | 2007-07-26 05:11:11 IST | 2007-07-26 05:11:11 IST | 156 | Unall |
| woman.jpg | | | | 2007-07-26 05:11:23 IST | 2007-08-04 21:34:29 IST | 2007-07-26 05:11:11 IST | 2007-07-26 05:11:11 IST | 11620 | Unall |
| winsxs | | | | 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 | Unall |
| winsxs | | | | 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 | Unall |
| winrm | | | | 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 | Unall |
| winevt | | | | 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 | Unall |
| winevt | | | | 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 | Unall |
| wfp | | | | 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 | Unall |
| wes_mantooth@pgp[2].txt | ▽ | | | 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 | Unall |
| whem | | | | 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 | Unall |

### 6.7.3 List of Installed Software in Suspect’s System

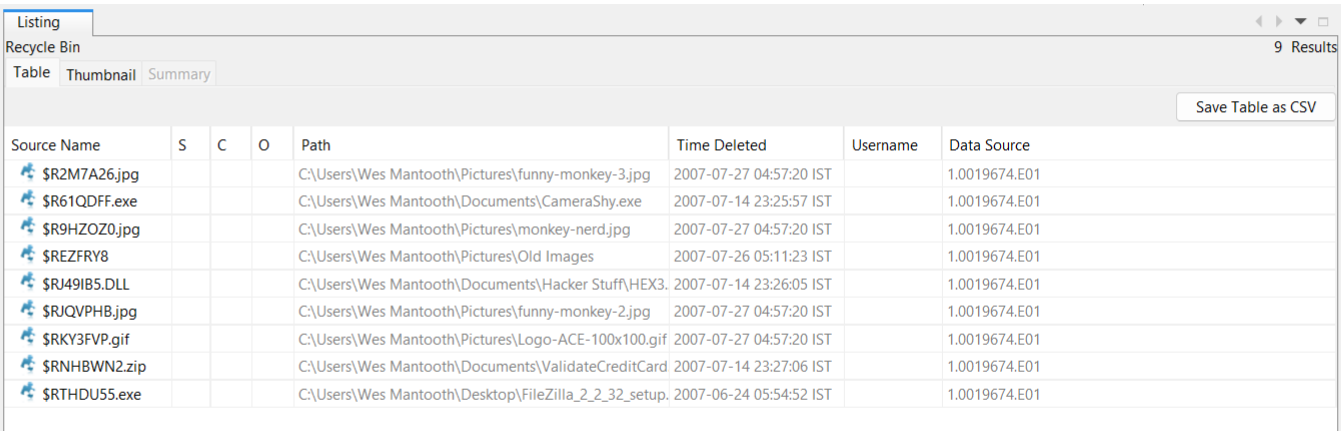


Installed Programs

40 Results

| Source Name | S | C | O | Program Name | Date/Time | Data Source |
|---|---|---|---|---|---|---|
| SOFTWARE | | | 1 | WebEx | 2007-10-10 10:12:40 IST | 1.0019674.E01 |
| SOFTWARE | | | 1 | FileZilla (remove only) | 2007-06-24 00:23:53 IST | 1.0019674.E01 |
| SOFTWARE | | | 1 | Microsoft Office Standard Edition 2003 v.11.0.5614.0 | 2007-04-17 23:25:28 IST | 1.0019674.E01 |
| SOFTWARE | | | 1 | RTC Client API v1.2 v.1.2.0000 | 2007-04-17 21:43:27 IST | 1.0019674.E01 |
| SOFTWARE | | | 1 | AccessData DNA 3 Worker v.3.3 | 2007-04-17 19:58:46 IST | 1.0019674.E01 |
| SOFTWARE | | | 1 | AccessData Registry Viewer v.1.5 | 2007-04-14 00:01:22 IST | 1.0019674.E01 |
| SOFTWARE | | | 1 | QuickTime | 2007-04-13 23:36:51 IST | 1.0019674.E01 |
| SOFTWARE | | | 1 | Adobe Reader 8 v.8.0.0 | 2007-04-12 23:26:59 IST | 1.0019674.E01 |
| SOFTWARE | | | 1 | VNC Free Edition 4.1.2 v.4.1.2 | 2007-04-11 17:24:00 IST | 1.0019674.E01 |
| SOFTWARE | | | 1 | TrueCrypt | 2007-04-11 01:37:31 IST | 1.0019674.E01 |
| SOFTWARE | | | 1 | Mozilla Firefox (2.0.0.3) v.2.0.0.3 (en-US) | 2007-04-10 17:55:21 IST | 1.0019674.E01 |
| SOFTWARE | | | 1 | AccessData FTK Imager v.2.5.1 | 2007-02-27 23:14:26 IST | 1.0019674.E01 |
| SOFTWARE | | | 1 | BestCrypt 8.0 | 2007-02-27 23:08:21 IST | 1.0019674.E01 |
| SOFTWARE | | | 1 | P2P Networking | 2007-02-27 23:03:51 IST | 1.0019674.E01 |
| SOFTWARE | | | 1 | AOL Uninstaller (Choose which Products to Remove) | 2007-02-27 20:57:42 IST | 1.0019674.E01 |
| SOFTWARE | | | 1 | Yahoo! Browser Services | 2007-02-27 20:28:40 IST | 1.0019674.E01 |

## 6.7.4 List of deleted items

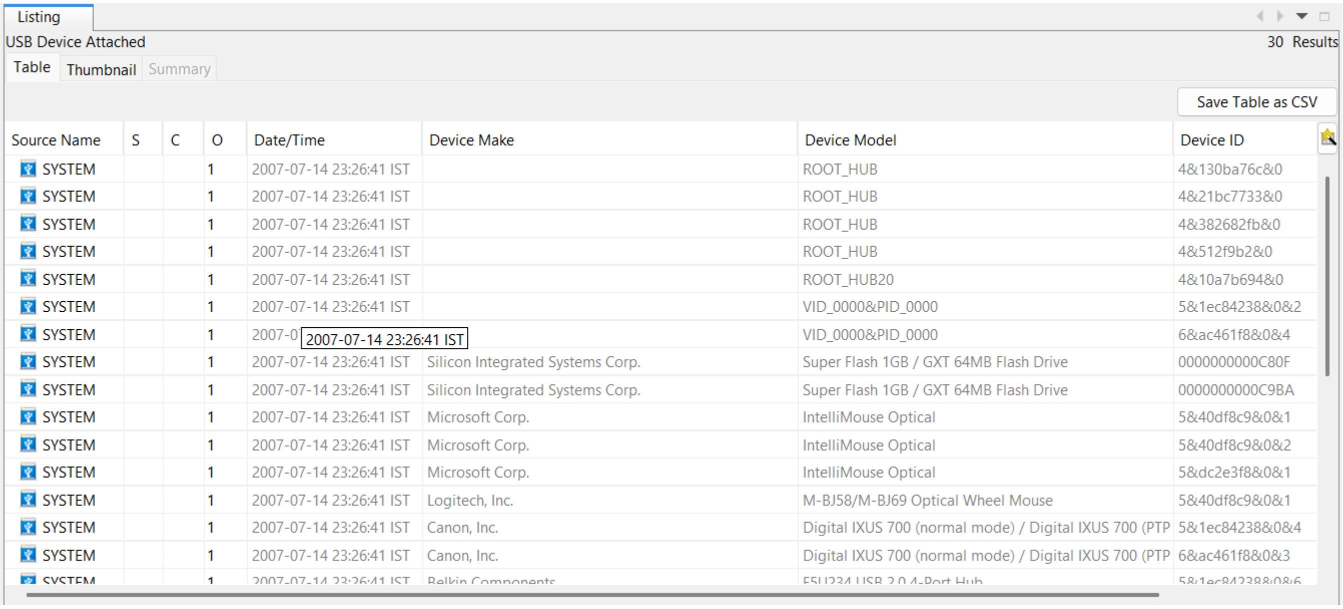


Recycle Bin

9 Results

| Source Name | S | C | O | Path | Time Deleted | Username | Data Source |
|---|---|---|---|---|---|---|---|
| $R2M7A26.jpg | | | | C:\Users\Wes Mantooth\Pictures\funny-monkey-3.jpg | 2007-07-27 04:57:20 IST | | 1.0019674.E01 |
| $R61QDFF.exe | | | | C:\Users\Wes Mantooth\Documents\CameraShy.exe | 2007-07-14 23:25:57 IST | | 1.0019674.E01 |
| $R9HZOZ0.jpg | | | | C:\Users\Wes Mantooth\Pictures\monkey-nerd.jpg | 2007-07-27 04:57:20 IST | | 1.0019674.E01 |
| $REZFRY8 | | | | C:\Users\Wes Mantooth\Pictures\Old Images | 2007-07-26 05:11:23 IST | | 1.0019674.E01 |
| $RJ49IB5.DLL | | | | C:\Users\Wes Mantooth\Documents\Hacker Stuff\HEX3. | 2007-07-14 23:26:05 IST | | 1.0019674.E01 |
| $RJQVPHB.jpg | | | | C:\Users\Wes Mantooth\Pictures\funny-monkey-2.jpg | 2007-07-27 04:57:20 IST | | 1.0019674.E01 |
| $RKY3FVP.gif | | | | C:\Users\Wes Mantooth\Pictures\Logo-ACE-100x100.gif | 2007-07-27 04:57:20 IST | | 1.0019674.E01 |
| $RNHBWN2.zip | | | | C:\Users\Wes Mantooth\Documents\ValidateCreditCard | 2007-07-14 23:27:06 IST | | 1.0019674.E01 |
| $RTHDU55.exe | | | | C:\Users\Wes Mantooth\Desktop\FileZilla_2_2_32_setup. | 2007-06-24 05:54:52 IST | | 1.0019674.E01 |

## 6.7.5 List of USB Devices Attached

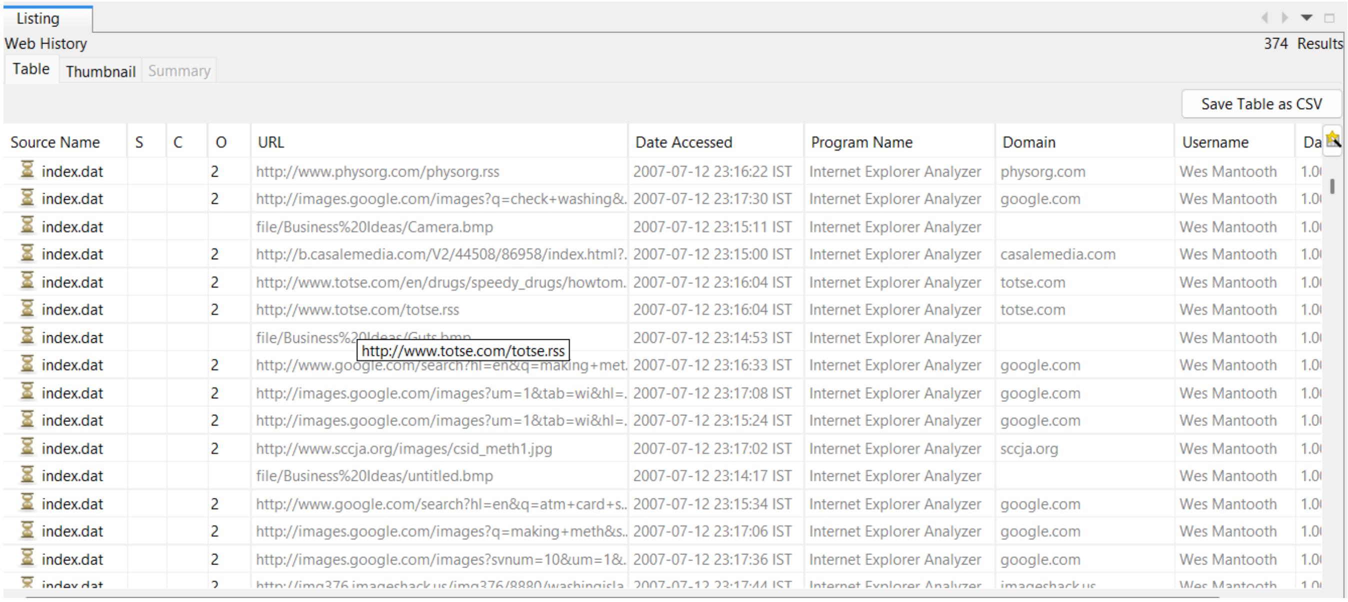


USB Device Attached

30 Results

| Source Name | S | C | O | Date/Time | Device Make | Device Model | Device ID |
|---|---|---|---|---|---|---|---|
| SYSTEM | | | 1 | 2007-07-14 23:26:41 IST | | ROOT_HUB | 4&130ba76c&0 |
| SYSTEM | | | 1 | 2007-07-14 23:26:41 IST | | ROOT_HUB | 4&21bc7733&0 |
| SYSTEM | | | 1 | 2007-07-14 23:26:41 IST | | ROOT_HUB | 4&382682fb&0 |
| SYSTEM | | | 1 | 2007-07-14 23:26:41 IST | | ROOT_HUB | 4&512f9b2&0 |
| SYSTEM | | | 1 | 2007-07-14 23:26:41 IST | | ROOT_HUB20 | 4&10a7b694&0 |
| SYSTEM | | | 1 | 2007-07-14 23:26:41 IST | | VID_0000&PID_0000 | 5&1ec84238&0&2 |
| SYSTEM | | | 1 | 2007-07-14 23:26:41 IST | | VID_0000&PID_0000 | 6&ac461f8&0&4 |
| SYSTEM | | | 1 | 2007-07-14 23:26:41 IST | Silicon Integrated Systems Corp. | Super Flash 1GB / GXT 64MB Flash Drive | 000000000C80F |
| SYSTEM | | | 1 | 2007-07-14 23:26:41 IST | Silicon Integrated Systems Corp. | Super Flash 1GB / GXT 64MB Flash Drive | 000000000C9BA |
| SYSTEM | | | 1 | 2007-07-14 23:26:41 IST | Microsoft Corp. | IntelliMouse Optical | 5&40df8c9&0&1 |
| SYSTEM | | | 1 | 2007-07-14 23:26:41 IST | Microsoft Corp. | IntelliMouse Optical | 5&40df8c9&0&2 |
| SYSTEM | | | 1 | 2007-07-14 23:26:41 IST | Microsoft Corp. | IntelliMouse Optical | 5&dc2e3f8&0&1 |
| SYSTEM | | | 1 | 2007-07-14 23:26:41 IST | Logitech, Inc. | M-BJ58/M-BJ69 Optical Wheel Mouse | 5&40df8c9&0&1 |
| SYSTEM | | | 1 | 2007-07-14 23:26:41 IST | Canon, Inc. | Digital IXUS 700 (normal mode) / Digital IXUS 700 (PTP | 5&1ec84238&0&4 |
| SYSTEM | | | 1 | 2007-07-14 23:26:41 IST | Canon, Inc. | Digital IXUS 700 (normal mode) / Digital IXUS 700 (PTP | 6&ac461f8&0&3 |
| SYSTEM | | | 1 | 2007-07-14 23:26:41 IST | Belkin Components | F5U234 USB 2.0 4-Port Hub | 5&1ec84238&0&6 |

## 6.7.6 Web browsing history of suspect

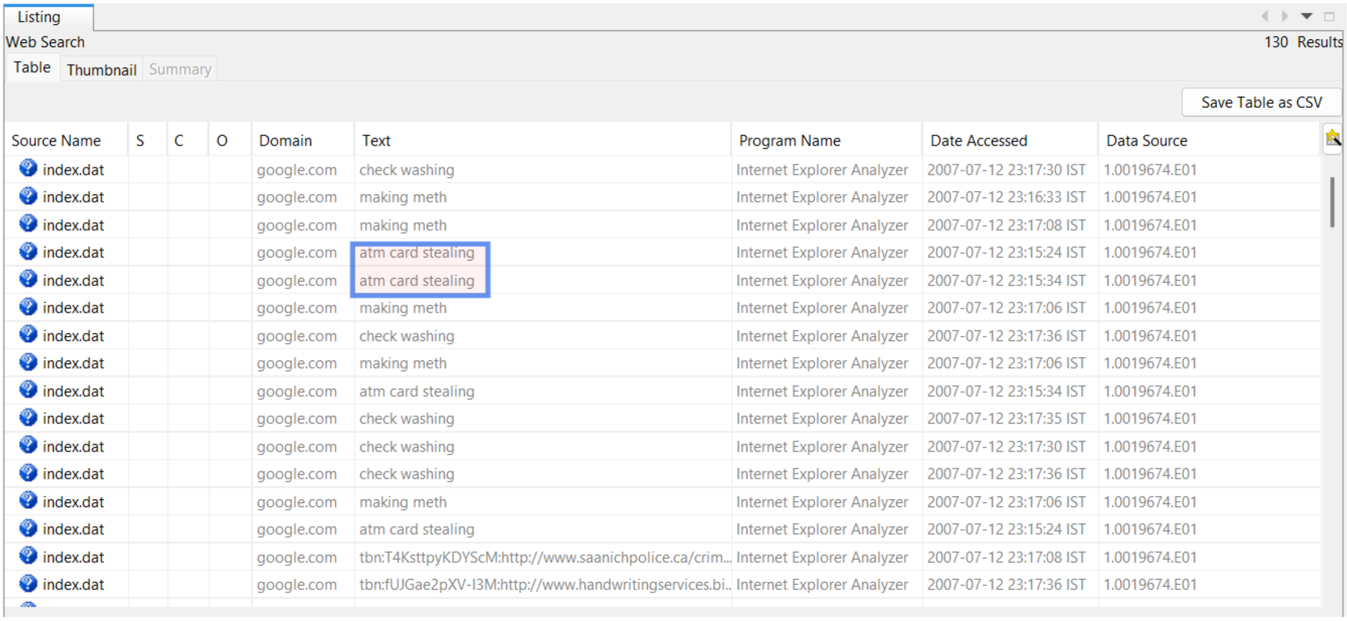


Web History

374 Results

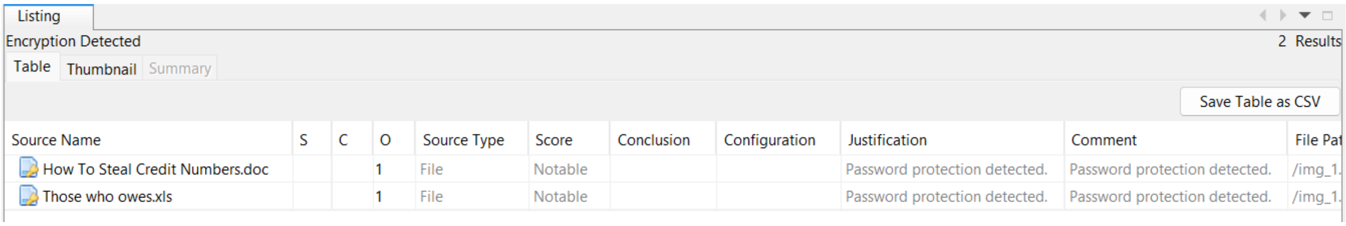
| Source Name | S | C | O | URL | Date Accessed | Program Name | Domain | Username | Da |
|---|---|---|---|---|---|---|---|---|---|
| index.dat | | | 2 | http://www.physorg.com/physorg.rss | 2007-07-12 23:16:22 IST | Internet Explorer Analyzer | physorg.com | Wes Mantooth | 1.0 |
| index.dat | | | 2 | http://images.google.com/images?q=check+washing&. | 2007-07-12 23:17:30 IST | Internet Explorer Analyzer | google.com | Wes Mantooth | 1.0 |
| index.dat | | | | file/Business%20Ideas/Camera.bmp | 2007-07-12 23:15:11 IST | Internet Explorer Analyzer | | Wes Mantooth | 1.0 |
| index.dat | | | 2 | http://b.casalemedia.com/V2/44508/86958/index.html?. | 2007-07-12 23:15:00 IST | Internet Explorer Analyzer | casalemedia.com | Wes Mantooth | 1.0 |
| index.dat | | | 2 | http://www.totse.com/en/drugs/speedy_drugs/howtom. | 2007-07-12 23:16:04 IST | Internet Explorer Analyzer | totse.com | Wes Mantooth | 1.0 |
| index.dat | | | 2 | http://www.totse.com/totse.rss | 2007-07-12 23:16:04 IST | Internet Explorer Analyzer | totse.com | Wes Mantooth | 1.0 |
| index.dat | | | | file/Business%20Ideas/Guts.bmp | 2007-07-12 23:14:53 IST | Internet Explorer Analyzer | | Wes Mantooth | 1.0 |
| index.dat | | | 2 | http://www.google.com/search?hl=en&q=making+met. | 2007-07-12 23:16:33 IST | Internet Explorer Analyzer | google.com | Wes Mantooth | 1.0 |
| index.dat | | | 2 | http://images.google.com/images?um=1&tab=wi&hl=. | 2007-07-12 23:17:08 IST | Internet Explorer Analyzer | google.com | Wes Mantooth | 1.0 |
| index.dat | | | 2 | http://images.google.com/images?um=1&tab=wi&hl=. | 2007-07-12 23:15:24 IST | Internet Explorer Analyzer | google.com | Wes Mantooth | 1.0 |
| index.dat | | | 2 | http://www.sccja.org/images/csid_meth1.jpg | 2007-07-12 23:17:02 IST | Internet Explorer Analyzer | sccja.org | Wes Mantooth | 1.0 |
| index.dat | | | | file/Business%20Ideas/untitled.bmp | 2007-07-12 23:14:17 IST | Internet Explorer Analyzer | | Wes Mantooth | 1.0 |
| index.dat | | | 2 | http://www.google.com/search?hl=en&q=atm+card+s.. | 2007-07-12 23:15:34 IST | Internet Explorer Analyzer | google.com | Wes Mantooth | 1.0 |
| index.dat | | | 2 | http://images.google.com/images?q=making+meth&s.. | 2007-07-12 23:17:06 IST | Internet Explorer Analyzer | google.com | Wes Mantooth | 1.0 |
| index.dat | | | 2 | http://images.google.com/images?svnum=10&um=1&. | 2007-07-12 23:17:36 IST | Internet Explorer Analyzer | google.com | Wes Mantooth | 1.0 |
| index.dat | | | 2 | http://img376.imageshack.us/img376/8880/washingisla | 2007-07-12 23:17:44 IST | Internet Explorer Analyzer | imageshack.us | Wes Mantooth | 1.0 |

## 6.7.7 Web Search history of suspect



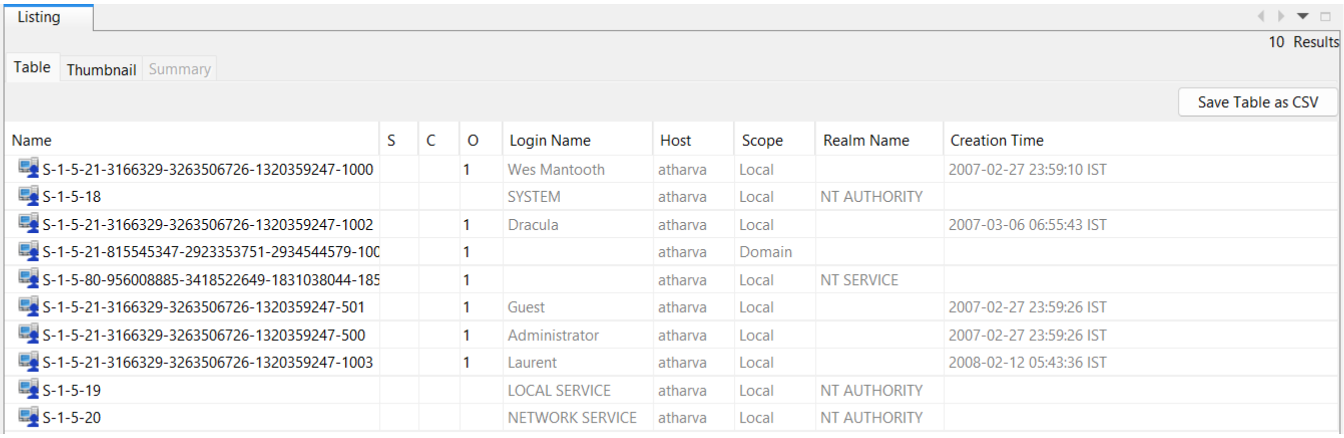
| Source Name | S | C | O | Domain | Text | Program Name | Date Accessed | Data Source |
|---|---|---|---|---|---|---|---|---|
| index.dat | | | | google.com | check washing | Internet Explorer Analyzer | 2007-07-12 23:17:30 IST | 1.0019674.E01 |
| index.dat | | | | google.com | making meth | Internet Explorer Analyzer | 2007-07-12 23:16:33 IST | 1.0019674.E01 |
| index.dat | | | | google.com | making meth | Internet Explorer Analyzer | 2007-07-12 23:17:08 IST | 1.0019674.E01 |
| index.dat | | | | google.com | atm card stealing | Internet Explorer Analyzer | 2007-07-12 23:15:24 IST | 1.0019674.E01 |
| index.dat | | | | google.com | atm card stealing | Internet Explorer Analyzer | 2007-07-12 23:15:34 IST | 1.0019674.E01 |
| index.dat | | | | google.com | making meth | Internet Explorer Analyzer | 2007-07-12 23:17:06 IST | 1.0019674.E01 |
| index.dat | | | | google.com | check washing | Internet Explorer Analyzer | 2007-07-12 23:17:36 IST | 1.0019674.E01 |
| index.dat | | | | google.com | making meth | Internet Explorer Analyzer | 2007-07-12 23:17:06 IST | 1.0019674.E01 |
| index.dat | | | | google.com | atm card stealing | Internet Explorer Analyzer | 2007-07-12 23:15:34 IST | 1.0019674.E01 |
| index.dat | | | | google.com | check washing | Internet Explorer Analyzer | 2007-07-12 23:17:35 IST | 1.0019674.E01 |
| index.dat | | | | google.com | check washing | Internet Explorer Analyzer | 2007-07-12 23:17:30 IST | 1.0019674.E01 |
| index.dat | | | | google.com | check washing | Internet Explorer Analyzer | 2007-07-12 23:17:36 IST | 1.0019674.E01 |
| index.dat | | | | google.com | making meth | Internet Explorer Analyzer | 2007-07-12 23:17:06 IST | 1.0019674.E01 |
| index.dat | | | | google.com | atm card stealing | Internet Explorer Analyzer | 2007-07-12 23:15:24 IST | 1.0019674.E01 |
| index.dat | | | | google.com | tbn:T4KsttpyKDYScM:http://www.saanichpolice.ca/crim... | Internet Explorer Analyzer | 2007-07-12 23:17:08 IST | 1.0019674.E01 |
| index.dat | | | | google.com | tbn:fUJGae2pXV-I3M:http://www.handwritingservices.bi.. | Internet Explorer Analyzer | 2007-07-12 23:17:36 IST | 1.0019674.E01 |

### 6.7.8 List of Encrypted Data Found



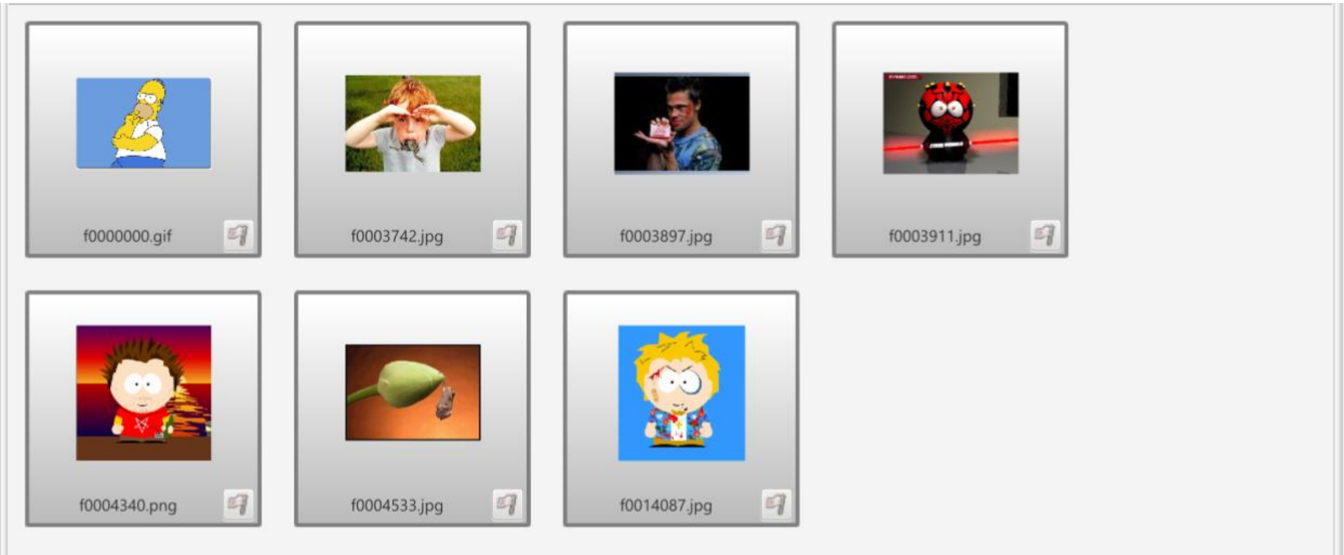
| Source Name | S | C | O | Source Type | Score | Conclusion | Configuration | Justification | Comment | File Pat |
|---|---|---|---|---|---|---|---|---|---|---|
| How To Steal Credit Numbers.doc | | | 1 | File | Notable | | | Password protection detected. | Password protection detected. | /img_1. |
| Those who owes.xls | | | 1 | File | Notable | | | Password protection detected. | Password protection detected. | /img_1. |

### 6.7.9 OS Account Details of Suspect

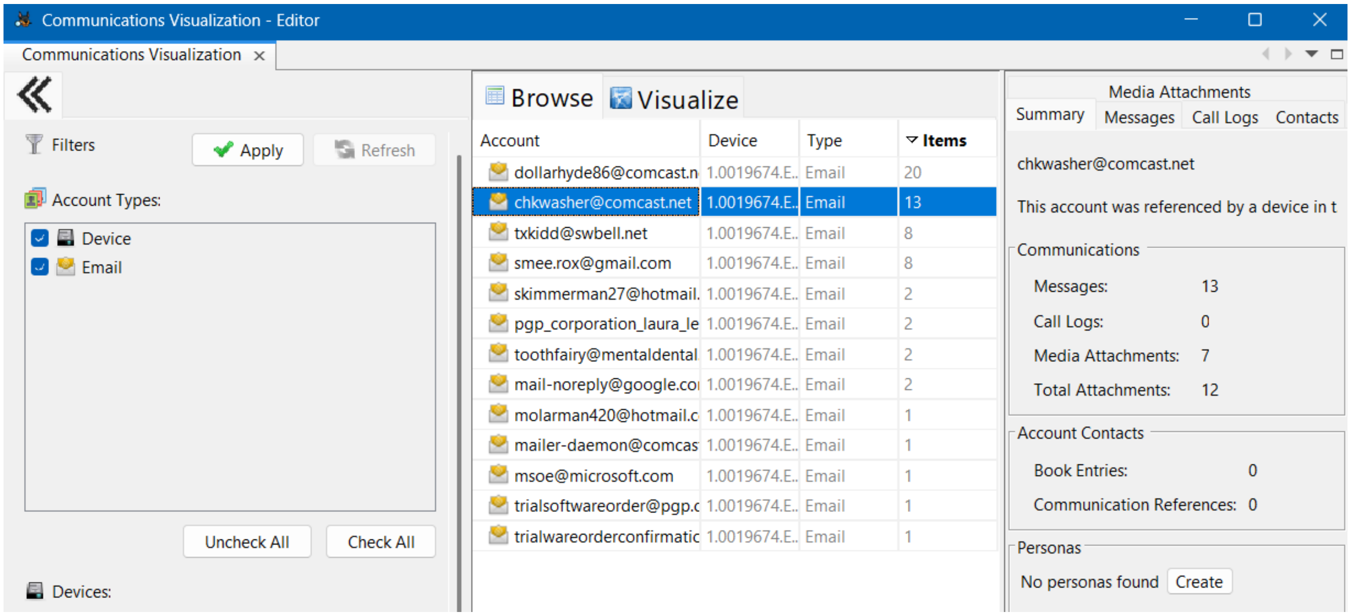


| Name | S | C | O | Login Name | Host | Scope | Realm Name | Creation Time |
|---|---|---|---|---|---|---|---|---|
| S-1-5-21-3166329-3263506726-1320359247-1000 | | | 1 | Wes Mantooth | atharva | Local | | 2007-02-27 23:59:10 IST |
| S-1-5-18 | | | | SYSTEM | atharva | Local | NT AUTHORITY | |
| S-1-5-21-3166329-3263506726-1320359247-1002 | | | 1 | Dracula | atharva | Local | | 2007-03-06 06:55:43 IST |
| S-1-5-21-815545347-2923353751-2934544579-100 | | | 1 | | atharva | Domain | | |
| S-1-5-80-956008885-3418522649-1831038044-185 | | | 1 | | atharva | Local | NT SERVICE | |
| S-1-5-21-3166329-3263506726-1320359247-501 | | | 1 | Guest | atharva | Local | | 2007-02-27 23:59:26 IST |
| S-1-5-21-3166329-3263506726-1320359247-500 | | | 1 | Administrator | atharva | Local | | 2007-02-27 23:59:26 IST |
| S-1-5-21-3166329-3263506726-1320359247-1003 | | | 1 | Laurent | atharva | Local | | 2008-02-12 05:43:36 IST |
| S-1-5-19 | | | | LOCAL SERVICE | atharva | Local | NT AUTHORITY | |
| S-1-5-20 | | | | NETWORK SERVICE | atharva | Local | NT AUTHORITY | |

### 6.7.10 Images Recovered



### 6.7.11 Emails Recovered



Account Types:

☑ Device

☑ Email

Devices:

| Account | Device | Type | Items |
|---|---|---|---|
| dollarhyde86@comcast.n | 1.0019674.E.. | Email | 20 |
| chkwasher@comcast.net | 1.0019674.E.. | Email | 13 |
| txkidd@swbell.net | 1.0019674.E.. | Email | 8 |
| smee.rox@gmail.com | 1.0019674.E.. | Email | 8 |
| skimmerman27@hotmail. | 1.0019674.E.. | Email | 2 |
| pgp_corporation_laura_le | 1.0019674.E.. | Email | 2 |
| toothfairy@mentaldental | 1.0019674.E.. | Email | 2 |
| mail-noreply@google.coı | 1.0019674.E.. | Email | 2 |
| molarman420@hotmail.c | 1.0019674.E.. | Email | 1 |
| mailer-daemon@comcas | 1.0019674.E.. | Email | 1 |
| msoe@microsoft.com | 1.0019674.E.. | Email | 1 |
| trialsoftwareorder@pgp.c | 1.0019674.E.. | Email | 1 |
| trialwareorderconfirmatic | 1.0019674.E.. | Email | 1 |

chkwasher@comcast.net

This account was referenced by a device in t

Communications

| | |
|---|---|
| Messages: | 13 |
| Call Logs: | 0 |
| Media Attachments: | 7 |
| Total Attachments: | 12 |

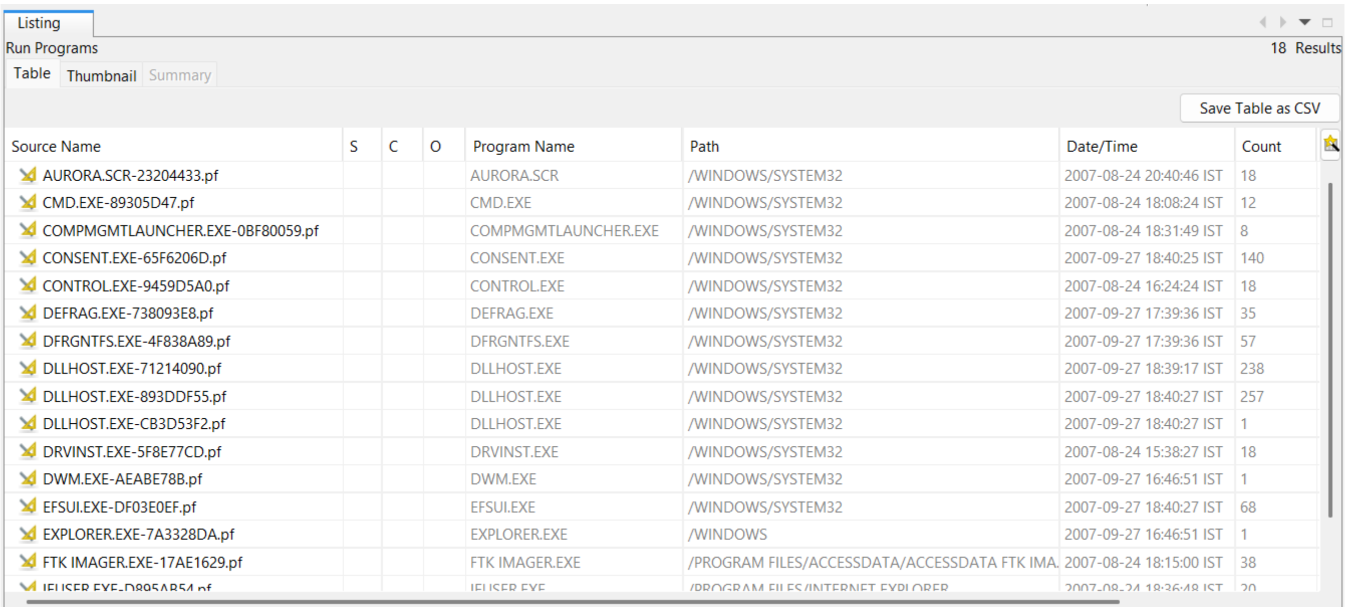
Account Contacts

| | |
|---|---|
| Book Entries: | 0 |
| Communication References: | 0 |

Personas

No personas found

### 6.7.12 List of Programs and Processes running

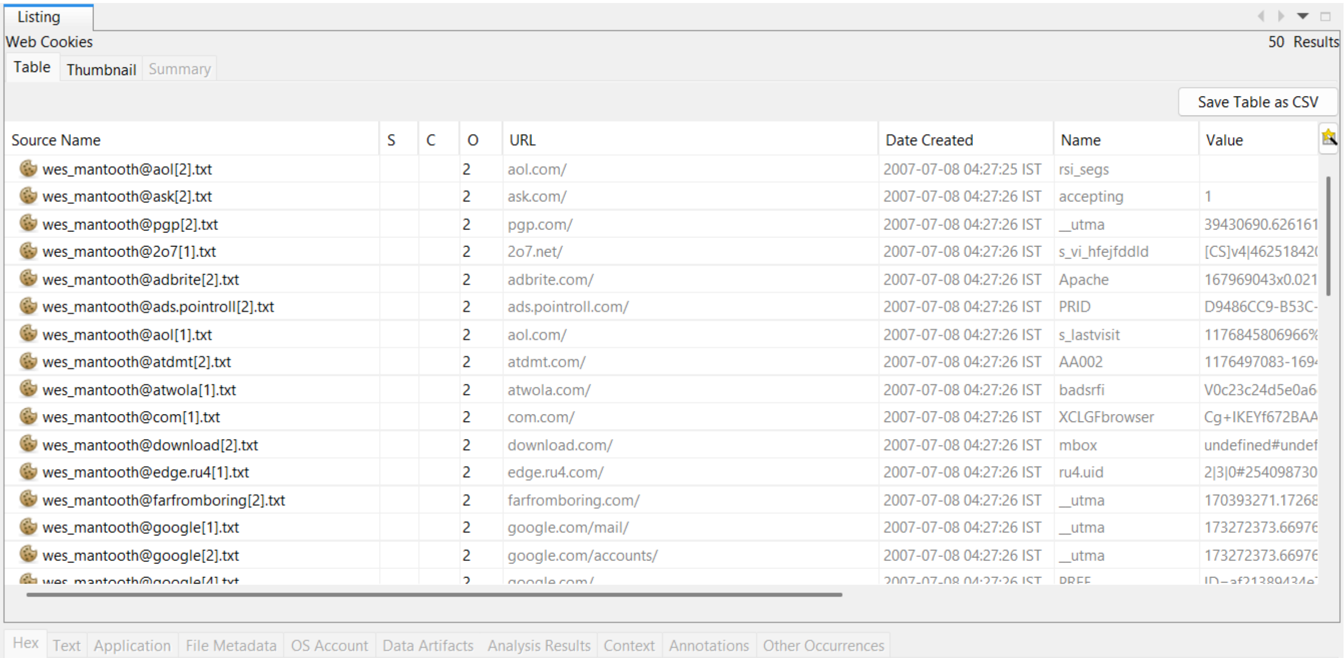


Run Programs

18 Results

| Source Name | S | C | O | Program Name | Path | Date/Time | Count |
|---|---|---|---|---|---|---|---|
| AURORA.SCR-23204433.pf | | | | AURORA.SCR | /WINDOWS/SYSTEM32 | 2007-08-24 20:40:46 IST | 18 |
| CMD.EXE-89305D47.pf | | | | CMD.EXE | /WINDOWS/SYSTEM32 | 2007-08-24 18:08:24 IST | 12 |
| COMPMGMTLAUNCHER.EXE-0BF80059.pf | | | | COMPMGMTLAUNCHER.EXE | /WINDOWS/SYSTEM32 | 2007-08-24 18:31:49 IST | 8 |
| CONSENT.EXE-65F6206D.pf | | | | CONSENT.EXE | /WINDOWS/SYSTEM32 | 2007-09-27 18:40:25 IST | 140 |
| CONTROL.EXE-9459D5A0.pf | | | | CONTROL.EXE | /WINDOWS/SYSTEM32 | 2007-08-24 16:24:24 IST | 18 |
| DEFRAG.EXE-738093E8.pf | | | | DEFRAG.EXE | /WINDOWS/SYSTEM32 | 2007-09-27 17:39:36 IST | 35 |
| DFRGNTFS.EXE-4F838A89.pf | | | | DFRGNTFS.EXE | /WINDOWS/SYSTEM32 | 2007-09-27 17:39:36 IST | 57 |
| DLLHOST.EXE-71214090.pf | | | | DLLHOST.EXE | /WINDOWS/SYSTEM32 | 2007-09-27 18:39:17 IST | 238 |
| DLLHOST.EXE-893DDF55.pf | | | | DLLHOST.EXE | /WINDOWS/SYSTEM32 | 2007-09-27 18:40:27 IST | 257 |
| DLLHOST.EXE-CB3D53F2.pf | | | | DLLHOST.EXE | /WINDOWS/SYSTEM32 | 2007-09-27 18:40:27 IST | 1 |
| DRVINST.EXE-5F8E77CD.pf | | | | DRVINST.EXE | /WINDOWS/SYSTEM32 | 2007-08-24 15:38:27 IST | 18 |
| DWM.EXE-AEABE78B.pf | | | | DWM.EXE | /WINDOWS/SYSTEM32 | 2007-09-27 16:46:51 IST | 1 |
| EFSUI.EXE-DF03E0EF.pf | | | | EFSUI.EXE | /WINDOWS/SYSTEM32 | 2007-09-27 18:40:27 IST | 68 |
| EXPLORER.EXE-7A3328DA.pf | | | | EXPLORER.EXE | /WINDOWS | 2007-09-27 16:46:51 IST | 1 |
| FTK IMAGER.EXE-17AE1629.pf | | | | FTK IMAGER.EXE | /PROGRAM FILES/ACCESSDATA/ACCESSDATA FTK IMA. | 2007-08-24 18:15:00 IST | 38 |
| IEUSER.EXE-D895AB54.pf | | | | IEUSER.EXE | /PROGRAM FILES/INTERNET EXPLORER | 2007-08-24 18:36:48 IST | 20 |

### 6.7.13 List of Web Cookies

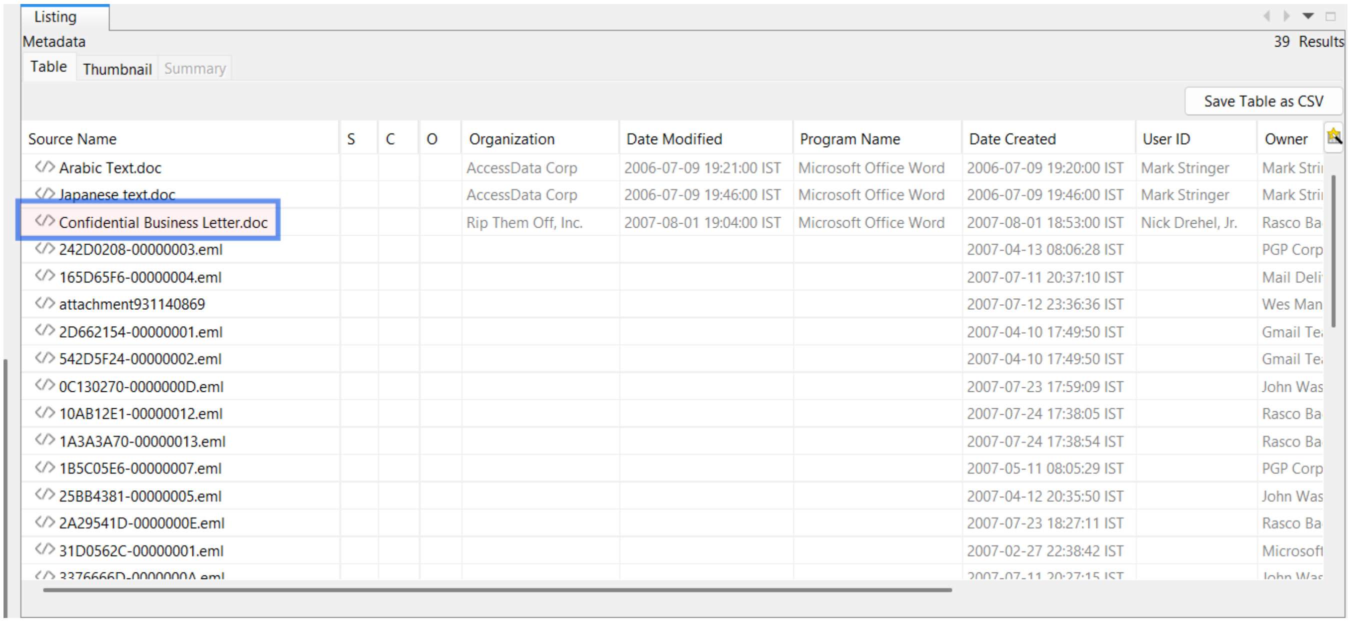


Web Cookies

50 Results

| Source Name | S | C | O | URL | Date Created | Name | Value |
|---|---|---|---|---|---|---|---|
| wes_mantooth@aol[2].txt | | | 2 | aol.com/ | 2007-07-08 04:27:25 IST | rsi_segs | |
| wes_mantooth@ask[2].txt | | | 2 | ask.com/ | 2007-07-08 04:27:26 IST | accepting | 1 |
| wes_mantooth@pgp[2].txt | | | 2 | pgp.com/ | 2007-07-08 04:27:26 IST | __utma | 39430690.626161 |
| wes_mantooth@2o7[1].txt | | | 2 | 2o7.net/ | 2007-07-08 04:27:26 IST | s_vi_hfejfddld | [CS]v4\|46251842( |
| wes_mantooth@adbrite[2].txt | | | 2 | adbrite.com/ | 2007-07-08 04:27:26 IST | Apache | 167969043x0.021 |
| wes_mantooth@ads.pointroll[2].txt | | | 2 | ads.pointroll.com/ | 2007-07-08 04:27:26 IST | PRID | D9486CC9-B53C- |
| wes_mantooth@aol[1].txt | | | 2 | aol.com/ | 2007-07-08 04:27:26 IST | s_lastvisit | 1176845806966% |
| wes_mantooth@atdmt[2].txt | | | 2 | atdmt.com/ | 2007-07-08 04:27:26 IST | AA002 | 1176497083-169 |
| wes_mantooth@atwola[1].txt | | | 2 | atwola.com/ | 2007-07-08 04:27:26 IST | badsrfi | V0c23c24d5e0a6 |
| wes_mantooth@com[1].txt | | | 2 | com.com/ | 2007-07-08 04:27:26 IST | XCLGFbrowser | Cg+IKEYf672BAA |
| wes_mantooth@download[2].txt | | | 2 | download.com/ | 2007-07-08 04:27:26 IST | mbox | undefined#undef |
| wes_mantooth@edge.ru4[1].txt | | | 2 | edge.ru4.com/ | 2007-07-08 04:27:26 IST | ru4.uid | 2\|3\|0#254098730 |
| wes_mantooth@farfromboring[2].txt | | | 2 | farfromboring.com/ | 2007-07-08 04:27:26 IST | __utma | 170393271.17268 |
| wes_mantooth@google[1].txt | | | 2 | google.com/mail/ | 2007-07-08 04:27:26 IST | __utma | 173272373.66976 |
| wes_mantooth@google[2].txt | | | 2 | google.com/accounts/ | 2007-07-08 04:27:26 IST | __utma | 173272373.66976 |
| wes_mantooth@google[4].txt | | | 2 | google.com/ | 2007-07-08 04:27:26 IST | PREF | ID=af21389434e |

## 6.7.14 Metadata

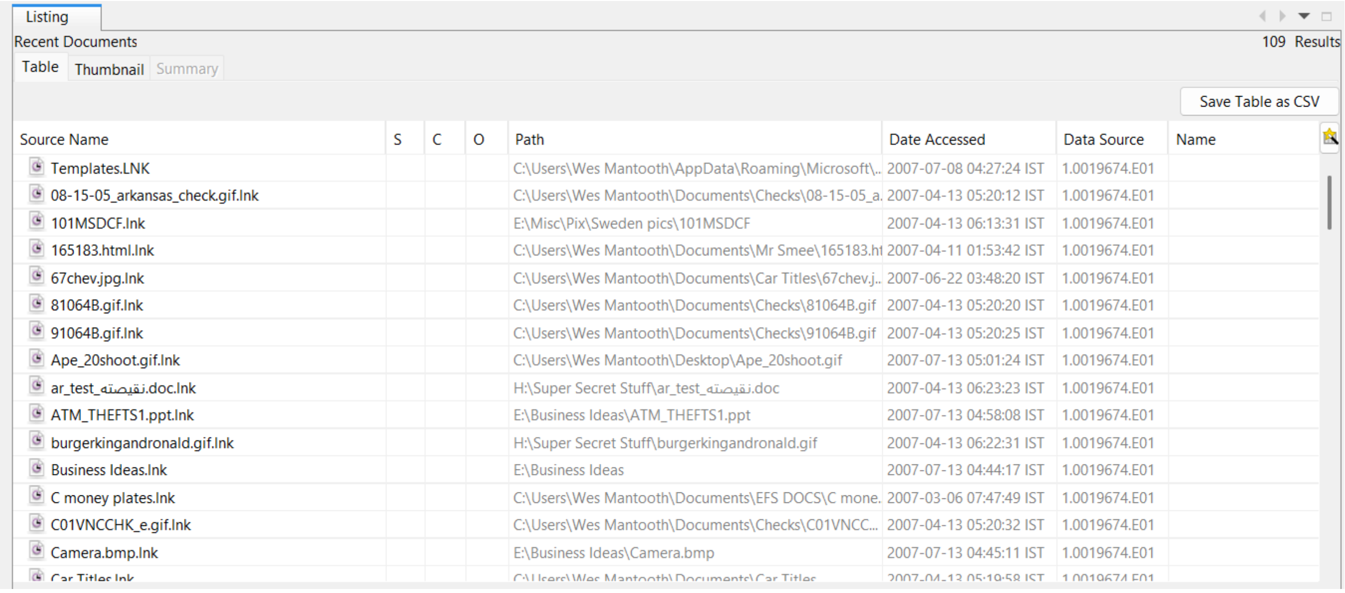


Metadata

39 Results

| Source Name | S | C | O | Organization | Date Modified | Program Name | Date Created | User ID | Owner |
|---|---|---|---|---|---|---|---|---|---|
| Arabic Text.doc | | | | AccessData Corp | 2006-07-09 19:21:00 IST | Microsoft Office Word | 2006-07-09 19:20:00 IST | Mark Stringer | Mark Stri |
| Japanese text.doc | | | | AccessData Corp | 2006-07-09 19:46:00 IST | Microsoft Office Word | 2006-07-09 19:46:00 IST | Mark Stringer | Mark Stri |
| Confidential Business Letter.doc | | | | Rip Them Off, Inc. | 2007-08-01 19:04:00 IST | Microsoft Office Word | 2007-08-01 18:53:00 IST | Nick Drehel, Jr. | Rasco Ba |
| 242D0208-00000003.eml | | | | | | | 2007-04-13 08:06:28 IST | | PGP Corp |
| 165D65F6-00000004.eml | | | | | | | 2007-07-11 20:37:10 IST | | Mail Deli |
| attachment931140869 | | | | | | | 2007-07-12 23:36:36 IST | | Wes Man |
| 2D662154-00000001.eml | | | | | | | 2007-04-10 17:49:50 IST | | Gmail Te |
| 542D5F24-00000002.eml | | | | | | | 2007-04-10 17:49:50 IST | | Gmail Te |
| 0C130270-0000000D.eml | | | | | | | 2007-07-23 17:59:09 IST | | John Was |
| 10AB12E1-00000012.eml | | | | | | | 2007-07-24 17:38:05 IST | | Rasco Ba |
| 1A3A3A70-00000013.eml | | | | | | | 2007-07-24 17:38:54 IST | | Rasco Ba |
| 1B5C05E6-00000007.eml | | | | | | | 2007-05-11 08:05:29 IST | | PGP Corp |
| 25BB4381-00000005.eml | | | | | | | 2007-04-12 20:35:50 IST | | John Was |
| 2A29541D-0000000E.eml | | | | | | | 2007-07-23 18:27:11 IST | | Rasco Ba |
| 31D0562C-00000001.eml | | | | | | | 2007-02-27 22:38:42 IST | | Microsoft |
| 3376666D-0000000A.eml | | | | | | | 2007-07-11 20:27:15 IST | | John Was |

## 6.7.15 Recent Documents Accessed



Recent Documents

109 Results

| Source Name | S | C | O | Path | Date Accessed | Data Source | Name |
|---|---|---|---|---|---|---|---|
| Templates.LNK | | | | C:\Users\Wes Mantooth\AppData\Roaming\Microsoft\.. | 2007-07-08 04:27:24 IST | 1.0019674.E01 | |
| 08-15-05_arkansas_check.gif.lnk | | | | C:\Users\Wes Mantooth\Documents\Checks\08-15-05_a. | 2007-04-13 05:20:12 IST | 1.0019674.E01 | |
| 101MSDCF.lnk | | | | E:\Misc\Pix\Sweden pics\101MSDCF | 2007-04-13 06:13:31 IST | 1.0019674.E01 | |
| 165183.html.lnk | | | | C:\Users\Wes Mantooth\Documents\Mr Smee\165183.ht | 2007-04-11 01:53:42 IST | 1.0019674.E01 | |
| 67chev.jpg.lnk | | | | C:\Users\Wes Mantooth\Documents\Car Titles\67chev.j.. | 2007-06-22 03:48:20 IST | 1.0019674.E01 | |
| 81064B.gif.lnk | | | | C:\Users\Wes Mantooth\Documents\Checks\81064B.gif | 2007-04-13 05:20:20 IST | 1.0019674.E01 | |
| 91064B.gif.lnk | | | | C:\Users\Wes Mantooth\Documents\Checks\91064B.gif | 2007-04-13 05:20:25 IST | 1.0019674.E01 | |
| Ape_20shoot.gif.lnk | | | | C:\Users\Wes Mantooth\Desktop\Ape_20shoot.gif | 2007-07-13 05:01:24 IST | 1.0019674.E01 | |
| ar_test_نقيصته.doc.lnk | | | | H:\Super Secret Stuff\ar_test_نقيصته.doc | 2007-04-13 06:23:23 IST | 1.0019674.E01 | |
| ATM_THEFTS1.ppt.lnk | | | | E:\Business Ideas\ATM_THEFTS1.ppt | 2007-07-13 04:58:08 IST | 1.0019674.E01 | |
| burgerkingandronald.gif.lnk | | | | H:\Super Secret Stuff\burgerkingandronald.gif | 2007-04-13 06:22:31 IST | 1.0019674.E01 | |
| Business Ideas.lnk | | | | E:\Business Ideas | 2007-07-13 04:44:17 IST | 1.0019674.E01 | |
| C money plates.lnk | | | | C:\Users\Wes Mantooth\Documents\EFS DOCS\C mone. | 2007-03-06 07:47:49 IST | 1.0019674.E01 | |
| C01VNCCHK_e.gif.lnk | | | | C:\Users\Wes Mantooth\Documents\Checks\C01VNCC... | 2007-04-13 05:20:32 IST | 1.0019674.E01 | |
| Camera.bmp.lnk | | | | E:\Business Ideas\Camera.bmp | 2007-07-13 04:45:11 IST | 1.0019674.E01 | |
| Car Titles.lnk | | | | C:\Users\Wes Mantooth\Documents\Car Titles | 2007-04-13 05:19:58 IST | 1.0019674.E01 | |

## 6.3 DRAFTING A COMPREHENSIVE FORENSIC REPORT

### 6.3.1 Drafting Reports based on previous case studies.

Reports are an integral part of any Forensic Investigation. A report documents and presents findings from a forensic investigation in a clear, structured, and legally admissible manner.

Importance of Documentation and Reporting

- Evidence Documentation – Provides a detailed account of digital evidence, ensuring integrity and authenticity.
- Legal Compliance – Helps in legal proceedings by adhering to forensic investigation standards.
- Incident Response – Aids organizations in understanding cyber incidents, identifying vulnerabilities, and preventing future attacks.
- Decision-Making – Supports law enforcement, corporate security teams, and courts in making informed decisions.
- Accountability & Transparency – Ensures a clear record of actions taken during an investigation, reducing the risk of disputes.

### 6.3.2 DFIR Report Writing Task

We were given a task to prepare Forensic Analysis reports based on past security incidents. I have followed Industry oriented format to prepare the report.

Link
https://drive.google.com/file/d/1orVZw2voNHpE7K8MCTPtq4Rb2XNQcyX/view?usp=drive_link

# CHAPTER: 7 CONCLUSION AND FUTURE WORK

# CHAPTER 7 CONCLUSION AND FUTURE WORK

## Conclusion

It was an amazing and exciting Internship where I gained immense technical exposure from chain chain of custody to analyzing image files. The company seniors were helpful and guidance resulted in the successful completion of this Internship.

## Future work

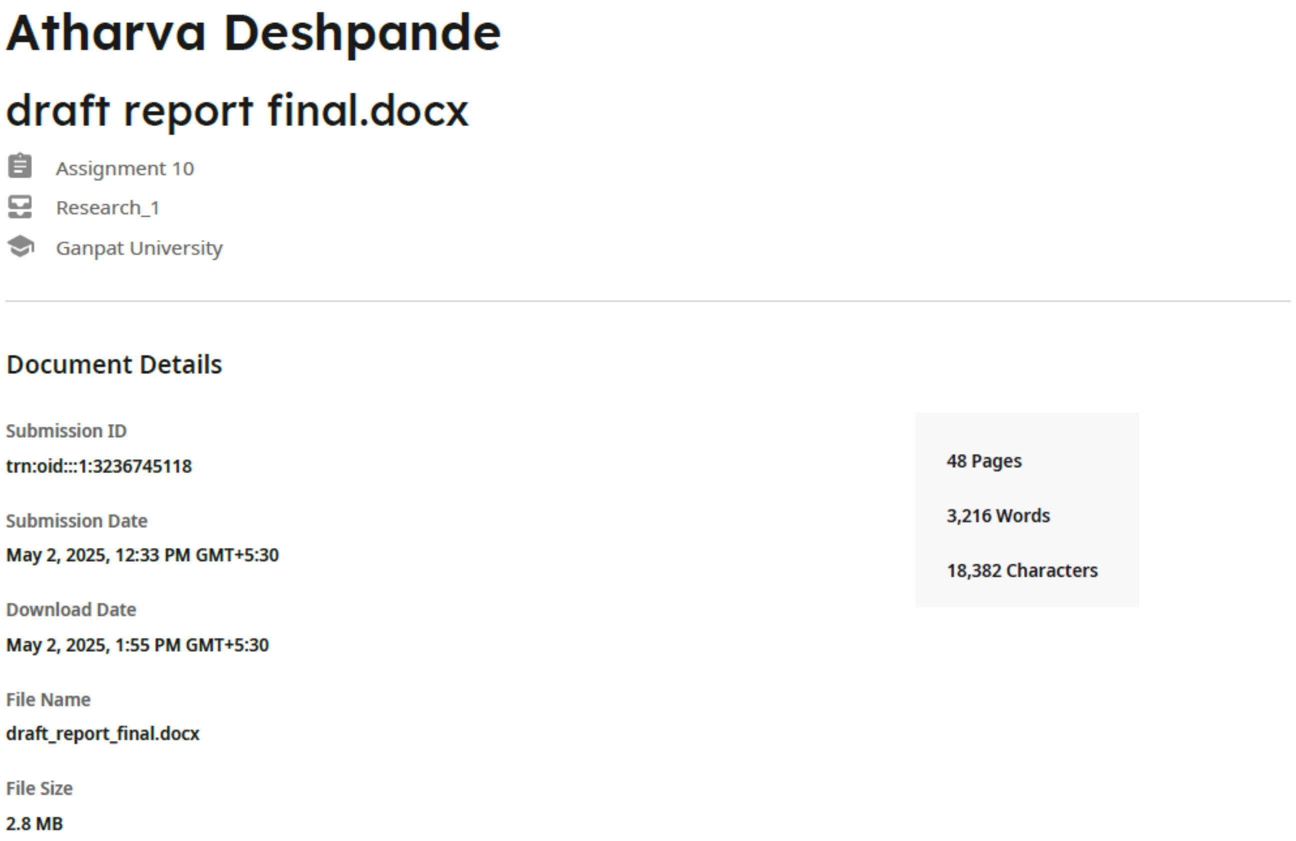
I am looking forward to work in this industry after gaining a handful of technical expertise. In addition, I also aspire in

- Assisting seniors in analysis of ram dump and digital device data.
- Solving Corporate cases (eg. Company Frauds)
- Preparing comprehensive reports after performing investigation.

# CHAPTER: 8 REFERENCES

# CHAPTER 8 REFERENCES

1) https://docs.google.com/document/d/1hr51ve1feKZzl3qpsUApXmbALOnnLsuuOHXJZZR37xw/edit?usp=sharing (Atharva, 2025)
2) https://www.ncbi.nlm.nih.gov/books/NBK551677 (Ashish , 2023)
3) Research Paper 1 : https://iajit.org/upload/files/Digital-Forensics-Techniques-and-Trends-A-Review.pdf (Himanshu Dubey, 2023)
4) Research Paper 2 : https://tijer.org/tijer/papers/TIJER2407038.pdf (Dr S Sarvanna, 2024)



# Atharva Deshpande

## draft report final.docx

Assignment 10

Research_1

Ganpat University

### Document Details

Submission ID

**trn:oid:::1:3236745118**

Submission Date

**May 2, 2025, 12:33 PM GMT+5:30**

Download Date

**May 2, 2025, 1:55 PM GMT+5:30**

File Name

**draft_report_final.docx**

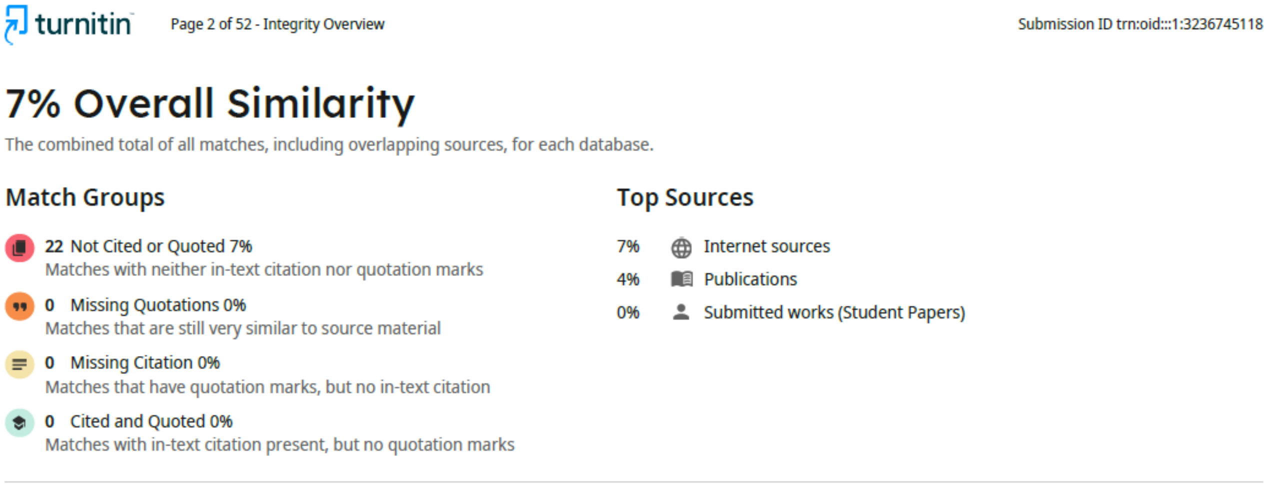
File Size

**2.8 MB**

**48 Pages**

**3,216 Words**

**18,382 Characters**



Page 2 of 52 - Integrity Overview

Submission ID trn:oid:::1:3236745118

## 7% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

### Match Groups

- 22 Not Cited or Quoted 7%
  Matches with neither in-text citation nor quotation marks
- 0 Missing Quotations 0%
  Matches that are still very similar to source material
- 0 Missing Citation 0%
  Matches that have quotation marks, but no in-text citation
- 0 Cited and Quoted 0%
  Matches with in-text citation present, but no quotation marks

### Top Sources

| | |
|---|---|
| 7% | Internet sources |
| 4% | Publications |
| 0% | Submitted works (Student Papers) |

# 7% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

## Match Groups

**22** Not Cited or Quoted 7%
Matches with neither in-text citation nor quotation marks

**0** Missing Quotations 0%
Matches that are still very similar to source material

**0** Missing Citation 0%
Matches that have quotation marks, but no in-text citation

**0** Cited and Quoted 0%
Matches with in-text citation present, but no quotation marks

## Top Sources

| | |
|---|---|
| 7% | Internet sources |
| 4% | Publications |
| 0% | Submitted works (Student Papers) |

## Match Groups

**22** Not Cited or Quoted 7%
Matches with neither in-text citation nor quotation marks

**0** Missing Quotations 0%
Matches that are still very similar to source material

**0** Missing Citation 0%
Matches that have quotation marks, but no in-text citation

**0** Cited and Quoted 0%
Matches with in-text citation present, but no quotation marks

## Top Sources

| | |
|---|---|
| 7% | Internet sources |
| 4% | Publications |
| 0% | Submitted works (Student Papers) |

## Top Sources

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

| | | | |
|---|---|---|---|
| 1 | Internet | ebin.pub | 2% |
| 2 | Internet | technodocbox.com | <1% |
| 3 | Internet | www.coursehero.com | <1% |
| 4 | Internet | en.wikipedia.org | <1% |
| 5 | Publication | Vedran Dakic, Mario Kovac, Igor Videc. "High-Performance Computing Storage Pe... | <1% |
| 6 | Internet | blog.bytesandpieces.com | <1% |
| 7 | Internet | docslib.org | <1% |
| 8 | Internet | www.ir.juit.ac.in:8080 | <1% |
| 9 | Internet | direitoshumanoseeticamedica.wordpress.com | <1% |
| 10 | Publication | "Quality and risk management in agri-food chains", Wageningen Academic Publis... | <1% |