# CYBER SECURITY UPSKILLING PROGRAM

قدم خلال مبادرة زنك/2 في جامعة البلقاء التطبيقية
بالتعاون مع أكاديمية سايبر شيلد

OCT 2024

# Digital Forensics Part

Version 1

INST.:ENG.ALI BANI BAKAR-0778642376(CYBER SHIELD ACADEMY)

DONE BY: ENG.  Dana Al-Mahrouk-0798697842-BAU.UNIV.

# Outline

1. Networks
2. Linux Essentials
3. Cybersecurity Foundation
4. Ethical Hacking
5. Digital Forensic Investigation

# Day 18

- Outline
  - Digital Forensics
    - Knowledge of Digital Forensics
    - Steps of Digital Forensics
  - Scenario
  - Best Practices
  - Memory
  - Virtual Memory
  - Custom Content Image
  - Forensic Image
  - AccessData FTK Imager
    - RAM Image

# Digital Forensics

- Digital forensics is the process of collecting, preserving, analyzing, and presenting digital evidence from digital devices in a way that is legally acceptable.
- To uncover information that can be crucial in **investigations** related to **cybercrimes**.

# Digital Forensics

**Primary Forensic Evidence:**
original digital data that is directly collected from devices involved in the investigation.

**Complete Evidence:**
gathering all possible data that could be relevant to the investigation.

**Digital Crime:**
any illegal activity that involves computers, networks, or digital devices.

**Evidence:**
any digital information that can be used to support or refute claims made during an investigation.

# Knowledge of Digital Forensics

1. Operating Systems
2. Networking and Network Security
3. Malware Analysis
4. Data Recovery Techniques
5. Programming and Scripting Skills
6. Incident Response and Investigation
7. Digital Evidence and Forensic Tools

# Steps followed in the digital forensics process

1 **Identification:** Identify the devices and data sources involved, Understand the type of digital crime or incident that has occurred.

2 **Preservation:** Create a forensic image (exact copy) of the data using specialized tools to avoid altering the original evidence.

3 **Examination:** Analyze the collected data to extract meaningful information and uncover evidence that may be useful in understanding the incident. (Recover deleted, hidden, or encrypted files)

4 **Analysis:** Interpret the data to identify patterns, relationships, or connections that can help explain the incident.(Determine the root cause of the incident, the attacker's methods, and the impact on the system)

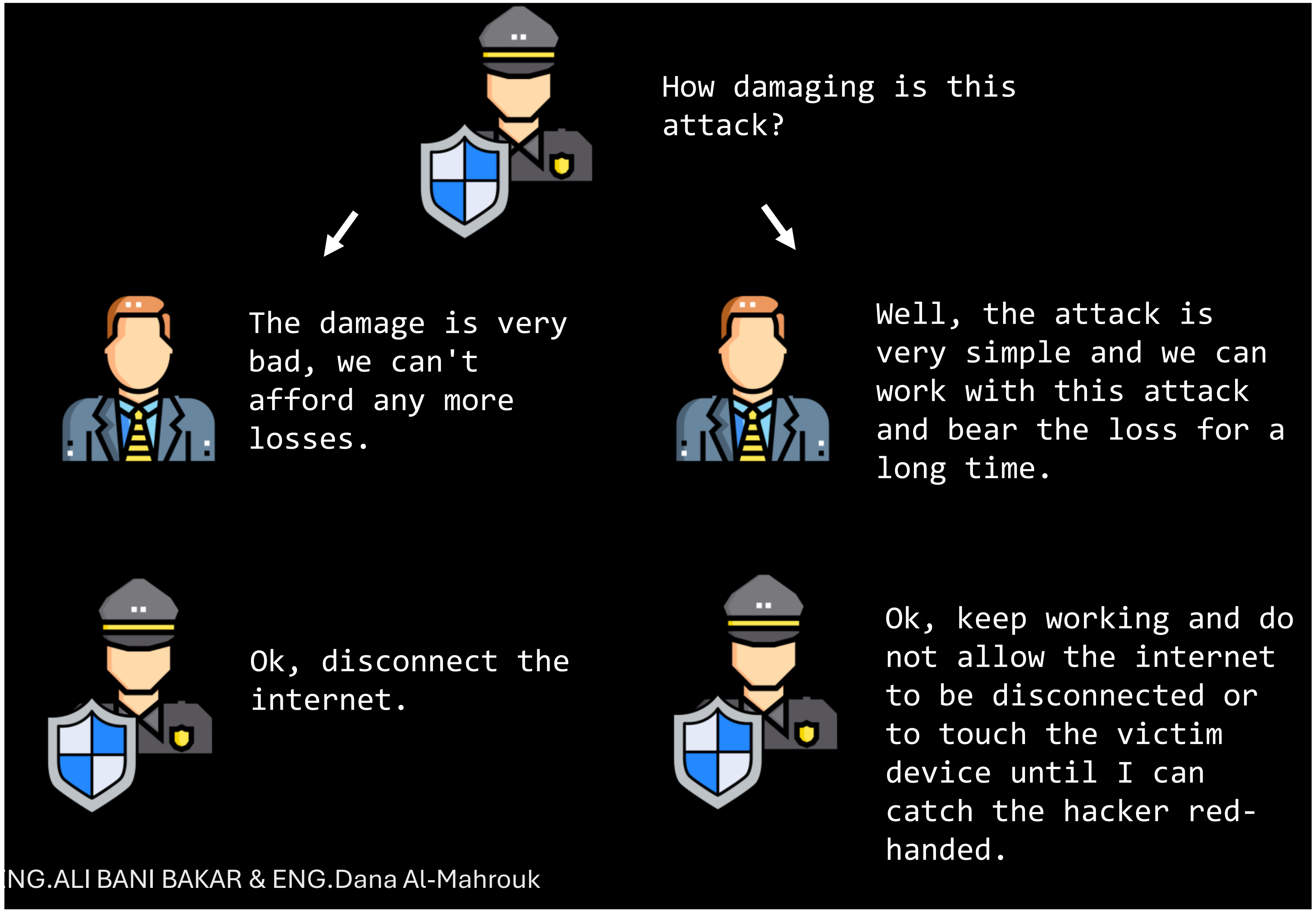
5 **Documentation:** Record all the findings, methods, tools, and processes used during the investigation to create a comprehensive report.

6 **Presentation:** Present the results of the analysis in a clear and understandable manner, suitable for legal proceedings or organizational decision-making.

# Cyber crime scenario in the bank

Please help me, the bank is being hacked now.

Please stay calm and focused now, do not allow employees to touch the attacked device until I arrive.



How damaging is this attack?

The damage is very bad, we can't afford any more losses.

Ok, disconnect the internet.

Well, the attack is very simple and we can work with this attack and bear the loss for a long time.

Ok, keep working and do not allow the internet to be disconnected or to touch the victim device until I can catch the hacker red-handed.

# Cont…

Reached.

Go directly to the infected device and take a image/snapshot of the RAM.
Use: FTK-Lite inside USB

- Capture volatile data (RAM, active network connections, running processes)

⚠ Installing a heavy program to take a image of the RAM in the device causes problems (the RAM will be overwritten)

FTK Imager Lite:
used for its speed, portability, and effectiveness in creating forensic images while maintaining data integrity.

# Best Practices

1 Disconnect the compromised systems from the network to stop the attacker's access without shutting them down completely (to avoid losing volatile data).

2 Ensure that all evidence is preserved in its original state. Use forensic tools to create bit-by-bit copies of data before performing any analysis.

3 Maintain a detailed record of every action taken during the investigation, including the collection, handling, and transfer of evidence and Document the timeline of events. This ensures that the evidence is admissible in court.

4 Analyze system logs, network traffic, file timestamps, and other relevant data to identify how the attack occurred, what systems were affected

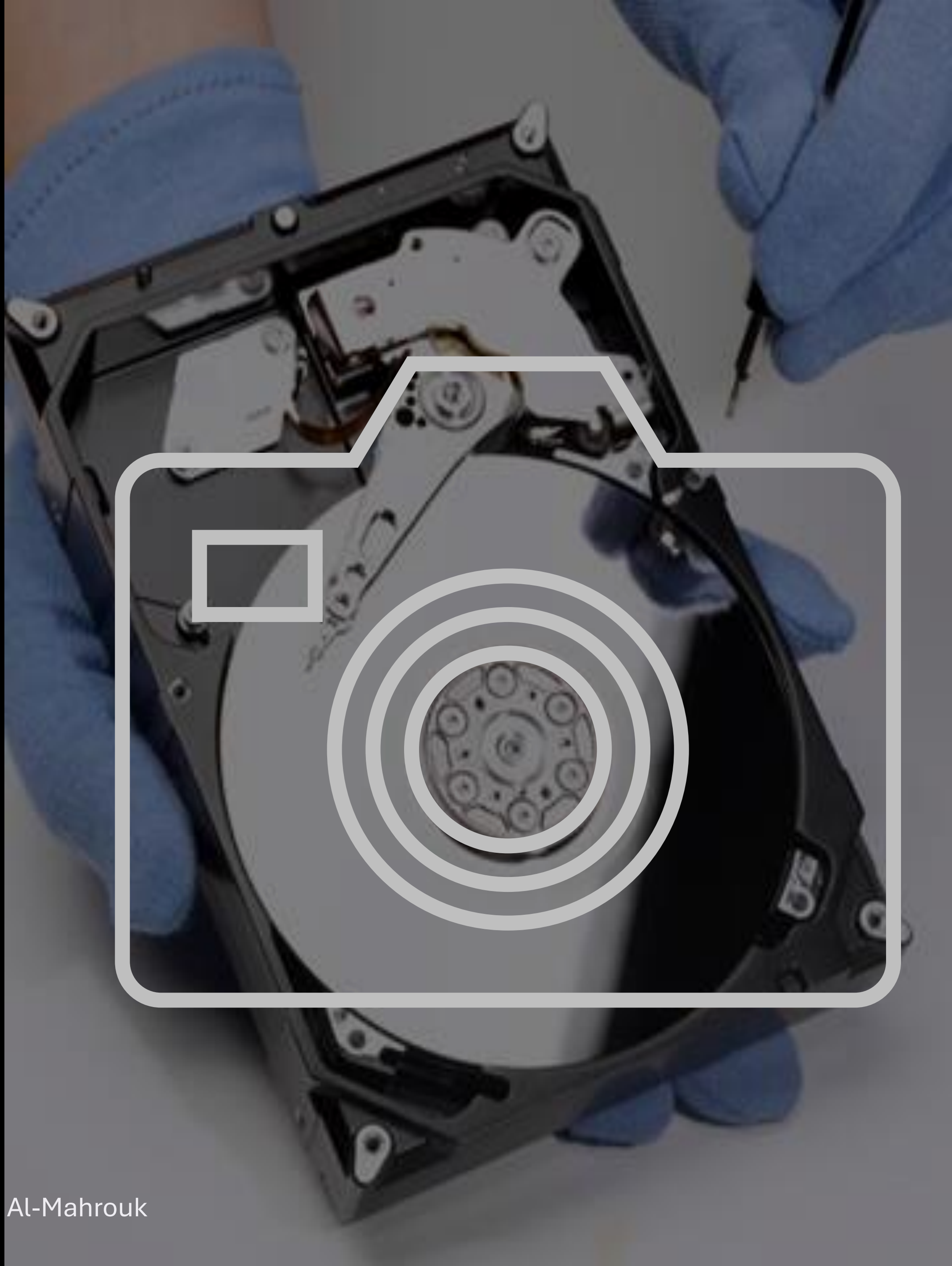
# Get complete evidence from hard disk

- Obtaining complete evidence from the hard disk…
- You must ensure that the flash drive has sufficient space to obtain an image of the entire hard disk (bit by bit), in order to ensure that you obtain the deleted data.

0.5 TB Data Used
4 TB Total

🚫 1 TB Flash

✓ 4 TB Flash



# Digital Forensics Phases

1 RAM image

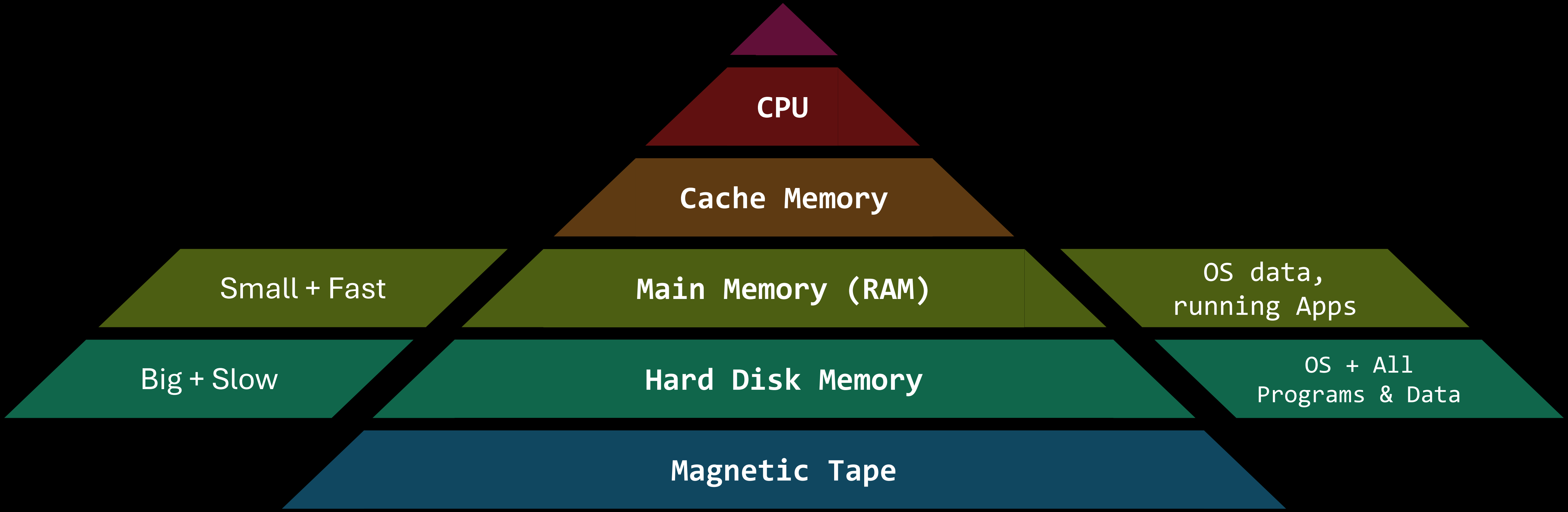
2 Check HD Encryption

3 Triage image

4 Analyze RAM & Triage Image

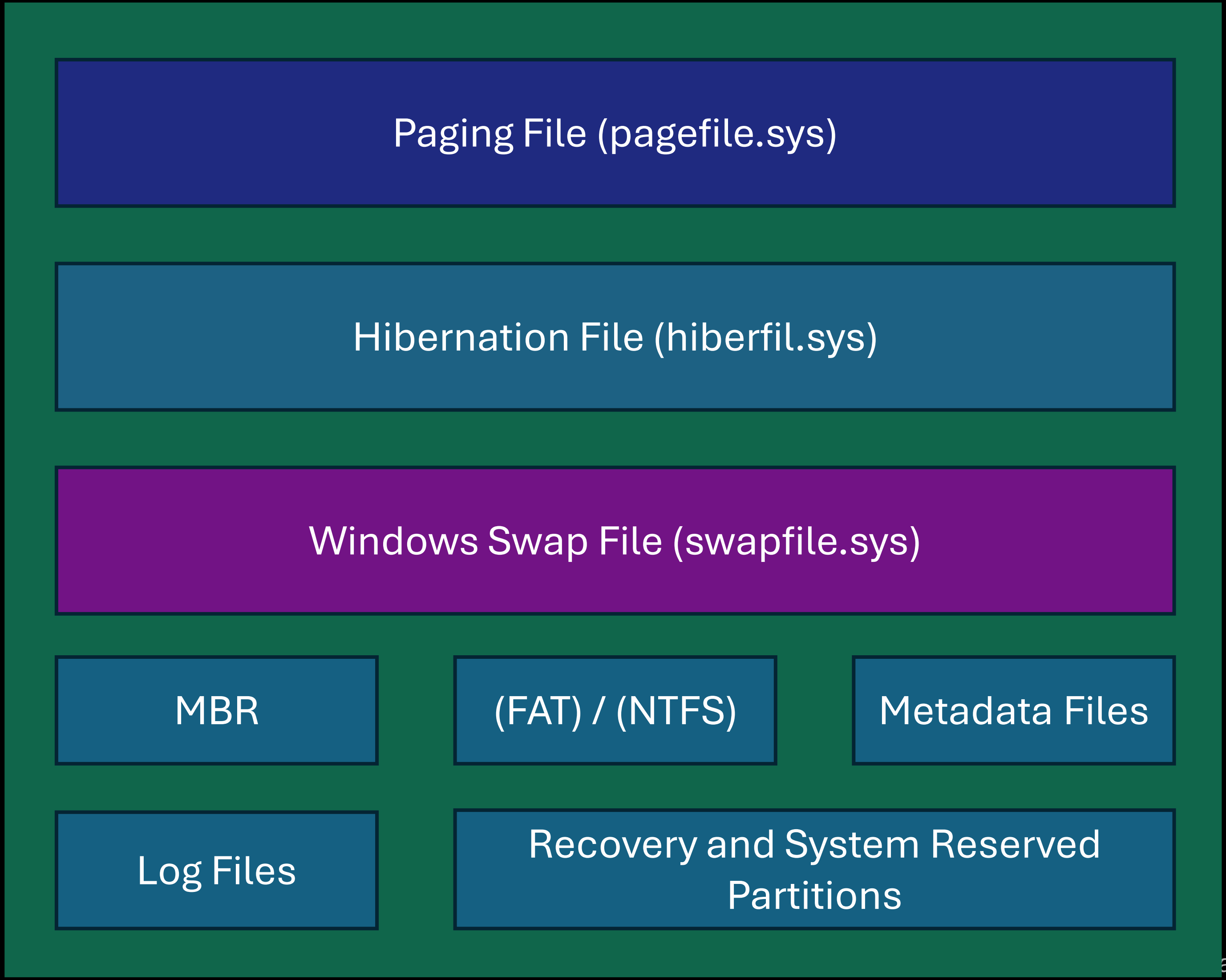
5 Hard disk Image

# Memory



INST. : ENG.ALI BANI BAKAR & ENG.Dana Al-Mahrouk

# Virtual Memory → Key Files in Hard disk



Paging File (pagefile.sys)

Hibernation File (hiberfil.sys)

Windows Swap File (swapfile.sys)

MBR

(FAT) / (NTFS)

Metadata Files

Log Files

Recovery and System Reserved Partitions

**Paging File:**
When the RAM is full, paging file to store parts of memory that aren't actively used. This process is called "paging”

**Hibernation File:**
During hibernation mode, the RAM are saved to this file on the so that the system can completely power down.

**Windows Swap File:**
works alongside pagefile.sys to handle memory paging and reduce memory usage by temporarily storing data.

# Custom Content

**1) SAM (Security Account Manager):** Stores hashed passwords for user accounts on the local machine.

**2) Security:** Contains security settings and policies applied to the system.

**3) Software:** Holds information about installed software and configuration settings.

**4) System:** Contains settings related to the hardware and system configuration, including services and drivers.

# Forensic Image

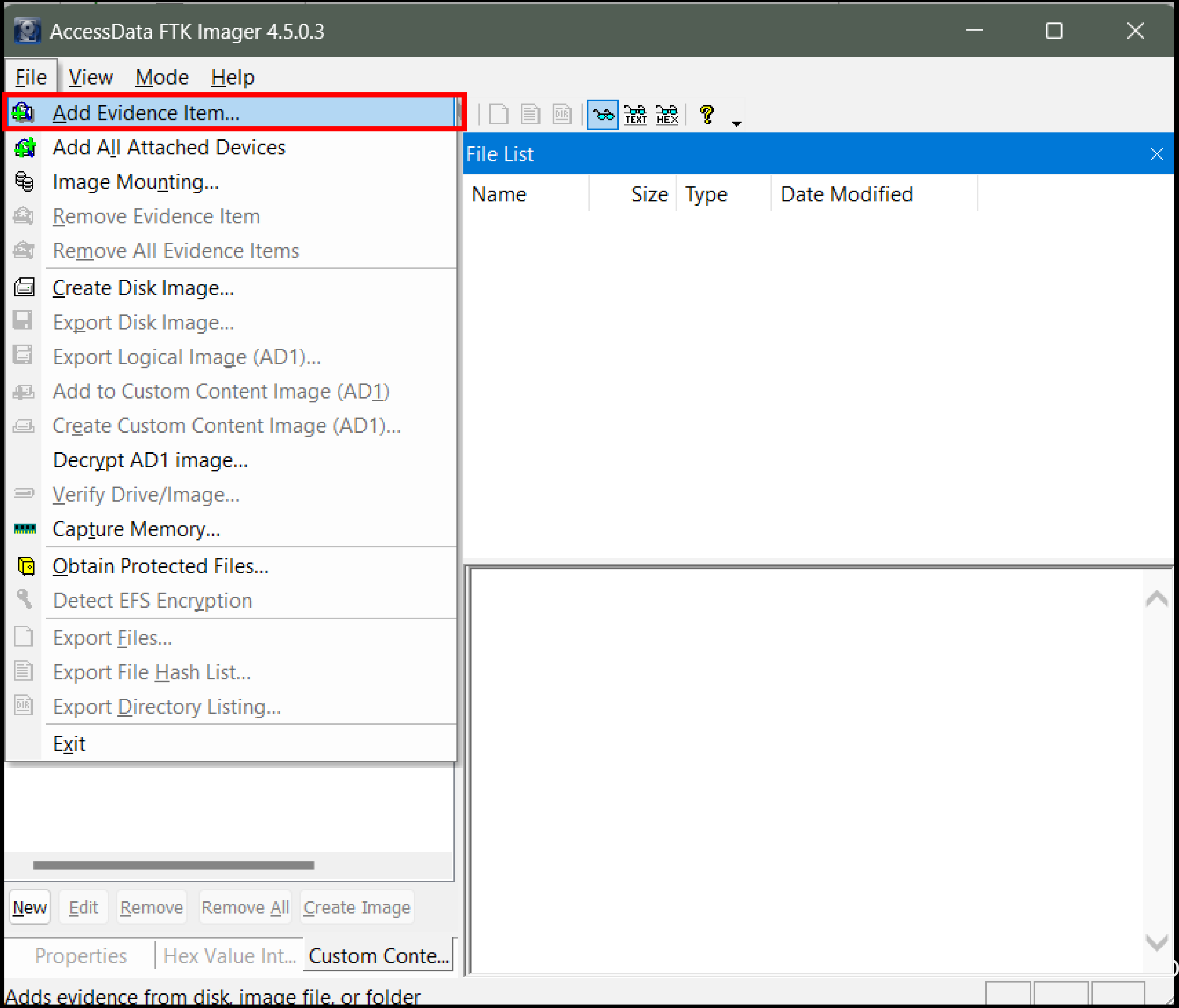
1. **NTUSER.DAT:** the user's registry hive (user-specific settings, recent activity, executed programs, recently accessed files, and more).
2. **Event Logs (*.evtx):** These logs record all the events happening on the system, such as logins, file access, errors, and software installation. → timeline of activities.
3. **Windows Registry** (**SAM, Security, Software, and System** hives) data about system's configuration, installed software, security settings, and user accounts.
4. **pagefile.sys, hiberfile.sys, and swapfile.sys** contain fragments of memory (RAM) that have been temporarily stored on the hard disk. This data often includes passwords, encryption keys, URLs, running processes, and other sensitive information that would otherwise be lost when the system is powered down.

# AccessData FTK Imager

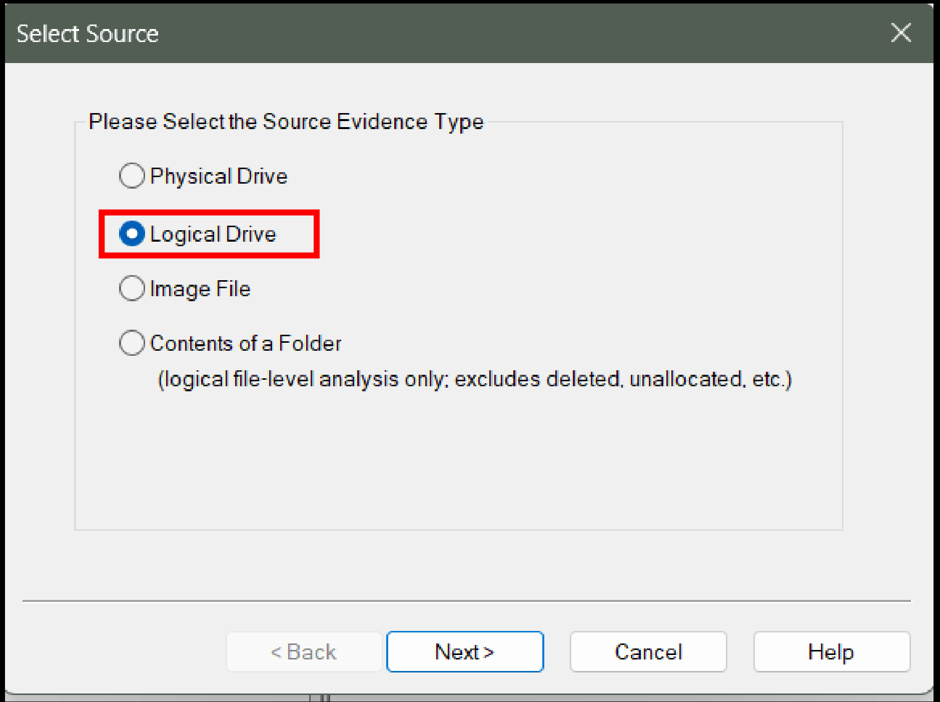
- AccessData FTK Imager: is a forensic imaging tool used to create exact copies of data from hard drives, removable media, and other storage devices.
- E01 (EnCase image file)
- DD (raw image)
- AD1 (AccessData custom image file)

- It ensures the integrity of the data by generating hash values (MD5, SHA-1)
- preview the contents of files and folders on a drive before imaging.
- display detailed information about the file system, including deleted files, hidden files, and system files.
- supports multiple file systems, including `FAT, NTFS, exFAT, HFS+, EXT2/3/4`.

# TRIAG Image

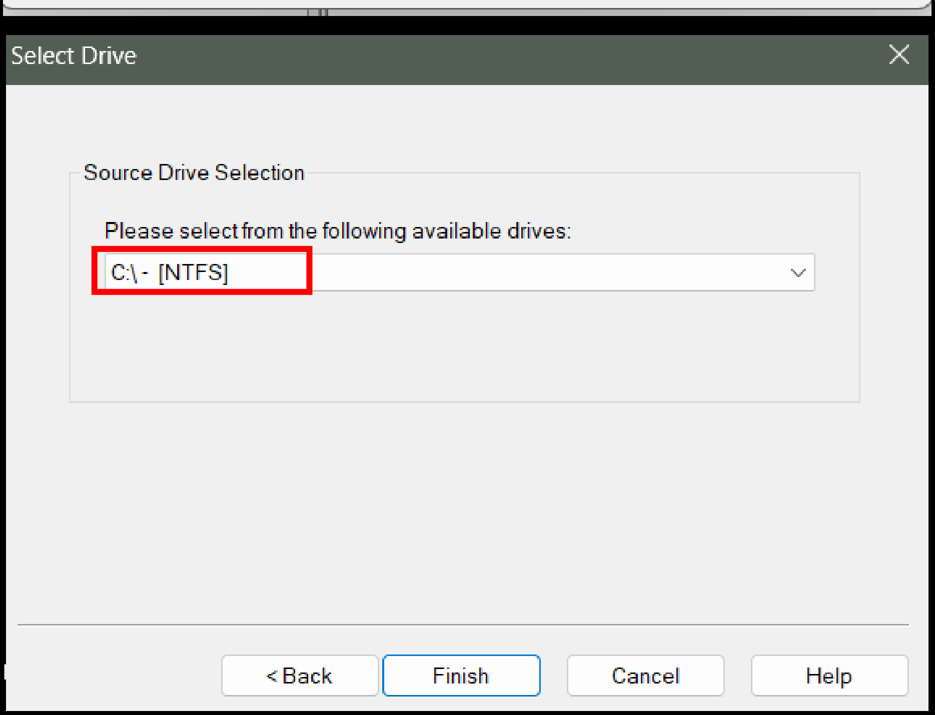


Adds evidence from disk, image file, or folder



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.)



Source Drive Selection

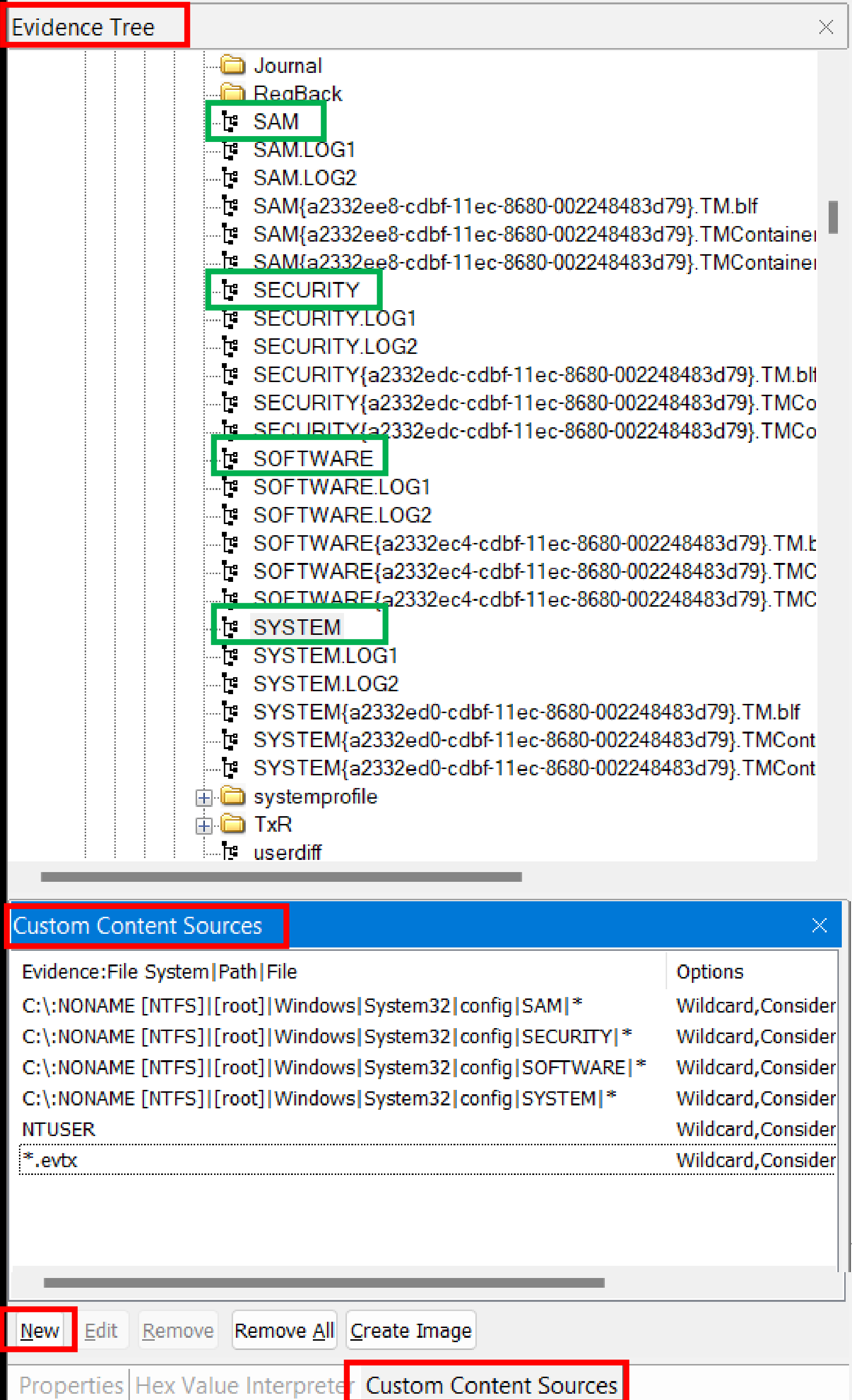
Please select from the following available drives:

C:\ - [NTFS]

Dana Al-Mahr

# TRIAG Image

- File → Add Evidence Item → Logical Drive → C:\-[NTFS] → Finish
- Custom Content Source:
  - Evidence Tree:
  - C:\ → NONAME[NIST] → [root] → Windows → System32 → config → SAM + SECURITY + SOFTWARE + SYSTEM
  - Right click → Add to Custom Content Image (AD1)
  - New → Edit → NTUSER + *.evtx
- File → Export Logic Image (AD1) → Add …



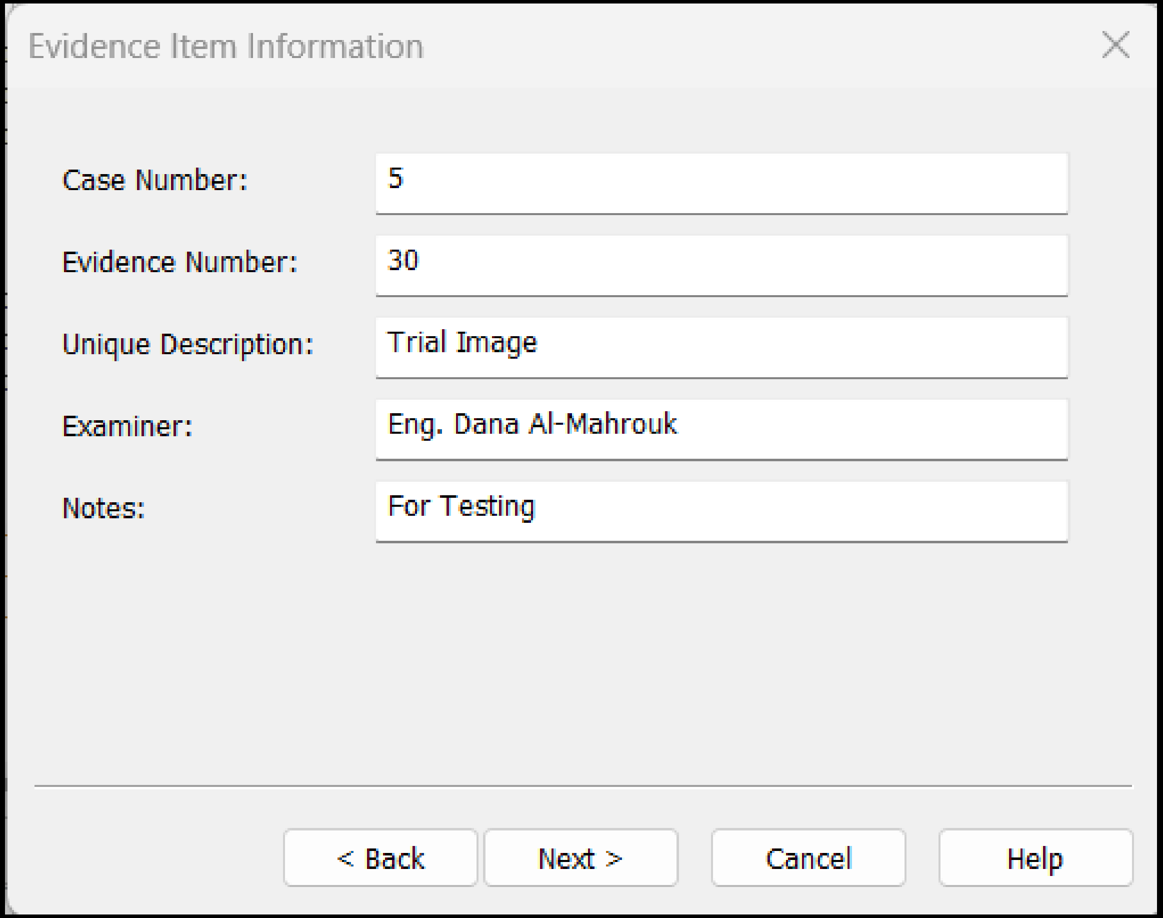
Evidence Tree

```
Journal
RegBack
SAM
SAM.LOG1
SAM.LOG2
SAM{a2332ee8-cdbf-11ec-8680-002248483d79}.TM.blf
SAM{a2332ee8-cdbf-11ec-8680-002248483d79}.TMContainer
SAM{a2332ee8-cdbf-11ec-8680-002248483d79}.TMContainer
SECURITY
SECURITY.LOG1
SECURITY.LOG2
SECURITY{a2332edc-cdbf-11ec-8680-002248483d79}.TM.blf
SECURITY{a2332edc-cdbf-11ec-8680-002248483d79}.TMCo
SECURITY{a2332edc-cdbf-11ec-8680-002248483d79}.TMCo
SOFTWARE
SOFTWARE.LOG1
SOFTWARE.LOG2
SOFTWARE{a2332ec4-cdbf-11ec-8680-002248483d79}.TM.b
SOFTWARE{a2332ec4-cdbf-11ec-8680-002248483d79}.TMC
SOFTWARE{a2332ec4-cdbf-11ec-8680-002248483d79}.TMC
SYSTEM
SYSTEM.LOG1
SYSTEM.LOG2
SYSTEM{a2332ed0-cdbf-11ec-8680-002248483d79}.TM.blf
SYSTEM{a2332ed0-cdbf-11ec-8680-002248483d79}.TMCont
SYSTEM{a2332ed0-cdbf-11ec-8680-002248483d79}.TMCont
systemprofile
TxR
userdiff
```

Custom Content Sources

| Evidence:File System\|Path\|File | Options |
|---|---|
| C:\:NONAME [NTFS]\|[root]\|Windows\|System32\|config\|SAM\|* | Wildcard,Consider |
| C:\:NONAME [NTFS]\|[root]\|Windows\|System32\|config\|SECURITY\|* | Wildcard,Consider |
| C:\:NONAME [NTFS]\|[root]\|Windows\|System32\|config\|SOFTWARE\|* | Wildcard,Consider |
| C:\:NONAME [NTFS]\|[root]\|Windows\|System32\|config\|SYSTEM\|* | Wildcard,Consider |
| NTUSER | Wildcard,Consider |
| *.evtx | Wildcard,Consider |

# Export Logic Image (AD1)



Evidence Item Information

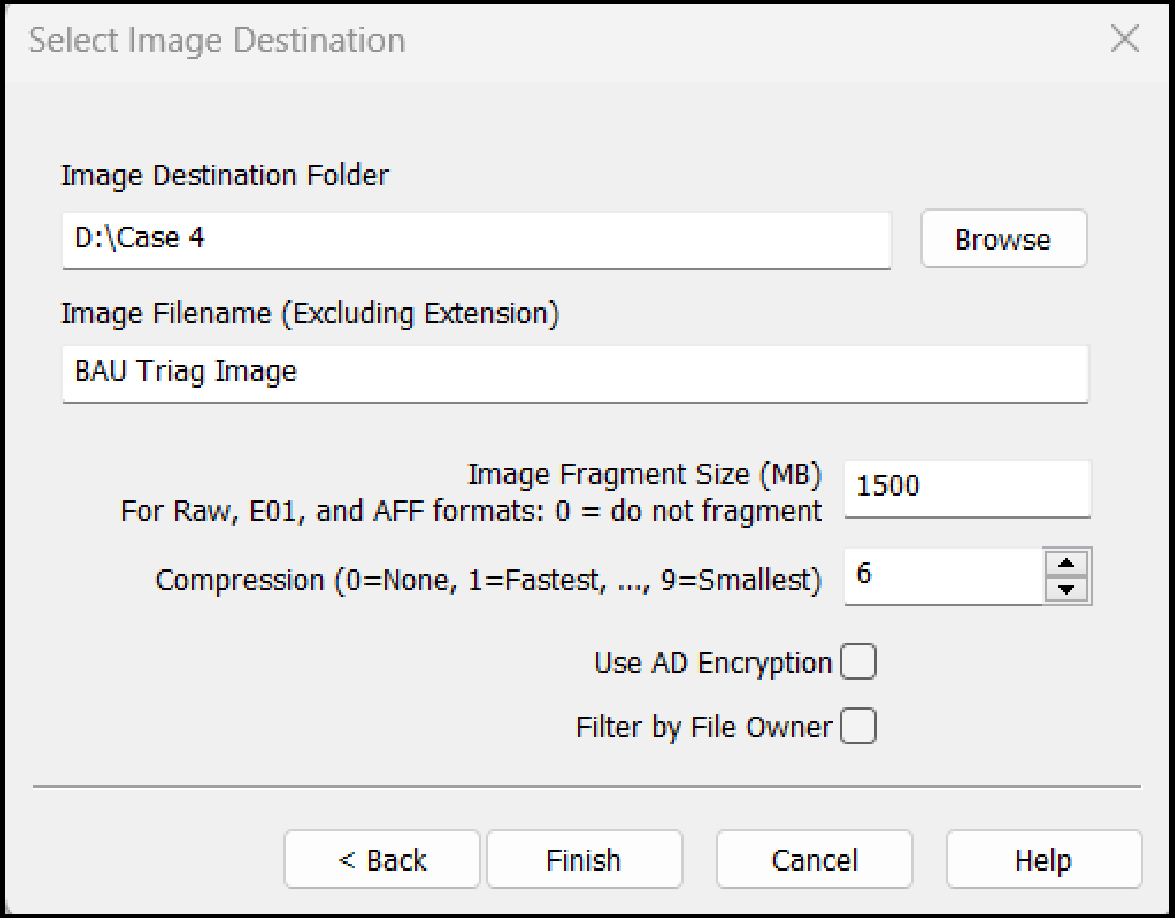
Case Number: 5

Evidence Number: 30

Unique Description: Trial Image

Examiner: Eng. Dana Al-Mahrouk

Notes: For Testing



Select Image Destination

Image Destination Folder: D:\Case 4

Image Filename (Excluding Extension): BAU Triag Image

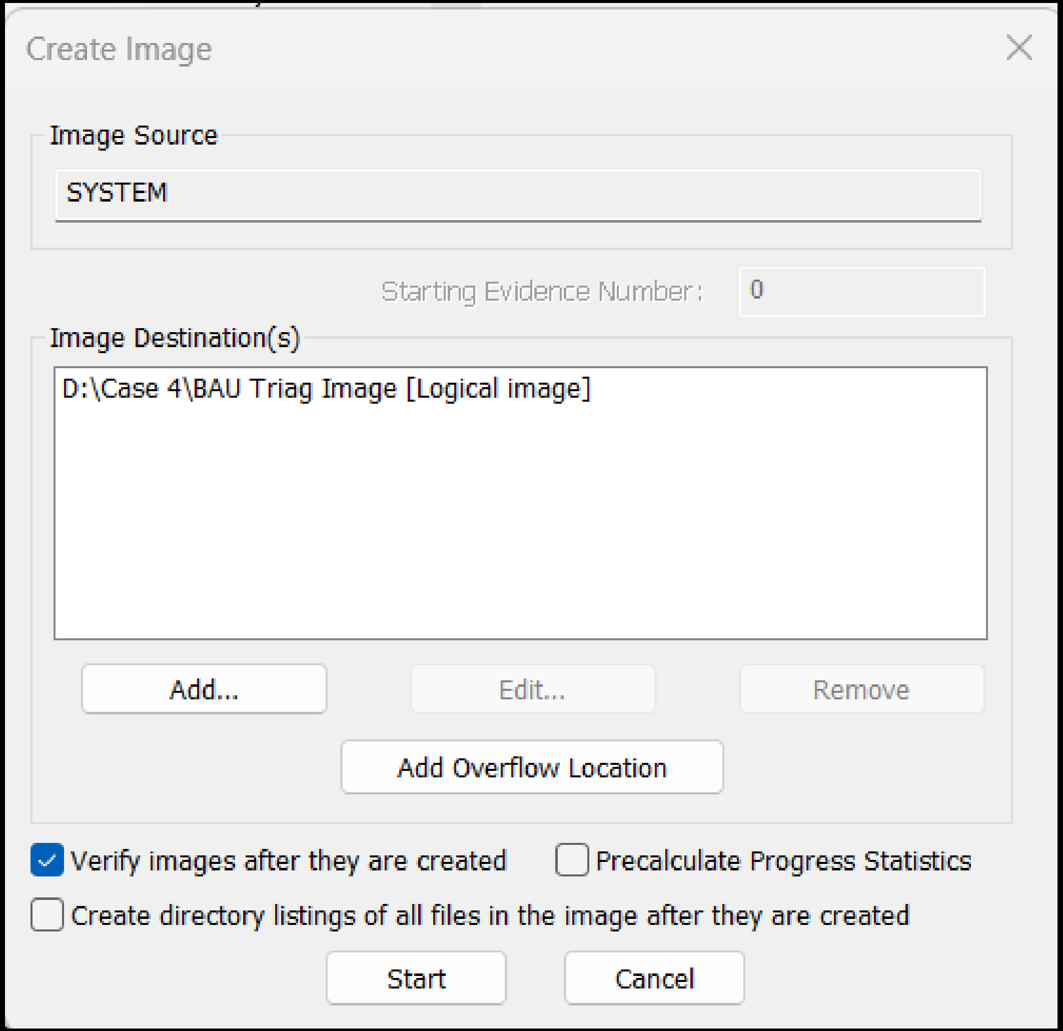
Image Fragment Size (MB)
For Raw, E01, and AFF formats: 0 = do not fragment: 1500

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

Use AD Encryption □

Filter by File Owner □

# Export Logic Image (AD1)



Create Image

Image Source

SYSTEM

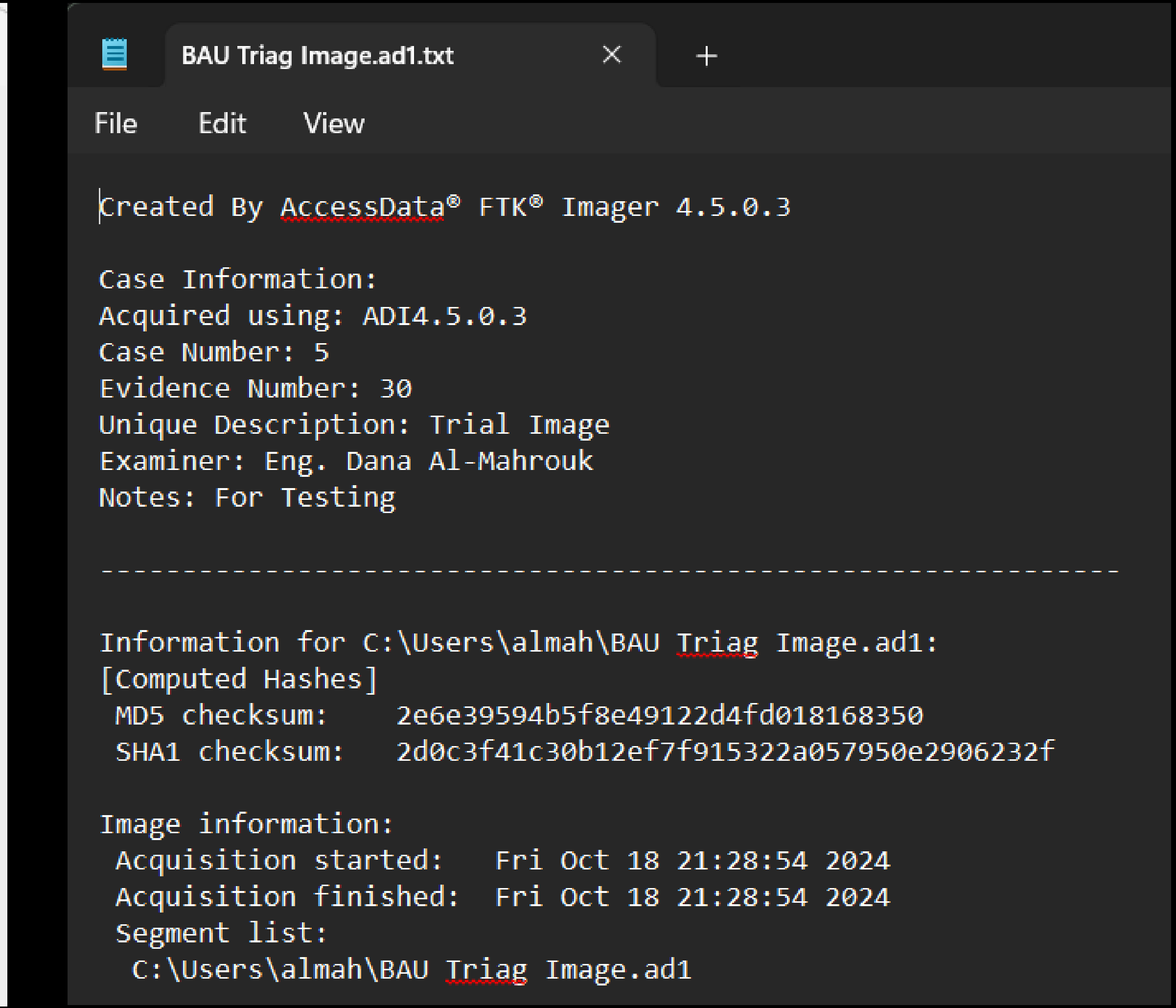
Starting Evidence Number: 0

Image Destination(s)

D:\Case 4\BAU Triag Image [Logical image]

☑ Verify images after they are created ☐ Precalculate Progress Statistics

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



```
Created By AccessData® FTK® Imager 4.5.0.3

Case Information:
Acquired using: ADI4.5.0.3
Case Number: 5
Evidence Number: 30
Unique Description: Trial Image
Examiner: Eng. Dana Al-Mahrouk
Notes: For Testing

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

Information for C:\Users\almah\BAU Triag Image.ad1:
[Computed Hashes]
 MD5 checksum:    2e6e39594b5f8e49122d4fd018168350
 SHA1 checksum:   2d0c3f41c30b12ef7f915322a057950e2906232f

Image information:
 Acquisition started:   Fri Oct 18 21:28:54 2024
 Acquisition finished:  Fri Oct 18 21:28:54 2024
 Segment list:
  C:\Users\almah\BAU Triag Image.ad1
```

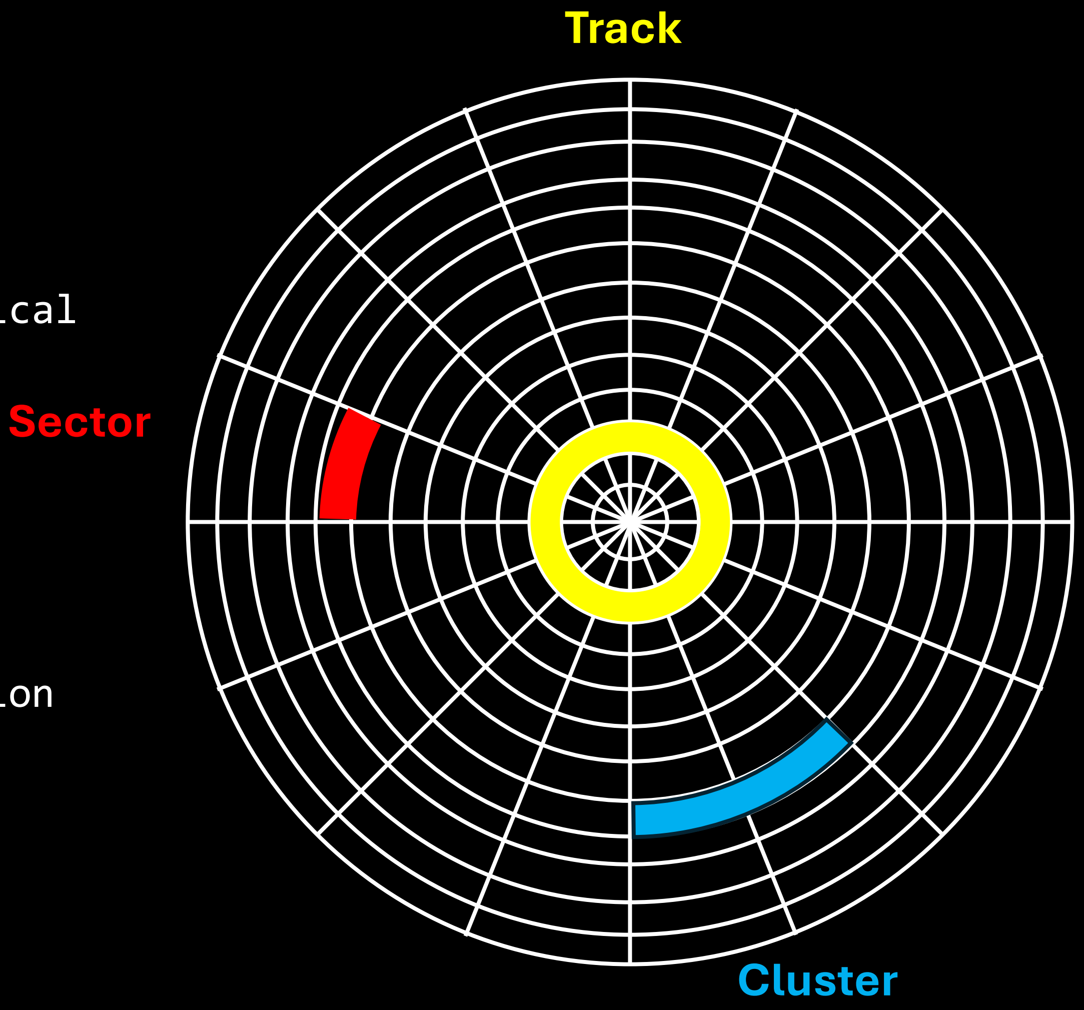
# Day 19

- Outline
  - Hard disk (Trunk, Sector, Cluster)
    - Cluster Size
    - booting a Windows OS
  - File Wiping (Data Erasure)
  - File Recovery
  - Formatting
  - File Wiping issues
  - C Language for OS
  - Create Disk Image
  - Disk Mounting

# Hard disk

- **Track:**
- **Sector:** 512 byte
- the smallest unit of data storage on a hard disk, physical units that the disk hardware reads and writes.

- **Cluster:** (allocation unit)
- A group of sectors that the file system uses to manage data on the disk.
- The cluster size depends on the file system and partition size.
- [optional → 2 sector]
- 1024 byte → 1 KB



# Q: sector=512-byte File size = 5.5KB

- Device 1:
- Cluster = 2 sector → 1024 bytes

- Use 5 clusters → 5125 bytes
- Use 6 clusters → 6144 bytes

- Losses:
- 5 clusters Full + cluster (512 bytes)
- Final File Size → 6144

- Device 2:
- Cluster = 4 sector → 2048 bytes

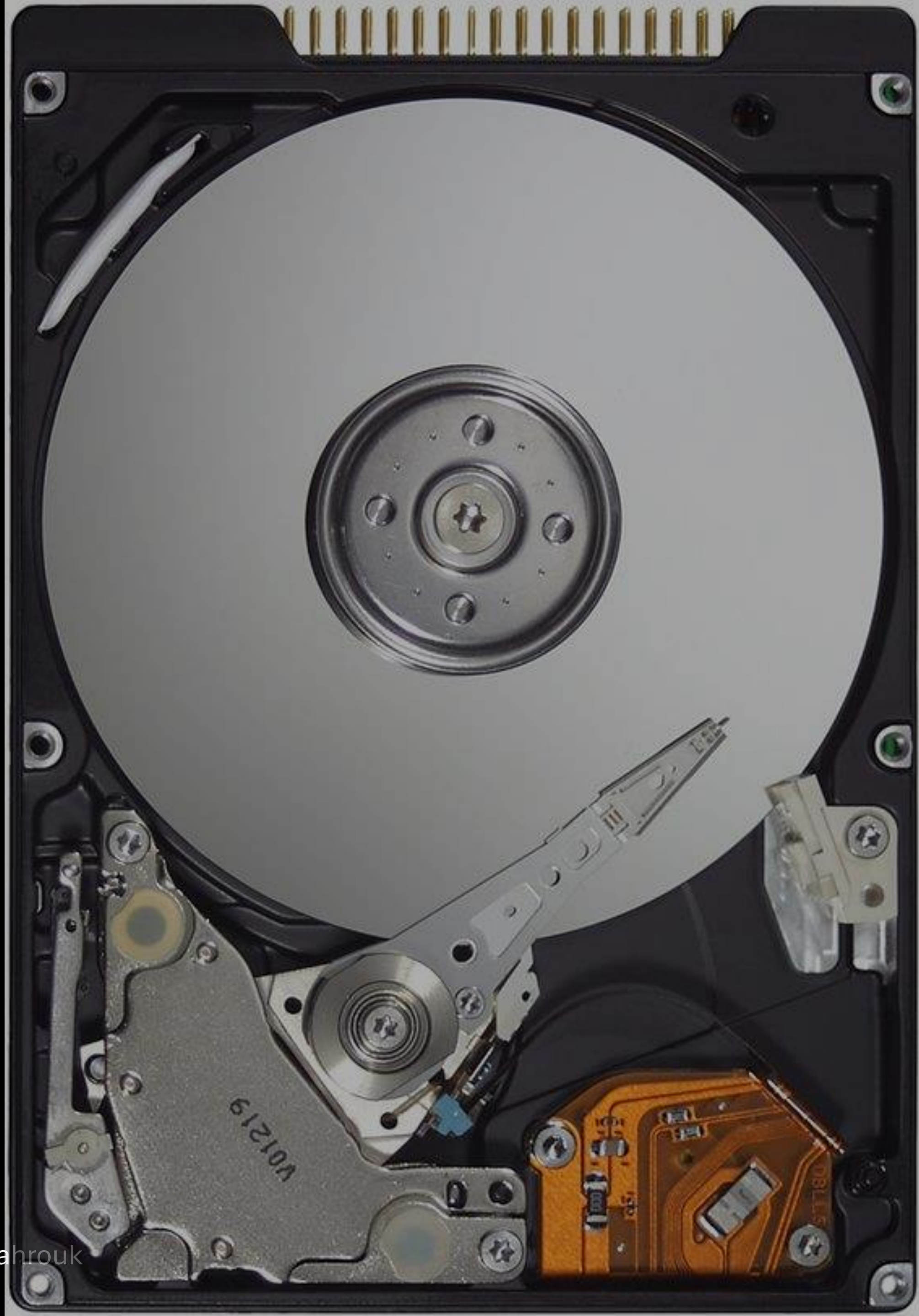
- Use 2 clusters → 4096 bytes
- Use 3 clusters → 6144 bytes

- Losses:
- 2 clusters Full + cluster (512 bytes)
- Final File Size → 6144

# Cluster Size

- Small Cluster:
- loss spaces decrease (no empty spaces)
- Long time to search / find data → read write

- Big Cluster:
- Loss spaces increase (a lot of empty spaces)
- Fast in read / write



# booting a Windows OS

- File System: [NTFS], [FAT32], [FAT16].
- OS → RAM [32-Bit] [64-Bit]
- CPU → [32-Bit] [64-Bit]

- File → start address, size

# Ex:

- Init Tag is 0
- Linux:

- touch note.txt
- rm note.txt
- touch note2.txt
- touch flower.jpg
- touch zinc.png
- rm flower.jpg
- rm zinc.png
- touch w.doc
- touch Book.txt
- rm w.doc
- touch BAU.exe
- touch cat.jpg

| Tag | Address | Data |
|---|---|---|
| 0 → 1 → 0 → 1 | 00000000 | Note.txt → note2.txt |
| 0 → 1 → 0 → 1 → 0 → 1 | 00000010 | Folwer.jpg → w.doc → cat.jpg |
| 0 → 1 → 0 → 1 | 00000020 | Zinc.png → BAU.exe |
| 0 → 1 | 00000030 | Book.txt |

- Test your knowledge
- Q: A customer wants you to recover some deleted data from his device, what advice would you give him until he reaches you? → (Don’t Overwrite → File Recovery)

- Q: How can we delete data while ensuring that no one can recover it? → (Overwrite Full Hard disk → File Wiping)

# File Wiping (Data Erasure)

- It involves overwriting the existing data with random patterns of ones and zeros multiple times to ensure the data is completely unrecoverable.

- Single-Pass Overwrite: Writes over the data once. This is often enough for most users, but not the most secure option.
- Multiple-Pass Overwrite: More secure methods like the DoD 5220.22-M standard perform three or more passes to overwrite the data, making recovery even harder.

# File Recovery

- File recovery is the process of restoring lost, deleted, or corrupted data from a storage device.
- When a file is deleted, the os **marks** the space occupied by that file as available but does not erase the data itself. File recovery software can locate these "deleted" files and restore them if they have not yet been overwritten.
- Overwriting: If new data has been written to the drive, it can overwrite the deleted files, making them impossible to recover.

# HW

- Q: The difference between making an image of the entire hard disk and making images of individual partitions or drives (like C:\, D:\, E:\, F:\)?

# File Wiping issues

- achieving 100% data deletion can be tricky due to a few technical reasons:

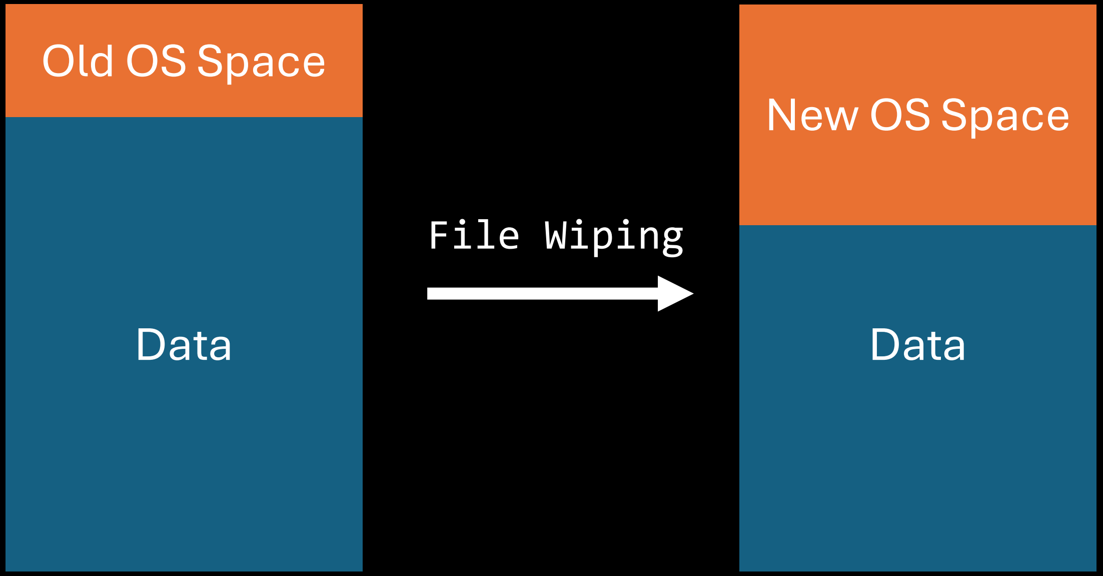
1. **File System Complexity:** Many modern file systems (like NTFS or ext4) **keep metadata**. Even after overwriting file contents, fragments of this metadata may still exist elsewhere on the disk.
2. **Data Caching:** OS and hard drives often **cache data for quick access**. Some of this cached data can persist even after deletion and might not be wiped in a standard deletion process.
3. **Over-Provisioning on SSDs:** SSDs use **hidden areas for efficient write operations**, which aren't accessible to standard wiping tools, leaving residual data.
4. **Shadow Copies and Backups:** Systems like Windows retain older file versions in backups, allowing deleted data to persist in snapshots.
5. **Logical vs. Physical Deletion:** Standard deletion removes only **file pointers**, not the data itself, which can still be recovered until **overwritten securely**.

- To truly wipe data, specialized tools and techniques (like `` `**secure erase**` `` for SSDs, or `` `**physical destruction**` `` of storage media) are often needed.

# File Wiping issues continue

- When installing a new OS or formatting a drive, leftover data from the previous system may remain because formatting usually only clears file pointers, not the actual data.
- This residual data, including sensitive information, can be recovered by someone with access to the disk. To fully erase old data and prevent exposure, a secure wipe should be done before installing the OS.

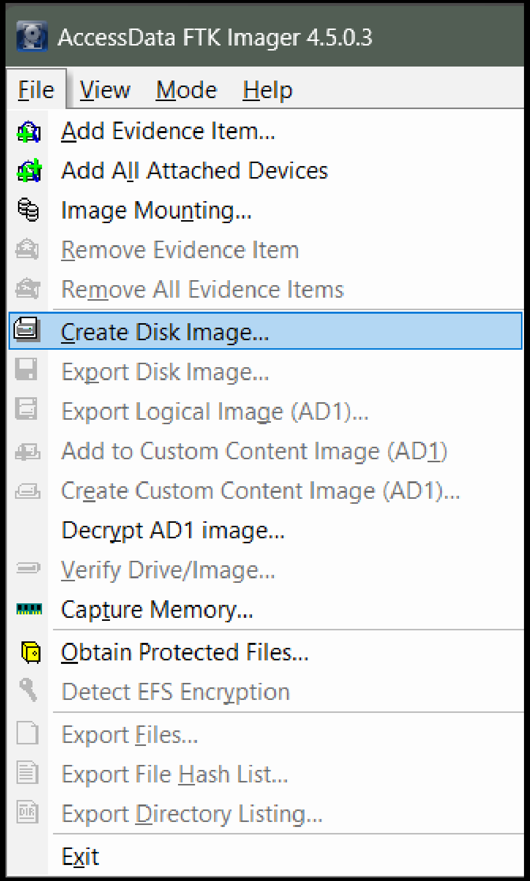
```
int mem[100];
```

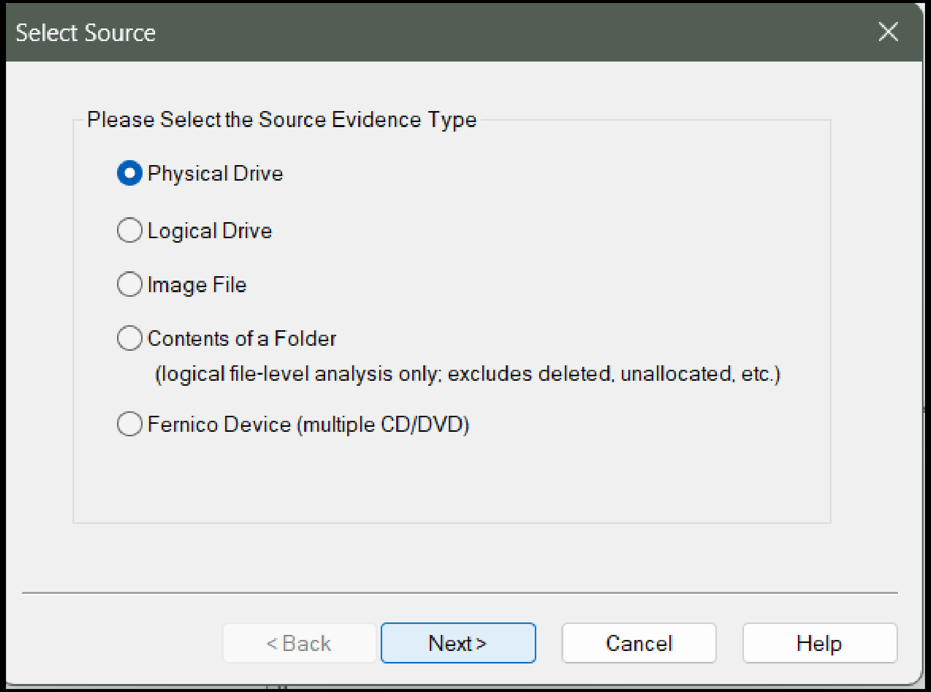


```
int mem[200];
```

Here the operating system reserves more space on the hard disk, as the data is in the operating system space now, if the operating system does not use this space and if this data is sensitive then it can be read by anyone who checks the hard disk.

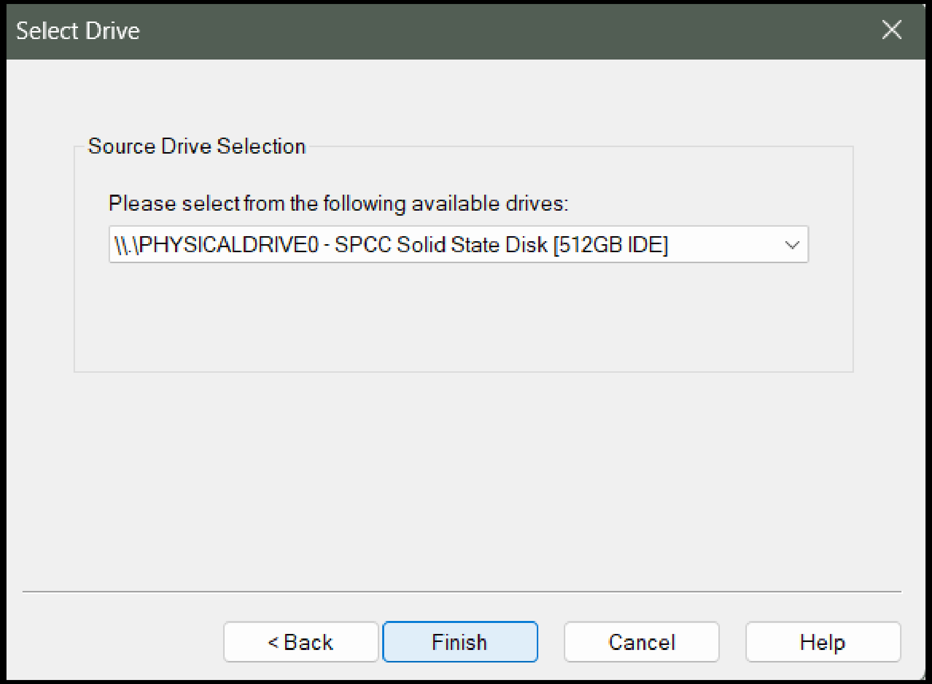
# Create Disk Image





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)

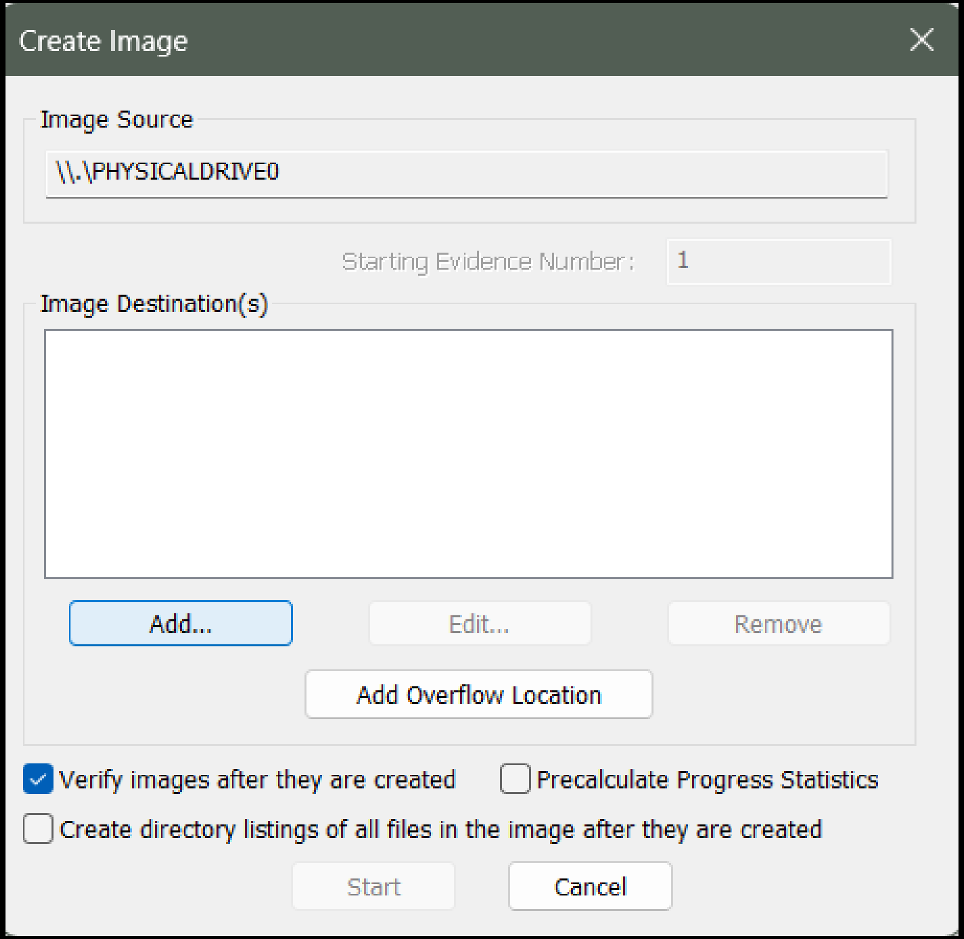


Source Drive Selection

Please select from the following available drives:

\\.\PHYSICALDRIVE0 - SPCC Solid State Disk [512GB IDE]

# Create Disk Image



Create Image

Image Source

\\.\PHYSICALDRIVE0

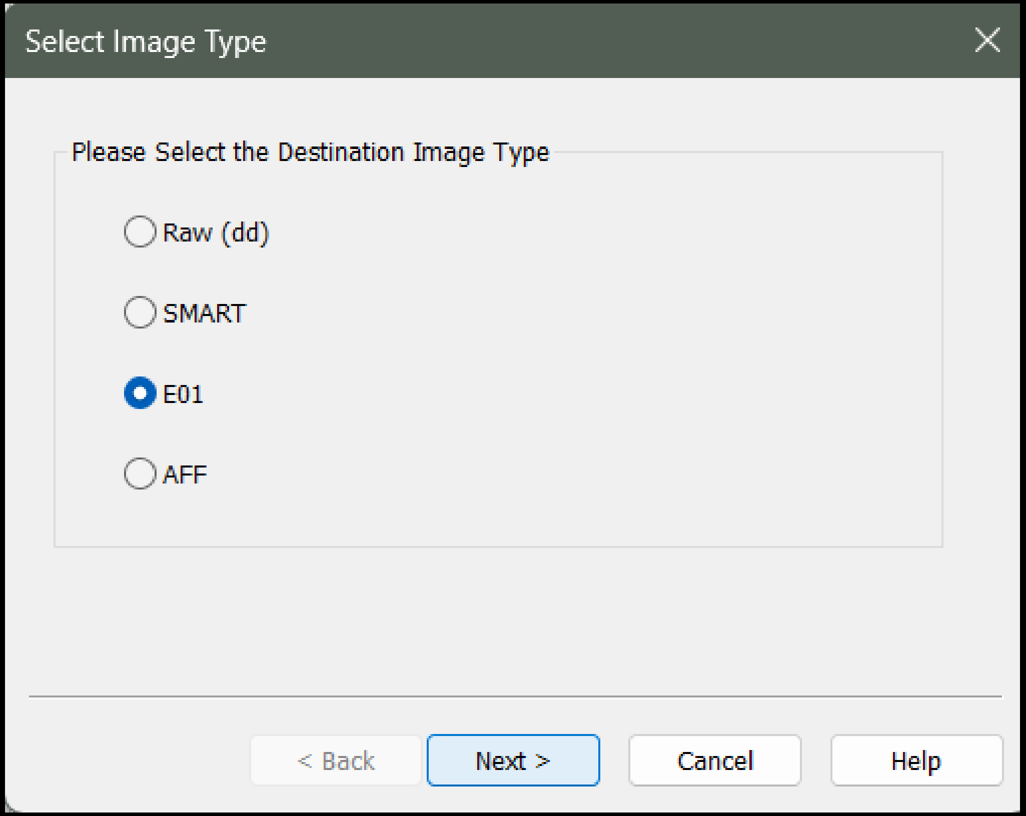
Starting Evidence Number: 1

Image Destination(s)

☑ Verify images after they are created

□ Precalculate Progress Statistics

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



Select Image Type

Please Select the Destination Image Type

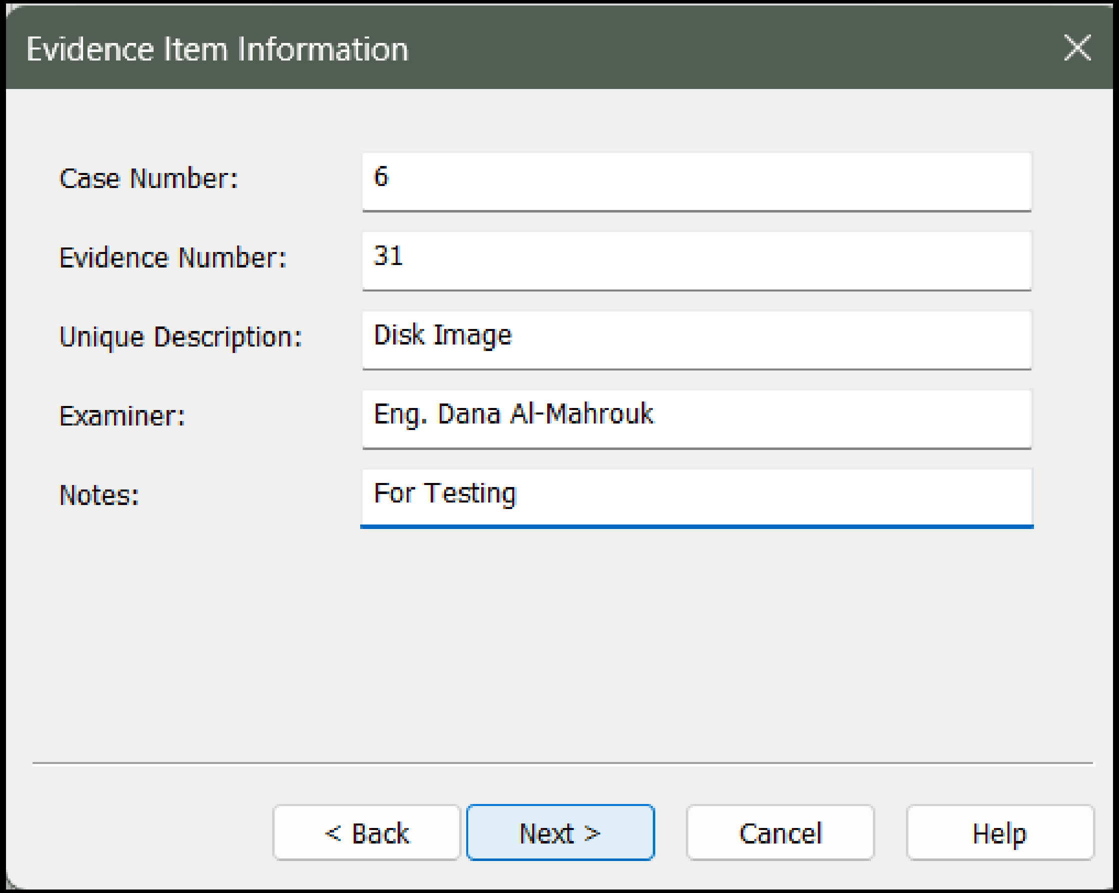
○ Raw (dd)

○ SMART

● E01

○ AFF

# Create Disk Image



Evidence Item Information

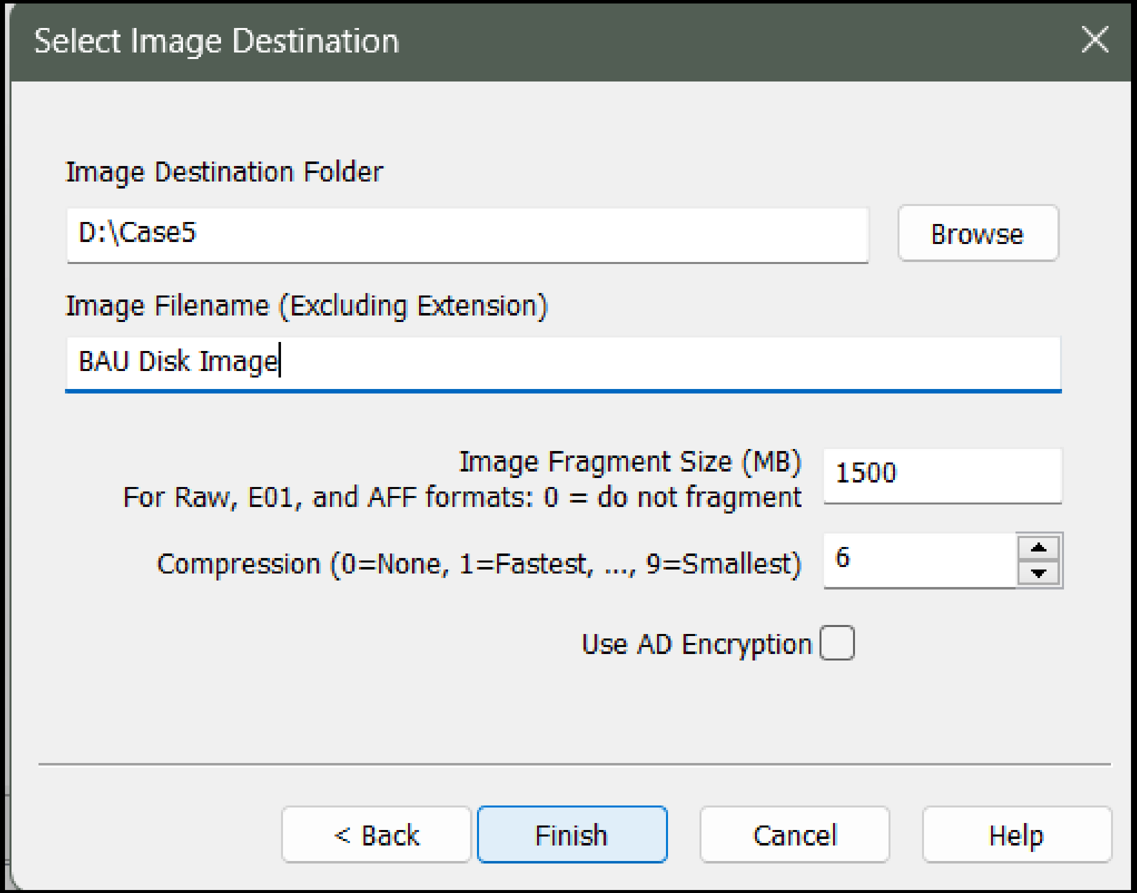
Case Number: 6

Evidence Number: 31

Unique Description: Disk Image

Examiner: Eng. Dana Al-Mahrouk

Notes: For Testing



Select Image Destination

Image Destination Folder: D:\Case5

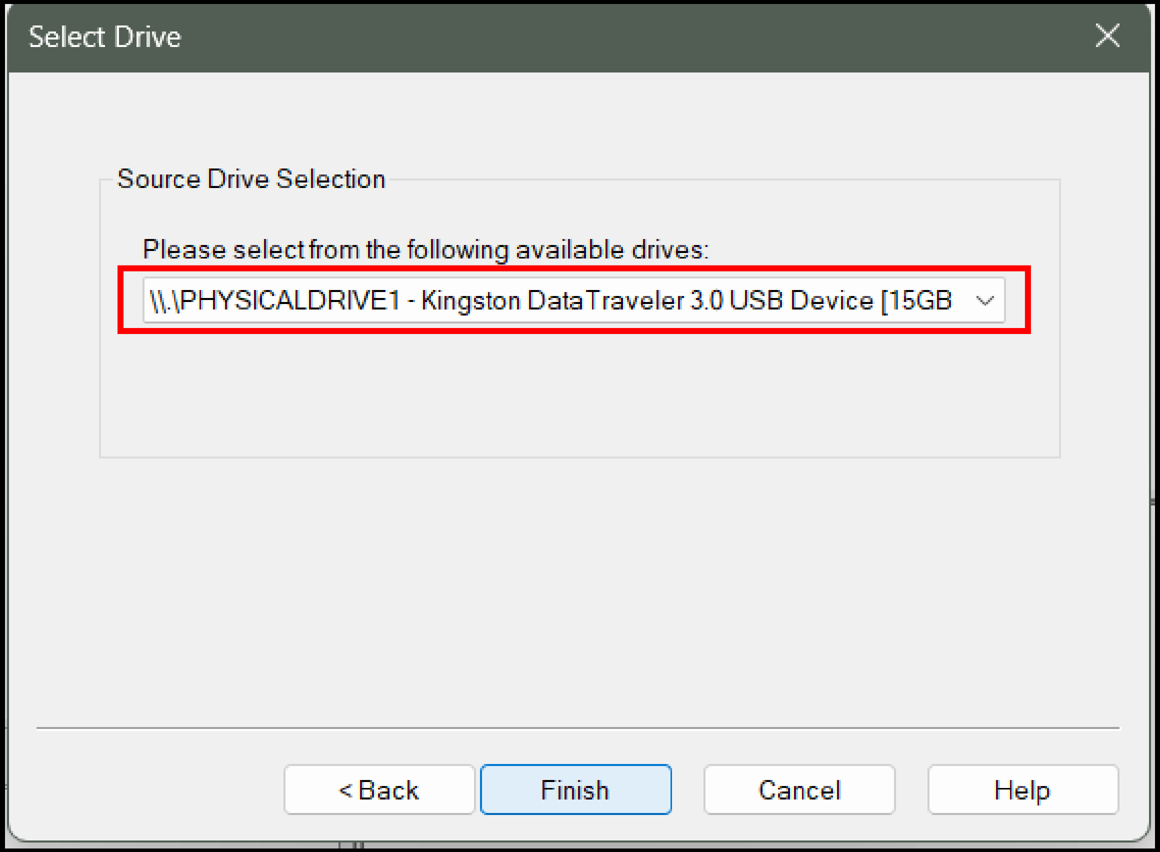
Image Filename (Excluding Extension): BAU Disk Image

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 □

# Create Disk Image (USB)

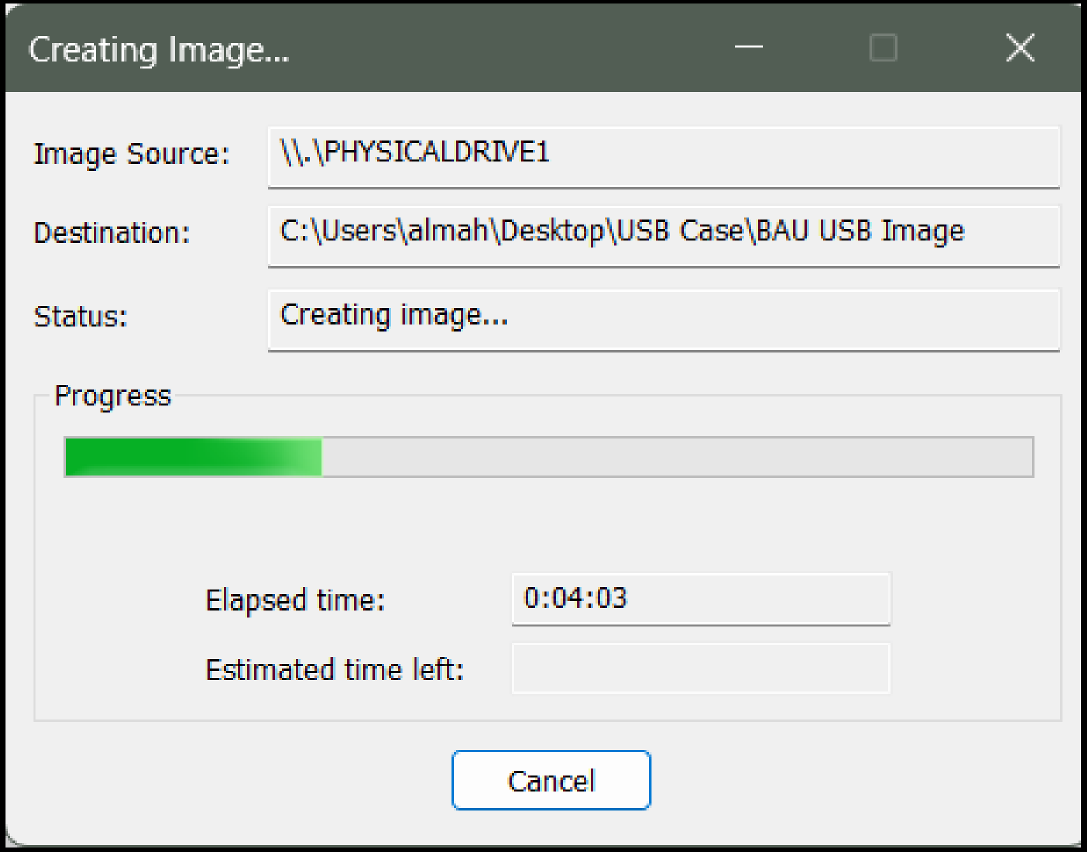


Select Drive

Source Drive Selection

Please select from the following available drives:

\\.\PHYSICALDRIVE1 - Kingston DataTraveler 3.0 USB Device [15GB



Creating Image...

Image Source: \\.\PHYSICALDRIVE1

Destination: C:\Users\almah\Desktop\USB Case\BAU USB Image

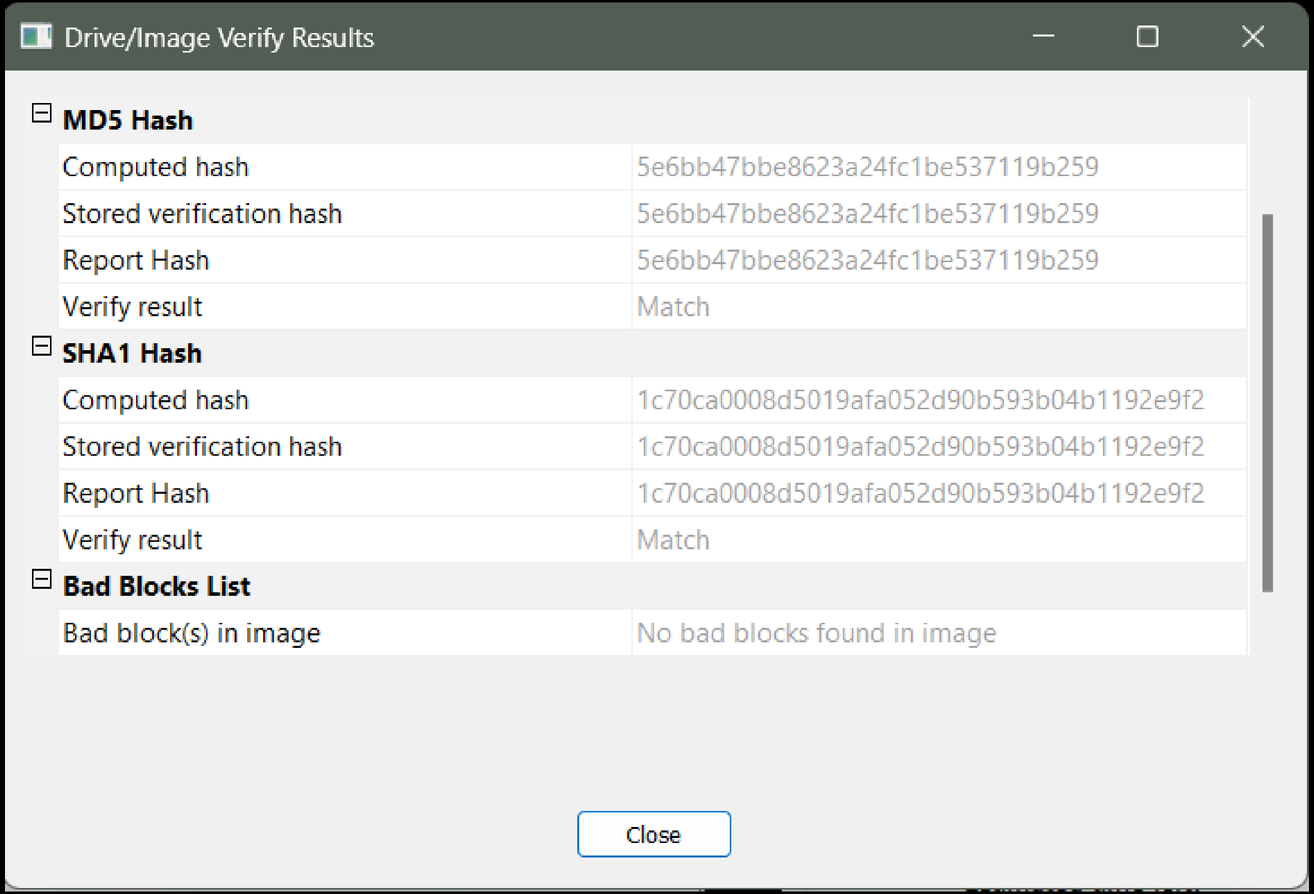
Status: Creating image...

Progress

Elapsed time: 0:04:03

Estimated time left:

# Result


Drive/Image Verify Results

| | |
|---|---|
| **⊟ MD5 Hash** | |
| Computed hash | 5e6bb47bbe8623a24fc1be537119b259 |
| Stored verification hash | 5e6bb47bbe8623a24fc1be537119b259 |
| Report Hash | 5e6bb47bbe8623a24fc1be537119b259 |
| Verify result | Match |
| **⊟ SHA1 Hash** | |
| Computed hash | 1c70ca0008d5019afa052d90b593b04b1192e9f2 |
| Stored verification hash | 1c70ca0008d5019afa052d90b593b04b1192e9f2 |
| Report Hash | 1c70ca0008d5019afa052d90b593b04b1192e9f2 |
| Verify result | Match |
| **⊟ Bad Blocks List** | |
| Bad block(s) in image | No bad blocks found in image |

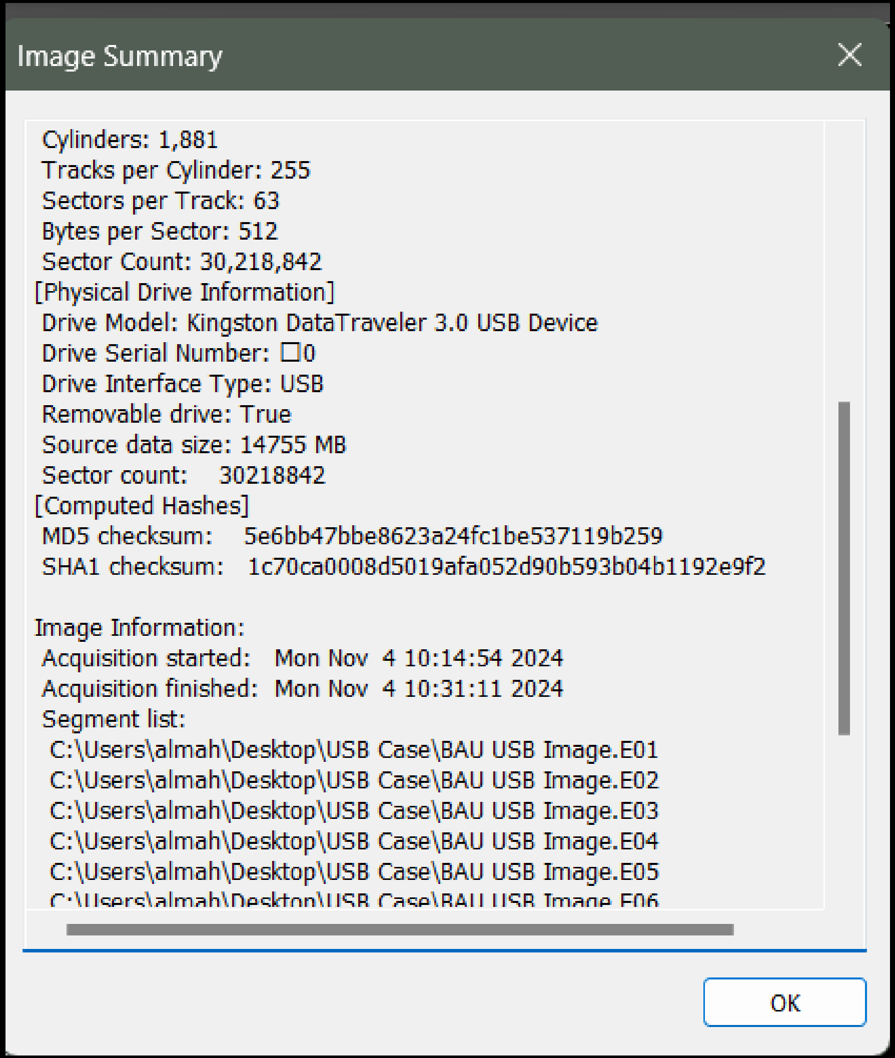
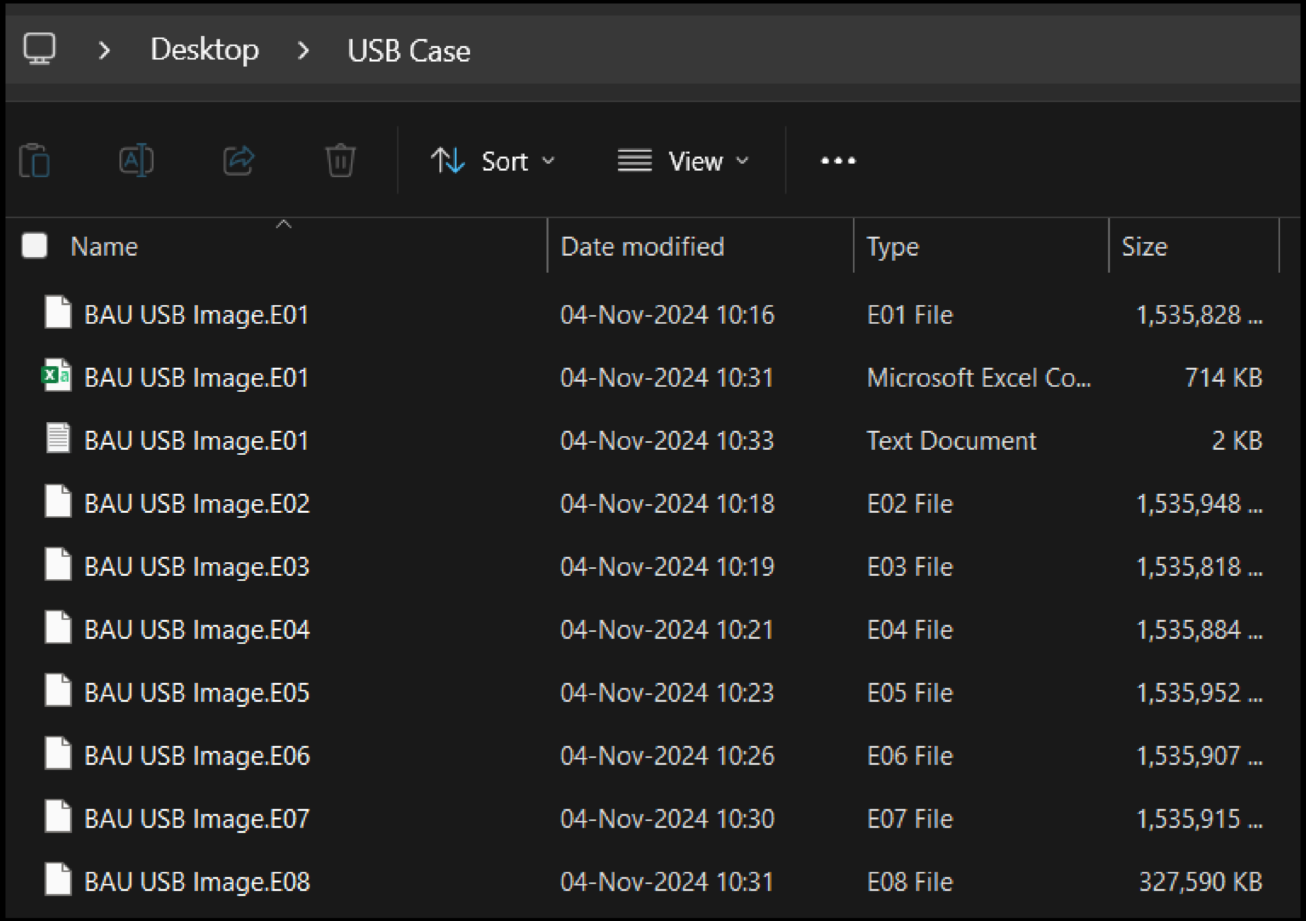


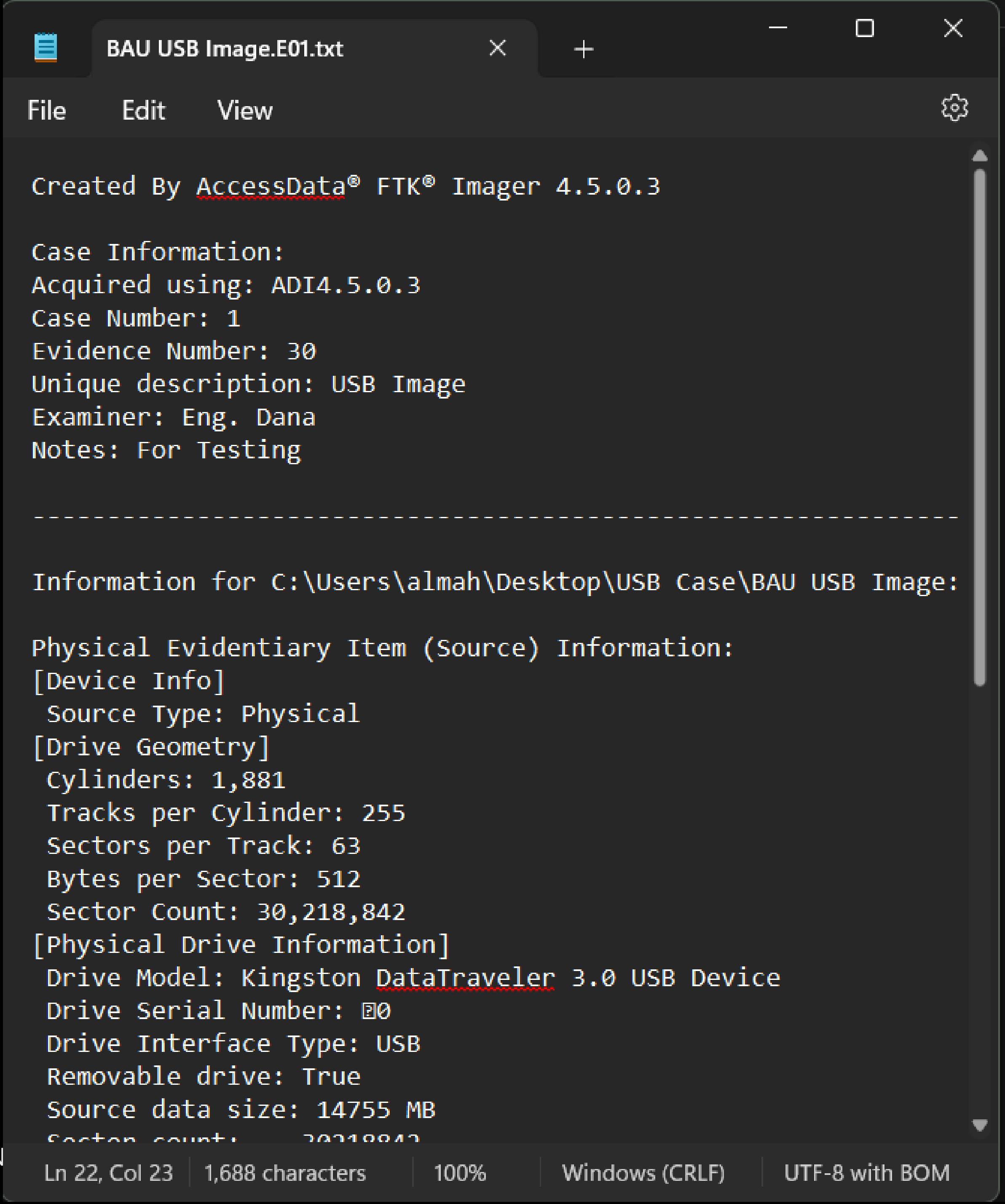
Image Summary

```
 Cylinders: 1,881
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 30,218,842
[Physical Drive Information]
 Drive Model: Kingston DataTraveler 3.0 USB Device
 Drive Serial Number: □0
 Drive Interface Type: USB
 Removable drive: True
 Source data size: 14755 MB
 Sector count:    30218842
[Computed Hashes]
 MD5 checksum:    5e6bb47bbe8623a24fc1be537119b259
 SHA1 checksum:   1c70ca0008d5019afa052d90b593b04b1192e9f2

Image Information:
 Acquisition started:   Mon Nov  4 10:14:54 2024
 Acquisition finished:  Mon Nov  4 10:31:11 2024
 Segment list:
  C:\Users\almah\Desktop\USB Case\BAU USB Image.E01
  C:\Users\almah\Desktop\USB Case\BAU USB Image.E02
  C:\Users\almah\Desktop\USB Case\BAU USB Image.E03
  C:\Users\almah\Desktop\USB Case\BAU USB Image.E04
  C:\Users\almah\Desktop\USB Case\BAU USB Image.E05
  C:\Users\almah\Desktop\USB Case\BAU USB Image.E06
```

# Result of USB Image



| Name | Date modified | Type | Size |
|---|---|---|---|
| BAU USB Image.E01 | 04-Nov-2024 10:16 | E01 File | 1,535,828 ... |
| BAU USB Image.E01 | 04-Nov-2024 10:31 | Microsoft Excel Co... | 714 KB |
| BAU USB Image.E01 | 04-Nov-2024 10:33 | Text Document | 2 KB |
| BAU USB Image.E02 | 04-Nov-2024 10:18 | E02 File | 1,535,948 ... |
| BAU USB Image.E03 | 04-Nov-2024 10:19 | E03 File | 1,535,818 ... |
| BAU USB Image.E04 | 04-Nov-2024 10:21 | E04 File | 1,535,884 ... |
| BAU USB Image.E05 | 04-Nov-2024 10:23 | E05 File | 1,535,952 ... |
| BAU USB Image.E06 | 04-Nov-2024 10:26 | E06 File | 1,535,907 ... |
| BAU USB Image.E07 | 04-Nov-2024 10:30 | E07 File | 1,535,915 ... |
| BAU USB Image.E08 | 04-Nov-2024 10:31 | E08 File | 327,590 KB |

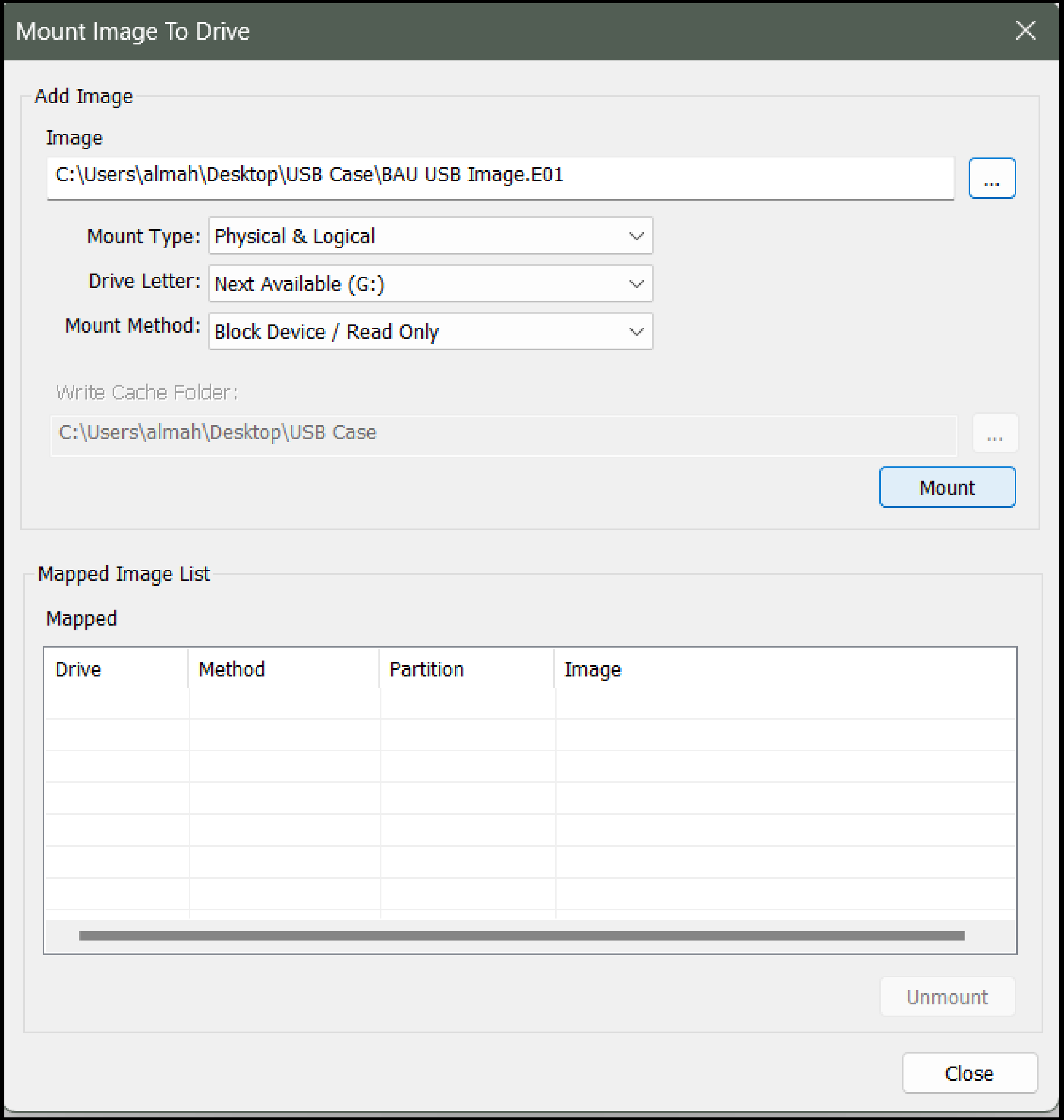


```
Created By AccessData® FTK® Imager 4.5.0.3

Case Information:
Acquired using: ADI4.5.0.3
Case Number: 1
Evidence Number: 30
Unique description: USB Image
Examiner: Eng. Dana
Notes: For Testing

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

Information for C:\Users\almah\Desktop\USB Case\BAU USB Image:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 1,881
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 30,218,842
[Physical Drive Information]
 Drive Model: Kingston DataTraveler 3.0 USB Device
 Drive Serial Number: □0
 Drive Interface Type: USB
 Removable drive: True
 Source data size: 14755 MB
 Sector count:    30218842
```

# Disk Mounting

- A disk image is a file that contains a complete copy of a storage device, including its file system, files, and metadata. Common formats include `.E01` (EnCase image files) and `.dd` or `.img` (raw image files).

- When you mount a disk image, you are essentially telling FTK to treat the image like a physical drive or partition, allowing you to access its contents.
- The software reads the disk image, interprets its file system, and makes the files and directories within that image accessible for forensic analysis.



Mount Image To Drive

Add Image

Image: C:\Users\almah\Desktop\USB Case\BAU USB Image.E01

Mount Type: Physical & Logical

Drive Letter: Next Available (G:)

Mount Method: Block Device / Read Only

Write Cache Folder: C:\Users\almah\Desktop\USB Case

Mapped Image List

Mapped

| Drive | Method | Partition | Image |
|---|---|---|---|

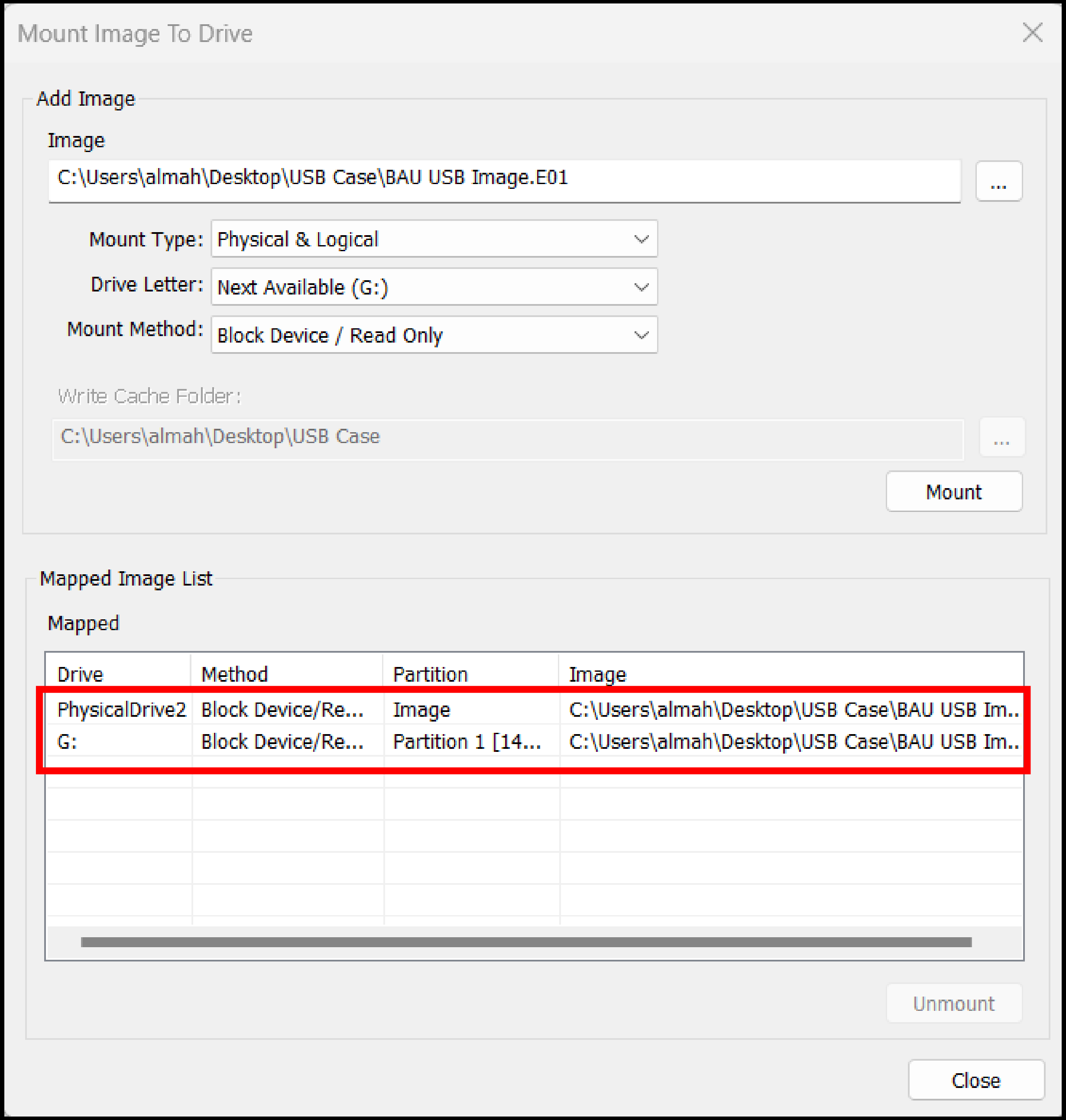
# Why is Mounting

- Q: Why is Mounting Important in Forensics?

- Efficiency: It provides a user-friendly way to access and analyze the contents of disk images without needing to write complex scripts or commands.

- Comprehensive Analysis: Mounting allows analysts to use FTK's advanced tools to conduct detailed investigations.

- Data Integrity: By working with a disk image rather than the original storage device, forensic investigators can ensure that the original evidence remains unaltered and can be preserved for legal proceedings.



Mount Image To Drive

Add Image

Image: C:\Users\almah\Desktop\USB Case\BAU USB Image.E01

Mount Type: Physical & Logical

Drive Letter: Next Available (G:)

Mount Method: Block Device / Read Only

Write Cache Folder: C:\Users\almah\Desktop\USB Case

Mapped Image List

Mapped

| Drive | Method | Partition | Image |
|---|---|---|---|
| PhysicalDrive2 | Block Device/Re... | Image | C:\Users\almah\Desktop\USB Case\BAU USB Im... |
| G: | Block Device/Re... | Partition 1 [14... | C:\Users\almah\Desktop\USB Case\BAU USB Im... |

# Day 20

- Outline
    - RAM Forensics
    - Analyze Memory
    - Volatility
        1. Imageinfo
        2. Pslist
        3. Pstree
        4. Malfind
        5. procdump -D
        6. Dlllist
        7. Getsids
        8. Privs
        9. Hashdump
        10. Netscan
        11. Cmdscan
        12. Iehistory
    - Threads
    - CPU

# RAM Forensics

- `RAM Forensics`: is the process of analyzing the contents of a computer's RAM (Random Access Memory) to extract valuable information that can aid in forensic investigations.

- RAM stores data temporarily while the system is running, including active processes, open files, network connections, and other volatile information that disappears when the system is powered off.
- By capturing and analyzing this data, investigators can gain insights into system activity and user behavior.

# Analyze Memory

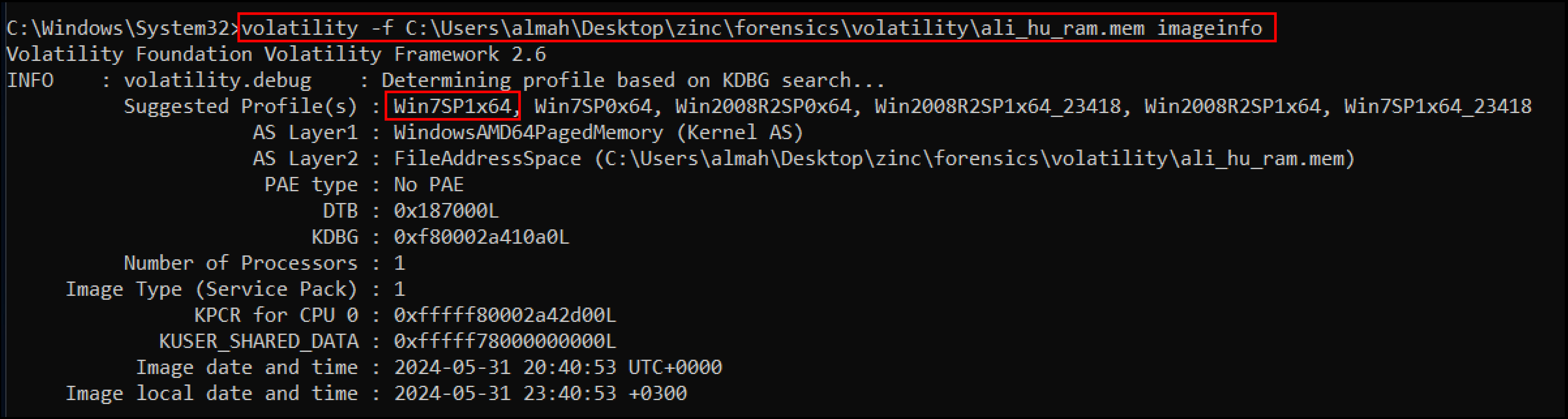
1. Malware Program
2. Hidden Processes
3. Listening Services
4. Network Connection
5. Registry Content
6. DLL Analysis
7. Password in clear Text

# Volatility

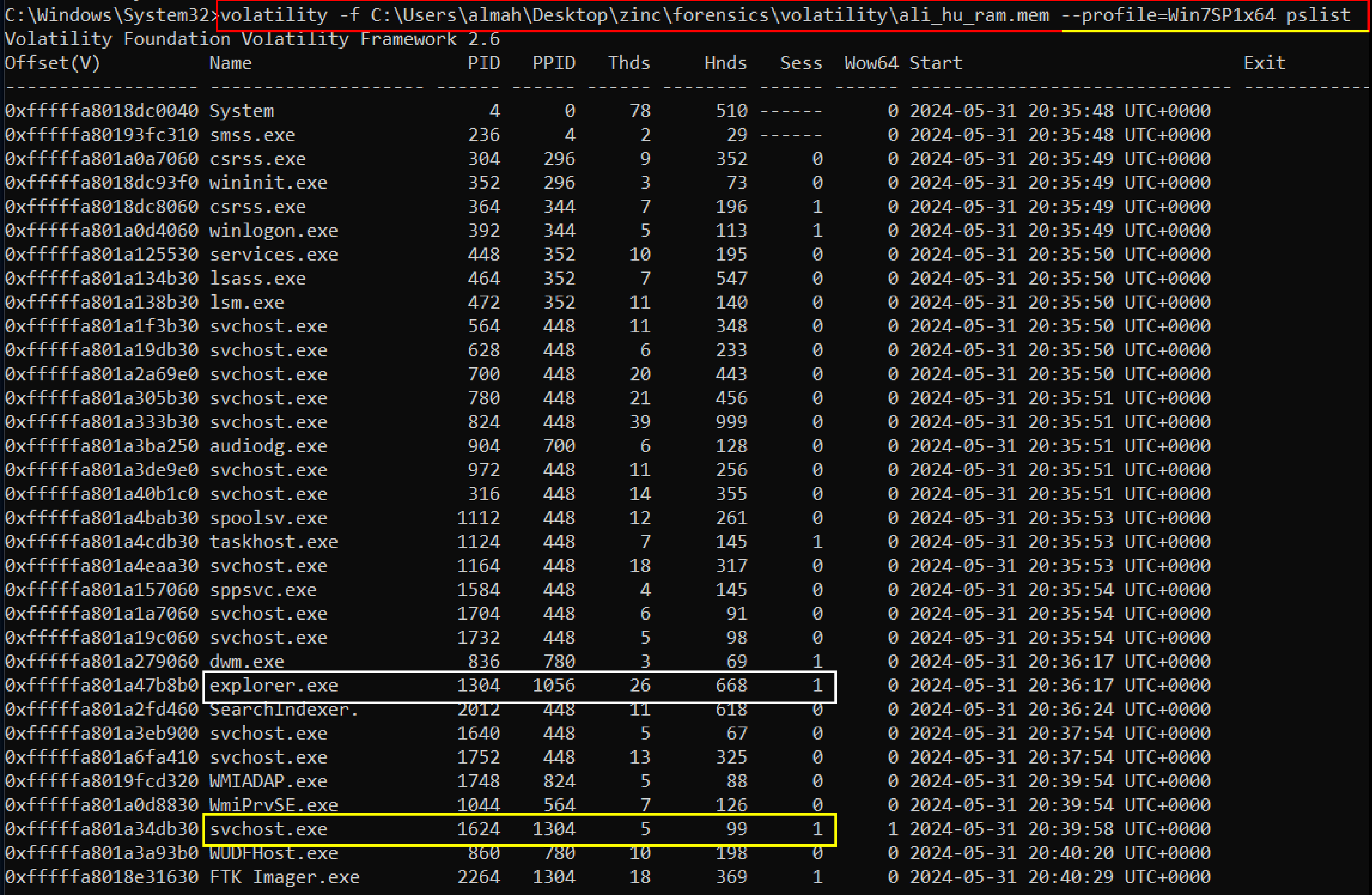
- Volatility is a powerful memory forensics framework used to analyze RAM dumps, for forensic and incident response purposes.
- Note: After Download it in Windows OS put the Application Path in Path variable in System Environment , or copy past the App in one of the Apps in Path variable (to be able to run in everywhere)
- Open CMD in Windows:
- `volatility --info` → app version & all command that you can use
- OS support **profile** → what is the OS for **Victim Device**.

# Imageinfo

- volatility -f <Path\to\.mem> imageinfo
- volatility -f C:\Users\almah\Desktop\zinc\forensics\volatility\ali_hu_ram.mem **imageinfo**



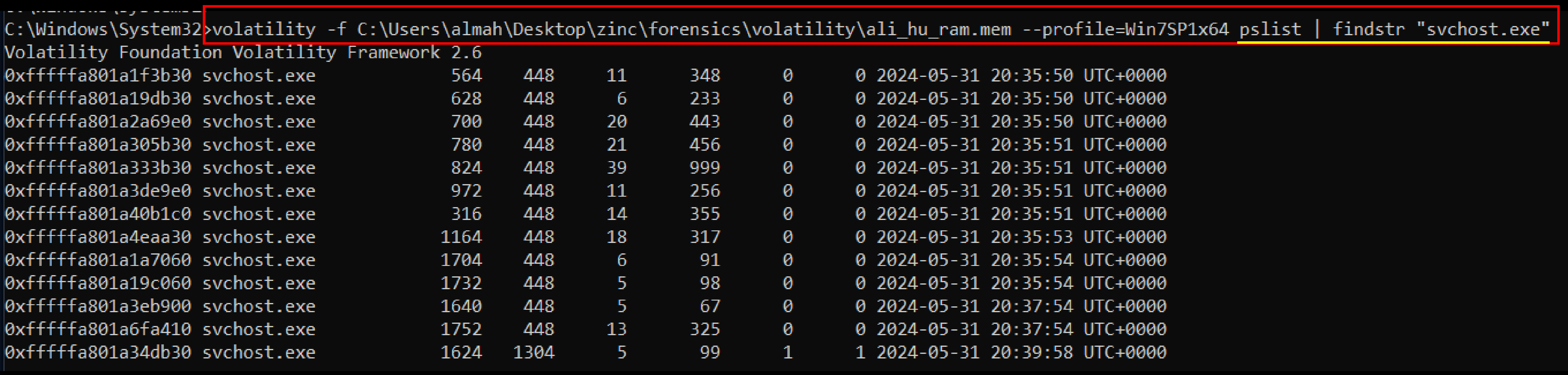
```
C:\Windows\System32>volatility -f C:\Users\almah\Desktop\zinc\forensics\volatility\ali_hu_ram.mem imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_23418
                     AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (C:\Users\almah\Desktop\zinc\forensics\volatility\ali_hu_ram.mem)
                      PAE type : No PAE
                           DTB : 0x187000L
                          KDBG : 0xf80002a410a0L
          Number of Processors : 1
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0xfffff80002a42d00L
             KUSER_SHARED_DATA : 0xfffff78000000000L
           Image date and time : 2024-05-31 20:40:53 UTC+0000
     Image local date and time : 2024-05-31 23:40:53 +0300
```



```
C:\Windows\System32>volatility -f C:\Users\almah\Desktop\zinc\forensics\volatility\ali_hu_ram.mem --profile=Win7SP1x64 pslist
Volatility Foundation Volatility Framework 2.6
Offset(V)          Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
------------------ -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------
0xfffffa8018dc0040 System                    4      0     78      510 ------      0 2024-05-31 20:35:48 UTC+0000
0xfffffa80193fc310 smss.exe                236      4      2       29 ------      0 2024-05-31 20:35:48 UTC+0000
0xfffffa801a0a7060 csrss.exe               304    296      9      352      0      0 2024-05-31 20:35:49 UTC+0000
0xfffffa8018dc93f0 wininit.exe             352    296      3       73      0      0 2024-05-31 20:35:49 UTC+0000
0xfffffa8018dc8060 csrss.exe               364    344      7      196      1      0 2024-05-31 20:35:49 UTC+0000
0xfffffa801a0d4060 winlogon.exe            392    344      5      113      1      0 2024-05-31 20:35:49 UTC+0000
0xfffffa801a125530 services.exe            448    352     10      195      0      0 2024-05-31 20:35:50 UTC+0000
0xfffffa801a134b30 lsass.exe               464    352      7      547      0      0 2024-05-31 20:35:50 UTC+0000
0xfffffa801a138b30 lsm.exe                 472    352     11      140      0      0 2024-05-31 20:35:50 UTC+0000
0xfffffa801a1f3b30 svchost.exe             564    448     11      348      0      0 2024-05-31 20:35:50 UTC+0000
0xfffffa801a19db30 svchost.exe             628    448      6      233      0      0 2024-05-31 20:35:50 UTC+0000
0xfffffa801a2a69e0 svchost.exe             700    448     20      443      0      0 2024-05-31 20:35:50 UTC+0000
0xfffffa801a305b30 svchost.exe             780    448     21      456      0      0 2024-05-31 20:35:51 UTC+0000
0xfffffa801a333b30 svchost.exe             824    448     39      999      0      0 2024-05-31 20:35:51 UTC+0000
0xfffffa801a3ba250 audiodg.exe             904    700      6      128      0      0 2024-05-31 20:35:51 UTC+0000
0xfffffa801a3de9e0 svchost.exe             972    448     11      256      0      0 2024-05-31 20:35:51 UTC+0000
0xfffffa801a40b1c0 svchost.exe             316    448     14      355      0      0 2024-05-31 20:35:51 UTC+0000
0xfffffa801a4bab30 spoolsv.exe            1112    448     12      261      0      0 2024-05-31 20:35:53 UTC+0000
0xfffffa801a4cdb30 taskhost.exe           1124    448      7      145      1      0 2024-05-31 20:35:53 UTC+0000
0xfffffa801a4eaa30 svchost.exe            1164    448     18      317      0      0 2024-05-31 20:35:53 UTC+0000
0xfffffa801a157060 sppsvc.exe             1584    448      4      145      0      0 2024-05-31 20:35:54 UTC+0000
0xfffffa801a1a7060 svchost.exe            1704    448      6       91      0      0 2024-05-31 20:35:54 UTC+0000
0xfffffa801a19c060 svchost.exe            1732    448      5       98      0      0 2024-05-31 20:35:54 UTC+0000
0xfffffa801a279060 dwm.exe                 836    780      3       69      1      0 2024-05-31 20:36:17 UTC+0000
0xfffffa801a47b8b0 explorer.exe           1304   1056     26      668      1      0 2024-05-31 20:36:17 UTC+0000
0xfffffa801a2fd460 SearchIndexer.         2012    448     11      618      0      0 2024-05-31 20:36:24 UTC+0000
0xfffffa801a3eb900 svchost.exe            1640    448      5       67      0      0 2024-05-31 20:37:54 UTC+0000
0xfffffa801a6fa410 svchost.exe            1752    448     13      325      0      0 2024-05-31 20:37:54 UTC+0000
0xfffffa8019fcd320 WMIADAP.exe            1748    824      5       88      0      0 2024-05-31 20:39:54 UTC+0000
0xfffffa801a0d8830 WmiPrvSE.exe           1044    564      7      126      0      0 2024-05-31 20:39:54 UTC+0000
0xfffffa801a34db30 svchost.exe            1624   1304      5       99      1      1 2024-05-31 20:39:58 UTC+0000
0xfffffa801a3a93b0 WUDFHost.exe            860    780     10      198      0      0 2024-05-31 20:40:20 UTC+0000
0xfffffa8018e31630 FTK Imager.exe         2264   1304     18      369      1      0 2024-05-31 20:40:29 UTC+0000
```

# Volatility Command

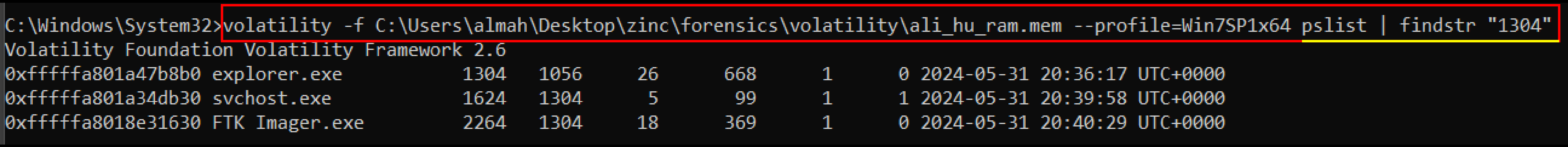
- volatility -f <Path\to\.mem> **--profile=Win7SP1x64** **pslist**
- **--info**
- **imageinfo**
- **--profile = <profile-name>**
- **pslist**
- **findstr = <str>**
- volatility -f <Path\to\.mem> --profile=Win7SP1x64 pslist | **findstr** "svchost.exe"



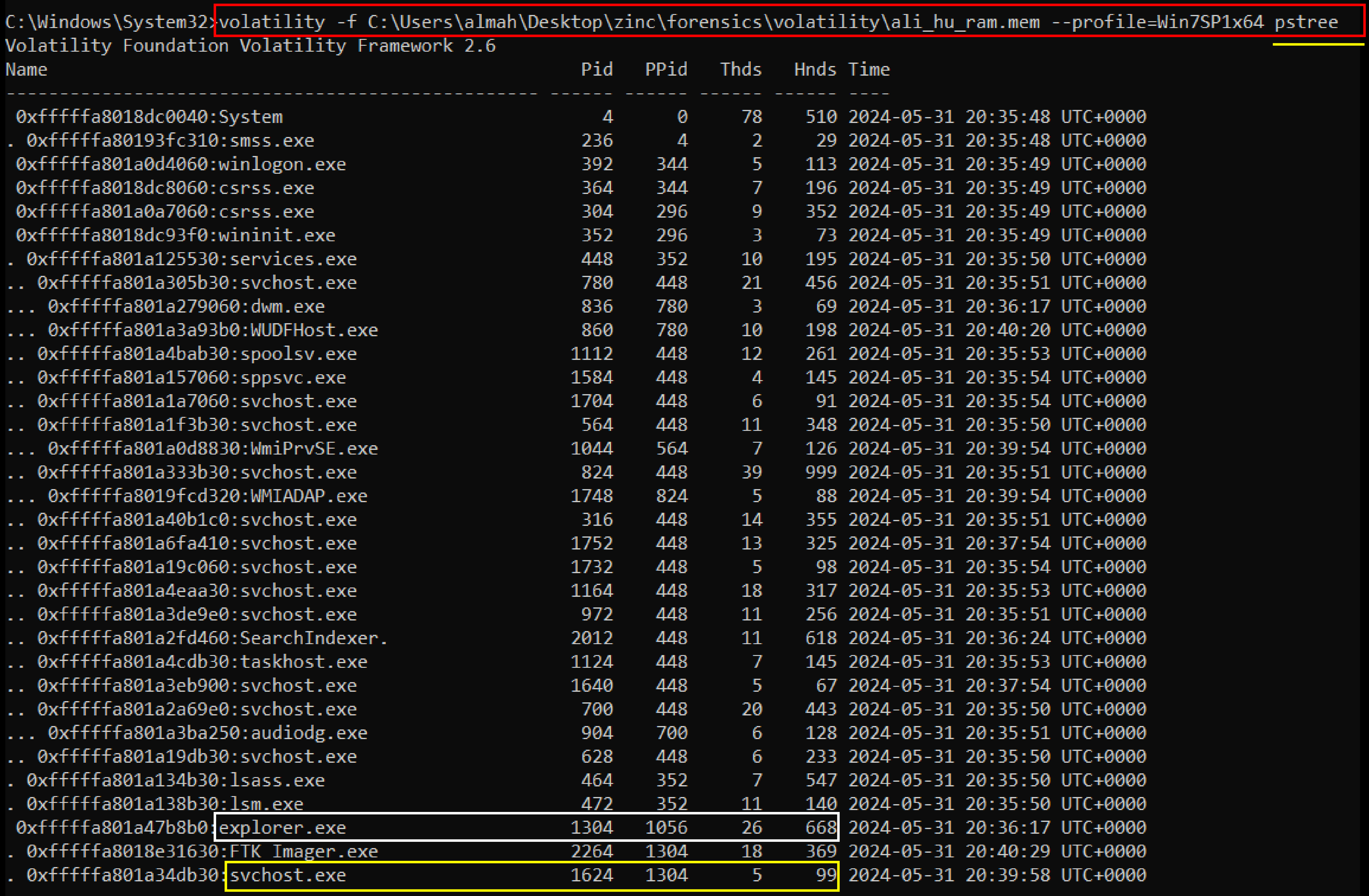
```
C:\Windows\System32>volatility -f C:\Users\almah\Desktop\zinc\forensics\volatility\ali_hu_ram.mem --profile=Win7SP1x64 pslist | findstr "svchost.exe"
Volatility Foundation Volatility Framework 2.6
0xfffffa801a1f3b30 svchost.exe             564    448     11      348      0      0 2024-05-31 20:35:50 UTC+0000
0xfffffa801a19db30 svchost.exe             628    448      6      233      0      0 2024-05-31 20:35:50 UTC+0000
0xfffffa801a2a69e0 svchost.exe             700    448     20      443      0      0 2024-05-31 20:35:50 UTC+0000
0xfffffa801a305b30 svchost.exe             780    448     21      456      0      0 2024-05-31 20:35:51 UTC+0000
0xfffffa801a333b30 svchost.exe             824    448     39      999      0      0 2024-05-31 20:35:51 UTC+0000
0xfffffa801a3de9e0 svchost.exe             972    448     11      256      0      0 2024-05-31 20:35:51 UTC+0000
0xfffffa801a40b1c0 svchost.exe             316    448     14      355      0      0 2024-05-31 20:35:51 UTC+0000
0xfffffa801a4eaa30 svchost.exe            1164    448     18      317      0      0 2024-05-31 20:35:53 UTC+0000
0xfffffa801a1a7060 svchost.exe            1704    448      6       91      0      0 2024-05-31 20:35:54 UTC+0000
0xfffffa801a19c060 svchost.exe            1732    448      5       98      0      0 2024-05-31 20:35:54 UTC+0000
0xfffffa801a3eb900 svchost.exe            1640    448      5       67      0      0 2024-05-31 20:37:54 UTC+0000
0xfffffa801a6fa410 svchost.exe            1752    448     13      325      0      0 2024-05-31 20:37:54 UTC+0000
0xfffffa801a34db30 svchost.exe            1624   1304      5       99      1      1 2024-05-31 20:39:58 UTC+0000
```

# Findstr

- volatility -f <Path> --profile=Win7SP1x64 pslist | **findstr "1304"**



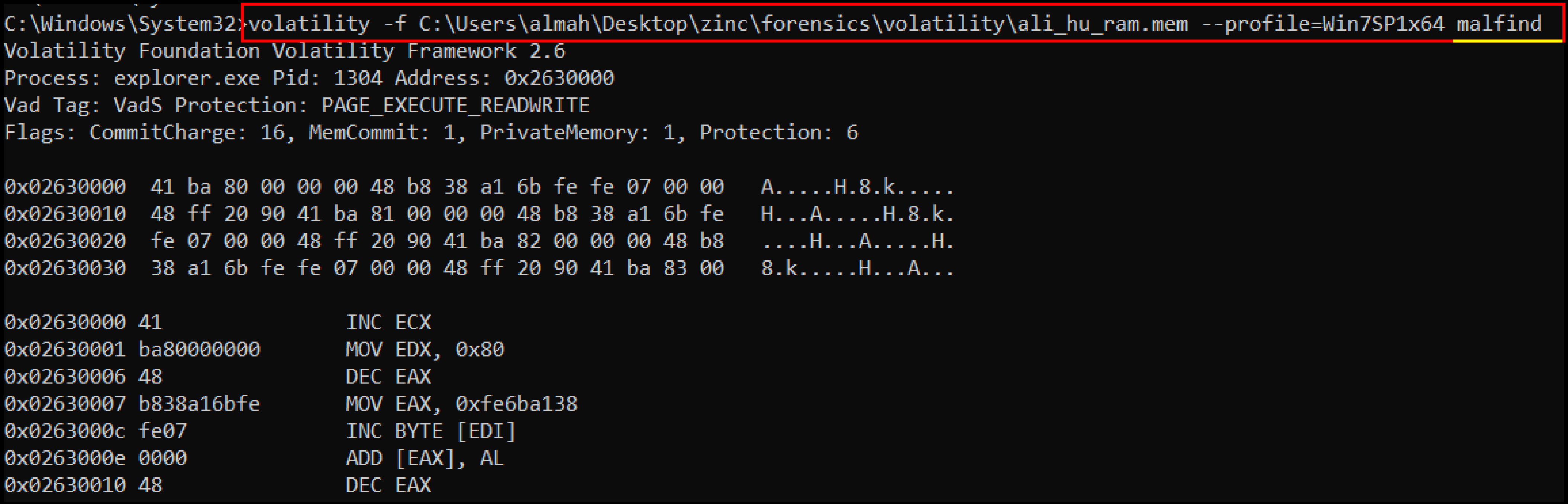
```
C:\Windows\System32>volatility -f C:\Users\almah\Desktop\zinc\forensics\volatility\ali_hu_ram.mem --profile=Win7SP1x64 pslist | findstr "1304"
Volatility Foundation Volatility Framework 2.6
0xfffffa801a47b8b0 explorer.exe           1304   1056     26      668      1      0 2024-05-31 20:36:17 UTC+0000
0xfffffa801a34db30 svchost.exe            1624   1304      5       99      1      1 2024-05-31 20:39:58 UTC+0000
0xfffffa8018e31630 FTK Imager.exe         2264   1304     18      369      1      0 2024-05-31 20:40:29 UTC+0000
```



```
C:\Windows\System32>volatility -f C:\Users\almah\Desktop\zinc\forensics\volatility\ali_hu_ram.mem --profile=Win7SP1x64 pstree
Volatility Foundation Volatility Framework 2.6
Name                                                  Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0xfffffa8018dc0040:System                              4      0     78    510 2024-05-31 20:35:48 UTC+0000
. 0xfffffa80193fc310:smss.exe                         236      4      2     29 2024-05-31 20:35:48 UTC+0000
 0xfffffa801a0d4060:winlogon.exe                      392    344      5    113 2024-05-31 20:35:49 UTC+0000
 0xfffffa8018dc8060:csrss.exe                         364    344      7    196 2024-05-31 20:35:49 UTC+0000
 0xfffffa801a0a7060:csrss.exe                         304    296      9    352 2024-05-31 20:35:49 UTC+0000
 0xfffffa8018dc93f0:wininit.exe                       352    296      3     73 2024-05-31 20:35:49 UTC+0000
. 0xfffffa801a125530:services.exe                     448    352     10    195 2024-05-31 20:35:50 UTC+0000
.. 0xfffffa801a305b30:svchost.exe                     780    448     21    456 2024-05-31 20:35:51 UTC+0000
... 0xfffffa801a279060:dwm.exe                        836    780      3     69 2024-05-31 20:36:17 UTC+0000
... 0xfffffa801a3a93b0:WUDFHost.exe                   860    780     10    198 2024-05-31 20:40:20 UTC+0000
.. 0xfffffa801a4bab30:spoolsv.exe                    1112    448     12    261 2024-05-31 20:35:53 UTC+0000
.. 0xfffffa801a157060:sppsvc.exe                     1584    448      4    145 2024-05-31 20:35:54 UTC+0000
.. 0xfffffa801a1a7060:svchost.exe                    1704    448      6     91 2024-05-31 20:35:54 UTC+0000
.. 0xfffffa801a1f3b30:svchost.exe                     564    448     11    348 2024-05-31 20:35:50 UTC+0000
... 0xfffffa801a0d8830:WmiPrvSE.exe                  1044    564      7    126 2024-05-31 20:39:54 UTC+0000
.. 0xfffffa801a333b30:svchost.exe                     824    448     39    999 2024-05-31 20:35:51 UTC+0000
... 0xfffffa8019fcd320:WMIADAP.exe                   1748    824      5     88 2024-05-31 20:39:54 UTC+0000
.. 0xfffffa801a40b1c0:svchost.exe                     316    448     14    355 2024-05-31 20:35:51 UTC+0000
.. 0xfffffa801a6fa410:svchost.exe                    1752    448     13    325 2024-05-31 20:37:54 UTC+0000
.. 0xfffffa801a19c060:svchost.exe                    1732    448      5     98 2024-05-31 20:35:54 UTC+0000
.. 0xfffffa801a4eaa30:svchost.exe                    1164    448     18    317 2024-05-31 20:35:53 UTC+0000
.. 0xfffffa801a3de9e0:svchost.exe                     972    448     11    256 2024-05-31 20:35:51 UTC+0000
.. 0xfffffa801a2fd460:SearchIndexer.                 2012    448     11    618 2024-05-31 20:36:24 UTC+0000
.. 0xfffffa801a4cdb30:taskhost.exe                   1124    448      7    145 2024-05-31 20:35:53 UTC+0000
.. 0xfffffa801a3eb900:svchost.exe                    1640    448      5     67 2024-05-31 20:37:54 UTC+0000
.. 0xfffffa801a2a69e0:svchost.exe                     700    448     20    443 2024-05-31 20:35:50 UTC+0000
... 0xfffffa801a3ba250:audiodg.exe                    904    700      6    128 2024-05-31 20:35:51 UTC+0000
.. 0xfffffa801a19db30:svchost.exe                     628    448      6    233 2024-05-31 20:35:50 UTC+0000
. 0xfffffa801a134b30:lsass.exe                        464    352      7    547 2024-05-31 20:35:50 UTC+0000
. 0xfffffa801a138b30:lsm.exe                          472    352     11    140 2024-05-31 20:35:50 UTC+0000
 0xfffffa801a47b8b0:explorer.exe                     1304   1056     26    668 2024-05-31 20:36:17 UTC+0000
. 0xfffffa8018e31630:FTK Imager.exe                  2264   1304     18    369 2024-05-31 20:40:29 UTC+0000
. 0xfffffa801a34db30:svchost.exe                     1624   1304      5     99 2024-05-31 20:39:58 UTC+0000
```

# Malware Find

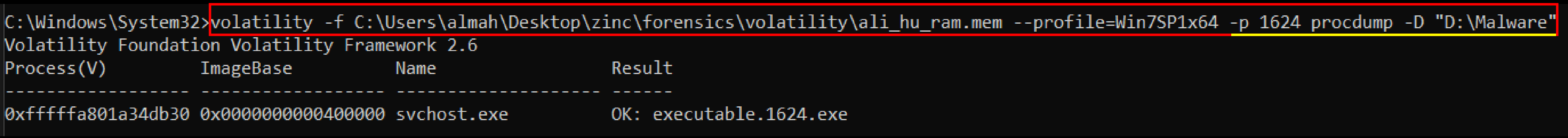
- volatility -f <Path..> --profile=Win7SP1x64 **malfind**



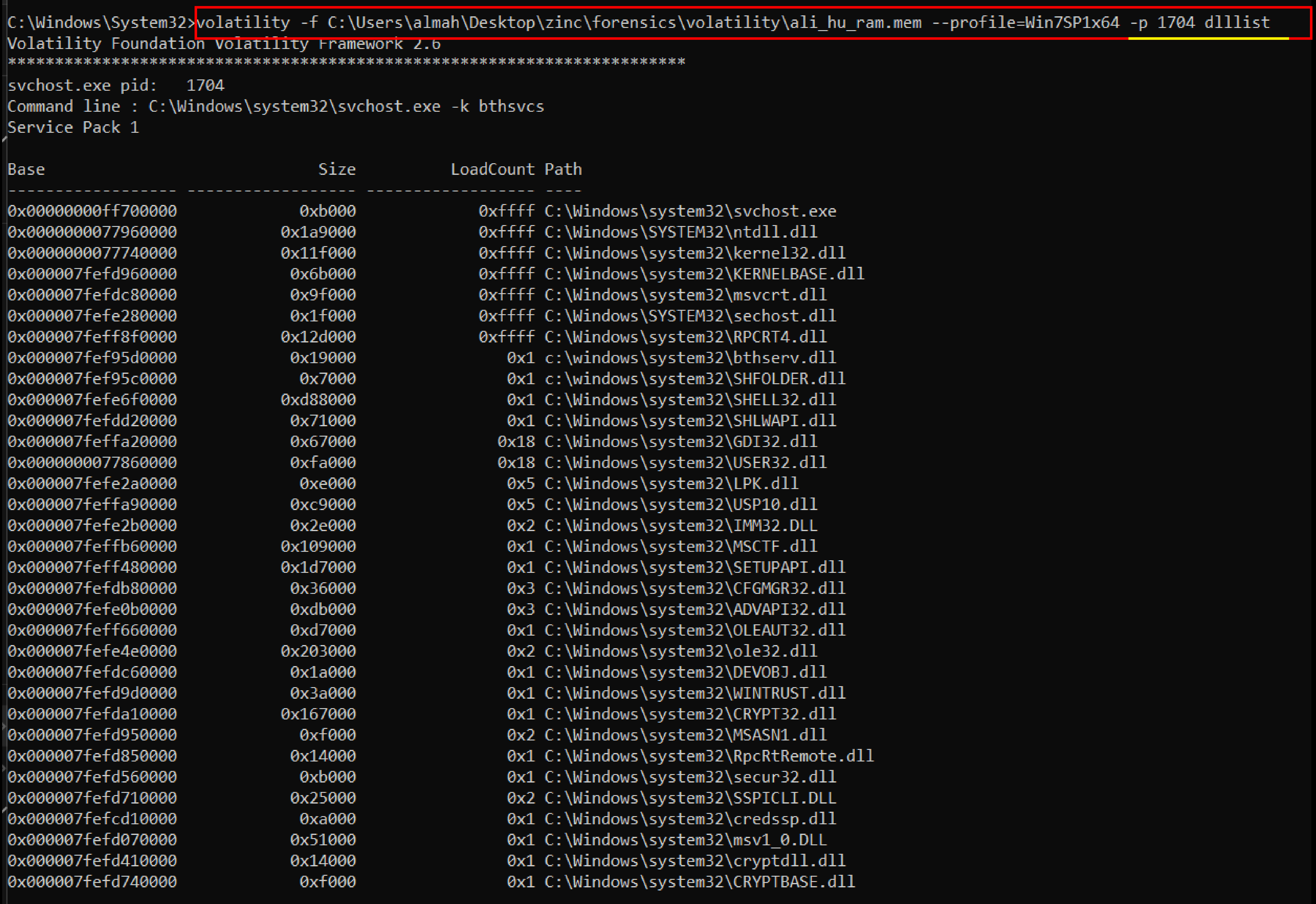
```
C:\Windows\System32>volatility -f C:\Users\almah\Desktop\zinc\forensics\volatility\ali_hu_ram.mem --profile=Win7SP1x64 malfind
Volatility Foundation Volatility Framework 2.6
Process: explorer.exe Pid: 1304 Address: 0x2630000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 16, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x02630000  41 ba 80 00 00 00 48 b8 38 a1 6b fe fe 07 00 00   A.....H.8.k.....
0x02630010  48 ff 20 90 41 ba 81 00 00 00 48 b8 38 a1 6b fe   H...A.....H.8.k.
0x02630020  fe 07 00 00 48 ff 20 90 41 ba 82 00 00 00 48 b8   ....H...A.....H.
0x02630030  38 a1 6b fe fe 07 00 00 48 ff 20 90 41 ba 83 00   8.k.....H...A...

0x02630000 41               INC ECX
0x02630001 ba80000000       MOV EDX, 0x80
0x02630006 48               DEC EAX
0x02630007 b838a16bfe       MOV EAX, 0xfe6ba138
0x0263000c fe07             INC BYTE [EDI]
0x0263000e 0000             ADD [EAX], AL
0x02630010 48               DEC EAX
```

# procdump -D

- volatility -f <Path..> --profile=Win7SP1x64 -p 1624 procdump -D "D:\Malware"



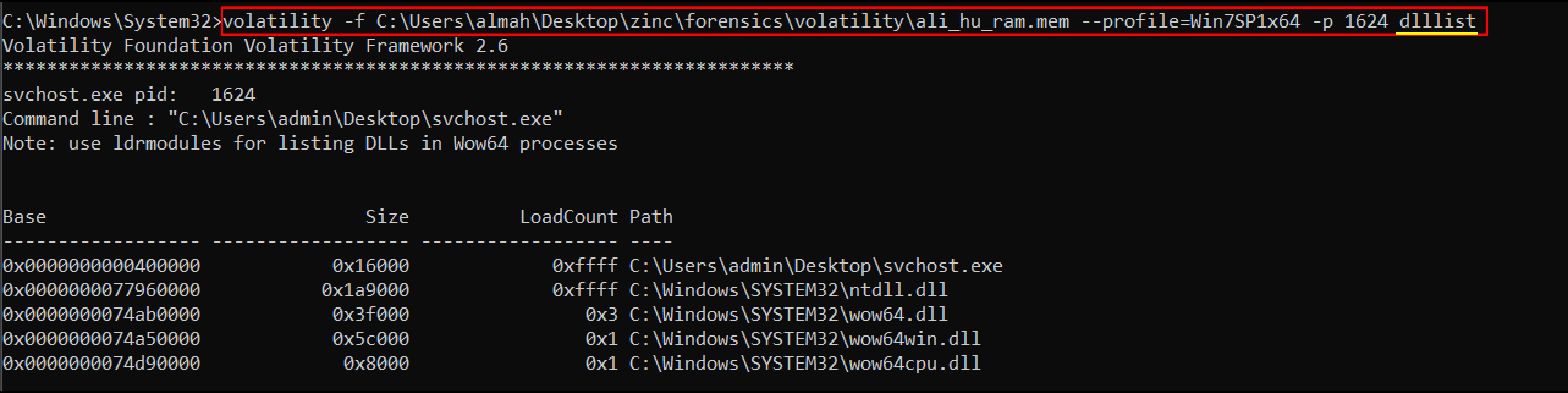
```
C:\Windows\System32>volatility -f C:\Users\almah\Desktop\zinc\forensics\volatility\ali_hu_ram.mem --profile=Win7SP1x64 -p 1624 procdump -D "D:\Malware"
Volatility Foundation Volatility Framework 2.6
Process(V)         ImageBase          Name                 Result
------------------ ------------------ -------------------- ------
0xfffffa801a34db30 0x0000000000400000 svchost.exe          OK: executable.1624.exe
```



```
C:\Windows\System32>volatility -f C:\Users\almah\Desktop\zinc\forensics\volatility\ali_hu_ram.mem --profile=Win7SP1x64 -p 1704 dlllist
Volatility Foundation Volatility Framework 2.6
************************************************************************
svchost.exe pid:   1704
Command line : C:\Windows\system32\svchost.exe -k bthsvcs
Service Pack 1

Base                             Size          LoadCount Path
------------------ ------------------ ------------------ ----
0x00000000ff700000             0xb000             0xffff C:\Windows\system32\svchost.exe
0x0000000077960000           0x1a9000             0xffff C:\Windows\SYSTEM32\ntdll.dll
0x0000000077740000           0x11f000             0xffff C:\Windows\system32\kernel32.dll
0x000007fefd960000            0x6b000             0xffff C:\Windows\system32\KERNELBASE.dll
0x000007fefdc80000            0x9f000             0xffff C:\Windows\system32\msvcrt.dll
0x000007fefe280000            0x1f000             0xffff C:\Windows\SYSTEM32\sechost.dll
0x000007feff8f0000           0x12d000             0xffff C:\Windows\system32\RPCRT4.dll
0x000007fef95d0000            0x19000                0x1 c:\windows\system32\bthserv.dll
0x000007fef95c0000             0x7000                0x1 c:\windows\system32\SHFOLDER.dll
0x000007fefe6f0000           0xd88000                0x1 C:\Windows\system32\SHELL32.dll
0x000007fefdd20000            0x71000                0x1 C:\Windows\system32\SHLWAPI.dll
0x000007feffa20000            0x67000               0x18 C:\Windows\system32\GDI32.dll
0x0000000077860000            0xfa000               0x18 C:\Windows\system32\USER32.dll
0x000007fefe2a0000             0xe000                0x5 C:\Windows\system32\LPK.dll
0x000007feffa90000            0xc9000                0x5 C:\Windows\system32\USP10.dll
0x000007fefe2b0000            0x2e000                0x2 C:\Windows\system32\IMM32.DLL
0x000007feffb60000           0x109000                0x1 C:\Windows\system32\MSCTF.dll
0x000007feff480000           0x1d7000                0x1 C:\Windows\system32\SETUPAPI.dll
0x000007fefdb80000            0x36000                0x3 C:\Windows\system32\CFGMGR32.dll
0x000007fefe0b0000            0xdb000                0x3 C:\Windows\system32\ADVAPI32.dll
0x000007feff660000            0xd7000                0x1 C:\Windows\system32\OLEAUT32.dll
0x000007fefe4e0000           0x203000                0x2 C:\Windows\system32\ole32.dll
0x000007fefdc60000            0x1a000                0x1 C:\Windows\system32\DEVOBJ.dll
0x000007fefd9d0000            0x3a000                0x1 C:\Windows\system32\WINTRUST.dll
0x000007fefda10000           0x167000                0x1 C:\Windows\system32\CRYPT32.dll
0x000007fefd950000             0xf000                0x2 C:\Windows\system32\MSASN1.dll
0x000007fefd850000            0x14000                0x1 C:\Windows\system32\RpcRtRemote.dll
0x000007fefd560000             0xb000                0x1 C:\Windows\system32\secur32.dll
0x000007fefd710000            0x25000                0x2 C:\Windows\system32\SSPICLI.DLL
0x000007fefcd10000             0xa000                0x1 C:\Windows\system32\credssp.dll
0x000007fefd070000            0x51000                0x1 C:\Windows\system32\msv1_0.DLL
0x000007fefd410000            0x14000                0x1 C:\Windows\system32\cryptdll.dll
0x000007fefd740000             0xf000                0x1 C:\Windows\system32\CRYPTBASE.dll
```

# DLL List

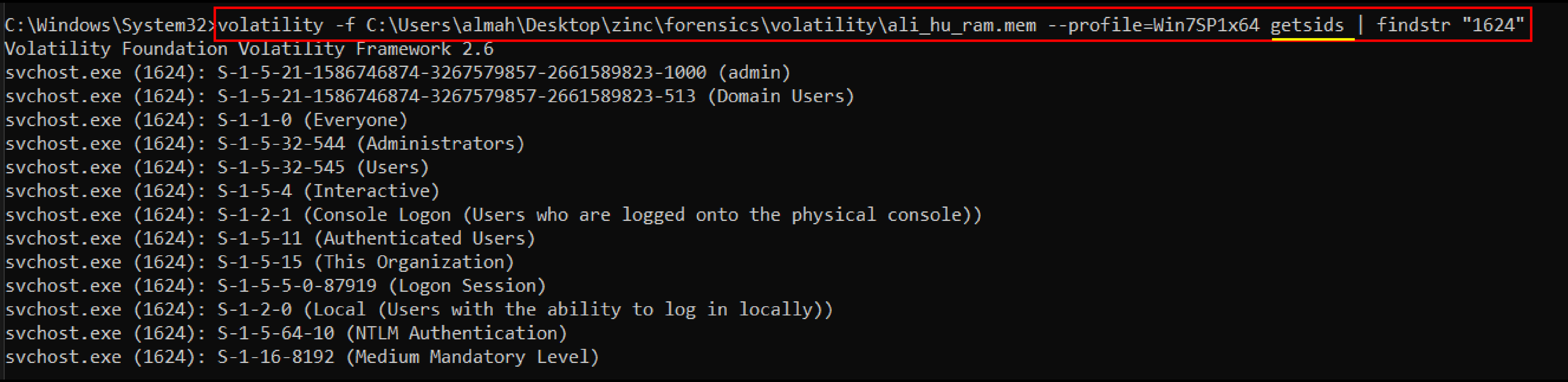
- volatility -f <Path..> --profile=Win7SP1x64 -p 1704 dlllist
- volatility -f <Path..> --profile=Win7SP1x64 -p 1624 dlllist
- **The DLL Must Be Same, because both are same program → No (May be Malware)**



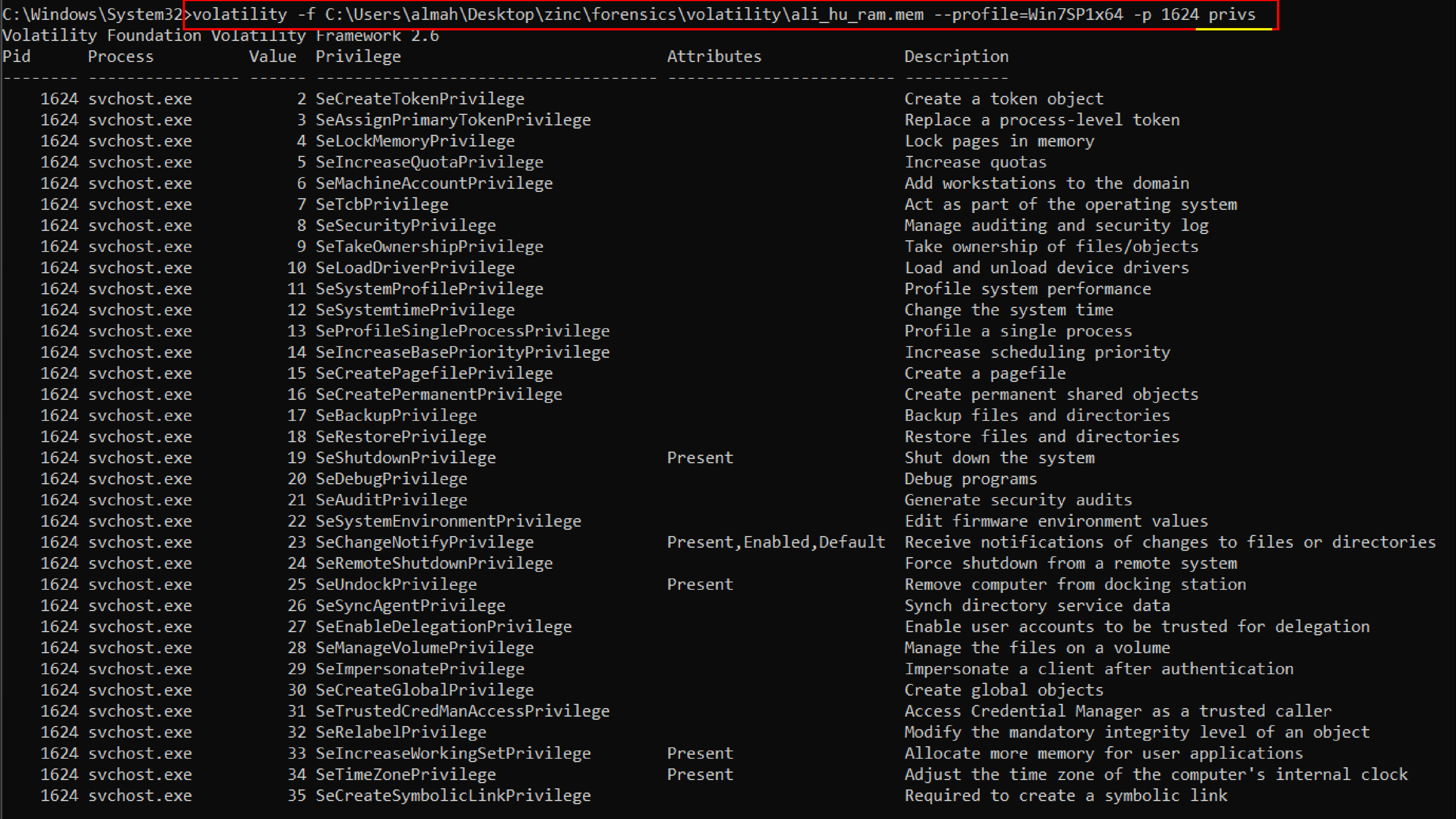
```
C:\Windows\System32>volatility -f C:\Users\almah\Desktop\zinc\forensics\volatility\ali_hu_ram.mem --profile=Win7SP1x64 -p 1624 dlllist
Volatility Foundation Volatility Framework 2.6
************************************************************************
svchost.exe pid:   1624
Command line : "C:\Users\admin\Desktop\svchost.exe"
Note: use ldrmodules for listing DLLs in Wow64 processes


Base                             Size          LoadCount Path
------------------ ------------------ ------------------ ----
0x0000000000400000            0x16000             0xffff C:\Users\admin\Desktop\svchost.exe
0x0000000077960000           0x1a9000             0xffff C:\Windows\SYSTEM32\ntdll.dll
0x0000000074ab0000            0x3f000                0x3 C:\Windows\SYSTEM32\wow64.dll
0x0000000074a50000            0x5c000                0x1 C:\Windows\SYSTEM32\wow64win.dll
0x0000000074d90000             0x8000                0x1 C:\Windows\SYSTEM32\wow64cpu.dll
```

# Get SID’s

- volatility -f <Path..> --profile=Win7SP1x64 **getsids** | findstr "1624"



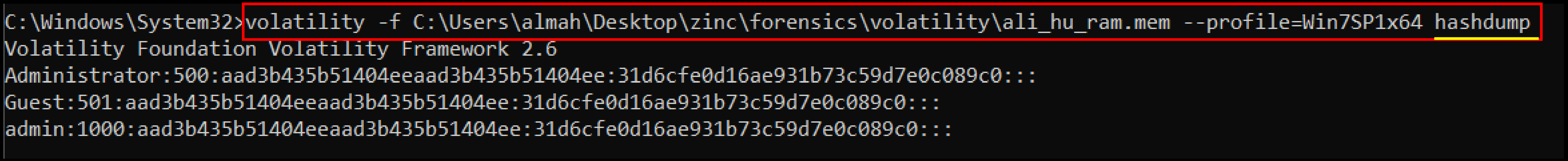
```
C:\Windows\System32>volatility -f C:\Users\almah\Desktop\zinc\forensics\volatility\ali_hu_ram.mem --profile=Win7SP1x64 getsids | findstr "1624"
Volatility Foundation Volatility Framework 2.6
svchost.exe (1624): S-1-5-21-1586746874-3267579857-2661589823-1000 (admin)
svchost.exe (1624): S-1-5-21-1586746874-3267579857-2661589823-513 (Domain Users)
svchost.exe (1624): S-1-1-0 (Everyone)
svchost.exe (1624): S-1-5-32-544 (Administrators)
svchost.exe (1624): S-1-5-32-545 (Users)
svchost.exe (1624): S-1-5-4 (Interactive)
svchost.exe (1624): S-1-2-1 (Console Logon (Users who are logged onto the physical console))
svchost.exe (1624): S-1-5-11 (Authenticated Users)
svchost.exe (1624): S-1-5-15 (This Organization)
svchost.exe (1624): S-1-5-5-0-87919 (Logon Session)
svchost.exe (1624): S-1-2-0 (Local (Users with the ability to log in locally))
svchost.exe (1624): S-1-5-64-10 (NTLM Authentication)
svchost.exe (1624): S-1-16-8192 (Medium Mandatory Level)
```



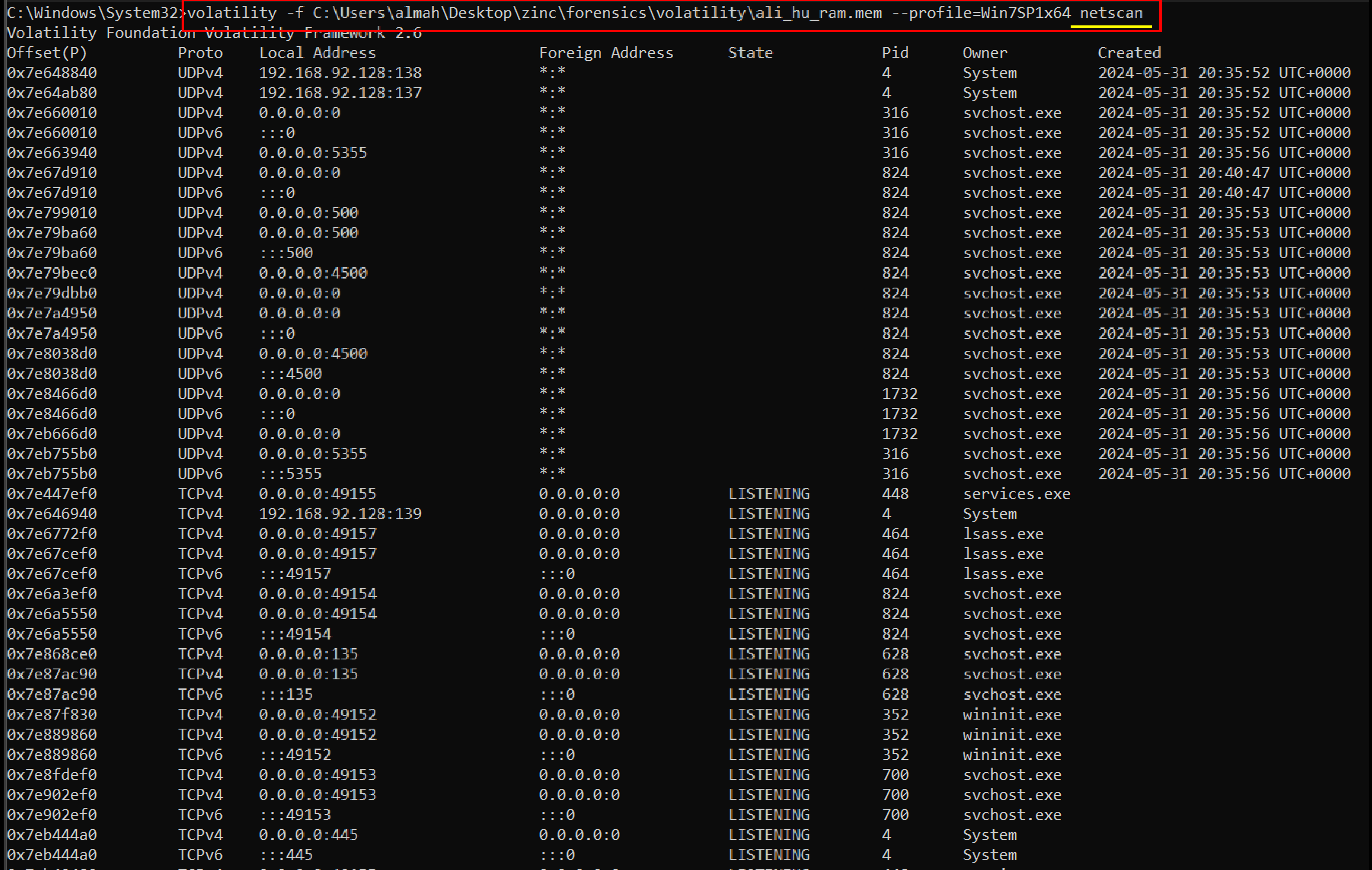
```
C:\Windows\System32>volatility -f C:\Users\almah\Desktop\zinc\forensics\volatility\ali_hu_ram.mem --profile=Win7SP1x64 -p 1624 privs
Volatility Foundation Volatility Framework 2.6
Pid      Process          Value  Privilege                            Attributes               Description
-------- ---------------- ------ ------------------------------------ ------------------------ -----------
    1624 svchost.exe           2 SeCreateTokenPrivilege                                        Create a token object
    1624 svchost.exe           3 SeAssignPrimaryTokenPrivilege                                 Replace a process-level token
    1624 svchost.exe           4 SeLockMemoryPrivilege                                         Lock pages in memory
    1624 svchost.exe           5 SeIncreaseQuotaPrivilege                                      Increase quotas
    1624 svchost.exe           6 SeMachineAccountPrivilege                                     Add workstations to the domain
    1624 svchost.exe           7 SeTcbPrivilege                                                Act as part of the operating system
    1624 svchost.exe           8 SeSecurityPrivilege                                           Manage auditing and security log
    1624 svchost.exe           9 SeTakeOwnershipPrivilege                                      Take ownership of files/objects
    1624 svchost.exe          10 SeLoadDriverPrivilege                                         Load and unload device drivers
    1624 svchost.exe          11 SeSystemProfilePrivilege                                      Profile system performance
    1624 svchost.exe          12 SeSystemtimePrivilege                                         Change the system time
    1624 svchost.exe          13 SeProfileSingleProcessPrivilege                               Profile a single process
    1624 svchost.exe          14 SeIncreaseBasePriorityPrivilege                               Increase scheduling priority
    1624 svchost.exe          15 SeCreatePagefilePrivilege                                     Create a pagefile
    1624 svchost.exe          16 SeCreatePermanentPrivilege                                    Create permanent shared objects
    1624 svchost.exe          17 SeBackupPrivilege                                             Backup files and directories
    1624 svchost.exe          18 SeRestorePrivilege                                            Restore files and directories
    1624 svchost.exe          19 SeShutdownPrivilege                  Present                  Shut down the system
    1624 svchost.exe          20 SeDebugPrivilege                                              Debug programs
    1624 svchost.exe          21 SeAuditPrivilege                                              Generate security audits
    1624 svchost.exe          22 SeSystemEnvironmentPrivilege                                  Edit firmware environment values
    1624 svchost.exe          23 SeChangeNotifyPrivilege              Present,Enabled,Default  Receive notifications of changes to files or directories
    1624 svchost.exe          24 SeRemoteShutdownPrivilege                                     Force shutdown from a remote system
    1624 svchost.exe          25 SeUndockPrivilege                    Present                  Remove computer from docking station
    1624 svchost.exe          26 SeSyncAgentPrivilege                                          Synch directory service data
    1624 svchost.exe          27 SeEnableDelegationPrivilege                                   Enable user accounts to be trusted for delegation
    1624 svchost.exe          28 SeManageVolumePrivilege                                       Manage the files on a volume
    1624 svchost.exe          29 SeImpersonatePrivilege                                        Impersonate a client after authentication
    1624 svchost.exe          30 SeCreateGlobalPrivilege                                       Create global objects
    1624 svchost.exe          31 SeTrustedCredManAccessPrivilege                               Access Credential Manager as a trusted caller
    1624 svchost.exe          32 SeRelabelPrivilege                                            Modify the mandatory integrity level of an object
    1624 svchost.exe          33 SeIncreaseWorkingSetPrivilege        Present                  Allocate more memory for user applications
    1624 svchost.exe          34 SeTimeZonePrivilege                  Present                  Adjust the time zone of the computer's internal clock
    1624 svchost.exe          35 SeCreateSymbolicLinkPrivilege                                 Required to create a symbolic link
```

# More….

- volatility -f <Path..> --profile=Win7SP1x64 -p 1624 privs
- volatility -f <Path..> --profile=Win7SP1x64 hashdump
- volatility -f <Path..> --profile=Win7SP1x64 netscan
- volatility -f <Path..> --profile=Win7SP1x64 cmdscan
- volatility -f <Path..> --profile=Win7SP1x64 iehistory



```
C:\Windows\System32>volatility -f C:\Users\almah\Desktop\zinc\forensics\volatility\ali_hu_ram.mem --profile=Win7SP1x64 hashdump
Volatility Foundation Volatility Framework 2.6
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
admin:1000:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```



```
C:\Windows\System32>volatility -f C:\Users\almah\Desktop\zinc\forensics\volatility\ali_hu_ram.mem --profile=Win7SP1x64 netscan
Volatility Foundation Volatility Framework 2.6
Offset(P)          Proto    Local Address                  Foreign Address      State            Pid      Owner          Created
0x7e648840         UDPv4    192.168.92.128:138             *:*                                   4        System         2024-05-31 20:35:52 UTC+0000
0x7e64ab80         UDPv4    192.168.92.128:137             *:*                                   4        System         2024-05-31 20:35:52 UTC+0000
0x7e660010         UDPv4    0.0.0.0:0                      *:*                                   316      svchost.exe    2024-05-31 20:35:52 UTC+0000
0x7e660010         UDPv6    :::0                           *:*                                   316      svchost.exe    2024-05-31 20:35:52 UTC+0000
0x7e663940         UDPv4    0.0.0.0:5355                   *:*                                   316      svchost.exe    2024-05-31 20:35:56 UTC+0000
0x7e67d910         UDPv4    0.0.0.0:0                      *:*                                   824      svchost.exe    2024-05-31 20:40:47 UTC+0000
0x7e67d910         UDPv6    :::0                           *:*                                   824      svchost.exe    2024-05-31 20:40:47 UTC+0000
0x7e799010         UDPv4    0.0.0.0:500                    *:*                                   824      svchost.exe    2024-05-31 20:35:53 UTC+0000
0x7e79ba60         UDPv4    0.0.0.0:500                    *:*                                   824      svchost.exe    2024-05-31 20:35:53 UTC+0000
0x7e79ba60         UDPv6    :::500                         *:*                                   824      svchost.exe    2024-05-31 20:35:53 UTC+0000
0x7e79bec0         UDPv4    0.0.0.0:4500                   *:*                                   824      svchost.exe    2024-05-31 20:35:53 UTC+0000
0x7e79dbb0         UDPv4    0.0.0.0:0                      *:*                                   824      svchost.exe    2024-05-31 20:35:53 UTC+0000
0x7e7a4950         UDPv4    0.0.0.0:0                      *:*                                   824      svchost.exe    2024-05-31 20:35:53 UTC+0000
0x7e7a4950         UDPv6    :::0                           *:*                                   824      svchost.exe    2024-05-31 20:35:53 UTC+0000
0x7e8038d0         UDPv4    0.0.0.0:4500                   *:*                                   824      svchost.exe    2024-05-31 20:35:53 UTC+0000
0x7e8038d0         UDPv6    :::4500                        *:*                                   824      svchost.exe    2024-05-31 20:35:53 UTC+0000
0x7e8466d0         UDPv4    0.0.0.0:0                      *:*                                   1732     svchost.exe    2024-05-31 20:35:56 UTC+0000
0x7e8466d0         UDPv6    :::0                           *:*                                   1732     svchost.exe    2024-05-31 20:35:56 UTC+0000
0x7eb666d0         UDPv4    0.0.0.0:0                      *:*                                   1732     svchost.exe    2024-05-31 20:35:56 UTC+0000
0x7eb755b0         UDPv4    0.0.0.0:5355                   *:*                                   316      svchost.exe    2024-05-31 20:35:56 UTC+0000
0x7eb755b0         UDPv6    :::5355                        *:*                                   316      svchost.exe    2024-05-31 20:35:56 UTC+0000
0x7e447ef0         TCPv4    0.0.0.0:49155                  0.0.0.0:0            LISTENING        448      services.exe
0x7e646940         TCPv4    192.168.92.128:139             0.0.0.0:0            LISTENING        4        System
0x7e6772f0         TCPv4    0.0.0.0:49157                  0.0.0.0:0            LISTENING        464      lsass.exe
0x7e67cef0         TCPv4    0.0.0.0:49157                  0.0.0.0:0            LISTENING        464      lsass.exe
0x7e67cef0         TCPv6    :::49157                       :::0                 LISTENING        464      lsass.exe
0x7e6a3ef0         TCPv4    0.0.0.0:49154                  0.0.0.0:0            LISTENING        824      svchost.exe
0x7e6a5550         TCPv4    0.0.0.0:49154                  0.0.0.0:0            LISTENING        824      svchost.exe
0x7e6a5550         TCPv6    :::49154                       :::0                 LISTENING        824      svchost.exe
0x7e868ce0         TCPv4    0.0.0.0:135                    0.0.0.0:0            LISTENING        628      svchost.exe
0x7e87ac90         TCPv4    0.0.0.0:135                    0.0.0.0:0            LISTENING        628      svchost.exe
0x7e87ac90         TCPv6    :::135                         :::0                 LISTENING        628      svchost.exe
0x7e87f830         TCPv4    0.0.0.0:49152                  0.0.0.0:0            LISTENING        352      wininit.exe
0x7e889860         TCPv4    0.0.0.0:49152                  0.0.0.0:0            LISTENING        352      wininit.exe
0x7e889860         TCPv6    :::49152                       :::0                 LISTENING        352      wininit.exe
0x7e8fdef0         TCPv4    0.0.0.0:49153                  0.0.0.0:0            LISTENING        700      svchost.exe
0x7e902ef0         TCPv4    0.0.0.0:49153                  0.0.0.0:0            LISTENING        700      svchost.exe
0x7e902ef0         TCPv6    :::49153                       :::0                 LISTENING        700      svchost.exe
0x7eb444a0         TCPv4    0.0.0.0:445                    0.0.0.0:0            LISTENING        4        System
0x7eb444a0         TCPv6    :::445                         :::0                 LISTENING        4        System
```

# Volatility Command Summary

imageinfo → Identifies the profile (OS version and architecture) for the memory dump.

pslist → Lists running processes within the memory dump.

pstree → Shows processes in a tree structure, helping identify parent-child relationships.

Malfind → Scans for potentially malicious code, helping detect injected code.

procdump -D "D:\Malware” → Dumps a specified process's memory to the given directory.

Dlllist → Lists (DLLs) loaded by each process, useful for identifying injected libraries.

INST. : ENG.ALI BANI BAKAR & ENG.Dana Al-Mahrouk

# Volatility Command Summary

Getsids → Retrieves (SIDs) associated with processes, privileges and user associations.

Privs → Displays privileges associated with a specific process.

Hashdump → Extracts password hashes from the memory dump.

Netscan → Scans for network connections and open ports.

Cmdscan → Recovers command-line history from open console sessions.

Iehistory → Extracts Internet Explorer browsing history from the memory dump.

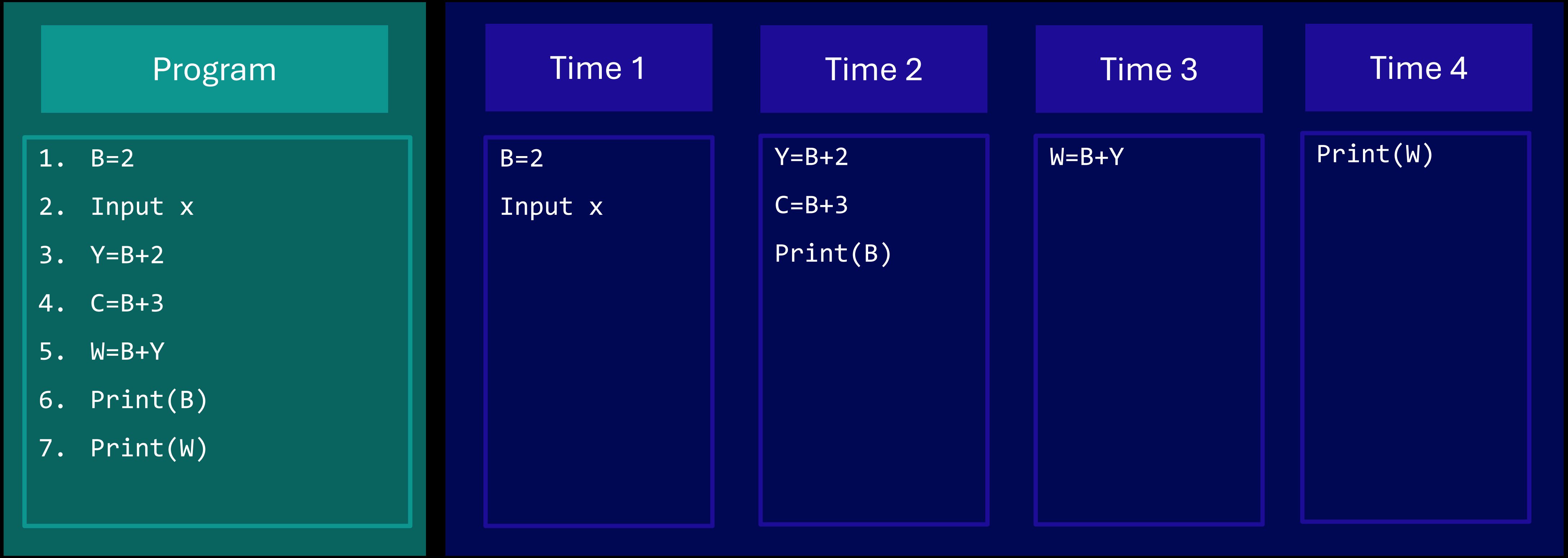
INST. : ENG.ALI BANI BAKAR & ENG.Dana Al-Mahrouk

# Volatility Command Summary

1. imageinfo → Identifies the profile (OS version and architecture) for the memory dump.
2. Pslist → Lists running processes within the memory dump.
3. Pstree → Shows processes in a tree structure, helping identify parent-child relationships.
4. Malfind → Scans for potentially malicious code within processes, helping detect injected code.
5. procdump -D "D:\Malware” → Dumps a specified process's memory to the given directory.
6. Dlllist → Lists (DLLs) loaded by each process, useful for identifying suspicious or injected libraries.
7. Getsids → Retrieves (SIDs) associated with processes, helpful for identifying privileges and user associations.
8. Privs → Displays privileges associated with a specific process, showing potential elevated permissions.
9. Hashdump → Extracts password hashes from the memory dump, useful for post-exploitation or forensic analysis.
10. Netscan → Scans for network connections and open ports, revealing network activity and potential communication with external IPs.
11. Cmdscan → Recovers command-line history from open console sessions.
12. Iehistory → Extracts Internet Explorer browsing history from the memory dump.

# Threads

- a thread is the smallest unit of a process that can be scheduled and executed independently by the operating system.
- It is importance for optimizing applications that require multitasking and responsiveness.



Program

```
1.  B=2
2.  Input x
3.  Y=B+2
4.  C=B+3
5.  W=B+Y
6.  Print(B)
7.  Print(W)
```

Time 1

```
B=2
Input x
```

Time 2

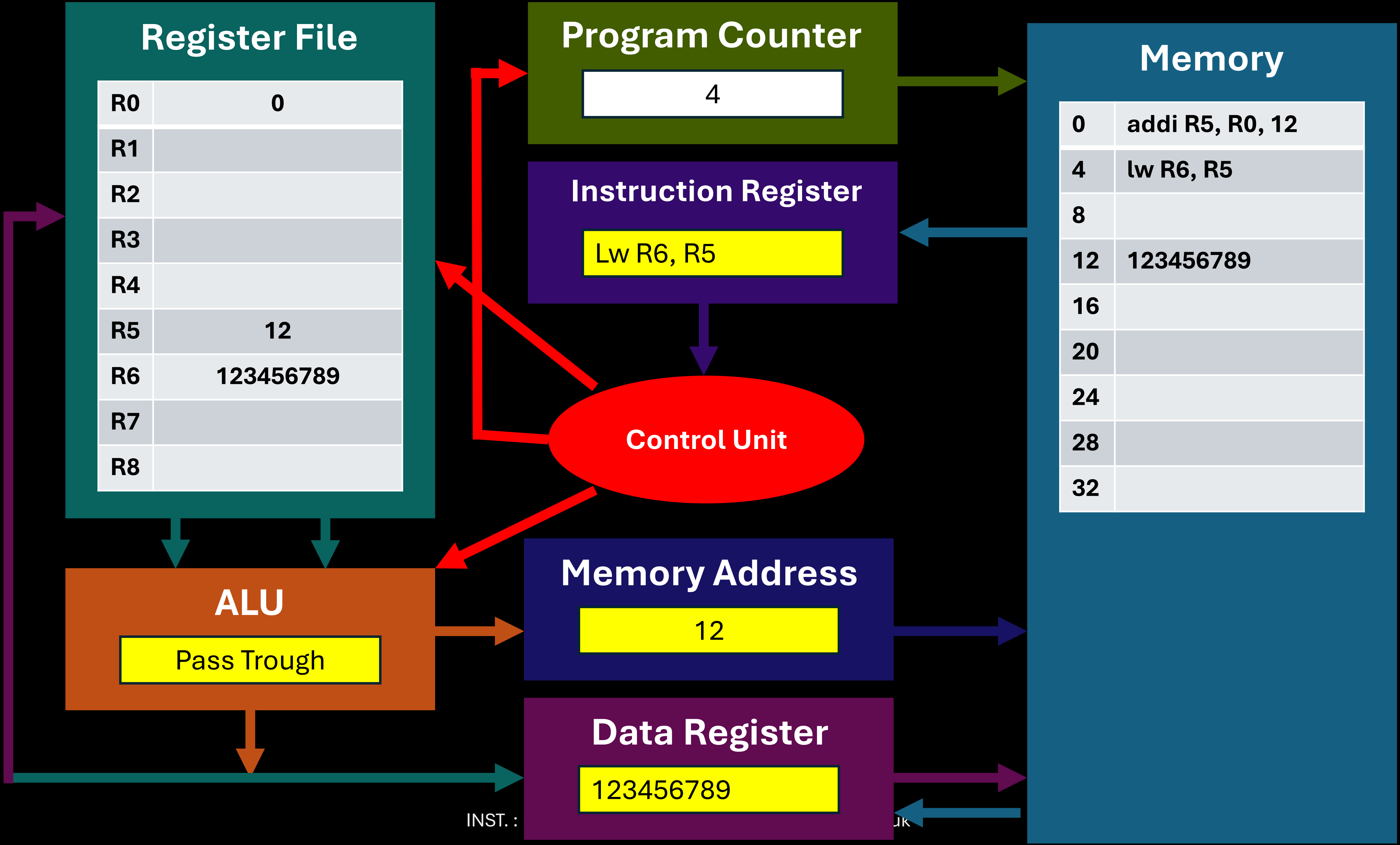
```
Y=B+2
C=B+3
Print(B)
```

Time 3

```
W=B+Y
```

Time 4

```
Print(W)
```



| | |
|---|---|
| R0 | 0 |
| R1 | |
| R2 | |
| R3 | |
| R4 | |
| R5 | 12 |
| R6 | 123456789 |
| R7 | |
| R8 | |

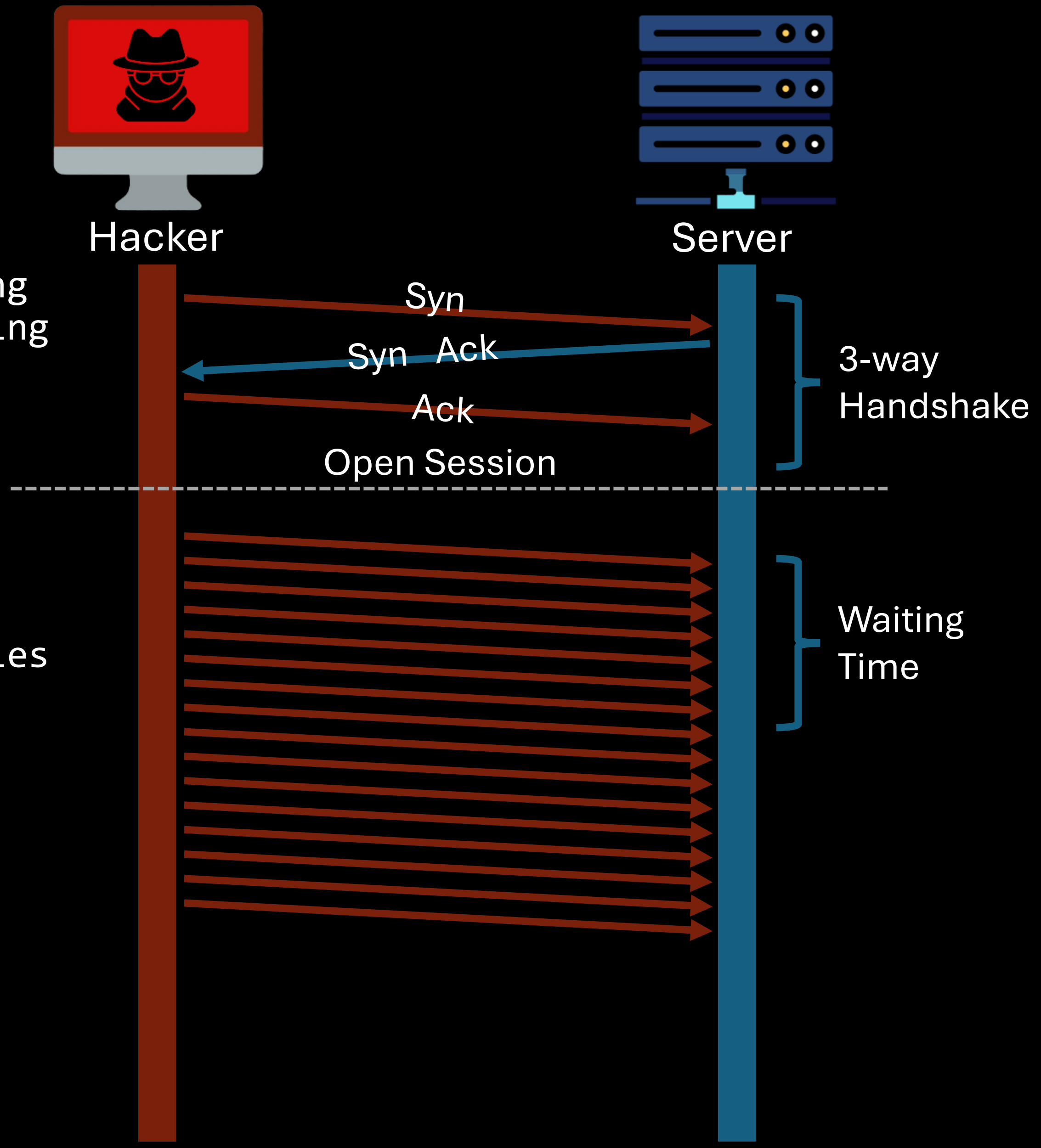
| | |
|---|---|
| 0 | addi R5, R0, 12 |
| 4 | lw R6, R5 |
| 8 | |
| 12 | 123456789 |
| 16 | |
| 20 | |
| 24 | |
| 28 | |
| 32 | |

# Day 21

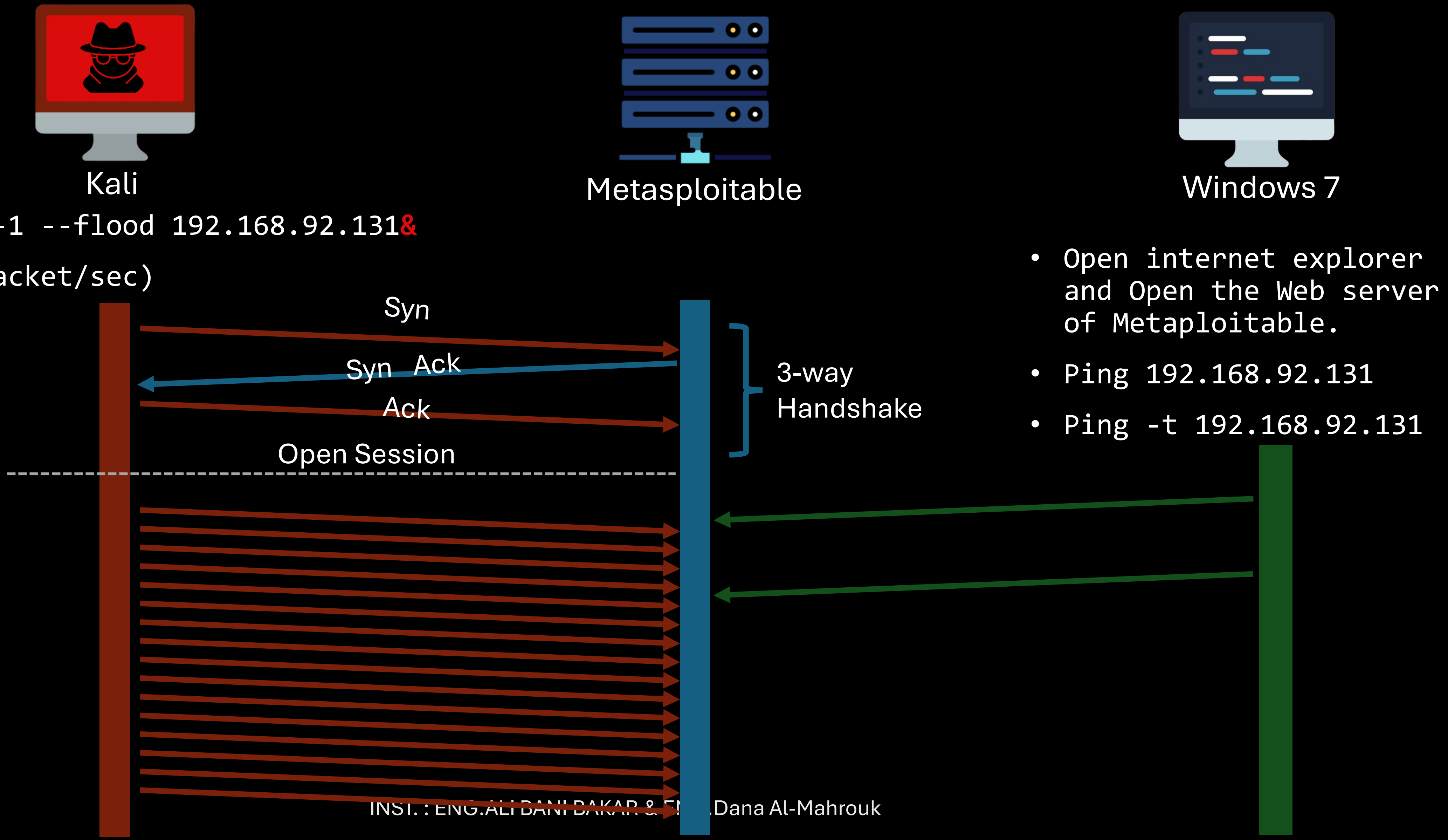
- Outline
  - DOS Attack
  - DOS Attack Lab
  - DDOS Attack
  - Image Resolution
  - RGB (Red  Green  Blue)
  - RBG Matrix Example (smiley face)

# DOS Attack

- is a malicious attempt to disrupt the normal functioning of a targeted server, service, or network by overwhelming it with a flood of unnecessary requests.
- This overloads the system, making it unresponsive to legitimate users.
- During a DoS attack, legitimate users experience increased waiting time or latency as the system struggles to respond.
- Firewall & IDS: Detect and block suspicious traffic.



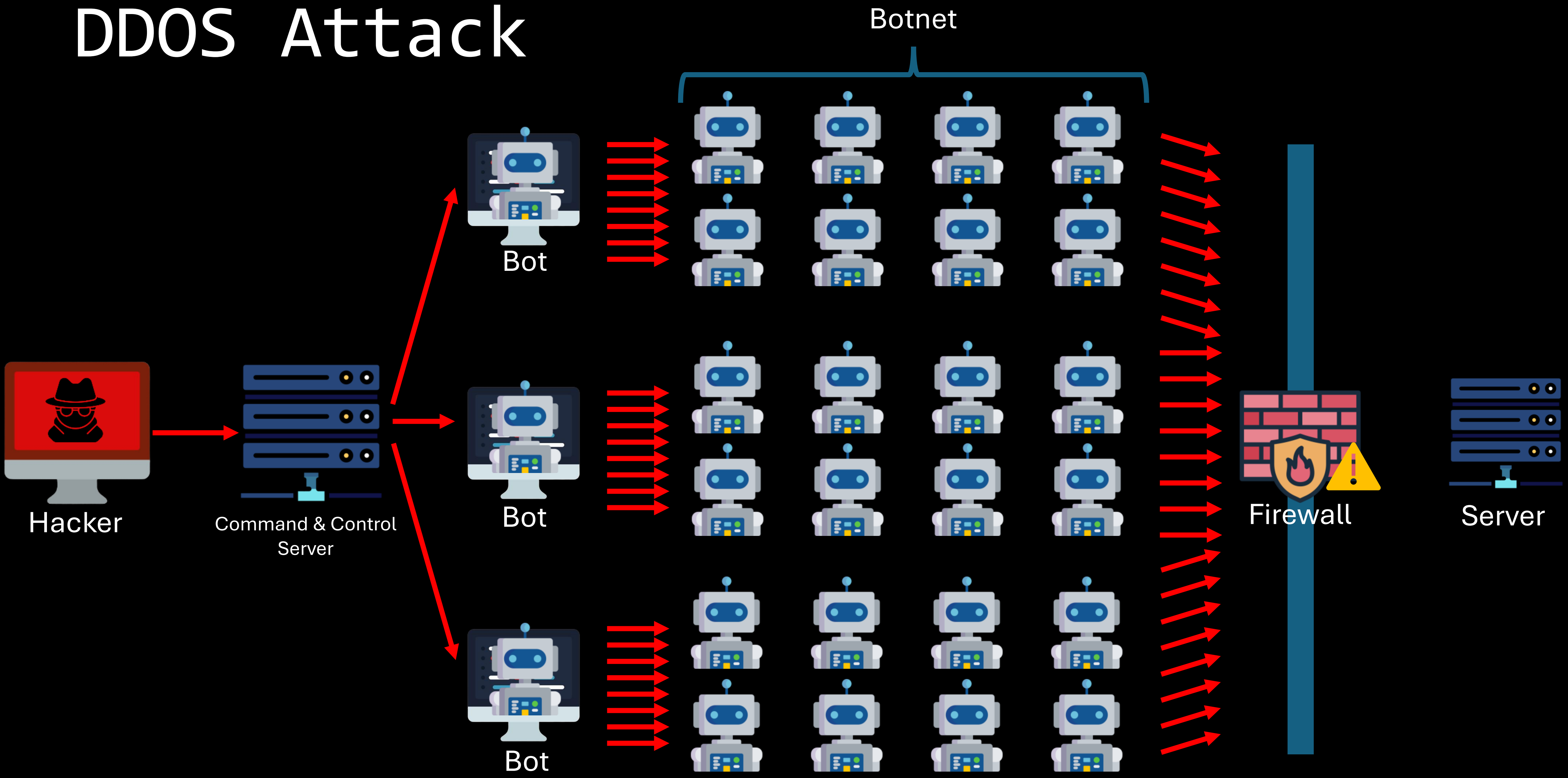
# DOS Attack Lab



- sudo hping3 -1 --flood 192.168.92.131&
- (1 Million packet/sec)

- Open internet explorer and Open the Web server of Metaploitable.
- Ping 192.168.92.131
- Ping -t 192.168.92.131

# DDOS Attack



Botnet

Bot

Bot

Bot

Hacker

Command & Control
Server

Firewall

Server

INST. : ENG.ALI BANI BAKAR & ENG.Dana Al-Mahrouk

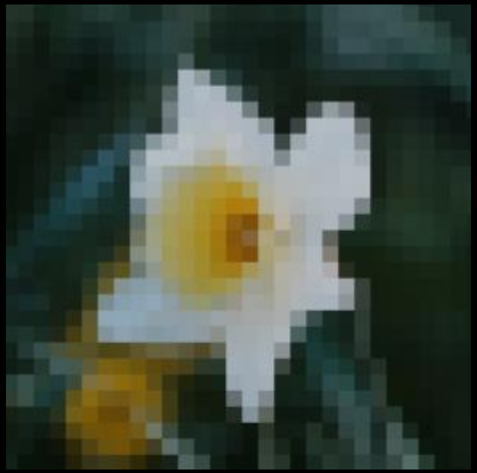
# DDOS Attack

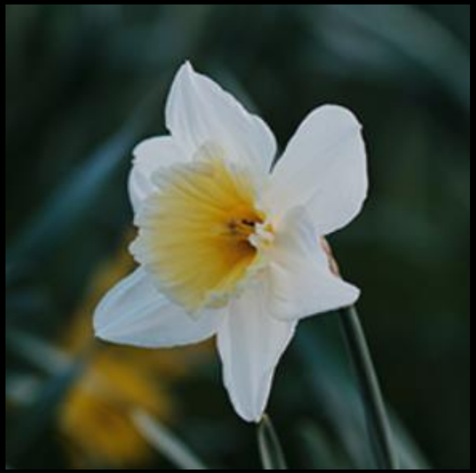
- is an advanced form of (DoS) attack where multiple compromised systems, often part of a **botnet**, are used to **flood a target with traffic**, causing disruption or complete downtime.
- The distributed nature makes it much **harder to detect** and defend against.
- traffic comes from thousands or even millions of devices spread across **different geographic locations**. This makes it difficult to distinguish between **legitimate traffic and malicious requests**.

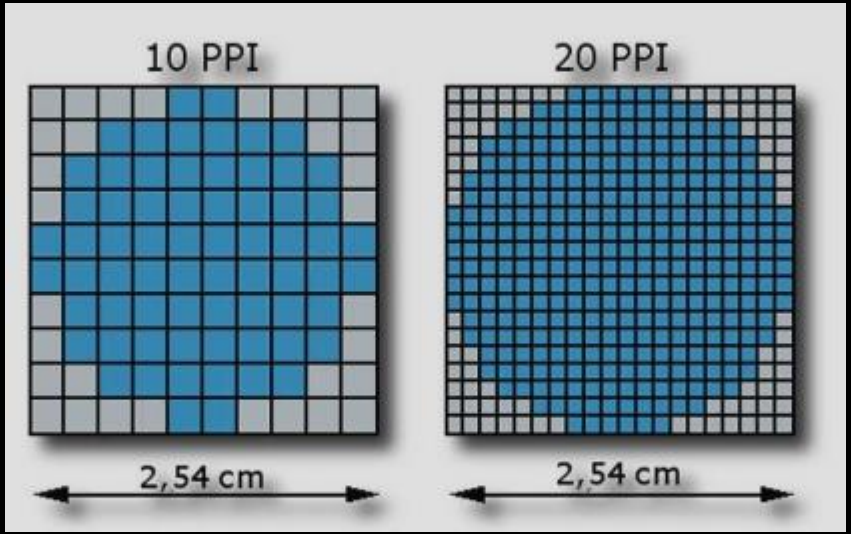
# Image Resolution

- It describes the sharpness or clarity of the image, with higher resolutions offering more detail.

| Format | Compression | Transparency | Best For | File Size |
|---|---|---|---|---|
| **JPEG (.jpg)** | Lossy | No | Photographs, web images | Small |
| **PNG (.png)** | Lossless | Yes | Logos, icons, graphics | Medium |
| **BMP (.bmp)** | Uncompressed | Limited | Image editing, archival | Large |

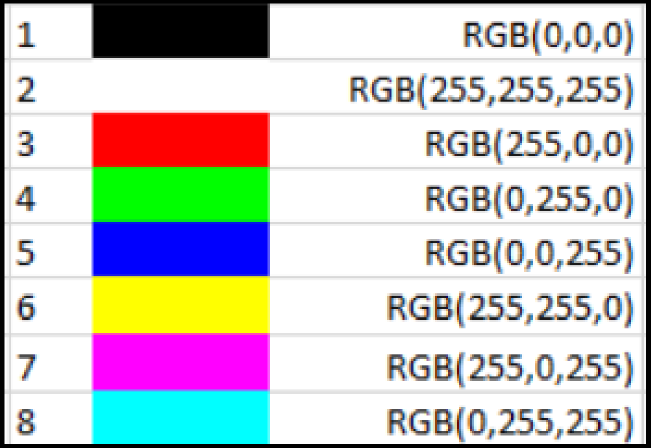




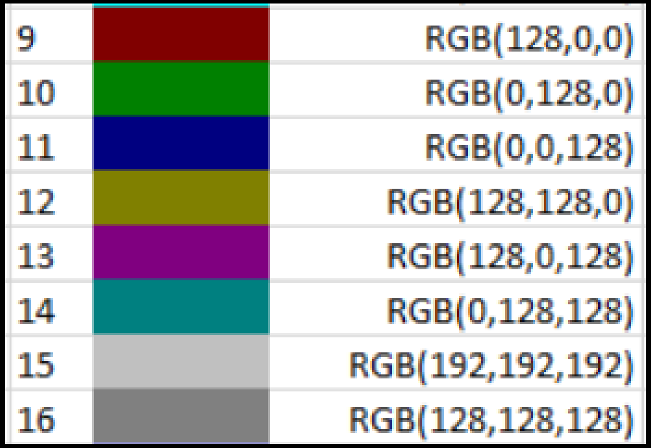


# RGB (Red Green Blue)

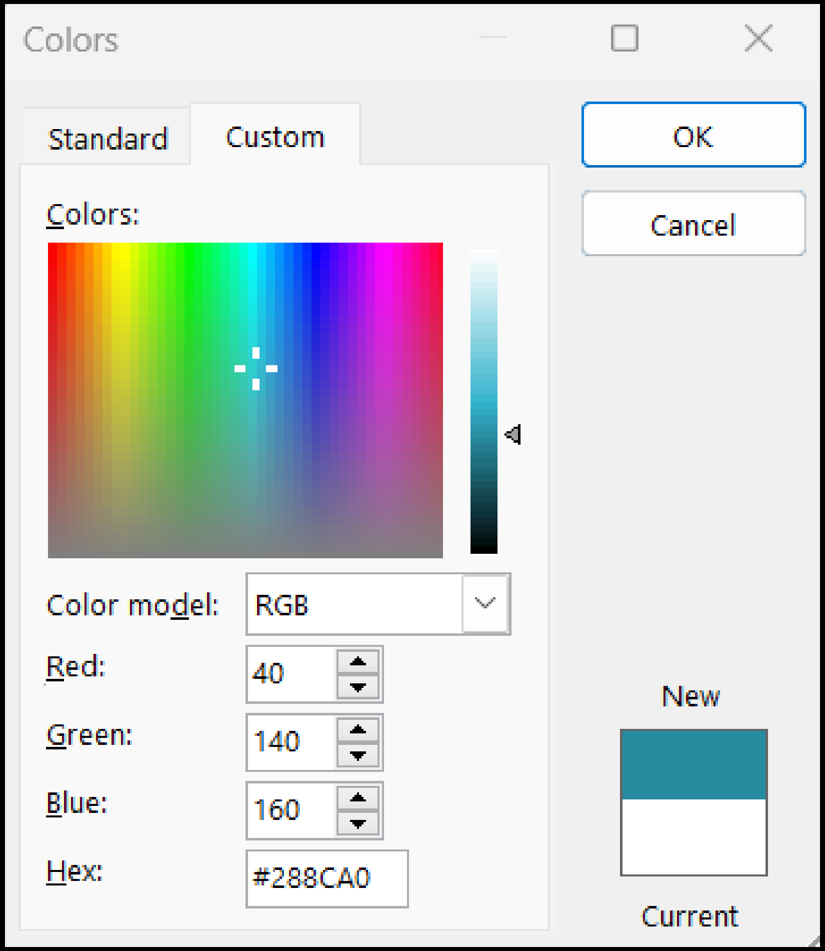
- Each color component (Red, Green, and Blue) can have a value from `0 to 255`, representing its intensity.
- `0` means no contribution of that color.
- `255` is the maximum intensity of that color.
- By varying the intensity of each of these three colors, you can create millions of different colors.



| | | |
|---|---|---|
| 1 | ⬛ | RGB(0,0,0) |
| 2 | ⬜ | RGB(255,255,255) |
| 3 | 🟥 | RGB(255,0,0) |
| 4 | 🟩 | RGB(0,255,0) |
| 5 | 🟦 | RGB(0,0,255) |
| 6 | 🟨 | RGB(255,255,0) |
| 7 | 🟪 | RGB(255,0,255) |
| 8 | 🟦 | RGB(0,255,255) |



| | | |
|---|---|---|
| 9 | 🟥 | RGB(128,0,0) |
| 10 | 🟩 | RGB(0,128,0) |
| 11 | 🟦 | RGB(0,0,128) |
| 12 | 🟨 | RGB(128,128,0) |
| 13 | 🟪 | RGB(128,0,128) |
| 14 | 🟦 | RGB(0,128,128) |
| 15 | ⬜ | RGB(192,192,192) |
| 16 | ⬛ | RGB(128,128,128) |



Color model: RGB

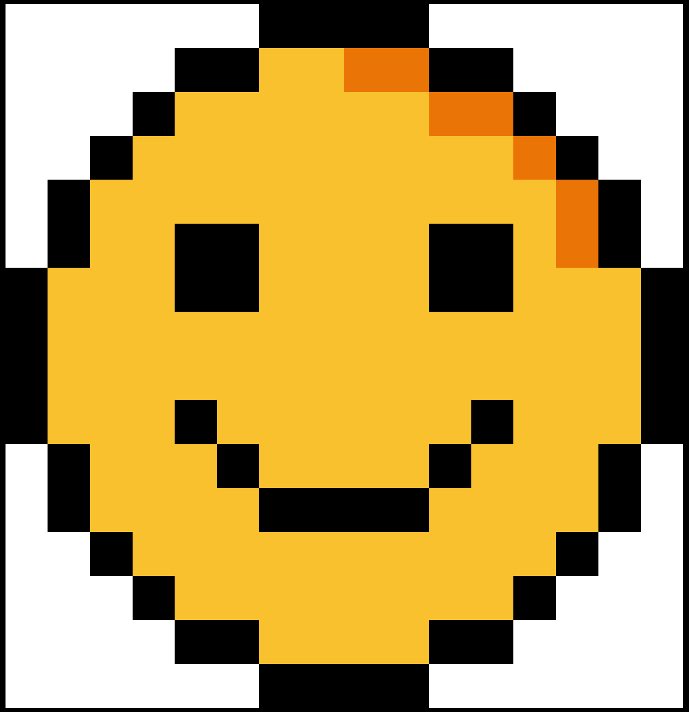
Red: 40

Green: 140

Blue: 160

Hex: #288CA0

# RBG Matrix Example



Group of Pixel

Image

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 255 | 255 | 255 | 255 | 255 | 255 | 0 | 0 | 0 | 0 | 255 | 255 | 255 | 255 | 255 | 255 |
| 255 | 255 | 255 | 255 | 0 | 0 | 255 | 255 | 255 | 255 | 0 | 0 | 255 | 255 | 255 | 255 |
| 255 | 255 | 255 | 0 | 255 | 255 | 255 | 255 | 255 | 255 | 255 | 255 | 0 | 255 | 255 | 255 |
| 255 | 255 | 0 | 255 | 255 | 255 | 255 | 255 | 255 | 255 | 255 | 255 | 255 | 0 | 255 | 255 |
| 255 | 0 | 255 | 255 | 255 | 255 | 255 | 255 | 255 | 255 | 255 | 255 | 255 | 255 | 0 | 255 |
| 255 | 0 | 255 | 255 | 0 | 0 | 255 | 255 | 255 | 255 | 0 | 0 | 255 | 255 | 0 | 255 |
| 0 | 255 | 255 | 255 | 0 | 0 | 255 | 255 | 255 | 255 | 0 | 0 | 255 | 255 | 255 | 0 |
| 0 | 255 | 255 | 255 | 255 | 255 | 255 | 255 | 255 | 255 | 255 | 255 | 255 | 255 | 255 | 0 |
| 0 | 255 | 255 | 255 | 255 | 255 | 255 | 255 | 255 | 255 | 255 | 255 | 255 | 255 | 255 | 0 |
| 0 | 255 | 255 | 255 | 0 | 255 | 255 | 255 | 255 | 255 | 255 | 0 | 255 | 255 | 255 | 0 |
| 255 | 0 | 255 | 255 | 255 | 0 | 255 | 255 | 255 | 255 | 0 | 255 | 255 | 255 | 0 | 255 |
| 255 | 0 | 255 | 255 | 255 | 255 | 0 | 0 | 0 | 0 | 255 | 255 | 255 | 255 | 0 | 255 |
| 255 | 255 | 0 | 255 | 255 | 255 | 255 | 255 | 255 | 255 | 255 | 255 | 255 | 0 | 255 | 255 |
| 255 | 255 | 255 | 0 | 255 | 255 | 255 | 255 | 255 | 255 | 255 | 255 | 0 | 255 | 255 | 255 |
| 255 | 255 | 255 | 255 | 0 | 0 | 255 | 255 | 255 | 255 | 0 | 0 | 255 | 255 | 255 | 255 |
| 255 | 255 | 255 | 255 | 255 | 255 | 0 | 0 | 0 | 0 | 255 | 255 | 255 | 255 | 255 | 255 |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 255 | 255 | 255 | 255 | 255 | 255 | 0 | 0 | 0 | 0 | 255 | 255 | 255 | 255 | 255 | 255 |
| 255 | 255 | 255 | 255 | 0 | 0 | 255 | 255 | 120 | 120 | 0 | 0 | 255 | 255 | 255 | 255 |
| 255 | 255 | 255 | 0 | 255 | 255 | 255 | 255 | 255 | 255 | 120 | 120 | 0 | 255 | 255 | 255 |
| 255 | 255 | 0 | 255 | 255 | 255 | 255 | 255 | 255 | 255 | 255 | 255 | 120 | 0 | 255 | 255 |
| 255 | 0 | 255 | 255 | 255 | 255 | 255 | 255 | 255 | 255 | 255 | 255 | 255 | 120 | 0 | 255 |
| 255 | 0 | 255 | 255 | 0 | 0 | 255 | 255 | 255 | 255 | 0 | 0 | 255 | 120 | 0 | 255 |
| 0 | 255 | 255 | 255 | 0 | 0 | 255 | 255 | 255 | 255 | 0 | 0 | 255 | 255 | 255 | 0 |
| 0 | 255 | 255 | 255 | 255 | 255 | 255 | 255 | 255 | 255 | 255 | 255 | 255 | 255 | 255 | 0 |
| 0 | 255 | 255 | 255 | 255 | 255 | 255 | 255 | 255 | 255 | 255 | 255 | 255 | 255 | 255 | 0 |
| 0 | 255 | 255 | 255 | 0 | 255 | 255 | 255 | 255 | 255 | 255 | 0 | 255 | 255 | 255 | 0 |
| 255 | 0 | 255 | 255 | 255 | 0 | 255 | 255 | 255 | 255 | 0 | 255 | 255 | 255 | 0 | 255 |
| 255 | 0 | 255 | 255 | 255 | 255 | 0 | 0 | 0 | 0 | 255 | 255 | 255 | 255 | 0 | 255 |
| 255 | 255 | 0 | 255 | 255 | 255 | 255 | 255 | 255 | 255 | 255 | 255 | 255 | 0 | 255 | 255 |
| 255 | 255 | 255 | 0 | 255 | 255 | 255 | 255 | 255 | 255 | 255 | 255 | 0 | 255 | 255 | 255 |
| 255 | 255 | 255 | 255 | 0 | 0 | 255 | 255 | 255 | 255 | 0 | 0 | 255 | 255 | 255 | 255 |
| 255 | 255 | 255 | 255 | 255 | 255 | 0 | 0 | 0 | 0 | 255 | 255 | 255 | 255 | 255 | 255 |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 255 | 255 | 255 | 255 | 255 | 255 | 0 | 0 | 0 | 0 | 255 | 255 | 255 | 255 | 255 | 255 |
| 255 | 255 | 255 | 255 | 0 | 0 | 45 | 45 | 0 | 0 | 0 | 0 | 255 | 255 | 255 | 255 |
| 255 | 255 | 255 | 0 | 45 | 45 | 45 | 45 | 45 | 45 | 0 | 0 | 0 | 255 | 255 | 255 |
| 255 | 255 | 0 | 45 | 45 | 45 | 45 | 45 | 45 | 45 | 45 | 45 | 0 | 0 | 255 | 255 |
| 255 | 0 | 45 | 45 | 45 | 45 | 45 | 45 | 45 | 45 | 45 | 45 | 45 | 0 | 0 | 255 |
| 255 | 0 | 45 | 45 | 0 | 0 | 45 | 45 | 45 | 45 | 0 | 0 | 45 | 0 | 0 | 255 |
| 0 | 45 | 45 | 45 | 0 | 0 | 45 | 45 | 45 | 45 | 0 | 0 | 45 | 45 | 45 | 0 |
| 0 | 45 | 45 | 45 | 45 | 45 | 45 | 45 | 45 | 45 | 45 | 45 | 45 | 45 | 45 | 0 |
| 0 | 45 | 45 | 45 | 45 | 45 | 45 | 45 | 45 | 45 | 45 | 45 | 45 | 45 | 45 | 0 |
| 0 | 45 | 45 | 45 | 0 | 45 | 45 | 45 | 45 | 45 | 45 | 0 | 45 | 45 | 45 | 0 |
| 255 | 0 | 45 | 45 | 45 | 0 | 45 | 45 | 45 | 45 | 0 | 45 | 45 | 45 | 0 | 255 |
| 255 | 0 | 45 | 45 | 45 | 45 | 0 | 0 | 0 | 0 | 45 | 45 | 45 | 45 | 0 | 255 |
| 255 | 255 | 0 | 45 | 45 | 45 | 45 | 45 | 45 | 45 | 45 | 45 | 45 | 0 | 255 | 255 |
| 255 | 255 | 255 | 0 | 45 | 45 | 45 | 45 | 45 | 45 | 45 | 45 | 0 | 255 | 255 | 255 |
| 255 | 255 | 255 | 255 | 0 | 0 | 45 | 45 | 45 | 45 | 0 | 0 | 255 | 255 | 255 | 255 |
| 255 | 255 | 255 | 255 | 255 | 255 | 0 | 0 | 0 | 0 | 255 | 255 | 255 | 255 | 255 | 255 |

# Day 22

- Outline
  - Autopsy
    A. Data Sources
    B. Views
       1. By Extension
       2. By MIME
    C. Deleted Files
    D. File System
    E. Extracted Content
       1. EXIF Metadata
       2. Encryption Suspected
       3. Extension Mismatch Detected
       4. Recent Documents
       5. Web Bookmarks
       6. Web Cookies
       7. Web Downloads
       8. Web History
       9. Web Search

# Day 22

- Outline
  - Autopsy
    - Keyword Hits
      - Single Literal Keyword Search
      - Single Regular Expression Search
      - Email Addresses
    - Hashset Hits
    - Email Messages
    - Interesting Items
    - Accounts
  - Create Case in Autopsy
  - SCO
    - S (Hash set)
    - C (Comment)
    - O (Occurrences)
  - Repository

AUTOPSY
DIGITAL FORENSICS

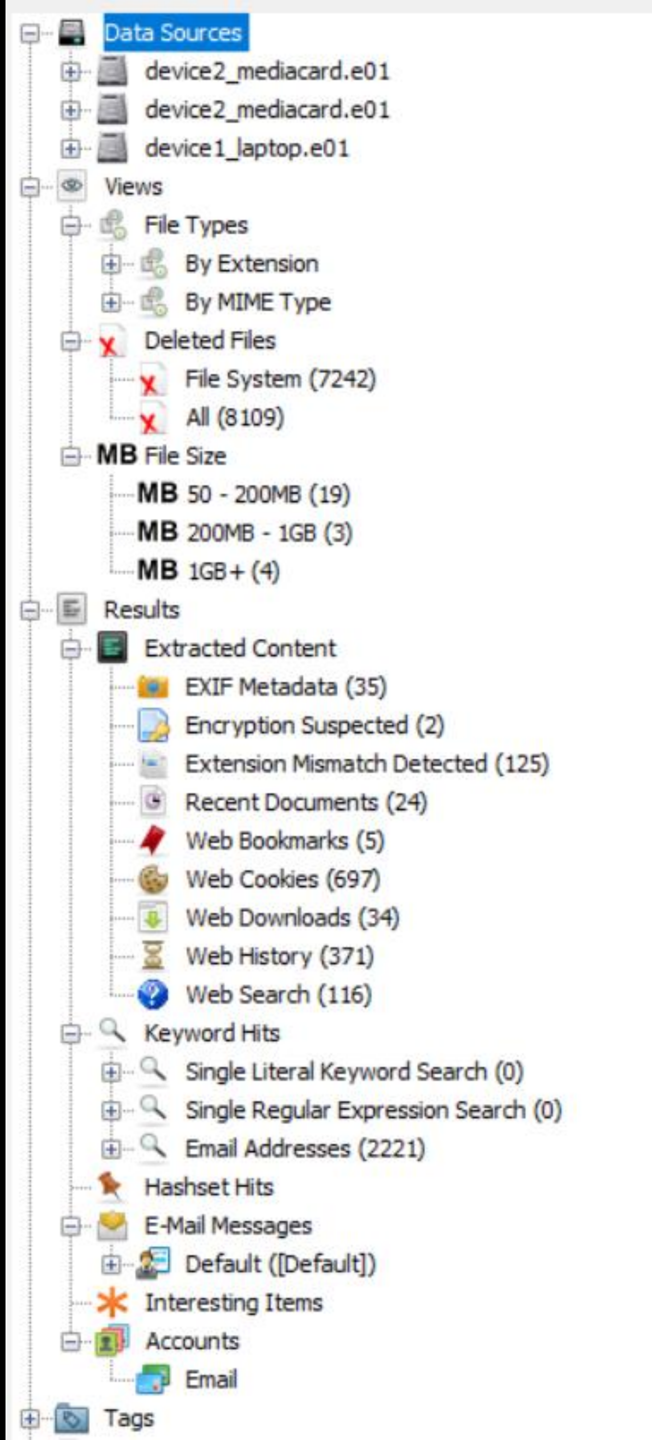
- Autopsy is a powerful digital forensics tool used to **analyze** hard drives, memory dumps, and other forms of **digital evidence**.
- It’s an open-source, graphical interface for The Sleuth Kit (TSK), a collection of command-line tools for forensic analysis.

## 1. Data Sources

`device2_mediacard.e01` and `device1_laptop.e01`:

These are **disk images** from different devices

Each `.e01` file represents an **EnCase forensic image**, a common format in digital forensics. By analyzing these images, investigators can access a **snapshot** of the device's data at the time it was captured.



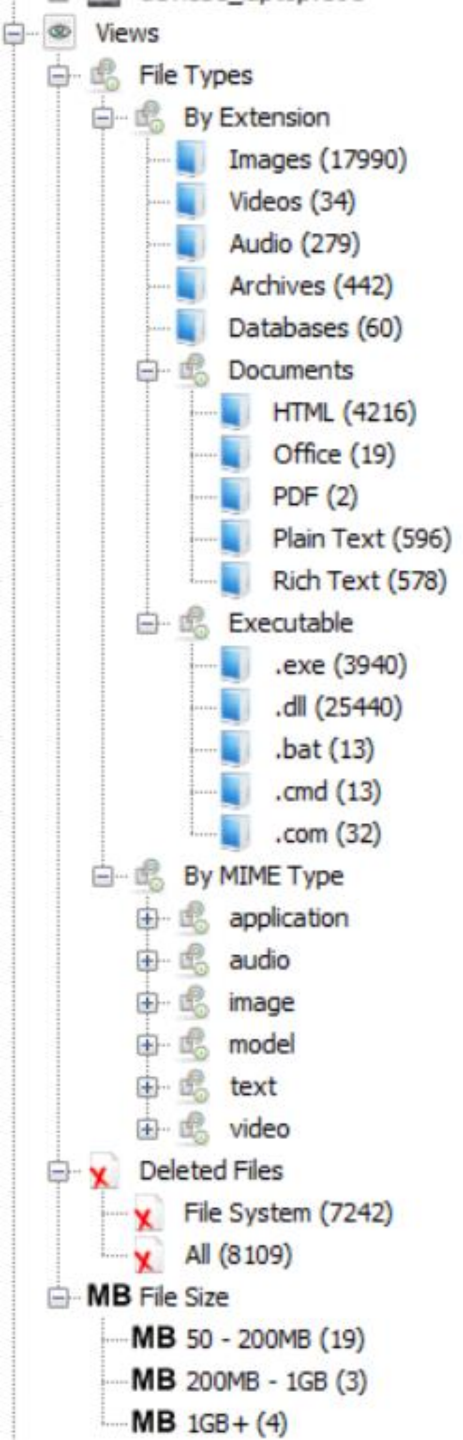
- Data Sources
  - device2_mediacard.e01
  - device2_mediacard.e01
  - device1_laptop.e01
- Views
  - File Types
    - By Extension
    - By MIME Type
  - Deleted Files
    - File System (7242)
    - All (8109)
  - MB File Size
    - MB 50 - 200MB (19)
    - MB 200MB - 1GB (3)
    - MB 1GB+ (4)
- Results
  - Extracted Content
    - EXIF Metadata (35)
    - Encryption Suspected (2)
    - Extension Mismatch Detected (125)
    - Recent Documents (24)
    - Web Bookmarks (5)
    - Web Cookies (697)
    - Web Downloads (34)
    - Web History (371)
    - Web Search (116)
  - Keyword Hits
    - Single Literal Keyword Search (0)
    - Single Regular Expression Search (0)
    - Email Addresses (2221)
  - Hashset Hits
  - E-Mail Messages
    - Default ([Default])
  - Interesting Items
  - Accounts
    - Email
- Tags

# Views

- **File Types**: Categorizes files by their types, this helps quickly identify specific file formats, and find if there are any miss match.

1. **By Extension**: Organizes files based on their **file extensions**, like (.jpg .pdf .docx, …) as users might see them in a file explorer..
2. **By MIME (Multipurpose Internet Mail Extensions) type**: a standard way to specify the nature of a file based on its **contents**.

- **Deleted Files**: Lists files that have been deleted, which may still be recoverable.
- **File System**: Shows a full view of all files, even system and hidden files. This is essential for understanding the underlying structure of the data and identifying any suspicious files that may not be easily visible.

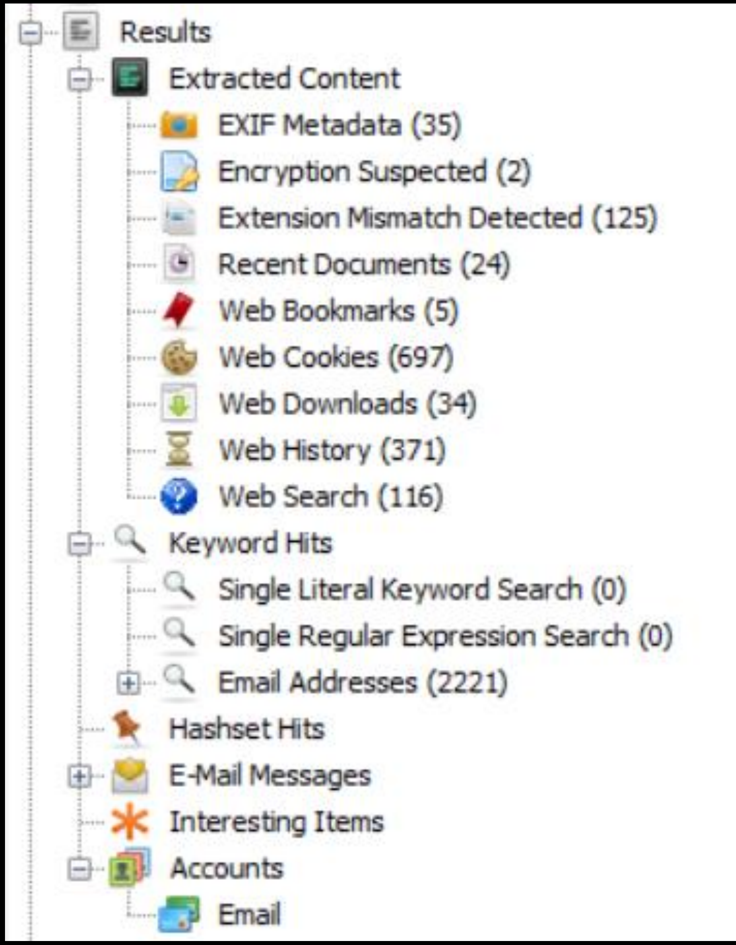


- Views
  - File Types
    - By Extension
      - Images (17990)
      - Videos (34)
      - Audio (279)
      - Archives (442)
      - Databases (60)
      - Documents
        - HTML (4216)
        - Office (19)
        - PDF (2)
        - Plain Text (596)
        - Rich Text (578)
      - Executable
        - .exe (3940)
        - .dll (25440)
        - .bat (13)
        - .cmd (13)
        - .com (32)
    - By MIME Type
      - application
      - audio
      - image
      - model
      - text
      - video
  - Deleted Files
    - File System (7242)
    - All (8109)
  - MB File Size
    - MB 50 - 200MB (19)
    - MB 200MB - 1GB (3)
    - MB 1GB+ (4)

# Results

A] Extracted Content:

1. **EXIF Metadata**: EXIF data, found in images, can reveal details like the camera model, date/time taken, and sometimes GPS location.
2. **Encryption Suspected**: Flags files that may be encrypted.
3. **Extension Mismatch Detected**: Identifies files whose extension doesn’t match its actual type.
4. **Recent Documents**: Lists files recently opened or edited. Useful for understanding which documents were actively used by the user.
5. **Web Bookmarks**: Displays saved web bookmarks.
6. **Web Cookies**: Lists web cookies, which track user sessions and preferences on websites.
7. **Web Downloads**: Tracks downloaded files, helping identify content that the user intentionally saved to the device.
8. **Web History**: Shows the browsing history, which provides insights into the websites the user visited.
9. **Web Search**: Lists search queries, indicating topics the user was interested in.



- Results
  - Extracted Content
    - EXIF Metadata (35)
    - Encryption Suspected (2)
    - Extension Mismatch Detected (125)
    - Recent Documents (24)
    - Web Bookmarks (5)
    - Web Cookies (697)
    - Web Downloads (34)
    - Web History (371)
    - Web Search (116)
  - Keyword Hits
    - Single Literal Keyword Search (0)
    - Single Regular Expression Search (0)
    - Email Addresses (2221)
  - Hashset Hits
  - E-Mail Messages
  - Interesting Items
  - Accounts
    - Email

# Results

B] **Keyword Hits**:

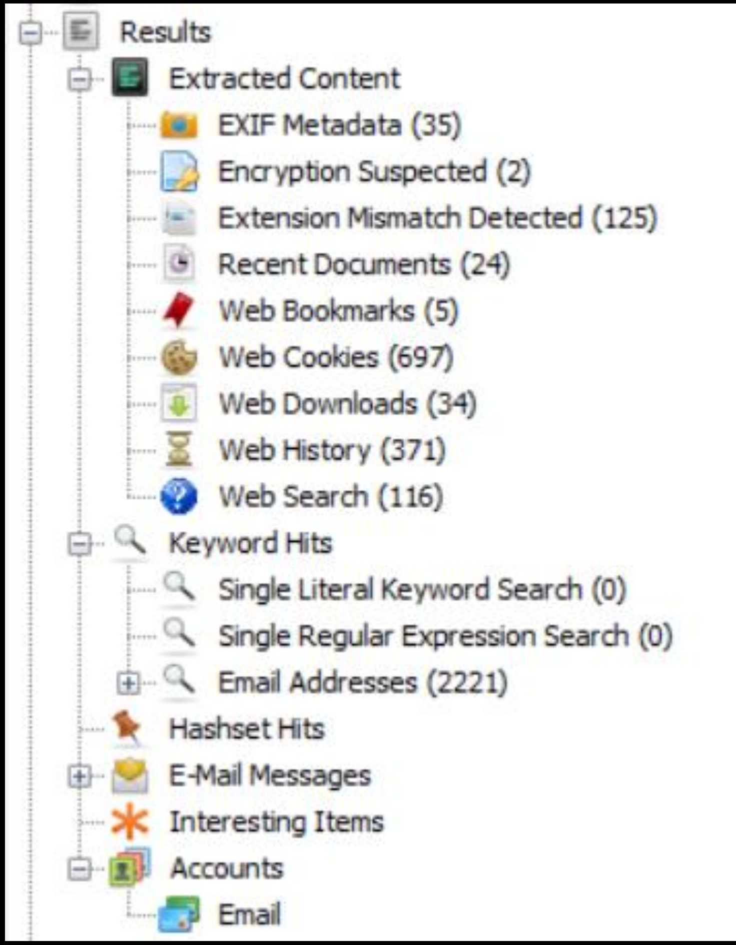
- **`Single Literal Keyword Search` and `Single Regular Expression Search`**: Searches for specific keywords or patterns (like email addresses, credit card numbers, or flagged terms) across the data.
- **Email Addresses**: Detects email addresses across files. This could be useful for identifying user accounts, contacts, or communication recipients.

C] **Hashset Hits**: Uses a hash database to compare file hashes, identifying known files, either trusted or malicious, depending on the database.

D] **Email Messages**: Lists and organizes email data, showing sender, recipient, subject, and content.

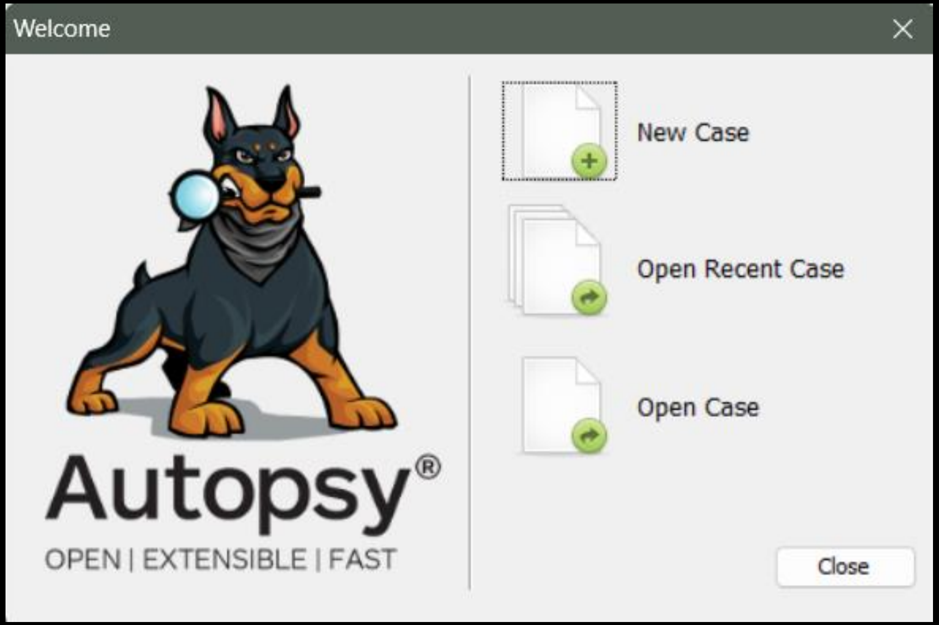
E] **Interesting Items**: Automatically flagged files based on criteria like unusual activity, high frequency of modification, or potential relevance to the investigation. Examples might include financial records or communication logs.

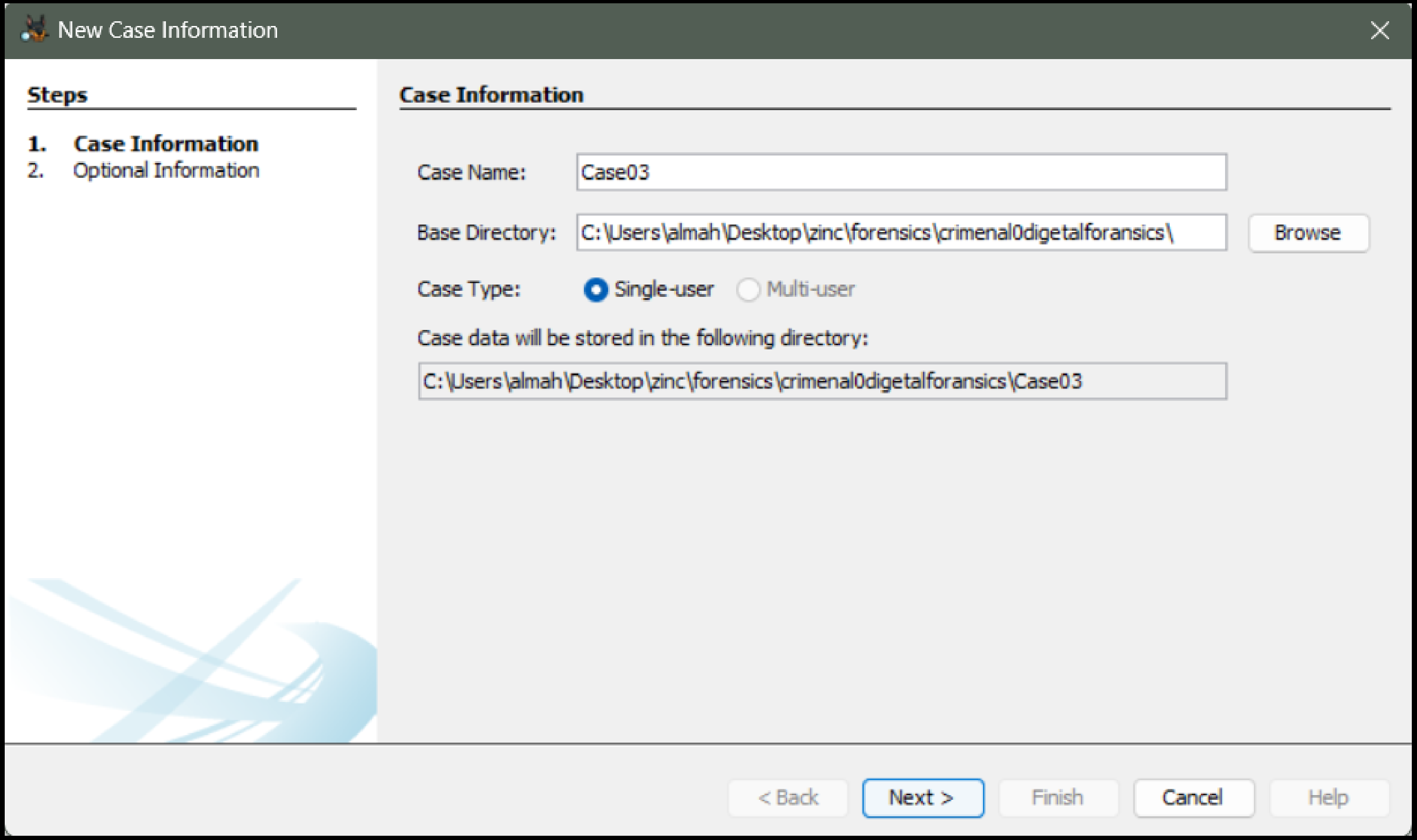
F] **Accounts**: Shows user accounts associated with the device, helping identify who accessed or controlled the device.



- Results
  - Extracted Content
    - EXIF Metadata (35)
    - Encryption Suspected (2)
    - Extension Mismatch Detected (125)
    - Recent Documents (24)
    - Web Bookmarks (5)
    - Web Cookies (697)
    - Web Downloads (34)
    - Web History (371)
    - Web Search (116)
  - Keyword Hits
    - Single Literal Keyword Search (0)
    - Single Regular Expression Search (0)
    - Email Addresses (2221)
  - Hashset Hits
  - E-Mail Messages
  - Interesting Items
  - Accounts
    - Email

# Create Case





**Steps**

1. **Case Information**
2. Optional Information

**Case Information**

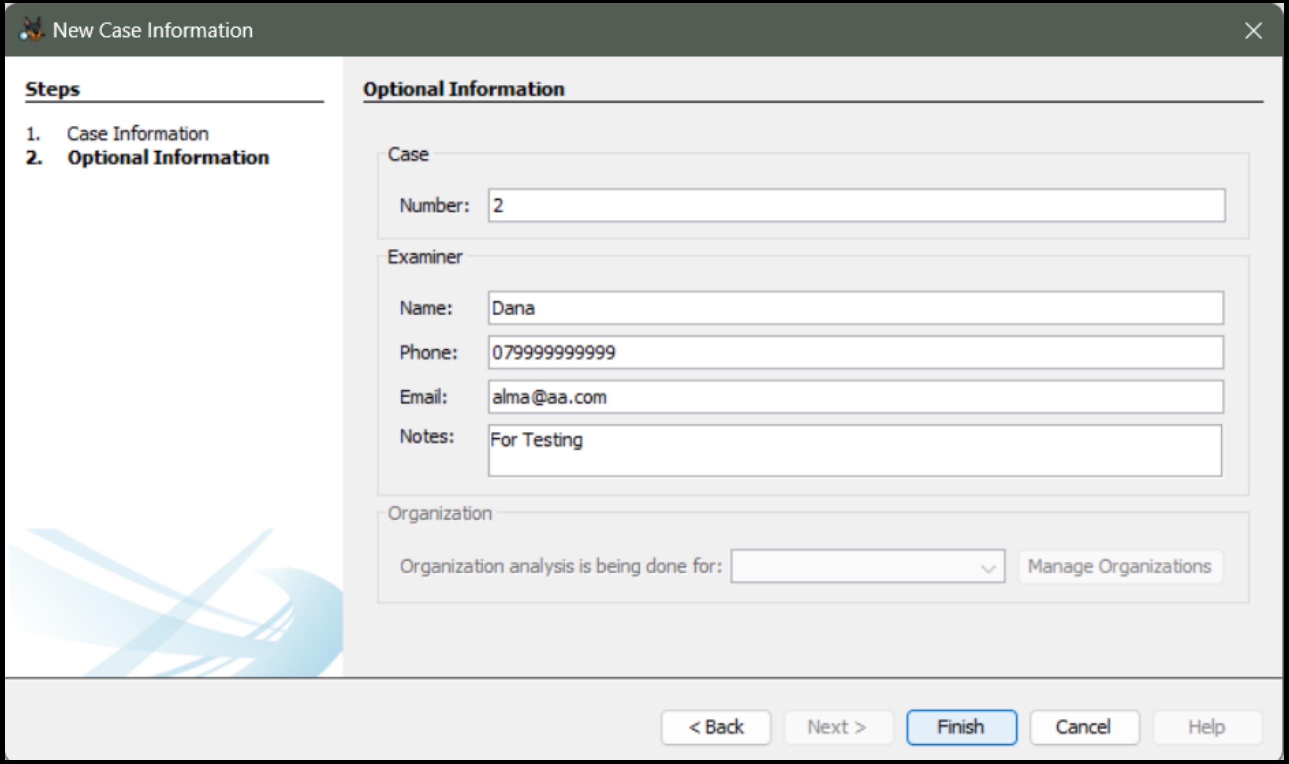
Case Name: Case03

Base Directory: C:\Users\almah\Desktop\zinc\forensics\crimenal0digetalforansics\

Case Type: ● Single-user ○ Multi-user

Case data will be stored in the following directory:

C:\Users\almah\Desktop\zinc\forensics\crimenal0digetalforansics\Case03



New Case Information

Steps

1. Case Information
2. **Optional Information**

**Optional Information**

Case

Number: 2

Examiner

Name: Dana

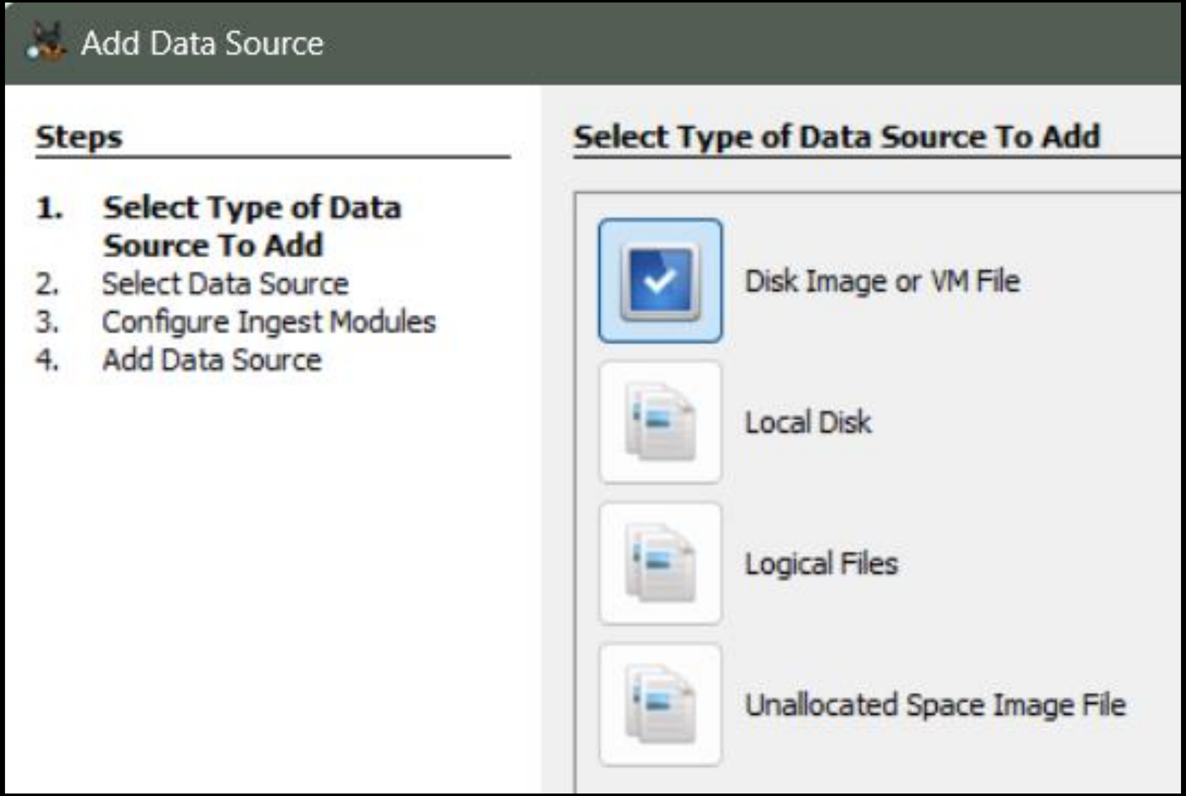
Phone: 079999999999

Email: alma@aa.com

Notes: For Testing

Organization

Organization analysis is being done for:



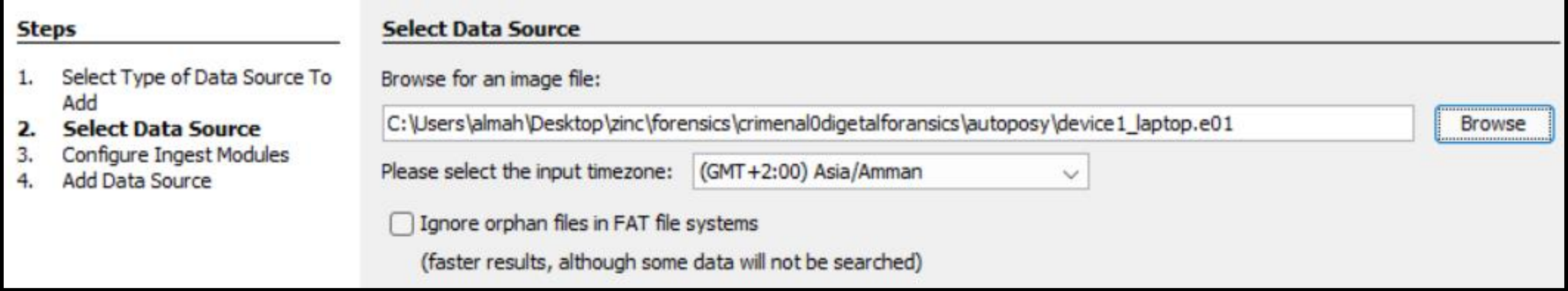
Add Data Source

Steps

1. **Select Type of Data Source To Add**
2. Select Data Source
3. Configure Ingest Modules
4. Add Data Source

**Select Type of Data Source To Add**

- ☑ Disk Image or VM File
- Local Disk
- Logical Files
- Unallocated Space Image File



Steps

1. Select Type of Data Source To Add
2. **Select Data Source**
3. Configure Ingest Modules
4. Add Data Source

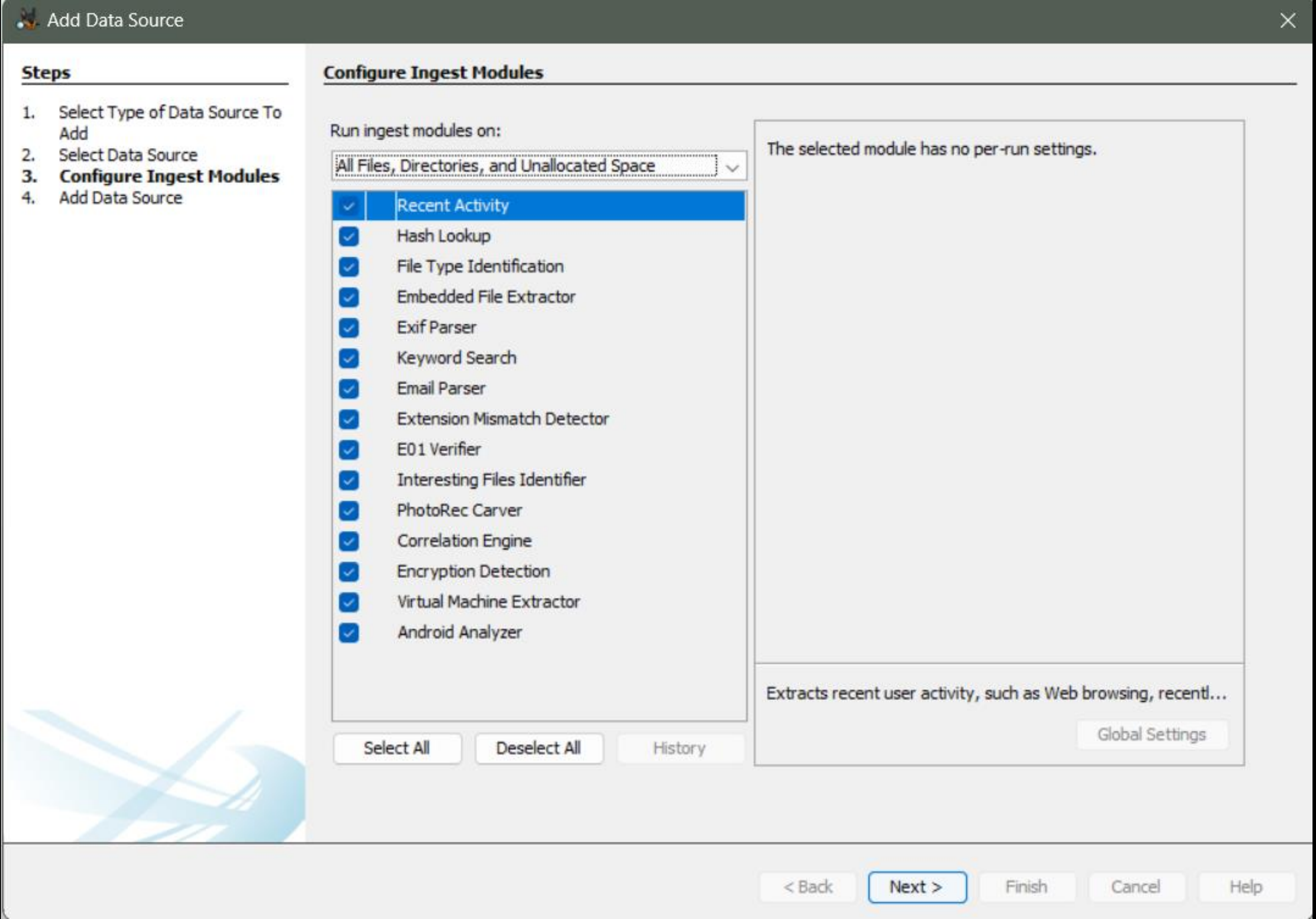
**Select Data Source**

Browse for an image file:

C:\Users\almah\Desktop\zinc\forensics\crimenal0digetalforansics\autoposy\device1_laptop.e01

Please select the input timezone: (GMT+2:00) Asia/Amman

□ Ignore orphan files in FAT file systems
(faster results, although some data will not be searched)



**Steps**

1. Select Type of Data Source To Add
2. Select Data Source
3. **Configure Ingest Modules**
4. Add Data Source

**Configure Ingest Modules**

Run ingest modules on:

All Files, Directories, and Unallocated Space

- ☑ Recent Activity
- ☑ Hash Lookup
- ☑ File Type Identification
- ☑ Embedded File Extractor
- ☑ Exif Parser
- ☑ Keyword Search
- ☑ Email Parser
- ☑ Extension Mismatch Detector
- ☑ E01 Verifier
- ☑ Interesting Files Identifier
- ☑ PhotoRec Carver
- ☑ Correlation Engine
- ☑ Encryption Detection
- ☑ Virtual Machine Extractor
- ☑ Android Analyzer

The selected module has no per-run settings.

Extracts recent user activity, such as Web browsing, recentl...

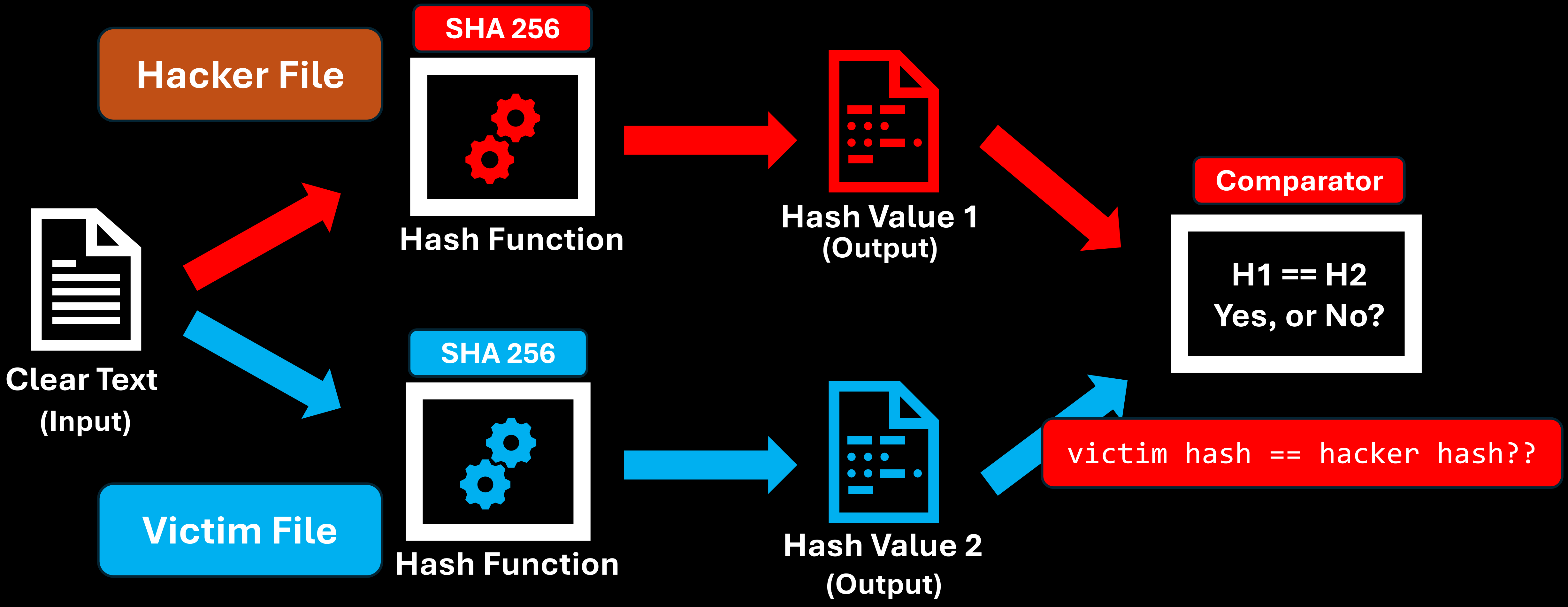
# SCO Colum

- S (Hash set) → This indicates that a file’s hash matches a known hash in a hash set. victim hash == hacker hash

- C (Comment) → A comment attached to a file by the investigator or an automated tool to add context or notes about that file.

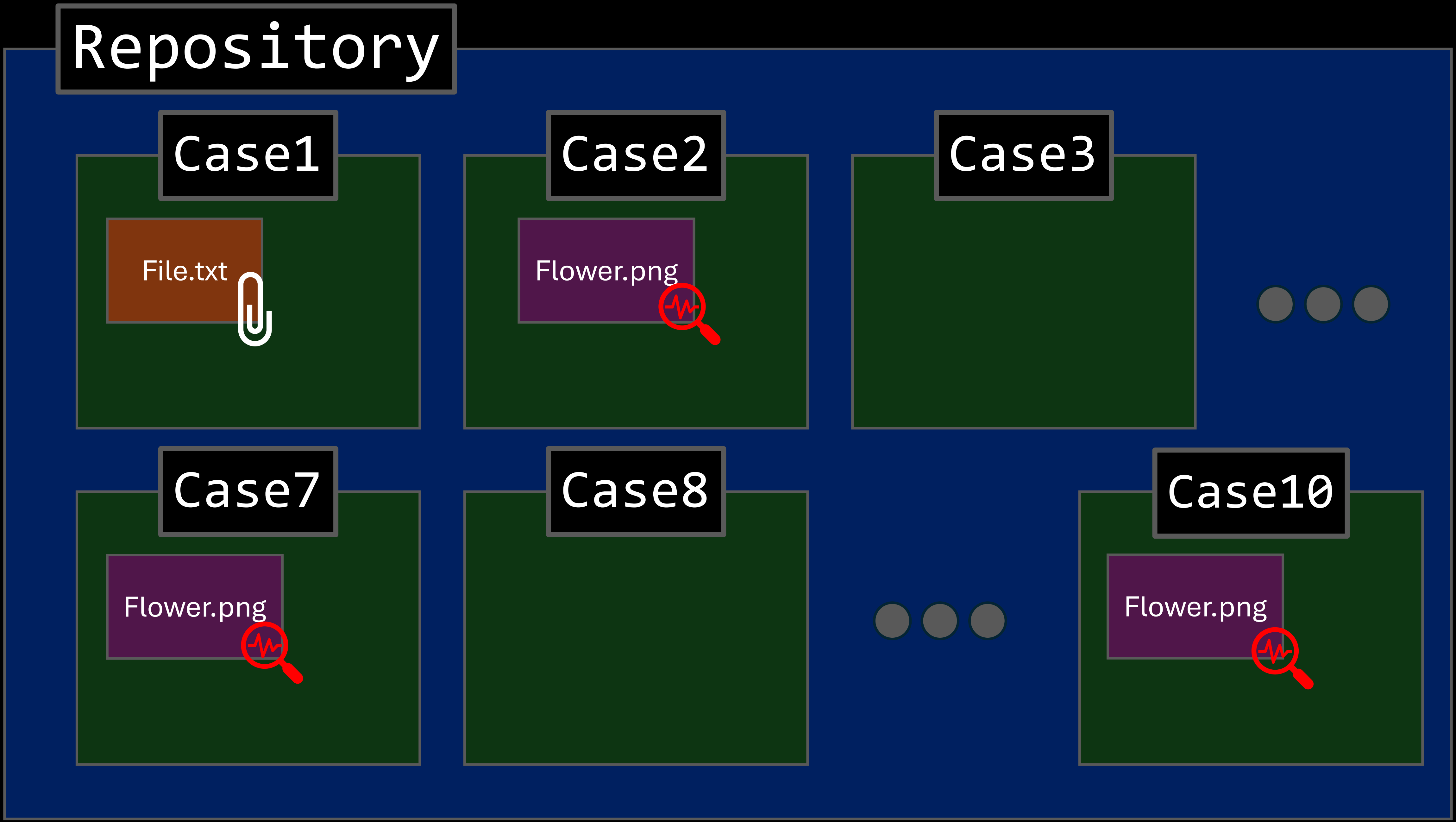
- O (Occurrences) → Indicates that the file has appeared in multiple cases, which can be crucial in identifying shared or commonly used files.

# S (Hash set)



victim hash == hacker hash??

INST. : ENG.ALI BANI BAKAR & ENG.Dana Al-Mahrouk



Repository

Case1

File.txt

Case2

Flower.png

Case3

Case7

Flower.png

Case8

Case10

Flower.png

# Day 23

- Outline
  - Data Artifacts
    - Web Artifacts
    - OS Artifacts
    - File System Artifacts
    - Application Artifacts
    - System Configuration Artifacts
    - Executable and Malware Artifacts
    - Keyword and Hash Set Matches
  - USP (Uninterruptible Power Supply)

# Data Artifacts

### Keyword and Hash Set Matches

- Keyword Hits
- Hash Set Hits

### Application Artifacts

- Email Artifacts
- Chat and Messaging Artifacts
- Application Logs

### Web Artifacts

- Web History
- Web Bookmarks
- Web Cookies
- Web Downloads

### System Configuration Artifacts

- Windows Registry
- System Logs
- Network Configuration

### OS Artifacts

- Recent Documents
- User Accounts
- Recycle Bin
- Prefetch Files (Windows)

### Executable and Malware Artifacts

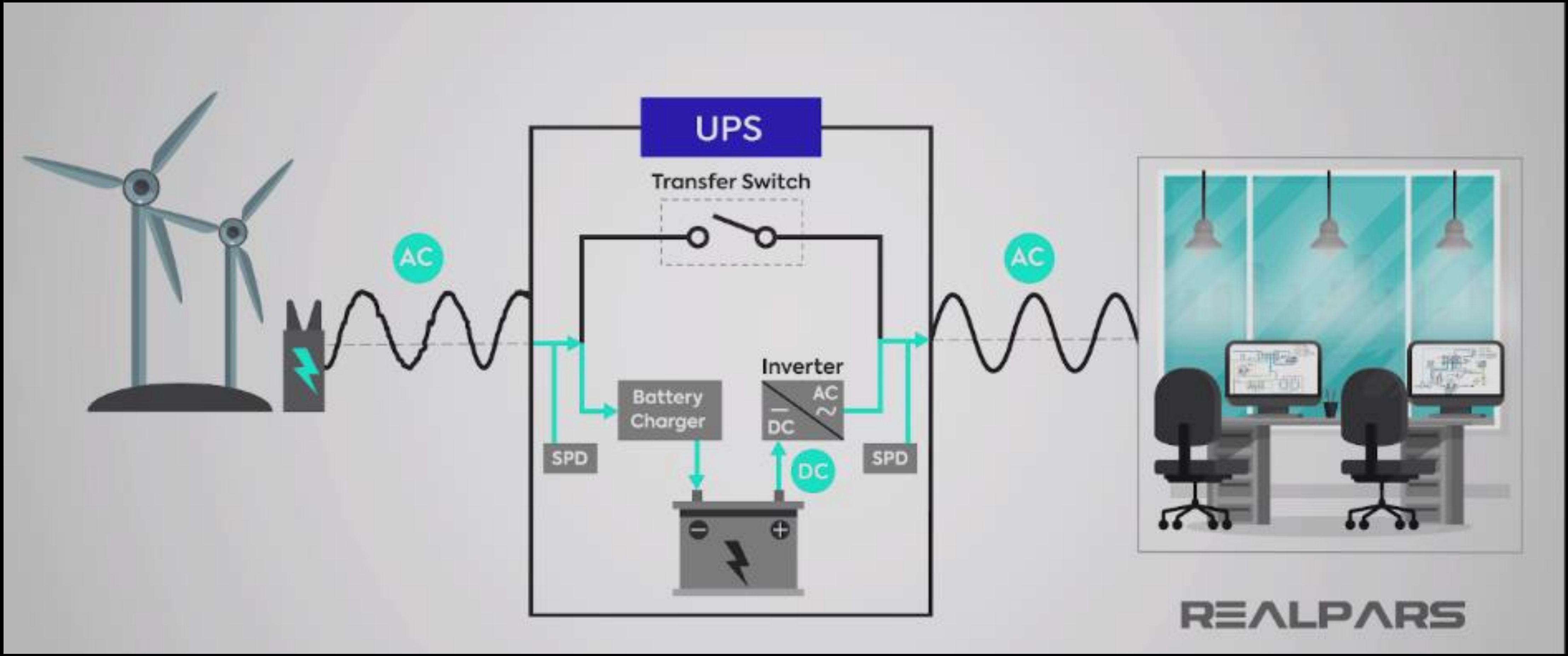
- Suspicious Executables
- Hash Matches
- Running Processes and Memory Dumps

### File System Artifacts

- File Metadata
- Deleted Files
- File Permissions

INST. : ENG.ALI BANI BAKAR & ENG.Dana Al-Mahrouk

# USP (Uninterruptible Power Supply)



## (Uninterruptible Power Supply)

is a device that provides backup power to electronic devices in case of a power failure or fluctuation. It helps protect critical equipment from unexpected shutdowns, data loss, and potential damage from power issues.