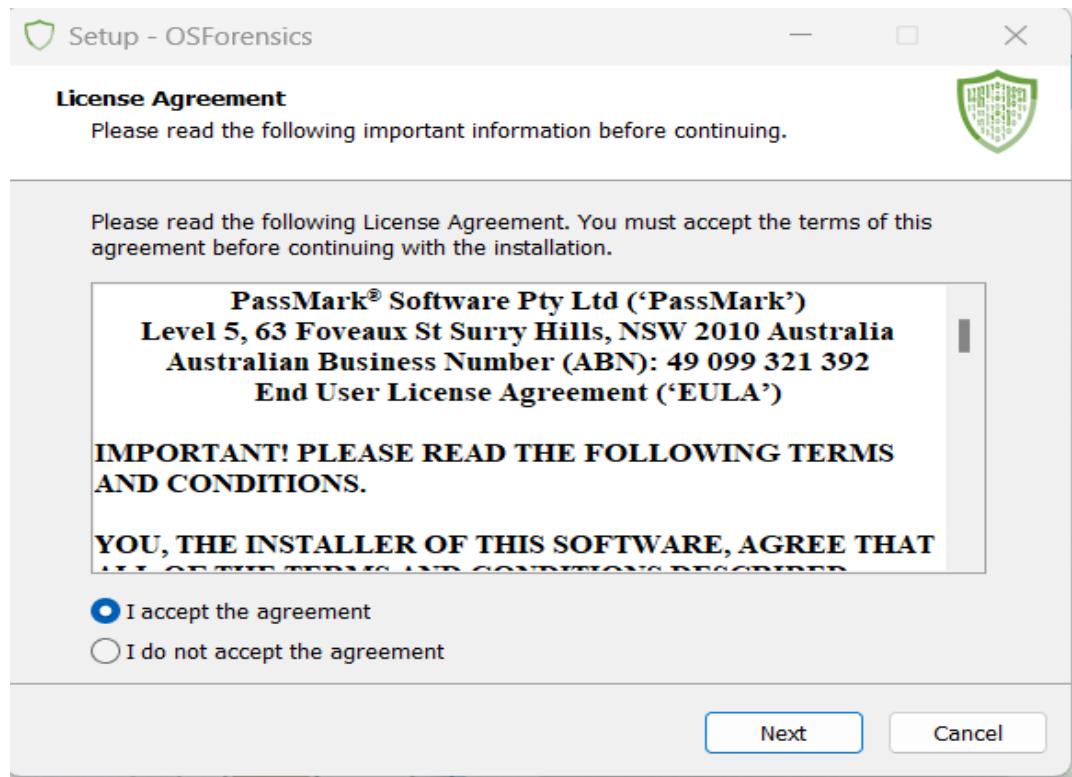


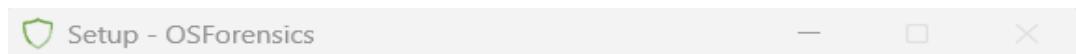
# Module-6

## Operating System Forensics

### Lab1: Discovering and Extracting Hidden Forensic Material on Computers Using OS Forensics

Lab objective: The objective of this lab is to learn how to investigate a suspect's computer to locate evidence of a crime. In this lab we will learn how to use the OSForensic tool.





## Completing the OSForensics Setup Wizard

**OSForensics**



PASSMARK  
SOFTWARE

Setup has finished installing OSForensics on your computer.  
The application may be launched by selecting the installed  
shortcuts.

Click Finish to exit Setup.

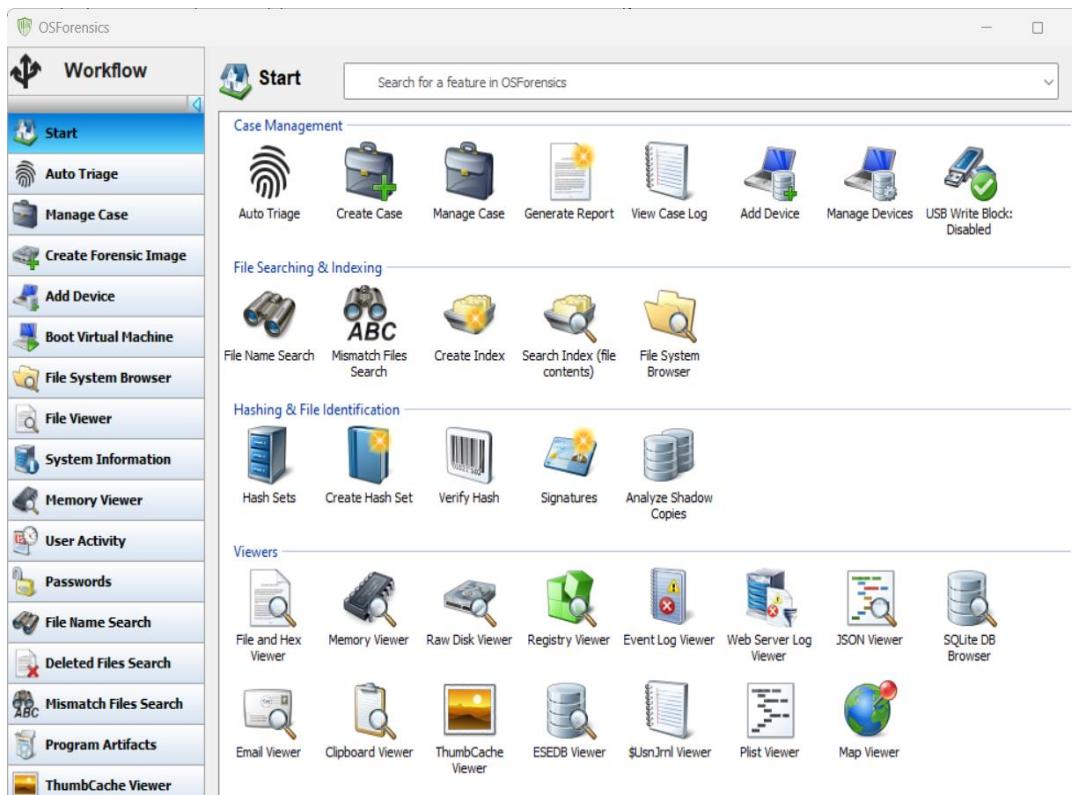
Launch OSForensics

Back

Finish



The image shows the OSForensics software interface. On the left is a vertical toolbar titled "Workflow" with icons for various forensic tasks: Start, Auto Triage, Manage Case, Create Forensic Image, Add Device, Boot Virtual Machine, File System Browser, File Viewer, System Information, Memory Viewer, User Activity, Passwords, File Name Search, Deleted Files Search, Mismatch Files Search, Program Artifacts, and ThumbCache Viewer. The main window displays the PassMark Software logo and the OSForensics shield logo. Text in the center says "PassMark Software" and "www.osforensics.com". Below that, it says "Unlicensed trial" and "Click on Continue for your 30day evaluation (30 Days left)". At the bottom are three buttons: "Continue Using Trial Version", "Upgrade to Professional Version", and "Exit".

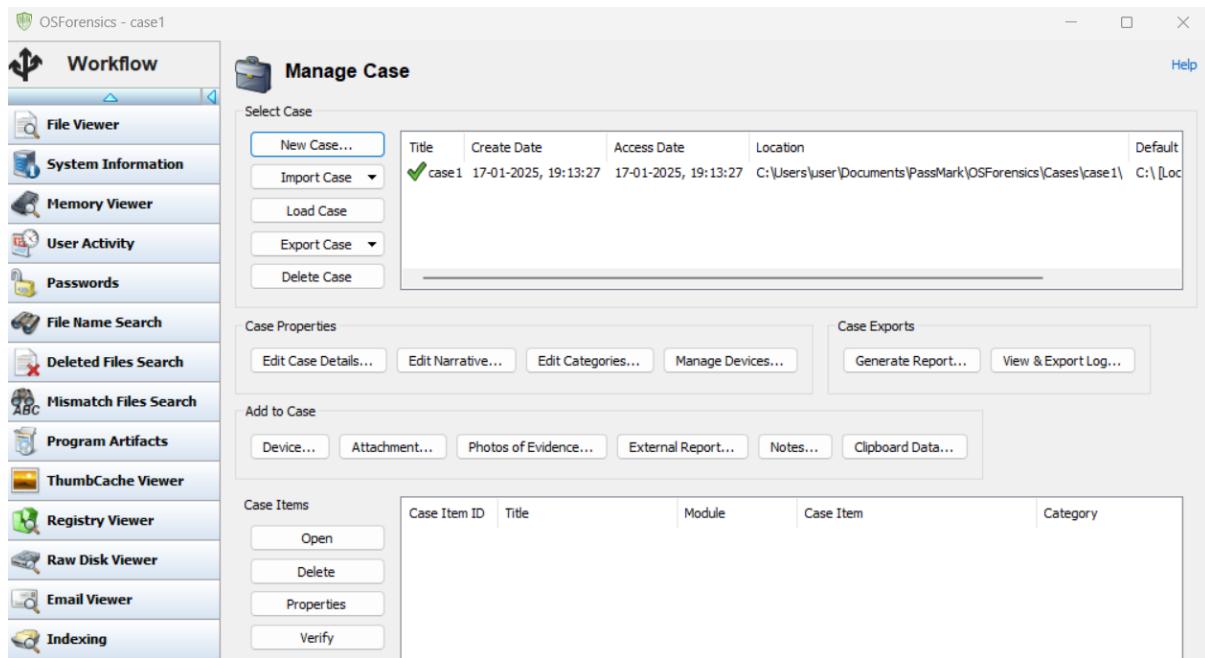


## Create a new case

New Case

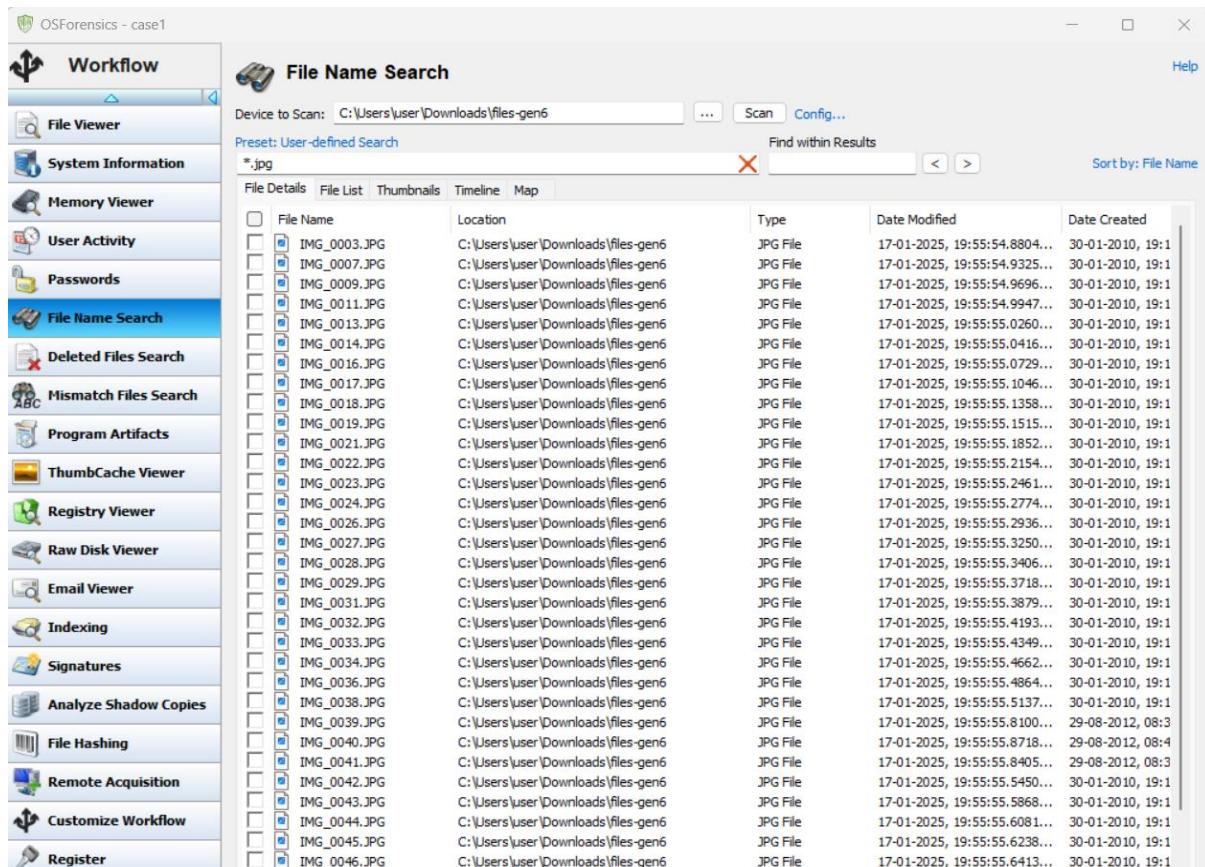
Chain of Custody		Custom Fields	Case Narrative	
Basic Case Data	Case Categories	Offense & Custody Data	Description of Evidence	
Case Name	<input type="text" value="case1"/>			
Case Type	<input type="text" value="Criminal"/>			
Investigator	<input type="text" value="Theertha"/>			
Organization	<input type="text" value="EC-council"/>			
Contact Details	<input type="text" value="www.eccouncil.org"/>			
Timezone	<input type="text" value="Local (UTC +5:30) Chennai, Kolkata, Mumbai, New"/>		<input checked="" type="checkbox"/> Account for Daylight Saving Time	
Display Date Format	<input type="text" value="17-01-2025 (Default)"/>		<input type="checkbox"/> Display timezone on dates	
Default Drive	<input type="text" value="C:\ [Local]"/>			
Acquisition Type	<input type="radio"/> Live Acquisition of Current Machine <input checked="" type="radio"/> Investigate Disk(s) from Another Machine			
Case Folder	<input checked="" type="radio"/> Default Location <input type="radio"/> Custom Location <input type="text" value="C:\Users\user\Documents\PassMark\OSForensics\Cases\case1\"/> <span style="float: right;"><input type="button" value="Browse"/></span>			
<input checked="" type="checkbox"/> Log case activity <input type="checkbox"/> Enable USB Write-block				
<input type="button" value="OK"/> <input type="button" value="Cancel"/>				

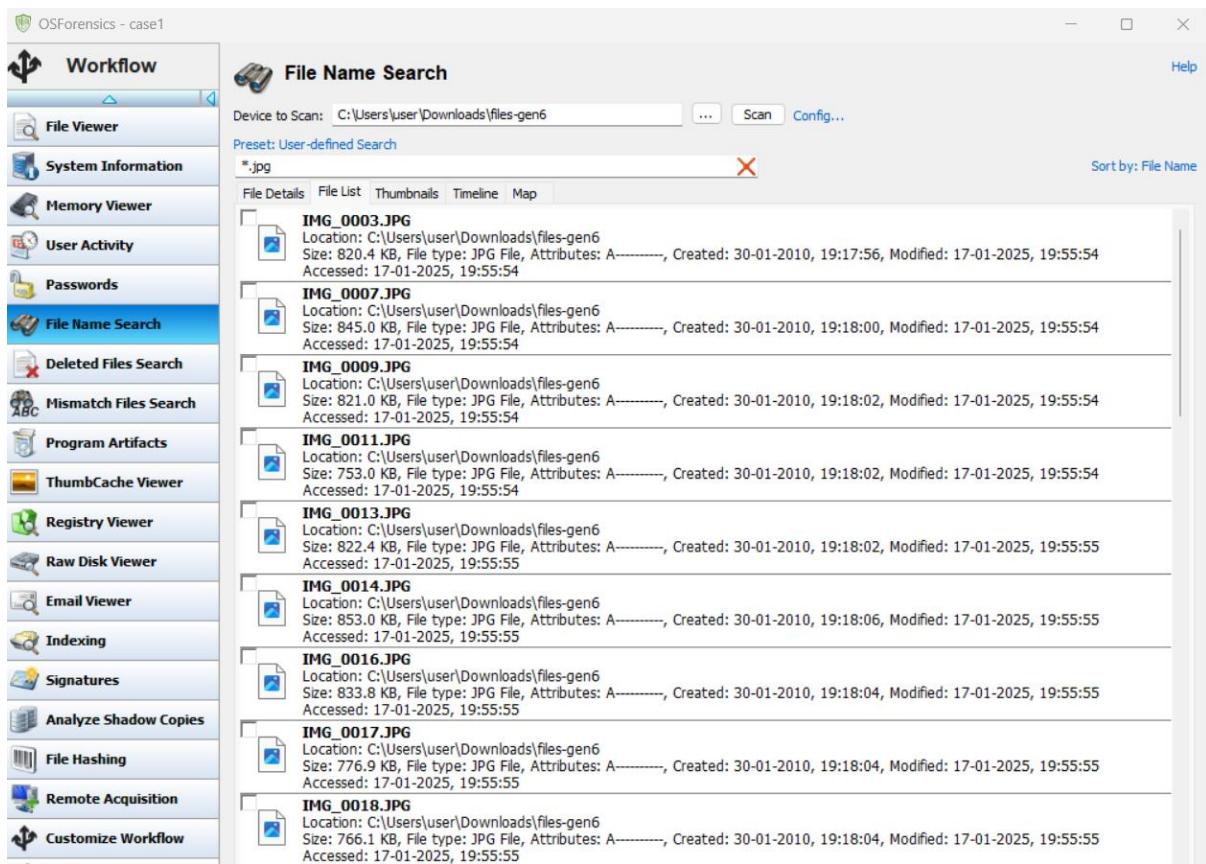
## A new case is created.



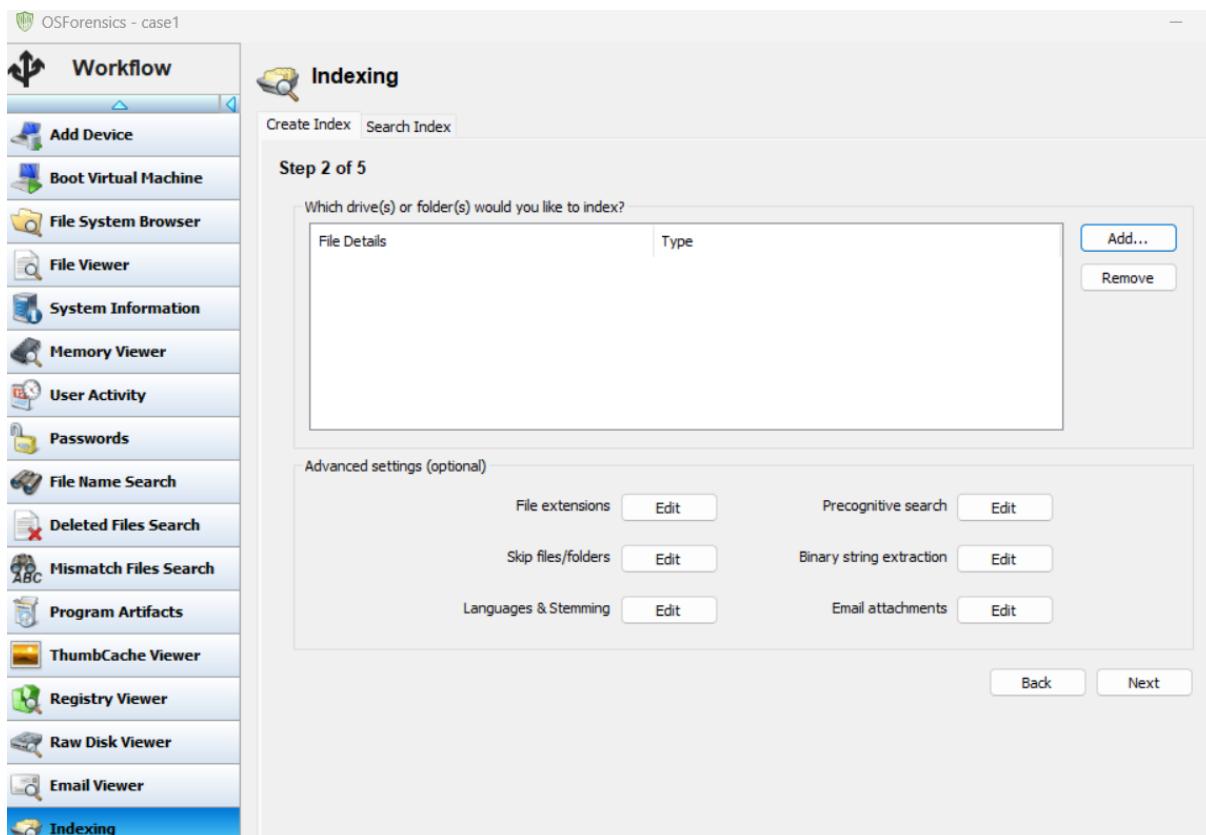
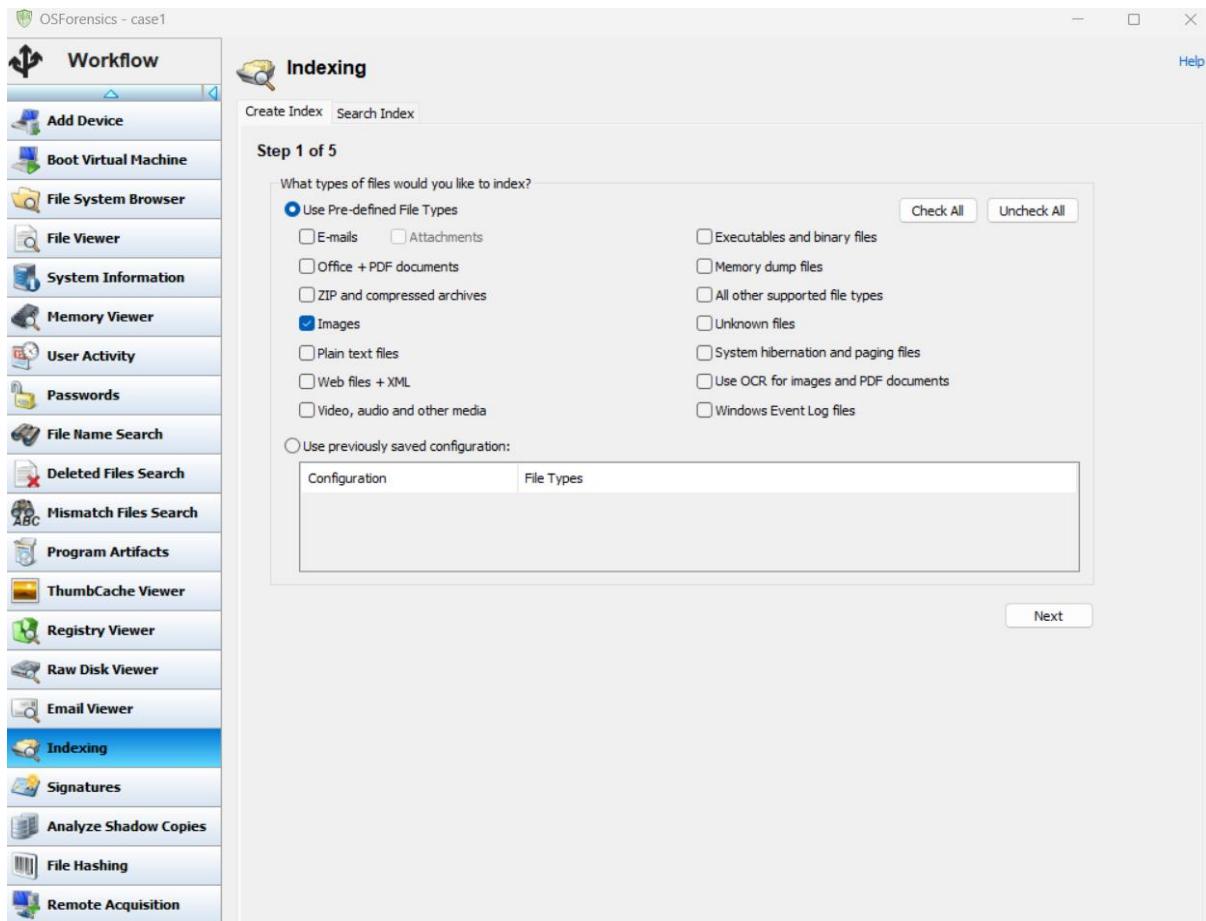
To search for files, type a filename in the search string.

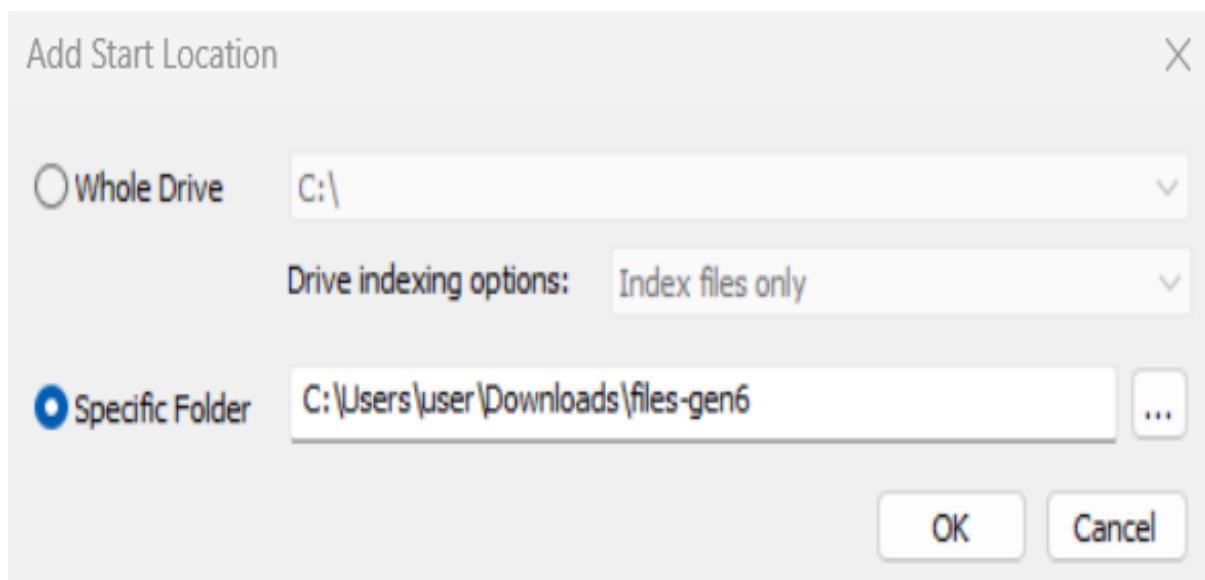
Here we are specifying the location to search for images. This displays all the images present in specified location





To create an index of the content click create index in the left pane of the window.





OSForensics - case1

**Workflow**

- Add Device
- Boot Virtual Machine
- File System Browser
- File Viewer
- System Information
- Memory Viewer
- User Activity
- Passwords
- File Name Search
- Deleted Files Search
- Mismatch Files Search
- Program Artifacts
- ThumbCache Viewer
- Registry Viewer

**Indexing**

Create Index Search Index

Step 2 of 5

Which drive(s) or folder(s) would you like to index?

File Details	Type	Add...	Remove
C:\Users\user\Downloads\files-gen6	Folder		

Advanced settings (optional)

File extensions	Edit	Precognitive search	Edit
Skip files/folders	Edit	Binary string extraction	Edit
Languages & Stemming	Edit	Email attachments	Edit

Back Next

 **Indexing**

Create Index Search Index

**Step 3 of 5**

Memory optimization / Indexing limits

Estimate the number of files (and size) being indexed. This will help optimize memory usage and index more efficiently.

Small  
 Medium  
 Large  
 Extreme  
 Don't know (Pre-scan required)  
 Custom

Max number of files = 5,00,000  
Max file size\* = 47 MB

Estimated RAM required: 4,600 MB (4.6 GB)  
Available RAM: 1,674 MB (1.7 GB)

(Not enough available RAM to proceed. Please reduce the number of threads and/or disable RAM drive)

\*Max file size does not apply to some file formats

Select number of threads:

Use RAM drive for temporary files to speed up indexing

 **Indexing**

Create Index Search Index

**Step 3 of 5**

Memory optimization / Indexing limits

Estimate the number of files (and size) being indexed. This will help optimize memory usage and index more efficiently.

Small  
 Medium  
 Large  
 Extreme  
 Don't know (Pre-scan required)  
 Custom

Pre-scan will determine these settings for you.  
This may take a while (from 5 minutes to 30 minutes) depending on the size of your data.

\*Max file size does not apply to some file formats

Select number of threads:

Use RAM drive for temporary files to speed up indexing

 **Indexing**

Create Index Search Index

**Step 4 of 5**

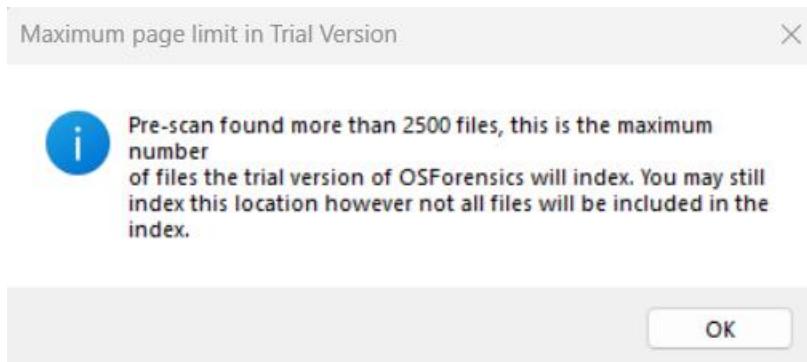
Please enter some details for the index

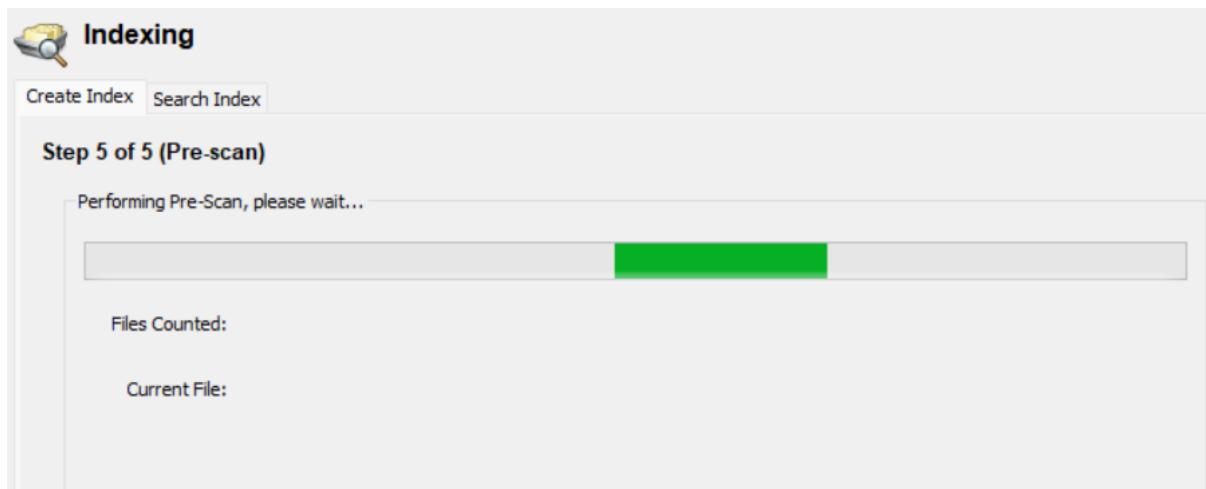
Index Title  
case1

Index Notes

Index of files in:  
C:\Users\user\Downloads\files-gen6

File extensions:  
.jpg, .jpeg, .jpe, .gif, .tiff, .tif, .png, .bmp, .heif, .heic



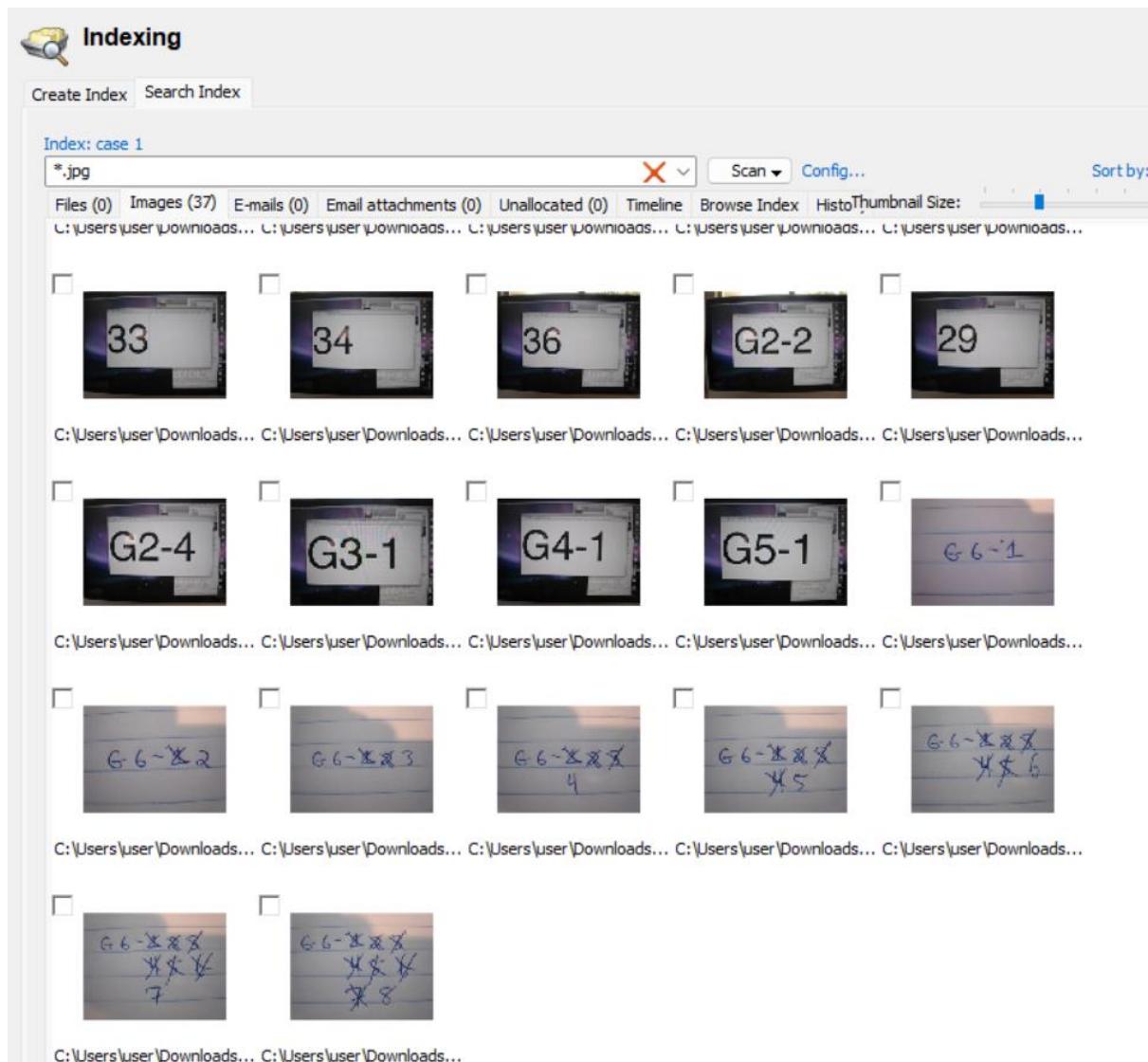


This screenshot shows the 'Indexing' application after the process has completed. The title 'Step 5 of 5' is still present. The main area displays various performance metrics in a grid format:

Start Time	Fri Jan 17 21:24:07 2025	Finish Time	Fri Jan 17 21:24:18 2025
Files Indexed	37	Time Elapsed	00:00:11
Emails Indexed	0	Peak Phys. Mem. Used	45 MB
Alerts	0	Peak Virt. Mem. Used	6626 MB
Warnings	0	Max File & Emails	2500
Total Bytes	27.77 MB	Unique Words	678

A large green progress bar at the bottom indicates the task is finished. Below the stats, a message 'Current Action: Finished' is shown next to a 'Show Log' button. At the bottom, there are buttons for '<< New Index', 'Save configuration', 'Show Precog Results', and 'Cancel'.

Now the index is created.



Click user activity to scan for evidence such as browsed websites, USB drives etc.

 **User Activity**

Device to Scan: C:\ Quick Scan Create Full Timeline

Activity Filters: Not active

Type keyword and press Enter to search

Config... Sort by: Time (Des)

All (0)

- Most Recently Used (0)
- Installed Programs (0)
- Autorun Commands (0)
- Clipboard (0)
- Event Logs (0)
- UserAssist (0)
- Jump Lists (0)
- Shellbags (0)
- Windows 10 Timeline (0)
- Cortana History (0)
- Recycle Bin (0)
- Shimcache (0)
- SRUM (0)
- Prefetch (0)
- Windows Search (0)
- BAM/DAM (0)
- Anti-Forensics Artifacts (0)
- Call History (0)
- Browser History (0)
- Downloads (0)
- Cookies (0)
- Search Terms (0)
- Website Logins (0)
- Form History (0)
- Bookmarks (0)
- Chat Logs (0)
- Peer-to-Peer (0)
- WLAN (0)
- Cryptocurrency Wallet Apps (0)
- Browser Custom Dictionary (0)
- USB (0)

File Details File List Timeline

**User Activity**

Device to Scan: C:\ Quick Scan Create Full Timeline

Activity Filters: Not active

Type keyword and press Enter to search

File Details File List Timeline Config... Sort by: Time (Desc)

All ( 4370 )

- Most Recently Used ( 141 )
- Installed Programs ( 646 )
- Autorun Commands ( 8 )
- Clipboard ( 0 )
- Event Logs ( 1 )
- UserAssist ( 8 )
- Jump Lists ( 1 )
- Shellbags ( 89 )
- Windows 10 Timeline ( 201 )
- Cortana History ( 1 )
- Recycle Bin ( 1 )
- Shimcache ( 0 )
- SRUM ( 0 )
- Prefetch ( 0 )
- Windows Search ( 0 )
- BAM/DAM ( 54 )
- Anti-Forensics ( 0 )
- Call History ( 0 )
- Browser History ( 0 )
- Downloads ( 1 )
- Cookies ( 0 )
- Search Terms ( 0 )
- Website Login ( 0 )
- Form History ( 0 )
- Bookmarks ( 8 )
- Chat Logs ( 0 )
- Peer-to-Peer ( 0 )
- WLAN ( 6 )
- Cryptocurrency Wallet Apps ( 0 )
- Browser Custom Dictionary ( 0 )
- USB ( 21 )

Summary:

Most Recently Used: 141  
Installed Programs: 646  
Autorun Commands: 8  
Event Logs: 1179  
UserAssist: 81  
Jump Lists: 118  
Shellbags: 89  
Windows 10 Timeline: 201  
Recycle Bin: 1  
BAM/DAM: 54  
Browser History: 1742  
Downloads: 15  
Search Terms: 34  
Website Logins: 5  
Form History: 20  
Bookmarks: 8  
WLAN: 6  
USB: 21  
Mounted Volumes: 1

Total Items: 4370

OK

Item	Activity Type	User	Time
p2cys24020_Lab5.docx	Most Recently Used [Link ...]	user	17-01-202
FORENSICS	Most Recently Used [Link ...]	user	17-01-202
ORENSICS/...	Browser History	user	17-01-202
0_Lab5.docx	Jump Lists	user	17-01-202
S	Jump Lists	user	17-01-202
0_Lab5.docx	Most Recently Used [Link ...]	user	17-01-202
0_Lab5.docx	Jump Lists	user	17-01-202
ScreenSke...	BAM/DAM	user	17-01-202
Windows.Cle...	BAM/DAM	user	17-01-202
irddiskVolu...	BAM/DAM	user	17-01-202
NAD.Broker...	BAM/DAM	user	17-01-202
S	Most Recently Used [Rece...	user	17-01-202
0_Lab5.docx	Most Recently Used [Rece...	user	17-01-202
0_Lab5.docx	Most Recently Used [MS ...]	user	17-01-202
8wekyb3d8...	BAM/DAM	user	17-01-202
Started Dow...	Event Logs	user	17-01-202
Installation...	Event Logs	user	17-01-202
sers/user/P...	Browser History	user	17-01-202
ts	Most Recently Used [Link ...]	user	17-01-202
t 2025-01-1...	Most Recently Used [Rece...	user	17-01-202
t 2025-01-1...	Jump Lists	user	17-01-202
t 2025-01-1...	Most Recently Used [Link ...]	user	17-01-202
ts	Jump Lists	user	17-01-202
ts	Jump Lists	user	17-01-202
sketch:edit?...	Browser History	user	17-01-202
sketch:edit?...	Jump Lists	user	17-01-202
Microsoft.ScreenSke...	UserAssist	user	17-01-202
ms-actioncenter:contr...	Browser History	user	17-01-202
ms-actioncenter:contr...	Jump Lists	user	17-01-202
Microsoft.Windows.Sh...	UserAssist	user	17-01-202
My Computer ({20d04...	Shellbags	user	17-01-202
	Shellbags	user	17-01-202
	Shellbags	user	17-01-202

Total Items: 4370 Items Searched: 4132 Items Found: 4370

To recover deleted files click deleted files search from the left pane, select a disk.

**Deleted Files Search**

Device to Scan: \\PhysicalDrive0: Partition 1 [441.33GB NTFS] Sort by: File Name Sec. Sort by: N/A

Preset: All Files

Type search pattern (eg. \*.txt) and press Enter to search

Scan Config... Enable Carving

File Details File List Thumbnails Timeline

File Name	Location	Size	Type	Source	Quality	Date

## Deleted Files Search

Device to Scan: \\PhysicalDrive0: Partition 1 [441.33GB NTFS]

Preset: All Files

Sort by: Disabled while scanning  
Sec. Sort by: Disabled while scanning

Enable Carving

	File Details	File List	Thumbnails	Timeline	Scan Status
<input type="checkbox"/>	M41617.lck Size: 512 Bytes, Attributes: A-, Location: \\PhysicalDrive0: Partition 1\\Virtual Machines\\kal\\kali.vmx.lck, Source: MFT Record, File Number: 1211 Created: 16-01-2025, 11:26:51, Modified: 16-01-2025, 11:26:51, Accessed: 16-01-2025, 11:26:51.6794566				
<input type="checkbox"/>	00380000000004BE56BB88E7E Size: 512 Bytes, Attributes: A-, Location: \\PhysicalDrive0: Partition 1:\\\$Extend\\\$Deleted\\, Source: MFT Record, File Number: 1214 Created: 17-01-2025, 00:17:22, Modified: 17-01-2025, 00:17:22, Accessed: 17-01-2025, 00:17:22.9890586				
<input type="checkbox"/>	00280000000004C30DA075CE Size: 512 Bytes, Attributes: A-, Location: \\PhysicalDrive0: Partition 1:\\\$Extend\\\$Deleted\\, Source: MFT Record, File Number: 1219 Created: 17-01-2025, 00:17:23, Modified: 17-01-2025, 00:17:23, Accessed: 17-01-2025, 00:17:23.0048598				
<input type="checkbox"/>	001B0000000004C502148C19 Size: 512 Bytes, Attributes: A-, Location: \\PhysicalDrive0: Partition 1:\\\$Extend\\\$Deleted\\, Source: MFT Record, File Number: 1221 Created: 17-01-2025, 00:17:22, Modified: 17-01-2025, 00:17:22, Accessed: 17-01-2025, 00:17:22.4069055				
<input type="checkbox"/>	M49268.lck Size: 512 Bytes, Attributes: A-, Location: \\PhysicalDrive0: Partition 1\\_unknown\\D30509.lck, Source: MFT Record, File Number: 1222 Created: 16-01-2025, 11:26:55, Modified: 16-01-2025, 11:26:55, Accessed: 16-01-2025, 11:26:55.9354612				
<input type="checkbox"/>	001D0000000004C7693E3F0F Size: 512 Bytes, Attributes: A-, Location: \\PhysicalDrive0: Partition 1:\\\$Extend\\\$Deleted\\, Source: MFT Record, File Number: 1223 Created: 16-01-2025, 11:26:55, Modified: 16-01-2025, 11:26:55, Accessed: 16-01-2025, 11:26:55.3679985				
<input type="checkbox"/>	M36941.lck Size: 512 Bytes, Attributes: A-, Location: \\PhysicalDrive0: Partition 1\\_unknown\\_, Source: MFT Record, File Number: 1224 Created: 16-01-2025, 11:26:55, Modified: 16-01-2025, 11:26:55, Accessed: 16-01-2025, 11:26:55.3679985				
<input type="checkbox"/>	M45467.lck Size: 512 Bytes, Attributes: A-, Location: \\PhysicalDrive0: Partition 1\\_unknown\\D30509.lck, Source: MFT Record, File Number: 1226 Created: 16-01-2025, 11:26:55, Modified: 16-01-2025, 11:26:55, Accessed: 16-01-2025, 11:26:55.3971076				
<input type="checkbox"/>	M21041.lck Size: 512 Bytes, Attributes: A-, Location: \\PhysicalDrive0: Partition 1\\_unknown\\_, Source: MFT Record, File Number: 1229 Created: 15-01-2025, 17:31:14, Modified: 15-01-2025, 17:31:14, Accessed: 15-01-2025, 17:31:14.4128641				
<input type="checkbox"/>	00100000000004C37F8B58E Size: 512 Bytes, Attributes: A-, Location: \\PhysicalDrive0: Partition 1:\\\$Extend\\\$Deleted\\, Source: MFT Record, File Number: 1231 Created: 15-01-2025, 17:31:14, Modified: 15-01-2025, 17:31:14, Accessed: 15-01-2025, 17:31:14.4128641				
<input type="checkbox"/>	00070000000004D0363FED3C Size: 512 Bytes, Attributes: A-, Location: \\PhysicalDrive0: Partition 1:\\\$Extend\\\$Deleted\\, Source: MFT Record, File Number: 1232 Created: 15-01-2025, 17:31:14, Modified: 15-01-2025, 17:31:14, Accessed: 15-01-2025, 17:31:14.6329489				
<input type="checkbox"/>	M33787.lck Size: 512 Bytes, Attributes: A-, Location: \\PhysicalDrive0: Partition 1\\Virtual Machines\\Kali\\kali.vmsd.lck, Source: MFT Record, File Number: 1233 Created: 15-01-2025, 17:31:15, Modified: 15-01-2025, 17:31:15, Accessed: 15-01-2025, 17:31:15.3048179				
<input type="checkbox"/>	folder.ico Size: 3.19 KB, Attributes: A-, Location: \\PhysicalDrive0: Partition 1\\\$RECYCLE.BIN\\S-1-5-21-1485989799-835829874-4213232815-1001\\, Source: MF Created: 05-09-2024, 17:45:14, Modified: 30-03-2013, 17:59:00, Accessed: 05-09-2024, 17:45:14.0000000				

## Mismatch Files Search

Folder to scan: C:\\Users\\user\\Downloads\\files-gen6

Preset: All

Exclude ext: , Exclude types: , Exclude folders:

File Details  File List  Thumbnails

<input type="checkbox"/>	IMG_0003.JPG Location: C:\\Users\\user\\Downloads\\files-gen6 Identified Type: JPEG image data, EXIF standard 2.2 Size: 820.4 KB, Created: 30-01-2010, 19:17:56, Modified: 17-01-2025, 19:55:54, Accessed: 17-01-2025, 22:19:22
<input type="checkbox"/>	IMG_0007.JPG Location: C:\\Users\\user\\Downloads\\files-gen6 Identified Type: JPEG image data, EXIF standard 2.2 Size: 845.0 KB, Created: 30-01-2010, 19:18:00, Modified: 17-01-2025, 19:55:54, Accessed: 17-01-2025, 22:19:22
<input type="checkbox"/>	IMG_0009.JPG Location: C:\\Users\\user\\Downloads\\files-gen6 Identified Type: JPEG image data, EXIF standard 2.2 Size: 821.0 KB, Created: 30-01-2010, 19:18:02, Modified: 17-01-2025, 19:55:54, Accessed: 17-01-2025, 22:19:22
<input type="checkbox"/>	IMG_0011.JPG Location: C:\\Users\\user\\Downloads\\files-gen6 Identified Type: JPEG image data, EXIF standard 2.2 Size: 753.0 KB, Created: 30-01-2010, 19:18:02, Modified: 17-01-2025, 19:55:54, Accessed: 17-01-2025, 22:19:22
<input type="checkbox"/>	IMG_0013.JPG Location: C:\\Users\\user\\Downloads\\files-gen6 Identified Type: JPEG image data, EXIF standard 2.2 Size: 822.4 KB, Created: 30-01-2010, 19:18:02, Modified: 17-01-2025, 19:55:55, Accessed: 17-01-2025, 22:19:22
<input type="checkbox"/>	IMG_0014.JPG Location: C:\\Users\\user\\Downloads\\files-gen6 Identified Type: JPEG image data, EXIF standard 2.2 Size: 853.0 KB, Created: 30-01-2010, 19:18:06, Modified: 17-01-2025, 19:55:55, Accessed: 17-01-2025, 22:19:22
<input type="checkbox"/>	IMG_0016.JPG Location: C:\\Users\\user\\Downloads\\files-gen6 Identified Type: JPEG image data, EXIF standard 2.2 Size: 833.8 KB, Created: 30-01-2010, 19:18:04, Modified: 17-01-2025, 19:55:55, Accessed: 17-01-2025, 22:19:22
<input type="checkbox"/>	IMG_0017.JPG Location: C:\\Users\\user\\Downloads\\files-gen6 Identified Type: JPEG image data, EXIF standard 2.2 Size: 776.9 KB, Created: 30-01-2010, 19:18:04, Modified: 17-01-2025, 19:55:55, Accessed: 17-01-2025, 22:19:22
<input type="checkbox"/>	IMG_0018.JPG Location: C:\\Users\\user\\Downloads\\files-gen6 Identified Type: JPEG image data, EXIF standard 2.2 Size: 766.1 KB, Created: 30-01-2010, 19:18:04, Modified: 17-01-2025, 19:55:55, Accessed: 17-01-2025, 22:19:22
<input type="checkbox"/>	IMG_0019.JPG Location: C:\\Users\\user\\Downloads\\files-gen6 Identified Type: JPEG image data, EXIF standard 2.2 Size: 844.0 KB, Created: 30-01-2010, 19:18:04, Modified: 17-01-2025, 19:55:55, Accessed: 17-01-2025, 22:19:22

To view the process running in system click memory viewer

The screenshot shows the OSForensics Memory Viewer interface. The main window displays a table of processes running in memory, with columns for Process, PID, CPU %, Total CPU Time, User Time, Kernel Time, and Process Create Time. The total memory usage is listed as 7.73 GB. A warning message is displayed in a modal dialog: "The memory viewer shows the active memory of the computer that OSForensics is currently running on. It cannot be used to show any information from an acquired drive or image." There is an "OK" button at the bottom of the dialog.

Process	PID	CPU %	Total CPU Time	User Time	Kernel Time	Process Create Time
Idle	0	99.21%	02:28:12.734	00:00:00.000	02:28:12.734	15-01-2025, 02:05:09
System	4	0.39%	00:19:46.546	00:00:00.000	00:19:46.546	15-01-2025, 02:05:09
Secure System	108		00:00:00.000	00:00:00.000	00:00:00.000	15-01-2025, 02:05:06
Registry	144		00:00:02.390	00:00:00.000	00:00:02.390	15-01-2025, 02:05:06
vmnetdhcp.exe	424		00:00:00.109	00:00:00.031	00:00:00.078	15-01-2025, 07:10:51
smss.exe	548		00:00:00.109	00:00:00.015	00:00:00.093	15-01-2025, 02:05:09
msedgewebview2.exe	556		00:00:16.046	00:00:08.531	00:00:07.515	17-01-2025, 17:54:24
chrome.exe	732		00:00:00.375	00:00:00.265	00:00:00.109	17-01-2025, 19:53:30
services.exe				12.375	00:00:14.390	15-01-2025, 02:05:15
csrss.exe				00.468	00:00:01.796	15-01-2025, 02:05:14
wininit.exe				00.031	00:00:00.062	15-01-2025, 02:05:15
svchost.exe				00.062	00:00:00.046	15-01-2025, 02:15:09
svchost.exe				00.078	00:00:00.281	15-01-2025, 02:05:18
LsaIso.exe				00.000	00:00:00.281	15-01-2025, 02:05:15
lsass.exe				41.750	00:00:28.093	15-01-2025, 02:05:15
svchost.exe				00.375	00:00:00.531	15-01-2025, 02:05:15
svchost.exe				00.187	00:00:00.187	15-01-2025, 02:05:15
svchost.exe				27.312	00:00:41.421	15-01-2025, 02:05:15

The screenshot shows the OSForensics Memory Viewer interface. The main window displays a table of processes running in memory, with columns for Process, PID, CPU %, Total CPU Time, User Time, Kernel Time, and Process Create Time. The total memory usage is listed as 7.73 GB. The "chrome.exe" process is selected, highlighted with a blue border. A detailed view of the memory layout for this process is shown in a separate window below, titled "Memory Layout". The layout table includes columns for Address Range, Size, State, Protection, Type, and Module.

Address Range	Size	State	Protection	Type	Module
0x0000000000000000 - 0x00000...	2048 MB	Free	NA	-	
0x000000007FFE0000 - 0x00000...	4 KB	Commit	RO	Private	
0x000000007FFE1000 - 0x00000...	4 KB	Commit	RO	Private	
0x000000007FFE2000 - 0x00000...	417522 MB	Free	NA	-	
0x000000666F200000 - 0x00000...	16 KB	Commit	RW	Private	
0x000000666F204000 - 0x00000...	144 KB	Reserved	-	Private	
0x000000666F228000 - 0x00000...	8 KB	Commit	RW	Private	
0x000000666F22A000 - 0x00000...	2 MB	Reserved	-	Private	
0x000000666F3000 - 0x00000...	52 KB	Commit	RW	Private	
0x000000666F302000 - 0x00000...	2 MB	...	-	Private	

To analyze the raw sectors of all physical disks and partitions click raw disk viewer and select a disk to view its raw disk components.

To retrieve detailed information about core component of the system, click system information

Name	Command	Internal	Architect...	Live Acquisi...	Drive Lette...	Image Acq...
Computer Name	SysInfoDll_GetComputerName	Yes	32/64	Yes	No	No
Operating system	SysInfoDll_GetOS	Yes	32/64	Yes	No	No
CPU Info	SysInfoDll_GetCPUInfo	Yes	32/64	Yes	No	No
Mem Info	SysInfoDll_GetMemoryInfo	Yes	32/64	Yes	No	No
Graphics Info	SysInfoDll_GetGraphicsInfo	Yes	32/64	Yes	No	No
USB Info	SysInfoDll_GetUSBInfo	Yes	32/64	Yes	No	No
Disk volume Info	SysInfoDll_GetSystemInfo_SM...	Yes	32/64	Yes	No	No
Disk drive Info	SysInfoDll_GetSystemInfo_SM...	Yes	32/64	Yes	No	No
Optical drive Info	SysInfoDll_GetSystemInfo_SM...	Yes	32/64	Yes	No	No
Network Info	SysInfoDll_GetSystemInfo_SM...	Yes	32/64	Yes	No	No
Ports Info	SysInfoDll_GetSystemInfo_SM...	Yes	32/64	Yes	No	No
Motherboard Info	SysInfoDll_GetMotherboardInfo	Yes	32/64	Yes	No	No
Printers	WinSpool.lib	Yes	32/64	Yes	No	No

**System Information**

Device to Scan: C:\ Scan

Command List: All Commands

Type search text and press Enter

Commands

Name	Command	Internal	Architect...	Live Acquisi...	Drive Lette...	Image Acq...
at.exe	at.exe	No	32/64	Yes	No	No
getmac.exe	getmac.exe	No	32/64	Yes	No	No
hostname.exe	hostname.exe	No	32/64	Yes	No	No
ipconfig.exe /all	ipconfig.exe /all	No	32/64	Yes	No	No
msinfo32.exe /report %t	msinfo32.exe /report %t	No	32/64	Yes	No	No
nbtstat.exe -n	nbtstat.exe -n	No	32/64	Yes	No	No
nbtstat.exe -A 127.0.0.1	nbtstat.exe -A 127.0.0.1	No	32/64	Yes	No	No
nbtstat.exe -S	nbtstat.exe -S	No	32/64	Yes	No	No
nbtstat.exe -c	nbtstat.exe -c	No	32/64	Yes	No	No
net.exe share	net.exe share	No	32/64	Yes	No	No
net.exe use	net.exe use	No	32/64	Yes	No	No
net.exe file	net.exe file	No	32/64	Yes	No	No
net.exe user	net.exe user	No	32/64	Yes	No	No
net.exe accounts	net.exe accounts	No	32/64	Yes	No	No
net.exe view	net.exe view	No	32/64	Yes	No	No
net.exe start	net.exe start	No	32/64	Yes	No	No
net.exe session	net.exe session	No	32/64	Yes	No	No
net.exe localgroup administrat...	net.exe localgroup administrat...	No	32/64	Yes	No	No
net.exe localgroup	net.exe localgroup	No	32/64	Yes	No	No
net.exe localgroup administrators	net.exe localgroup administrators	No	32/64	Yes	No	No
net.exe group	net.exe group	No	32/64	Yes	No	No
netstat.exe -ao	netstat.exe -ao	No	32/64	Yes	No	No
netstat.exe -no	netstat.exe -no	No	32/64	Yes	No	No
openfiles.exe /query /v	openfiles.exe /query /v	No	32	Yes	No	No
quser.exe	quser.exe	No	32/64	Yes	No	No
route.exe print	route.exe print	No	32/64	Yes	No	No
sc.exe query	sc.exe query	No	32/64	Yes	No	No
sc.exe queryex	sc.exe queryex	No	32/64	Yes	No	No
srvcheck.exe	srvcheck.exe	No	32	Yes	No	No
ping 127.0.0.1	ping 127.0.0.1	No	32/64	Yes	No	No
tasklist.exe /svc	tasklist.exe /svc	No	32/64	Yes	No	No
whoami.exe	whoami.exe	No	32/64	Yes	No	No
manage-bde.exe -status	manage-bde.exe -status	No	32/64	Yes	No	No

To verify the integrity of file by calculating their hash values, click file hashing.

**OSForensics - case1**

**Workflow**

- File Viewer
- System Information
- Memory Viewer
- User Activity
- Passwords
- File Name Search
- Deleted Files Search
- Mismatch Files Search
- Program Artifacts
- ThumbCache Viewer
- Registry Viewer
- Raw Disk Viewer
- Email Viewer
- Indexing
- Signatures
- Analyze Shadow Copies
- File Hashing**
- Remote Acquisition
- Customize Workflow
- Register
- Exit

**File Hashing**

Hash Sets Verify/Create Hash

File  Volume  Text

File  ... Calculate

Hash Function SHA-1 Secondary Hash Function MD5

Upper case output

Progress

Data Hashed

Calculated Hash

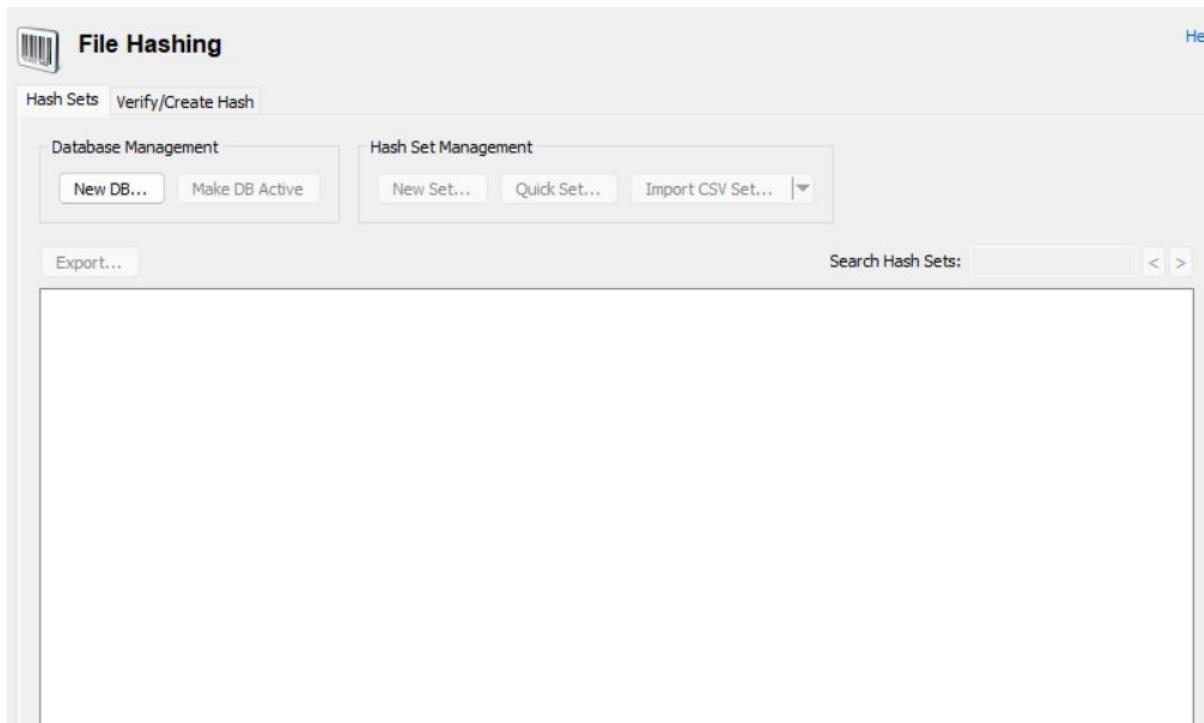
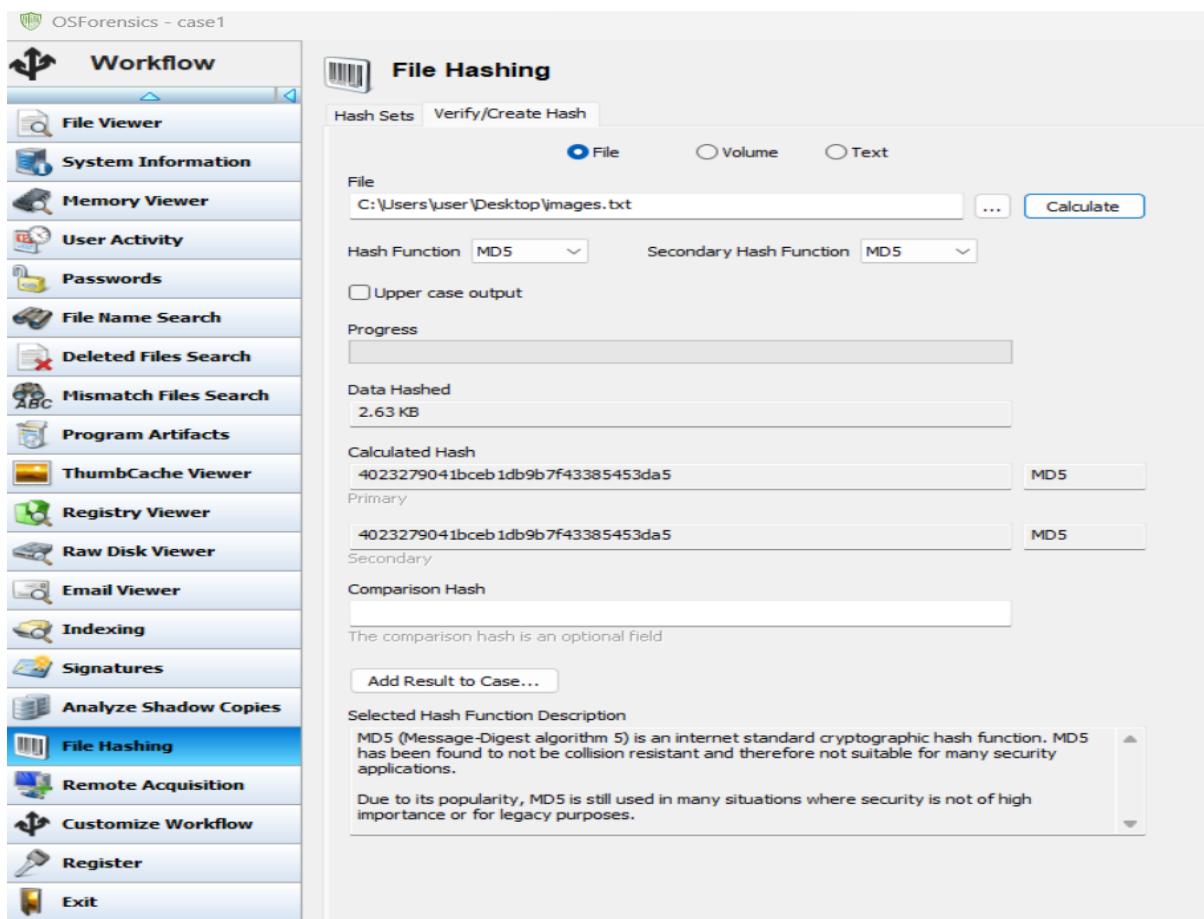
Primary

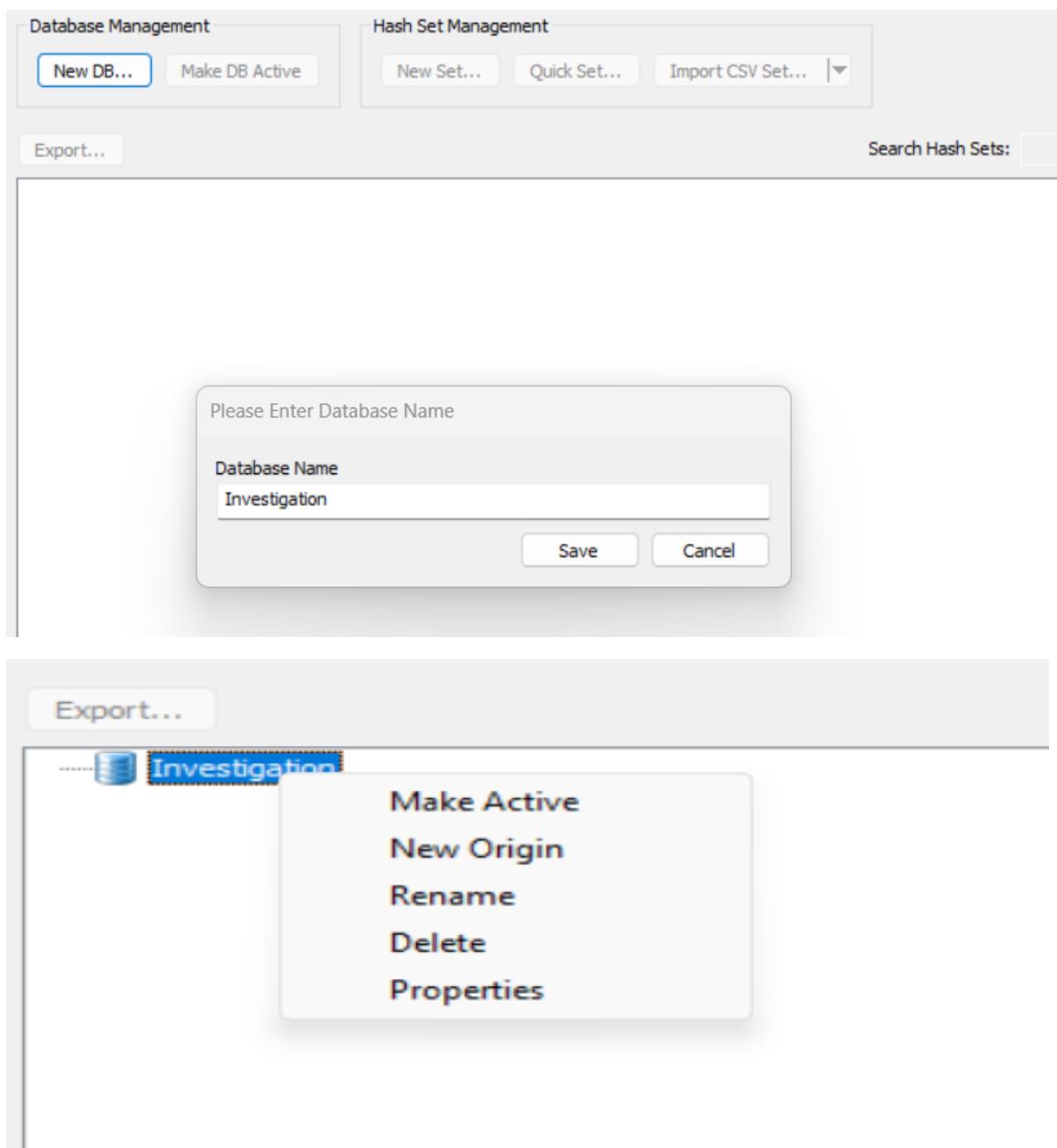
Secondary

Comparison Hash   
The comparison hash is an optional field

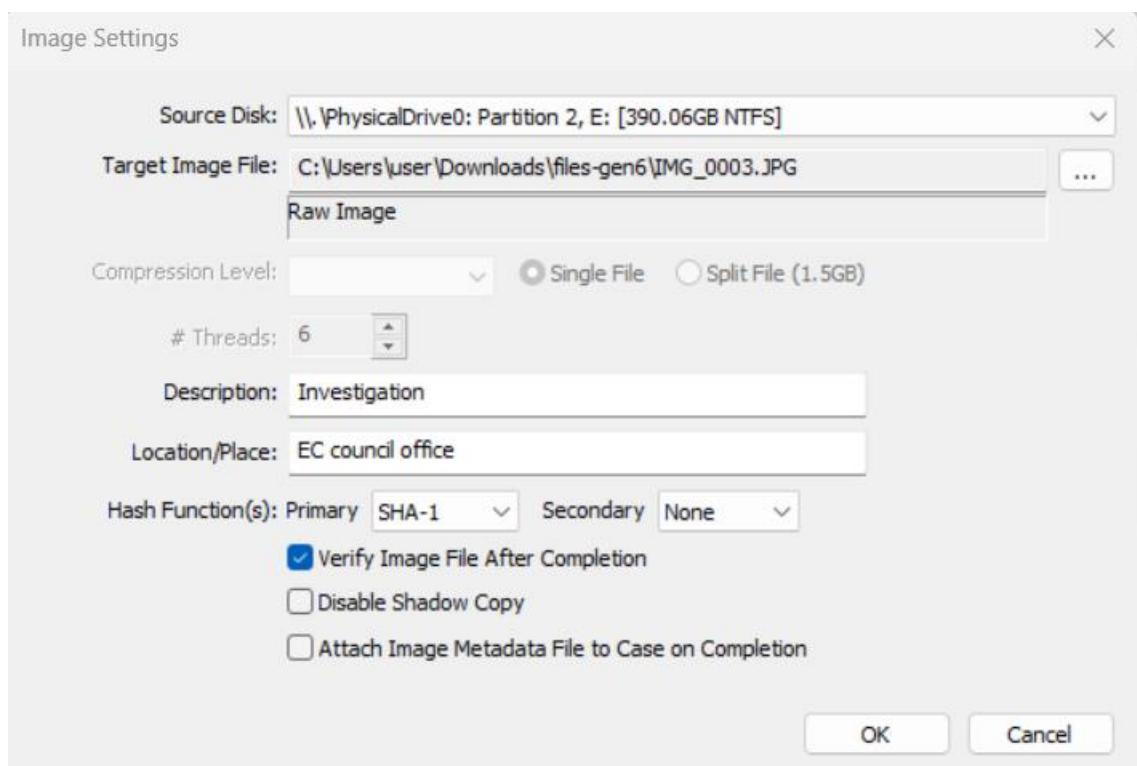
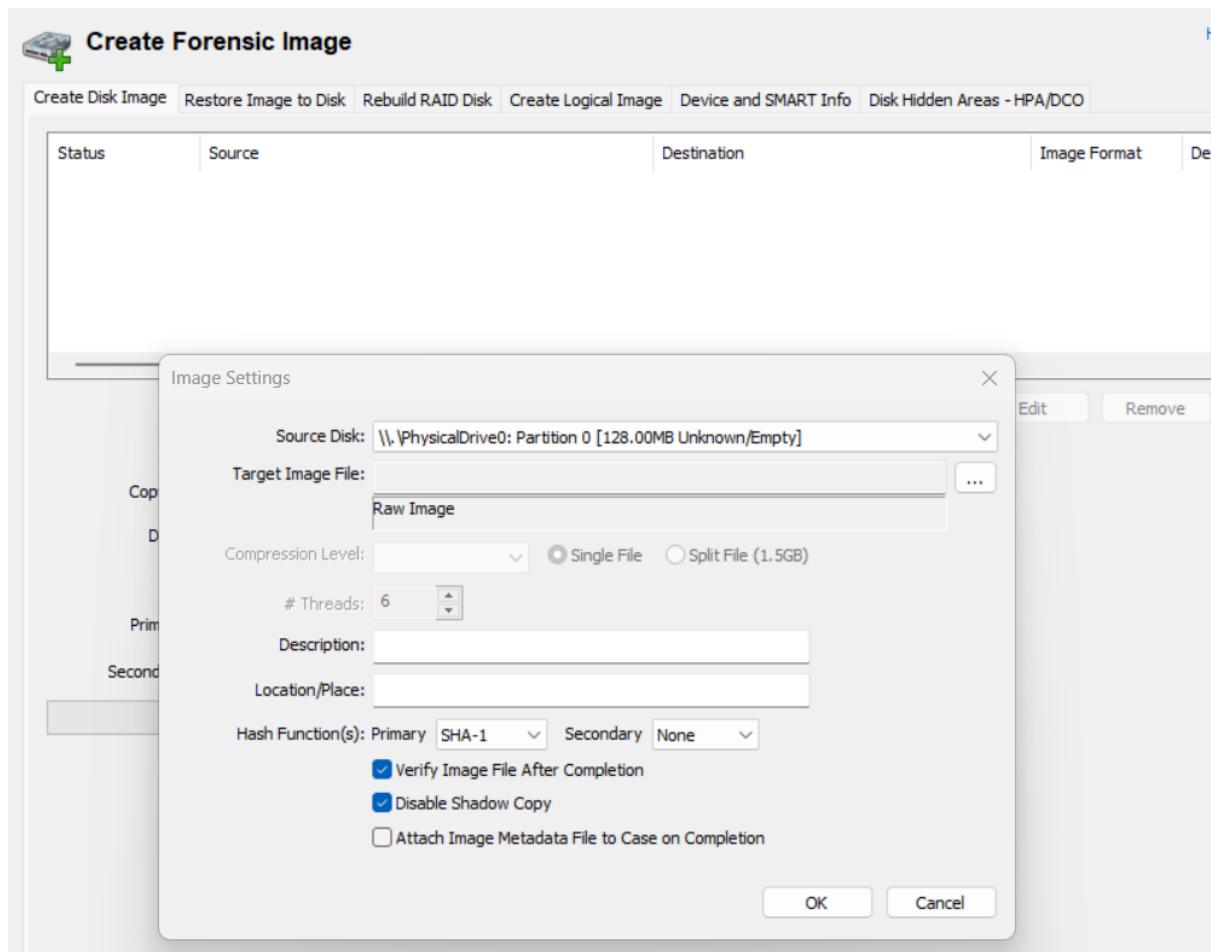
Add Result to Case...

Selected Hash Function Description





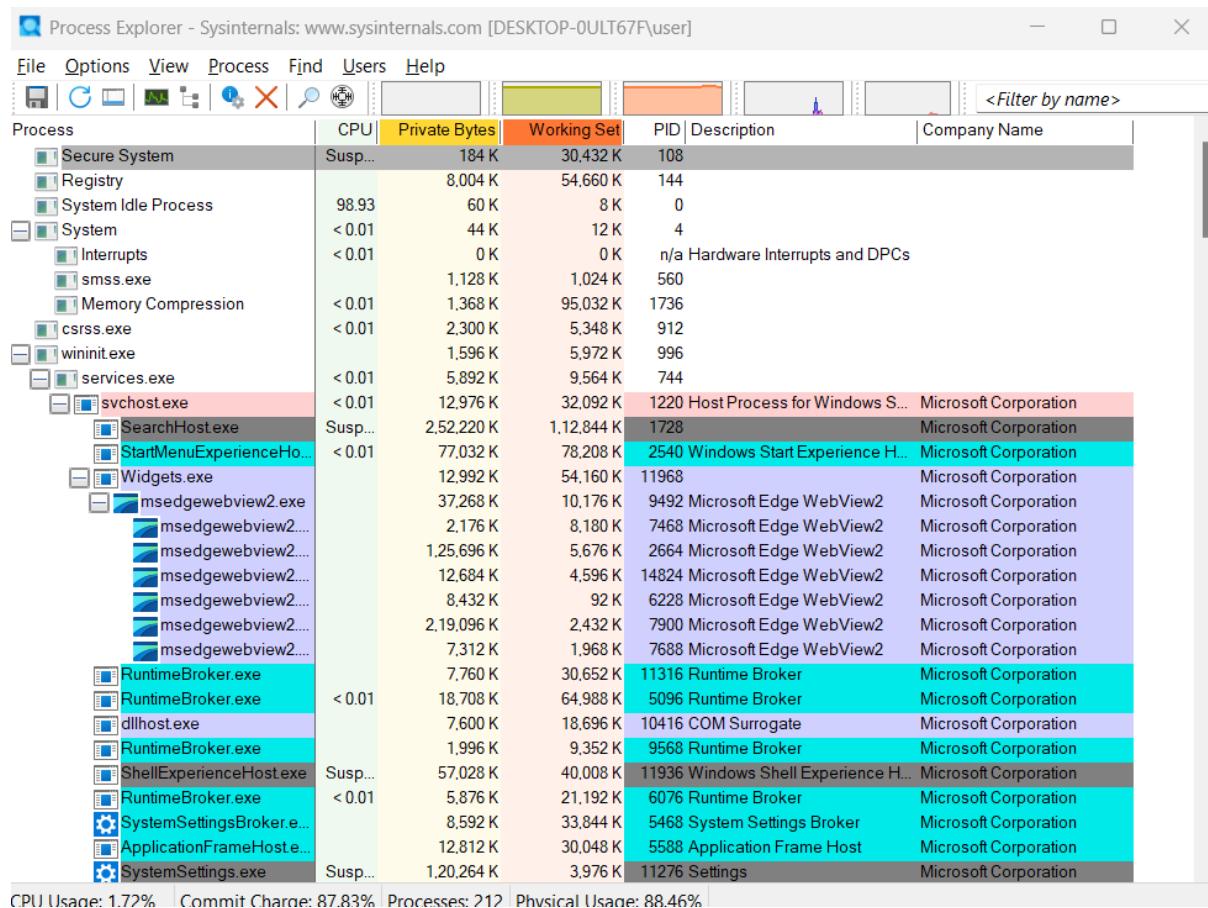
generate exact copies of partitions or whole drive



## Lab2: Extracting information about Loaded Processes Using Process Explorer

Objective: The purpose of this lab is to learn how to investigate loaded processes. In this lab we will learn how to use Process Explorer.

Process Explorer GUI appears, displaying all the details of all the process running on the machine



Process Explorer lists all the running processes in the left pane, and details of each process such as CPU usage, PID etc in the right pane.

Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-0ULT67F\user]

This screenshot shows the Process Explorer interface with the following details:

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
smss.exe		1,128 K	1,024 K	560		
Memory Compression		1,384 K	1,10,924 K	1736		
csrss.exe		2,300 K	5,300 K	912		
wininit.exe		1,596 K	5,972 K	996		
services.exe		5,720 K	9,444 K	744		
svchost.exe	< 0.01	12,740 K	31,944 K	1220	Host Process for Windows S...	Microsoft Corporation
SearchHost.exe	Susp...	2,52,220 K	1,12,844 K	1728	2540 Windows Start Experience H...	Microsoft Corporation
StartMenuExperienceHo...		77,060 K	78,208 K			
Widgets.exe		12,916 K	53,808 K	11968		
msedgewebview2.exe		37,268 K	10,176 K	9492	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2....		2,176 K	8,048 K	7468	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2....		1,25,696 K	5,676 K	2664	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2....		12,684 K	4,596 K	14824	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2....		8,432 K	92 K	6228	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2....		2,19,096 K	2,432 K	7900	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2....		7,312 K	1,988 K	7688	Microsoft Edge WebView2	Microsoft Corporation
RuntimeBroker.exe		7,620 K	30,572 K	11316	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		19,752 K	67,180 K	5096	Runtime Broker	Microsoft Corporation
dllhost.exe		7,544 K	18,636 K	10416	COM Surrogate	Microsoft Corporation
RuntimeBroker.exe	Susp...	1,928 K	9,300 K	9568	Runtime Broker	Microsoft Corporation
ShellExperienceHost.exe		59,756 K	62,044 K	11936	Windows Shell Experience H...	Microsoft Corporation
RuntimeBroker.exe		5,876 K	27,412 K	6076	Runtime Broker	Microsoft Corporation
SystemSettingsBroker.e...		8,520 K	33,768 K	5468	System Settings Broker	Microsoft Corporation
ApplicationFrameHost...		12,812 K	29,796 K	5588	Application Frame Host	Microsoft Corporation
SystemSettings.exe	Susp...	1,20,264 K	3,620 K	11276	Settings	Microsoft Corporation
WidgetService.exe		4,788 K	21,744 K	11228	WidgetService.exe	Microsoft Corporation
WmiPrvSE.exe		4,324 K	13,412 K	14568		
LockApp.exe	Susp...	47,088 K	65,940 K	7788	LockApp.exe	Microsoft Corporation
RuntimeBroker.exe		11,896 K	41,820 K	1164	Runtime Broker	Microsoft Corporation
FileCoAuth.exe		6,648 K	27,060 K	12644	Microsoft OneDriveFile Co-A...	Microsoft Corporation

CPU Usage: 1.90% Commit Charge: 79.47% Processes: 211 Physical Usage: 89.65%

To view system information go to view in the menu bar and select system information

Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-0ULT67F\user]

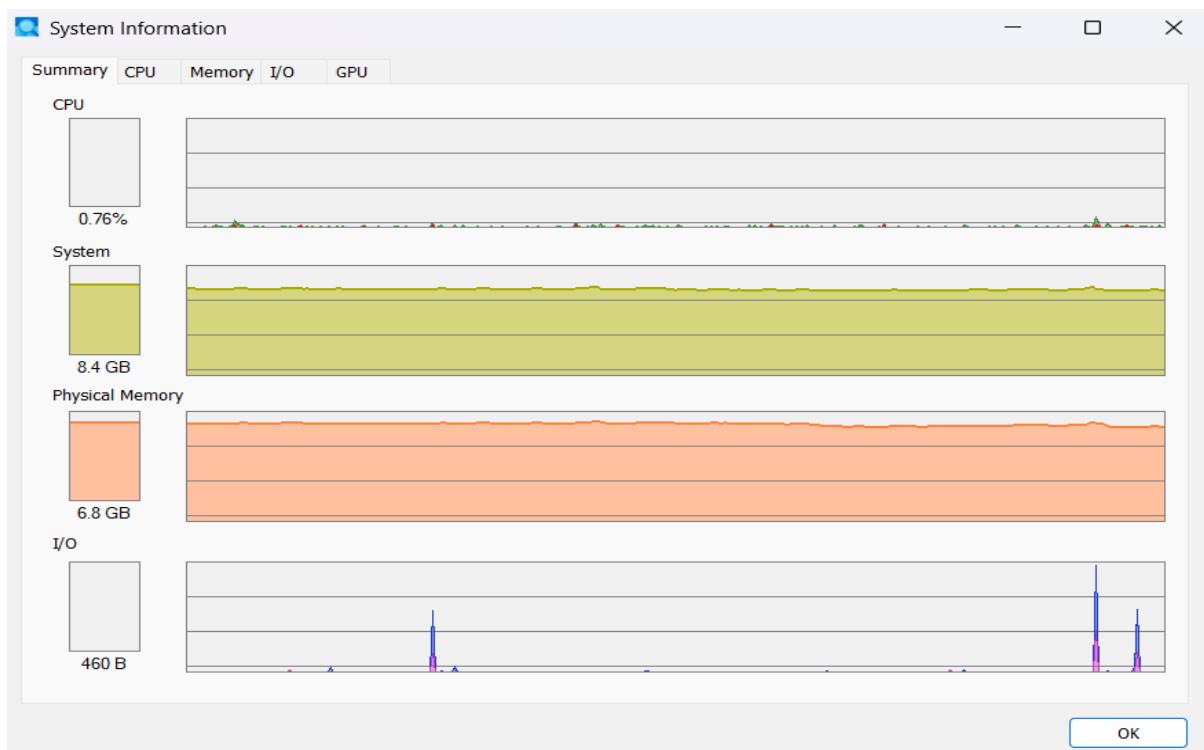
This screenshot shows the Process Explorer interface with the View menu open, displaying the following options:

- System Information... (selected)
- Show Process Tree
- Show Column Heatmaps
- Scroll to New Processes
- Show Unnamed Handles and Mappings
- Show Processes From All Users
- Opacity
- Show Lower Pane
- Lower Pane View
- Refresh Now
- Update Speed
- Organize Column Sets...
- Save Column Set...
- Load Column Set
- Select Columns...

The main pane displays the same process list as the previous screenshot.

CPU Usage: 2.06% Commit Charge: 78.97% Processes: 211 Physical Usage: 87.96%

It will displays global system performance metrics.



To view DLLs click view->lower pane view->DLLs

The Process Explorer window shows the following details:

- File Options View Process Find Users Help**
- View Submenu:**
  - System Information... Ctrl+I
  - Show Process Tree Ctrl+T
  - Show Column Heatmaps
  - Scroll to New Processes
  - Show Unnamed Handles and Mappings
  - Show Processes From All Users
  - Opacity
  - Show Lower Pane Ctrl+L
  - Lower Pane View** (selected)
  - Refresh Now F5
  - Update Speed
  - Organize Column Sets...
  - Save Column Set...
  - Load Column Set
  - Select Columns...
- Table View:** Shows a list of processes with columns for PID, Description, and Company Name.

PID	Description	Company Name
560		
1736		
912		
996		
744		
1220	Host Process for Windows S...	Microsoft Corporation
1728		Microsoft Corporation
2540	Windows Start Experience H...	Microsoft Corporation
1968		Microsoft Corporation
9492	Microsoft Edge WebView2	Microsoft Corporation
7688	Microsoft Edge WebView2	Microsoft Corporation
1316	Runtime Broker	Microsoft Corporation
5096	Runtime Broker	Microsoft Corporation
10416	COM Surrogate	Microsoft Corporation
9568	Runtime Broker	Microsoft Corporation
11936	Windows Shell Experience H...	Microsoft Corporation
6076	Runtime Broker	Microsoft Corporation
5468	System Settings Broker	Microsoft Corporation
5588	Application Frame Host	Microsoft Corporation
11276	Settings	Microsoft Corporation
11228	WidgetService.exe	Microsoft Corporation
7788	LockApp.exe	Microsoft Corporation
1164	Runtime Broker	Microsoft Corporation
12644	Microsoft OneDriveFile Co-A...	Microsoft Corporation

CPU Usage: 1.33% Commit Charge: 78.40% Processes: 210 Physical Usage: 84.22%

Here we can view the list of DLLs for the selected process in the bottom pane window.

The screenshot shows the Process Explorer interface with the following details:

- Top Bar:** File, Options, View, Process, Find, Users, DLL, Help.
- Process Tree:** smss.exe, Memory Compression, csrss.exe, wininit.exe, services.exe, svchost.exe (selected), SearchHost.exe, StartMenuExperienceHo..., Widgets.exe, msedgewebview2.exe, msedgewebview2..., msedgewebview2..., msedgewebview2..., msedgewebview2... (all under Widgets.exe).
- Bottom Tab:** Handles, DLLs (selected), Threads.
- DLL List Table:**

Name	Description	Company Name	Path
{6AF0698E-D558-4F...			C:\ProgramData\Microsoft\Windows\Caches\{6AF0698E-D5...
{AFBF9F1A-8EE8-4...			C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{...
{DDF571F2-BE98-4...			C:\ProgramData\Microsoft\Windows\Caches\{DDF571F2-BE...
advapi32.dll	Advanced Windows 32 Base API	Microsoft Corporation	C:\Windows\System32\advapi32.dll
apphelp.dll	Application Compatibility Client Libr...	Microsoft Corporation	C:\Windows\System32\apphelp.dll
AppXDeploymentCli...	AppX Deployment Client DLL	Microsoft Corporation	C:\Windows\System32\AppXDeploymentClient.dll
BCP47mrm.dll	BCP47 Language Classes for Res...	Microsoft Corporation	C:\Windows\System32\BCP47mrm.dll
bcrypt.dll	Windows Cryptographic Primitives ...	Microsoft Corporation	C:\Windows\System32\bcrypt.dll
bcryptprimitives.dll	Windows Cryptographic Primitives ...	Microsoft Corporation	C:\Windows\System32\bcryptprimitives.dll
biwinrt.dll	Windows Background Broker Infras...	Microsoft Corporation	C:\Windows\System32\biwinrt.dll
C_1252.NLS			C:\Windows\System32\C_1252.NLS
C_1252.NLS			C:\Windows\System32\C_1252.NLS
C_28591.NLS			C:\Windows\System32\C_28591.NLS
C_437.NLS			C:\Windows\System32\C_437.NLS
- Metrics:** CPU Usage: 1.50%, Commit Charge: 78.82%, Processes: 209, Physical Usage: 86.11%.

To view the properties of DLL right click a required DLL from the DLL list and select properties.

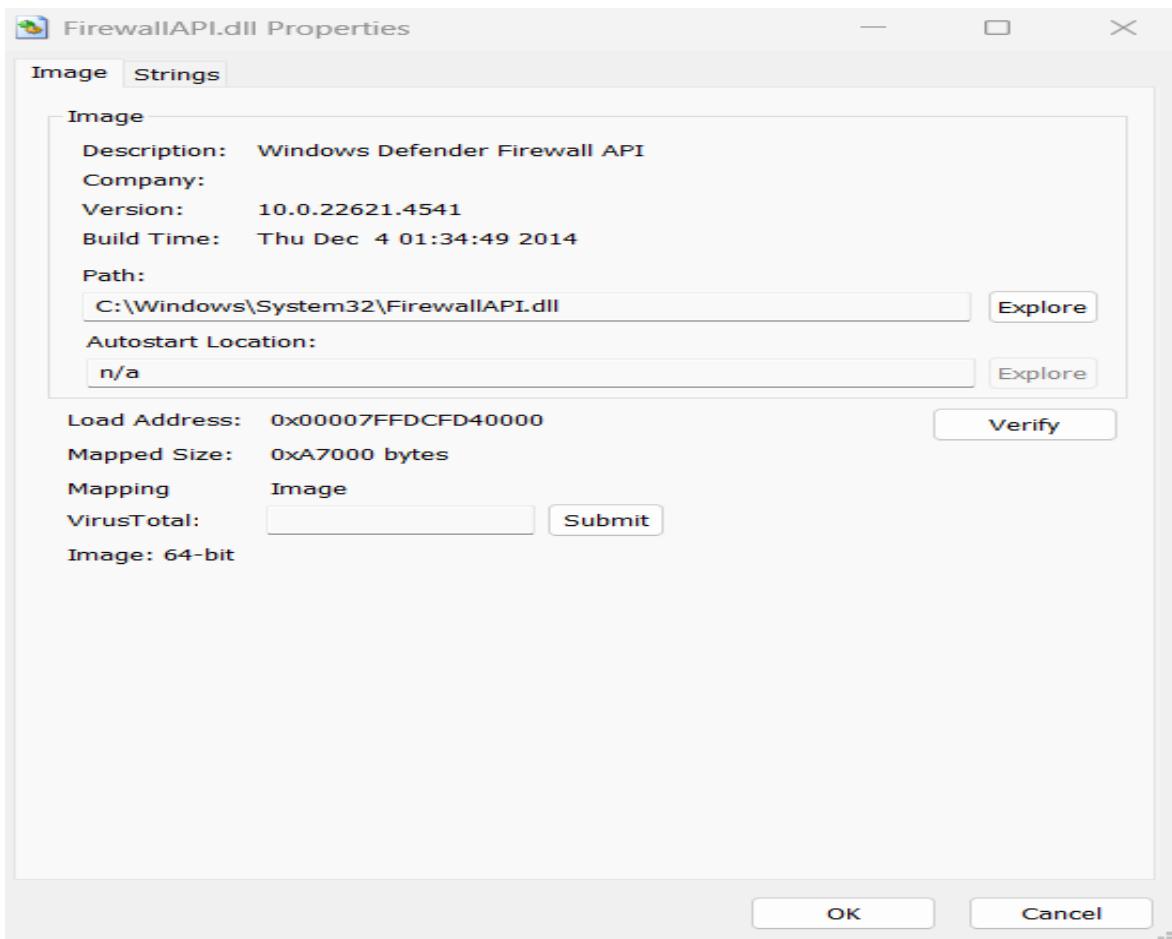
The screenshot shows the Process Explorer interface with the following details:

- Bottom Tab:** Handles, DLLs (selected), Threads.
- DLL List Table:**

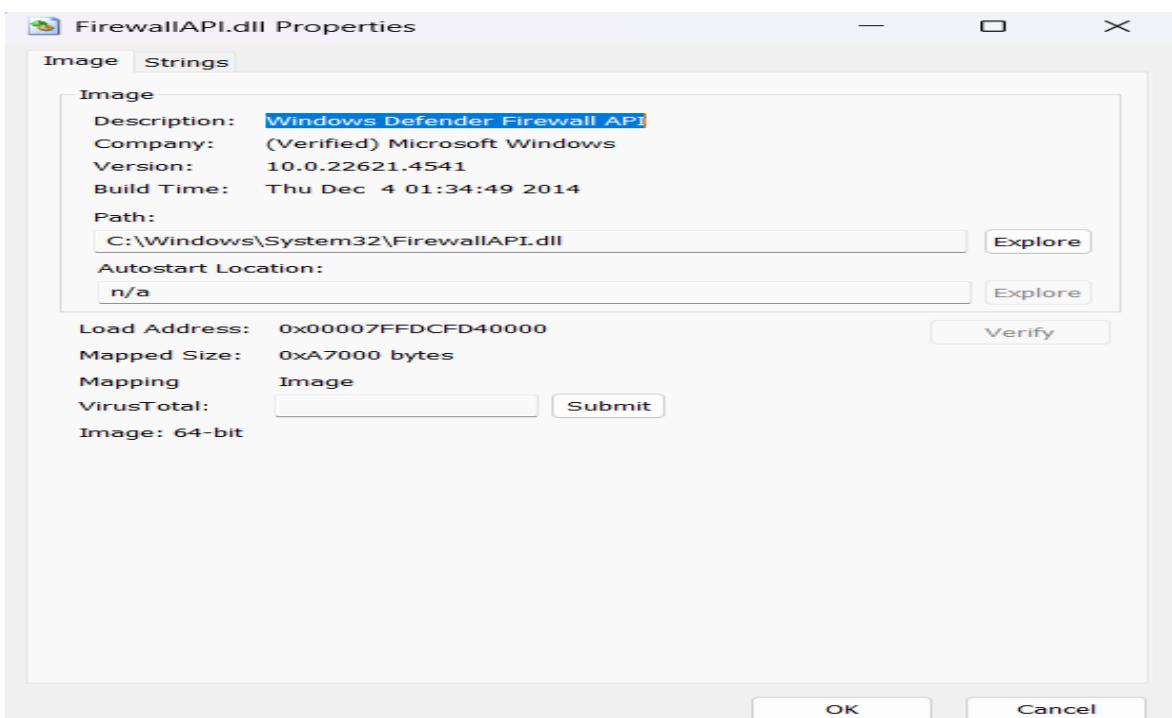
Name	Description	Company Name	Path
advapi32.dll	Advanced Windows 32 Base API	Microsoft Corporation	C:\Windows\System32\advapi32.dll
bcrypt.dll	Windows Cryptographic Primitives ...	Microsoft Corporation	C:\Windows\System32\bcrypt.dll
bcryptprimitives.dll	Windows Cryptographic Primitives ...	Microsoft Corporation	C:\Windows\System32\bcryptprimitives.dll
C_1252.NLS			C:\Windows\System32\C_1252.NLS
C_1252.NLS			C:\Windows\System32\C_1252.NLS
C_437.NLS			C:\Windows\System32\C_437.NLS
crypt32.dll	Crypto API32	Microsoft Corporation	C:\Windows\System32\crypt32.dll
FirewallAPI.dll		Microsoft Corporation	C:\Windows\System32\FirewallAPI.dll
fwbase.dll		Microsoft Corporation	C:\Windows\System32\fwbase.dll
gdi32.dll	Search Online...	Microsoft Corporation	C:\Windows\System32\gdi32.dll
gdi32full.dll		Microsoft Corporation	C:\Windows\System32\gdi32full.dll
kernel32.dll		Microsoft Corporation	C:\Windows\System32\kernel32.dll
KernelBase.dll	Windows NT BASE API Client DLL	Microsoft Corporation	C:\Windows\System32\KernelBase.dll
- Context Menu:** Properties..., Search Online..., Ctrl+M, Check VirusTotal.
- Metrics:** CPU Usage: 1.50%, Commit Charge: 79.40%, Processes: 212, Physical Usage: 83.01%.

This displays the DLL properties in images and strings tabs.

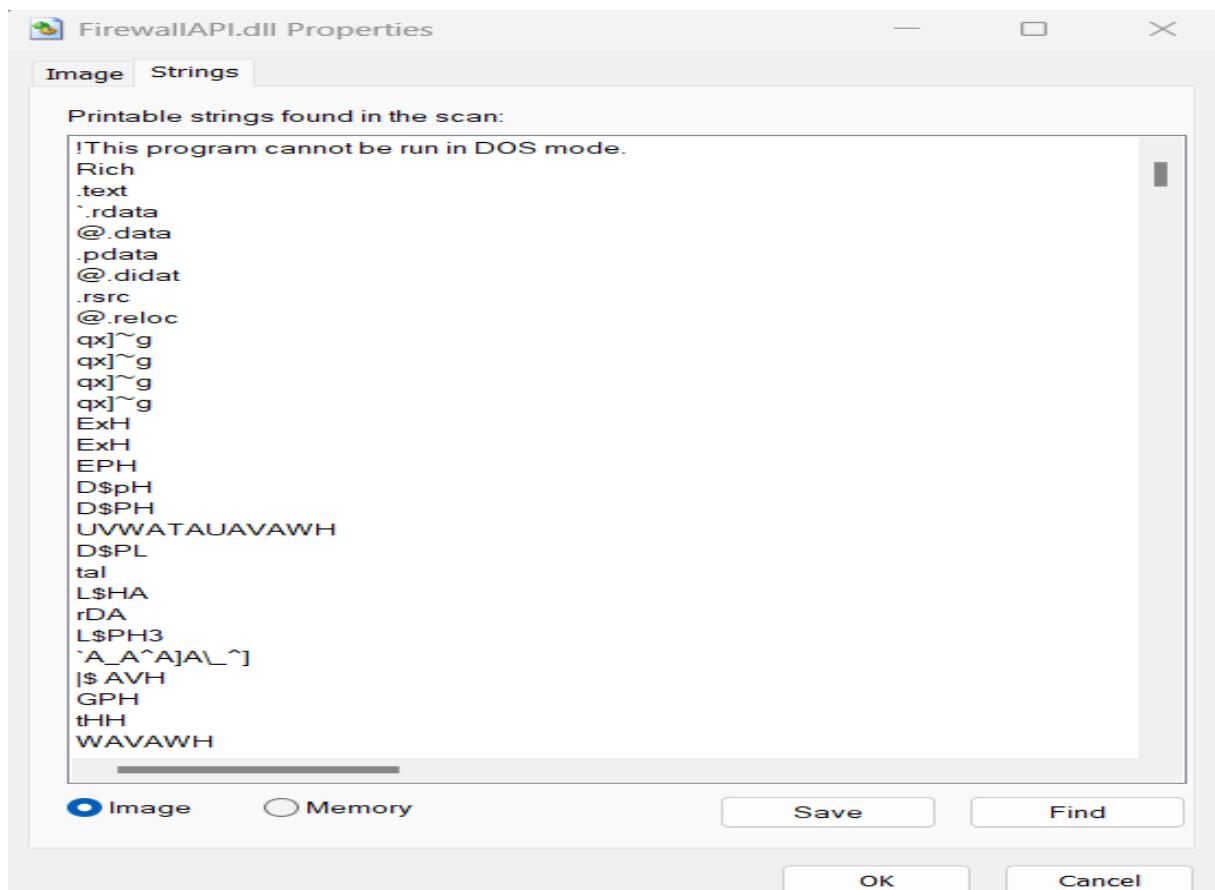
The image tab contains details of the DLL such as Company name, version path of DLL etc.



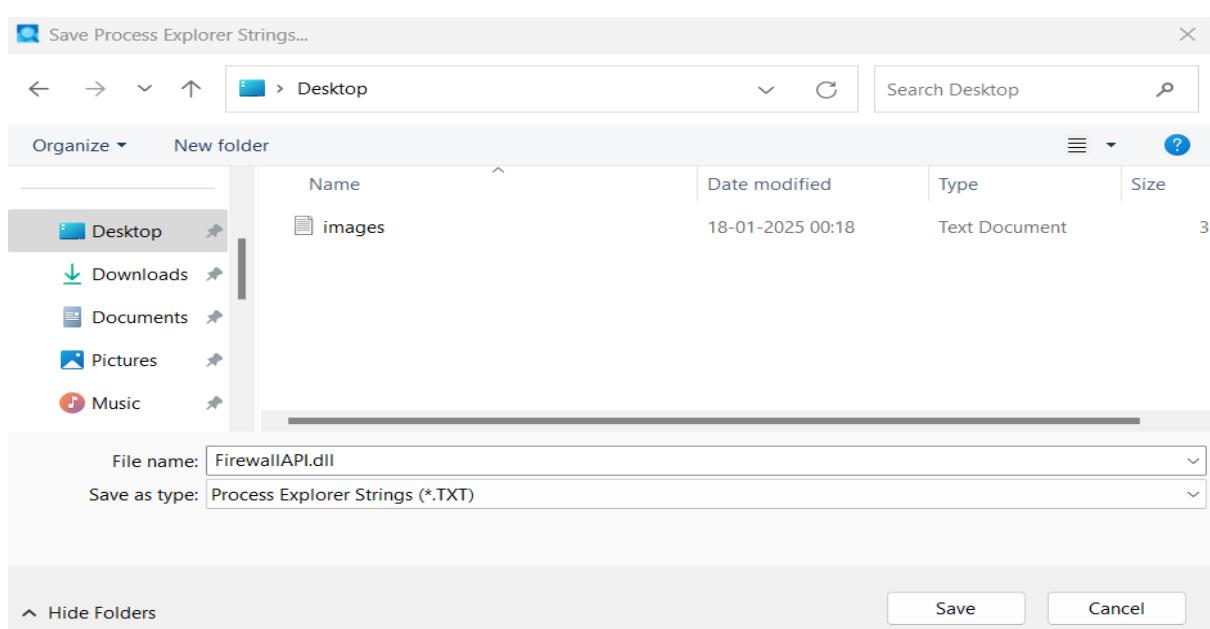
Click verify button to check for signature of a process. Here the Company's name appears to be Microsoft Windows so the process is said to be legitimate.



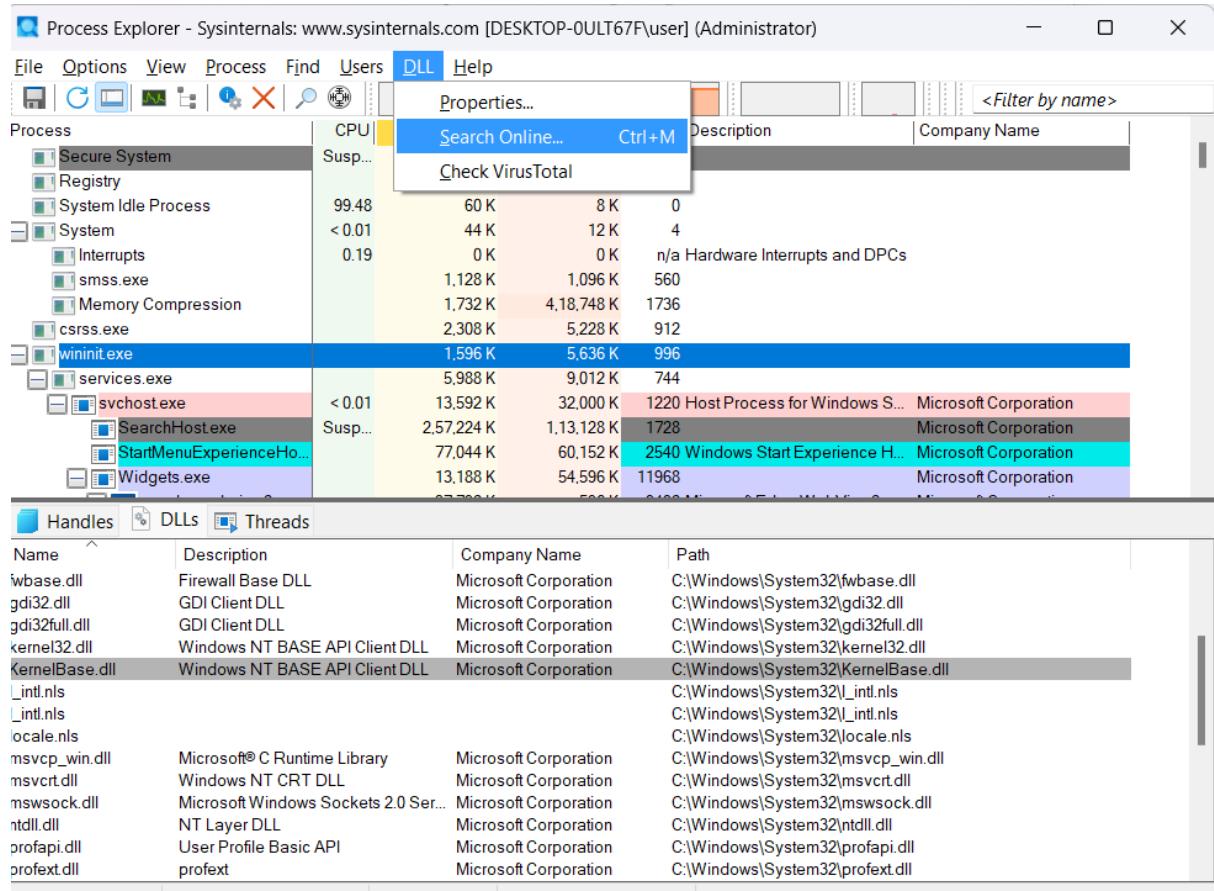
By clicking the string tab it lists any Unicode Strings found in the selected process. Examining this helps to find if the process is associated with any malware.



We can save image or memory string in text format



The search online option searches the selected DLL on the internet by launching an Internet Browser.



Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-0ULT67F\user] (Administrator)

**DLL** Help

File Options View Process Find Users **DLL** Help

Process CPU Susp... Description Company Name

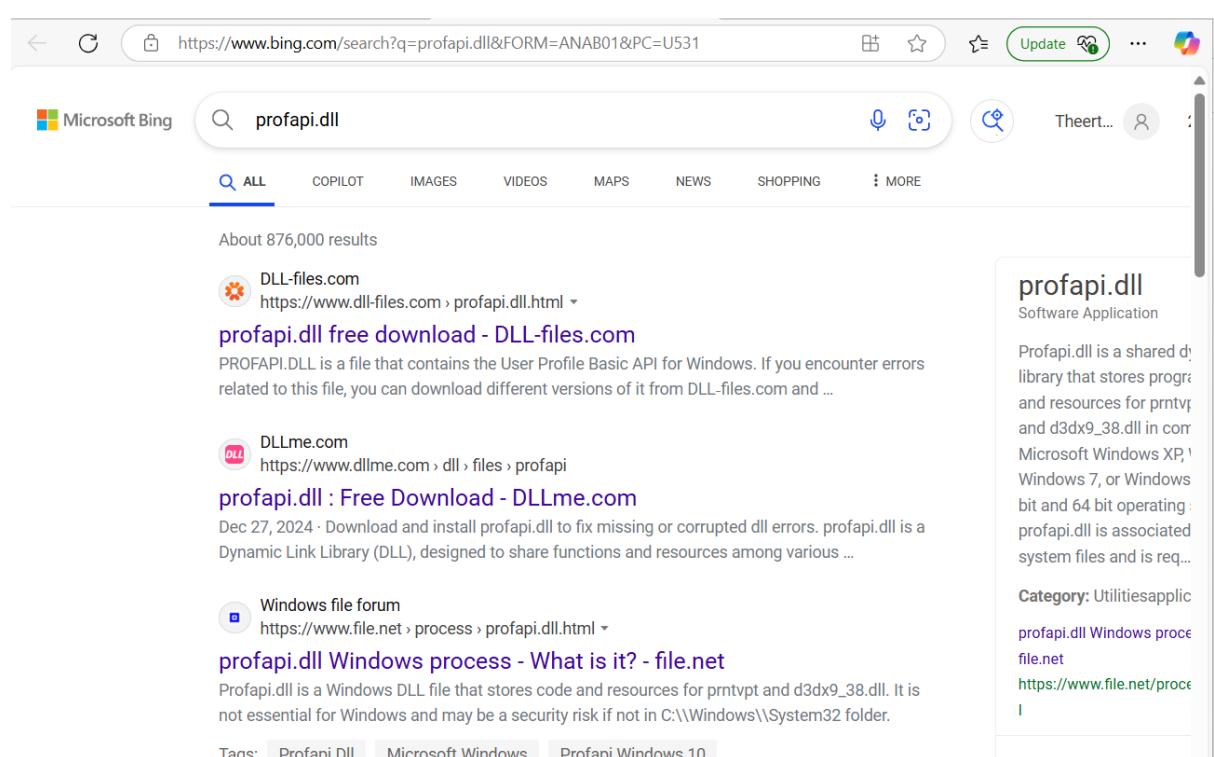
Secure System Registry System Idle Process System

Interruptions smss.exe Memory Compression csrss.exe wininit.exe services.exe svchost.exe SearchHost.exe StartMenuExperienceHo... Widgets.exe

Properties... Search Online... Ctrl+M Check VirusTotal

Name	Description	Company Name	Path
fwbase.dll	Firewall Base DLL	Microsoft Corporation	C:\Windows\System32\fwbase.dll
gdi32.dll	GDI Client DLL	Microsoft Corporation	C:\Windows\System32\gdi32.dll
gdi32full.dll	GDI Client DLL	Microsoft Corporation	C:\Windows\System32\gdi32full.dll
kernel32.dll	Windows NT BASE API Client DLL	Microsoft Corporation	C:\Windows\System32\kernel32.dll
<b>KernelBase.dll</b>	<b>Windows NT BASE API Client DLL</b>	<b>Microsoft Corporation</b>	<b>C:\Windows\System32\KernelBase.dll</b>
_intl.nls			C:\Windows\System32\_intl.nls
_intl.nls			C:\Windows\System32\_intl.nls
locale.nls			C:\Windows\System32\locale.nls
msvcp_win.dll	Microsoft® C Runtime Library	Microsoft Corporation	C:\Windows\System32\msvcp_win.dll
msvcr.dll	Windows NT CRT DLL	Microsoft Corporation	C:\Windows\System32\msvcr.dll
mswsock.dll	Microsoft Windows Sockets 2.0 Ser...	Microsoft Corporation	C:\Windows\System32\mswsock.dll
ntdll.dll	NT Layer DLL	Microsoft Corporation	C:\Windows\System32\ntdll.dll
profapi.dll	User Profile Basic API	Microsoft Corporation	C:\Windows\System32\profapi.dll
profext.dll	profext	Microsoft Corporation	C:\Windows\System32\profext.dll

CPU Usage: 0.94% Commit Charge: 79.40% Processes: 211 Physical Usage: 83.74%



Microsoft Bing

https://www.bing.com/search?q=profapi.dll&FORM=ANAB01&PC=U531

profapi.dll

ALL COPILOT IMAGES VIDEOS MAPS NEWS SHOPPING MORE

About 876,000 results

**DLL-files.com**  
https://www.dll-files.com › profapi.dll.html

**profapi.dll free download - DLL-files.com**

PROFAPI.DLL is a file that contains the User Profile Basic API for Windows. If you encounter errors related to this file, you can download different versions of it from DLL-files.com and ...

**DLLme.com**  
https://www.dllme.com › dll › files › profapi

**profapi.dll : Free Download - DLLme.com**

Dec 27, 2024 · Download and install profapi.dll to fix missing or corrupted dll errors. profapi.dll is a Dynamic Link Library (DLL), designed to share functions and resources among various ...

**Windows file forum**  
https://www.file.net › process › profapi.dll.html

**profapi.dll Windows process - What is it? - file.net**

Profapi.dll is a Windows DLL file that stores code and resources for prntvpt and d3dx9\_38.dll. It is not essential for Windows and may be a security risk if not in C:\Windows\System32 folder.

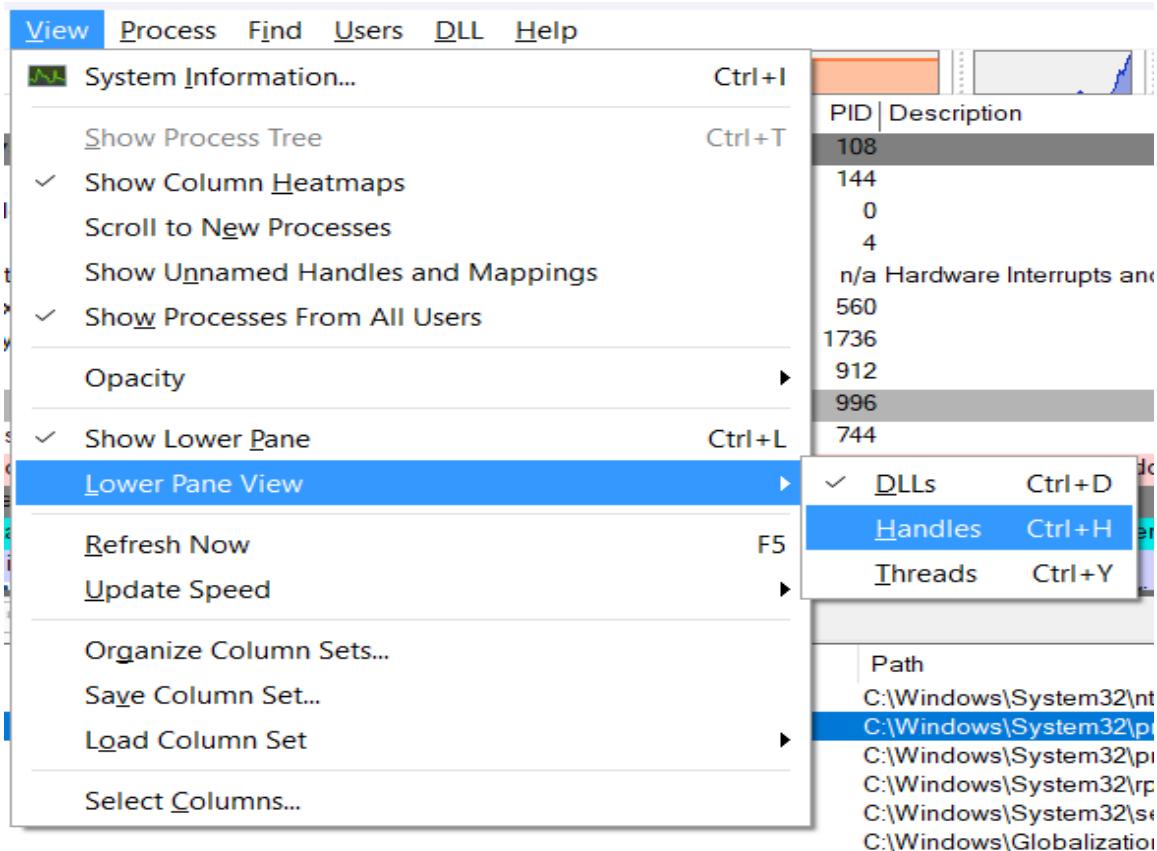
Tags: Profapi.Dll Microsoft Windows Profapi Windows 10

**profapi.dll**  
Software Application

Profapi.dll is a shared DLL library that stores program and resources for prntvpt and d3dx9\_38.dll in core Microsoft Windows XP, Windows 7, or Windows 10 bit and 64 bit operating systems. profapi.dll is associated with system files and is required by several applications.

**Category:** Utilities applications  
**profapi.dll Windows processes:** file.net  
<https://www.file.net/processes/profapi.dll>

To view the handles of particular process click view ->Lower pane view->Handles



The screenshot shows the main Process Explorer window. The 'Handles' tab is selected in the bottom navigation bar. The main pane displays a list of handles with columns for Type, Name, and various performance metrics like CPU, Private Bytes, Working Set, PID, Description, and Company Name. The 'Handles' tab is also highlighted in the bottom navigation bar.

Type	Name
ALPC Port	\RPC Control\WMsgKRpc0E5610
ALPC Port	\RPC Control\WindowsShutdown
Desktop	\Winlogon
Desktop	\Disconnect
Desktop	\Default
Directory	\BaseNamedObjects
Directory	\GLOBAL??
Directory	\GLOBAL??
Event	\BaseNamedObjects\TermSrvReadyEvent
Event	\BaseNamedObjects\FirstWinlogonCheck
Event	\BaseNamedObjects\WinlogonLogoff
Event	\BaseNamedObjects\UMSServicesStarted
Event	\LSA\_ISO\_READY
File	C:\Windows\System32

To close handle right click handle and close.

Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-0ULT67F\user] (Administrator)

File Options View Process Find Users Handle Help

**Close Handle**

Process	CPU	Properties...	PID	Description	Company Name
Secure System	Susp...	104 K	56,284 K	108	144
Registry		7,192 K			
System Idle Process	100.00	60 K	8 K	0	
System	< 0.01	44 K	12 K	4	
Interrupts		0 K	0 K	n/a	Hardware Interrupts and DPCs
smss.exe		1,128 K	1,096 K	560	
Memory Compression		1,740 K	4,24,928 K	1736	
csrss.exe		2,308 K	5,224 K	912	
wininit.exe		1,596 K	5,636 K	996	
services.exe		5,736 K	8,904 K	744	
svchost.exe	< 0.01	13,864 K	32,136 K	1220	Host Process for Windows S...
SearchHost.exe	Susp...	2,57,224 K	1,13,116 K	1728	Microsoft Corporation
StarMenuExperienceHo...		77,016 K	60,180 K	2540	Windows Start Experience H...
Widgets.exe		13,004 K	54,568 K	11968	Microsoft Corporation

Handles DLLs Threads

Type Name

- ALPC Port \RPC Control\WMsgKRpc0E5610
- ALPC Port \RPC Control\WindowsShutdown
- Desktop \Winlogon
- Desktop \Disconnect
- Desktop \Default
- Directory \BaseNamedObjects
- Directory \GLOBAL??
- Directory \IGI ORAI ??

### Process Explorer Warning



Forcing a handle closed can lead to an application crash and system instability.

Continue with close?

Yes

No

DLLs Handles Threads

Type Name

- File C:\Windows
- File \Device\NamedPipe
- File \Device\Mailslot
- File \Device\NamedPipe
- File \Device\NamedPipe
- File \Device\Mailslot
- File \Device\Mailslot
- File \Device\NamedPipe
- File \Device\Mailslot

File Properties... Session Manager\Memory Management

Key Search Online... Ctrl+M

Process Check VirusTotal

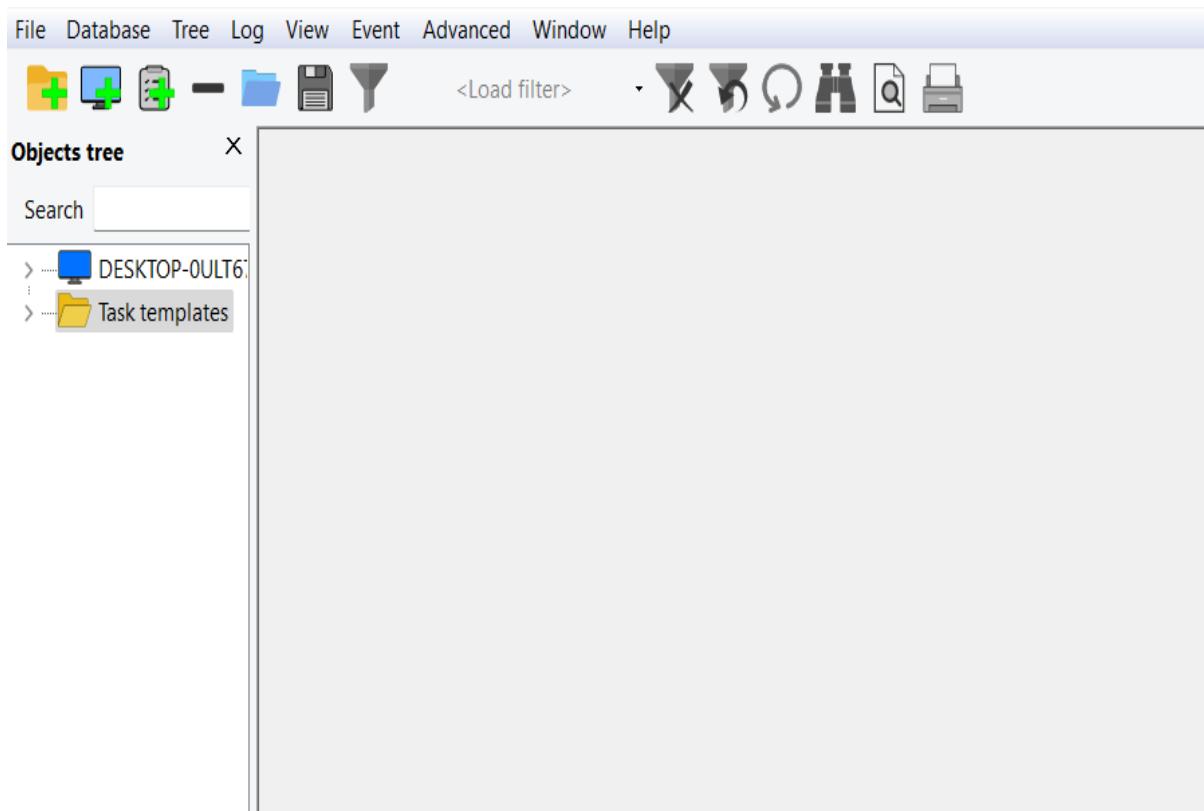
CPU Usage: 1.67% Commit Charge: 82.34% Processes: 209 Physical Usage: 92.84%

## **LAB-3: Viewing, Monitoring, and Analyzing Events Using the Event Log Explorer Tool**

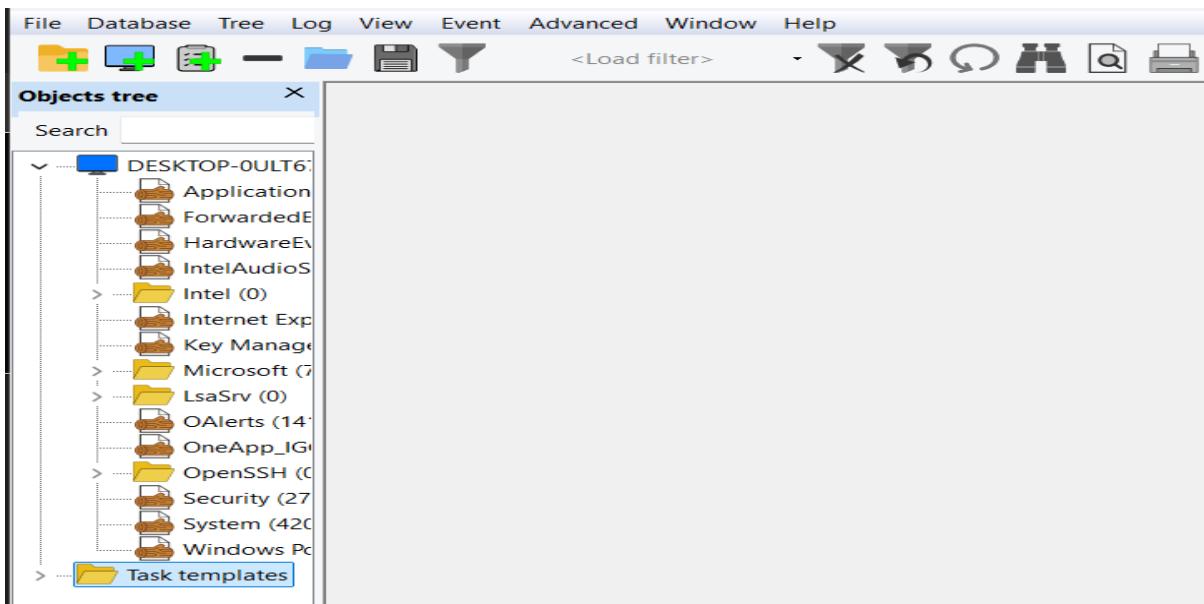
The objective of this lab is to help forensic investigators learn how to view, monitor, and analyze various events. Here we monitor and analyze:

- I. Security logs
- II. System logs
- III. Application logs
- IV. Other logs of Microsoft Windows OS.

Event Log Explorer main window appears, displaying an empty log view area and object area pane with windows server virtual machine's computer name.



By clicking arrow in the leftside we can see all available event logs.



By double clicking Application in the object tree pane we can see application events.

Type	Date	Time	Event	Source	Category	User	Computer
Information	20-01-2025	22:37:12	16394	Microsoft-Windows None	N/A		DESKTOP-0ULT67F
Information	20-01-2025	22:36:42	16384	Microsoft-Windows None	N/A		DESKTOP-0ULT67F
Information	20-01-2025	22:36:11	16394	Microsoft-Windows None	N/A		DESKTOP-0ULT67F
Information	20-01-2025	22:35:41	16384	Microsoft-Windows None	N/A		DESKTOP-0ULT67F
Information	20-01-2025	22:35:11	16394	Microsoft-Windows None	N/A		DESKTOP-0ULT67F
Information	20-01-2025	22:34:40	16384	Microsoft-Windows None	N/A		DESKTOP-0ULT67F
Information	20-01-2025	22:34:09	16394	Microsoft-Windows None	N/A		DESKTOP-0ULT67F
Information	20-01-2025	22:33:38	16384	Microsoft-Windows None	N/A		DESKTOP-0ULT67F
Information	20-01-2025	22:33:08	16394	Microsoft-Windows None	N/A		DESKTOP-0ULT67F
Information	20-01-2025	22:32:37	16384	Microsoft-Windows None	N/A		DESKTOP-0ULT67F
Information	20-01-2025	22:32:07	16394	Microsoft-Windows None	N/A		DESKTOP-0ULT67F
Information	20-01-2025	22:30:57	16384	Microsoft-Windows None	N/A		DESKTOP-0ULT67F
Information	20-01-2025	22:30:26	16394	Microsoft-Windows None	N/A		DESKTOP-0ULT67F
Information	20-01-2025	22:29:39	16384	Microsoft-Windows None	N/A		DESKTOP-0ULT67F
Information	20-01-2025	22:29:09	16394	Microsoft-Windows None	N/A		DESKTOP-0ULT67F
Information	20-01-2025	22:28:52	326	ESENT	General	N/A	DESKTOP-0ULT67F
Information	20-01-2025	22:28:52	105	ESENT	General	N/A	DESKTOP-0ULT67F
Information	20-01-2025	22:28:52	302	ESENT	Logging/Recovery	N/A	DESKTOP-0ULT67F
Information	20-01-2025	22:28:52	301	ESENT	Logging/Recovery	N/A	DESKTOP-0ULT67F
Information	20-01-2025	22:28:52	301	ESENT	Logging/Recovery	N/A	DESKTOP-0ULT67F
Information	20-01-2025	22:28:52	300	ESENT	Logging/Recovery	N/A	DESKTOP-0ULT67F
Information	20-01-2025	22:28:52	102	ESENT	General	N/A	DESKTOP-0ULT67F

**Description**

Offline downlevel migration succeeded.

Event Log Explorer also displays the events of Applicure DFS Replication, dotDefenderAudit, Hardware Events, Key Management service, OAlerts, Security, System, Windows Powershell.

Selecting any event displays the description of the event in the Description pane at the lower end of the window.

Application on DESKTOP-0ULT67F x

2693 1 UTC+5:30

Type	Date	Time	Event	Source	Category	User	Computer
Information	20-01-2025	22:37:12	16394	Microsoft-Windows	None	N/A	DESKTOP-0ULT67F
Information	20-01-2025	22:36:42	16384	Microsoft-Windows	None	N/A	DESKTOP-0ULT67F
Information	20-01-2025	22:36:11	16394	Microsoft-Windows	None	N/A	DESKTOP-0ULT67F
Information	20-01-2025	22:35:41	16384	Microsoft-Windows	None	N/A	DESKTOP-0ULT67F
Information	20-01-2025	22:35:11	16394	Microsoft-Windows	None	N/A	DESKTOP-0ULT67F
Information	20-01-2025	22:34:40	16384	Microsoft-Windows	None	N/A	DESKTOP-0ULT67F
Information	20-01-2025	22:34:09	16394	Microsoft-Windows	None	N/A	DESKTOP-0ULT67F
Information	20-01-2025	22:33:38	16384	Microsoft-Windows	None	N/A	DESKTOP-0ULT67F
Information	20-01-2025	22:33:08	16394	Microsoft-Windows	None	N/A	DESKTOP-0ULT67F
Information	20-01-2025	22:32:37	16384	Microsoft-Windows	None	N/A	DESKTOP-0ULT67F
Information	20-01-2025	22:32:07	16394	Microsoft-Windows	None	N/A	DESKTOP-0ULT67F
Information	20-01-2025	22:30:57	16384	Microsoft-Windows	None	N/A	DESKTOP-0ULT67F
Information	20-01-2025	22:30:26	16394	Microsoft-Windows	None	N/A	DESKTOP-0ULT67F
Information	20-01-2025	22:29:39	16384	Microsoft-Windows	None	N/A	DESKTOP-0ULT67F
Information	20-01-2025	22:29:09	16394	Microsoft-Windows	None	N/A	DESKTOP-0ULT67F
Information	20-01-2025	22:28:52	326	ESENT	General	N/A	DESKTOP-0ULT67F
Information	20-01-2025	22:28:52	105	ESENT	General	N/A	DESKTOP-0ULT67F
Information	20-01-2025	22:28:52	302	ESENT	Logging/Recovery	N/A	DESKTOP-0ULT67F
Information	20-01-2025	22:28:52	301	ESENT	Logging/Recovery	N/A	DESKTOP-0ULT67F
Information	20-01-2025	22:28:52	301	ESENT	Logging/Recovery	N/A	DESKTOP-0ULT67F
Information	20-01-2025	22:28:52	301	ESENT	Logging/Recovery	N/A	DESKTOP-0ULT67F
Information	20-01-2025	22:28:52	300	ESENT	Logging/Recovery	N/A	DESKTOP-0ULT67F
Information	20-01-2025	22:28:52	102	ESENT	General	N/A	DESKTOP-0ULT67F

**Description**

svchost (10704,D,0) DS\_Token\_DB: The database engine started a new instance (0). (Time=0 seconds)

Additional Data:  
IpposV2[] = 00000015:0006:0000 - 00000015:000E:0F5D - 00000017:0004:0000 - 00000017:0004:0000 (00000000:0000:0000)  
cRelnts = 1  
RBSOn = 0

Description Data

**Filter**

Apply filter to:

Active event log view (Application on DESKTOP-0ULT67F)  
 Event log view(s) on your choice

Event types

Verbose  
 Information  
 Warning  
 Error  
 Critical  
 Audit Success  
 Audit Failure

Source:    Exclude

Category:    Exclude

User:    Exclude

Computer:    Exclude

Event ID(s):   Exclude

Enter ID numbers and/or ID ranges, separated by commas, use exclamation mark to exclude criteria (e.g. 1-19,100,250-450!10,255)

Text in description:

Date  Time  Separately  
From: 20-01-2025  00:00:00  To: 20-01-2025  00:00:00   Exclude

Display event for the last 0  days 0  hours  Exclude

Custom columns Description params

Name	Operator	Value
Custom column 1		
Custom column 2		
Custom column 3		
Custom column 4		
Custom column 5		

Clear  Load...  Save...  Case sensitive  OK  Cancel

To filter the events click the filter icon in the toolbar. It will popup a new filter window. Choose source, category, computer

**Filter**

Apply filter to:

Active event log view (Application on DESKTOP-0ULT67F)  
 Event log view(s) on your choice

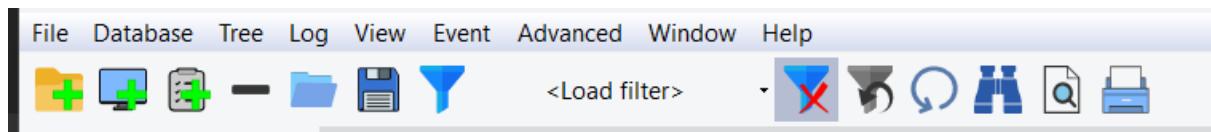
<b>Event types</b> <input checked="" type="checkbox"/> Verbose <input checked="" type="checkbox"/> Information <input checked="" type="checkbox"/> Warning <input checked="" type="checkbox"/> Error <input checked="" type="checkbox"/> Critical <input checked="" type="checkbox"/> Audit Success <input checked="" type="checkbox"/> Audit Failure	<b>Source:</b> ESENT <input type="button" value="..."/> <input type="checkbox"/> Exclude <b>Category:</b> Logging/Recovery <input type="button" value="..."/> <input type="checkbox"/> Exclude <b>User:</b> <input type="button" value="..."/> <input type="checkbox"/> Exclude <b>Computer:</b> DESKTOP-0ULT67F <input type="button" value="..."/> <input type="checkbox"/> Exclude																		
<b>Event ID(s):</b> <input type="text"/> <input type="checkbox"/> Exclude Enter ID numbers and/or ID ranges, separated by commas, use exclamation mark to exclude criteria (e.g. 1-19,100,250-450!10,255)																			
<b>Text in description:</b> <input type="text"/> <input type="checkbox"/> ReqExp <input type="checkbox"/> Exclude <input type="checkbox"/> Date <input type="checkbox"/> Time <input type="checkbox"/> Separately From: <input type="text" value="20-01-2025"/> <input type="button" value="..."/> <input type="text" value="00:00:00"/> <input type="button" value="..."/> To: <input type="text" value="20-01-2025"/> <input type="button" value="..."/> <input type="text" value="00:00:00"/> <input type="button" value="..."/> <input type="checkbox"/> Exclude																			
Display event for the last <input type="text" value="0"/> <input type="button" value="up"/> days <input type="text" value="0"/> <input type="button" value="up"/> hours <input type="checkbox"/> Exclude																			
<b>Custom columns</b> <b>Description params</b> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Name</th> <th>Operator</th> <th>Value</th> </tr> </thead> <tbody> <tr><td>Custom column 1</td><td></td><td></td></tr> <tr><td>Custom column 2</td><td></td><td></td></tr> <tr><td>Custom column 3</td><td></td><td></td></tr> <tr><td>Custom column 4</td><td></td><td></td></tr> <tr><td>Custom column 5</td><td></td><td></td></tr> </tbody> </table>		Name	Operator	Value	Custom column 1			Custom column 2			Custom column 3			Custom column 4			Custom column 5		
Name	Operator	Value																	
Custom column 1																			
Custom column 2																			
Custom column 3																			
Custom column 4																			
Custom column 5																			

Case sensitive

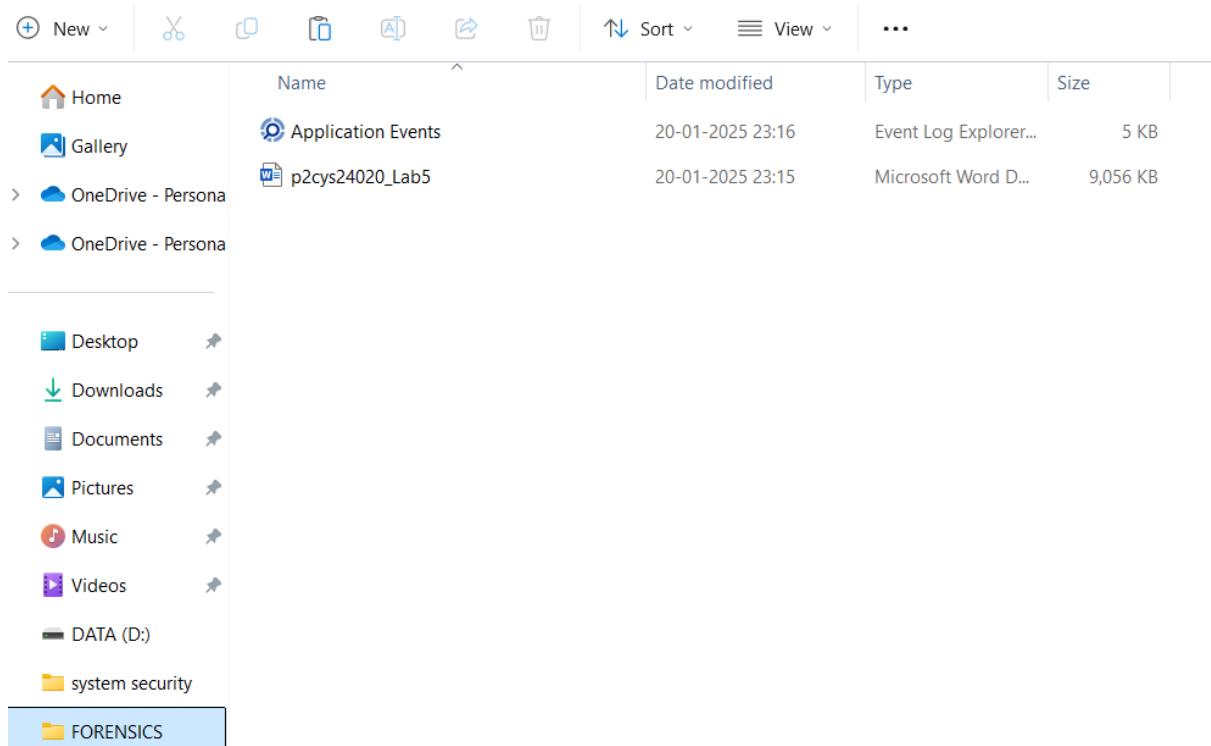
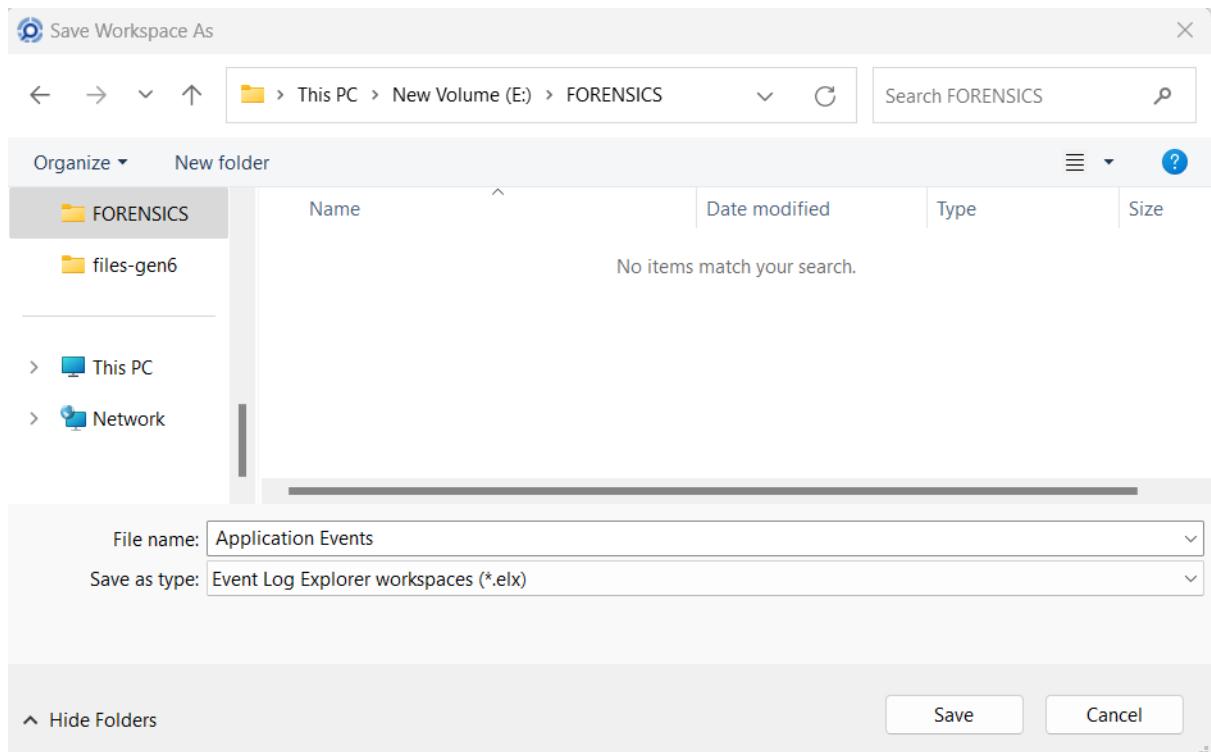
Click ok.

It will display all the events related to that filter.

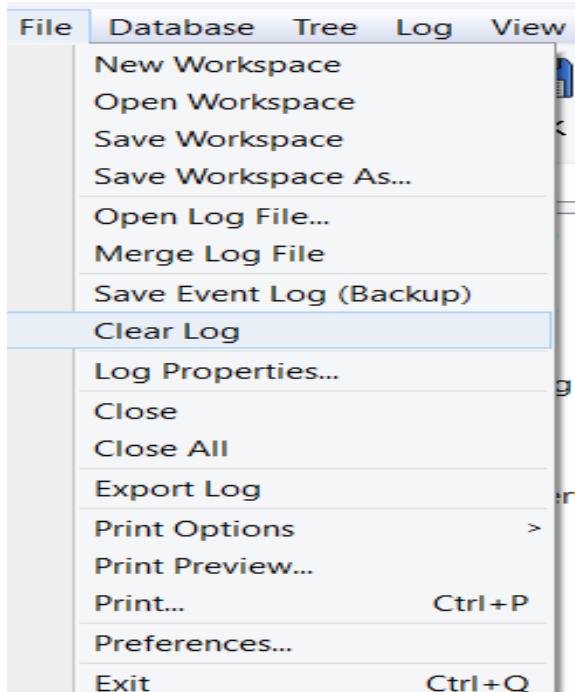
To clear the filter click clear filter icon in the toolbar.



We can save the event logs.



We can clear the logs

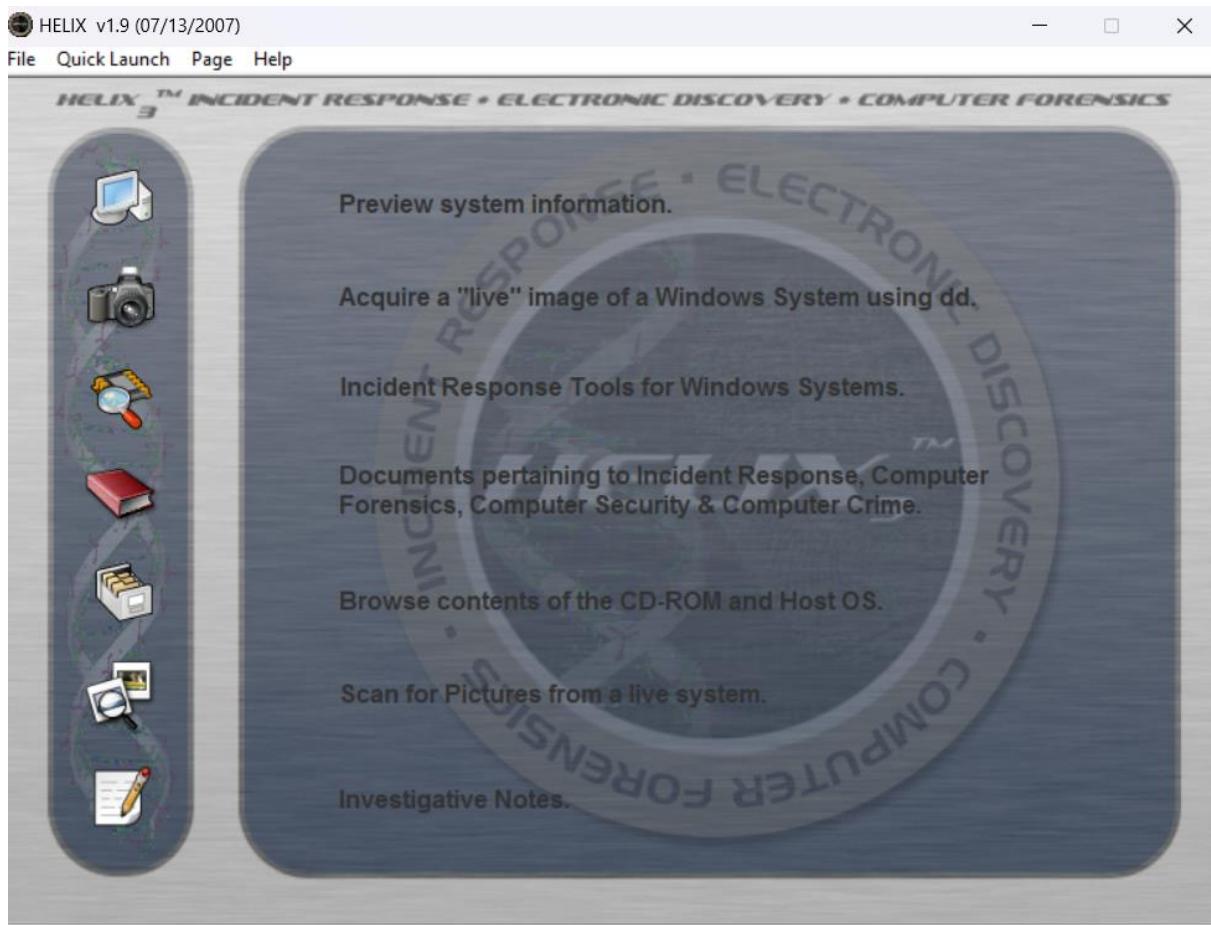


A screenshot of the Windows Event Viewer application. The title bar shows 'File Database Tree Log View Event Advanced Window Help'. The main interface has two panes. The left pane, titled 'Objects tree', shows a tree view of event logs under 'DESKTOP-0ULT67F (local)'. The right pane, titled 'Application on DESKTOP-0ULT67F', displays a table of events. The table columns are: Type, Date, Time, Event, Source, Category, User, and Computer. A single event entry is visible in the table, showing a type of 'Information' (indicated by an 'i' icon). The table header includes filters for 'Type', 'Date', 'Time', 'Event', 'Source', 'Category', 'User', and 'Computer', with 'UTC+5:30' selected for the time zone.

## Lab-4: Performing a Computer Forensic Investigation Using the Helix Tool

Objective: The objective of this lab is to learn how to investigate a computer based crime Using the Helix Tool.





By clicking the system information we can see the full system information. It displays the os information, owner information, network information, drives and the file types.

This screenshot shows the 'System Information' page of the HELIX software. The left sidebar has a highlighted icon for a computer monitor. The main content area is titled 'System Information'. It includes sections for 'Operating System', 'Owner Information', 'Network Information', 'Drive', 'Label', 'Type', and 'Size'.

**Operating System:**

**Owner Information:**

- Owner: user
- Organization:
- Admin: No
- Admin Rights: Yes

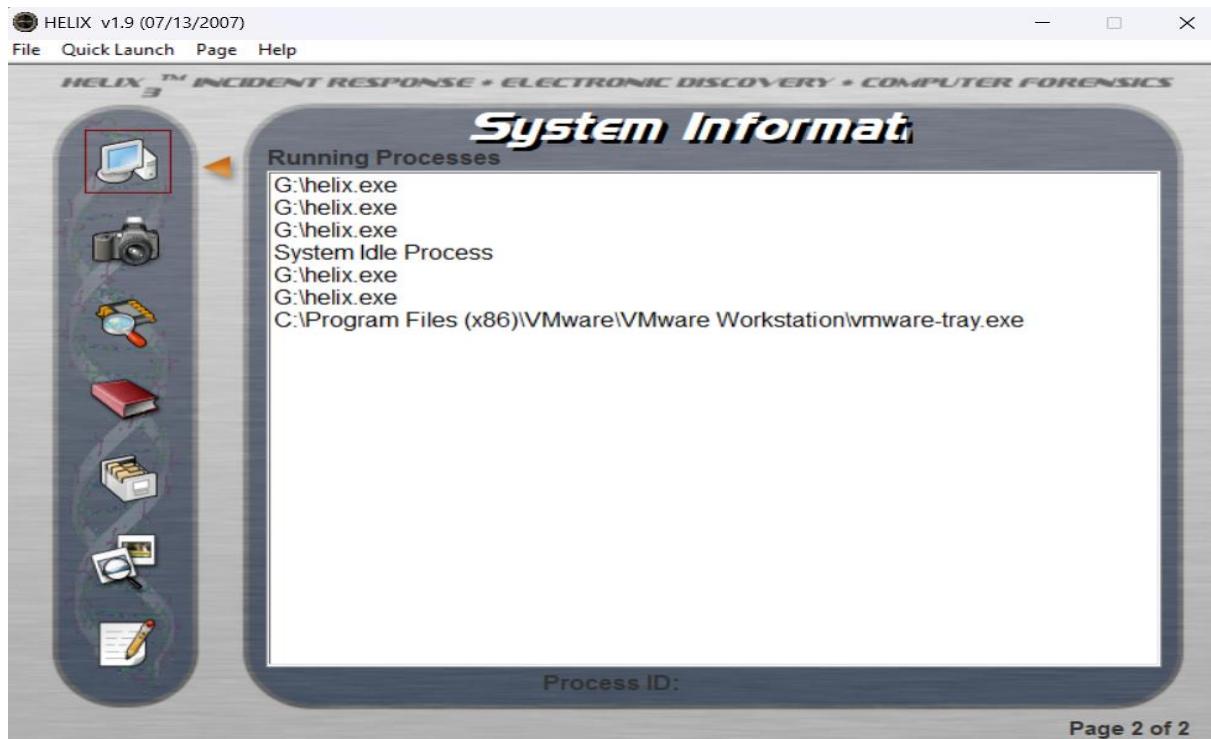
**Network Information:**

- Host: DESKTOP-0ULT67F
- User: user
- IP: 192.168.56.1
- NIC: 005056c00001
- Domain:

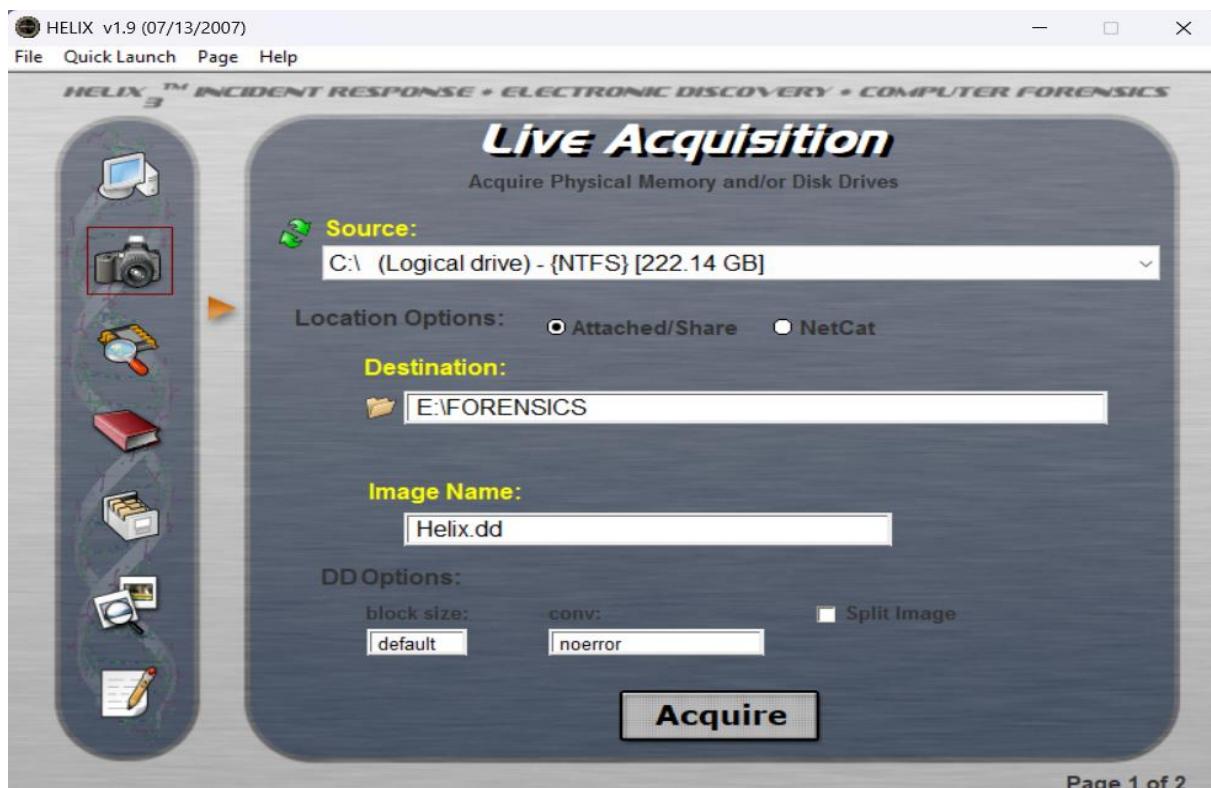
Drive:	Label:	Type:	Size:
C:\	(Logical drive)	NTFS	227474.9 MB
D:\	(Logical drive)	NTFS	451921.9 MB
E:\	(Logical drive)	NTFS	399416.9 MB
F:\	(Logical drive)	NTFS	51199.9 MB
G:\	(Logical drive)	CDFS	700.6 MB

Page 1 of 2

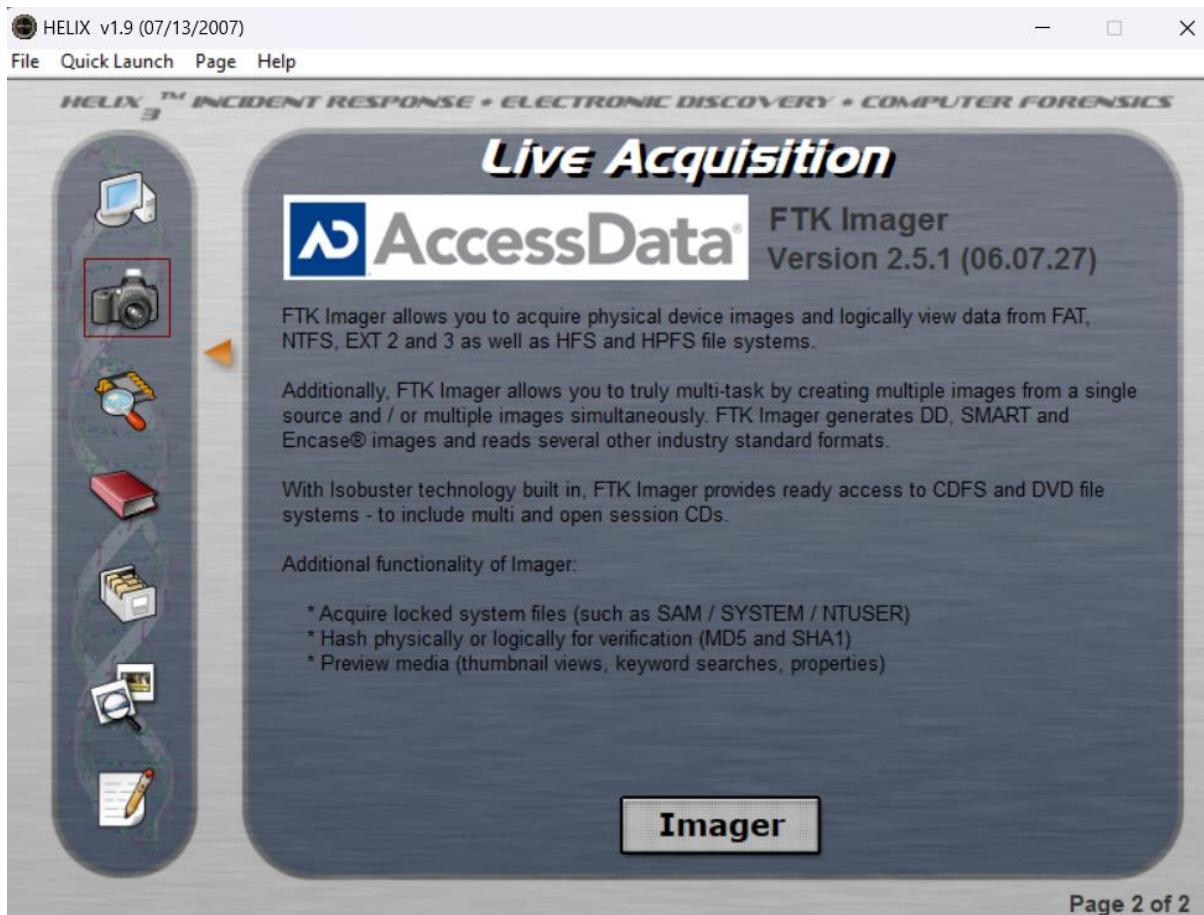
By clicking that yellow arrow in front of system symbol we can see all the process running in our system.



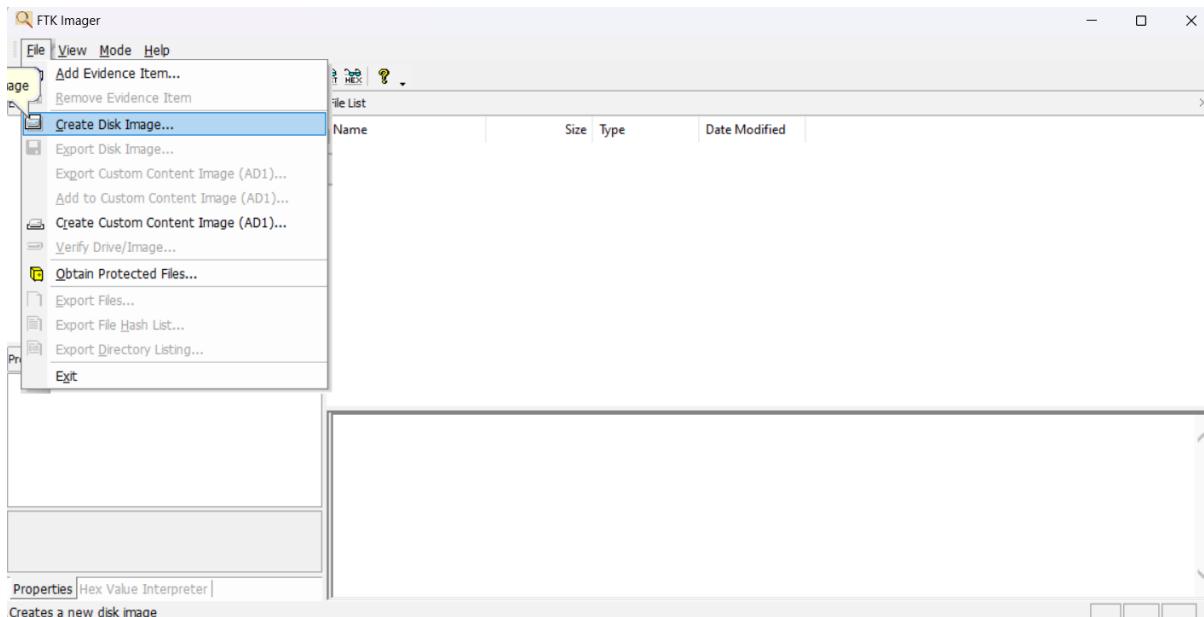
Click the acquisition icon to acquire physical memory or disk drives.



To create an image of a folder with the help of AccessData FTK Imager  
Click imager.



Page 2 of 2



Choose contents of a folder as evidence type. And then click next to create an image.

## Select Source



Please Select the Source Evidence Type

- Physical Drive
- Logical Drive
- Image File
- Contents of a folder  
(logical file-level analysis only; excludes deleted, unallocated, etc.)
- Femico Device (CD/DVD)

< Back

Next >

Cancel

Help

## FTK Imager



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, they are not supported by the current version of FTK. Logical image support will be added to FTK in a future release.

Do you want to continue?

Yes

No

## Select File



Evidence Source Selection

Please enter the source path:

C:\Users\user\Downloads\files-gen6

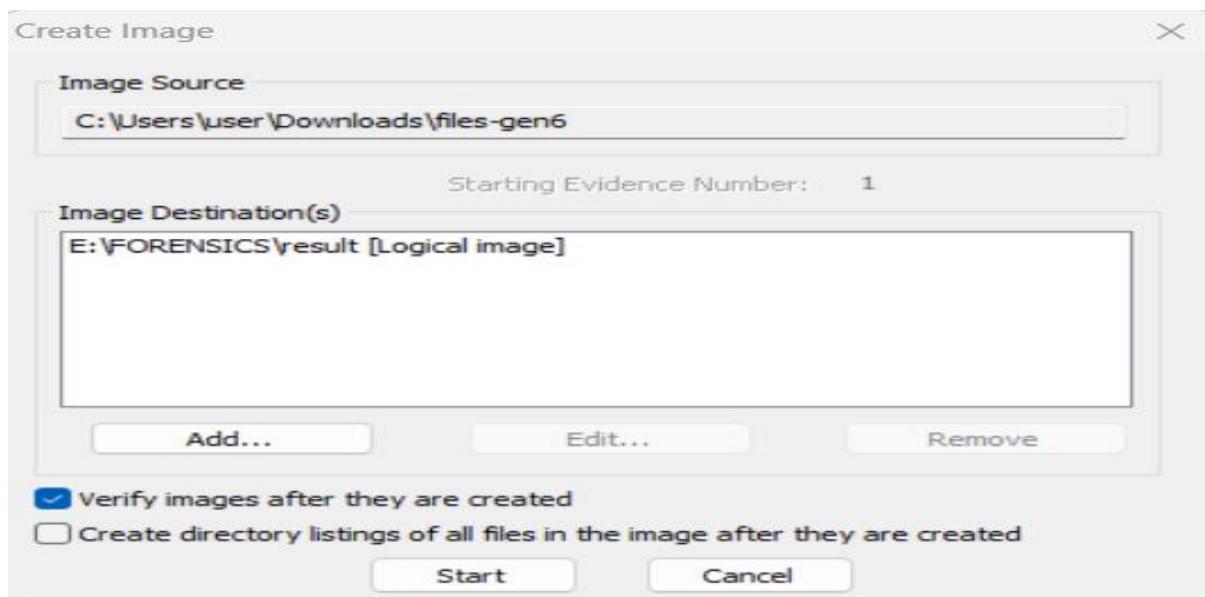
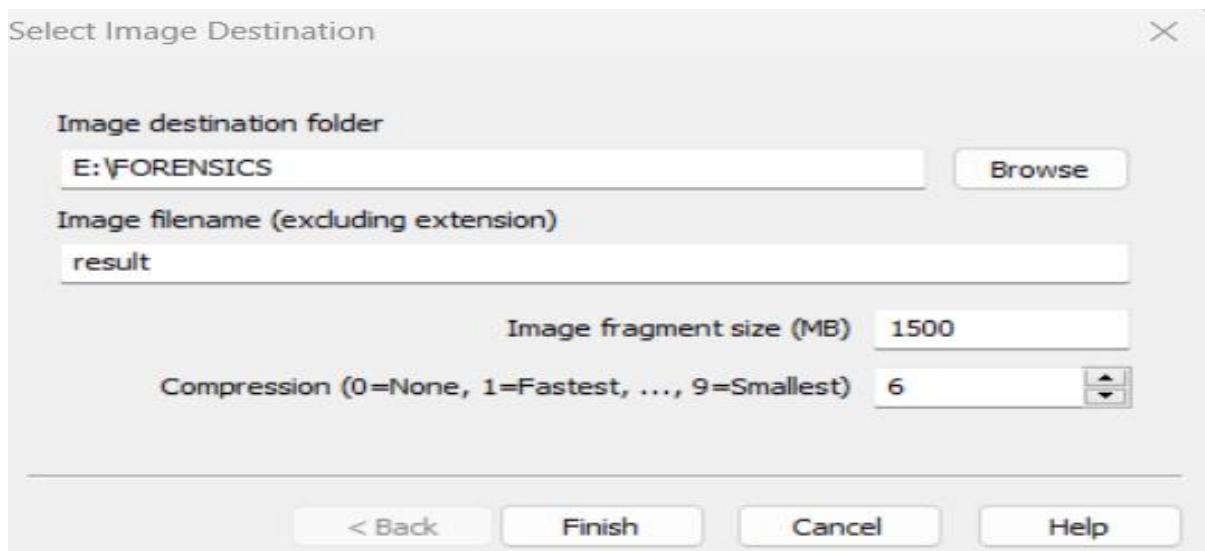
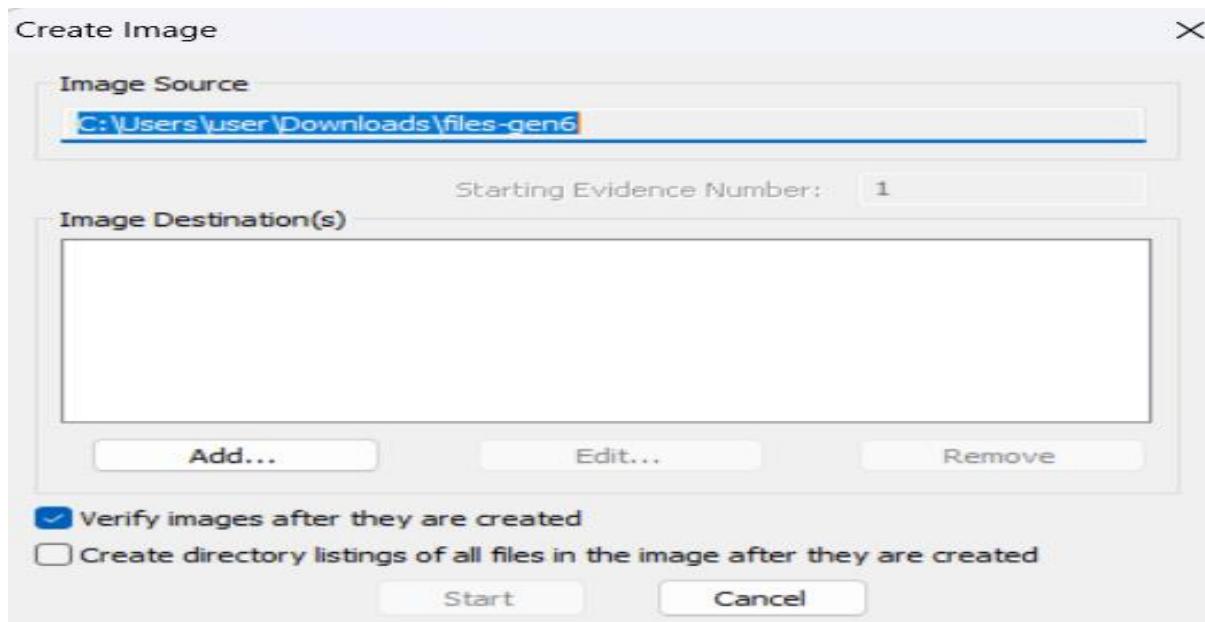
Browse

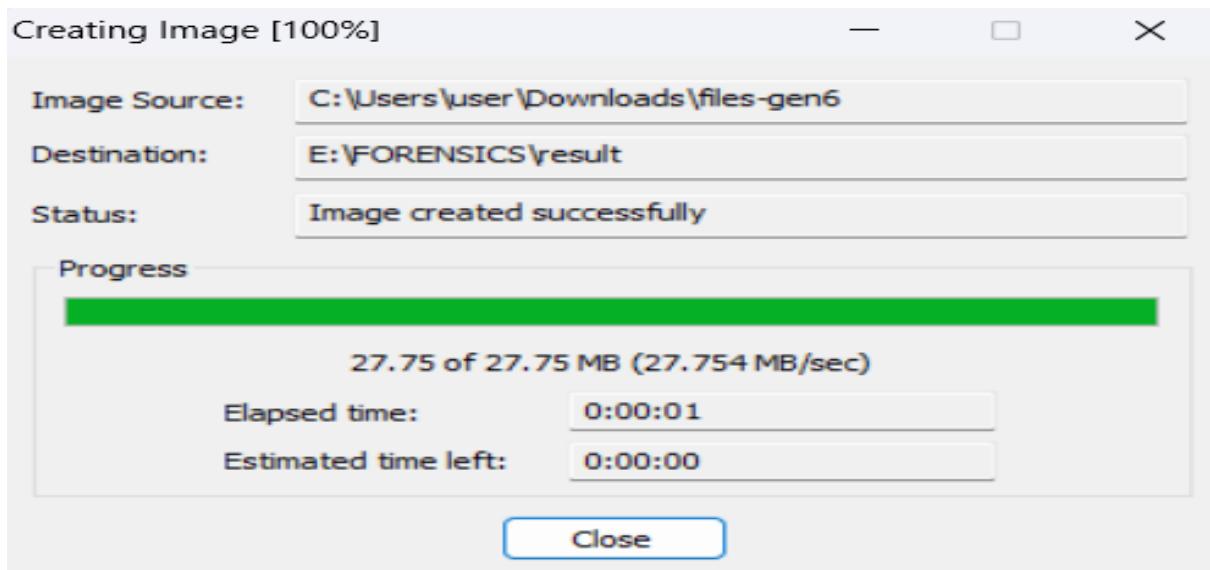
< Back

Finish

Cancel

Help





← → ↑ ↓ ⌂ > This PC > New Volume (E:) > FORENSICS

Name	Date modified	Type	Size
Application Events	20-01-2025 23:16	Event Log Explorer...	5 KB
p2cys24020_Lab5	21-01-2025 10:26	Microsoft Word D...	13,663 KB
result.ad1	21-01-2025 10:25	AD1 File	28,280 KB
result	21-01-2025 10:25	Text Document	4 KB

FTK Imager

Add Evidence Item... (Adds evidence from disk, image file, or folder)

- Create Disk Image...
- Export Disk Image...
- Export Custom Content Image (AD1)...
- Add to Custom Content Image (AD1)...
- Create Custom Content Image (AD1)...
- Verify Drive/Image...
- Obtain Protected Files...
- Export Files...
- Export File Hash List...
- Export Directory Listing...
- Exit

Properties Hex Value Interpreter

Adds evidence from disk, image file, or folder

This screenshot shows the FTK Imager application interface. At the top, there's a navigation bar with icons for back, forward, up, and down, followed by "This PC", "New Volume (E:)", and "FORENSICS". Below the navigation bar is a file explorer window displaying a list of files. The files listed are "Application Events" (Event Log Explorer..., 5 KB), "p2cys24020\_Lab5" (Microsoft Word D..., 13,663 KB), "result.ad1" (AD1 File, 28,280 KB), and "result" (Text Document, 4 KB). The "result.ad1" file is selected. On the left side, there's a sidebar with a tree view showing "OneDrive - Personal", "Desktop", "Downloads", "Documents", and "Pictures". The main menu on the left includes "File", "View", "Mode", and "Help". The "File" menu is expanded, showing options like "Add Evidence Item...", "Create Disk Image...", "Export Disk Image...", "Export Custom Content Image (AD1)...", "Add to Custom Content Image (AD1)...", "Create Custom Content Image (AD1)...", "Verify Drive/Image...", "Obtain Protected Files...", "Export Files...", "Export File Hash List...", "Export Directory Listing...", and "Exit". A tooltip for "Add Evidence Item..." says "(Adds evidence from disk, image file, or folder)". At the bottom, there are tabs for "Properties" and "Hex Value Interpreter", and a status bar message "Adds evidence from disk, image file, or folder".

Select Source X

Please Select the Source Evidence Type

Physical Drive  
 Logical Drive  
 Image File  
 Contents of a folder  
(logical file-level analysis only; excludes deleted, unallocated, etc.)

---

[< Back](#) [Next >](#) [Cancel](#) [Help](#)

Select File X

Evidence Source Selection

Please enter the source path:

C:\Users\user\Downloads\ntfs-img-kw-1.dd

[Browse](#)

---

[< Back](#) [Finish](#) [Cancel](#) [Help](#)

FTK Imager

File View Mode Help

Evidence Tree

- ntfs-img-kw-1.dd
  - KW-SRCH-1 [NTFS]
    - [root]
    - unallocated space
    - orphan

File List

Name	Size	Type	Date Modified
\$Extend	1 KB	Directory	23-10-2003 17:...
dir-n-6	1 KB	Directory	23-10-2003 17:...
dir-r-4	1 KB	Directory	23-10-2003 17:...
System Volume Infor...	1 KB	Directory	24-10-2003 16:...
\$AttrDef	3 KB	Regular file	23-10-2003 17:...
\$BadClus	0 KB	Regular file	23-10-2003 17:...
\$Bitmap	2 KB	Regular file	23-10-2003 17:...
\$Boot	8 KB	Regular file	23-10-2003 17:...
\$I30	4 KB	NTFS index all...	24-10-2003 16:...
\$LogFile	2,048 KB	Regular file	23-10-2003 17:...
\$MFT	39 KB	Regular file	23-10-2003 17:...
\$MFTMirr	4 KB	Regular file	23-10-2003 17:...
\$Secure	1 KB	Regular file	23-10-2003 17:...

Hex Editor View

```

00 30 00 00 00 01 00 00 00-00 10 00 00 08 00 00 00 | 0 ..... .
10 10 00 00 00 28 00 00 00-28 00 00 00 01 00 00 00 | .....{ - - - .
20 00 00 00 00 00 00 00 00-18 00 00 00 03 00 00 00 | ..... .
30 00 00 00 00 00 00 00 00-00-00-00-00-00-00-00-00 | ..... .

```

Cursor pos = 0

For Help, press F1

FTK Imager

File View Mode Help

Evidence Tree

- ntfs-img-kw-1.dd
  - KW-SRCH-1 [NTFS]
    - [root]
      - \$BadClus
      - \$Extend
      - \$Secure
      - dir-n-6
      - dir-r-4
      - file-n-5.dat
      - file-n-3.dat
    - System Volume Information
      - \_restore(A25F48CA-6632-4143-8EF8-)
      - unallocated space
      - orphan

File List

Name	Size	Type	Date Modified
\$ObjId	1 KB	Regular file	23-10-2003 17:...
\$Quota	1 KB	Regular file	23-10-2003 17:...
\$Reparse	1 KB	Regular file	23-10-2003 17:...

Hex Editor View

```

000 30 00 00 00 01 00 00 00-00 10 00 00 08 00 00 00 | 0 ..... .
010 10 00 00 00 48 01 00 00-48 01 00 00 00 00 00 00 | 0 .. H .. H .. .
020 19 00 00 00 00 01 00-60 00 4e 00 00 00 00 00 00 | ..... N .. .
030 0b 00 00 00 00 0b 00-40 c0 b4 ed 88 99 c3 01 | ..... @À i .. À ..
040 40 c0 b4 ed 88 99 c3 01-40 c0 b4 ed 88 99 c3 01 | @À i .. À @À i .. À ..
050 40 c0 b4 ed 88 99 c3 01-00 00 00 00 00 00 00 00 | @À i .. À .. .
060 00 00 00 00 00 00 00-26 00 00 20 00 00 00 00 00 | ..... g .. .
070 06 03 24 00 4f 00 62 00-6a 00 49 00 64 00 00 00 | .. $ .. o .. b .. j .. I .. d .. .
080 18 00 00 00 00 00 85 2f-60 00 4e 00 00 00 00 00 | ..... / .. N .. .
090 0b 00 00 00 00 0b 00-40 c0 b4 ed 88 99 c3 01 | ..... @À i .. À ..
0a0 40 c0 b4 ed 88 99 c3 01-40 c0 b4 ed 88 99 c3 01 | @À i .. À @À i .. À ..
0b0 40 c0 b4 ed 88 99 c3 01-00 00 00 00 00 00 00 00 | @À i .. À .. .
0c0 00 00 00 00 00 00 00-26 00 00 20 00 00 00 00 00 | ..... g .. .
0d0 06 03 24 00 51 00 75 00-6f 00 74 00 61 00 00 00 | .. $ .. Q .. u .. o .. t .. a ..

```

Cursor pos = 0

For Help, press F1

Properties of the image file can be viewed by clicking the properties tab.

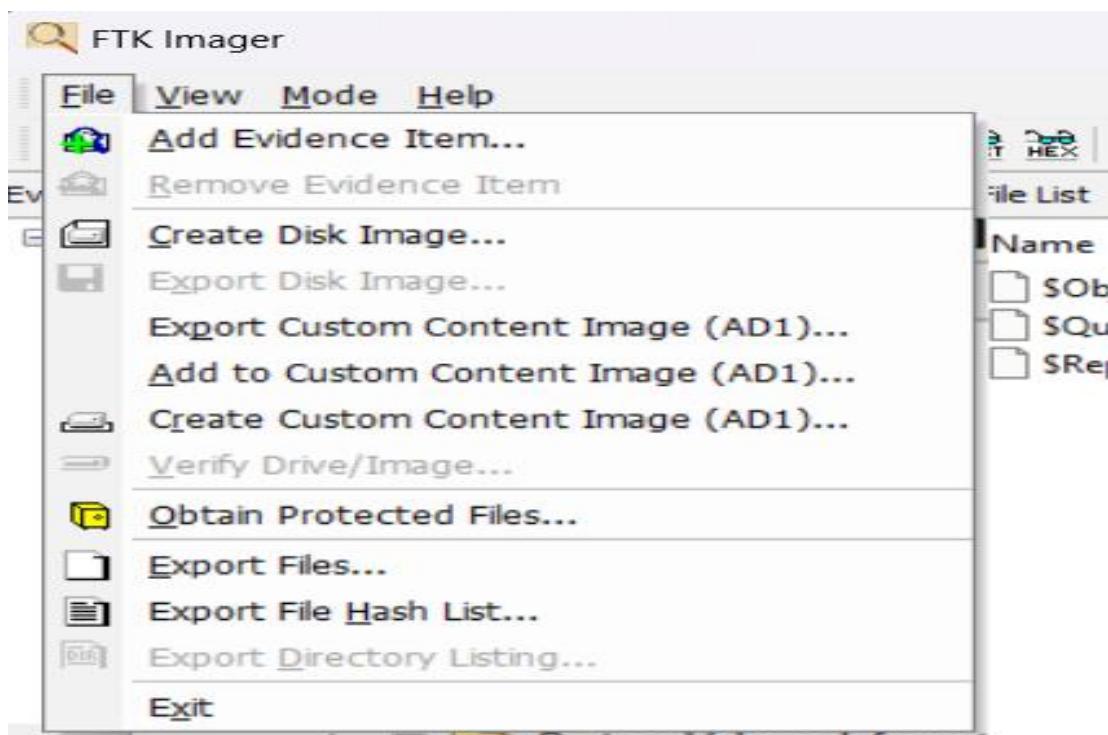
The screenshot shows the FTK Imager interface. On the left, a 'Properties' dialog box is open, showing details for a file named '\$Extend'. The 'General' tab is selected, displaying the following information:

Name	\$Extend
File Class	Directory
File Size	344
Physical Size	344
Date Accessed	23-10-2003 17:12:59
Date Created	23-10-2003 17:12:59
Date Modified	23-10-2003 17:12:59

To the right of the properties dialog is a hex dump of the file's content. The dump shows bytes from 000 to 0d0, with values such as 30 00 00 00 01 00 00. A cursor position indicator at the bottom right of the dump area shows 'Cursor pos = 0'.

For Help, press F1

Now exit the ftk imager by clicking exit in file menu



## Incident Response



Windows Forensic Toolchest (WFT)



First Responder Utility (FRU)



Incident Response Collection Report (IRCR2)



Agile Risk Management's Nigilant32



Start a NetCat Listener

Nigilant32 is based on filesystem forensics code provided by the Sleuthkit Project ([www.sleuthkit.org](http://www.sleuthkit.org)), however, unlike its predecessor, Nigilant32 is a gui based application. In addition, Nigilant32 contains features that allow the user to collect volatile system information in the event of a computer security incident.

Page 1 of 3

Notice



You are about to run:  
The Nigilant32 program from Agile Risk Management

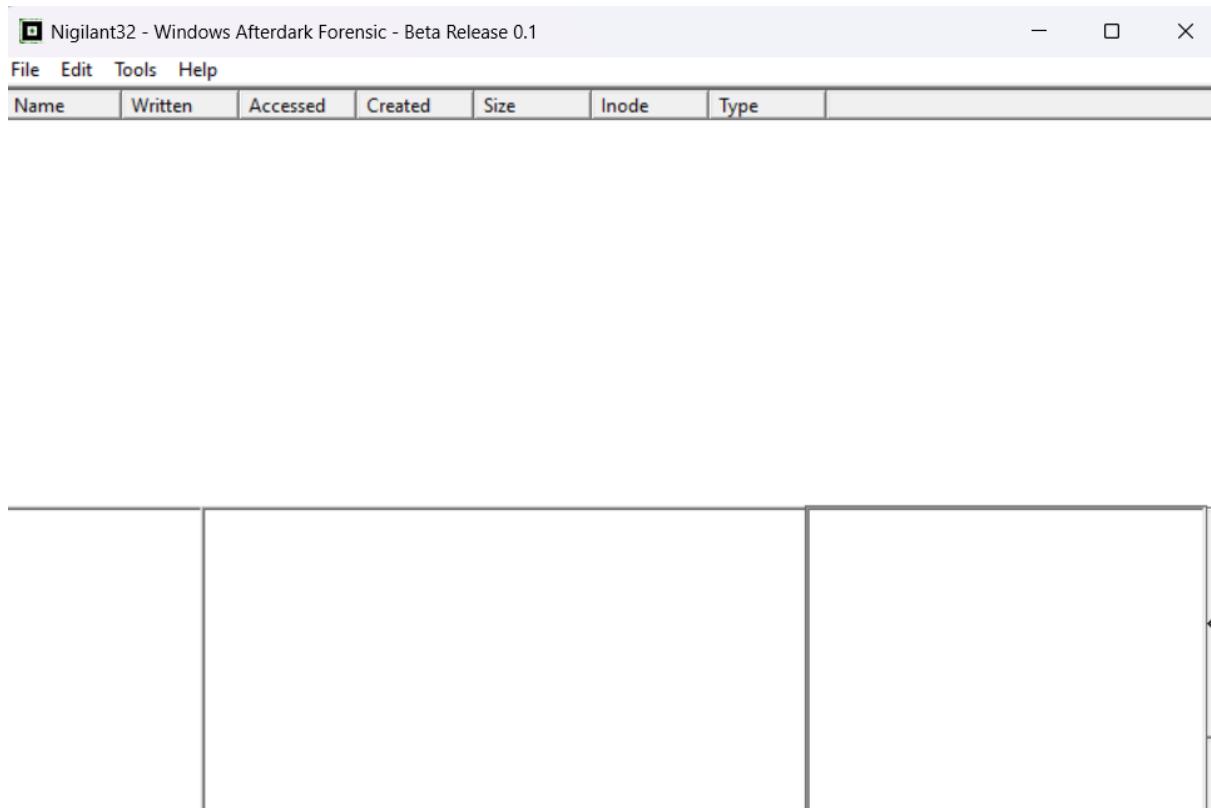
IS THIS OK?

Yes

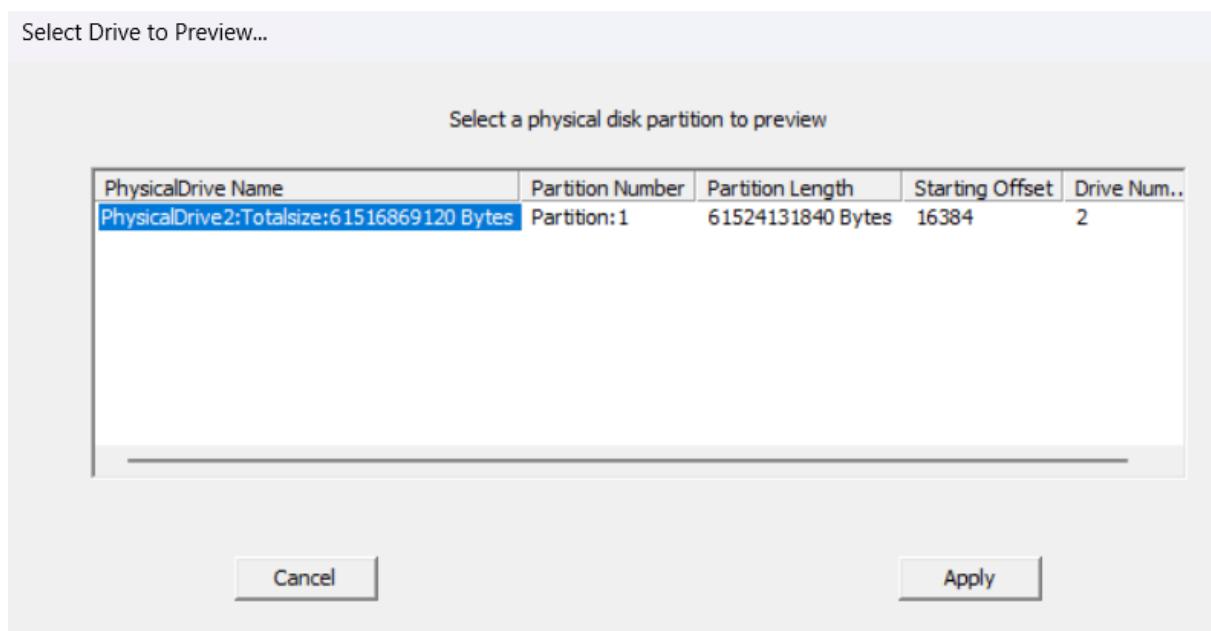
No



Start a NetCat Listener



Here we can preview the hard drive



It displays the files and folders pertaining to the partition.

Nigilant32 - Windows Afterdark Forensic - Beta Release 0.1

File Edit Tools Help

Name	Written	Accessed	Created	Size	I...	Typ
\$AttrDef	Wed Jan 22 08:50:18 2025	Wed Jan 22 08:50:18 2025	Wed Jan 22 08:50:18 2025	2560	4	0
\$BadClus	Wed Jan 22 08:50:18 2025	Wed Jan 22 08:50:18 2025	Wed Jan 22 08:50:18 2025	1394585600	8	0
\$Bitmap	Wed Jan 22 08:50:18 2025	Wed Jan 22 08:50:18 2025	Wed Jan 22 08:50:18 2025	1877568	6	0
\$Boot	Wed Jan 22 08:50:18 2025	Wed Jan 22 08:50:18 2025	Wed Jan 22 08:50:18 2025	8192	7	0
\$Extend	Wed Jan 22 08:50:18 2025	Wed Jan 22 08:50:18 2025	Wed Jan 22 08:50:18 2025	552	11	1
\$LogFile	Wed Jan 22 08:50:18 2025	Wed Jan 22 08:50:18 2025	Wed Jan 22 08:50:18 2025	67108864	2	0
SMFT	Wed Jan 22 08:50:18 2025	Wed Jan 22 08:50:18 2025	Wed Jan 22 08:50:18 2025	262144	0	0
SMFTMirr	Wed Jan 22 08:50:18 2025	Wed Jan 22 08:50:18 2025	Wed Jan 22 08:50:18 2025	4096	1	0
\$Secure	Wed Jan 22 08:50:18 2025	Wed Jan 22 08:50:18 2025	Wed Jan 22 08:50:18 2025	272072	9	0
\$UpCase	Wed Jan 22 08:50:18 2025	Wed Jan 22 08:50:18 2025	Wed Jan 22 08:50:18 2025	131104	10	0
\$Volume	Wed Jan 22 08:50:18 2025	Wed Jan 22 08:50:18 2025	Wed Jan 22 08:50:18 2025	0	3	0
.	Sun Jan 26 18:20:48 2025	Sun Jan 26 18:23:37 2025	Sun Jan 26 18:20:48 2025	4152	5	1
Helix_V1.9-07-13-2007.iso	Wed Jan 22 10:44:49 2025	Sun Jan 26 18:21:52 2025	Wed Jan 22 10:44:49 2025	734644391	40	0
System Volume Information	Wed Jan 22 09:50:27 2025	Sun Jan 26 18:22:12 2025	Wed Jan 22 09:50:27 2025	700	26	1

#### Live Machine Snapshot

```
Service Display Name: Realtek RT640 NT Driver
Service Name: rt640x64
Binary Path: \SystemRoot\System32\drivers\rt640x64.sys
Process Id: 0
Service Start Type: On Demand Start

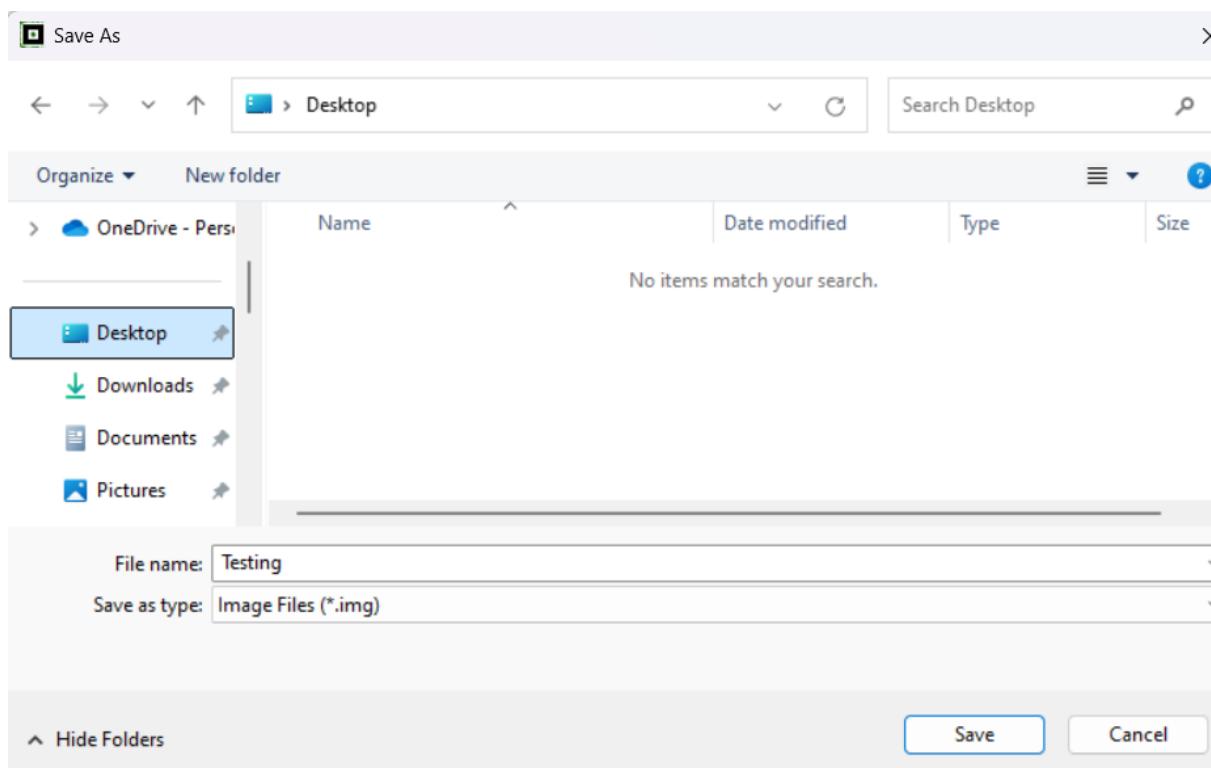
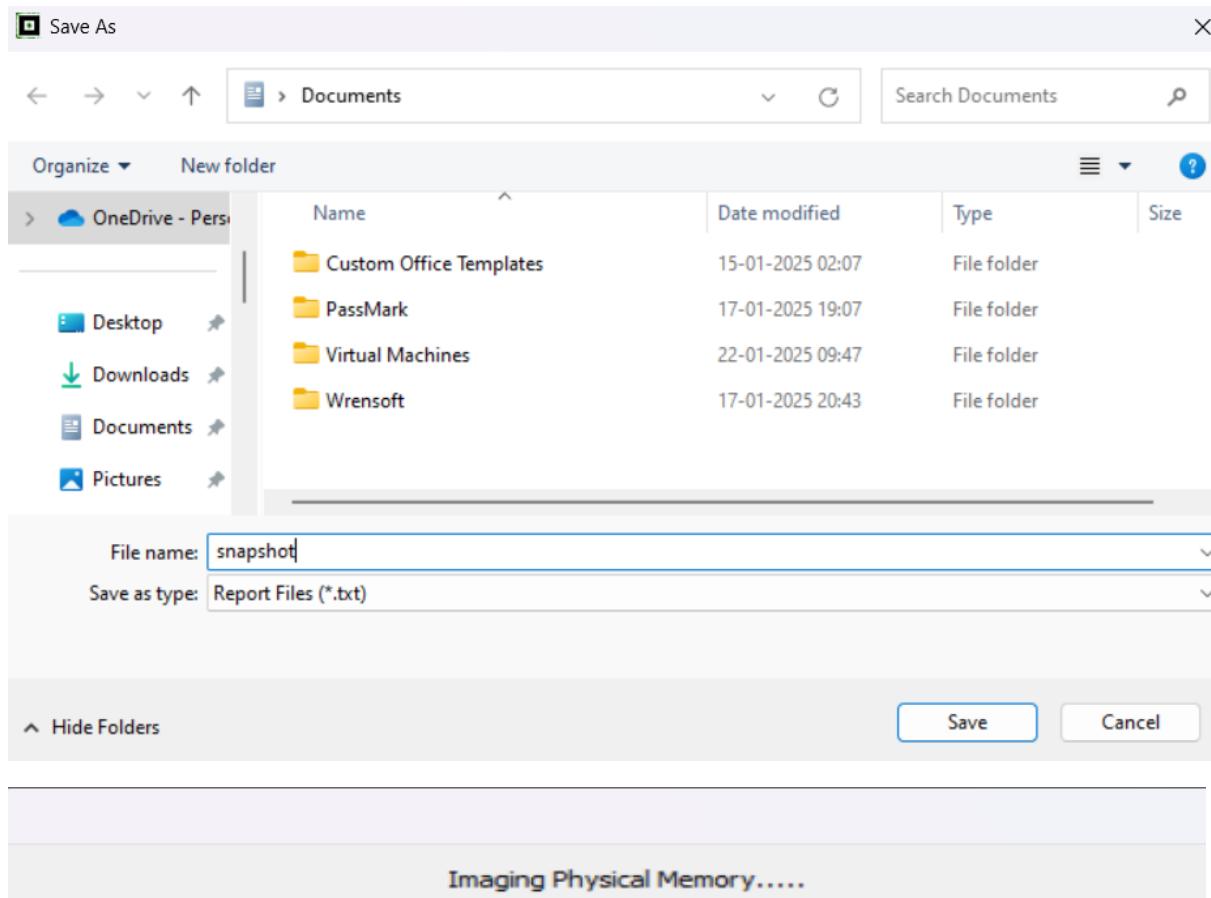
Service Display Name: Realtek NetAdapter Driver
Service Name: rtcx21
Binary Path: \SystemRoot\System32\DriverStore\FileRepository\rtcx21x64.inf_amd64_516e5c9b75c49dc2\rtcx21x64.sys
Process Id: 0
Service Start Type: On Demand Start

Service Display Name: Realtek Audio Universal Service
Service Name: RtkAudioUniversalService
Binary Path: C:\Windows\System32\DriverStore\FileRepository\realtekservice.inf_amd64_c60facea9c32a6cb\RtkAudUService64.exe"
Process Id: 4296
Service Start Type: Startup

Error Retrieving Service Information
Error Retrieving Scheduled Task Information
```

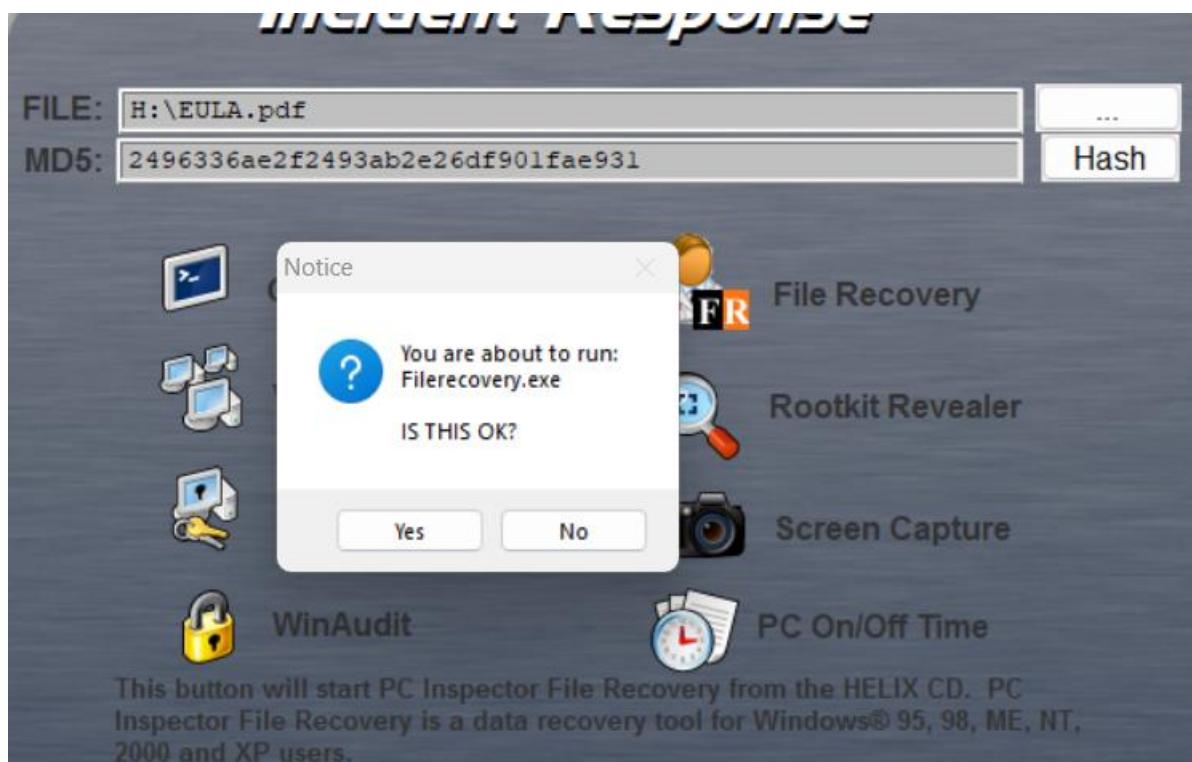
Save

Cancel

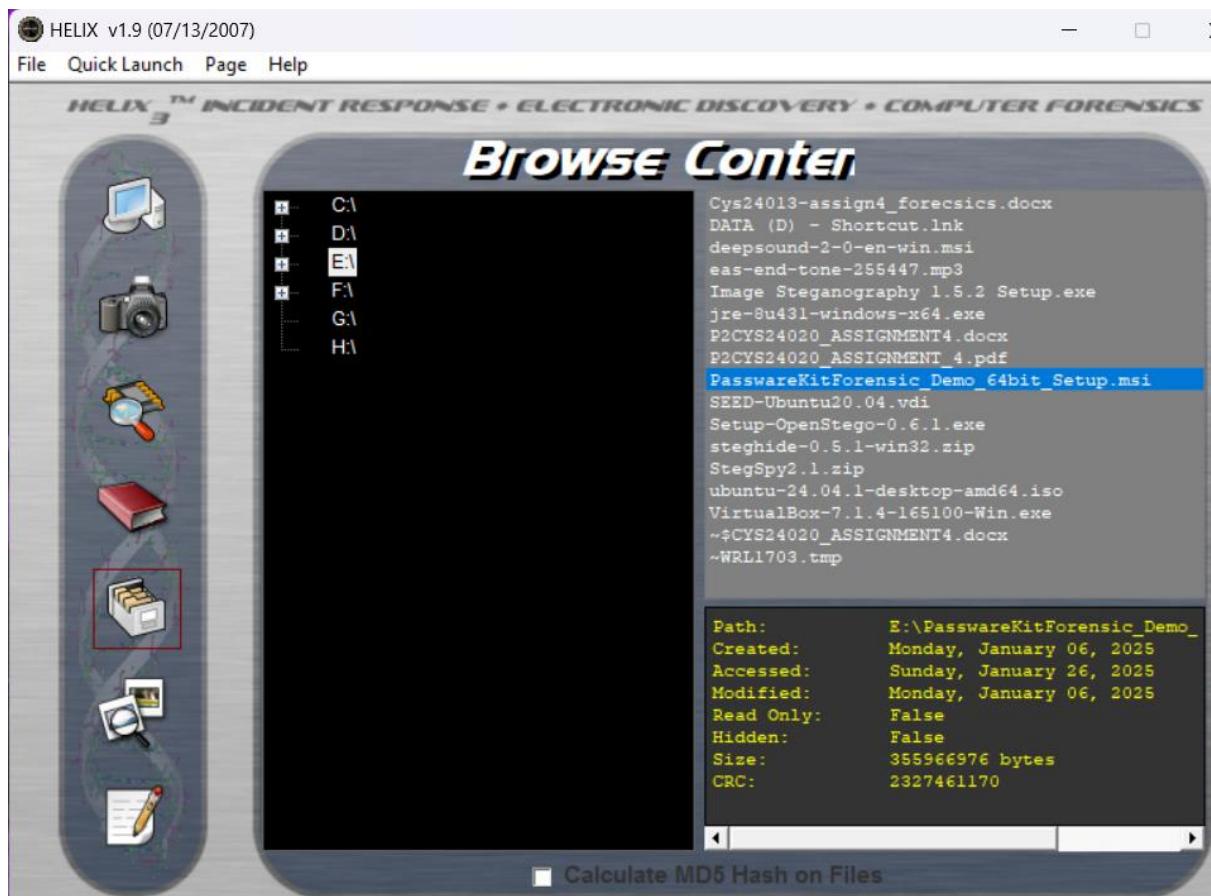
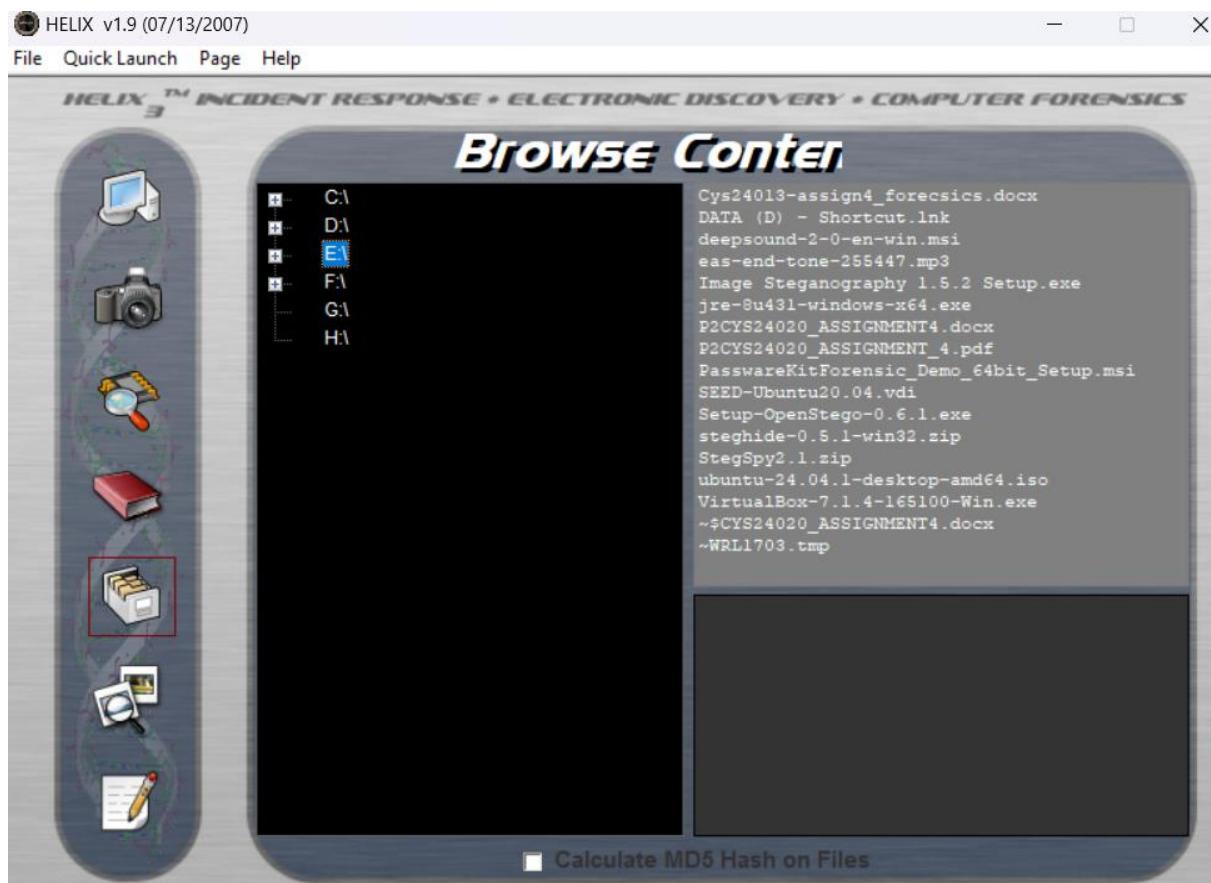


To generate an MD5 hash value of a file select a file .

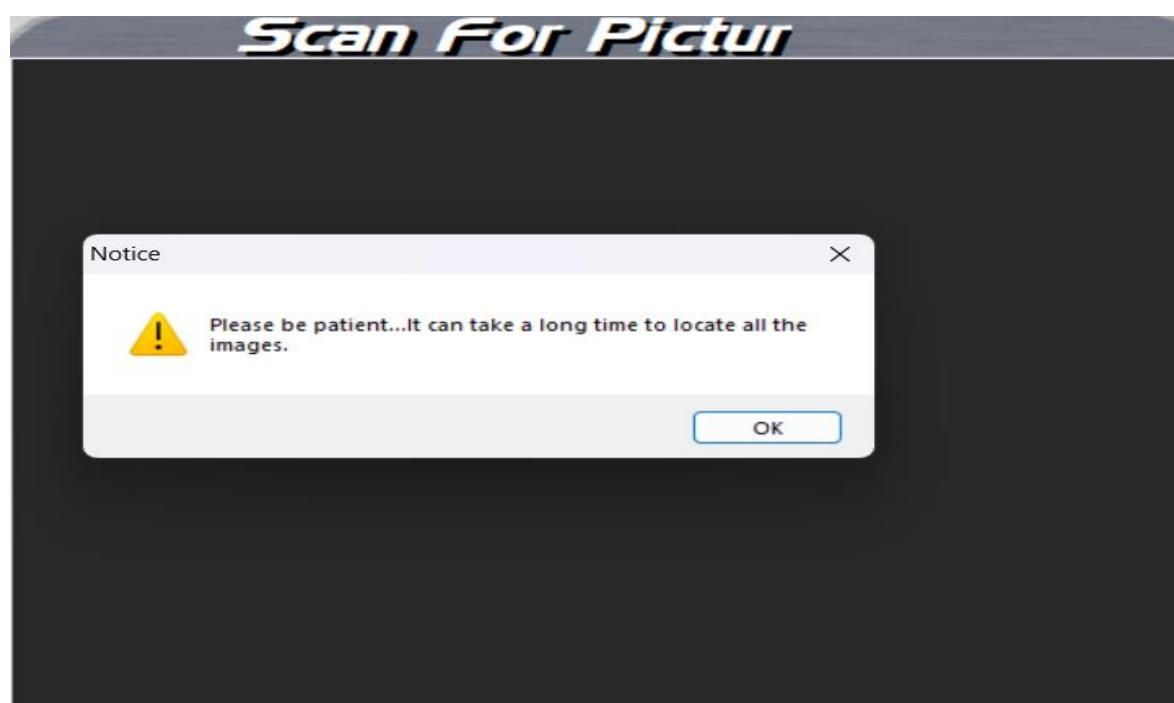
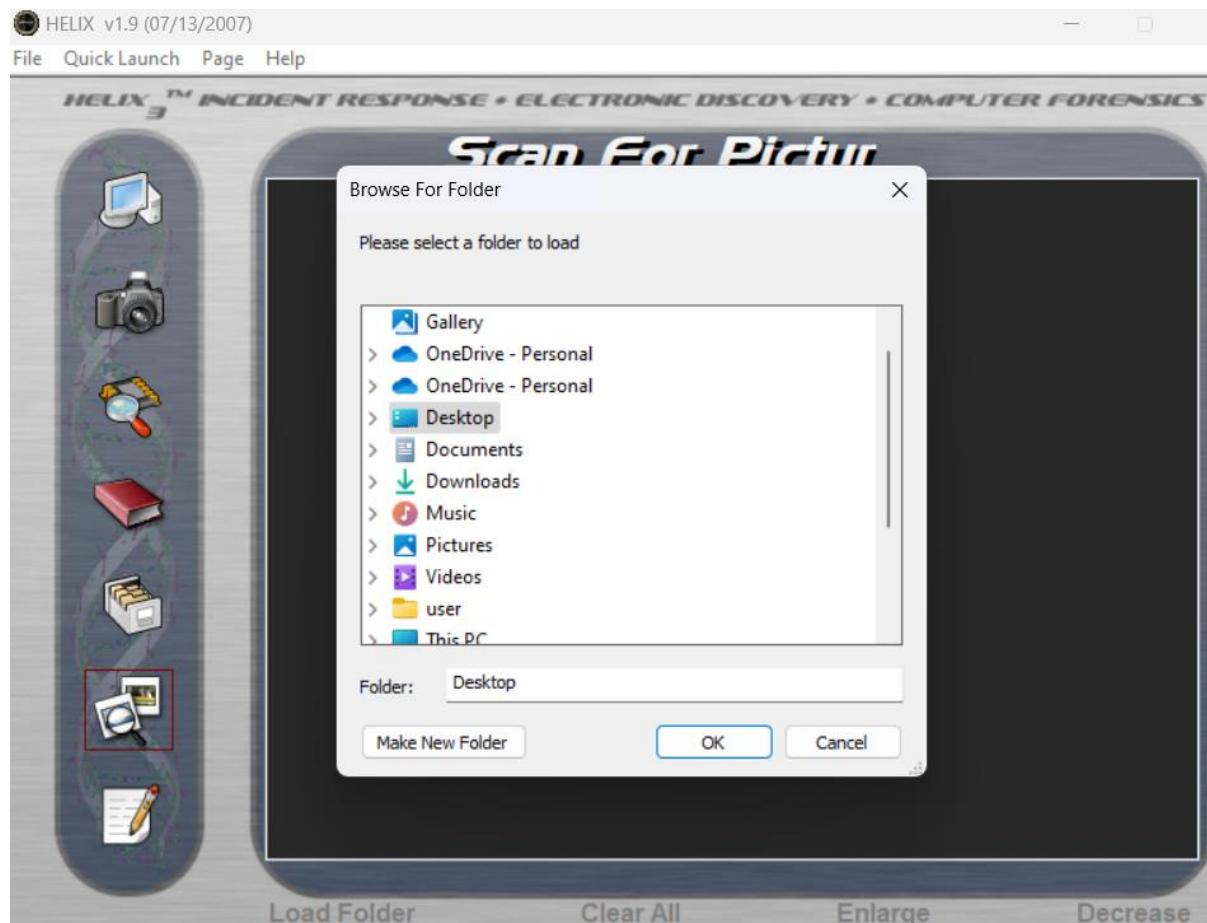




To know the content of drive click browse icon in left pane.it displays the drive.



To scan image click scan for pictures





## Lab5: Acquiring Volatile Data in Linux System.

The objective of this lab is to help to learn to gather volatile data from a live linux system and analyze it to find traces of attack to define the type, impact points path as well as the perpetrator.

Uname -a is used to gather Linux system information in sequence including kernel name, hostname, kernal release, and machine hardware name.

```
theertha@cys24020:~$ uname -a
Linux cys24020 6.11.0-13-generic #14-Ubuntu SMP PREEMPT_DYNAMIC Sat Nov 30 23:51:51 U
TC 2024 x86_64 x86_64 x86_64 GNU/Linux
```

Sudo su: The user will be changed from theertha to root.

```
theertha@cys24020:~$ sudo su
[sudo] password for theertha:
root@cys24020:/home/theertha#
```

The lshw command help in printing hardware details of the system. Use -short option to print the summary of information.

```

root@cys24020:/home/theertha# lshw -short
H/W path          Device   Class      Description
=====
/0                  system    VMware Virtual Platform
/0/0                bus       440BX Desktop Reference Platform
/0/1                memory   86KiB BIOS
/0/1/0              processor 11th Gen Intel(R) Core(TM) i5-1135G7 @
/0/1/1              memory   16KiB L1 cache
/0/2                memory   16KiB L1 cache
/0/5                processor 11th Gen Intel(R) Core(TM) i5-1135G7 @
CPU
/0/5/95             memory   16KiB L1 cache
/0/6                processor CPU
/0/6/96             memory   16KiB L1 cache
/0/7                processor CPU
/0/7/97             memory   16KiB L1 cache
/0/8                processor CPU
/0/8/98             memory   16KiB L1 cache
/0/9                processor CPU
/0/9/99             memory   16KiB L1 cache
/0/a                processor CPU

/0/100/17.1         bridge   PCI Express Root Port
/0/100/17.2         bridge   PCI Express Root Port
/0/100/17.3         bridge   PCI Express Root Port
/0/100/17.4         bridge   PCI Express Root Port
/0/100/17.5         bridge   PCI Express Root Port
/0/100/17.6         bridge   PCI Express Root Port
/0/100/17.7         bridge   PCI Express Root Port
/0/100/18            bridge   PCI Express Root Port
/0/100/18.1         bridge   PCI Express Root Port
/0/100/18.2         bridge   PCI Express Root Port
/0/100/18.3         bridge   PCI Express Root Port
/0/100/18.4         bridge   PCI Express Root Port
/0/100/18.5         bridge   PCI Express Root Port
/0/100/18.6         bridge   PCI Express Root Port
/0/100/18.7         bridge   PCI Express Root Port
/1                  system
/2                  input    Power Button
/3                  input    AT Translated Set 2 keyboard
/4                  input    VirtualPS/2 VMware VMMouse
/5                  input    VirtualPS/2 VMware VMMouse
root@cys24020:/home/theertha# 

```

By entering 'w' it will print uptime details.

```

root@cys24020:/home/theertha# w
 09:57:52 up 19 min,  5 users,  load average: 0.06, 0.23, 0.38
USER   TTY     FROM           LOGIN@   IDLE   JCPU   PCPU   WHAT
theertha  tty2      -        09:38  19:43  0.12s  0.10s /usr/libexec/gnome-s
theertha      -        09:38  19:22  0.00s  2.53s /usr/lib/systemd/sys
root    pts/1      -        09:42  1.00s  0.13s  0.10s w
root      -        09:42  19:22  0.00s  0.44s /usr/lib/systemd/sys
root    pts/3      -        09:51  6:45   0.01s  ?      bash
root@cys24020:/home/theertha# 

```

last -a: used to gather the last login sessions

```

last-a [Read-Only]
Open Save
1 [0;1;32m●[0m rsyslog.service - System Logging Service
2   Loaded: loaded ([0]8;;file:///cys24020/usr/lib/systemd/system/rsyslog.service[0]/usr/lib/systemd/system/rsyslog.service[0]8;;[0]; [0;1;32menabled[0m; preset:
3     Active: [0;1;32mactive (running)[0m since Sun 2025-01-26 10:10:33 IST; 13s ago
4   Invocation: f45a95322ea74d4ea9ffcc90e01d447
5 TriggeredBy: [0;1;32m●[0m syslog.socket
6     Docs: [0]8;;man:rsyslogd(8)[0]man:rsyslogd(8)[0]8;;[0]
7       [0]8;;man:rsyslog.conf(5)[0]man:rsyslog.conf(5)[0]8;;[0]
8         [0]8;;https://www.rsyslog.com/doc/[0]https://www.rsyslog.com/doc/[0]8;;[0]
9   Process: 6726 ExecStartPre=/usr/lib/rsyslog/reload-apparmor-profile (code=exited, status=0/SUCCESS)
10    Main PID: 6730 (rsyslogd)
11      Tasks: 4 (limit: 1830)
12     Memory: 1.2M (peak: 5M)
13       CPU: 239ms
14     CGroup: /system.slice/rsyslog.service
15       └─[0;38;5;245m6730 /usr/sbin/rsyslogd -n -iNONE[0m
16
17 Jan 26 10:10:33 cys24020 systemd[1]: Starting rsyslog.service - System Logging Service...
18 Jan 26 10:10:33 cys24020 rsyslogd[6730]: imuxsock: Acquired UNIX socket '/run/systemd/journal/syslog' (fd 3) from systemd. [v8.2406.0]
19 Jan 26 10:10:33 cys24020 systemd[1]: Started rsyslog.service - System Logging Service.
20 Jan 26 10:10:33 cys24020 rsyslogd[6730]: rsyslogd's groupid changed to 102
21 Jan 26 10:10:33 cys24020 rsyslogd[6730]: rsyslogd's userid changed to 102
22 Jan 26 10:10:33 cys24020 rsyslogd[6730]: [origin software="rsyslogd" swVersion="8.2406.0" x-pid="6730" x-info="https://www.rsyslog.com"] start

```

Plain Text ▾ Tab Width: 8 ▾ Ln 1, Col 1 INS

**netstat:** to check network status of the system.

```

root@cys24020:/home/theertha# netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address          Foreign Address        State
tcp     0      0  cys24020:59020           a104-115-39-49.dep:http TIME_WAIT
tcp     0      0  cys24020:47248           ec2-3-233-158-26.https ESTABLISHED
tcp     0      0  cys24020:55320           217.138.110.34.bc:https ESTABLISHED
tcp     0      0  cys24020:38336           104.18.32.47:https ESTABLISHED
tcp     0      0  cys24020:47526           166.188.117.34.bc:https ESTABLISHED
tcp     0      0  cys24020:45972           172.64.155.209:https ESTABLISHED
tcp     0      0  cys24020:38276           93.243.107.34.bc.:https ESTABLISHED
udp     0      0  cys24020:bootpc          192.168.184.254:bootps ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags     Type            State           I-Node Path
unix  2      [ ]  DGRAM           CONNECTED        36704
unix  3      [ ]  STREAM          CONNECTED        32063  /run/systemd/journal/stdout
unix  3      [ ]  STREAM          CONNECTED        25616  /run/dbus/system_bus_socket
unix  3      [ ]  STREAM          CONNECTED        32632  /run/user/1000/bus
unix  3      [ ]  STREAM          CONNECTED        30640
unix  3      [ ]  STREAM          CONNECTED        60007  /run/user/1000/bus
unix  3      [ ]  STREAM          CONNECTED        31529  /run/user/1000/bus
unix  3      [ ]  STREAM          CONNECTED        30760  /run/systemd/journal/stdout
unix  3      [ ]  STREAM          CONNECTED        29429  /run/systemd/journal/stdout
unix  3      [ ]  STREAM          CONNECTED        23128  /run/systemd/journal/stdout
unix  3      [ ]  STREAM          CONNECTED        19267
unix  3      [ ]  STREAM          CONNECTED        46191
unix  3      [ ]  STREAM          CONNECTED        30654  /run/user/1000/bus
unix  3      [ ]  STREAM          CONNECTED        25657  /run/dbus/system_bus_socket
unix  3      [ ]  STREAM          CONNECTED        30708

```

**Ifconfig -a:** By using this command we can review the current network settings.

```

root@cys24020:/home/theertha# ifconfig -a
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
      inet 192.168.184.131  netmask 255.255.255.0  broadcast 192.168.184.255
      inet6 fe80::20c:29ff:fed7:3e98  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:d7:3e:98  txqueuelen 1000  (Ethernet)
          RX packets 106762  bytes 132303839 (132.3 MB)
          RX errors 0  dropped 0  overruns 0  frame 0
          TX packets 42611  bytes 3607395 (3.6 MB)
          TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
      inet 127.0.0.1  netmask 255.0.0.0
      inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
          RX packets 1449  bytes 154264 (154.2 KB)
          RX errors 0  dropped 0  overruns 0  frame 0
          TX packets 1449  bytes 154264 (154.2 KB)
          TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

```

The lsof command will help us to find all the open files associated with particular ports ,services and processes.

lsof > openfile.txt: used to save a text file in home directory, containing the result.

```
root@cys24020:/home/theertha# lsof > openfiles.txt
lsof: WARNING: can't stat() fuse.portal file system /run/user/1000/doc
      Output information may be incomplete.
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1000/gvfs
      Output information may be incomplete.
```

Open	▼	• openfiles.txt ~/						⚙️	☰	↶	✖
COMMAND	PID	TID	TASKCMD	USER	FD	TYPE	DEVICE	SIZE/OFF	NODE	NAME	
systemd	1			root	cwd	DIR	8,2	4096	2	/	
systemd	1			root	rtd	DIR	8,2	4096	2	/	
systemd	1			root	txt	REG	8,2	109008	413518	/usr/lib/	
systemd/systemd											
systemd	1			root	mem	REG	8,2	772248	416356	/usr/lib/x86_64-	
linux-gnu/libzstd.so.1.5.6				root	mem	REG	8,2	5604704	415690	/usr/lib/x86_64-	
systemd	1			root	mem	REG	8,2	403704	415646	/usr/lib/x86_64-	
linux-gnu/libcrypto.so.3				root	mem	REG	8,2	207072	415969	/usr/lib/x86_64-	
systemd	1			root	mem	REG	8,2	2182752	415656	/usr/lib/x86_64-	
linux-gnu/libbpf.so.1.4.5				root	mem	REG	8,2	121632	415753	/usr/lib/x86_64-	
systemd	1			root	mem	REG	8,2	116960	415950	/usr/lib/x86_64-	
linux-gnu/liblzma.so.5.6.2				root	mem	REG	8,2	637712	416094	/usr/lib/x86_64-	
systemd	1			root	mem	REG	8,2	26848	415668	/usr/lib/x86_64-	
linux-gnu/libc.so.6				root	mem	REG	8,2	72064	416074	/usr/lib/x86_64-	
systemd	1			root	mem	REG	8,2	16384			
linux-gnu/libelf-0.191.so				root	mem	REG	8,2	0			
systemd	1			root	mem	REG	8,2	0			
linux-gnu/libkmod.so.2.4.1				root	mem	REG	8,2	0			
systemd	1			root	mem	REG	8,2	0			
linux-gnu/libz.so.1.3.1				root	mem	REG	8,2	0			
systemd	1			root	mem	REG	8,2	0			
linux-gnu/libpcre2-8.so.0.11.2				root	mem	REG	8,2	0			
systemd	1			root	mem	REG	8,2	0			
linux-gnu/libcap-ng.so.0.0.0				root	mem	REG	8,2	0			
systemd	1			root	mem	REG	8,2	0			
linux-gnu/libbam.so.0.85.1				root	mem	REG	8,2	0			

We can view the loaded modules in linux system using the command lsmod.

```
root@cys24020:/home/theertha# lsmod
Module            Size  Used by
isofs             61440  2
snd_seq_dummy     12288  0
snd_hrtimer       12288  1
intel_rapl_msr   20480  0
intel_rapl_common 53248  1 intel_rapl_msr
intel_uncore_frequency_common 16384  0
intel_pmc_core   118784 0
intel_vsec        20480  1 intel_pmc_core
pmt_telemetry    16384  1 intel_pmc_core
pmt_class         16384  1 pmt_telemetry
snd_ens1371       36864  1
snd_ac97_codec   196608 1 snd_ens1371
crct10dif_pclmul 12288  1
gameport          24576  1 snd_ens1371
polyval_clmulni  12288  0
polyval_generic   12288  1 polyval_clmulni
ghash_clmulni_intel 16384  0
ac97_bus          12288  1 snd_ac97_codec
sha256_ssse3     32768  0
sha1_ssse3        32768  0
aesni_intel      122880 0
snd_pcm           196608 2 snd_ac97_codec,snd_ens1371
crypto_simd      16384  1 aesni_intel
```

Install a linux auditing tool called auditd. The auditing tool consists of utilities that would help in creating records about system information.

```
root@cys24020:/home/theertha# apt install auditd
Installing:
  auditd

Installing dependencies:
  libauparse0t64

Suggested packages:
  audispd-plugins

Summary:
  Upgrading: 0, Installing: 2, Removing: 0, Not Upgrading: 115
  Download size: 270 kB
  Space needed: 878 kB / 10.6 GB available

Continue? [Y/n] y
Get:1 http://in.archive.ubuntu.com/ubuntu oracular/main amd64 libauparse0t64 amd64 1:4.0.1-1ubuntu2 [62.0 kB]
Get:2 http://in.archive.ubuntu.com/ubuntu oracular/main amd64 auditd amd64 1:4.0.1-1ubuntu2 [209 kB]
Fetched 270 kB in 18s (14.8 kB/s)
Selecting previously unselected package libauparse0t64:amd64.
(Reading database ... 156104 files and directories currently installed.)
Preparing to unpack .../libauparse0t64_1%3a4.0.1-1ubuntu2_amd64.deb ...
```

Gather details of all the login attempts made to the system by issuing the command aureport.

```
root@cys24020:/home/theertha# sudo aureport
Summary Report
=====
Range of time in logs: 01/26/2025 11:10:53.589 - 01/26/2025 11:16:39.582
Selected time for report: 01/26/2025 11:10:53 - 01/26/2025 11:16:39.582
Number of changes in configuration: 0
Number of changes to accounts, groups, or roles: 0
Number of logins: 0
Number of failed logins: 0
Number of authentications: 0
Number of failed authentications: 0
Number of users: 3
Number of terminals: 5
Number of host names: 1
Number of executables: 4
Number of commands: 3
Number of files: 0
Number of AVC's: 0
Number of MAC events: 0
Number of failed syscalls: 0
Number of anomaly events: 0
Number of responses to anomaly events: 0
Number of crypto events: 0
>Show Apps < Show Integrity events: 0
```

Determine the User ID of a particular user using id root command and the track all the user events pertaining to the userid with ausearch command. Syntax of the command is **ausearch -ui <userID> -- interpret**. Here the user Id is 0.

```

root@cys24020:/home/theertha# id root
uid=0(root) gid=0(root) groups=0(root)
root@cys24020:/home/theertha# ausearch -ui 0 --interpret
-----
type=DAEMON_START msg=audit(01/26/2025 11:10:53.589:5856) : op=start ver=4.0.1 format=enriched kerne
l=6.11.0-13-generic auid	unset pid=8437 uid=root ses	unset subj=unconfined res=success
-----
type=SERVICE_START msg=audit(01/26/2025 11:10:53.593:205) : pid=1 uid=root auid	unset ses=unset subj
=unconfined msg='unit=auditd comm=systemd exe=/usr/lib/systemd/systemd hostname=? addr=? terminal=? res=success'
-----
type=USER_END msg=audit(01/26/2025 11:10:53.605:206) : pid=8409 uid=root auid=theertha ses=3 subj=un
confined msg='op=PAM:session_close grantors=pam_limits,pam_env,pam_env,pam_permit,pam_umask,pam_unix
acct=root exe=/usr/bin/sudo hostname=? addr=? terminal=/dev/pts/2 res=success'
[ubuntu 24.10 amd64]
type=CRED_U1SP msg=audit(01/26/2025 11:10:53.605:207) : pid=8409 uid=root auid=theertha ses=3 subj=u
nconfined msg='op=PAM:setcred grantors=pam_permit acct=root exe=/usr/bin/sudo hostname=? addr=? term
inal=/dev/pts/2 res=success'
-----
type=USER_ACCT msg=audit(01/26/2025 11:11:10.814:208) : pid=8449 uid=root auid=theertha ses=3 subj=u
nconfined msg='op=PAM:accounting grantors=pam_permit,pam_localuser acct=root exe=/usr/bin/sudo hostn
ame=? addr=? terminal=/dev/pts/2 res=success'
-----
type=USER_CMD msg=audit(01/26/2025 11:11:10.819:209) : pid=8449 uid=root auid=theertha ses=3 subj=u
nconfined msg='cwd=/home/theertha cmd=systemctl enable audited exe=/usr/bin/sudo terminal=pts/2 res=su

```

Linux stores the scheduled tasks in /var/spool/cron and /etc/cron.daily the system files. Find the scheduled task by verifying these files.

```

root@cys24020:/home/theertha# ls /var/spool/cron
crontabs

```

The cron files also store data about the tasks scheduled hourly,daily,,weekly and monthly. To view the daily scheduled task files go to /etc/cron.daily

```

root@cys24020:/home/theertha# ls /etc/cron.daily
@anacron  apport  apt-compat  dpkg  logrotate  man-db  sysstat

```

The .bash\_history file contains the command history in the linux system.

GNU nano 8.1	.bash_history
ishw-short	
ishw -short	
lshw-short	
lshw -short	
w	
last -a	
apt install wtmpdb	
last -a	
sudo chmod 644 /var/lib/wtmpdb/wtmp.db	
ls -ld /var/lib/wtmpdb	
sudo touch /var/lib/wtmpdb/wtmp.db	
sudo chmod 644 /var/lib/wtmpdb/wtmp.db	
last -a	
sudo apt-get install --reinstall rsyslog	
sudo systemctl restart rsyslog	
sudo systemctl status rsyslog	
last -a	
sudo systemctl status rsyslog	
last -a	
ls -l /var/log/wtmp	
sudo mv /var/lib/wtmpdb /var/lib/wtmpdb.old	
*.* /var/log/wtmp	
sudo systemctl restart rsyslog	
last -a	
sudo nano /etc/rsyslog.conf	
sudo mv /var/lib/wtmpdb /var/lib/wtmpdb.old	

We can find the arp cache by using arp command

```
root@cys24020:/home/theertha# arp
Address          HWtype  HWaddress          Flags Mask    Iface
192.168.184.254 ether   00:50:56:f8:d4:54  C      ens33
_gateway         ether   00:50:56:f6:65:b7  C      ens3
```

By using ps command we can view the running process in the system.

```
root@cys24020:/home/theertha# ps
  PID TTY      TIME CMD
  6284 pts/4    00:00:00 sudo
  6285 pts/4    00:00:00 su
  6286 pts/4    00:00:00 bash
  6554 pts/4    00:00:00 ps
root@cys24020:/home/theertha#
```

We can use the option auxww to view all details of the running processes.

```
root@cys24020:/home/theertha# ps auxww
USER     PID %CPU %MEM   VSZ   RSS TTY      STAT START  TIME COMMAND
root      1  0.1  0.6 23500 10404 ?
root      2  0.0  0.0     0     0 ?        Ss 11:47 0:06 /sbin/init splash
root      3  0.0  0.0     0     0 ?        S 11:47 0:00 [kthreadd]
root      4  0.0  0.0     0     0 ?        I< 11:47 0:00 [pool_workqueue_release]
root      5  0.0  0.0     0     0 ?        I< 11:47 0:00 [kworker/R-rcu_gp]
root      6  0.0  0.0     0     0 ?        I< 11:47 0:00 [kworker/R-sync_wq]
root      7  0.0  0.0     0     0 ?        I< 11:47 0:00 [kworker/R-stub_flushwq]
root      8  0.0  0.0     0     0 ?        I 11:47 0:02 [kworker/R-netns]
root     11  0.0  0.0     0     0 ?        I 11:47 0:00 [kworker/0:0-events]
root     12  0.0  0.0     0     0 ?        I< 11:47 0:00 [kworker/u512:0 ipv6_addrconf]
root     13  0.0  0.0     0     0 ?        I 11:47 0:00 [kworker/R-mm_percpu_wq]
root     14  0.0  0.0     0     0 ?        I 11:47 0:00 [rcu_tasks_kthread]
root     15  0.0  0.0     0     0 ?        I 11:47 0:00 [rcu_tasks_rude_kthread]
root     16  0.0  0.0     0     0 ?        S 11:47 0:00 [ksoftirqd/0]
root     17  0.0  0.0     0     0 ?        I 11:47 0:01 [rcu_preempt]
root     18  0.0  0.0     0     0 ?        S 11:47 0:00 [rcu_exp_par_gp_kthread_worker/1]
root     19  0.0  0.0     0     0 ?        S 11:47 0:00 [rcu_exp_gp_kthread_worker]
root     20  0.0  0.0     0     0 ?        S 11:47 0:00 [migration/0]
root     21  0.0  0.0     0     0 ?        S 11:47 0:00 [idle_inject/0]
root     22  0.0  0.0     0     0 ?        S 11:47 0:00 [cpuhp/0]
root     23  0.0  0.0     0     0 ?        S 11:47 0:00 [cpuhp/1]
root     24  0.0  0.0     0     0 ?        S 11:47 0:00 [idle_inject/1]
```

We can find the ports related to a particular process bu using the command ss -l -p -n | grep <PID>

```
root@cys24020:/home/theertha# ss -l -p -n | grep 2150
u_str LISTEN 0      4096                               /run/user/1000/bus 30151           * 0      users:(("dbus-daemon",pid=2150,fd=3),("systemd",pid=2108,fd=33))
```

```
root@cys24020:/home/theertha# ls /proc
 1  1705 207 2210 239 2548 2959 3735 4528 59  6464 75  908      filesystems  pressure
101 18 208 2218 24 2551 2960 3761 4532 6  6485 76  91      fs          schedstat
1015 186 209 222 240 2558 2984 38 4539 60  65 77  94      interrupts  scsi
102 187 2094 2229 2404 2562 2991 39 4624 6025 6500 78  945     iomem       self
103 188 21 223 2407 2566 3 4 47 6026 6510 79  95      ioports     slabinfo
11 189 210 224 241 2568 3028 40 4750 6055 6543 8  953     irq          softirqs
111 19 2108 225 2417 2577 3029 41 4751 6056 6596 80  96      kallsyms   stat
113 190 211 2256 242 2588 31 412 4769 6057 66 81  961      kcore        swaps
12 191 2115 226 243 26 3107 42 4775 6058 6617 82  963      keys          sys
128 192 212 227 244 2673 3109 4237 4780 61  6626 828  97      key-users   sysrq-trigger
129 193 213 228 245 27 3141 4241 48 6184 6673 83  acpi        kmsg        sysvipc
13 194 2135 229 246 2724 3163 4243 49 62  6674 830  asound      kpagegroup  thread-self
14 195 2136 23 247 2742 32 43 5 6268 67 84  bootconfig  kpagecount timer_list
1411 196 214 230 2487 2745 323 438 50 6275 6715 840  buddyinfo  kpageflags  tty
1414 197 2145 231 25 2746 324 4385 51 6282 6728 841  bus        latency_stats  uptime
1423 198 2147 232 2504 2754 3241 4392 52 6284 68 85  cgroups    loadavg    version
1425 199 2149 2320 2526 2774 34 44 5217 6285 688 86  cmdline    locks      version_signature
1430 2 215 2321 2528 2781 3472 4435 53 6286 689 87  consoles   mdstat    vmallocinfo
1437 20 2150 233 2532 279 35 4440 56 63 69 871  cpuminfo  meminfo    vmstat
1488 200 216 2337 2533 2793 3595 4441 569 6310 7 88  crypto     misc      zoneinfo
15 2005 217 234 2534 2800 36 4448 57 6366 70 883  devices    modules
1537 201 218 235 2535 2811 3641 4454 5712 6371 71 888  diskstats  mounts
16 202 219 236 2536 2814 3656 4465 573 6394 719 89  dma        mpt
1661 203 22 2361 2537 2820 3662 4475 58 64 72 890  driver     mtrr
169 204 220 2369 2541 2845 3706 4477 580 6401 720 894  dynamic_debug net
17 205 2200 237 2543 2874 373 45 5841 642 73 90  execdomains pagetypeinfo
170 206 221 238 2547 2926 3732 4527 5899 6459 74 903  fb        partitions
```

Clipboard stores the details of files or text copied recently. Copy and review the clipboard contents using the xclip command.

```
root@cys24020:/home/theertha# cat .bash_history | xclip
root@cys24020:/home/theertha# xclip -o
sudo apt-get install latrace
sudo apt update
apt search latrace
apt install latrace
sudo apt install latrace
sudo apt-get install latrace
sudo apt update
sudo apt install ltrace
sudo apt install latrace
sudo dpkg -i /path/to/latrace-package.deb
sudo apt-get install latrace
sudo apt update
sudo apt-get install latrace
gedit hello.c
sudo apt install gedit
gedit hello.c
gedit hello.h
gedit helloMain.c
gcc -fPIC --shared -o libhello.so hello.c
sudo apt install gcc
gcc -fPIC --shared -o libhello.so hello.c
gcc -o hello helloMain.c -lhello -L
sudo dpkg -i
sudo dpkg --i
sudo dpkg -i latrace_0.5.11-1_amd64.deb
sudo dpkg -i latrace_0.5. 11-1_amd64.deb
latrace /hello
```

To search for ELF files we can use find command

```
root@cys24020:/home/theertha# sudo find / -type f -exec file {} \; | grep ELF
/snap/gnome-42-2204/176/lib/udev/libinput-device-group: ELF 64-bit LSB pie executable, x86-64, version 1 (SYSV), dynamic
ally linked, interpreter /lib64/ld-linux-x86-64.so.2, BuildID[sha1]=5fc3af120dd06fc5a839ef9a7c6057b31b64573, for GNU/Li
nux 3.2.0, stripped
/snap/gnome-42-2204/176/lib/udev/libinput-fuzz-extract: ELF 64-bit LSB pie executable, x86-64, version 1 (SYSV), dynamic
ally linked, interpreter /lib64/ld-linux-x86-64.so.2, BuildID[sha1]=5382884b004f32cb7d0171eae2898497424ae2d1, for GNU/Li
nux 3.2.0, stripped
/snap/gnome-42-2204/176/lib/udev/libinput-fuzz-to-zero: ELF 64-bit LSB pie executable, x86-64, version 1 (SYSV), dynamic
ally linked, interpreter /lib64/ld-linux-x86-64.so.2, BuildID[sha1]=2db913ec2072a838ad117d002f1597368b423260, for GNU/Li
nux 3.2.0, stripped
/snap/gnome-42-2204/176/lib/x86_64-linux-gnu/bindtextdomain.so: ELF 64-bit LSB shared object, x86-64, version 1 (SYSV),
dynamically linked, BuildID[sha1]=0407d5415cf1e176dc69bf9534ec886f76158f7f, stripped
/snap/gnome-42-2204/176/lib/x86_64-linux-gnu/libc_malloc_debug.so.0: ELF 64-bit LSB shared object, x86-64, version 1 (SY
SV), dynamically linked, BuildID[sha1]=cc26c0258b14008f18b0364da4a36fd0215fab6, for GNU/Linux 3.2.0, stripped
/snap/gnome-42-2204/176/lib/x86_64-linux-gnu/libcrypt.so.1: ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dyna
mically linked, BuildID[sha1]=8f3f100ca1e8ff066713aa1e719ce71b46db0296, stripped
/snap/gnome-42-2204/176/lib/x86_64-linux-gnu/libdbus-1.so.3.19.13: ELF 64-bit LSB shared object, x86-64, version 1 (SYSV
), dynamically linked, BuildID[sha1]=63e8b99215502138cb63af6d65851a5e837ed49, stripped
/snap/gnome-42-2204/176/lib/x86_64-linux-gnu/libexpat.so.1.8.7: ELF 64-bit LSB shared object, x86-64, version 1 (SYSV),
dynamically linked, BuildID[sha1]=488cc1472bb121a12e1c77bb58fe0a5c52f2aa9, stripped
/snap/gnome-42-2204/176/lib/x86_64-linux-gnu/libpgp-error.so.0: ELF 64-bit LSB shared object, x86-64, version 1 (SYSV),
dynamically linked, BuildID[sha1]=3fbec71c67bee60d8aef00697ee187079b0fb307, stripped
/snap/gnome-42-2204/176/lib/x86_64-linux-gnu/liblzma.so.5.2.5: ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), d
ynamically linked, BuildID[sha1]=b85da6c48eb60a646615392559483b93617ef265, stripped
/snap/gnome-42-2204/176/lib/x86_64-linux-gnu/liblzo2.so.2.0.0: ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), d
ynamically linked, BuildID[sha1]=799961dd8869c85cea74b91c1f9f5e86e339c036, stripped
/snap/gnome-42-2204/176/lib/x86_64-linux-gnu/libpcre.so.3.13.3: ELF 64-bit LSB shared object, x86-64, version 1 (SYSV),
dynamically linked, BuildID[sha1]=3982f316c887e3ad9598015fa5bae8557320476a, stripped
/snap/gnome-42-2204/176/lib/x86_64-linux-gnu/libselinux.so.1: ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dv
```

```
/snap/gnome-42-2204/176/usr/lib/libcogl-path.so.20.4.3: ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked, BuildID[sha1]=f937fec0e32e51fae5f419a72966e669e19d74aa, stripped
/snap/gnome-42-2204/176/usr/lib/libcogl.so.20.4.3: ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked, BuildID[sha1]=94311bb1e9477510701c347332db227cc71c9d45, stripped
/snap/gnome-42-2204/176/usr/lib/libgee-0.8.so.2.6.1: ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked, BuildID[sha1]=51bce7b899d1ce2730a1027efcd04d534b87ef5c, stripped
/snap/gnome-42-2204/176/usr/lib/libgionmm-2.4.so.1.3.0: ELF 64-bit LSB shared object, x86-64, version 1 (GNU/Linux), dynamically linked, BuildID[sha1]=70224e590eeb8cd50d7c47d905c15aa3758f288c, stripped
/snap/gnome-42-2204/176/usr/lib/libglibmm-2.4.so.1.3.0: ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked, BuildID[sha1]=0a7aea13a8cccf13a4014790986d66ceda93d779, stripped
/snap/gnome-42-2204/176/usr/lib/libglibmm_generate_extra_defs-2.4.so.1.3.0: ELF 64-bit LSB shared object, x86-64, version 1 (GNU/Linux), dynamically linked, BuildID[sha1]=12ddb551d176950685c5d3337e83eb0e3c2815e, stripped
/snap/gnome-42-2204/176/usr/lib/libltdl.so.7.3.2: ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked, BuildID[sha1]=25ece783035b2982eb58f3b5fe18bae64b0984ad, stripped
```

We can analyze the headers and sections of ELF files using the readelf command.

```
root@cys24020:/home/theertha# readelf -h /snap/gnome-42-2204/176/usr/lib/libglibmm_generate_extra_defs-2.4.so.1.3.0
ELF Header:
  Magic: 7f 45 4c 46 02 01 01 03 00 00 00 00 00 00 00 00
  Class: ELF64
  Data: 2's complement, little endian
  Version: 1 (current)
  OS/ABI: UNIX - GNU
  ABI Version: 0
  Type: DYN (Shared object file)
  Machine: Advanced Micro Devices X86-64
  Version: 0x1
  Entry point address: 0x0
  Start of program headers: 64 (bytes into file)
  Start of section headers: 789488 (bytes into file)
  Flags: 0x0
  Size of this header: 64 (bytes)
  Size of program headers: 56 (bytes)
  Number of program headers: 11
  Size of section headers: 64 (bytes)
  Number of section headers: 30
  Section header string table index: 29
```

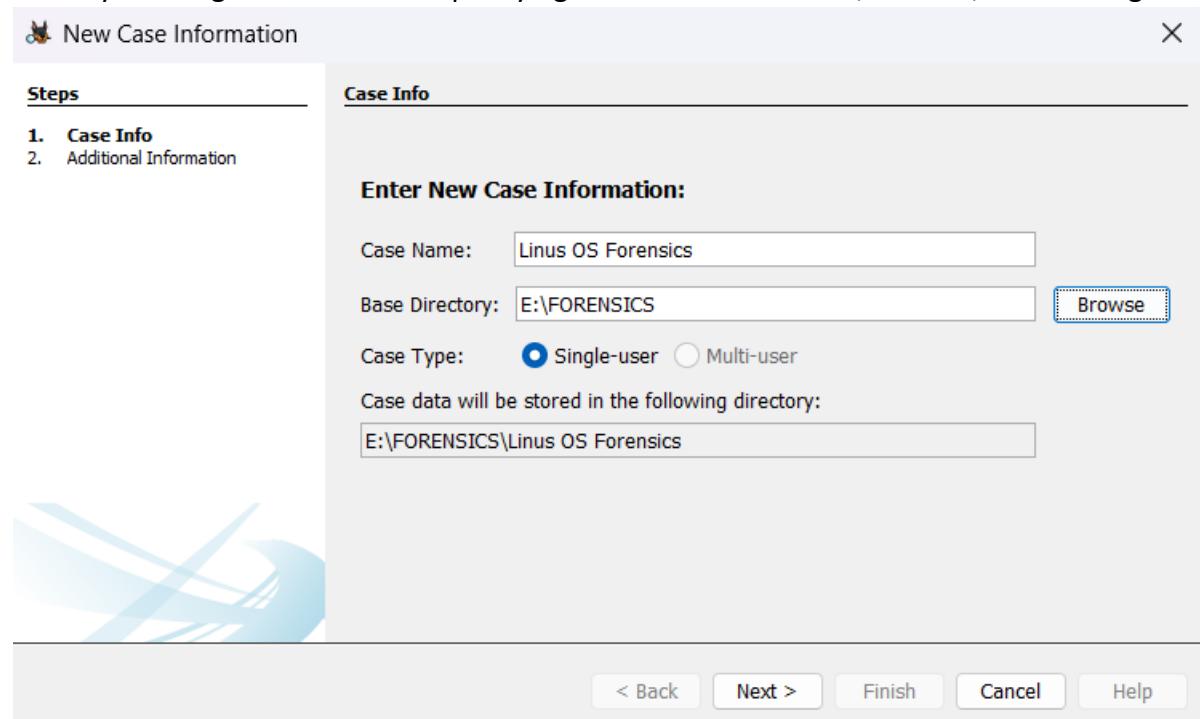
## Lab6: Analyzing Non-Volatile Data in Linux System

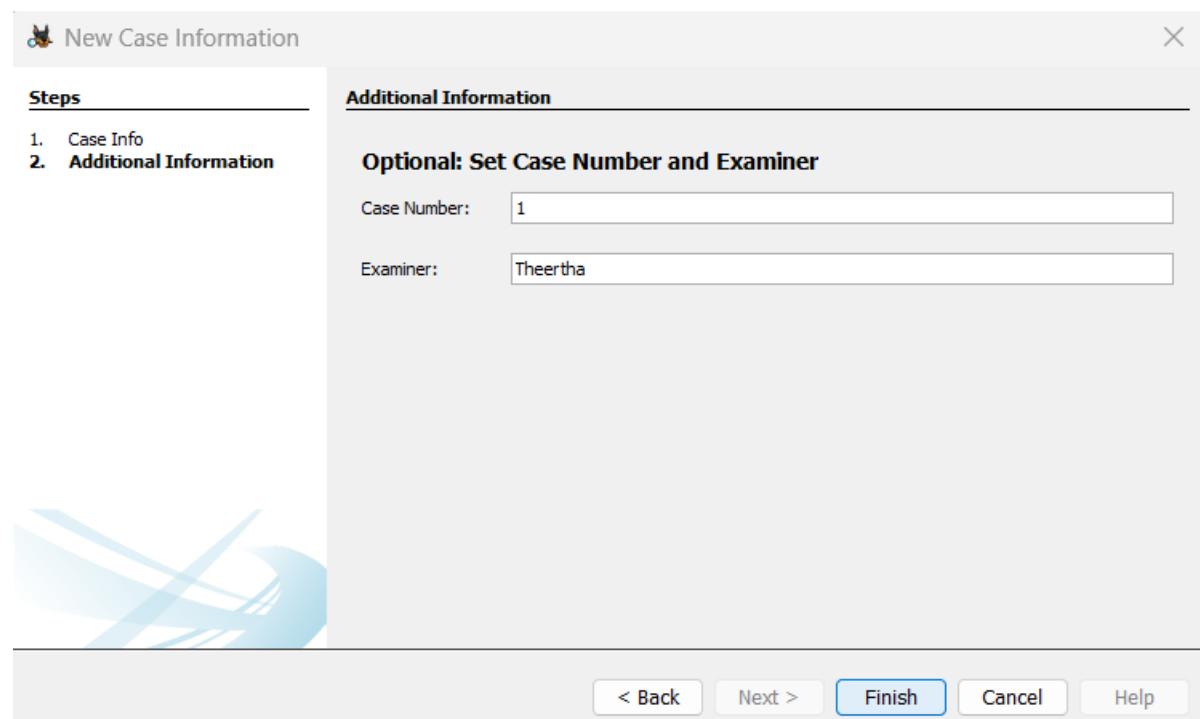
The objective of this lab is to learn how to analyze an image of a Linux hard disk and gather required evidence from it.



Autopsy is a widely used open-source digital forensics tool that helps investigators analyze and recover data from storage devices in criminal, civil, and cybersecurity investigations. It provides a graphical user interface (GUI) for The Sleuth Kit (TSK), making it easier to perform various forensic tasks.

Start by creating a new case and specifying details like case name, number, and investigator.

A screenshot of the 'New Case Information' window. The title bar says 'New Case Information' with a close button 'X'. On the left, a sidebar titled 'Steps' shows '1. Case Info' and '2. Additional Information' as completed steps. The main area is titled 'Case Info' and contains the following fields:  
Case Name:   
Base Directory:    
Case Type:  Single-user  Multi-user  
Case data will be stored in the following directory:  
  
At the bottom are buttons: '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.

A screenshot of the 'Additional Information' window. The title bar says 'New Case Information' with a close button 'X'. On the left, a sidebar titled 'Steps' shows '1. Case Info' and '2. Additional Information' as completed steps. The main area is titled 'Additional Information' and contains the following fields:  
Optional: Set Case Number and Examiner  
Case Number:   
Examiner:   
At the bottom are buttons: '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.

Add the evidence source, such as a disk image, physical drive, or logical files.

 Add Data Source

**Steps**

- 1. Enter Data Source Information**
- Configure Ingest Modules
- Add Data Source

**Enter Data Source Information wizard (Step 1 of 3)**

Select source type to add: **Image File**

Browse for an image file:  
C:\Users\user\Downloads\ntfs-img-kw-1.dd

Please select the input timezone: **(GMT+5:30) Asia/Calcutta**

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

Press 'Next' to analyze the input data, extract volume and file system data, and populate a local database.

< Back  Finish Cancel Help

 Add Data Source

**Steps**

- Enter Data Source Information
- 2. Configure Ingest Modules**
- Add Data Source

**Configure Ingest Modules wizard (Step 2 of 3)**

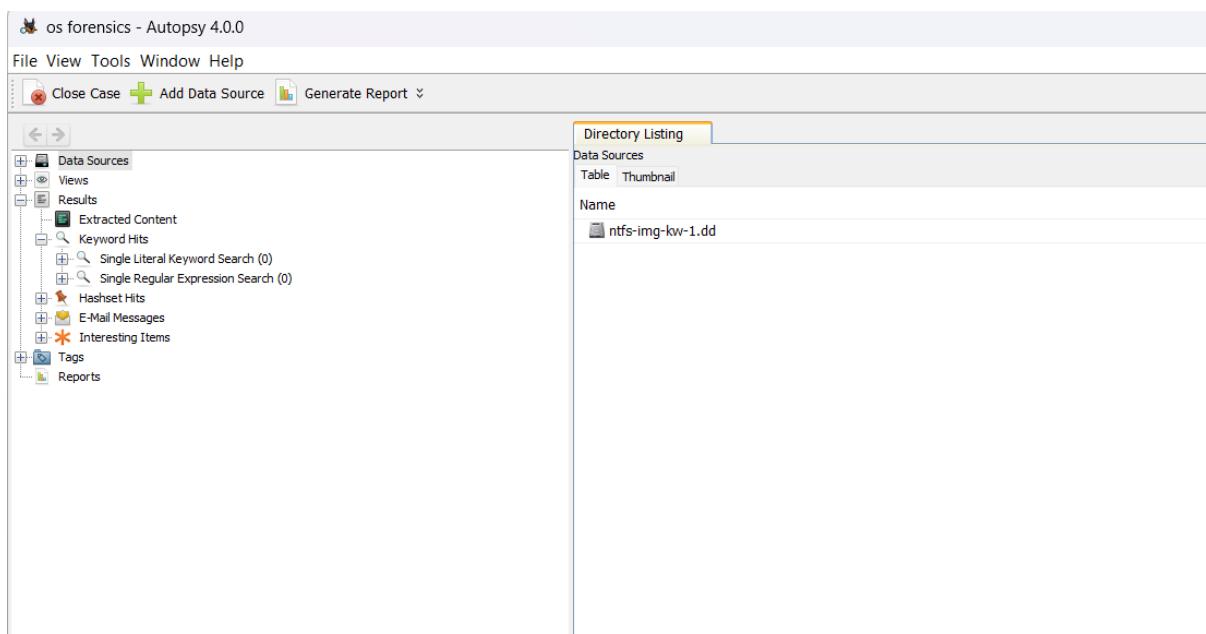
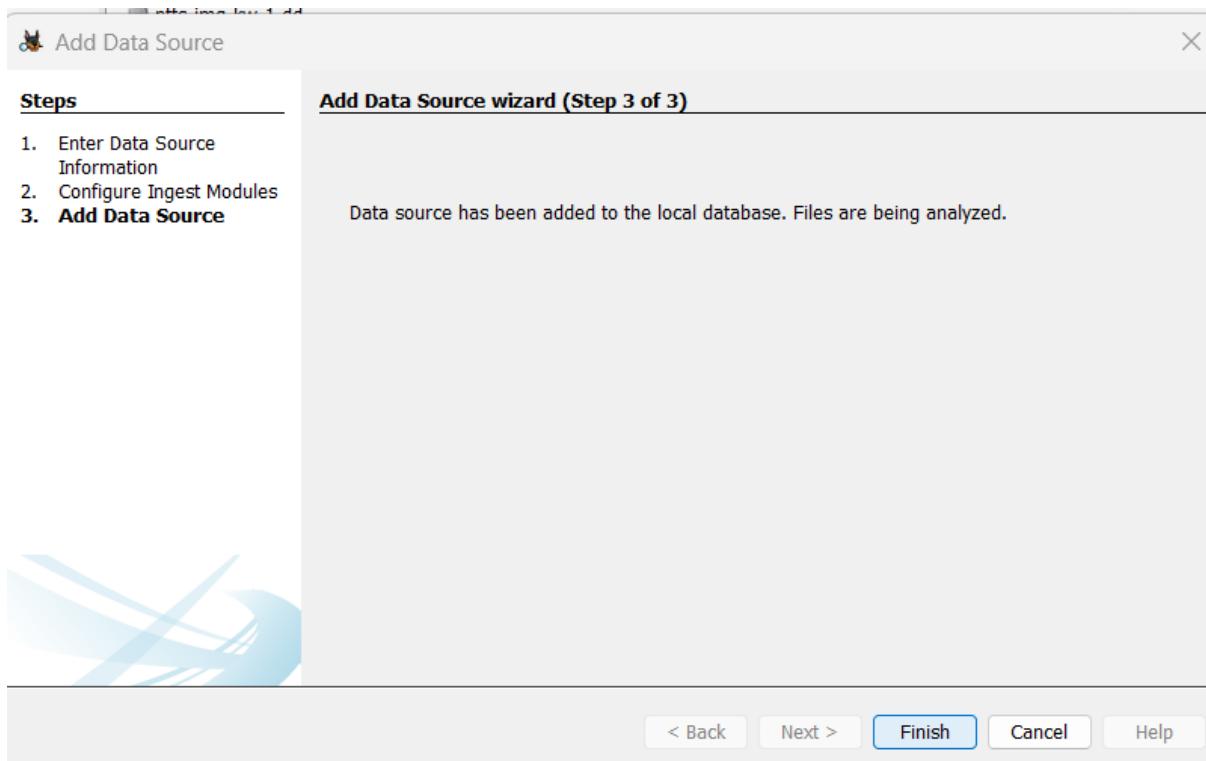
Configure the ingest modules you would like to run on this data source.

Recent Activity  
Hash Lookup  
File Type Identification  
Embedded File Extractor  
Exif Parser  
Keyword Search  
Email Parser  
Extension Mismatch Detector  
E01 Verifier  
 **Android Analyzer**  
 Interesting Files Identifier  
 PhotoRec Carver

Select All Deselect All  Process Unallocated Space

Extracts Android system and thir... Advanced

< Back  Finish Cancel Help



os forensics - Autopsy 4.0.0

File View Tools Window Help

Close Case Add Data Source Generate Report

Directory Listing /img\_ntfs-ing-kw-1.dd

Name	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(M)
file-r-2.dat	2003-10-23 12:32:00 IST	2003-10-24 21:57:35 IST	2003-10-24 21:57:35 IST	2003-10-24 21:57:35 IST	120	Unallocated	Unalloc
\$Extend	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	344	Allocated	Allocat
\$OrphanFiles	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocat
\$Unalloc	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocat
[current folder]	2003-10-24 21:57:57 IST	2003-10-24 21:57:57 IST	2003-10-24 21:57:57 IST	2003-10-24 21:57:57 IST	56	Allocated	Allocat
dir-n-6	2003-10-23 22:49:30 IST	2003-10-23 22:49:30 IST	2003-10-23 22:49:30 IST	2003-10-23 22:49:30 IST	48	Allocated	Allocat
dir-r-4	2003-10-23 22:46:19 IST	2003-10-23 22:46:19 IST	2003-10-23 22:46:19 IST	2003-10-23 22:46:19 IST	48	Allocated	Allocat
System Volume Information	2003-10-24 21:56:41 IST	2003-10-24 21:56:41 IST	2003-10-24 21:56:41 IST	2003-10-24 21:56:41 IST	440	Allocated	Allocat
\$AttribDef	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2560	Allocated	Allocat
\$BadClus	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	0	Allocated	Allocat
\$BadClus:\$Bad	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	8224768	Allocated	Allocat
\$Bitmap	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2008	Allocated	Allocat
\$Boot	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	8192	Allocated	Allocat
\$LogFile	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2097152	Allocated	Allocat
\$MFT	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	39936	Allocated	Allocat
\$MFTMirr	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	4096	Allocated	Allocat
\$Secure:\$SDS	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	264040	Allocated	Allocat
\$UpCase	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	131072	Allocated	Allocat
\$Volume	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	0	Allocated	Allocat
file-n-1.dat	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocat

os forensics - Autopsy 4.0.0

File View Tools Window Help

Close Case Add Data Source Generate Report

Directory Listing /img\_ntfs-ing-kw-1.dd/System Volume Information

Name	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Mode
[current folder]	2003-10-24 21:56:41 IST	2003-10-24 21:56:41 IST	2003-10-24 21:56:41 IST	2003-10-23 22:45:55 IST	440	Allocated	Allocated	dr-xr-xr-x
[parent folder]	2003-10-24 21:57:57 IST	2003-10-24 21:57:57 IST	2003-10-24 21:57:57 IST	2003-10-23 22:42:59 IST	56	Allocated	Allocated	dr-xr-xr-x
_restore(A25F48CA-6632-4143-8E98-000000000000)	2003-10-23 22:45:56 IST	2003-10-23 22:45:56 IST	2003-10-23 22:45:56 IST	2003-10-23 22:45:55 IST	48	Allocated	Allocated	drwxrwxrwx
tracking.log	2003-10-24 21:58:13 IST	2003-10-24 21:58:13 IST	2003-10-24 21:58:13 IST	2003-10-24 21:56:40 IST	20480	Allocated	Allocated	rr-xr-xr-x

Hex Strings File Metadata Results Indexed Text Media

Page: 1 of 1 Page: Go to Page: Jump to Offset: 0

```

0x00000000: 30 00 00 00 01 00 00 00 00 20 00 00 08 00 00 00 0
0x00000010: 10 00 00 00 A8 01 00 00 A8 01 00 00 00 00 00 00 00 0
0x00000020: 1C 00 00 00 00 00 AE 67 70 00 5A 00 00 00 00 00 00 0
0x00000030: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0
0x00000040: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0
0x00000050: 50 0F E5 D1 4B 5A C3 01 00 00 00 00 00 00 00 00 00 0
0x00000060: 50 0F E5 D1 4B 5A C3 01 00 00 00 00 00 00 00 00 00 0
0x00000070: 0C 03 74 00 72 00 E1 00 00 00 E9 00 E9 00 E9 00 E9 00 0
0x00000080: E7 00 2E 00 E6 00 E7 00 E6 00 34 00 38 00 00 00 00 00 0
0x00000090: 20 00 00 00 00 00 33 E4 B0 00 9E 00 00 00 00 00 00 0
0x000000A0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0
0x000000B0: A0 7C FF 81 89 99 C3 01 A0 7C FF 81 89 99 C3 01 00 00 00 0
0x000000C0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0

```

The file that are marked with a red cross are the deleted files, which have been recovered by Autopsy.

Directory Listing						
/img_ntfs-img-kw-1.dd						
Table		Thumbnail				
Name	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
x_file-r-2.dat	2003-10-23 12:32:00 IST	2003-10-24 21:57:35 IST	2003-10-24 21:57:35 IST	2003-10-24 21:57:35 IST	120	Unallocated
\$Extend	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	344	Allocated
\$OrphanFiles	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated
\$Unalloc	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated
[current folder]	2003-10-24 21:57:57 IST	2003-10-24 21:57:57 IST	2003-10-24 21:57:57 IST	2003-10-23 22:42:59 IST	56	Allocated
dir-n-6	2003-10-23 22:49:30 IST	2003-10-23 22:49:30 IST	2003-10-23 22:49:30 IST	2003-10-23 22:49:01 IST	48	Allocated
dir-r-4	2003-10-23 22:46:19 IST	2003-10-23 22:46:19 IST	2003-10-23 22:46:19 IST	2003-10-23 22:45:55 IST	48	Allocated
System Volume Information	2003-10-24 21:56:41 IST	2003-10-24 21:56:41 IST	2003-10-24 21:56:41 IST	2003-10-23 22:45:55 IST	440	Allocated
\$AttrDef	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2560	Allocated
\$BadClus	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	0	Allocated
\$BadClus:\$Bad	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	8224768	Allocated
\$Bitmap	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2008	Allocated
\$Boot	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	8192	Allocated
\$LogFile	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2097152	Allocated
\$MFT	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	39936	Allocated
\$MFTMirr	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	4096	Allocated
\$Secure:\$SDS	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	264040	Allocated
\$UpCase	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	131072	Allocated
\$Volume	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	0	Allocated
file-r-1.dat	2003-10-23 12:34:14 IST	2003-10-23 22:47:50 IST	2003-10-23 22:47:50 IST	2003-10-23 22:47:50 IST	20000	Allocated

Directory Listing						
/img_ntfs-img-kw-1.dd						
Table		Thumbnail				
Name	Modified Time	Change Time	Access Time	Created Time	Size	
x_file-r-2.dat	2003-10-23 12:32:00 IST	2003-10-24 21:57:35 IST	2003-10-24 21:57:35 IST	2003-10-24 21:57:35 IST	120	
\$Extend	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	344	
\$OrphanFiles	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	
\$Unalloc	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	
[current folder]	2003-10-24 21:57:57 IST	2003-10-24 21:57:57 IST	2003-10-24 21:57:57 IST	2003-10-23 22:42:59 IST	56	
dir-n-6	2003-10-23 22:49:30 IST	2003-10-23 22:49:30 IST	2003-10-23 22:49:30 IST	2003-10-23 22:49:01 IST	48	
dir-r-4	2003-10-23 22:46:19 IST	2003-10-23 22:46:19 IST	2003-10-23 22:46:19 IST	2003-10-23 22:45:55 IST	48	
System Volume Information	2003-10-24 21:56:41 IST	2003-10-24 21:56:41 IST	2003-10-24 21:56:41 IST	2003-10-23 22:45:55 IST	440	
\$AttrDef	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2560	
\$BadClus	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	0	
\$BadClus:\$Bad	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	8224768	
\$Bitmap	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2008	
\$Boot	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	8192	
\$LogFile	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2097152	
\$MFT	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	39936	
\$MFTMirr	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	4096	
\$Secure:\$SDS	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	264040	
\$UpCase	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	131072	
\$Volume	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	2003-10-23 22:42:59 IST	0	
file-r-1.dat	2003-10-23 12:34:14 IST	2003-10-23 22:47:50 IST	2003-10-23 22:47:50 IST	2003-10-23 22:47:50 IST	20000	

Hex	Strings	File Metadata	Results	Indexed Text	Media

Name	/img_ntfs-img-kw-1.dd//\$Unalloc
Type	Virtual Directory
Size	0
File Name Allocation	Allocated
Metadata Allocation	Allocated
Modified	0000-00-00 00:00:00
Accessed	0000-00-00 00:00:00
Created	0000-00-00 00:00:00

Directory Listing

Name	Location	Modified Time	Change Time	Access Time	Create
file-r-2.dat	/img_ntfs-img-kw-1.dd/file-r-2.dat	2003-10-23 12:32:00 IST	2003-10-24 21:57:35 IST	2003-10-24 21:57:35 IST	2003-1

Hex Strings File Metadata Results Indexed Text Media

Page: 1 of 1 Page Go to Page: Jump to Offset 0

```

0x00000000: 24 5C 8E 29 97 81 CC 91 C7 45 CA CC 1A B0 7F 7A $\\.)....E....z
0x00000010: 65 7E 0C 64 EA 10 7C D0 35 81 01 F6 D5 75 D9 74 e~.d..|5....u.t
0x00000020: 0F E9 18 BC 70 E2 B5 4C 45 6A D9 QA DB F0 3B FE .i...p..LEj....;.
0x00000030: 1B E2 A5 19 32 91 F5 21 45 95 E7 82 6B E4 46 DE ...2..!E...k.F.
0x00000040: 8E 04 3F 8A 4C 38 A5 84 86 36 C9 29 75 6A 6A FB ..?L8...6.)ujj.
0x00000050: 96 E3 D4 DE 72 2D 75 6E 61 6C 6C 6F 63 EA EA 0C ....r-unalloc...
0x00000060: 51 9F A9 46 CE A3 DA 2D 1B B5 88 8C 8B 22 FF B5 Q..F....-...."..
0x00000070: AA 72 98 82 99 DC EF 97 .r.....

```

Select result folder from leftpane. It contains sections such as extracted content, keyword hits, hashset hits etc. Analyse these file to look malware files as well as metadata files.

