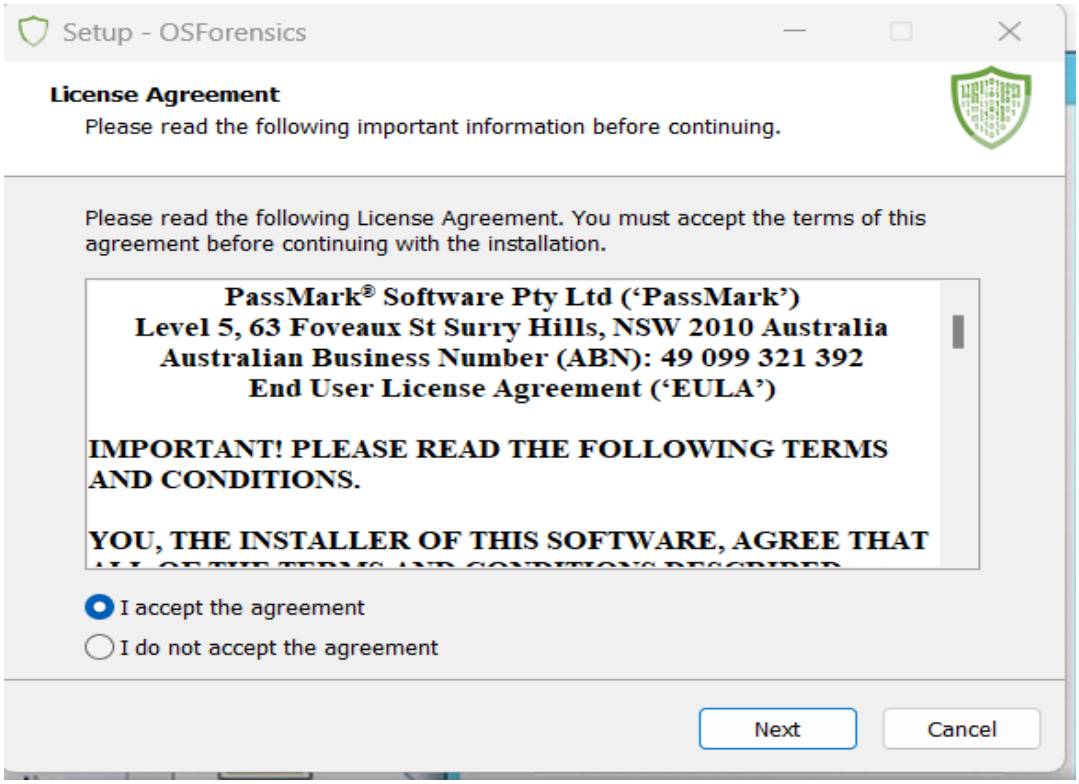
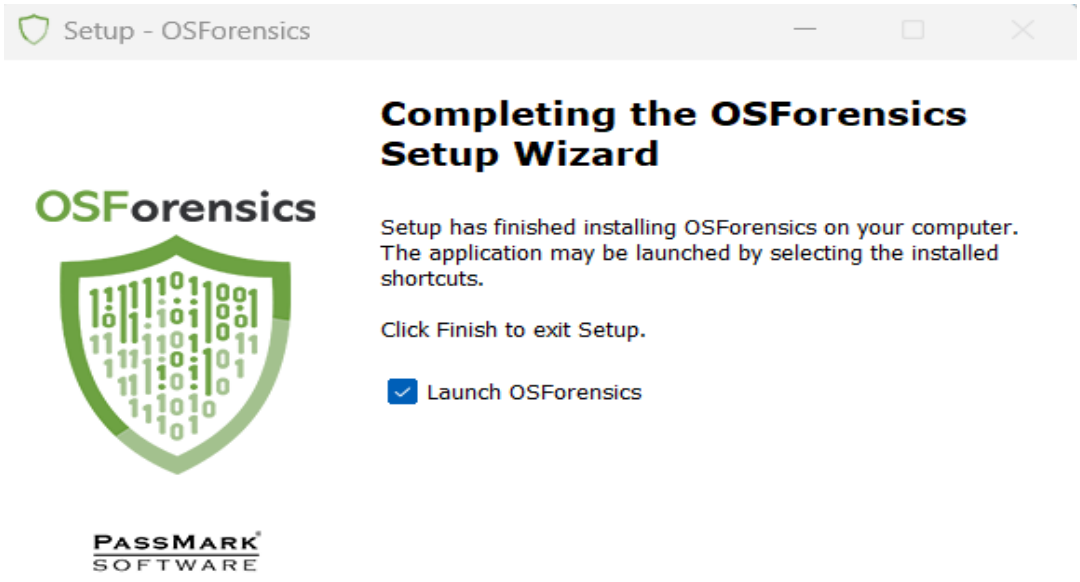
Module-6

Operating System Forensics

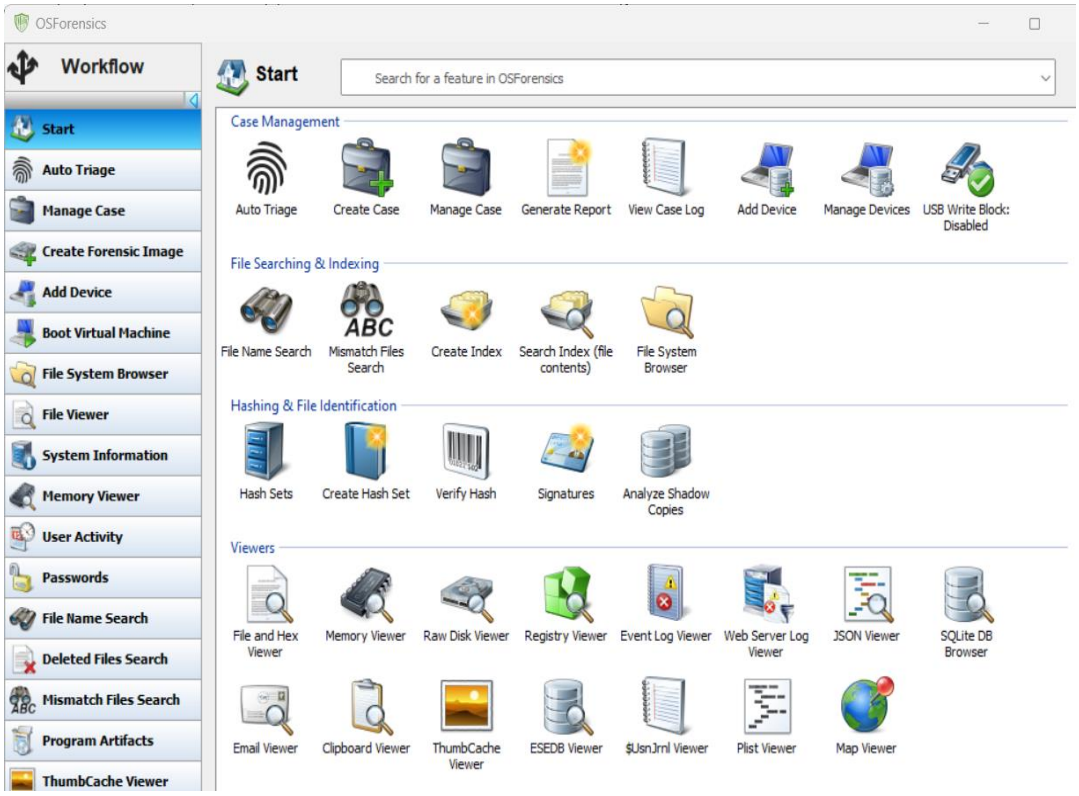
Lab1: Discovering and Extracting Hidden Forensic Material on Computers Using OS Forensics

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.

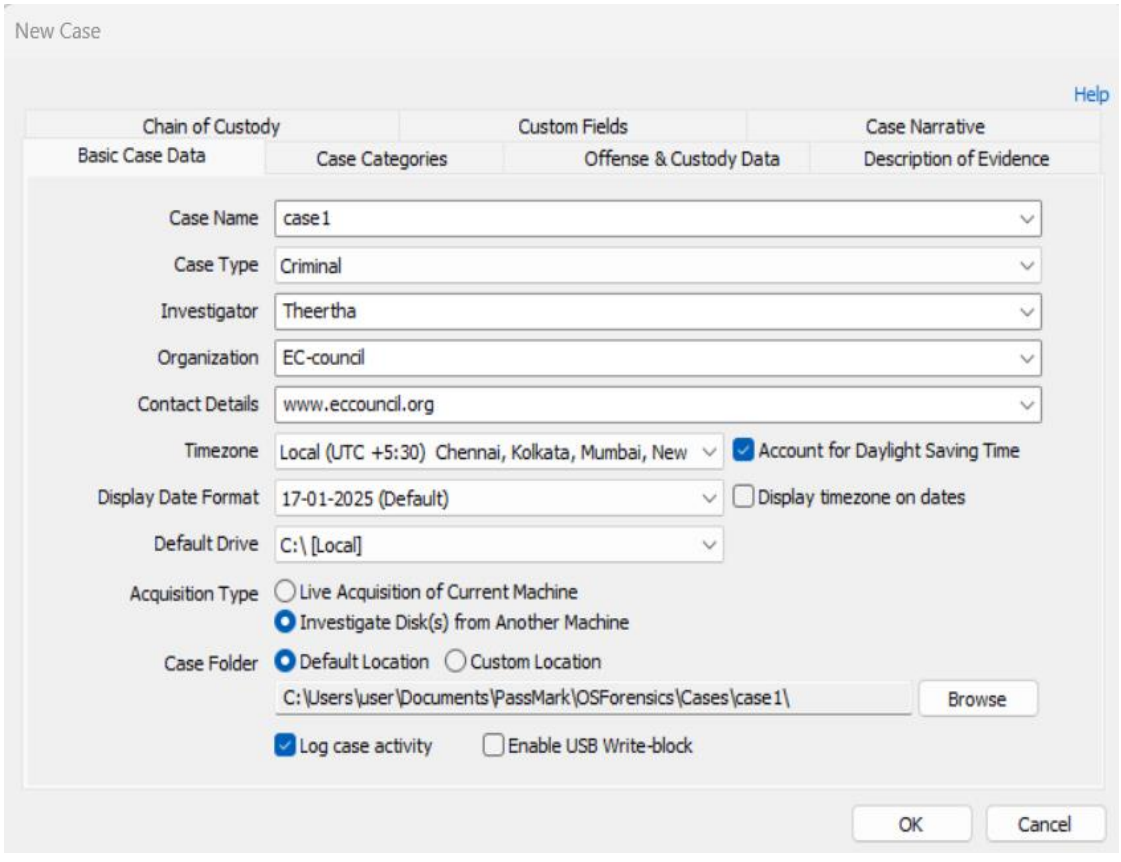



Setup - OSForensics
Completing the OSForensics Setup Wizard
OSForensics
Setup has finished installing OSForensics on your computer. The application may be launched by selecting the installed shortcuts.
Click Finish to exit Setup.
Launch OSForensics
PASSMARK SOFTWARE
Back
Finish

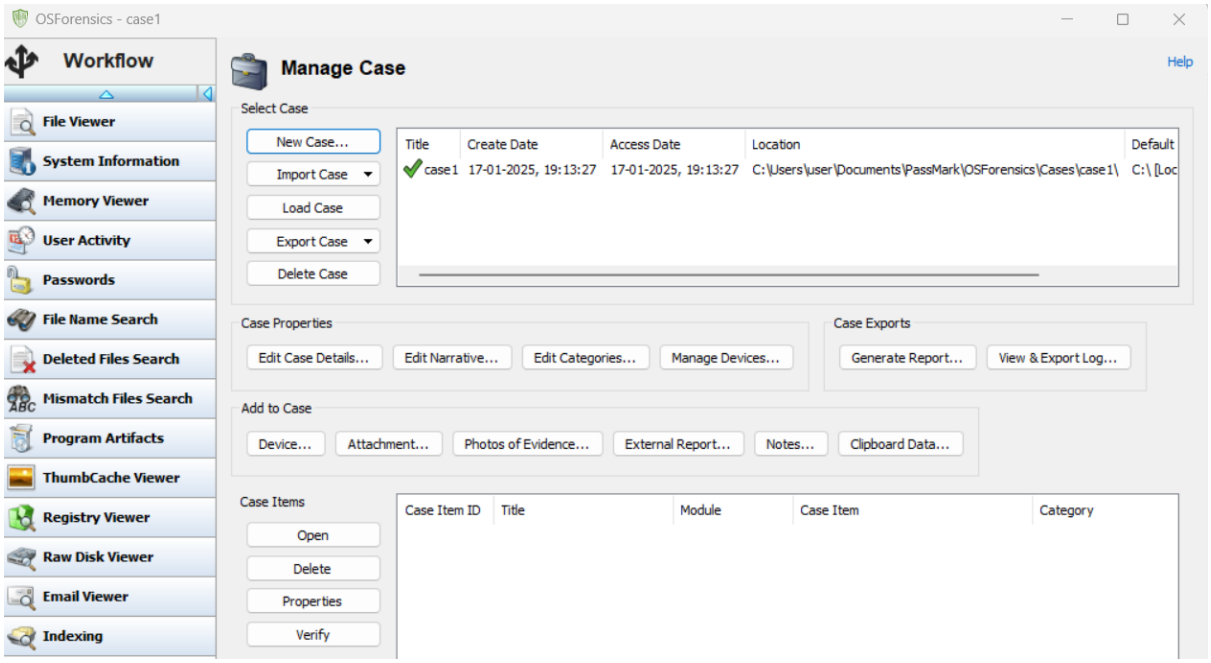

OSForensics
Workflow
Start
Auto Triage
Manage Case
Create Forensic Image
Add Device
Boot Virtual Machine
File System Browser
File Viewer
System Information
Memory Viewer
User Activity
Passwords
File Name Search
Deleted Files Search
Mismatch Files Search
Program Artifacts
PassMark® Software
OSForensics
PassMark Software
www.osforensics.com
Unlicensed trial
Click on Continue for your 30day evaluation
(30 Days left)
Continue Using Trial Version
Upgrade to Professional Version
Exit



Create a new case

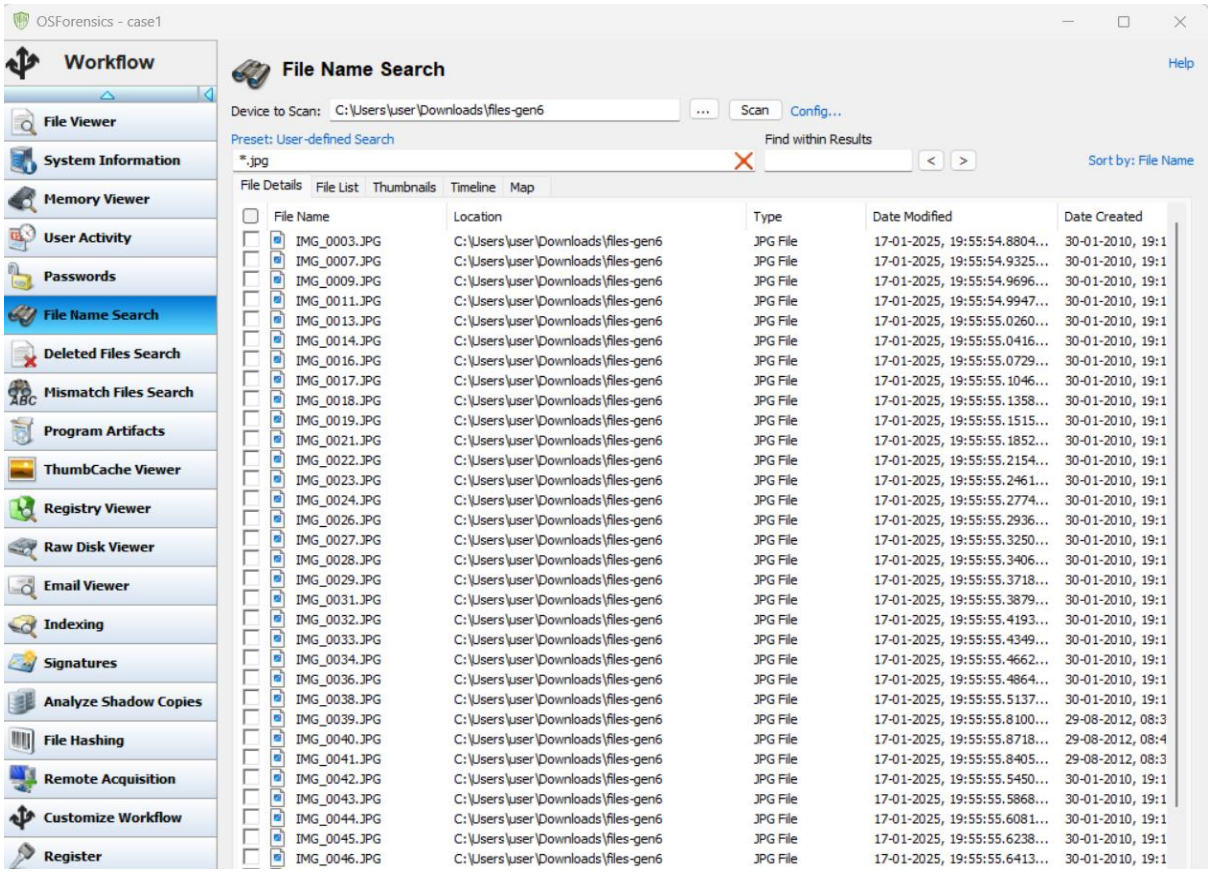


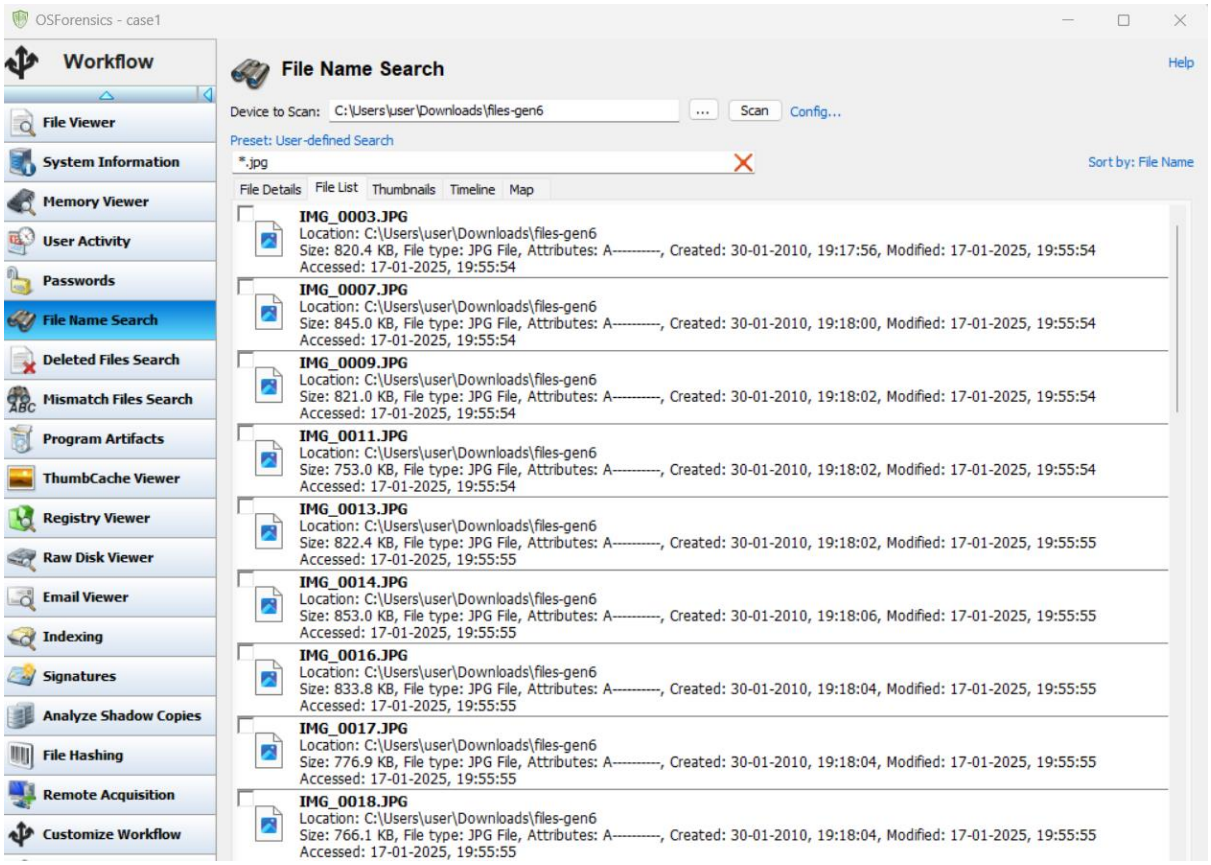
A new case is created.



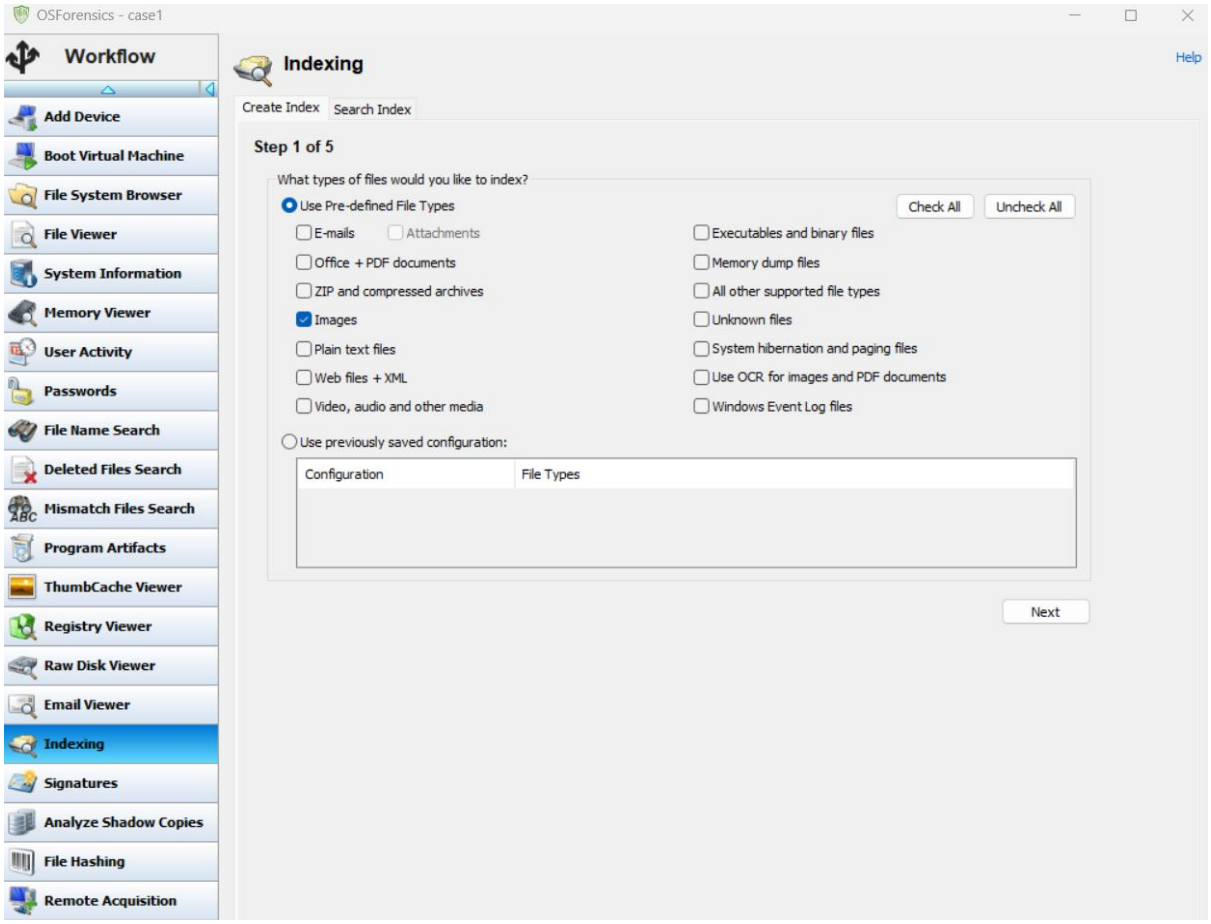
To serach for files , type a filename in the search string.

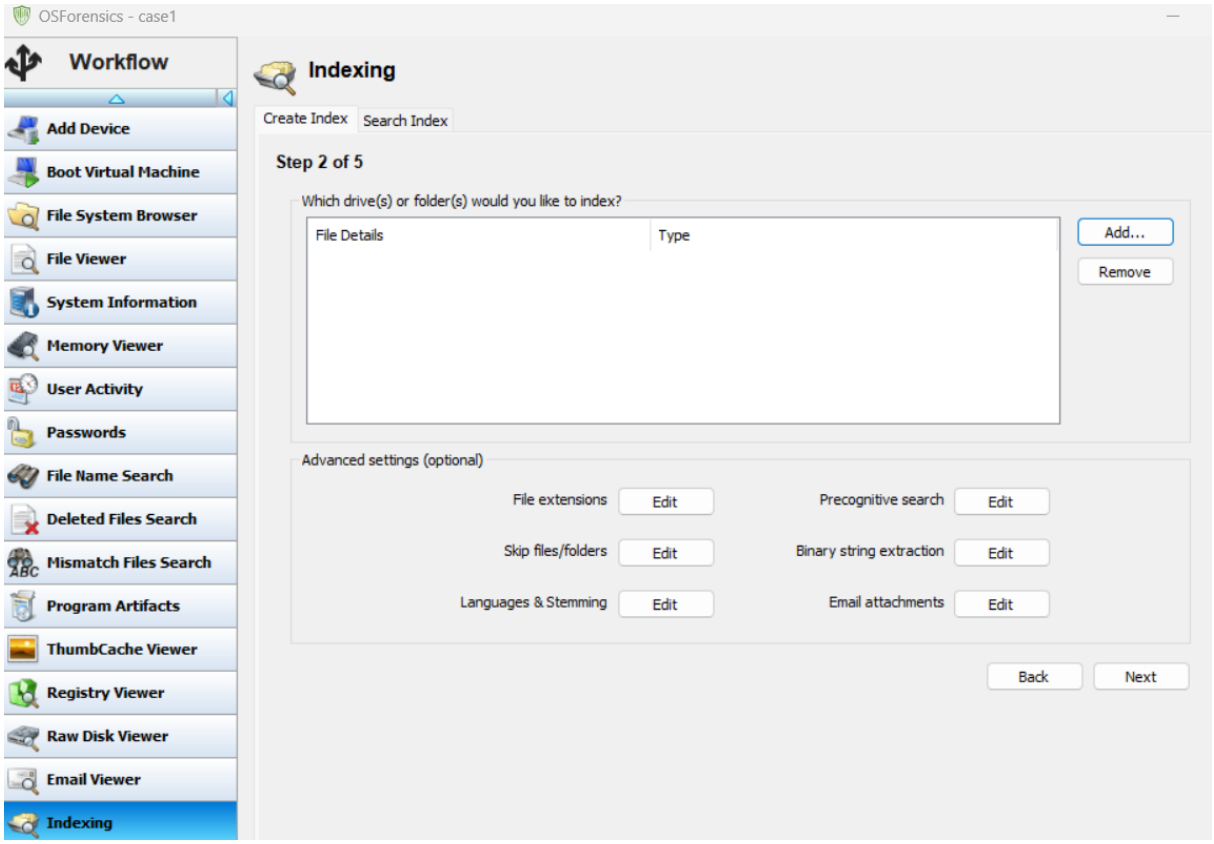
Here we are specifying the location to search for images. This displays all the images present in specified location

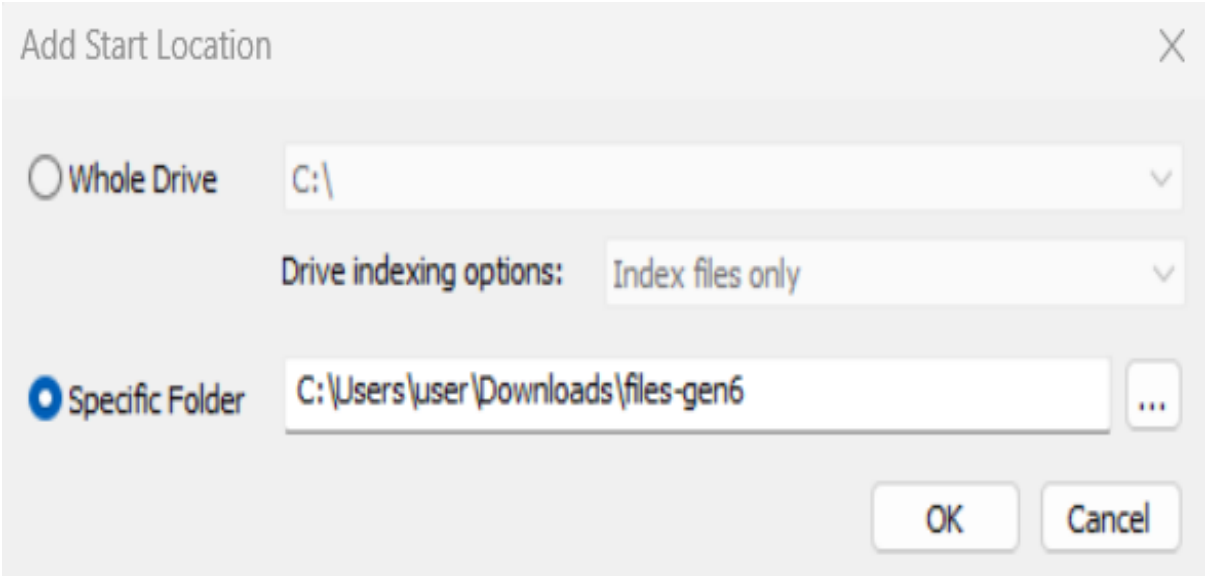


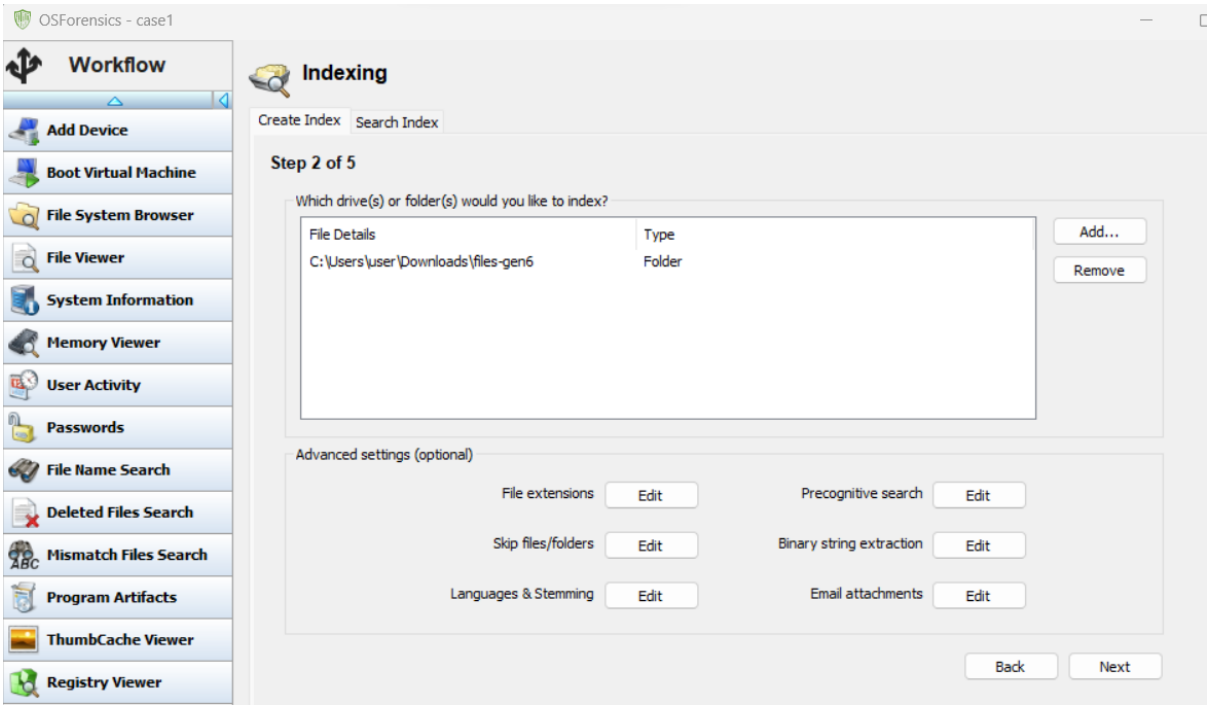


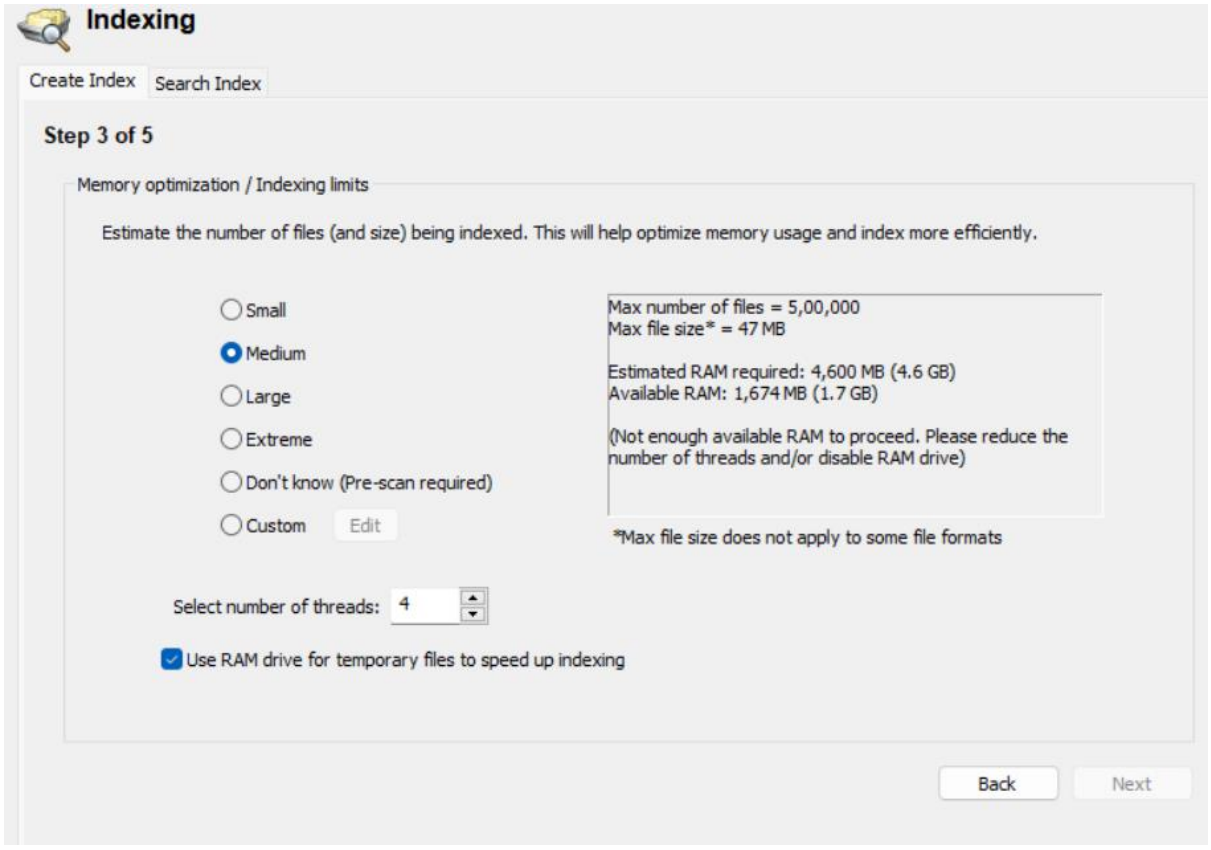
To create an index of the content click create index in the left pane of the window.

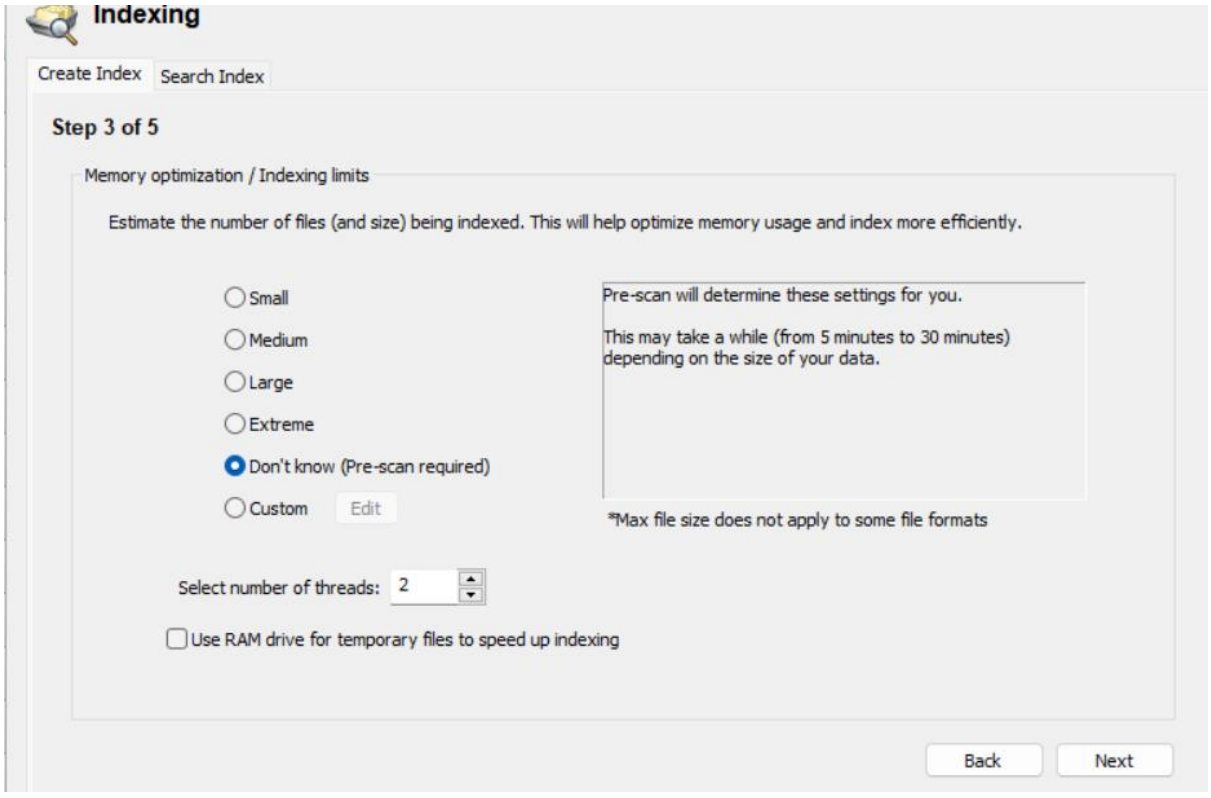

OSForensics - case1
Workflow
Add Device
Boot Virtual Machine
File System Browser
File Viewer
System Information
Memory Viewer
User Activity
Passwords
File Name Search
Deleted Files Search
Mismatch Files Search
Program Artifacts
ThumbCache Viewer
Registry Viewer
Raw Disk Viewer
Email Viewer
Indexing
Signatures
Analyze Shadow Copies
File Hashing
Remote Acquisition
Indexing
Help
Create Index
Search Index
Step 1 of 5
What types of files would you like to index?
Use Pre-defined File Types
Check All
Uncheck All
E-mails
Attachments
Office + PDF documents
ZIP and compressed archives
Images
Plain text files
Web files + XML
Video, audio and other media
Executables and binary files
Memory dump files
All other supported file types
Unknown files
System hibernation and paging files
Use OCR for images and PDF documents
Windows Event Log files
Use previously saved configuration:
Configuration
File Types
Next

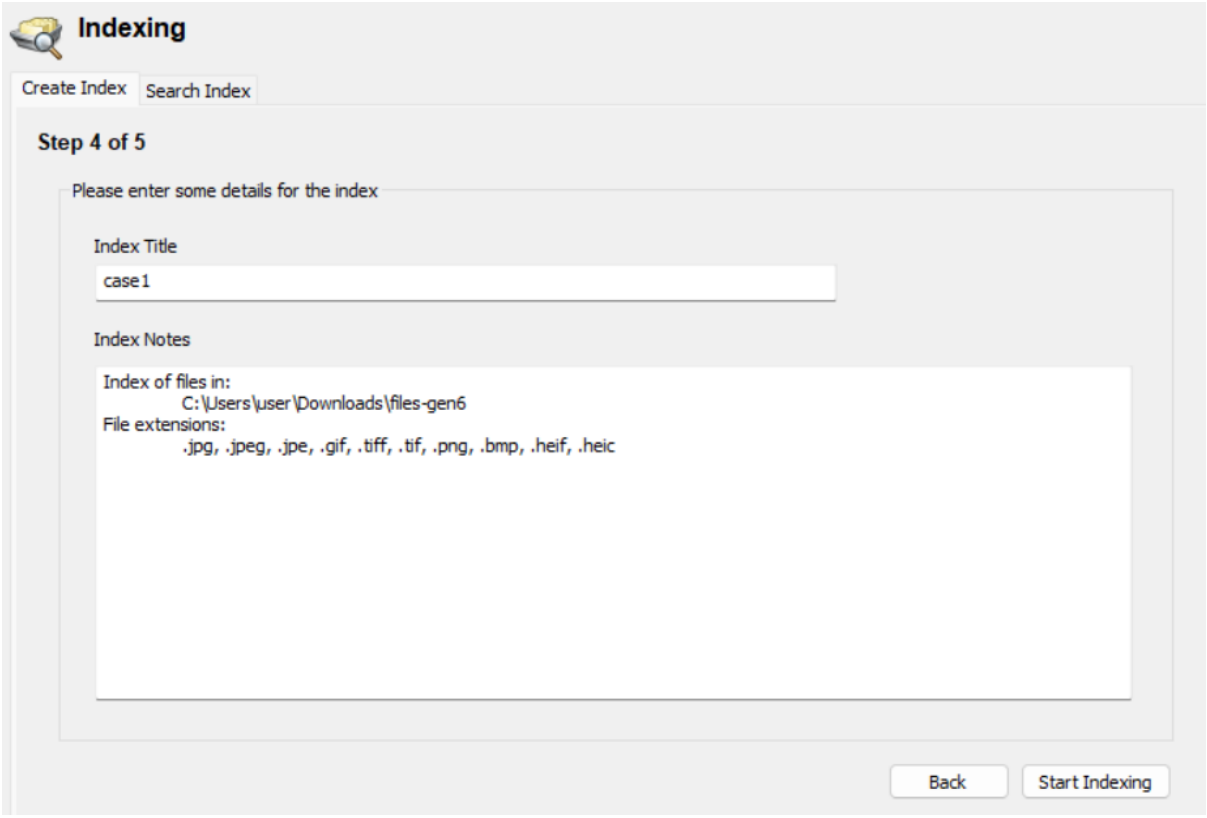

OSForensics - case1
Workflow
Add Device
Boot Virtual Machine
File System Browser
File Viewer
System Information
Memory Viewer
User Activity
Passwords
File Name Search
Deleted Files Search
Mismatch Files Search
Program Artifacts
ThumbCache Viewer
Registry Viewer
Raw Disk Viewer
Email Viewer
Indexing
Indexing
Create Index
Search Index
Step 2 of 5
Which drive(s) or folder(s) would you like to index?
File Details
Type
Add...
Remove
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

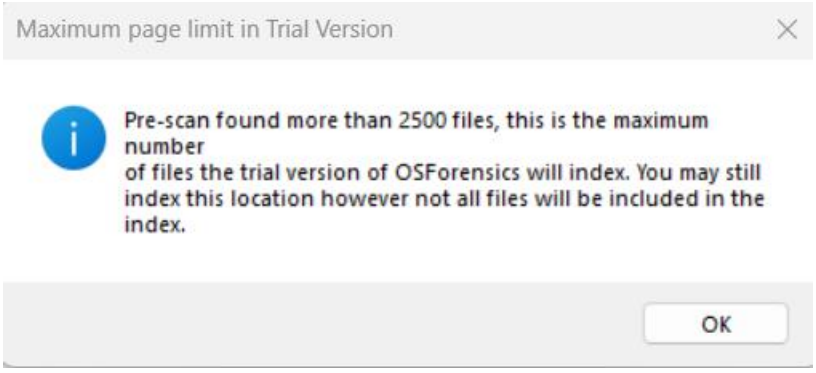

Add Start Location
Whole Drive
C:\
Drive indexing options:
Index files only
Specific Folder
C:\Users\user\Downloads\files-gen6
...
OK
Cancel

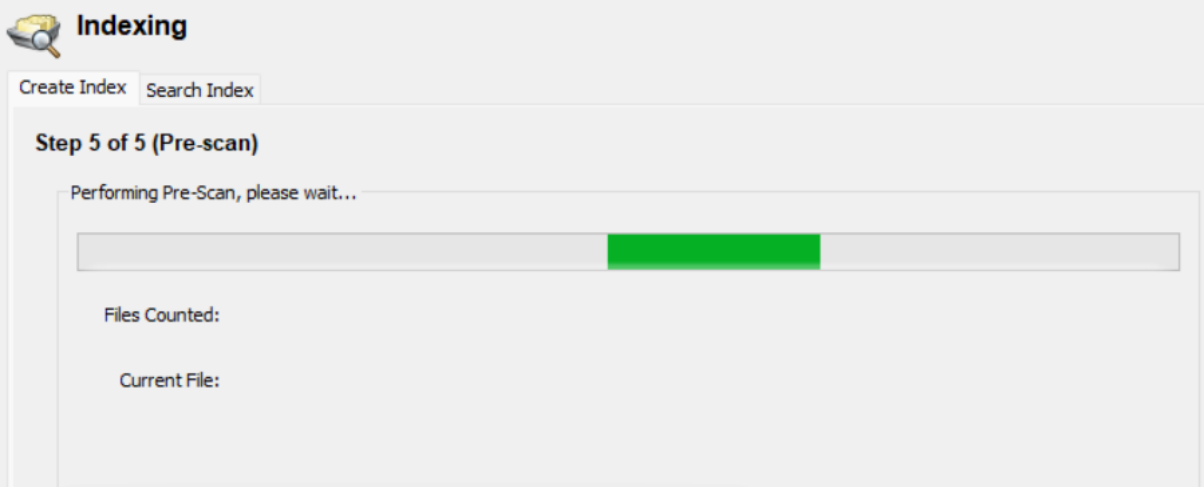

OSForensics - case1
Workflow
Add Device
Boot Virtual Machine
File System Browser
File Viewer
System Information
Memory Viewer
User Activity
Passwords
File Name Search
Deleted Files Search
Mismatch Files Search
Program Artifacts
ThumbCache Viewer
Registry Viewer
Indexing
Create Index
Search Index
Step 2 of 5
Which drive(s) or folder(s) would you like to index?
File Details
Type
C:\Users\user\Downloads\files-gen6
Folder
Add...
Remove
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

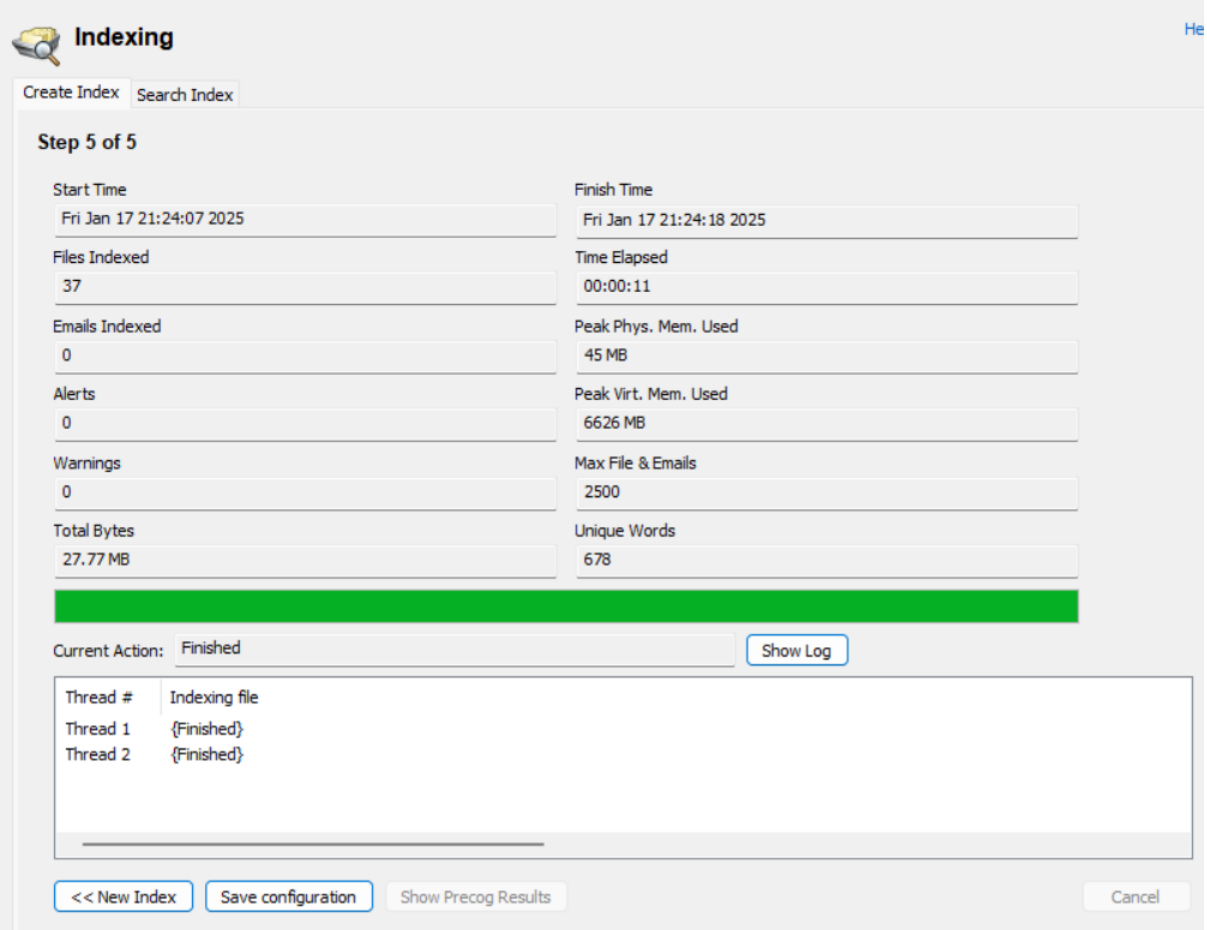

Indexing
Create Index
Search Index
Step 3 of 5
Memory optimization / Indexing limits
Estimate the number of files (and size) being indexed. This will help optimize memory usage and index more efficiently.
Small
Medium
Large
Extreme
Don't know (Pre-scan required)
Custom
Edit
Max number of files = 5,00,000
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: 4
Use RAM drive for temporary files to speed up indexing
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
Edit
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: 2
Use RAM drive for temporary files to speed up indexing
Back
Next

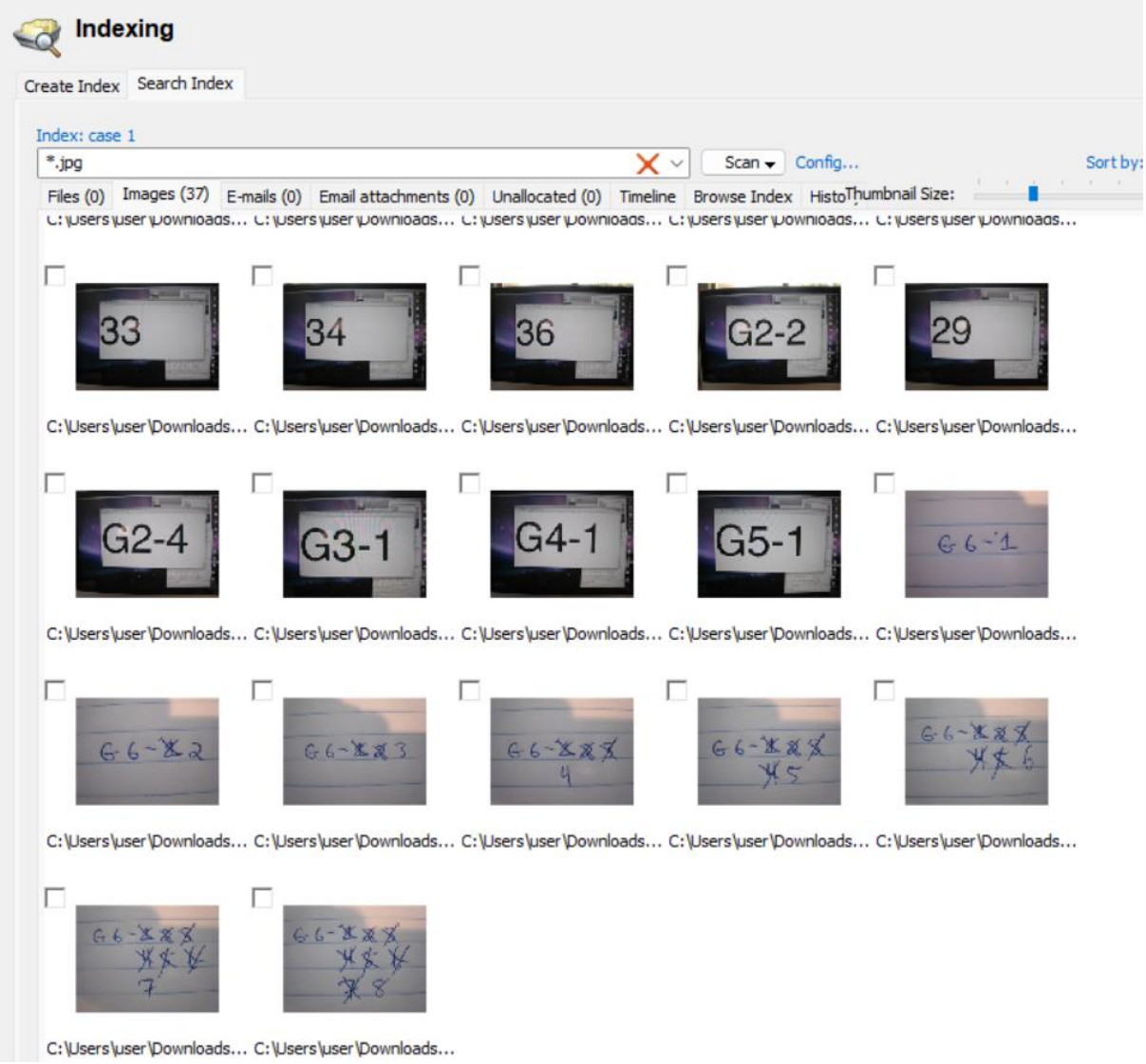

Indexing
Create Index
Search Index
Step 4 of 5
Please enter some details for the index
Index Title
case1
Index Notes
Index of files in:
C:\Users\user\Downloads\files-gen6
File extensions:
.jpg, .jpeg, .jpe, .gif, .tiff, .tif, .png, .bmp, .heif, .heic
Back
Start Indexing


Maximum page limit in Trial Version
Pre-scan found more than 2500 files, this is the maximum number
of files the trial version of OSForensics will index. You may still index this location however not all files will be included in the index.
OK

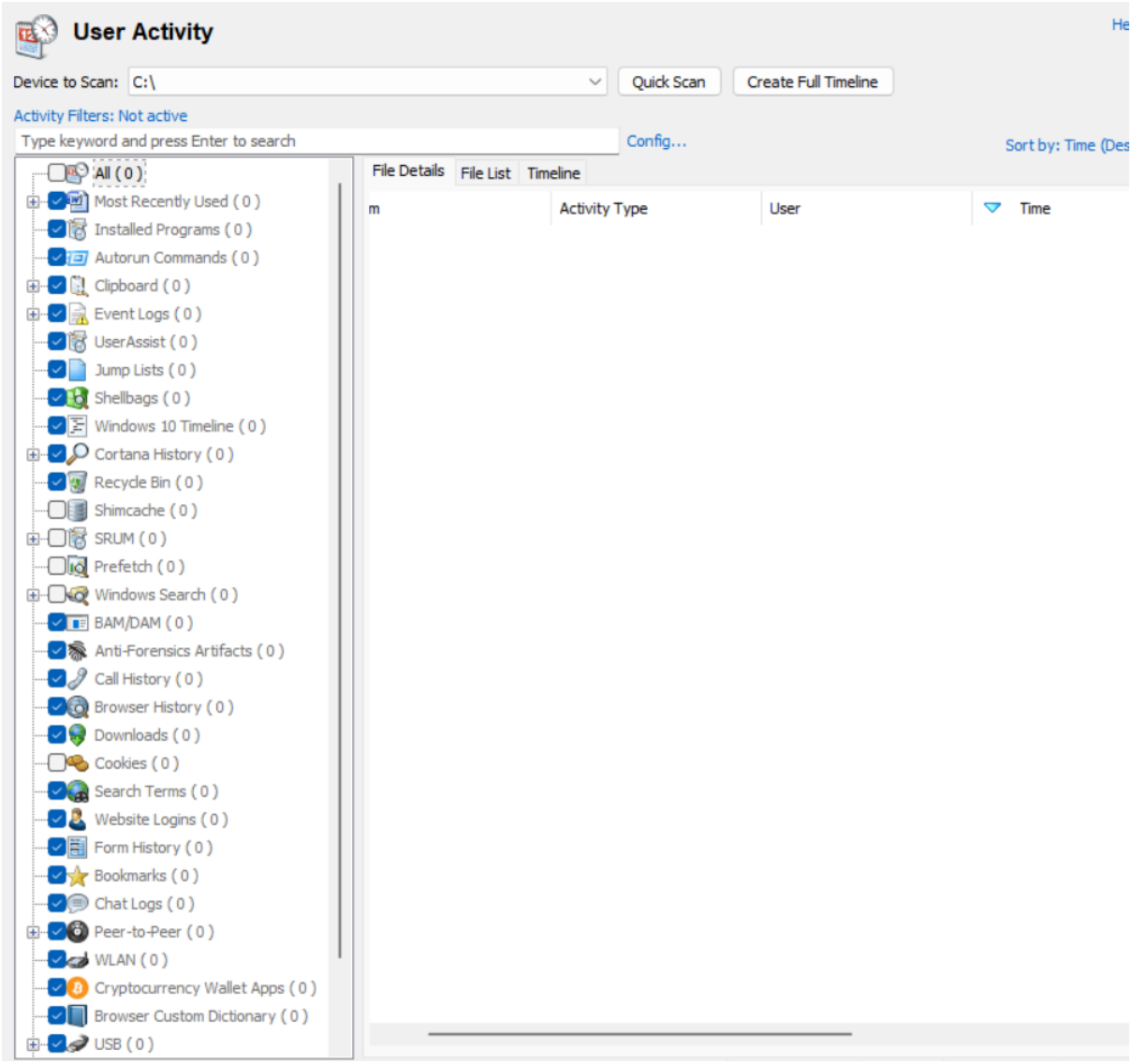


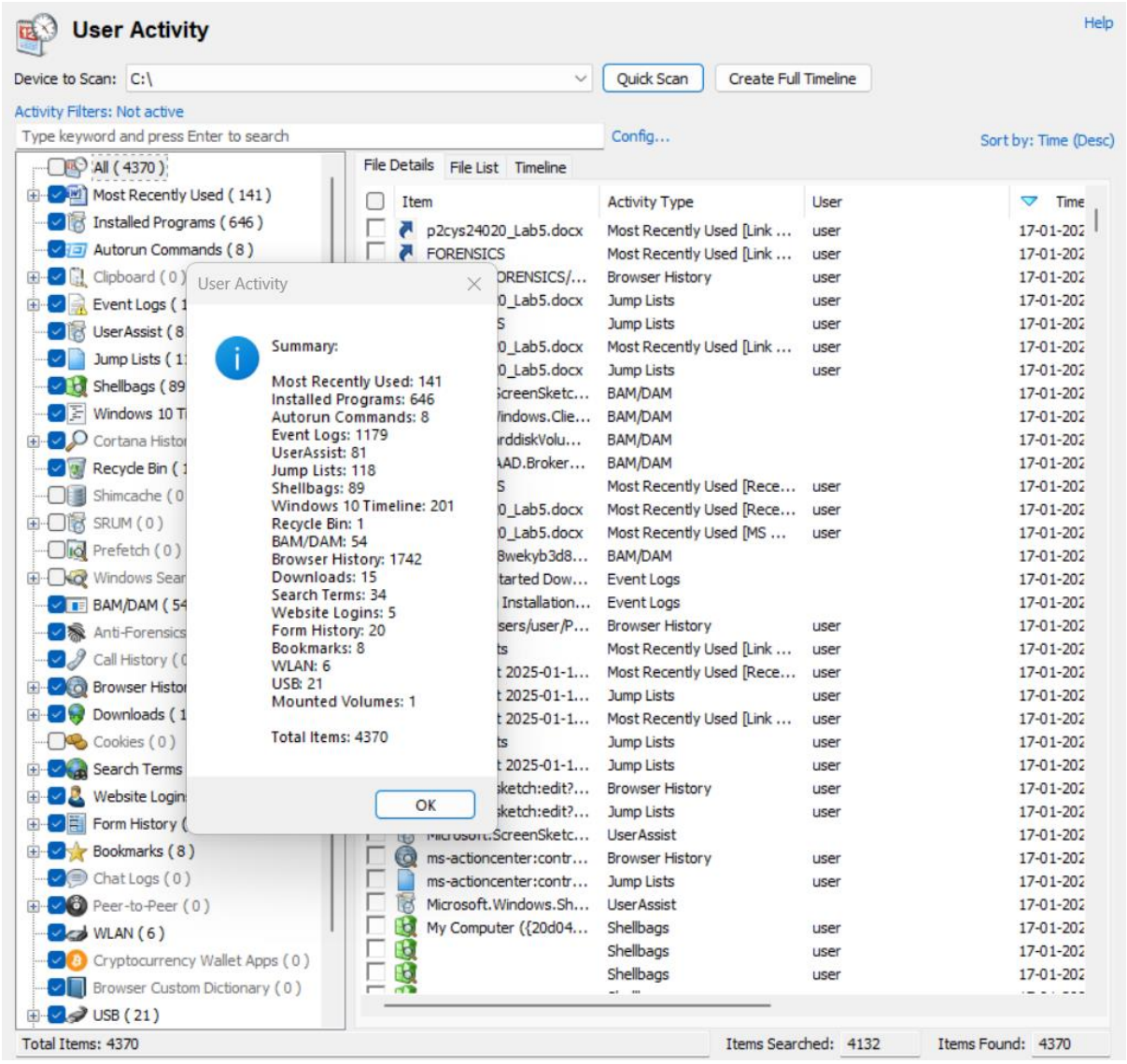


Now the index is created.

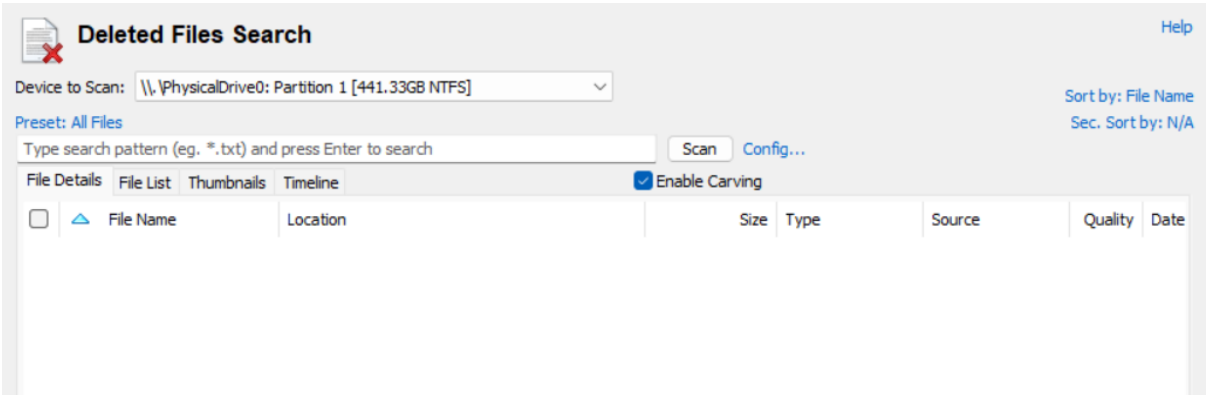


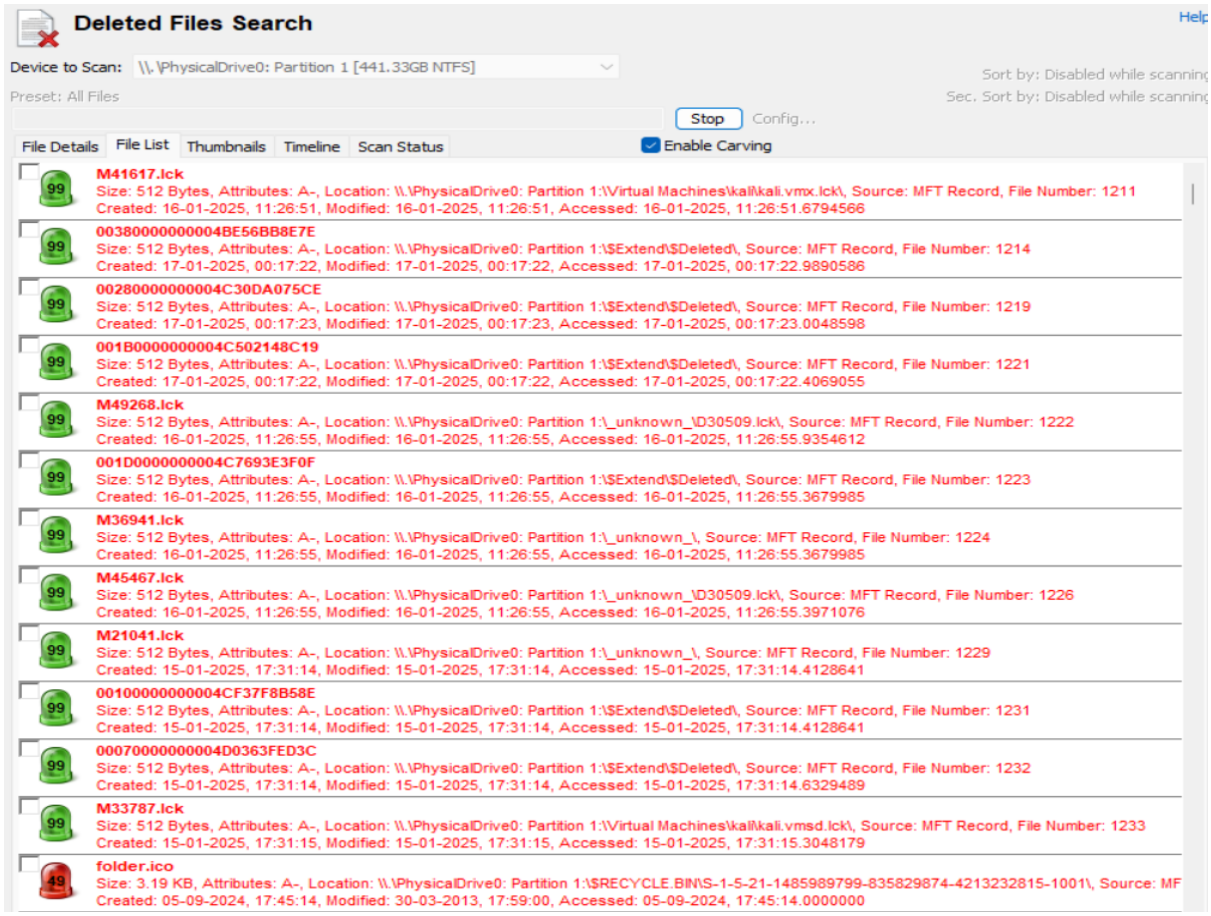
Click user activity to scan for evidence such as browsed websites, USB drives etc.

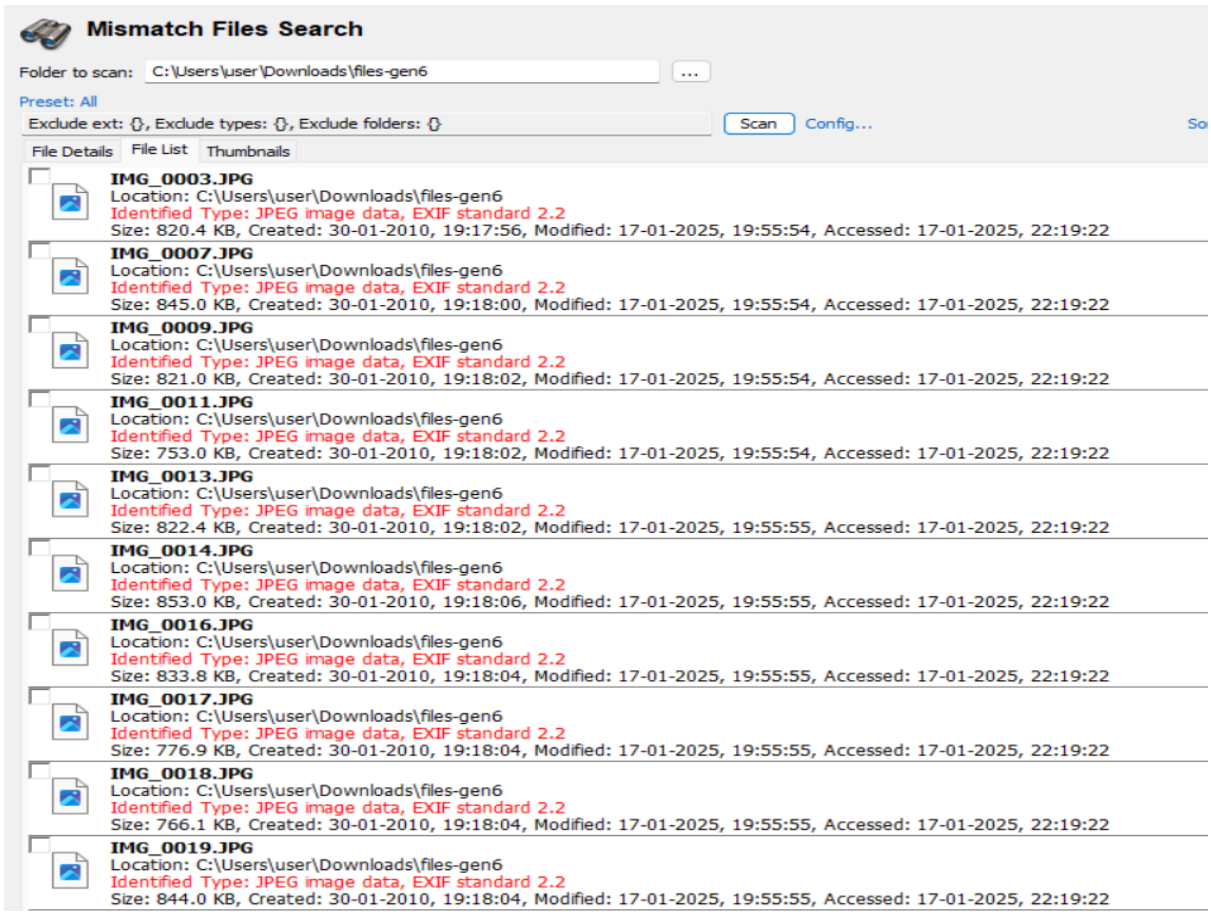

User Activity
Device to Scan: C:\
Quick Scan
Create Full Timeline
Activity Filters: Not active
Type keyword and press Enter to search
Config...
Sort by: Time (Des
All (0)
Most Recently Used (0)
Installed Programs (0)
Autorun Commands (0)
Clipboard (0)
Event Logs (0)
UserAssist (0)
Jump Lists (0)
Shellbags (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
m
Activity Type
User
Time



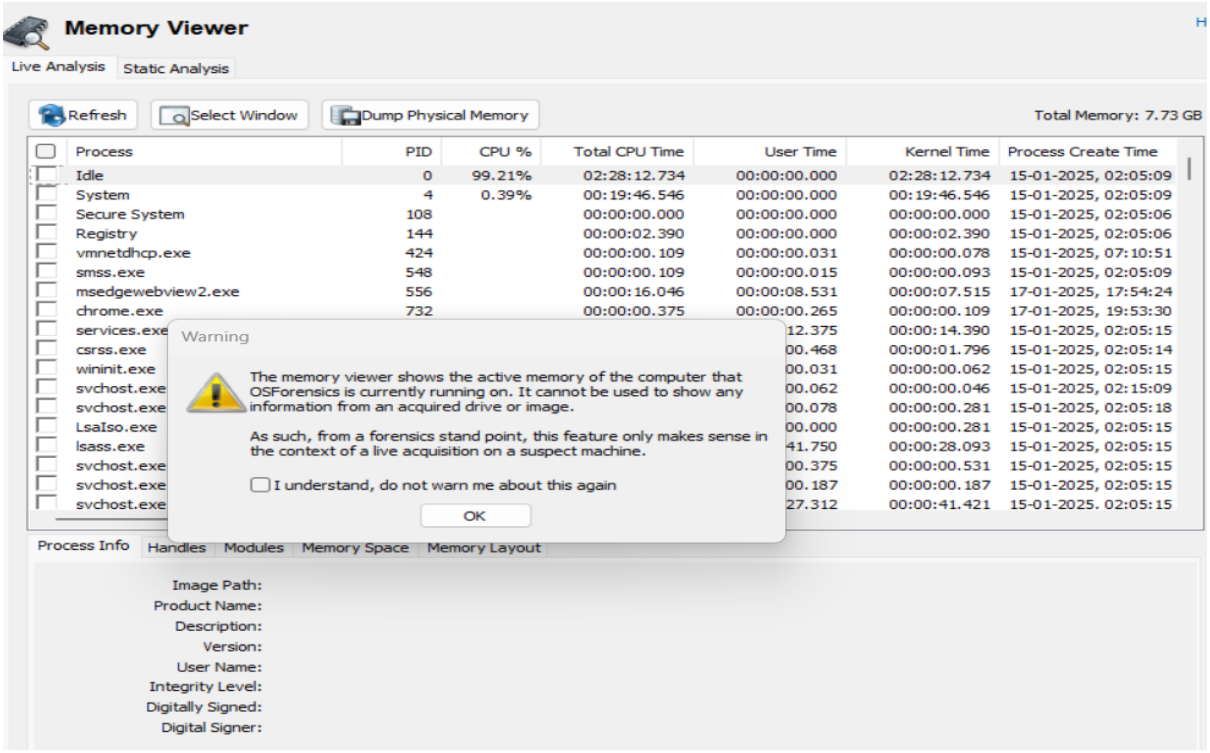
To recover deleted files click deleted files search from the left pane, select a disk.

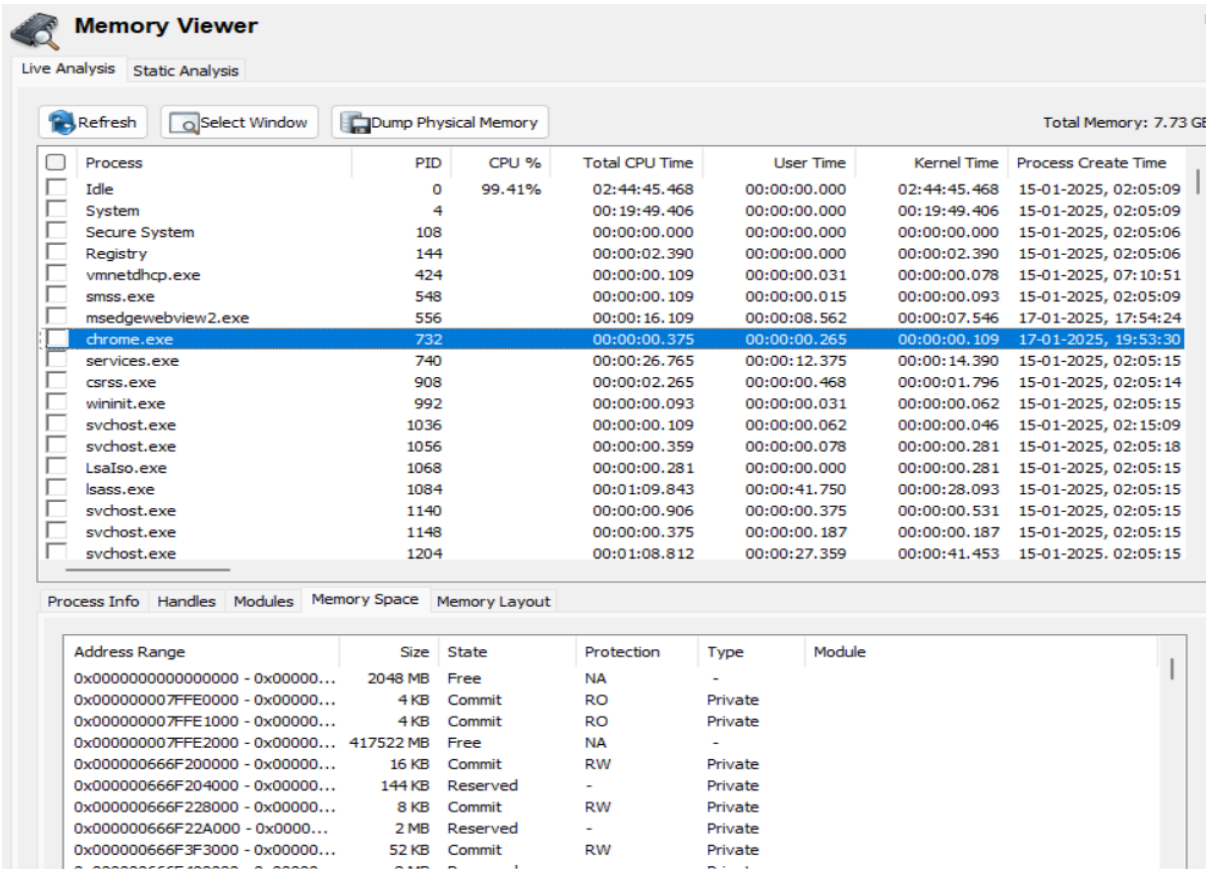



Deleted Files Search
Help
Device to Scan: \\.\PhysicalDrive0: Partition 1 [441.33GB NTFS]
Sort by: Disabled while scanning
Preset: All Files
Sec. Sort by: Disabled while scanning
Stop
Config...
File Details
File List
Thumbnails
Timeline
Scan Status
Enable Carving
M41617.lck
Size: 512 Bytes, Attributes: A-, Location: \\.\PhysicalDrive0: Partition 1:\Virtual Machines\kali\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
00380000000004BE56BB8E7E
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
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
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
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
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
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
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
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
00100000000004CF37F8B58E
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
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
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
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

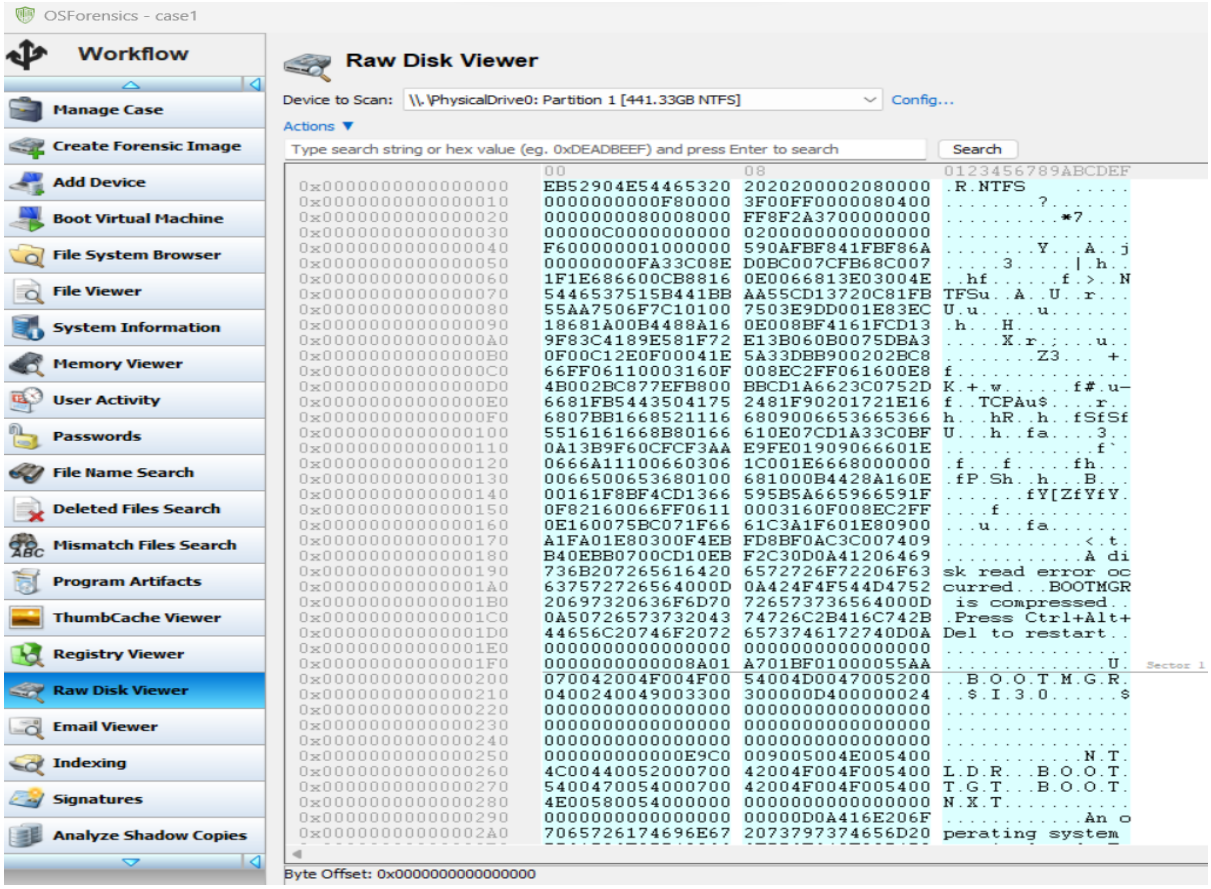

Mismatch Files Search
Folder to scan: C:\Users\user\Downloads\files-gen6
...
Preset: All
Exclude ext: {}, Exclude types: {}, Exclude folders: {}
Scan
Config...
File Details
File List
Thumbnails
IMG_0003.JPG
Location: C:\Users\user\Downloads\files-gen6
Identified Type: JPEG image data, EXIF standard 2.2
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
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
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
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
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
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
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
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
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
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

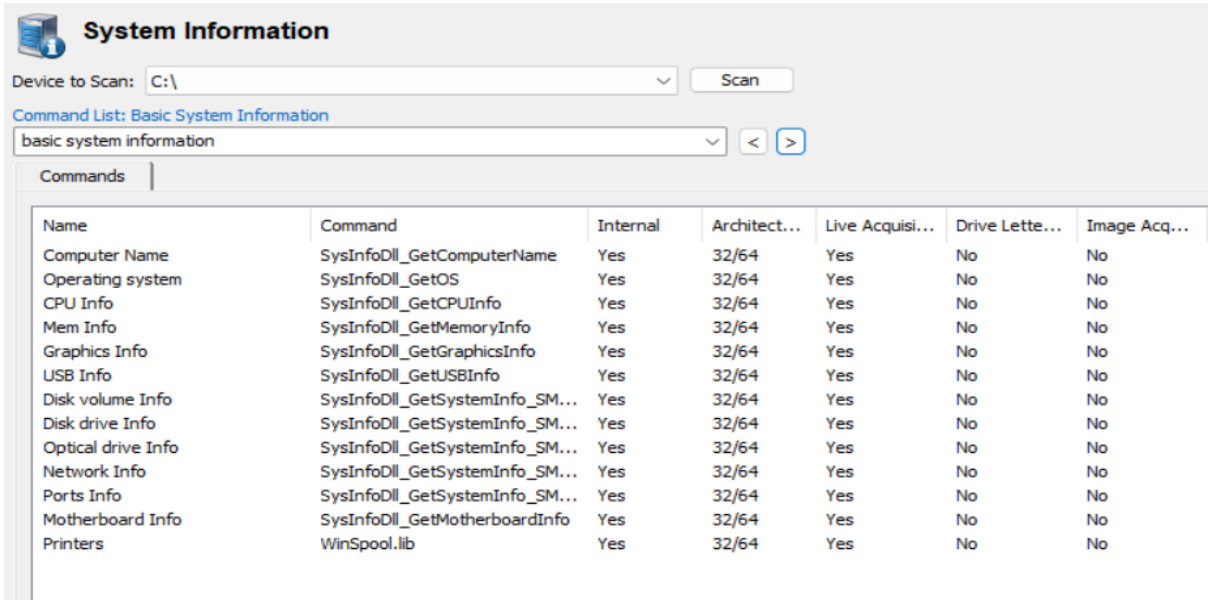




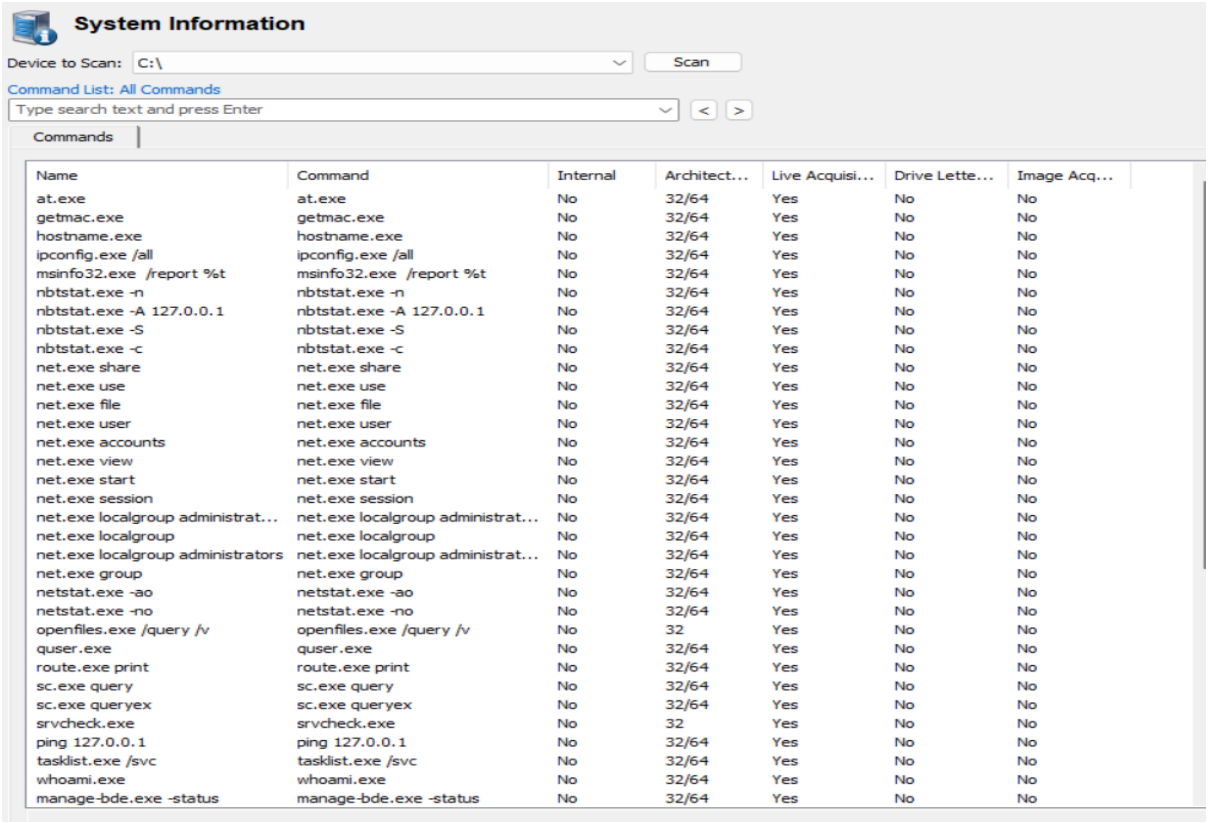
To analyze the raw sectors of all physical disks and partitions click raw disk viewer and select a disk to view its raw disk components.



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

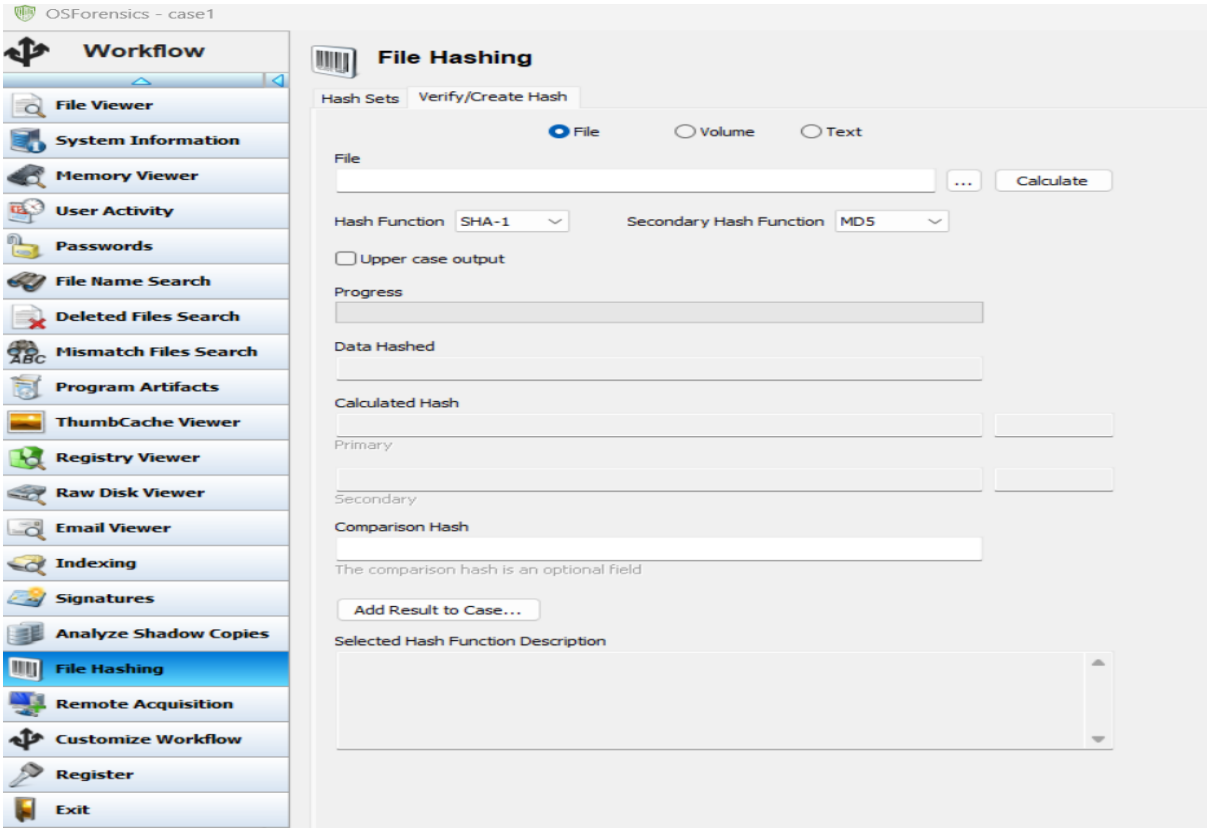


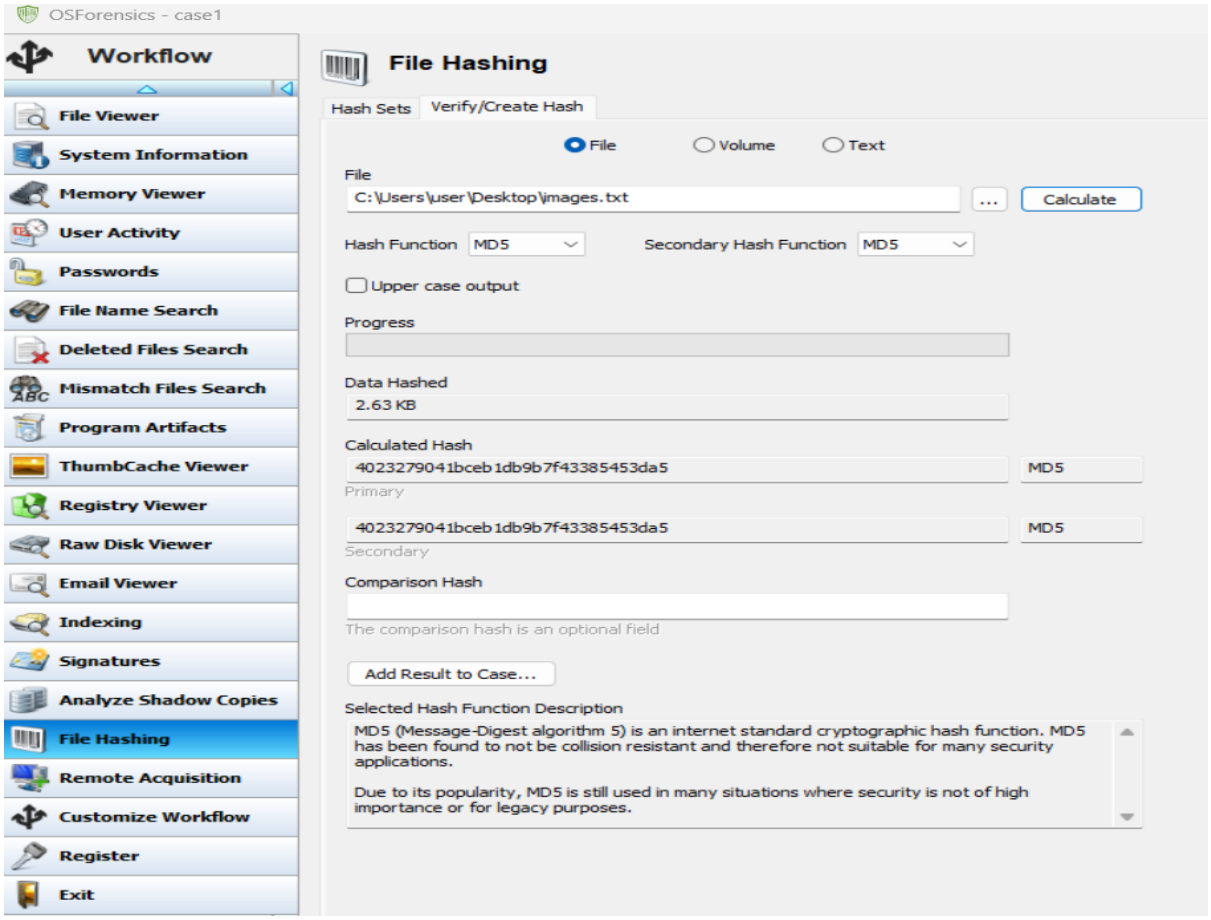
Name	Command	Internal	Architect...	Live Acquisi...	Drive Lette...	Image Acq...
Computer Name	SysInfoDll_GetComputerName	Yes	32/64	Yes	No	No
Operating system	SysInfoDll_GetOS	Yes	32/64	Yes	No	No
CPU Info	SysInfoDll_GetCPUInfo	Yes	32/64	Yes	No	No
Mem Info	SysInfoDll_GetMemoryInfo	Yes	32/64	Yes	No	No
Graphics 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

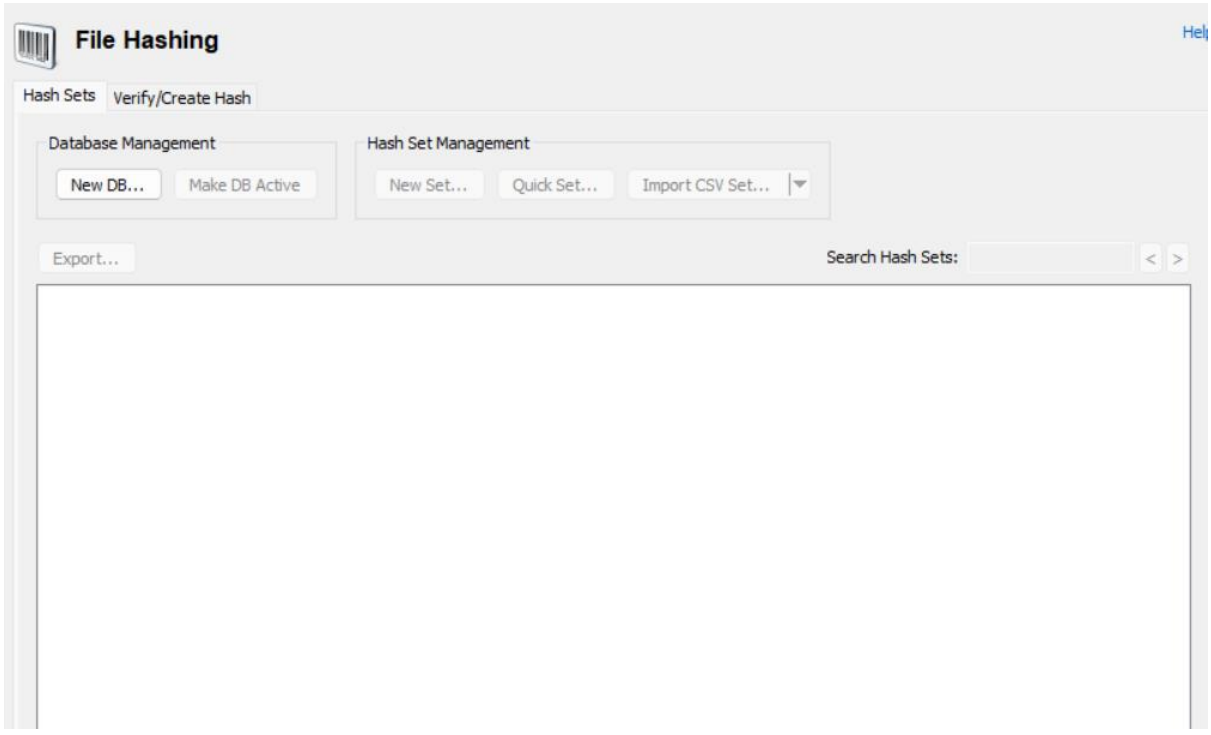


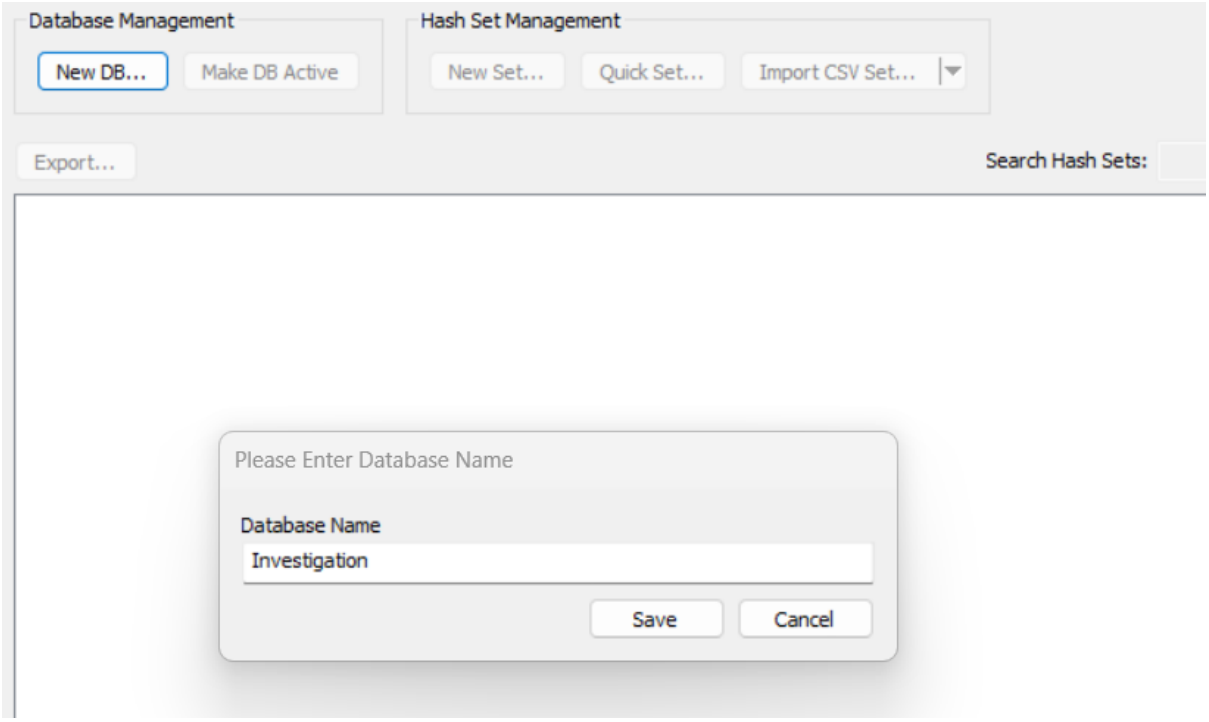
Name	Command	Internal	Architect...	Live Acquisi...	Drive Lette...	Image Acq...
at.exe	at.exe	No	32/64	Yes	No	No
getmac.exe	getmac.exe	No	32/64	Yes	No	No
hostname.exe	hostname.exe	No	32/64	Yes	No	No
ipconfig.exe /all	ipconfig.exe /all	No	32/64	Yes	No	No
msinfo32.exe /report %t	msinfo32.exe /report %t	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 administrat...	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

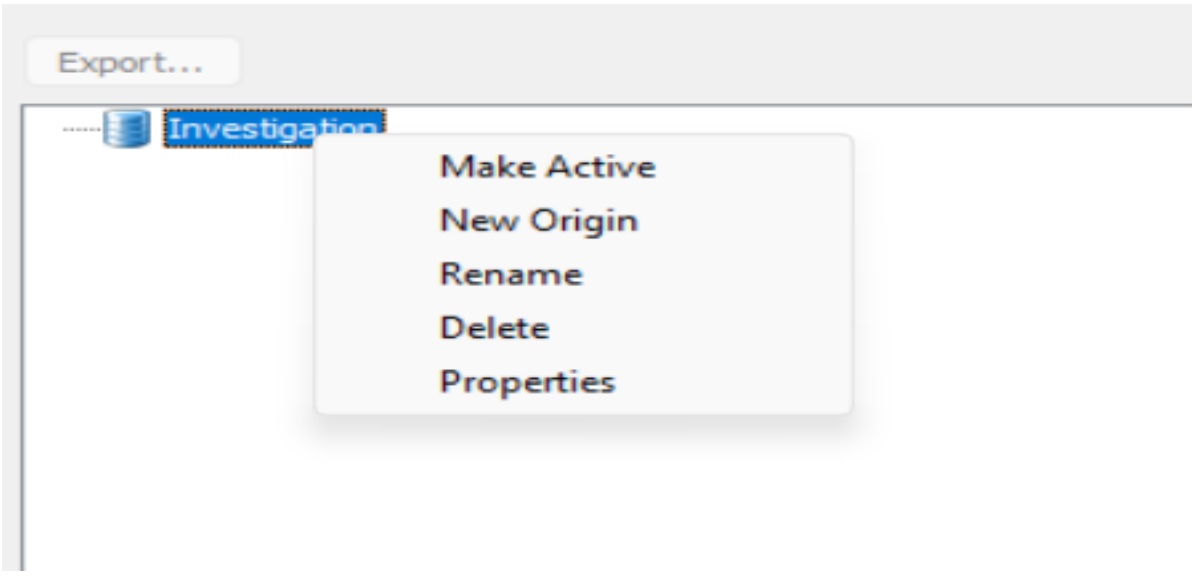
To verify the integrity of file by calculating their hash values, click file hashing.



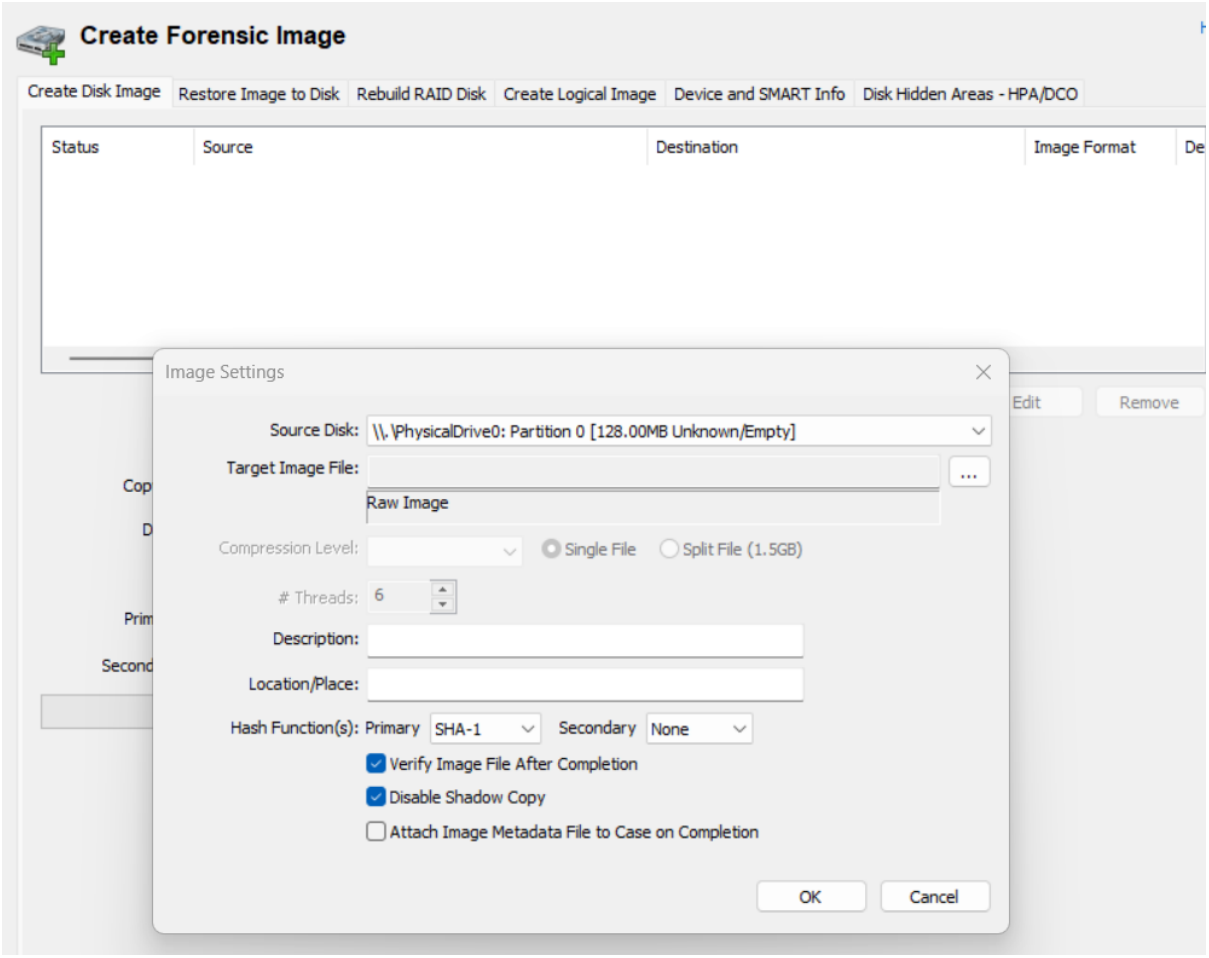

OSForensics - case1
Workflow
File Viewer
System Information
Memory Viewer
User Activity
Passwords
File Name Search
Deleted Files Search
Mismatch Files Search
Program Artifacts
ThumbCache Viewer
Registry Viewer
Raw Disk Viewer
Email Viewer
Indexing
Signatures
Analyze Shadow Copies
File Hashing
Remote Acquisition
Customize Workflow
Register
Exit
File Hashing
Hash Sets
Verify/Create Hash
File
Volume
Text
File
C:\Users\user\Desktop\jmages.txt
...
Calculate
Hash Function
MD5
Secondary Hash Function
MD5
Upper case output
Progress
Data Hashed
2.63 KB
Calculated Hash
4023279041bceb1db9b7f43385453da5
MD5
Primary
4023279041bceb1db9b7f43385453da5
MD5
Secondary
Comparison Hash
The comparison hash is an optional field
Add Result to Case...
Selected Hash Function Description
MD5 (Message-Digest algorithm 5) is an internet standard cryptographic hash function. MD5 has been found to not be collision resistant and therefore not suitable for many security applications.
Due to its popularity, MD5 is still used in many situations where security is not of high importance or for legacy purposes.


File Hashing
Hash Sets
Verify/Create Hash
Database Management
New DB...
Make DB Active
Hash Set Management
New Set...
Quick Set...
Import CSV Set...
Export...
Search Hash Sets:





generate exact copies of partitions or whole drive


Create Forensic Image
Create Disk Image
Restore Image to Disk
Rebuild RAID Disk
Create Logical Image
Device and SMART Info
Disk Hidden Areas - HPA/DCO
Status
Source
Destination
Image Format
Image Settings
Source Disk: \\.\PhysicalDrive0: Partition 0 [128.00MB Unknown/Empty]
Target Image File:
Raw Image
Compression Level:
Single File
Split File (1.5GB)
Threads: 6
Description:
Location/Place:
Hash Function(s): Primary SHA-1 Secondary None
Verify Image File After Completion
Disable Shadow Copy
Attach Image Metadata File to Case on Completion
OK
Cancel
Edit
Remove

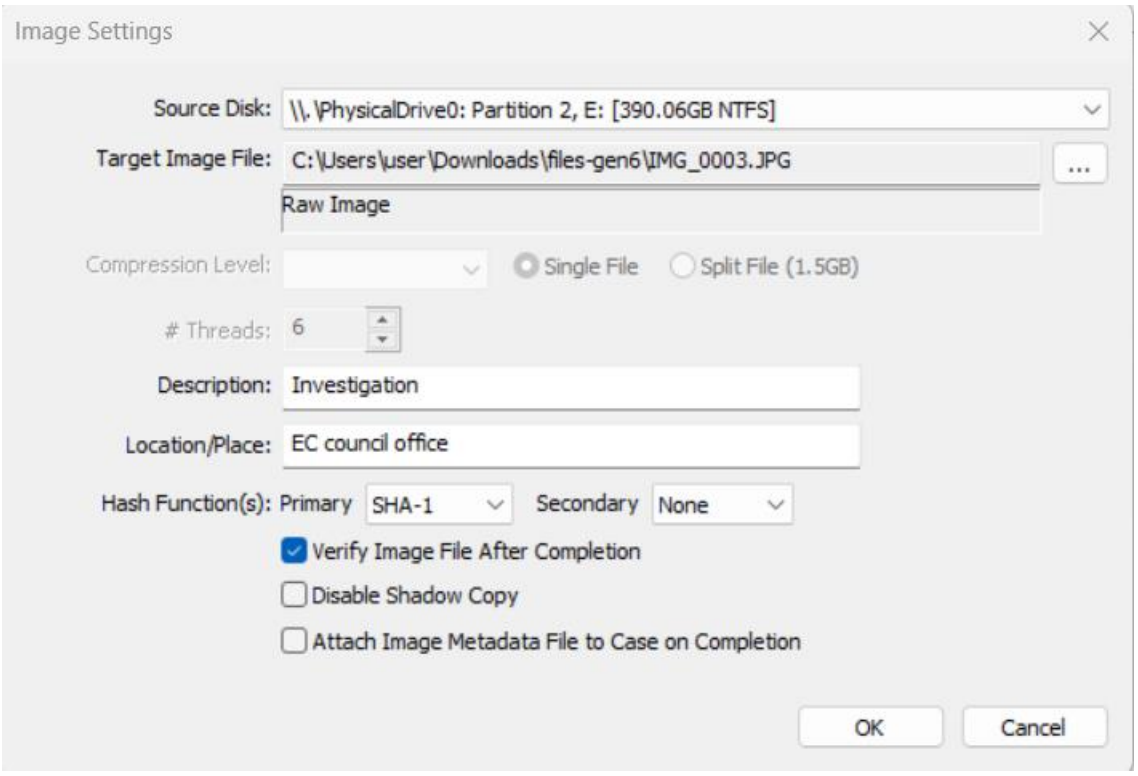
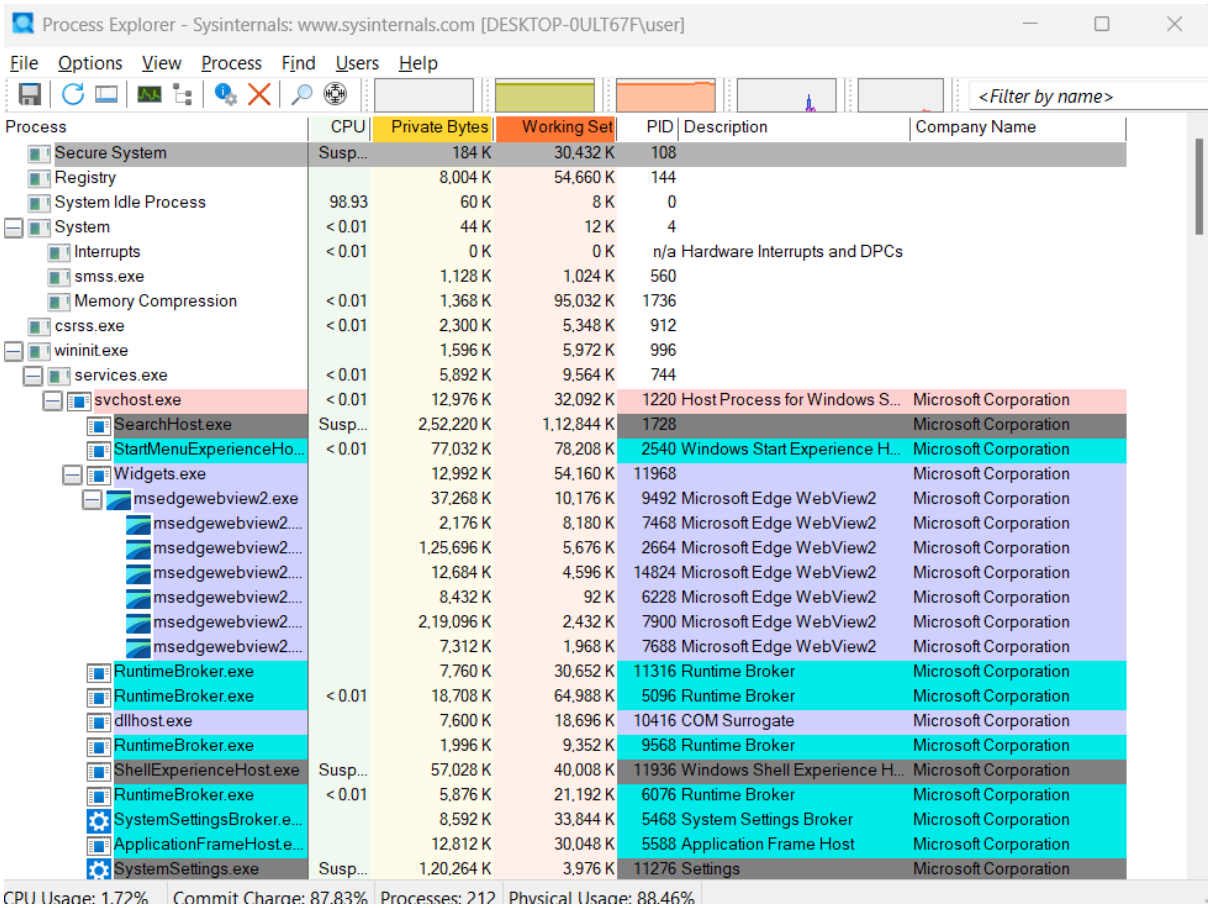


Image Settings
Source Disk: \\.\PhysicalDrive0: Partition 2, E: [390.06GB NTFS]
Target Image File: C:\Users\user\Downloads\files-gen6\IMG_0003.JPG
Raw Image
Compression Level:
Single File
Split File (1.5GB)
Threads: 6
Description: Investigation
Location/Place: EC council office
Hash Function(s): Primary SHA-1 Secondary None
Verify Image File After Completion
Disable Shadow Copy
Attach Image Metadata File to Case on Completion
OK
Cancel

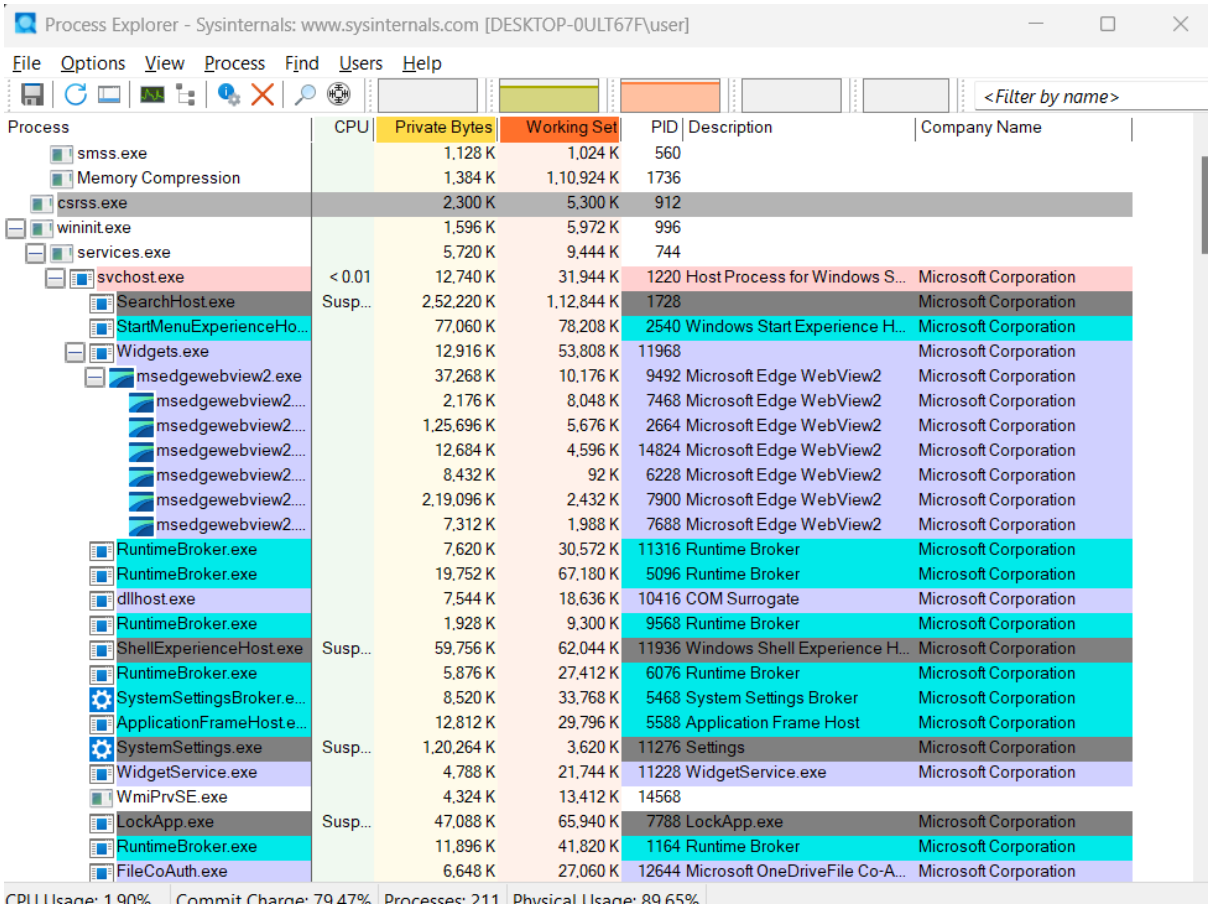
Lab2: Extracting information about Loaded Processes Using Process Explorer

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.

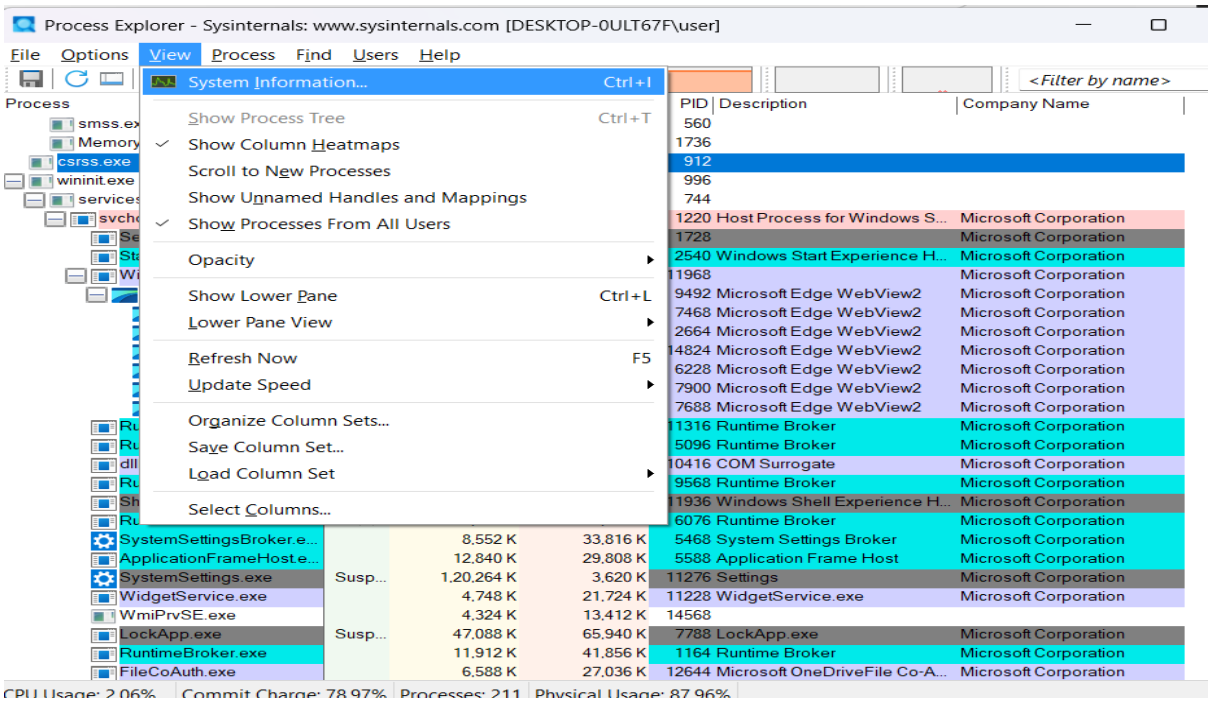
Proecess Explorer GUI appears, displaying all the details of all the process running on the machine



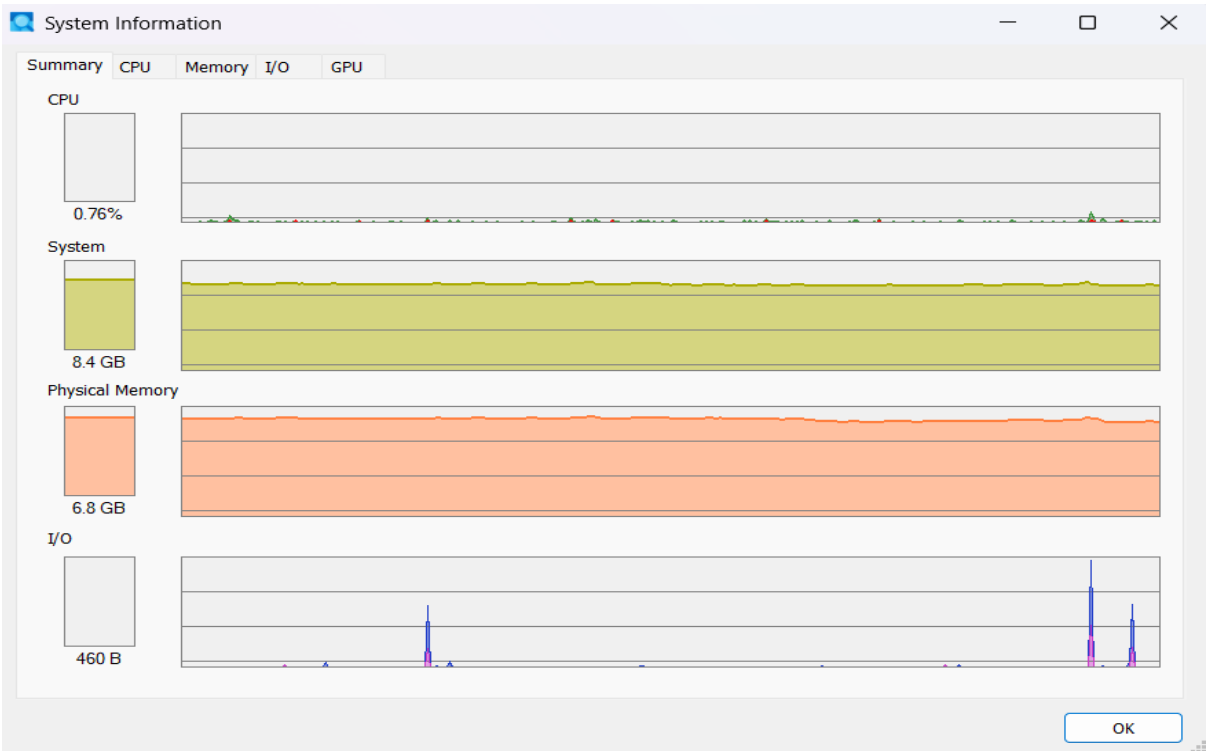
Process Explorer lists all the running processes in the left pane, and details of each process such as CPU usage, PID etc in the right pane.



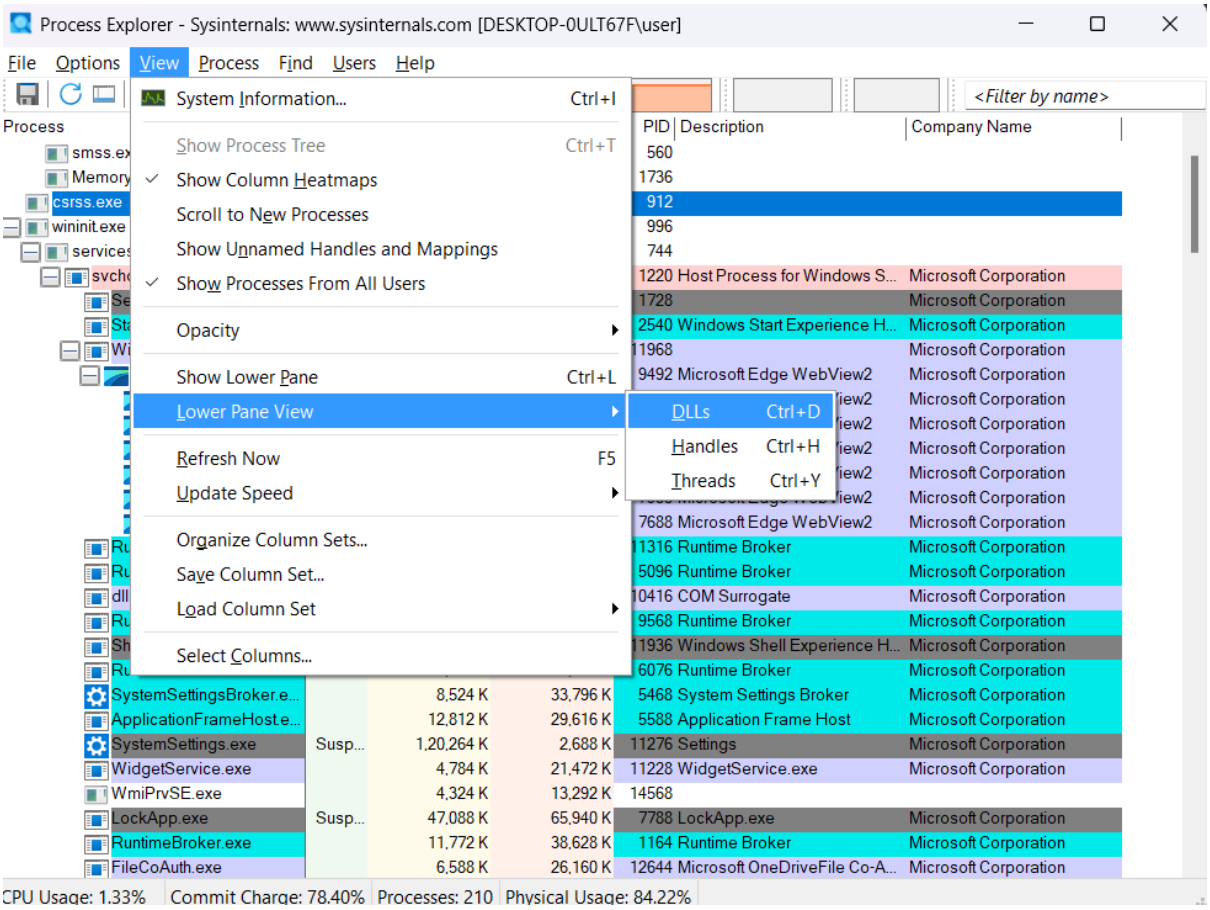
To view system information go to view in the menu bar and select system information



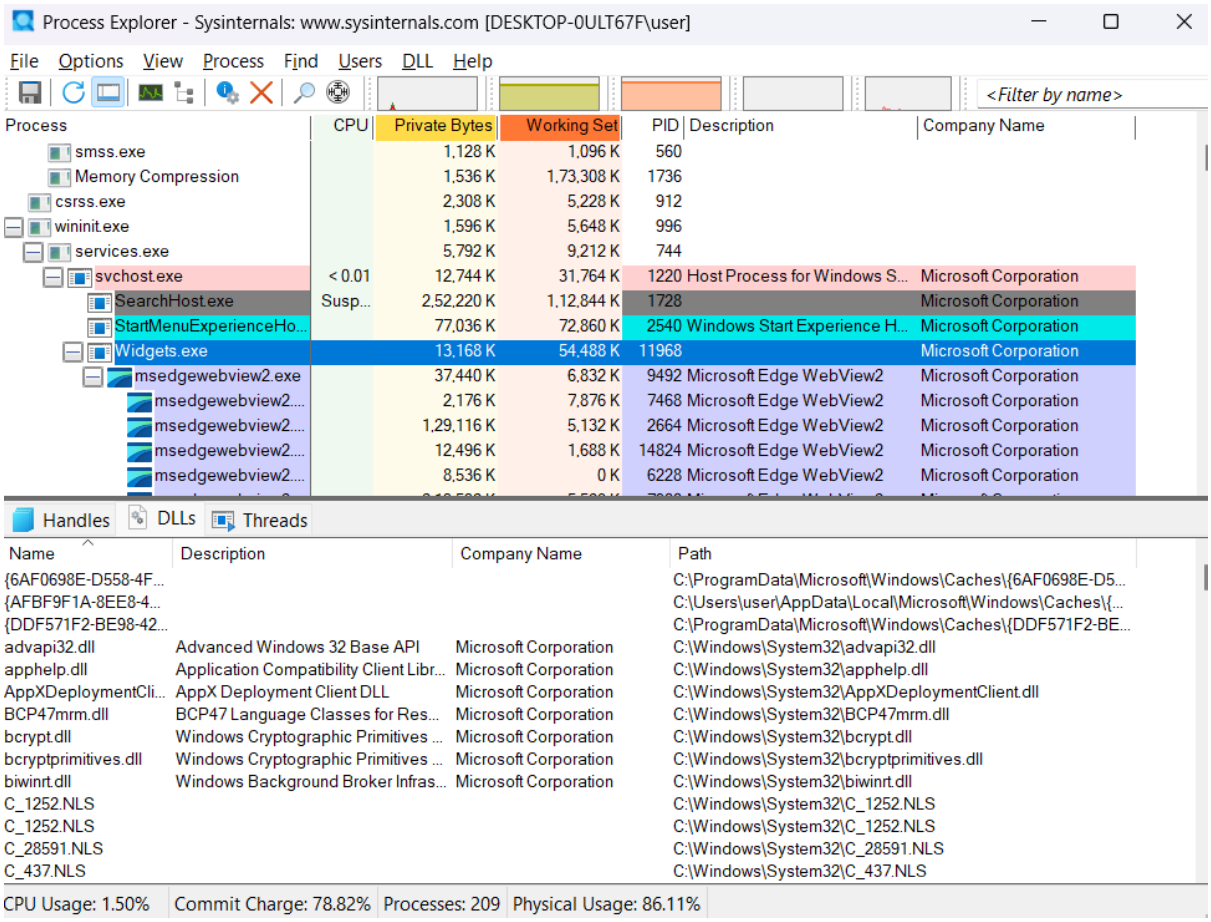
It will displays global system performance metrics.



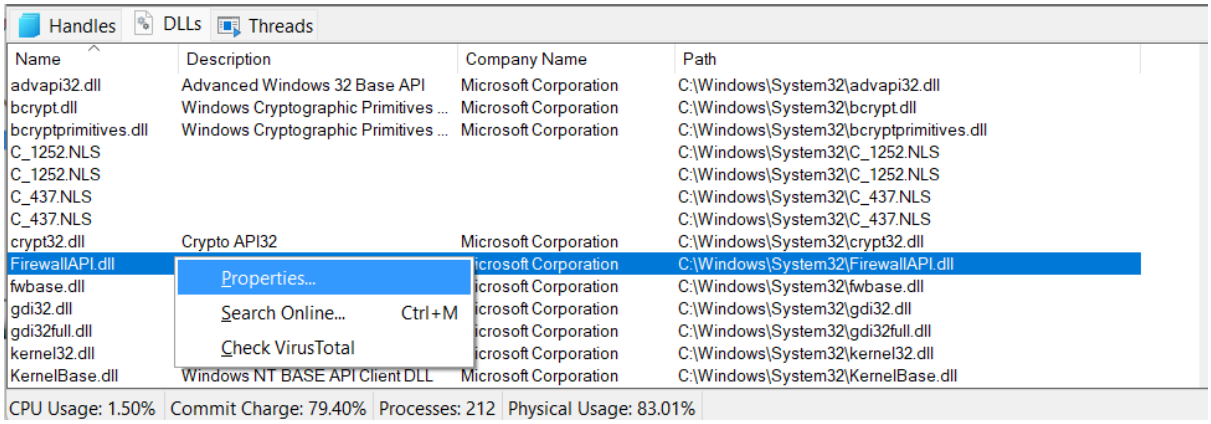
To view DLLs click view->lower pane view->DLLs



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

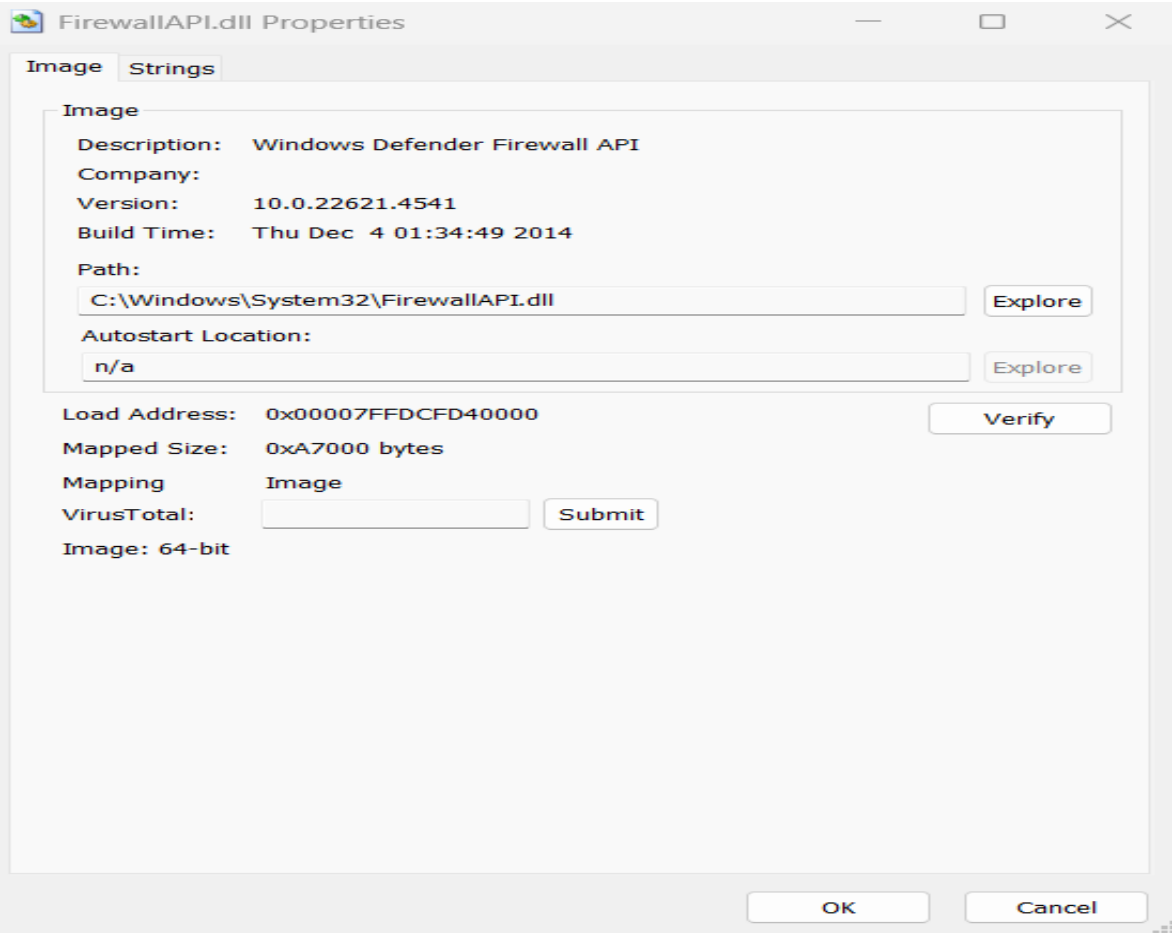


To view the properties of DLL right click a required DLL from the DLL list and select properties.

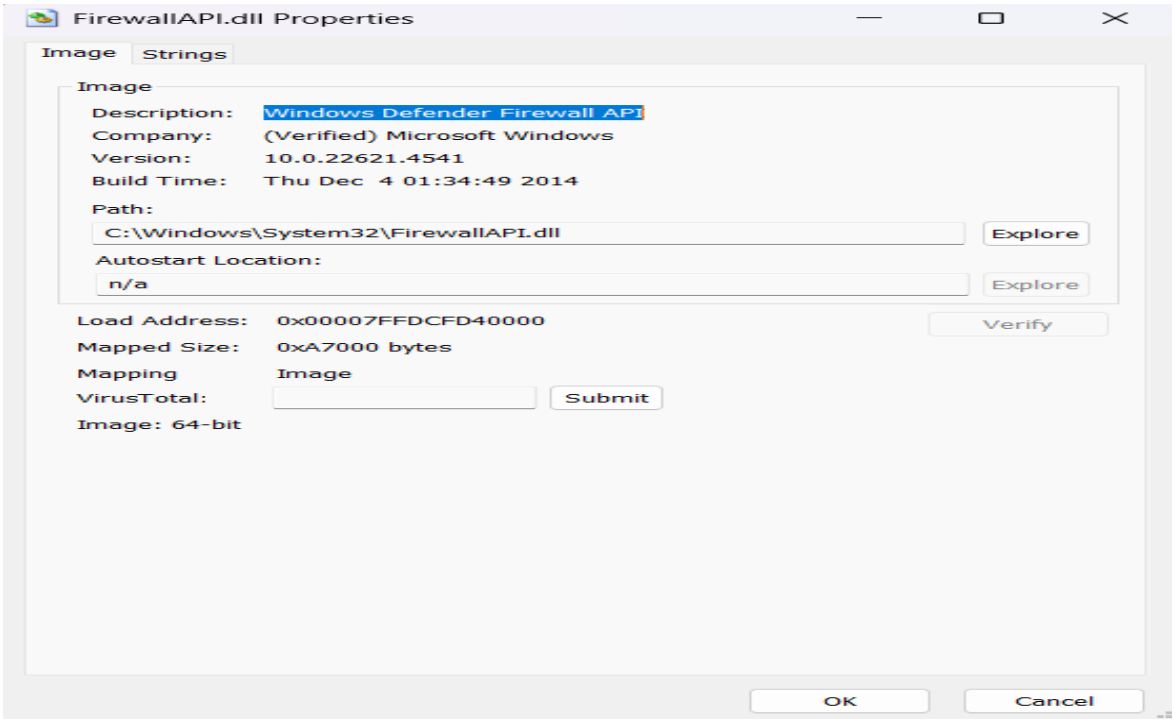


This displays the DLL properties in images and strings tabs.

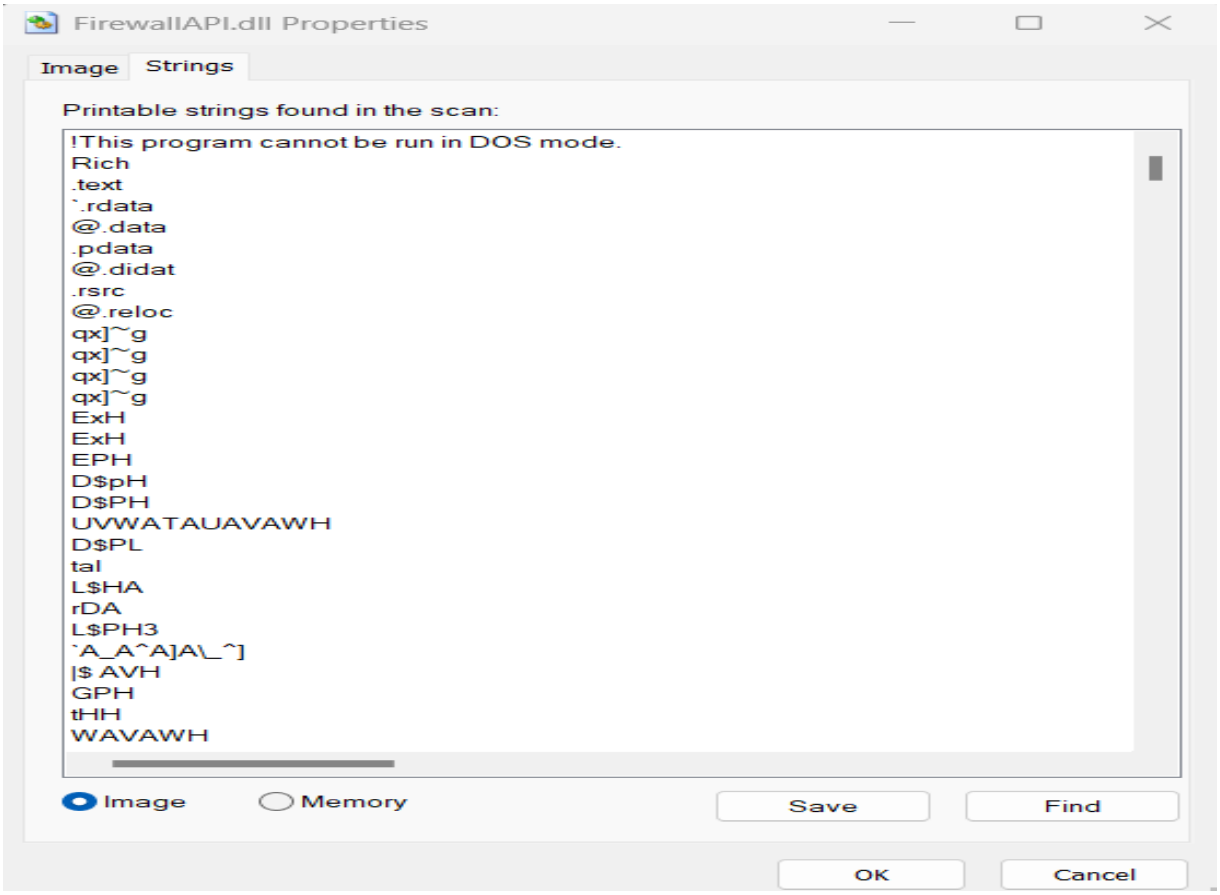
The image tab contains details of the DLL such as Company name, version path of DLL etc.



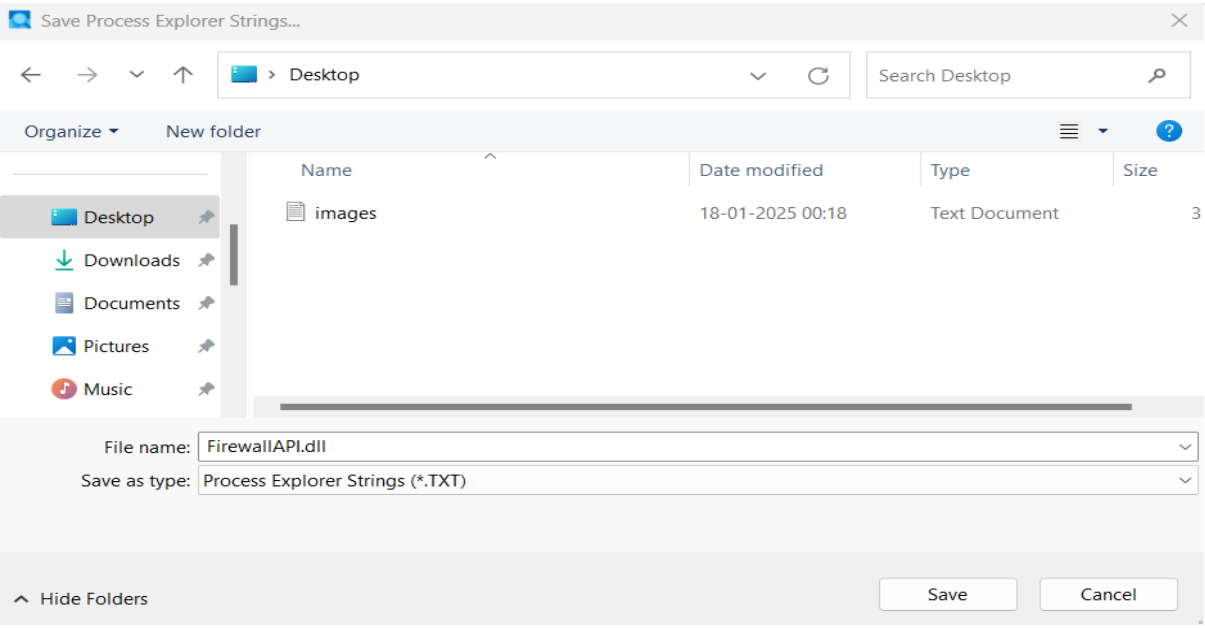
Click verify button to check for signature of a process. Here the Company's name appears to be Microsoft Windows so the process is said to be legitimate.



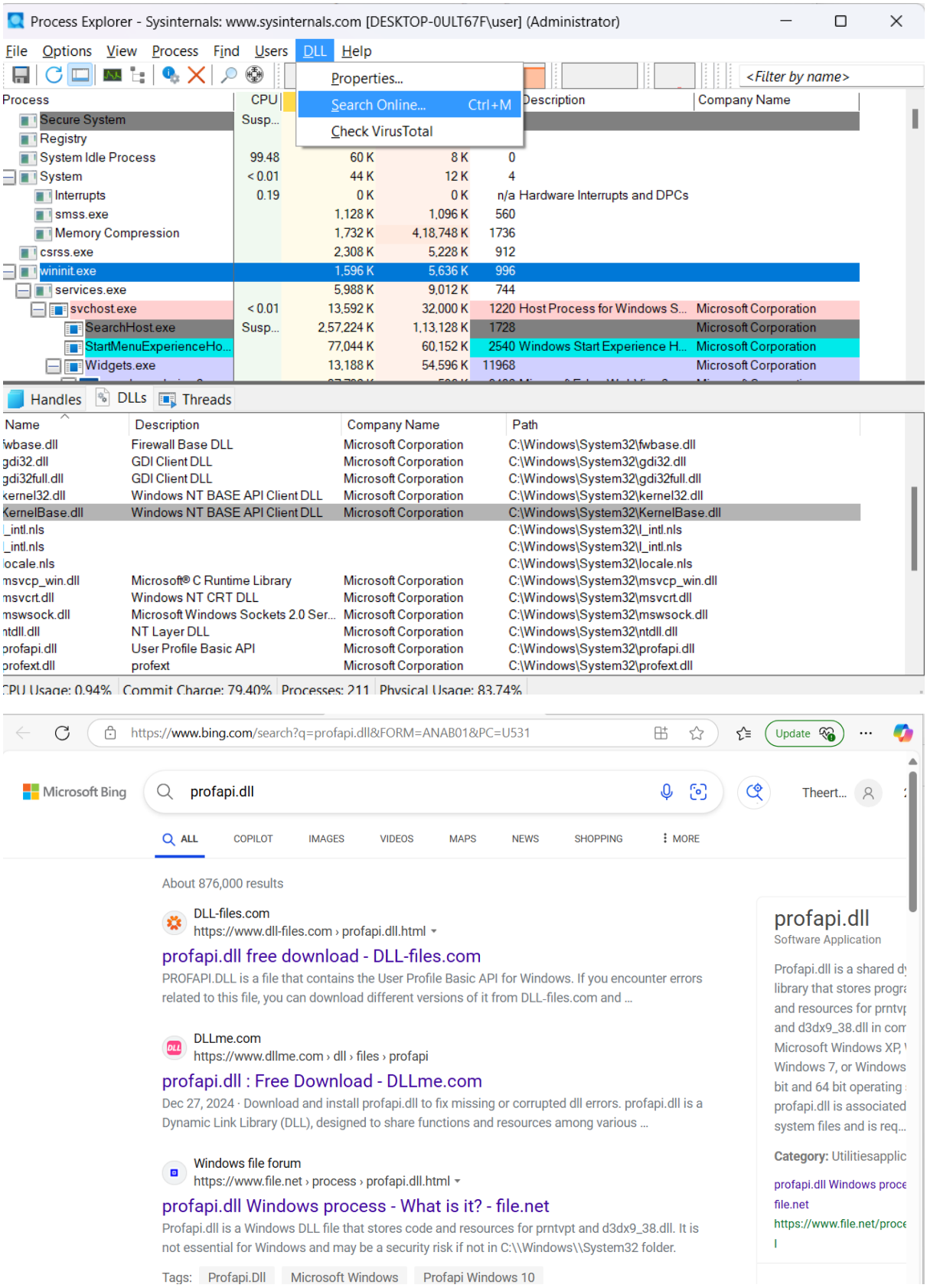
By clicking the string tab it lists any Unicode Strings found in the selected process. Examining this helps to find if the process is associated with any malware.



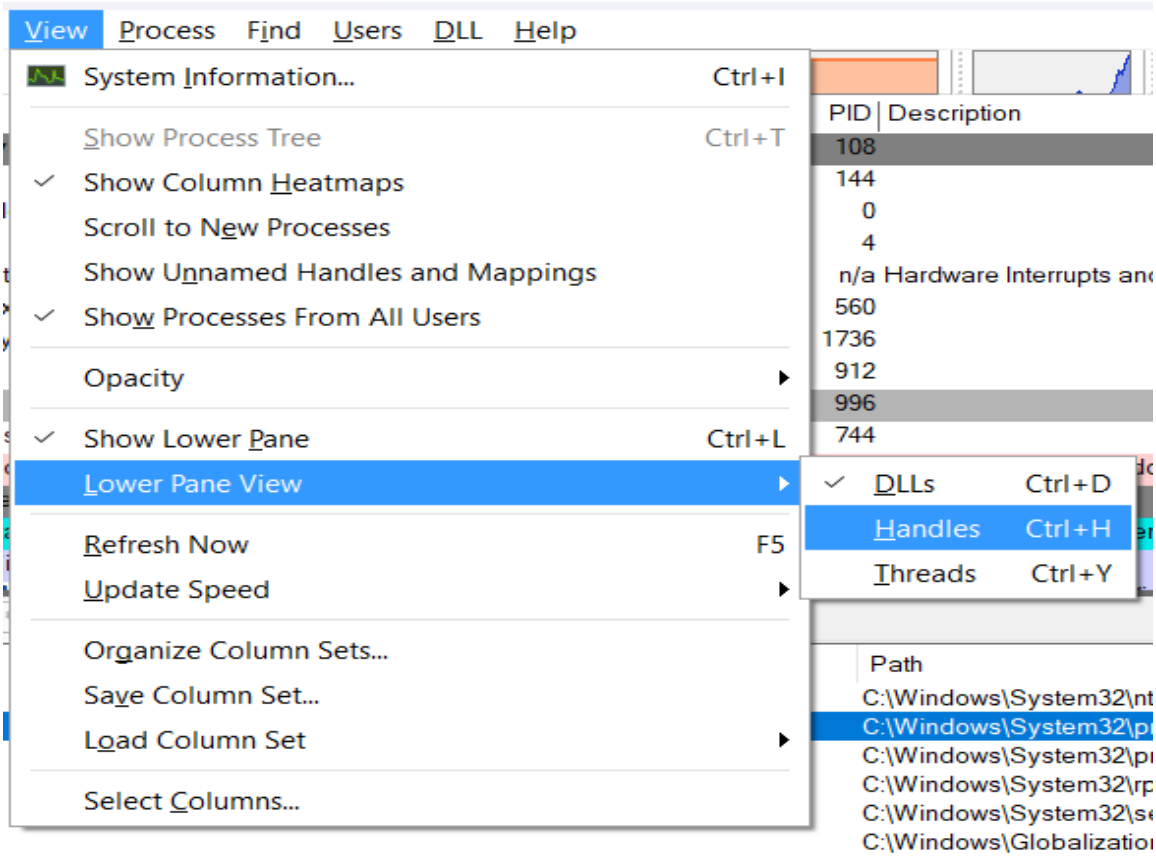
We can save image or memory string in text format

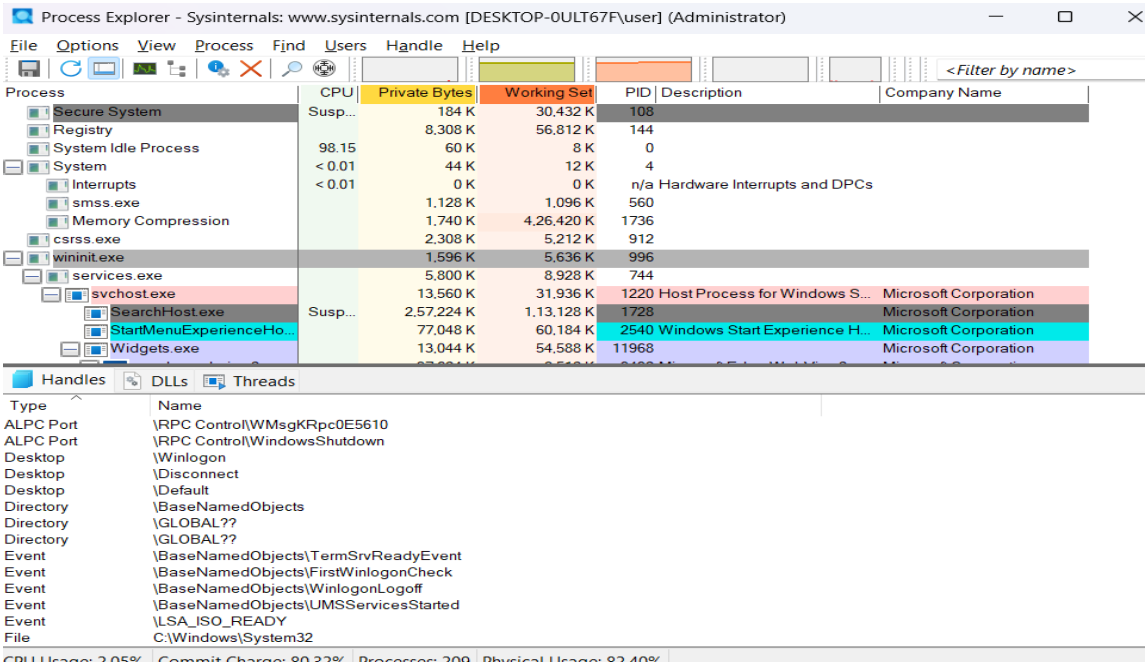


The serach online option searches the selected DLL on the internet by launching an Internet Browser.

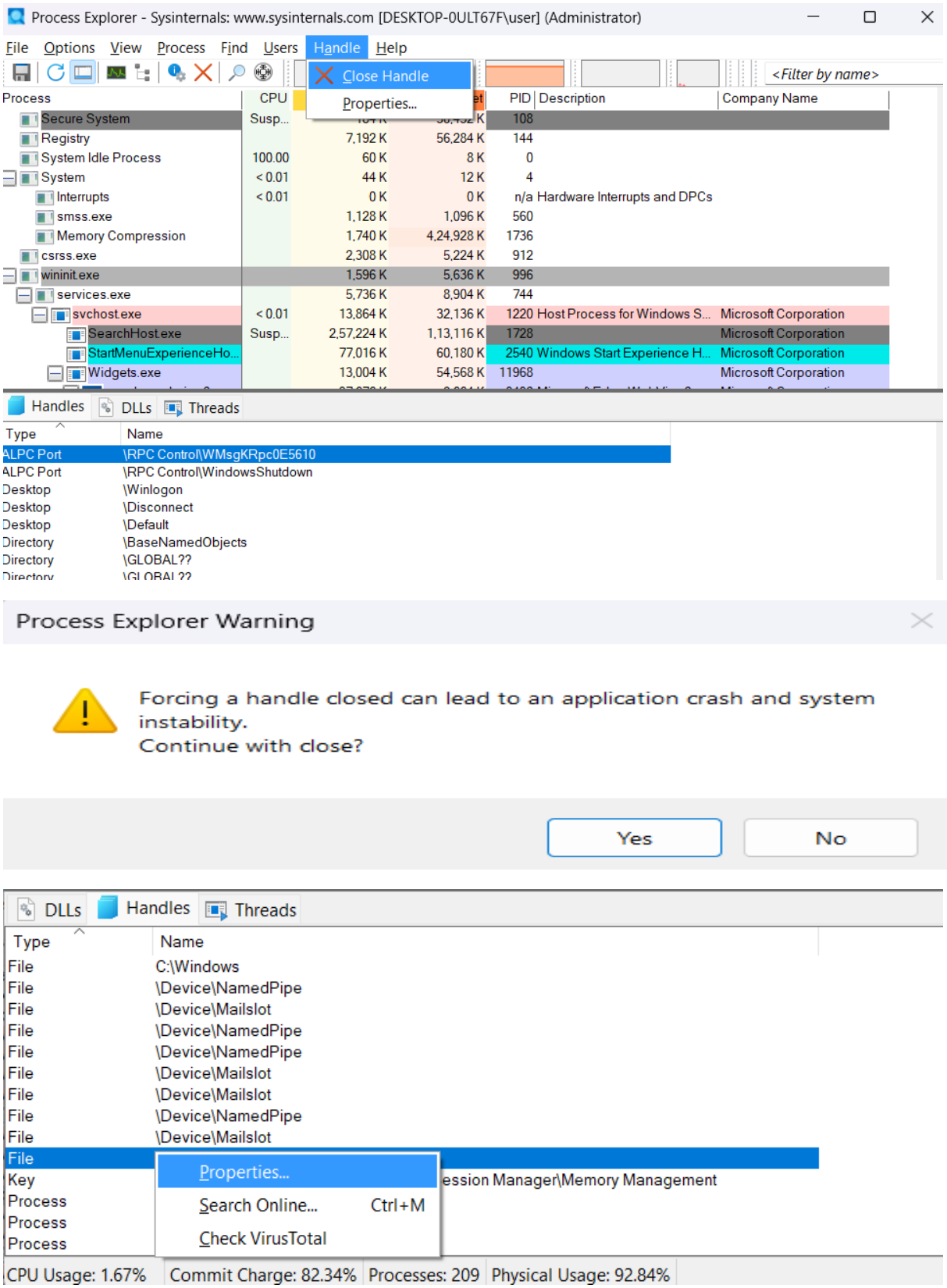


To view the handles of particular process click view ->Lower pane view->Handles





To close handle right click handle and close.

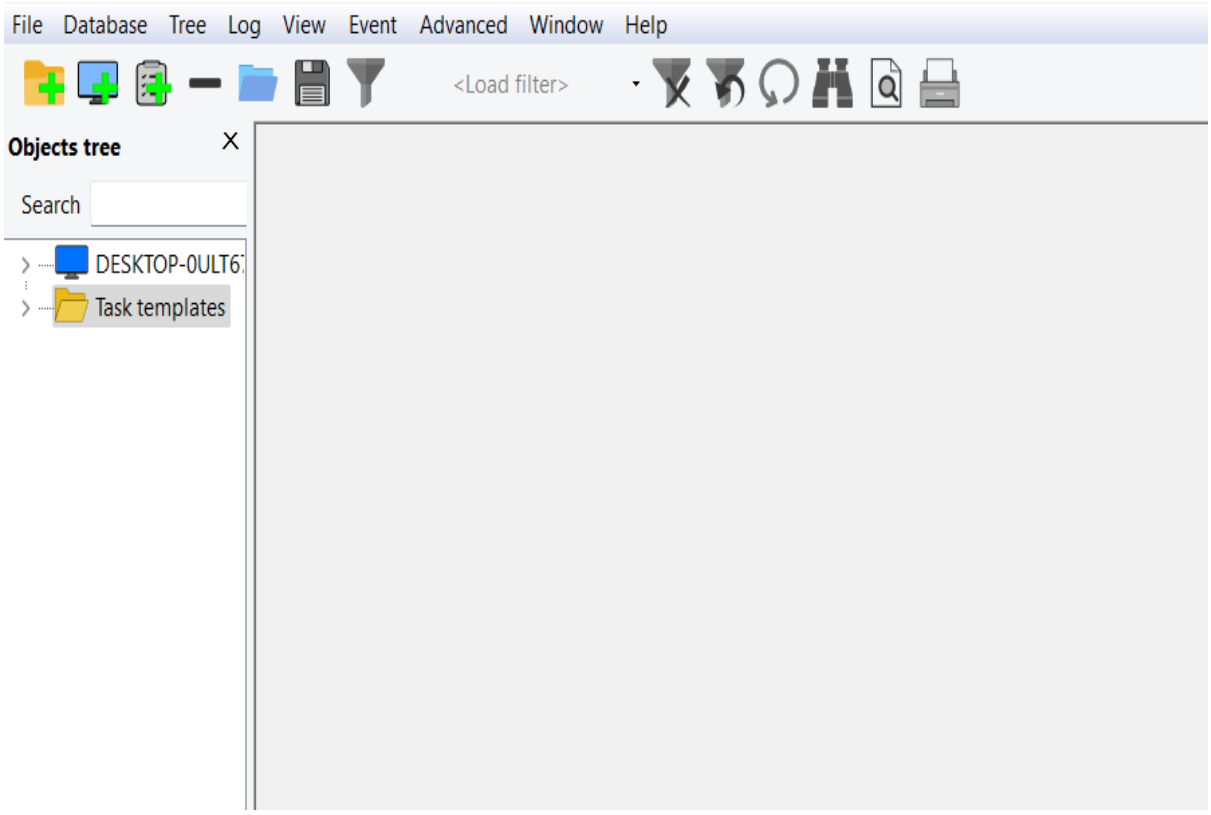

Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-0ULT67F\user] (Administrator)
File Options View Process Find Users Handle Help
Close Handle
Properties...
<Filter by name>
Process CPU PID Description Company Name
Secure System Susp... 108
Registry 7,192 K 56,284 K 144
System Idle Process 100.00 60 K 8 K 0
System < 0.01 44 K 12 K 4
Interrupts < 0.01 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... Microsoft Corporation
SearchHost.exe Susp... 2,57,224 K 1,13,116 K 1728 Microsoft Corporation
StartMenuExperienceHo... 77,016 K 60,180 K 2540 Windows Start Experience H... Microsoft Corporation
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??
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
Key ession Manager\Memory Management
Process
Process
Process
Properties...
Search Online... Ctrl+M
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

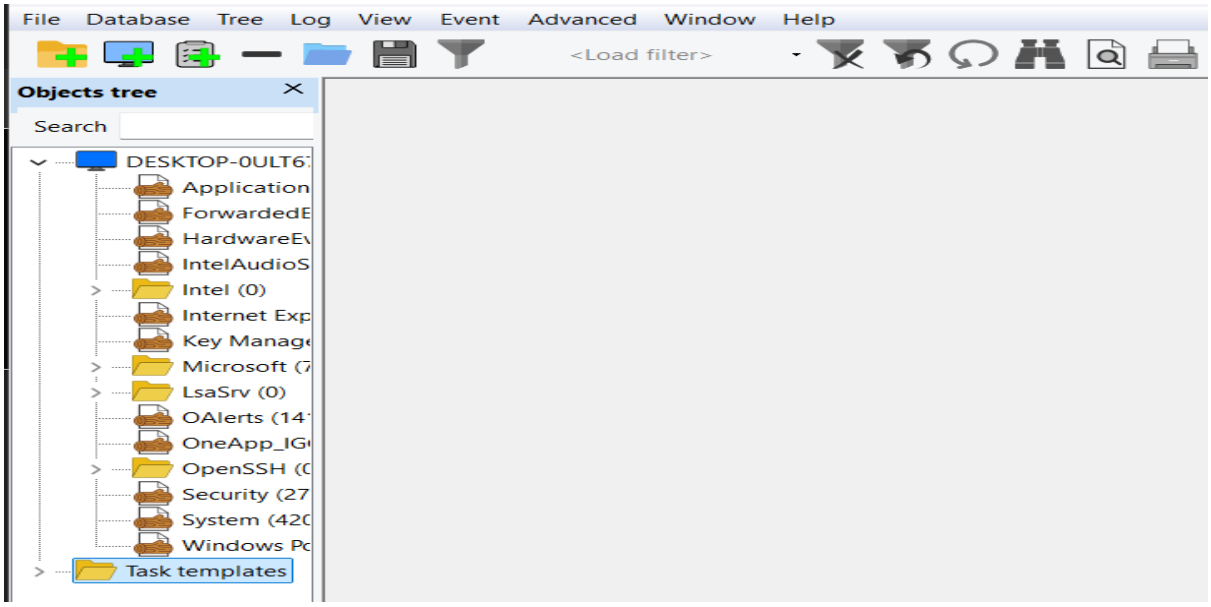
The objective of this lab is to help forensic investigators learn how to view, monitor, and analyze various events. Here we monitor and analyze:

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

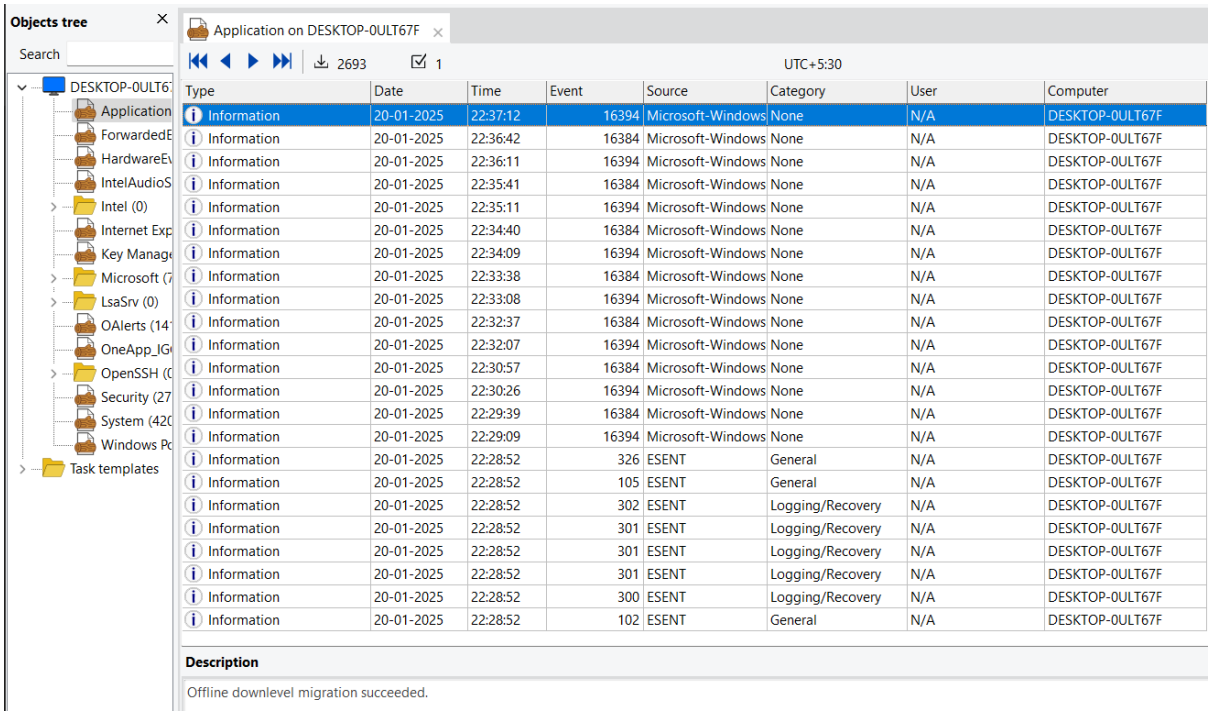
Event Log Explorer main window appears, displaying an empty log view area and object area pane with windows server virtual machine's computer name.



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

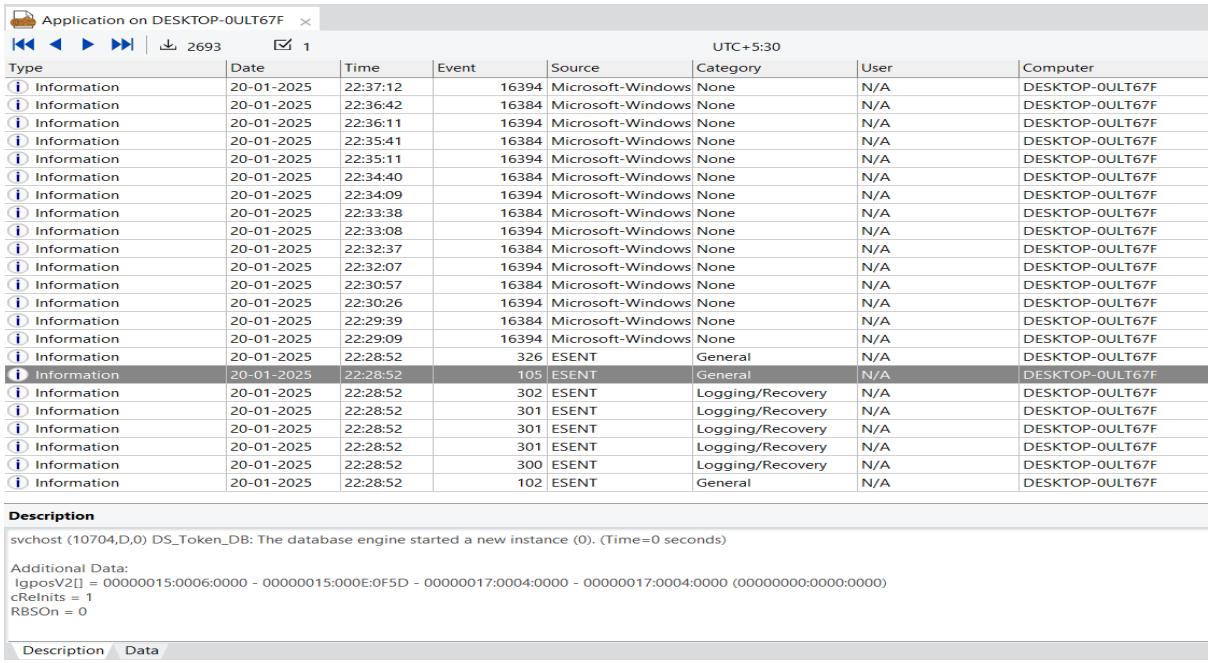


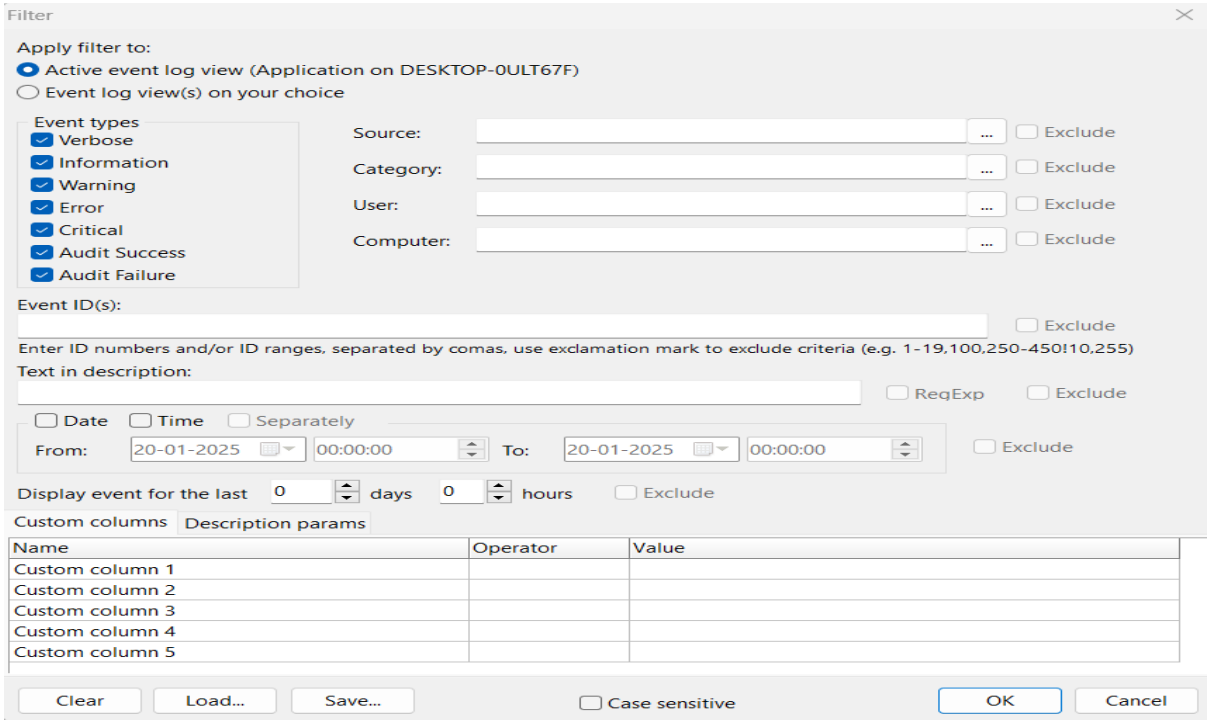
By double clicking Application in the object tree pane we can see application events.



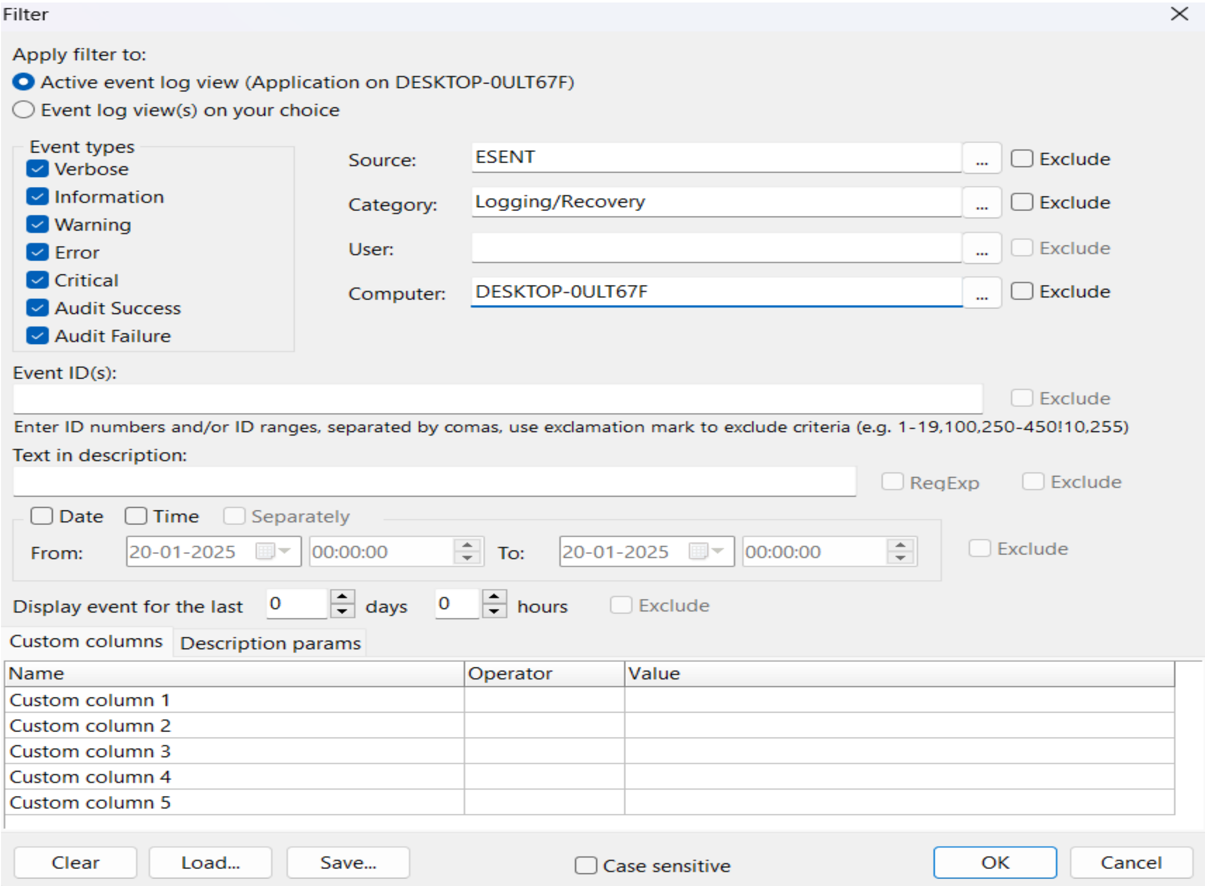
Event Log Explorer also displays the events of Applicure DFS Replication, dotDefenderAudit, Hardware Events, Key Management service, OAlerts, Security, System, Windows Powershell.

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



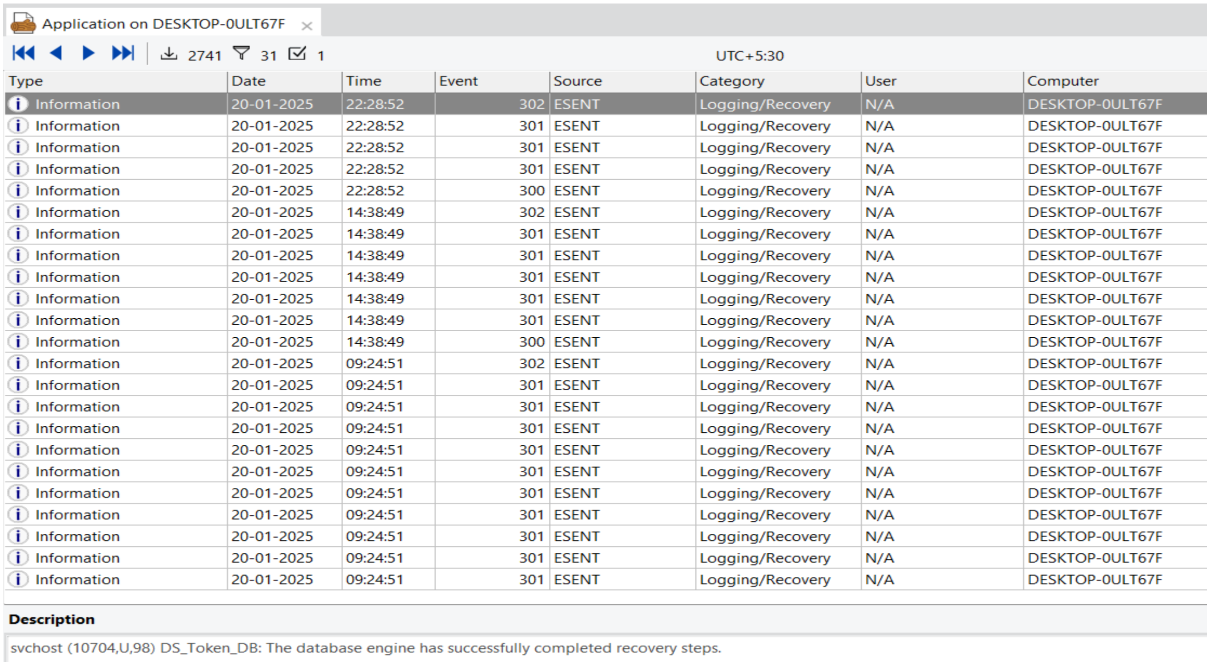


To filter the events click the filter icon in the toolbar. It will popup a new filter window. Choose source, category, computer



Click ok.

It will display all the events related to that filter.

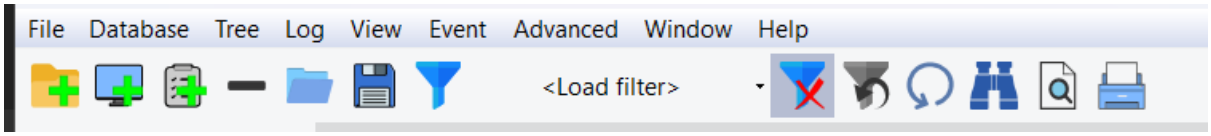


Type	Date	Time	Event	Source	Category	User	Computer
Information	20-01-2025	22:28:52	302	ESENT	Logging/Recovery	N/A	DESKTOP-0ULT67F
Information	20-01-2025	22:28:52	301	ESENT	Logging/Recovery	N/A	DESKTOP-0ULT67F
Information	20-01-2025	22:28:52	301	ESENT	Logging/Recovery	N/A	DESKTOP-0ULT67F
Information	20-01-2025	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	14:38:49	302	ESENT	Logging/Recovery	N/A	DESKTOP-0ULT67F
Information	20-01-2025	14:38:49	301	ESENT	Logging/Recovery	N/A	DESKTOP-0ULT67F
Information	20-01-2025	14:38:49	301	ESENT	Logging/Recovery	N/A	DESKTOP-0ULT67F
Information	20-01-2025	14:38:49	301	ESENT	Logging/Recovery	N/A	DESKTOP-0ULT67F
Information	20-01-2025	14:38:49	301	ESENT	Logging/Recovery	N/A	DESKTOP-0ULT67F
Information	20-01-2025	14:38:49	301	ESENT	Logging/Recovery	N/A	DESKTOP-0ULT67F
Information	20-01-2025	14:38:49	300	ESENT	Logging/Recovery	N/A	DESKTOP-0ULT67F
Information	20-01-2025	09:24:51	302	ESENT	Logging/Recovery	N/A	DESKTOP-0ULT67F
Information	20-01-2025	09:24:51	301	ESENT	Logging/Recovery	N/A	DESKTOP-0ULT67F
Information	20-01-2025	09:24:51	301	ESENT	Logging/Recovery	N/A	DESKTOP-0ULT67F
Information	20-01-2025	09:24:51	301	ESENT	Logging/Recovery	N/A	DESKTOP-0ULT67F
Information	20-01-2025	09:24:51	301	ESENT	Logging/Recovery	N/A	DESKTOP-0ULT67F
Information	20-01-2025	09:24:51	301	ESENT	Logging/Recovery	N/A	DESKTOP-0ULT67F
Information	20-01-2025	09:24:51	301	ESENT	Logging/Recovery	N/A	DESKTOP-0ULT67F
Information	20-01-2025	09:24:51	301	ESENT	Logging/Recovery	N/A	DESKTOP-0ULT67F
Information	20-01-2025	09:24:51	301	ESENT	Logging/Recovery	N/A	DESKTOP-0ULT67F
Information	20-01-2025	09:24:51	301	ESENT	Logging/Recovery	N/A	DESKTOP-0ULT67F
Information	20-01-2025	09:24:51	301	ESENT	Logging/Recovery	N/A	DESKTOP-0ULT67F

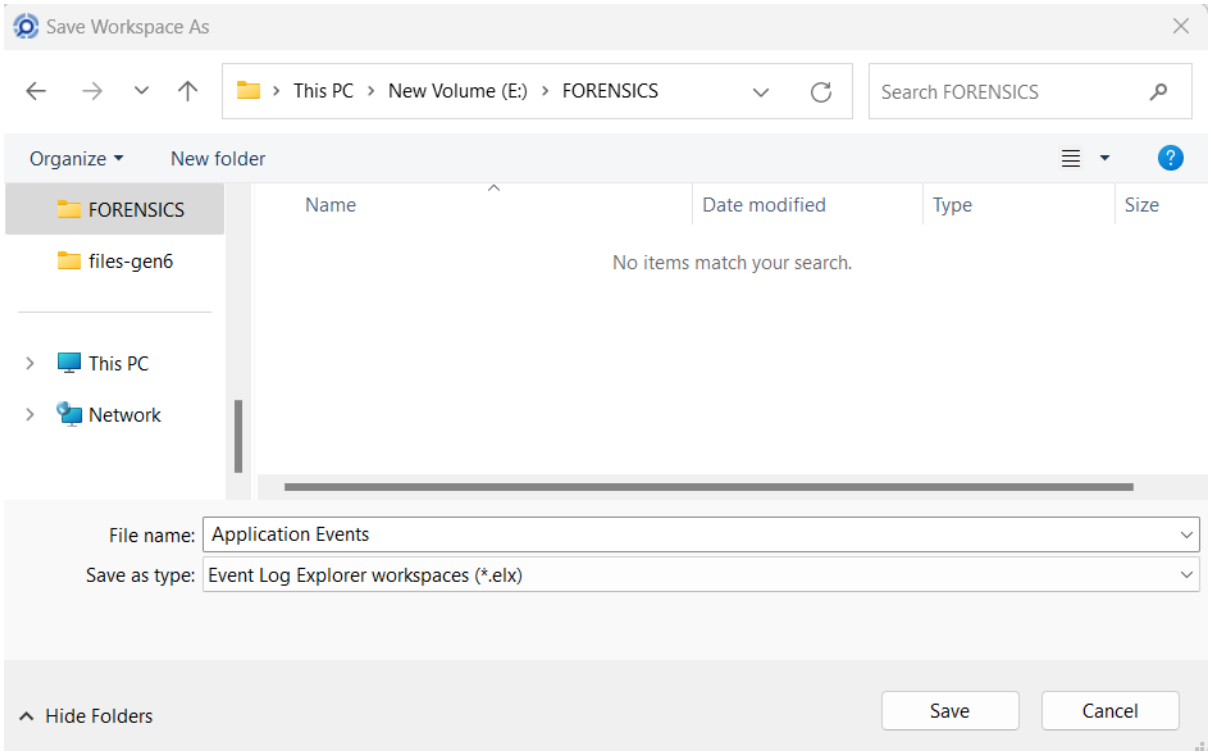
Description

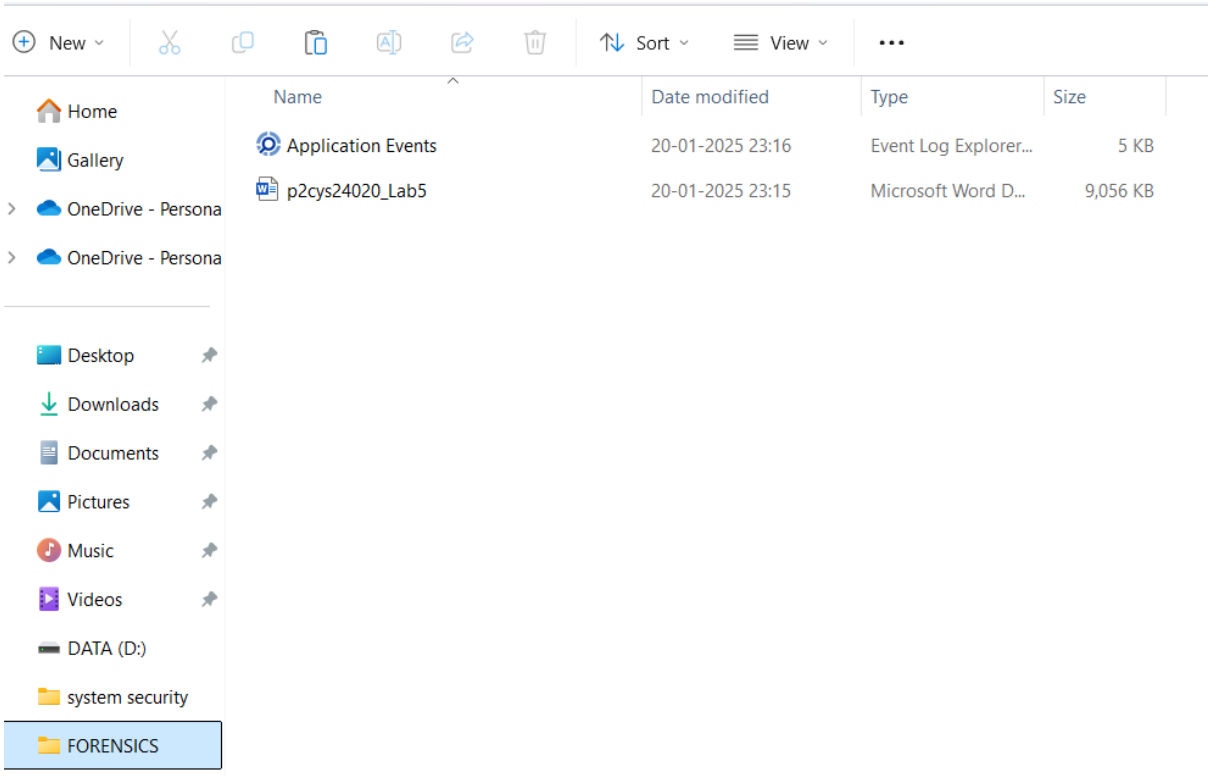
svchost (10704,U,98) DS_Token_DB: The database engine has successfully completed recovery steps.

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

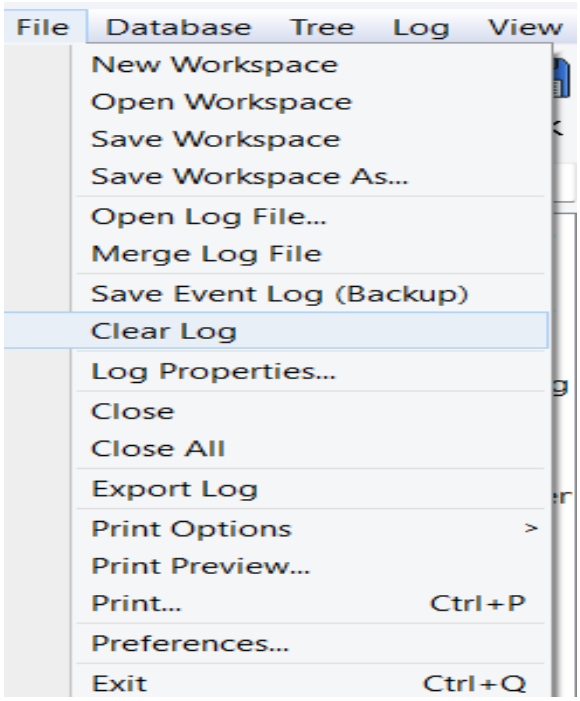


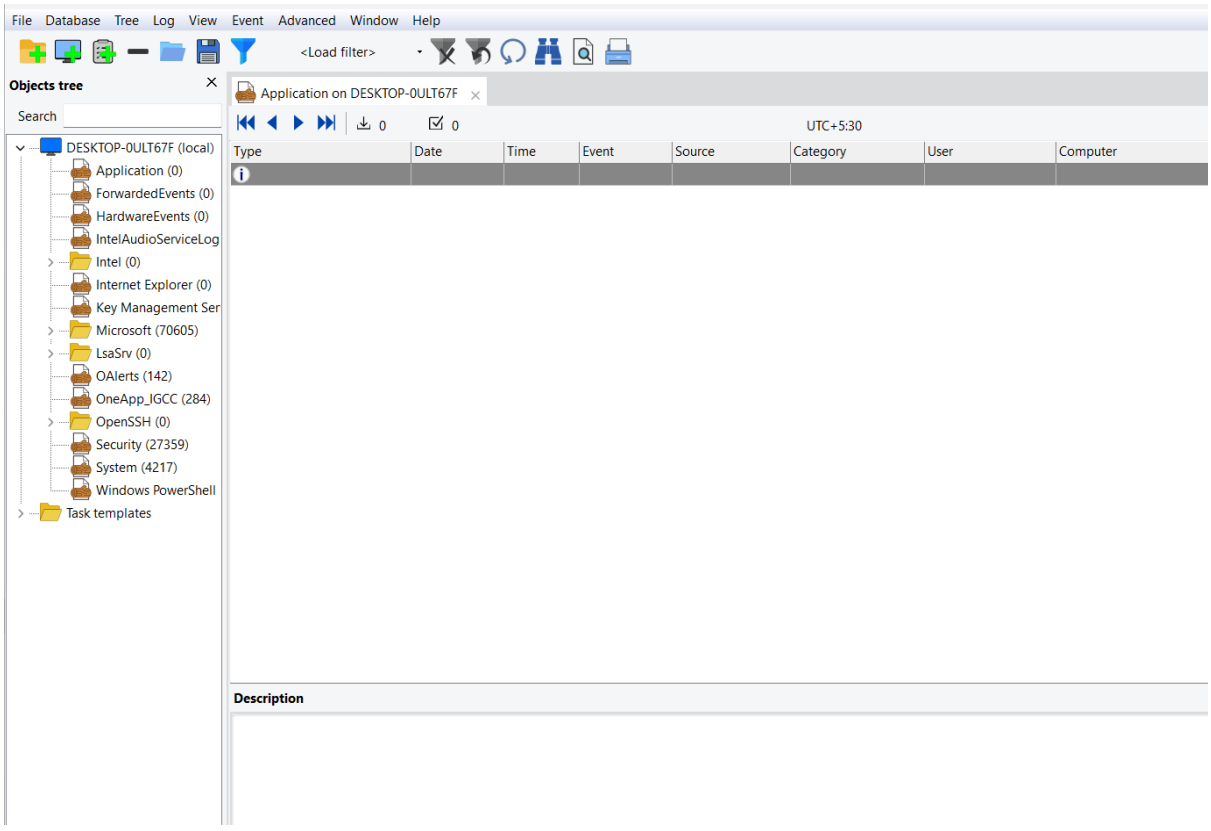
We can save the event logs.





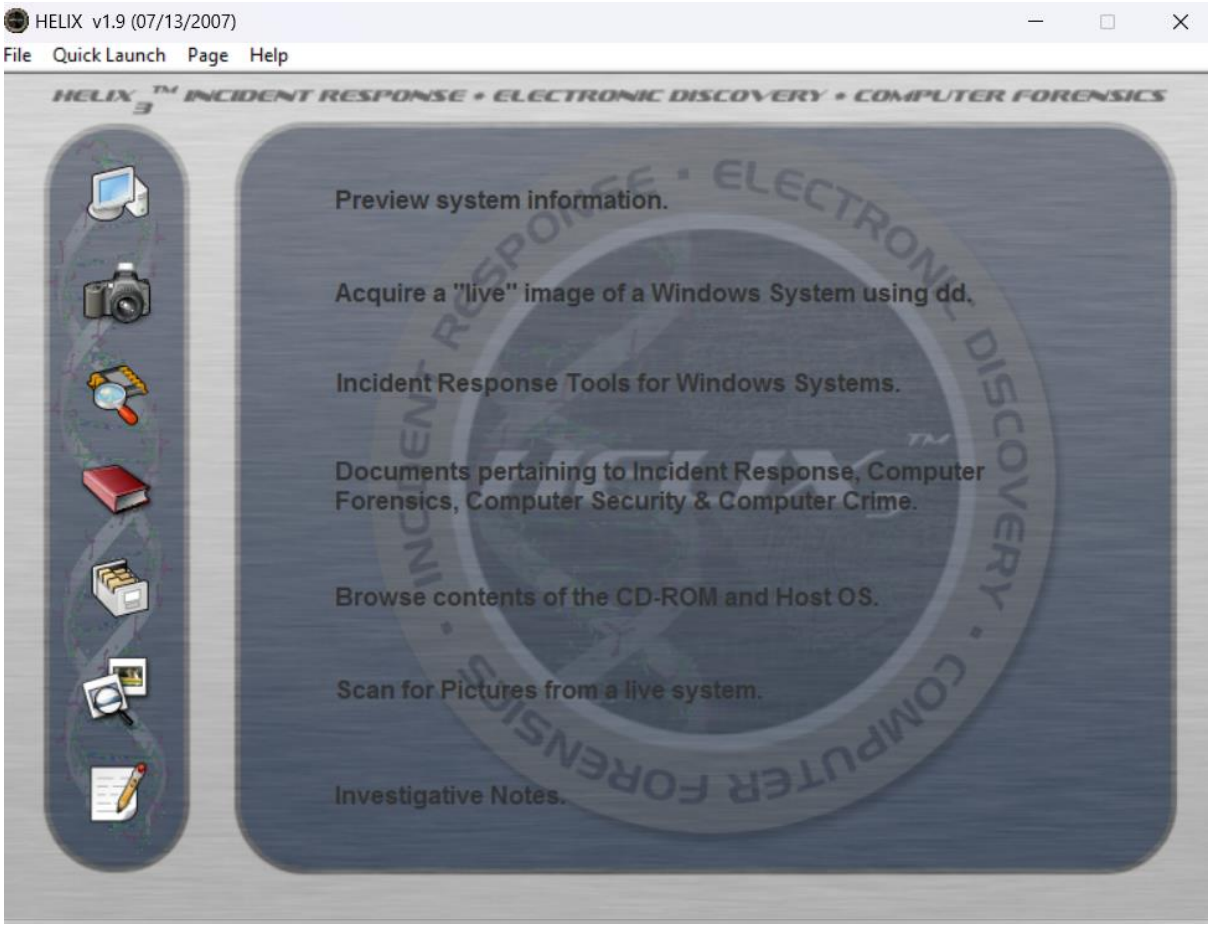
We can clear the logs



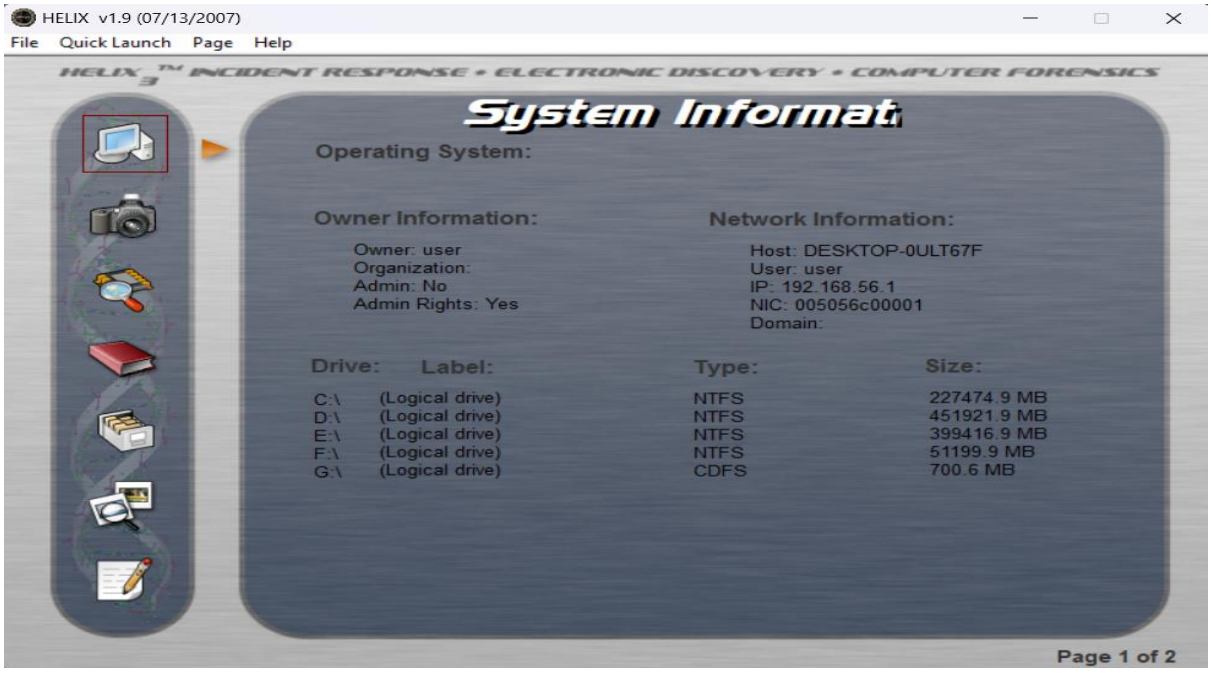


Lab-4: Performing a Computer Forensic Investigation Using the Helix Tool

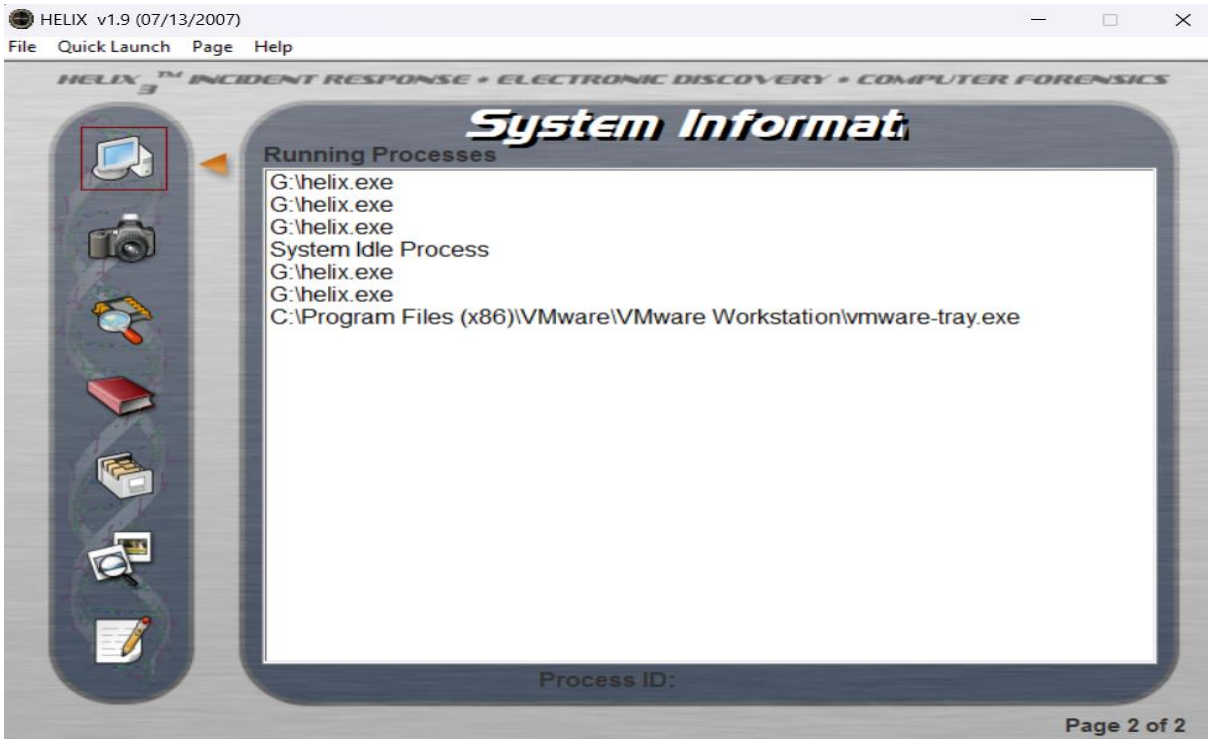
Objective: The objective of this lab is to learn how to investigate a computer based crime Using the Helix Tool.



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.

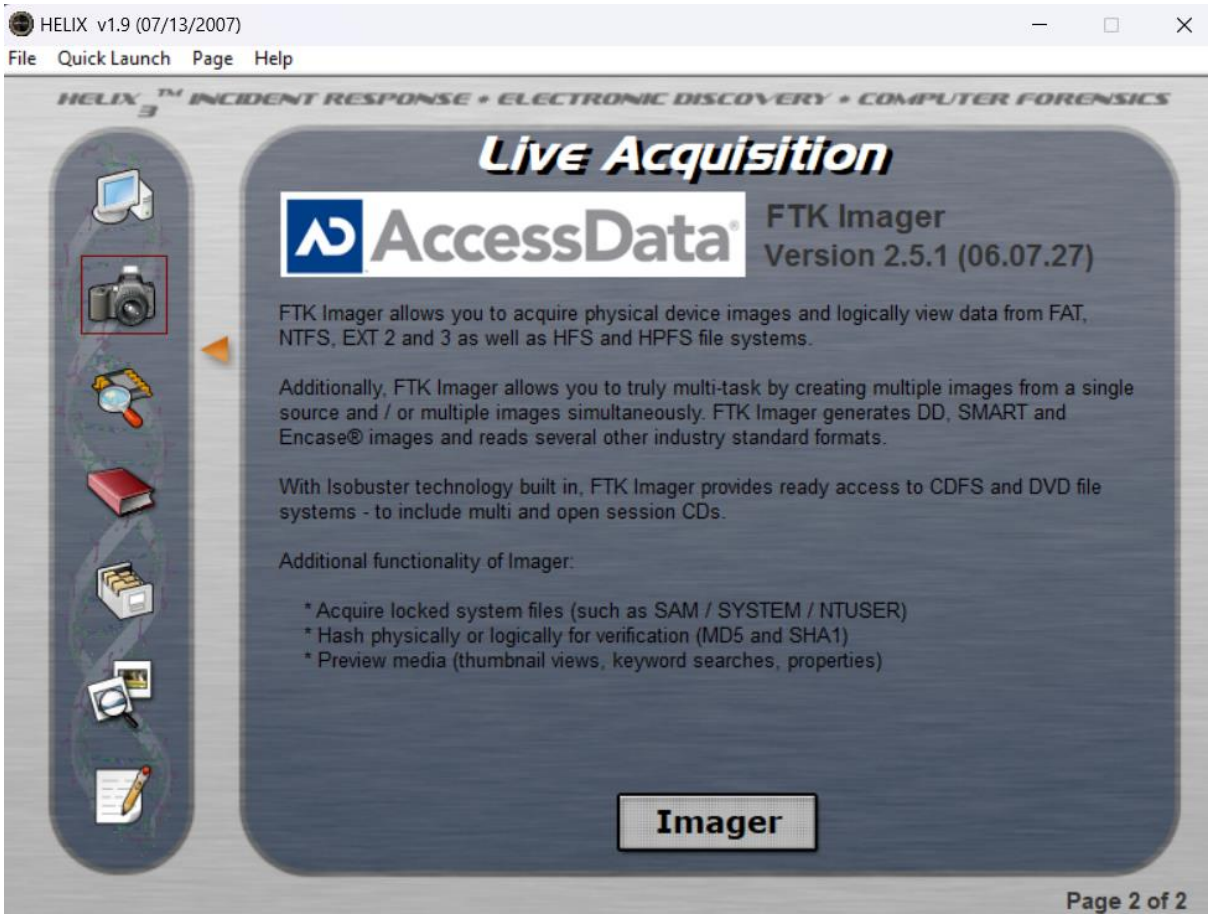


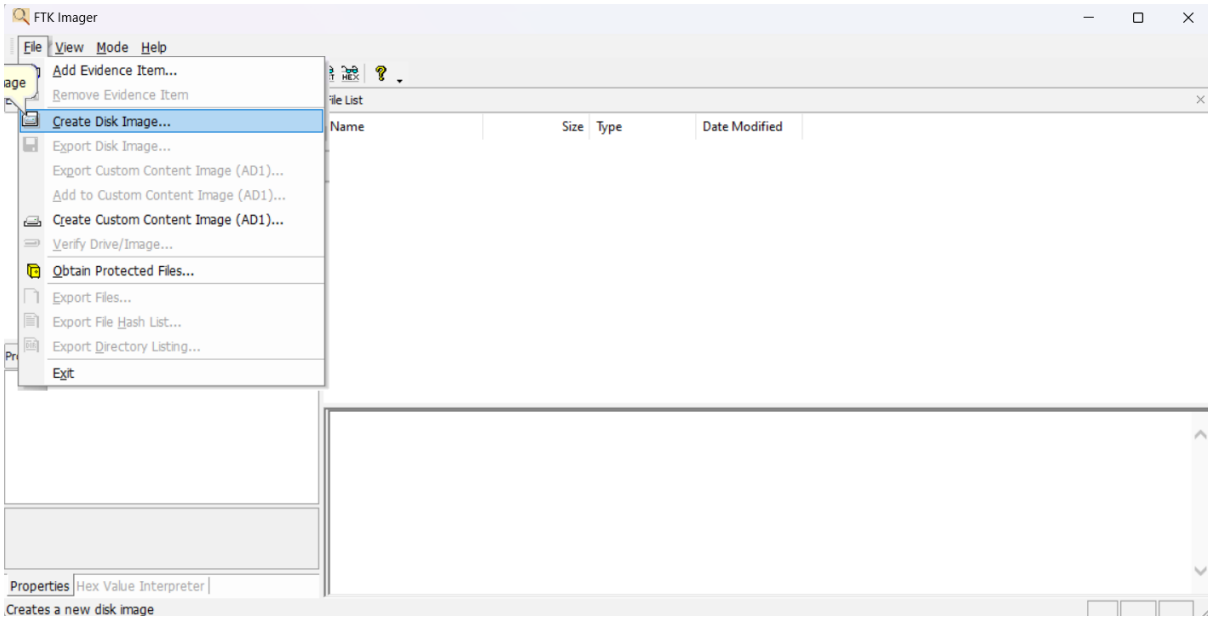
By clicking that yellow arrow in front of system symbol we can see all the process running in our system.



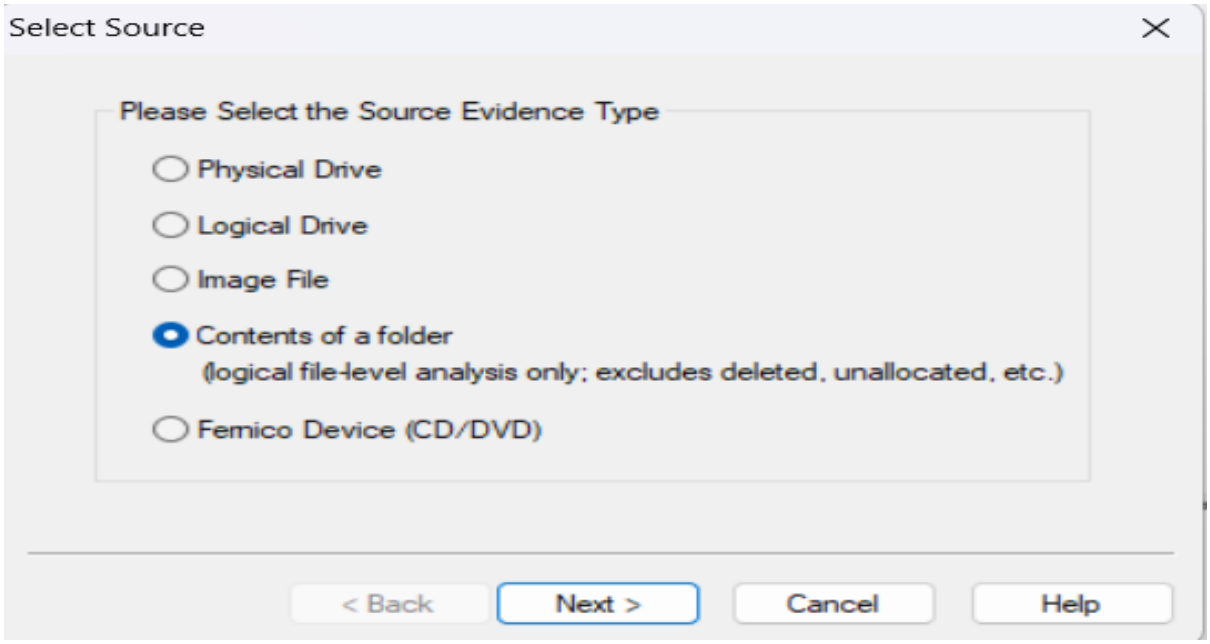
Click the acquisition icon to acquire physical memory or disk drives.

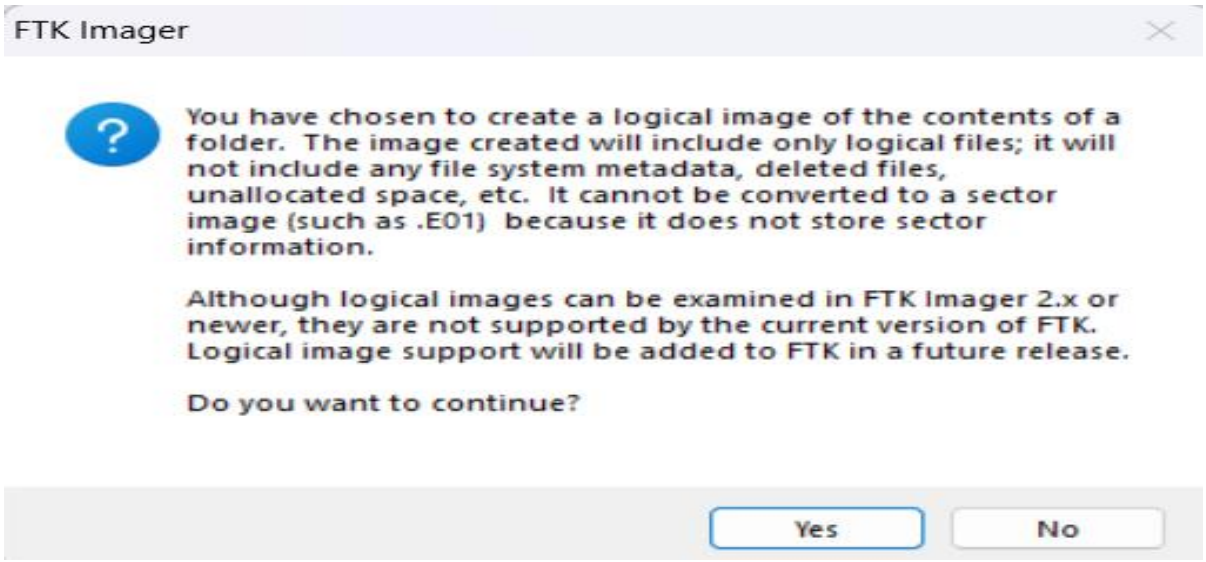
To create an image of a folder with the help of AccessData FTK Imager Click imager.

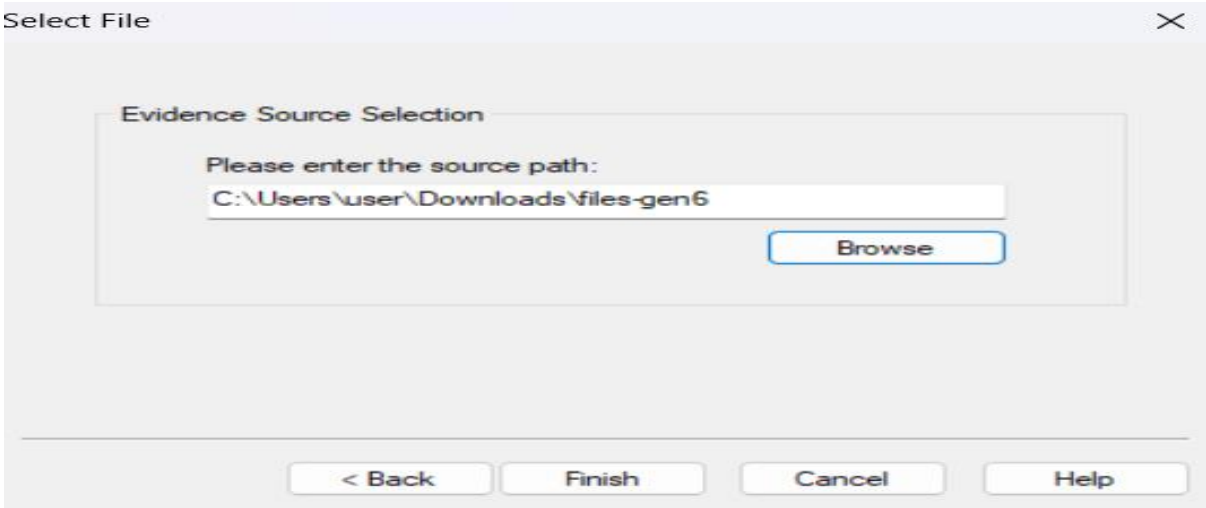


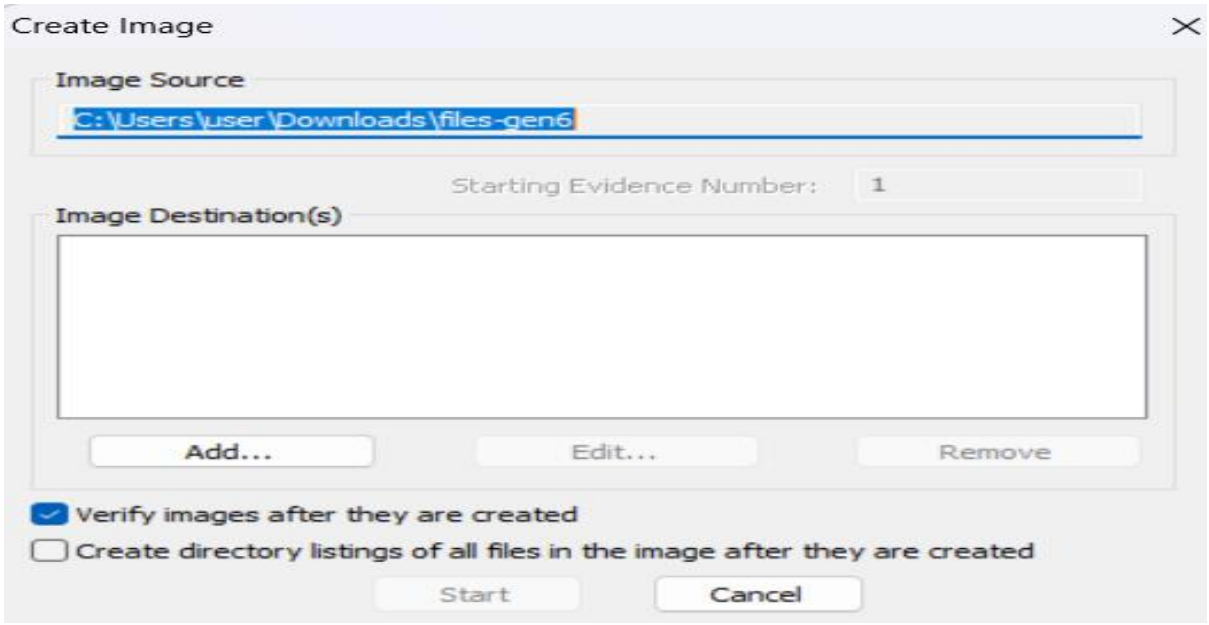


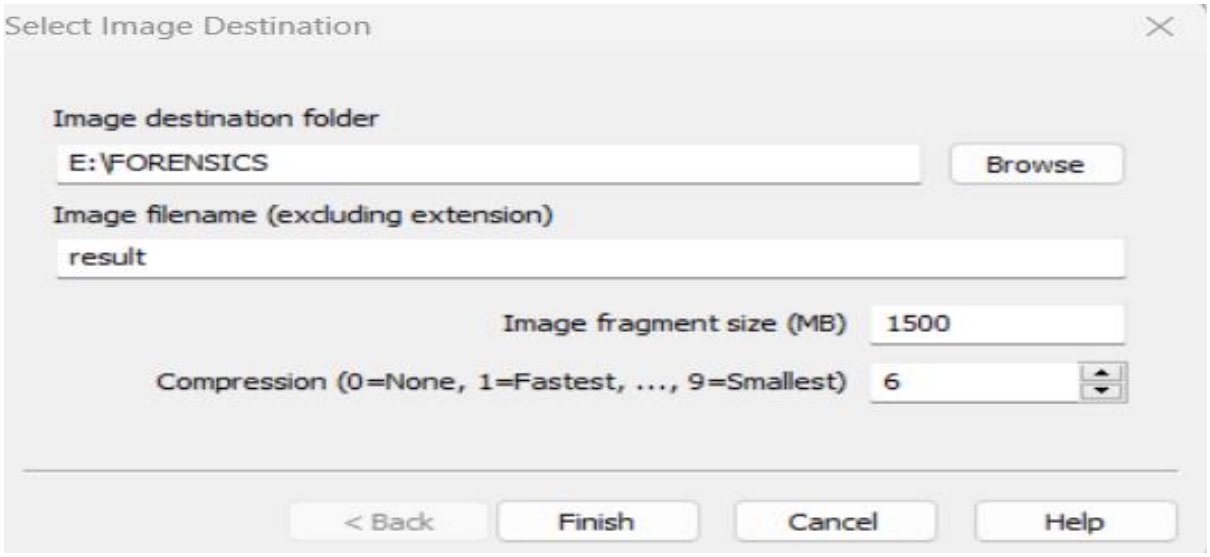
Choose contents of a folder as evidence type. And then click next to create an image.

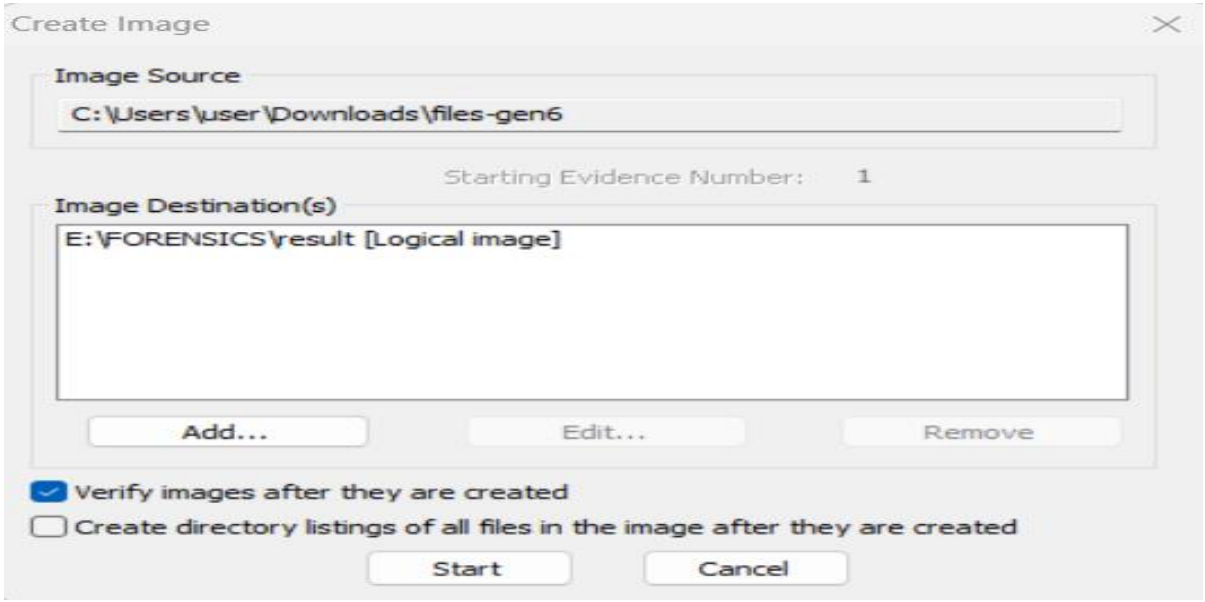

Select Source
Please Select the Source Evidence Type
Physical Drive
Logical Drive
Image File
Contents of a folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)
Femico Device (CD/DVD)
< Back
Next >
Cancel
Help

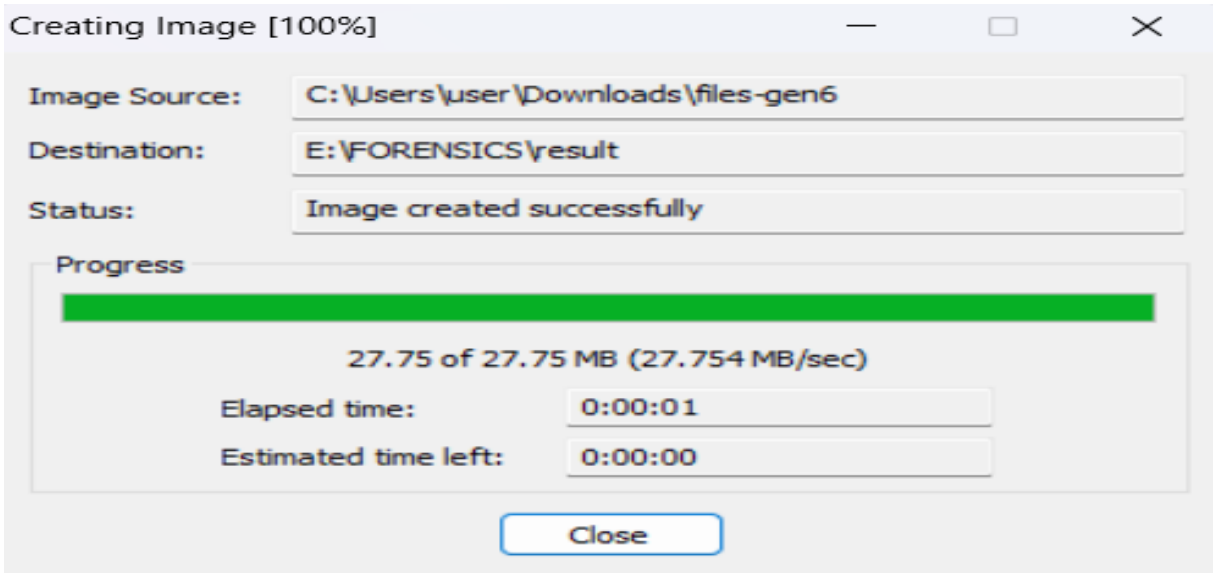

FTK Imager
You have chosen to create a logical image of the contents of a folder. The image created will include only logical files; it will not include any file system metadata, deleted files, unallocated space, etc. It cannot be converted to a sector image (such as .E01) because it does not store sector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

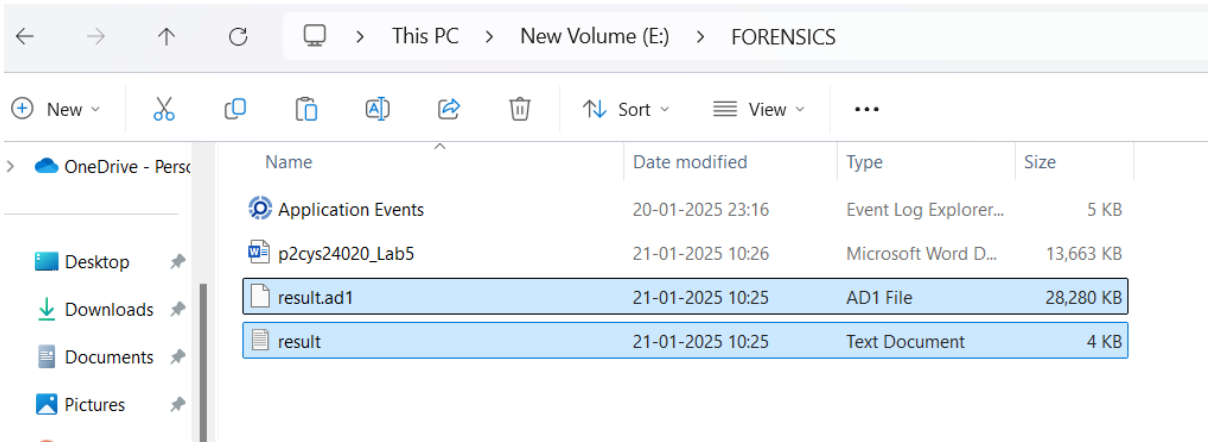

Select File
Evidence Source Selection
Please enter the source path:
C:\Users\user\Downloads\files-gen6
Browse
< Back
Finish
Cancel
Help

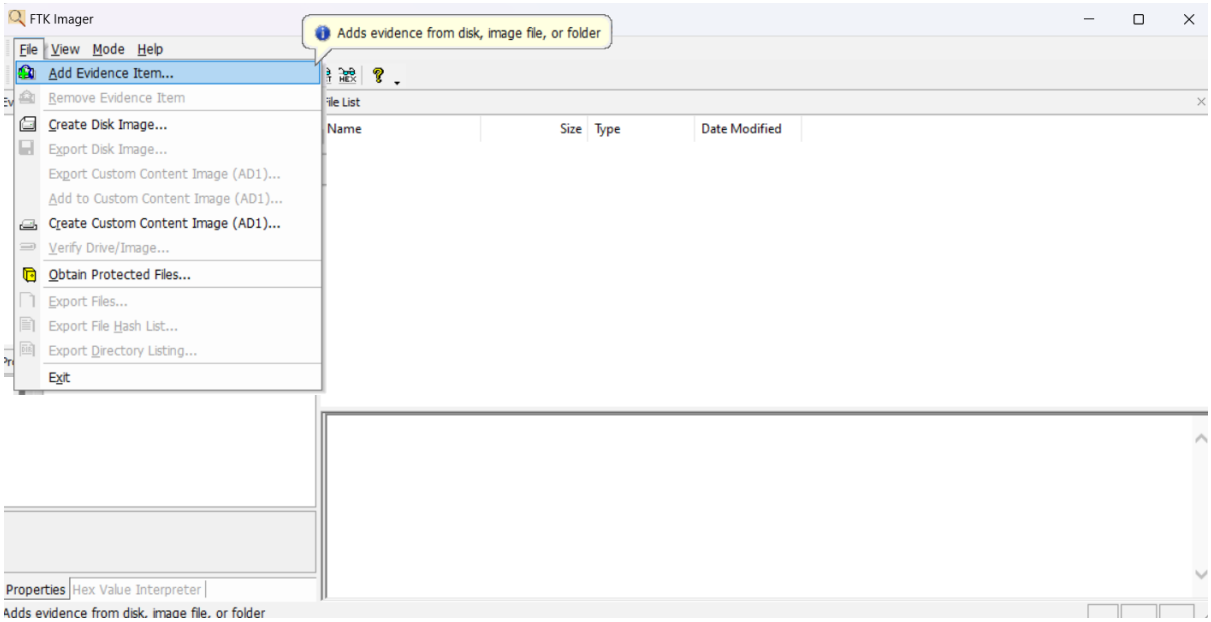

Create Image
Image Source
C:\Users\user\Downloads\files-gen6
Starting Evidence Number: 1
Image Destination(s)
Add...
Edit...
Remove
Verify images after they are created
Create directory listings of all files in the image after they are created
Start
Cancel

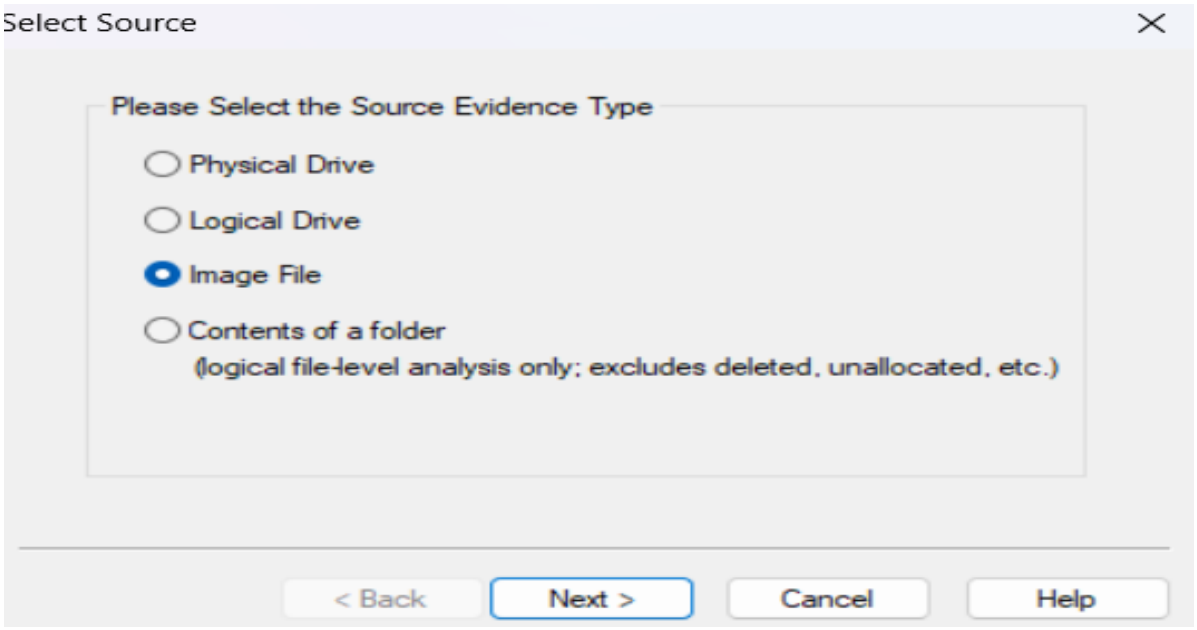

Select Image Destination
Image destination folder
E:\FORENSICS
Browse
Image filename (excluding extension)
result
Image fragment size (MB) 1500
Compression (0=None, 1=Fastest, ..., 9=Smallest) 6
< Back
Finish
Cancel
Help

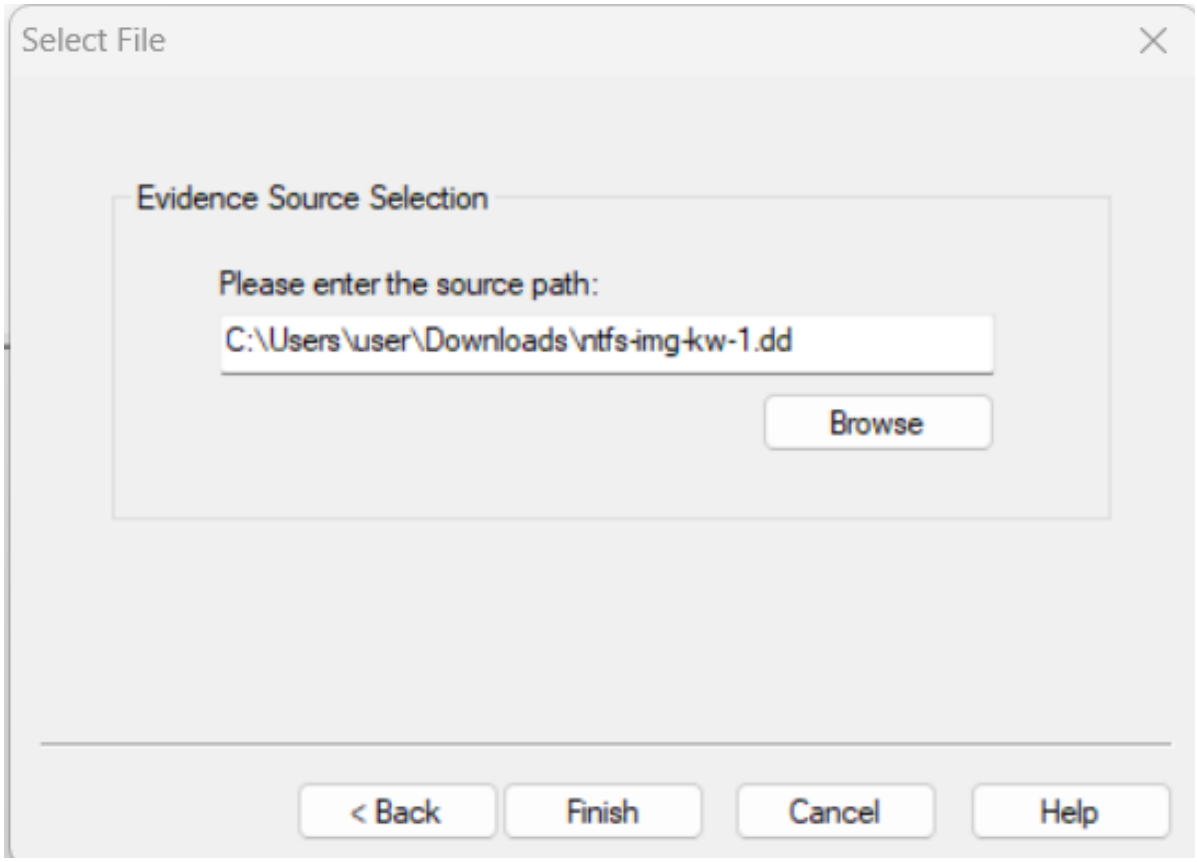

Create Image
Image Source
C:\Users\user\Downloads\files-gen6
Starting Evidence Number: 1
Image Destination(s)
E:\FORENSICS\result [Logical image]
Add...
Edit...
Remove
Verify images after they are created
Create directory listings of all files in the image after they are created
Start
Cancel

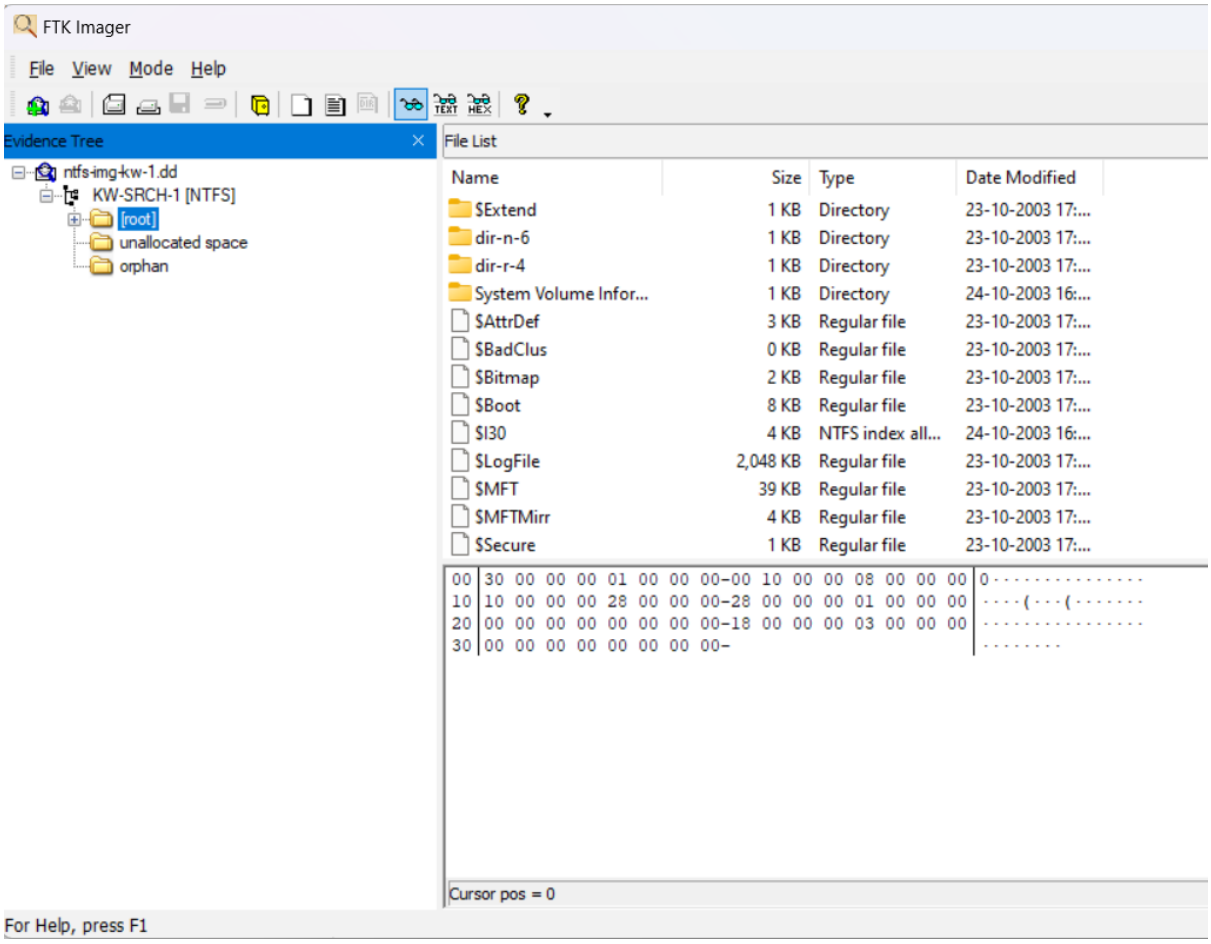

Creating Image [100%]
Image Source:
C:\Users\user\Downloads\files-gen6
Destination:
E:\FORENSICS\result
Status:
Image created successfully
Progress
27.75 of 27.75 MB (27.754 MB/sec)
Elapsed time:
0:00:01
Estimated time left:
0:00:00
Close

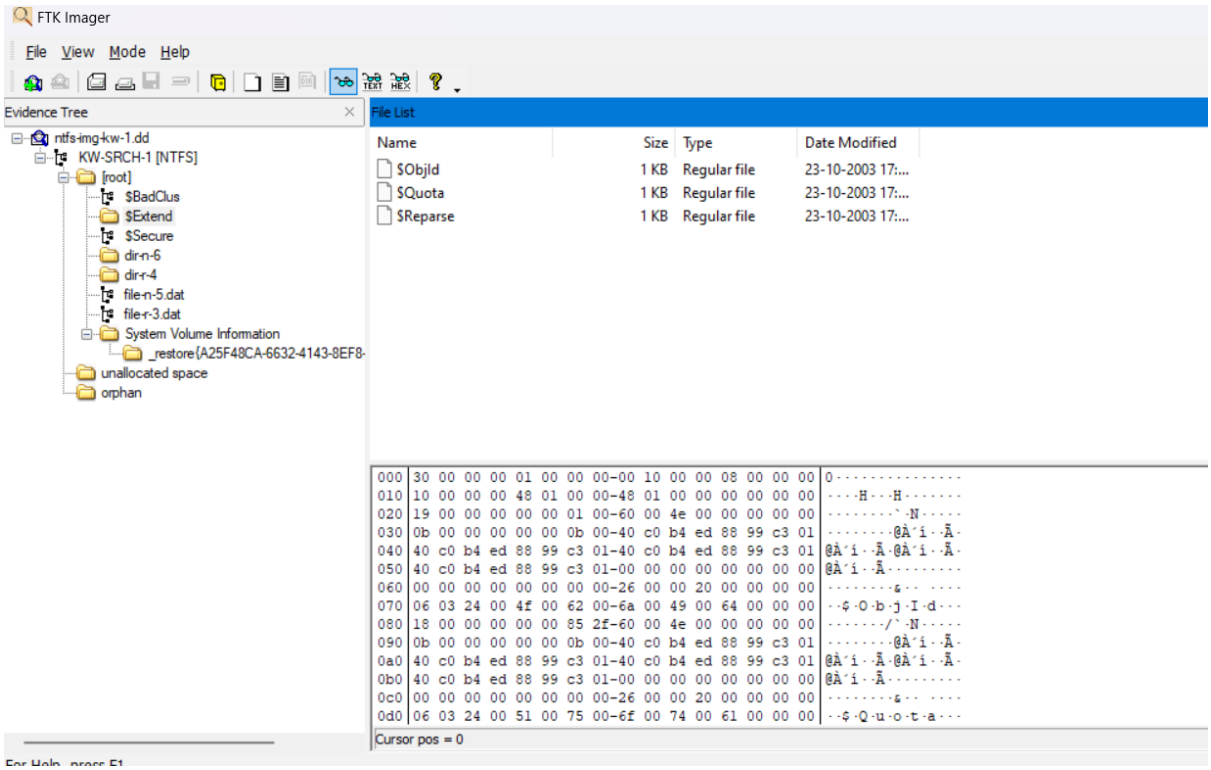

This PC
New Volume (E:)
FORENSICS
New
Sort
View
OneDrive - Perso
Desktop
Downloads
Documents
Pictures
Name
Date modified
Type
Size
Application Events
20-01-2025 23:16
Event Log Explorer...
5 KB
p2cys24020_Lab5
21-01-2025 10:26
Microsoft Word D...
13,663 KB
result.ad1
21-01-2025 10:25
AD1 File
28,280 KB
result
21-01-2025 10:25
Text Document
4 KB


FTK Imager
File View Mode Help
Add Evidence Item...
Remove 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...
Exit
Adds evidence from disk, image file, or folder
File List
Name
Size
Type
Date Modified
Properties
Hex Value Interpreter
Adds evidence from disk, image file, or folder

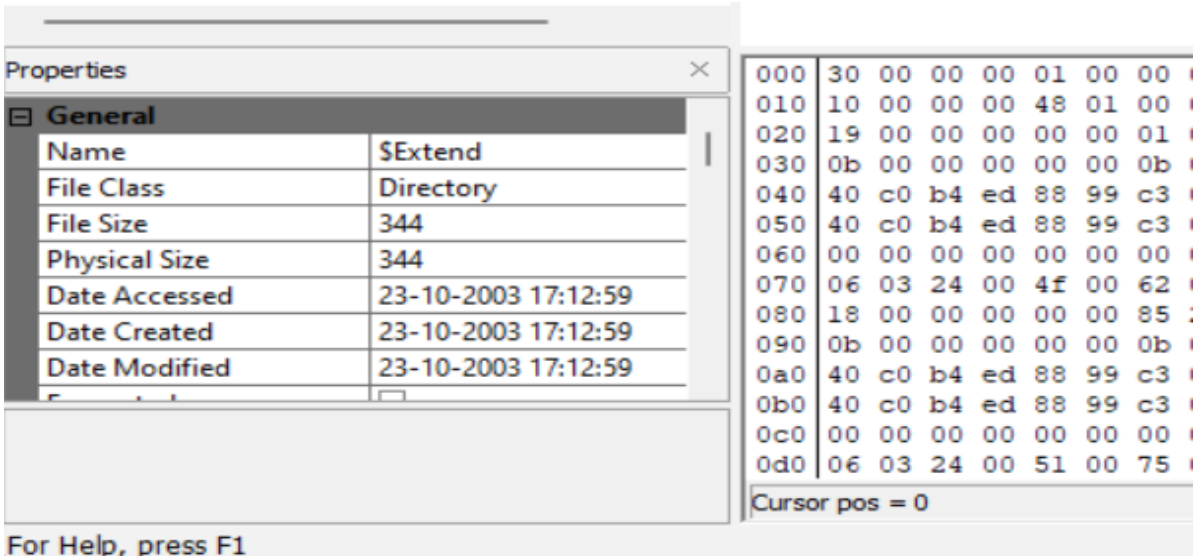

Select Source
Please Select the Source Evidence Type
Physical Drive
Logical Drive
Image File
Contents of a folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)
< Back
Next >
Cancel
Help


Select File
Evidence Source Selection
Please enter the source path:
C:\Users\user\Downloads\ntfs-img-kw-1.dd
Browse
< Back
Finish
Cancel
Help

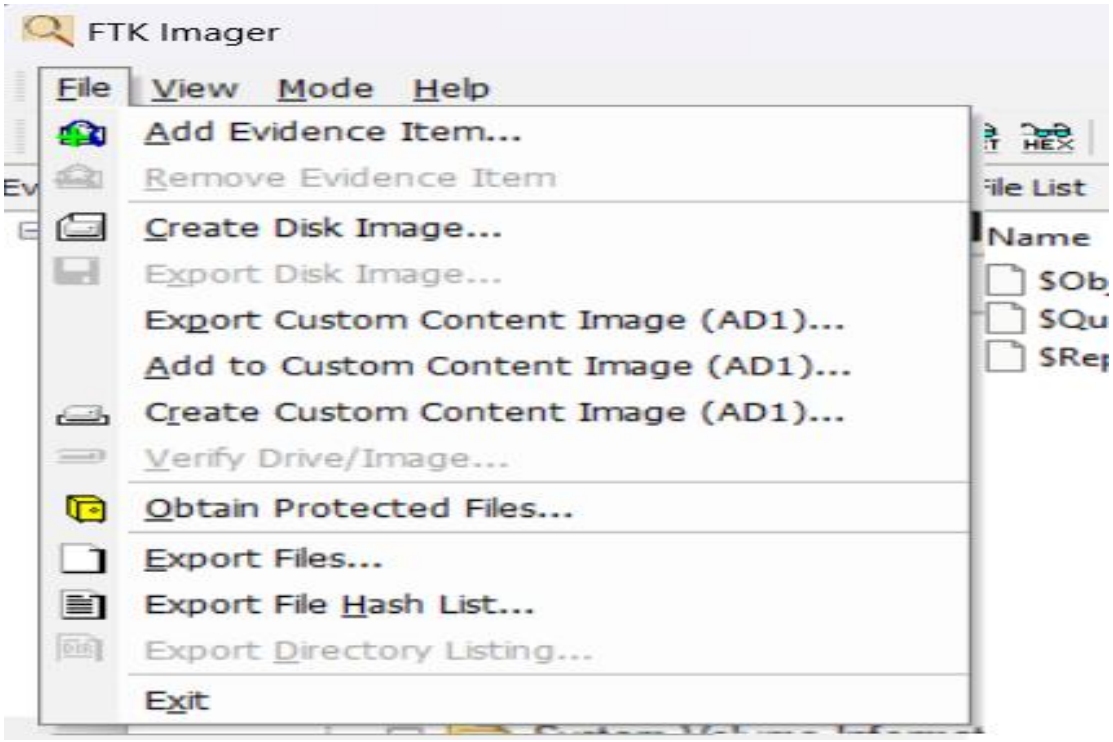


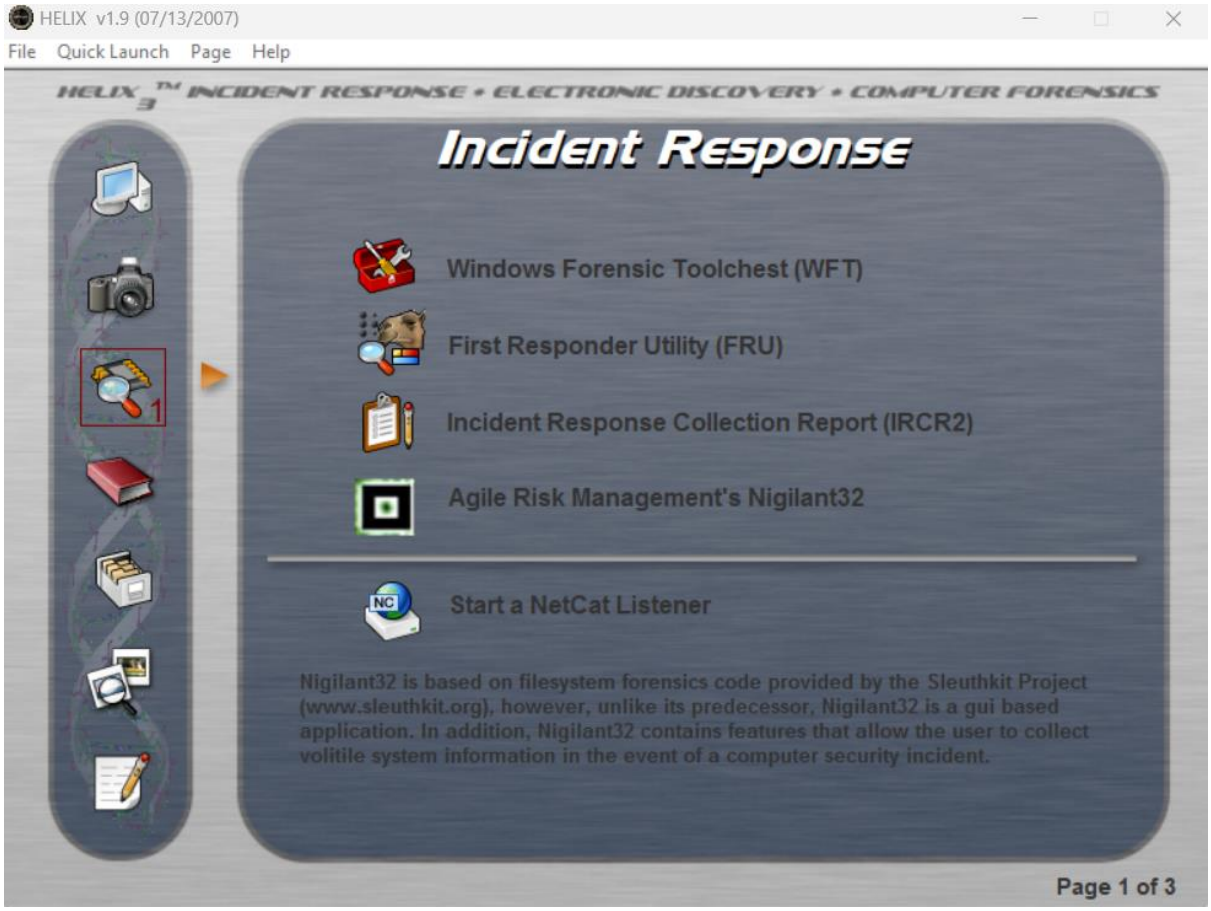


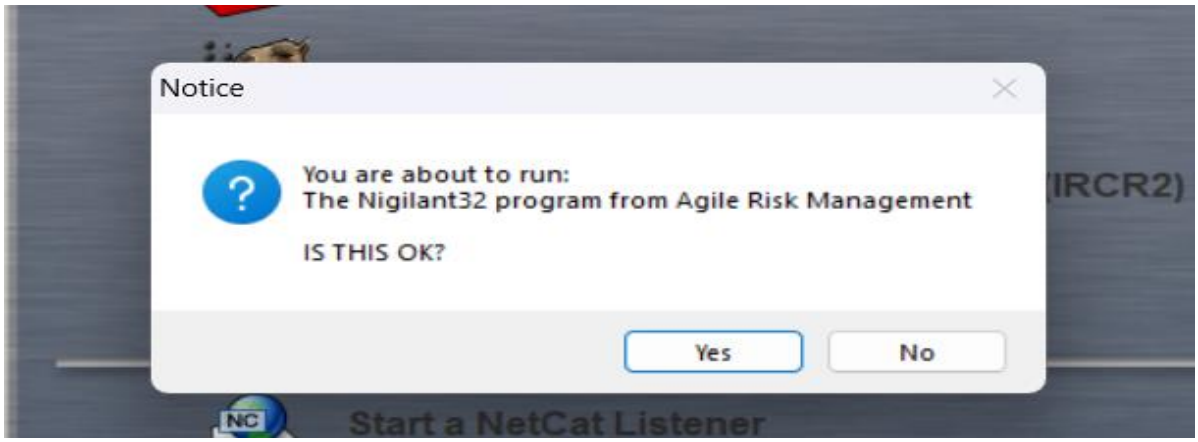
Properties of the image file can be viewed by clicking the properties tab.

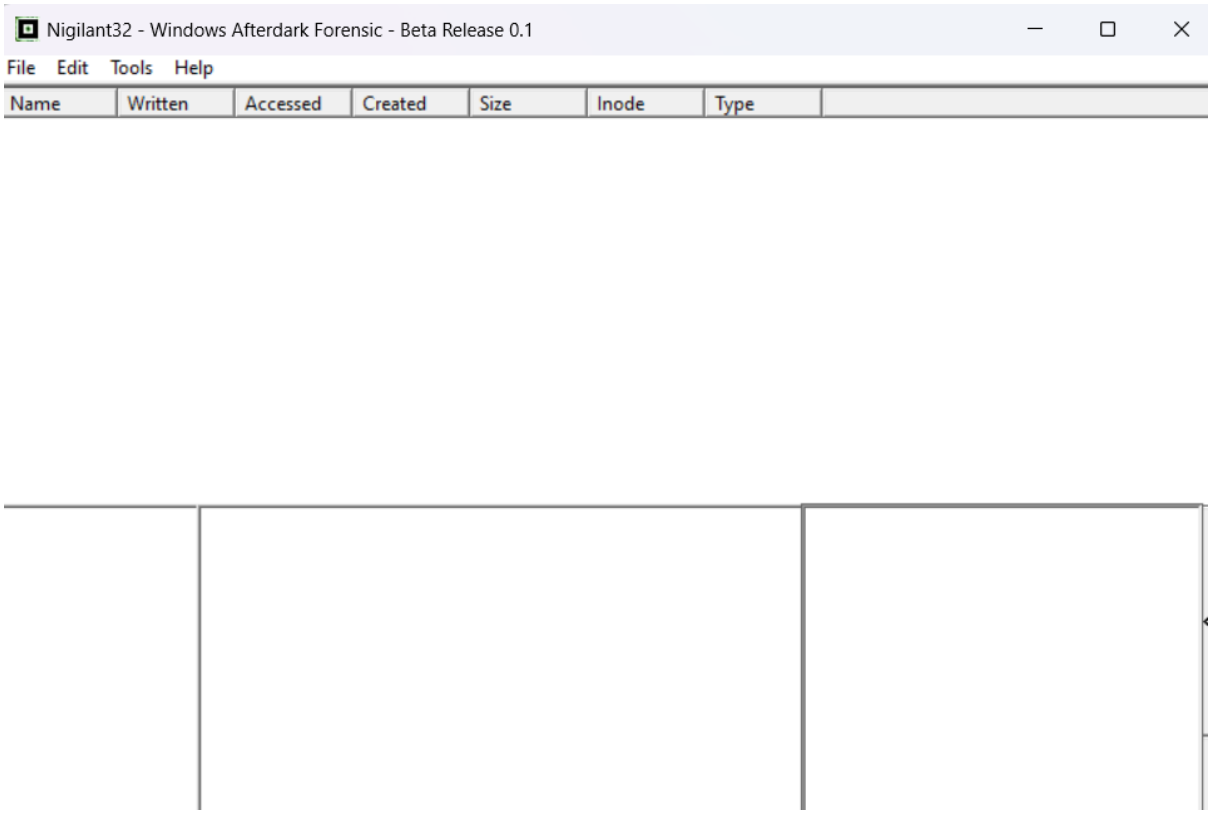


Now exit the ftk imager by clicking exit in file menu

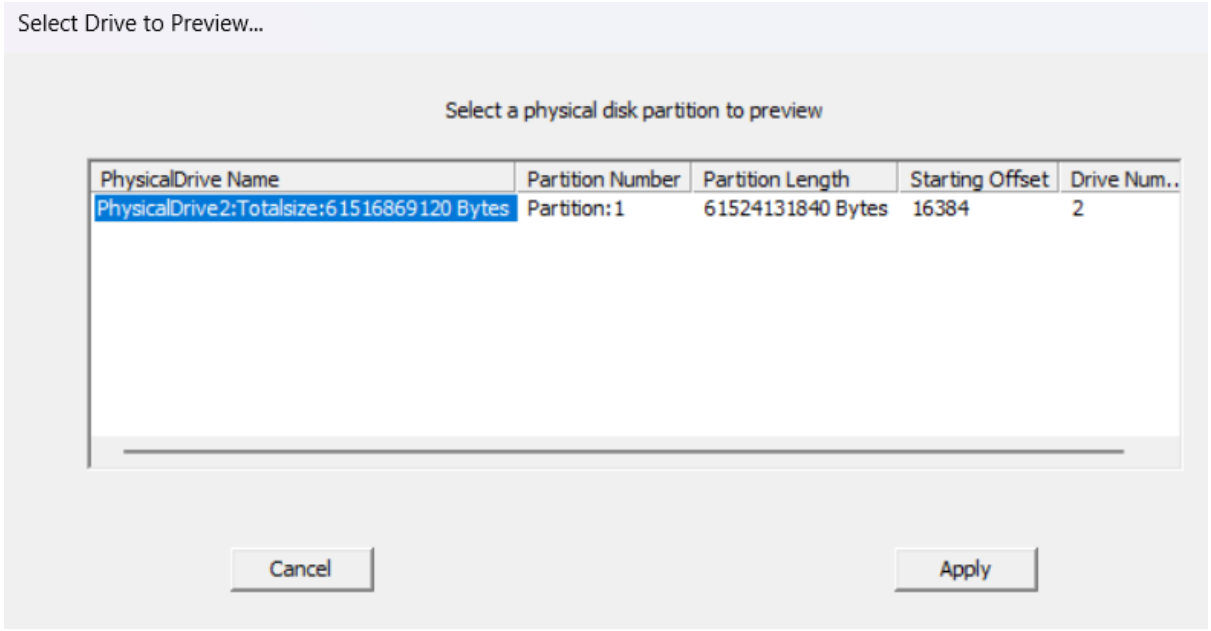



HELIX v1.9 (07/13/2007)
File Quick Launch Page Help
HELIX 3™ INCIDENT RESPONSE • ELECTRONIC DISCOVERY • COMPUTER FORENSICS
Incident Response
Windows Forensic Toolchest (WFT)
First Responder Utility (FRU)
Incident Response Collection Report (IRCR2)
Agile Risk Management's Nigilant32
Start a NetCat Listener
Nigilant32 is based on filesystem forensics code provided by the Sleuthkit Project (www.sleuthkit.org), however, unlike its predecessor, Nigilant32 is a gui based application. In addition, Nigilant32 contains features that allow the user to collect volitile system information in the event of a computer security incident.
Page 1 of 3

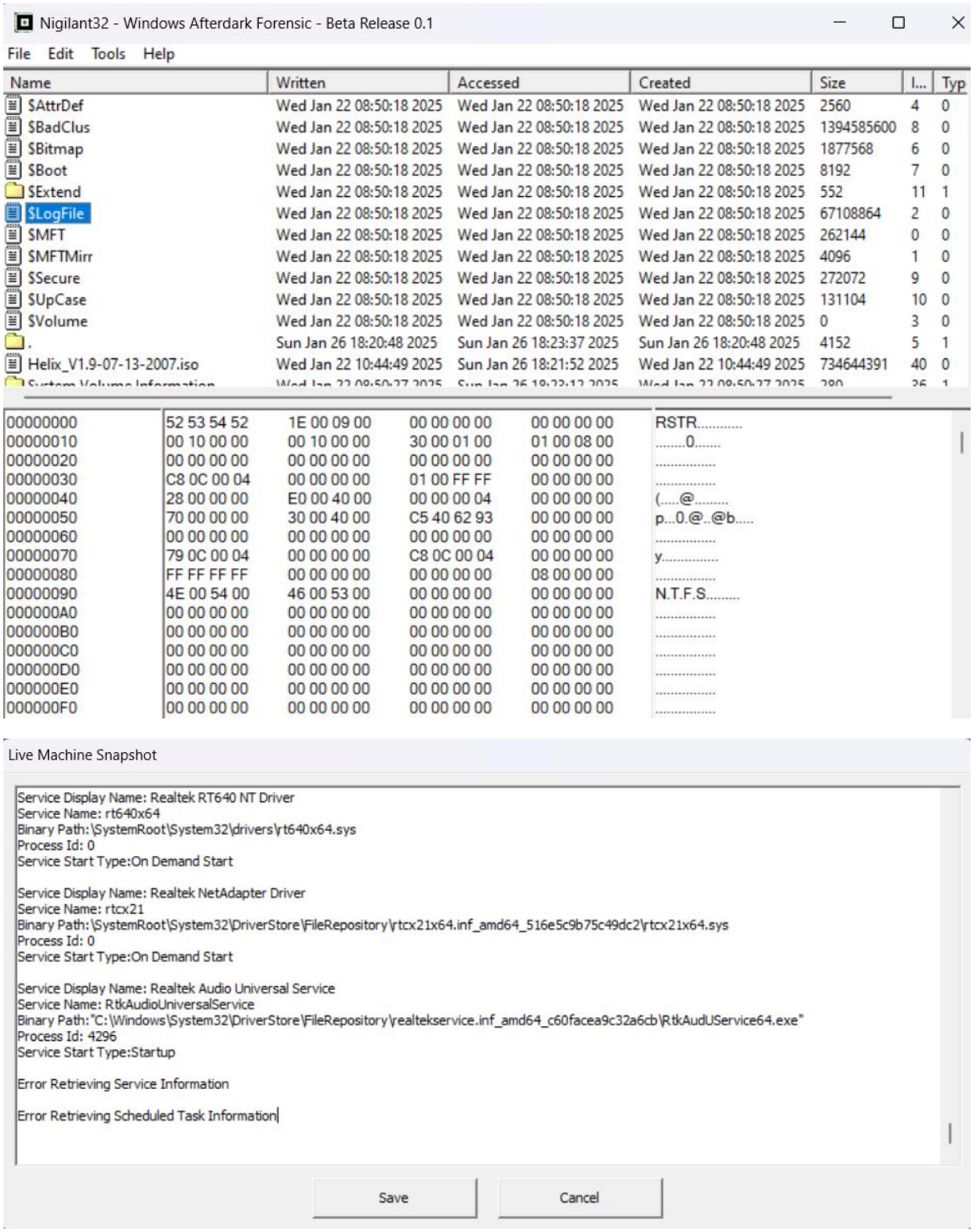

Notice
You are about to run:
The Nigilant32 program from Agile Risk Management
IS THIS OK?
Yes
No
Start a NetCat Listener

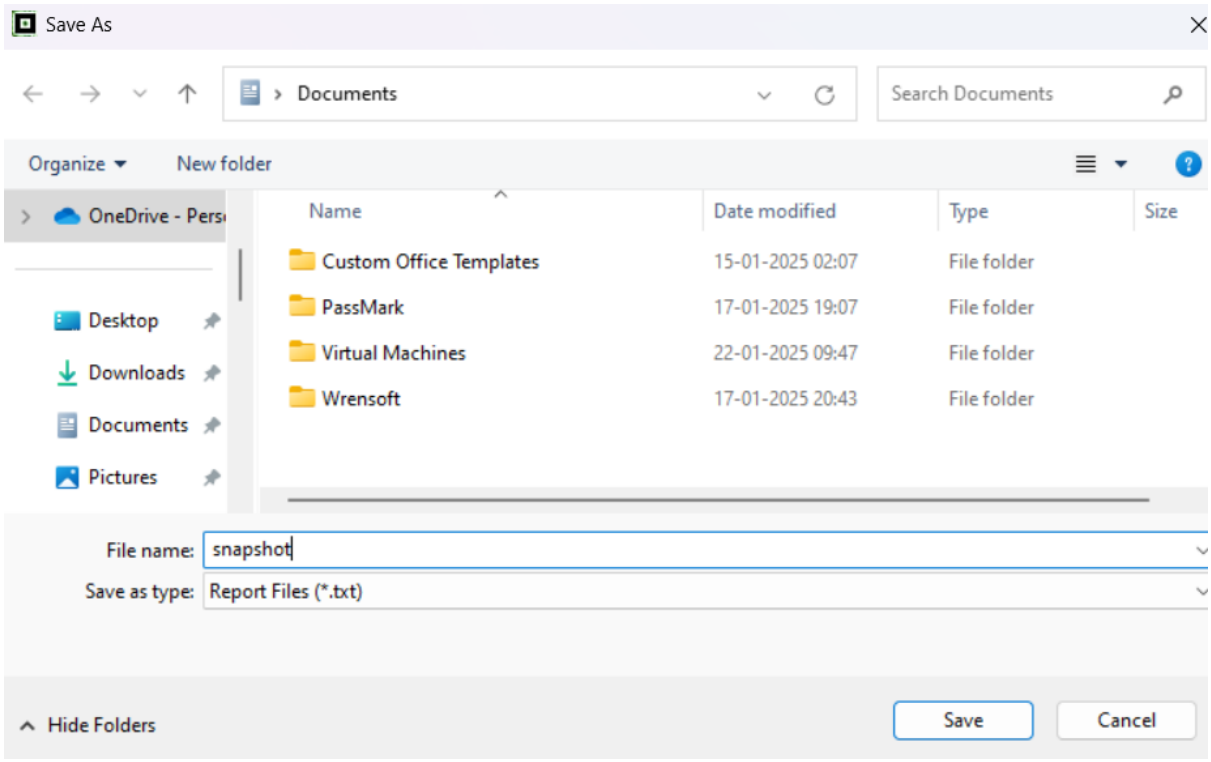


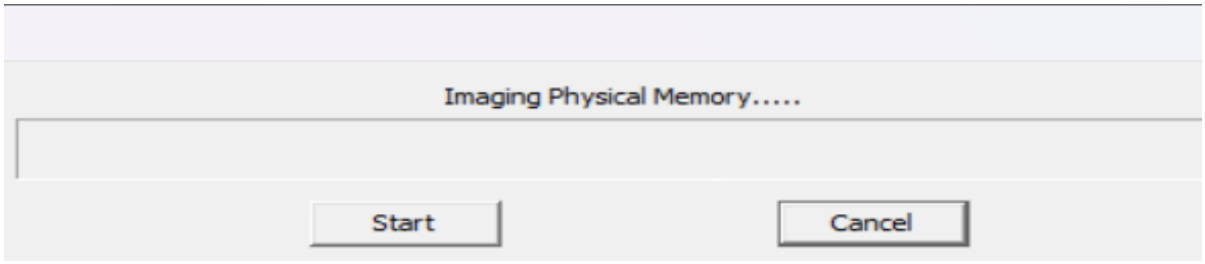
Here we can preview the hard drive

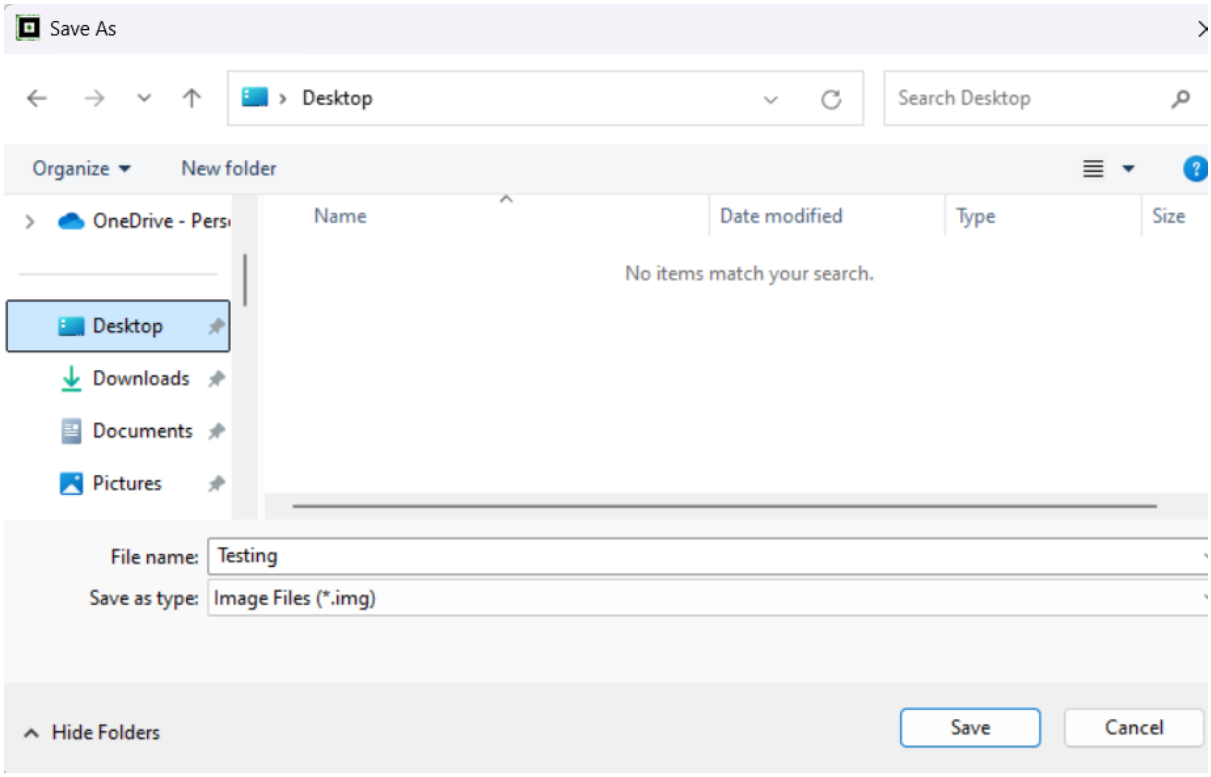


It displays the files and folders pertaining to the partition.

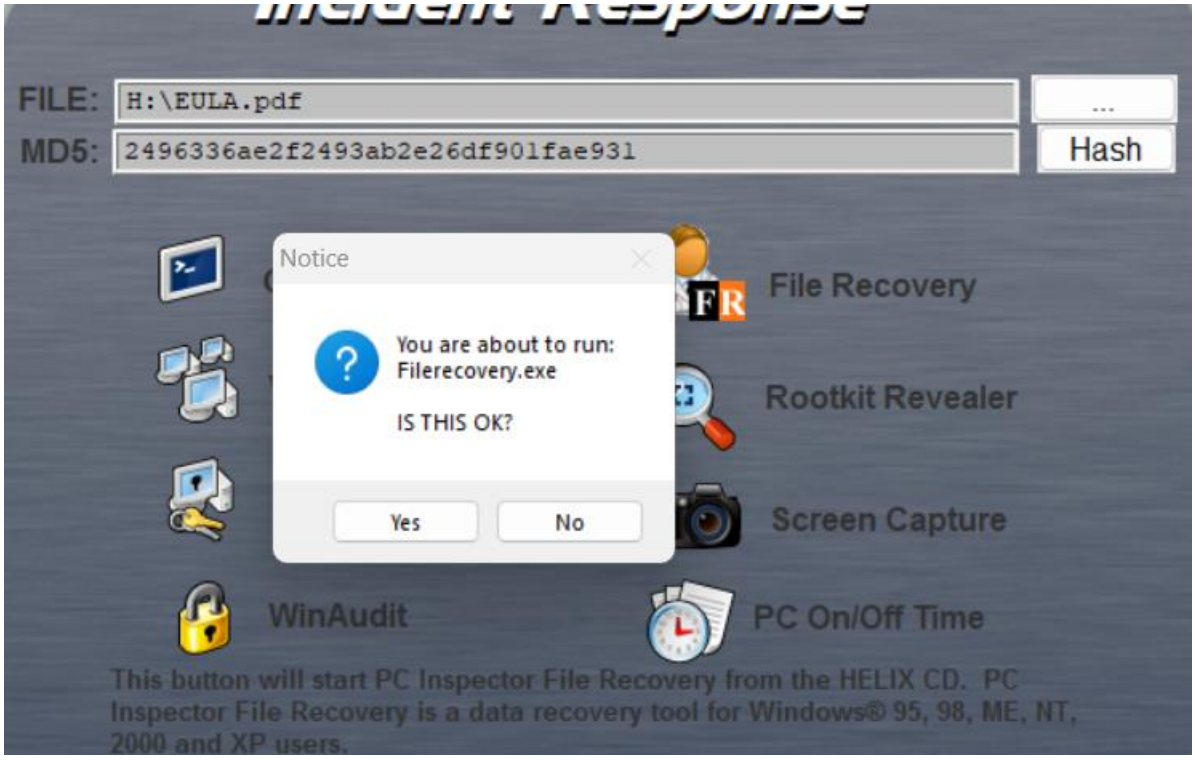

Nigilant32 - Windows Afterdark Forensic - Beta Release 0.1
File Edit Tools Help
Name Written Accessed Created Size I... Typ
$AttrDef Wed Jan 22 08:50:18 2025 Wed Jan 22 08:50:18 2025 Wed Jan 22 08:50:18 2025 2560 4 0
$BadClus Wed Jan 22 08:50:18 2025 Wed Jan 22 08:50:18 2025 Wed Jan 22 08:50:18 2025 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
$MFT Wed Jan 22 08:50:18 2025 Wed Jan 22 08:50:18 2025 Wed Jan 22 08:50:18 2025 262144 0 0
$MFTMirr 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
00000000 52 53 54 52 1E 00 09 00 00 00 00 00 00 00 00 00 RSTR.....
00000010 00 10 00 00 00 10 00 00 30 00 01 00 01 00 08 00 ....0.....
00000020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000030 C8 0C 00 04 00 00 00 00 01 00 FF FF 00 00 00 00 .....
00000040 28 00 00 00 E0 00 40 00 00 00 00 04 00 00 00 00 (.....@.....
00000050 70 00 00 00 30 00 40 00 C5 40 62 93 00 00 00 00 p...0.@..@b.....
00000060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000070 79 0C 00 04 00 00 00 00 C8 0C 00 04 00 00 00 00 y.....
00000080 FF FF FF FF 00 00 00 00 00 00 00 00 08 00 00 00 .....
00000090 4E 00 54 00 46 00 53 00 00 00 00 00 00 00 00 00 N.T.F.S.....
000000A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000000B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000000C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000000D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000000E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000000F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
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


Save As
Documents
Search Documents
Organize
New folder
OneDrive - Pers
Name
Date modified
Type
Size
Custom Office Templates
15-01-2025 02:07
File folder
PassMark
17-01-2025 19:07
File folder
Virtual Machines
22-01-2025 09:47
File folder
Wrensoft
17-01-2025 20:43
File folder
Desktop
Downloads
Documents
Pictures
File name:
snapshot
Save as type:
Report Files (*.txt)
Hide Folders
Save
Cancel

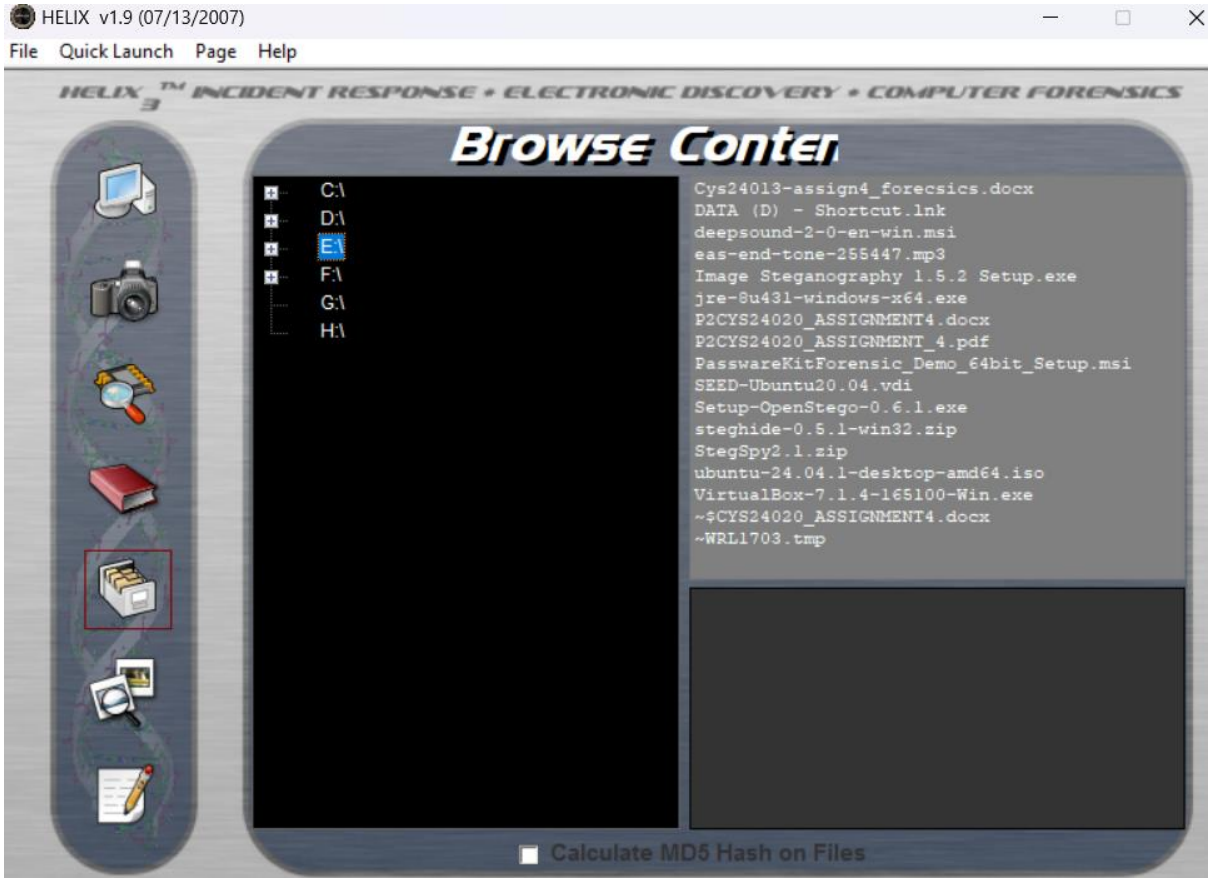

Imaging Physical Memory.....
Start
Cancel

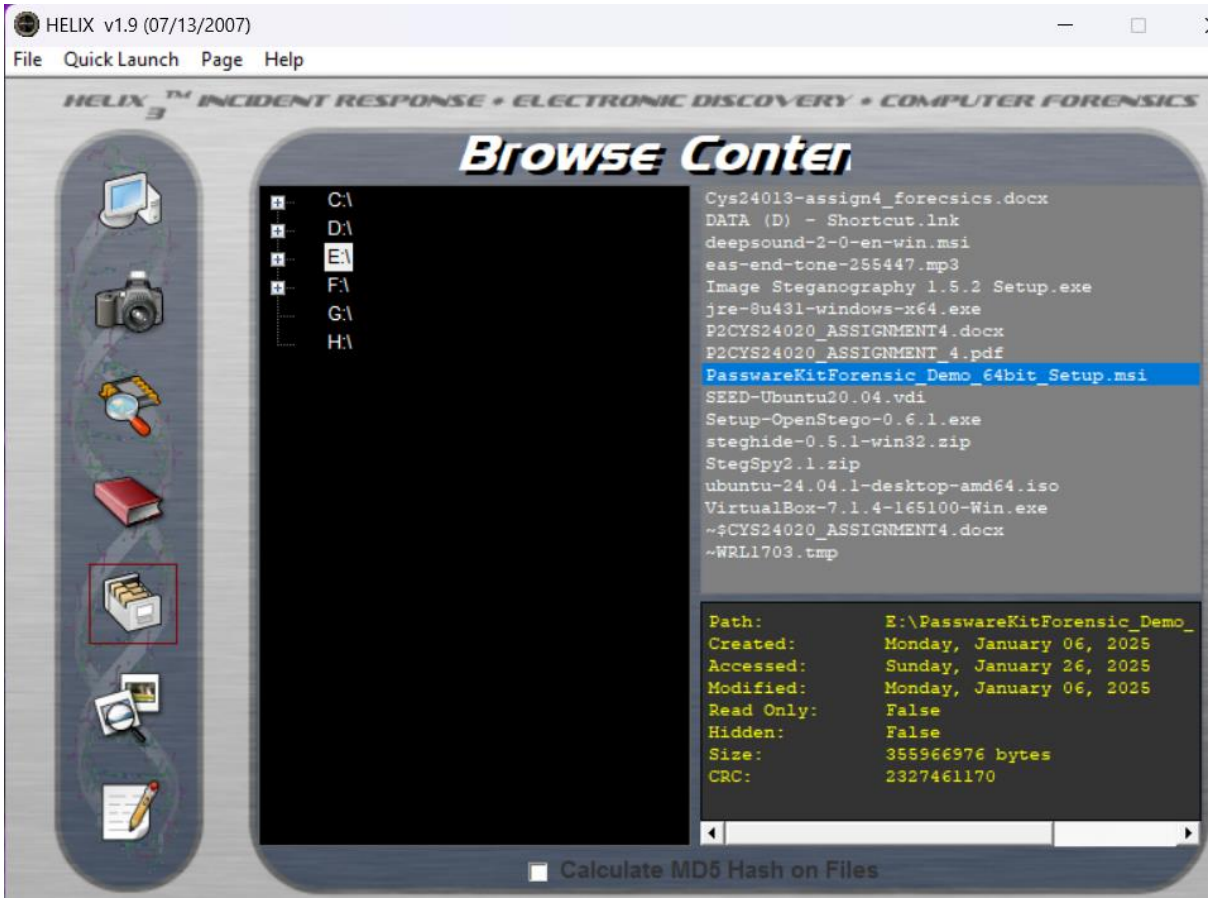

Save As
Desktop
Search Desktop
Organize
New folder
OneDrive - Pers
Name
Date modified
Type
Size
No items match your search.
Desktop
Downloads
Documents
Pictures
File name:
Testing
Save as type:
Image Files (*.img)
Hide Folders
Save
Cancel

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

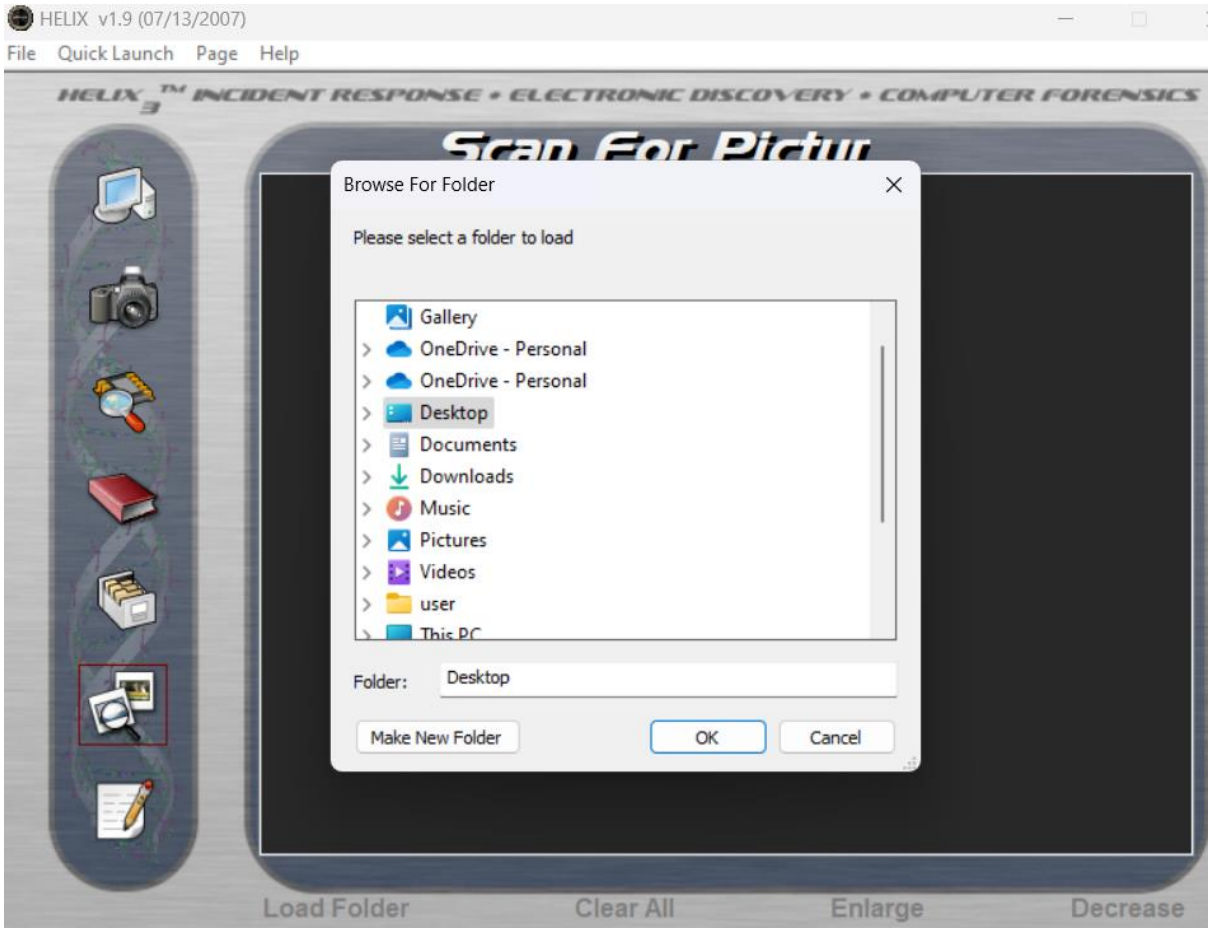


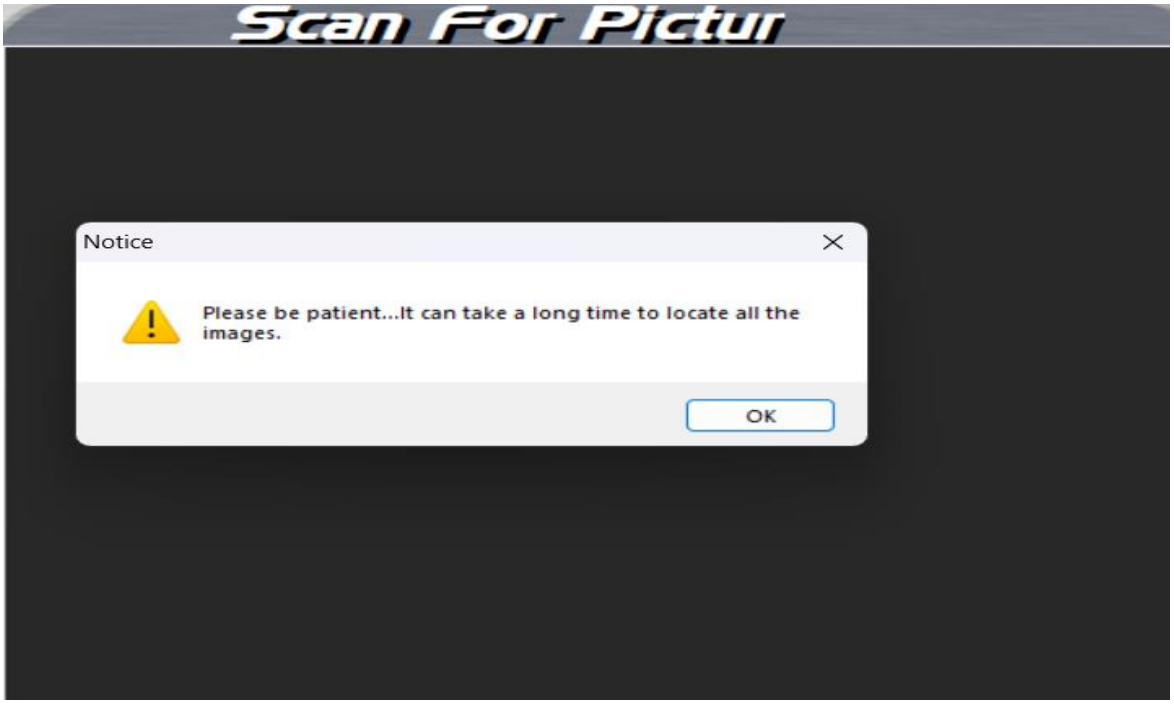
To know the content of drive click browse icon in left pane.it displays the drive.


HELIX v1.9 (07/13/2007)
File Quick Launch Page Help
INCIDENT RESPONSE • ELECTRONIC DISCOVERY • COMPUTER FORENSICS
Browse Conten
C:\
D:\
E:\
F:\
G:\
H:\
Cys24013-assign4_forecsics.docx
DATA (D) - Shortcut.lnk
deepsound-2-0-en-win.msi
eas-end-tone-255447.mp3
Image Steganography 1.5.2 Setup.exe
jre-8u431-windows-x64.exe
P2CYS24020_ASSIGNMENT4.docx
P2CYS24020_ASSIGNMENT_4.pdf
PasswareKitForensic_Demo_64bit_Setup.msi
SEED-Ubuntu20.04.vdi
Setup-OpenStego-0.6.1.exe
steghide-0.5.1-win32.zip
StegSpy2.1.zip
ubuntu-24.04.1-desktop-amd64.iso
VirtualBox-7.1.4-165100-Win.exe
~$CYS24020_ASSIGNMENT4.docx
~WRL1703.tmp
Calculate MD5 Hash on Files


HELIX v1.9 (07/13/2007)
File Quick Launch Page Help
INCIDENT RESPONSE • ELECTRONIC DISCOVERY • COMPUTER FORENSICS
Browse Conten
C:\
D:\
E:\
F:\
G:\
H:\
Cys24013-assign4_forecsics.docx
DATA (D) - Shortcut.lnk
deepsound-2-0-en-win.msi
eas-end-tone-255447.mp3
Image Steganography 1.5.2 Setup.exe
jre-8u431-windows-x64.exe
P2CYS24020_ASSIGNMENT4.docx
P2CYS24020_ASSIGNMENT_4.pdf
PasswareKitForensic_Demo_64bit_Setup.msi
SEED-Ubuntu20.04.vdi
Setup-OpenStego-0.6.1.exe
steghide-0.5.1-win32.zip
StegSpy2.1.zip
ubuntu-24.04.1-desktop-amd64.iso
VirtualBox-7.1.4-165100-Win.exe
~$CYS24020_ASSIGNMENT4.docx
~WRL1703.tmp
Path: E:\PasswareKitForensic_Demo_
Created: Monday, January 06, 2025
Accessed: Sunday, January 26, 2025
Modified: Monday, January 06, 2025
Read Only: False
Hidden: False
Size: 355966976 bytes
CRC: 2327461170
Calculate MD5 Hash on Files

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.

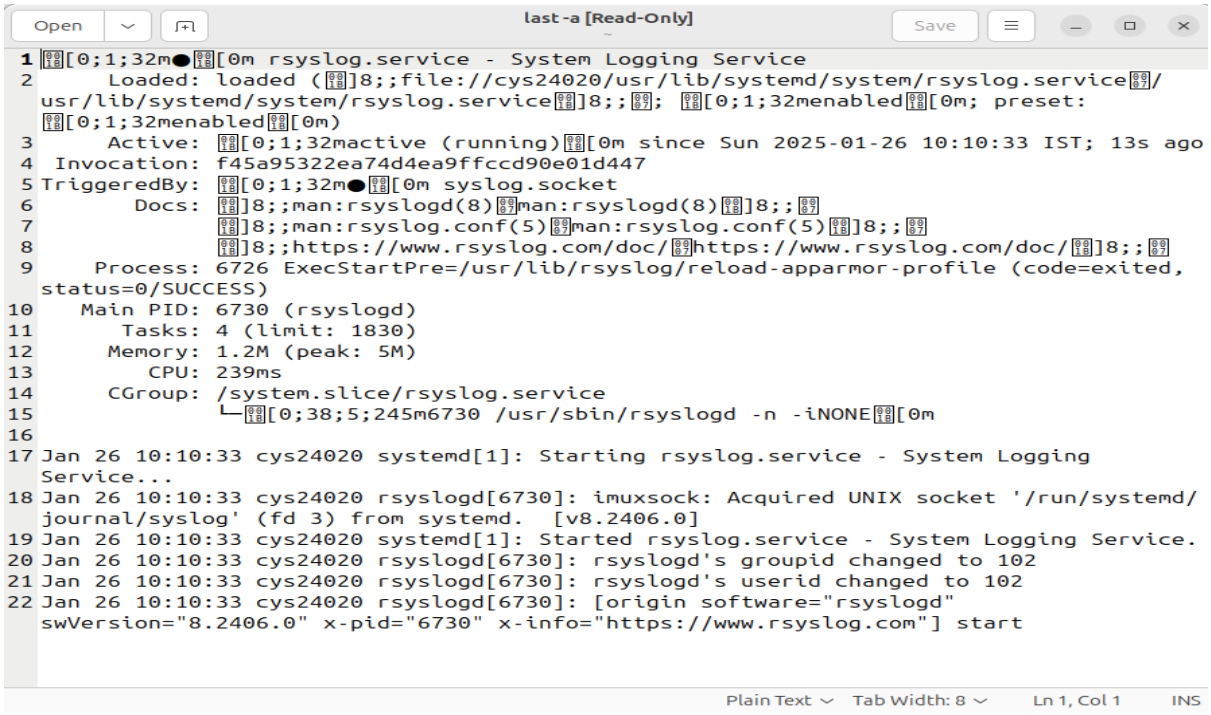
```
root@cys24020:/home/theertha# lshw -short
H/W path           Device      Class          Description
========================================================
                               system         VMware Virtual Platform
/0                             bus            440BX Desktop Reference Platform
/0/0                           memory         86KiB BIOS
/0/1                           processor      11th Gen Intel(R) Core(TM) i5-1135G7 @
/0/1/0                         memory         16KiB L1 cache
/0/1/1                         memory         16KiB L1 cache
/0/2                           processor      11th Gen Intel(R) Core(TM) i5-1135G7 @
/0/5                           processor      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                 input0      input          Power Button
/3                 input1      input          AT Translated Set 2 keyboard
/4                 input3      input          VirtualPS/2 VMware VMMouse
/5                 input4      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



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 netwok 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, comtaining 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
systemd      1                            root  mem       REG              8,2   5604704     415690 /usr/lib/x86_64-
linux-gnu/libcrypto.so.3
systemd      1                            root  mem       REG              8,2    403704     415646 /usr/lib/x86_64-
linux-gnu/libbpf.so.1.4.5
systemd      1                            root  mem       REG              8,2    207072     415969 /usr/lib/x86_64-
linux-gnu/liblzma.so.5.6.2
systemd      1                            root  mem       REG              8,2   2182752     415656 /usr/lib/x86_64-
linux-gnu/libc.so.6
systemd      1                            root  mem       REG              8,2    121632     415753 /usr/lib/x86_64-
linux-gnu/libelf-0.191.so
systemd      1                            root  mem       REG              8,2    116960     415950 /usr/lib/x86_64-
linux-gnu/libkmod.so.2.4.1
systemd      1                            root  mem       REG              8,2    121272     416355 /usr/lib/x86_64-
linux-gnu/libz.so.1.3.1
systemd      1                            root  mem       REG              8,2    637712     416094 /usr/lib/x86_64-
linux-gnu/libpcre2-8.so.0.11.2
systemd      1                            root  mem       REG              8,2     26848     415668 /usr/lib/x86_64-
linux-gnu/libcap-ng.so.0.0.0
systemd      1                            root  mem       REG              8,2     72064     416074 /usr/lib/x86_64-
linux-gnu/libpam.so.0.85.1
```

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 f 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_DISP 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=un
confined msg='cwd=/home/theertha cmd=systemctl enable auditd 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
0anacron  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                     ens33
```

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 ?        Ss   11:47   0:06 /sbin/init splash
root           2  0.0  0.0      0     0 ?        S    11:47   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        S    11:47   0:00 [pool_workqueue_release]
root           4  0.0  0.0      0     0 ?        I<   11:47   0:00 [kworker/R-rcu_gp]
root           5  0.0  0.0      0     0 ?        I<   11:47   0:00 [kworker/R-sync_wq]
root           6  0.0  0.0      0     0 ?        I<   11:47   0:00 [kworker/R-slub_flushwq]
root           7  0.0  0.0      0     0 ?        I<   11:47   0:00 [kworker/R-netns]
root           8  0.0  0.0      0     0 ?        I    11:47   0:02 [kworker/0:0-events]
root          11  0.0  0.0      0     0 ?        I    11:47   0:00 [kworker/u512:0-ipv6_addrconf]
root          12  0.0  0.0      0     0 ?        I<   11:47   0:00 [kworker/R-mm_percpu_wq]
root          13  0.0  0.0      0     0 ?        I    11:47   0:00 [rcu_tasks_kthread]
root          14  0.0  0.0      0     0 ?        I    11:47   0:00 [rcu_tasks_rude_kthread]
root          15  0.0  0.0      0     0 ?        I    11:47   0:00 [rcu_tasks_trace_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]
```

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-d
aemon",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       kpagecgroup    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  cpuinfo      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]=5fc3af120dd06fc5a839efe9a7c6057b31b64573, 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]=cc26c0258b14008f18b0364da4a36fd0215fabe6, 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]=63e8b99215502138cb63afd6d65851a5e837ed49, 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]=488cca1472bb121a12e1c77bb58fe0a5c52f2aa9, stripped
/snap/gnome-42-2204/176/lib/x86_64-linux-gnu/libgpg-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), dy
```

```
/snap/gnome-42-2204/176/usr/lib/libcogl-path.so.20.4.3: ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamica
lly 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 l
inked, 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/libgiomm-2.4.so.1.3.0: ELF 64-bit LSB shared object, x86-64, version 1 (GNU/Linux), dyna
mically 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), dynamica
lly 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, versio
n 1 (GNU/Linux), dynamically linked, BuildID[sha1]=12ddbb551d176950685c5d3337e83eb0e3c2815e, 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 li
nked, BuildID[sha1]=25ece783035b2982eb58f3b5fe18bae64b0984ad, stripped
```

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

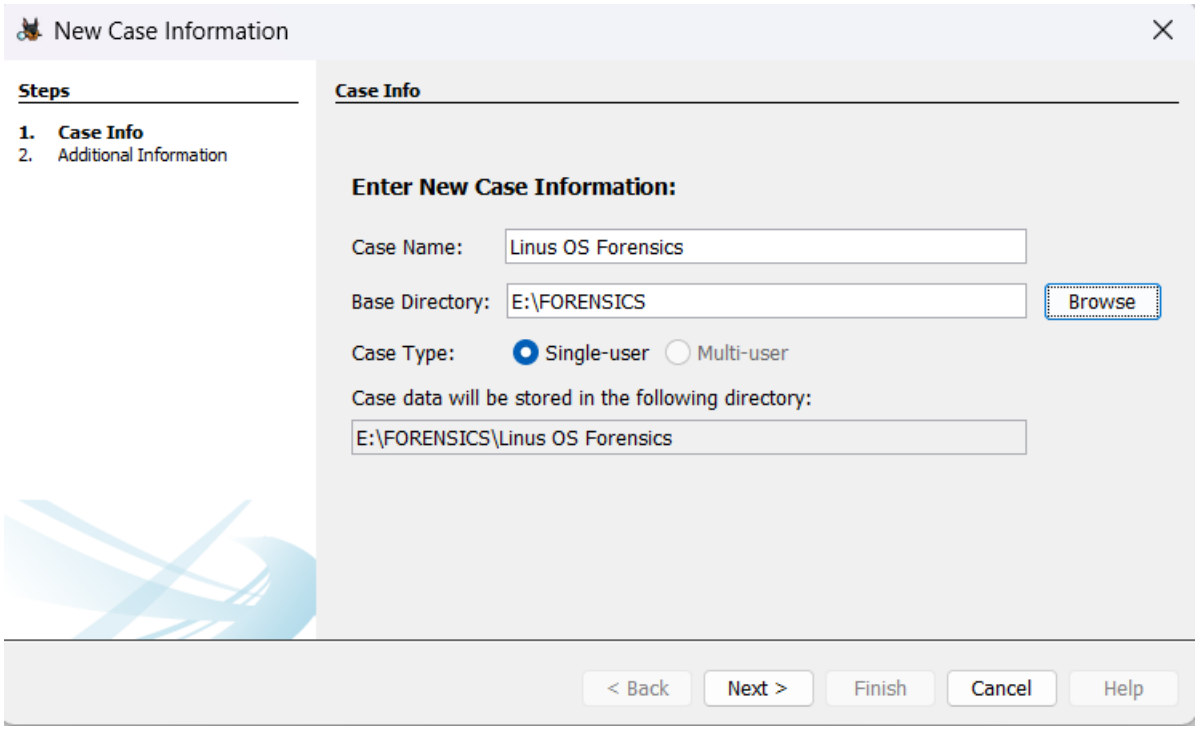
```
root@cys24020:/home/theertha# readelf -h /snap/gnome-42-2204/176/usr/lib/libglibmm_generate_extra_defs-2.4.so.1.3.0
ELF Header:
  Magic:   7f 45 4c 46 02 01 01 03 00 00 00 00 00 00 00 00
  Class:                             ELF64
  Data:                              2's complement, little endian
  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
```

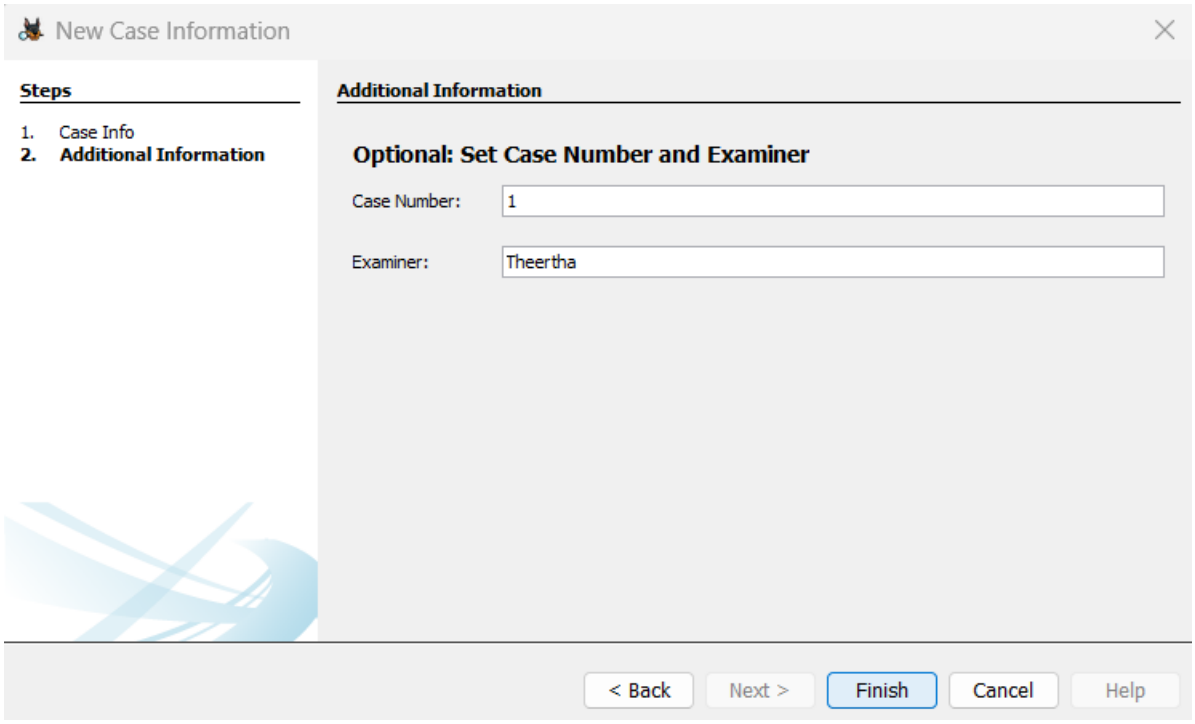
Lab6: Analyzing Non-Volatile Data in Linux System

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

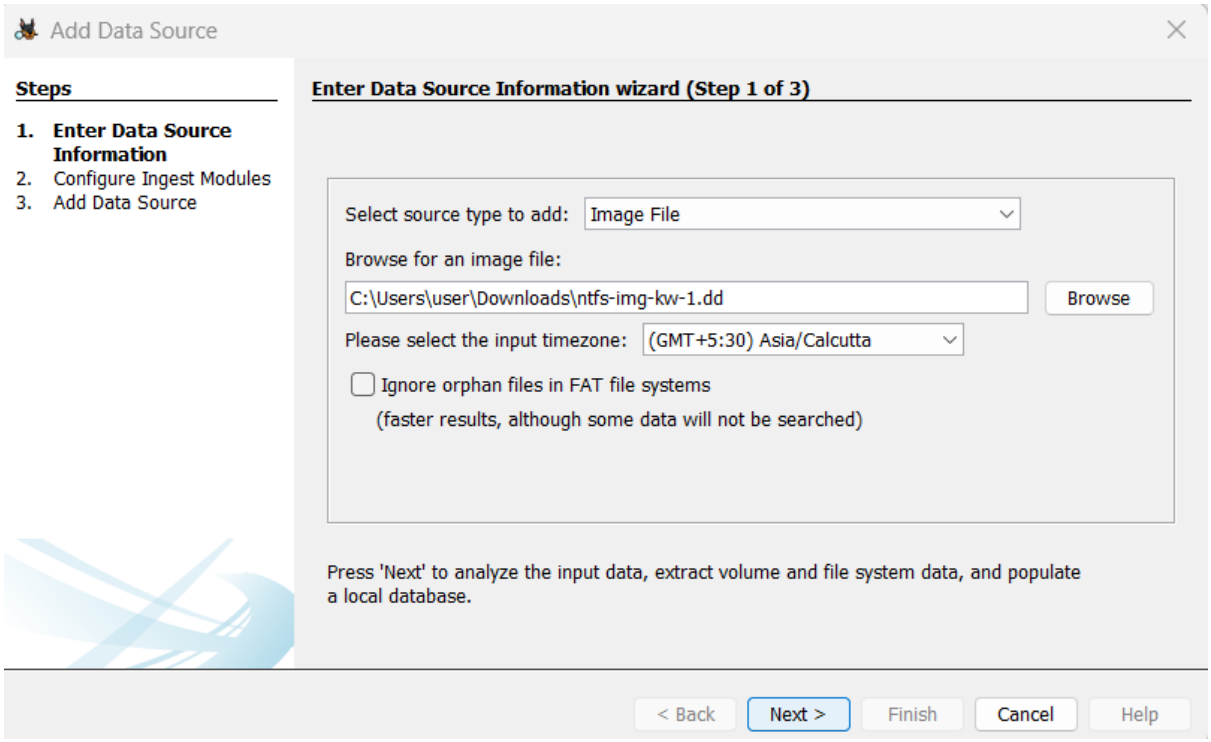
Autopsy is a widely used open-source digital forensics tool that helps investigators analyze and recover data from storage devices in criminal, civil, and cybersecurity investigations. It provides a graphical user interface (GUI) for The Sleuth Kit (TSK), making it easier to perform various forensic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

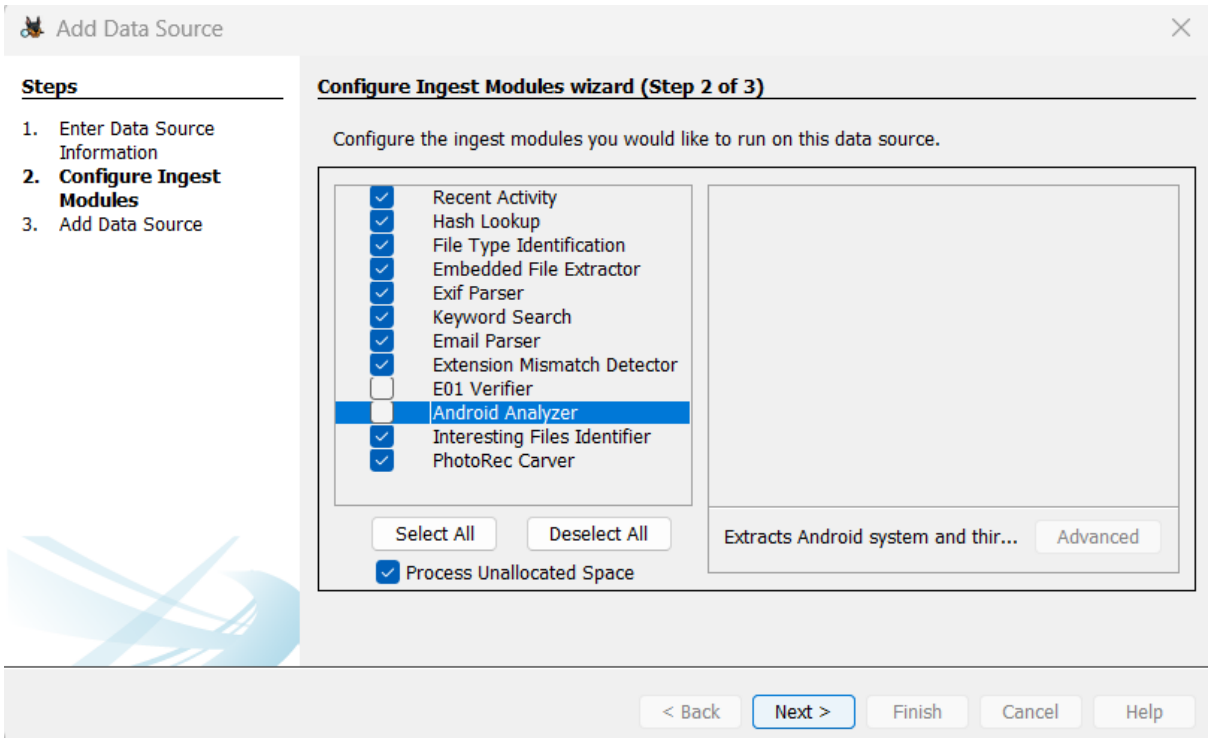
Start by creating a new case and specifying details like case name, number, and investigator.

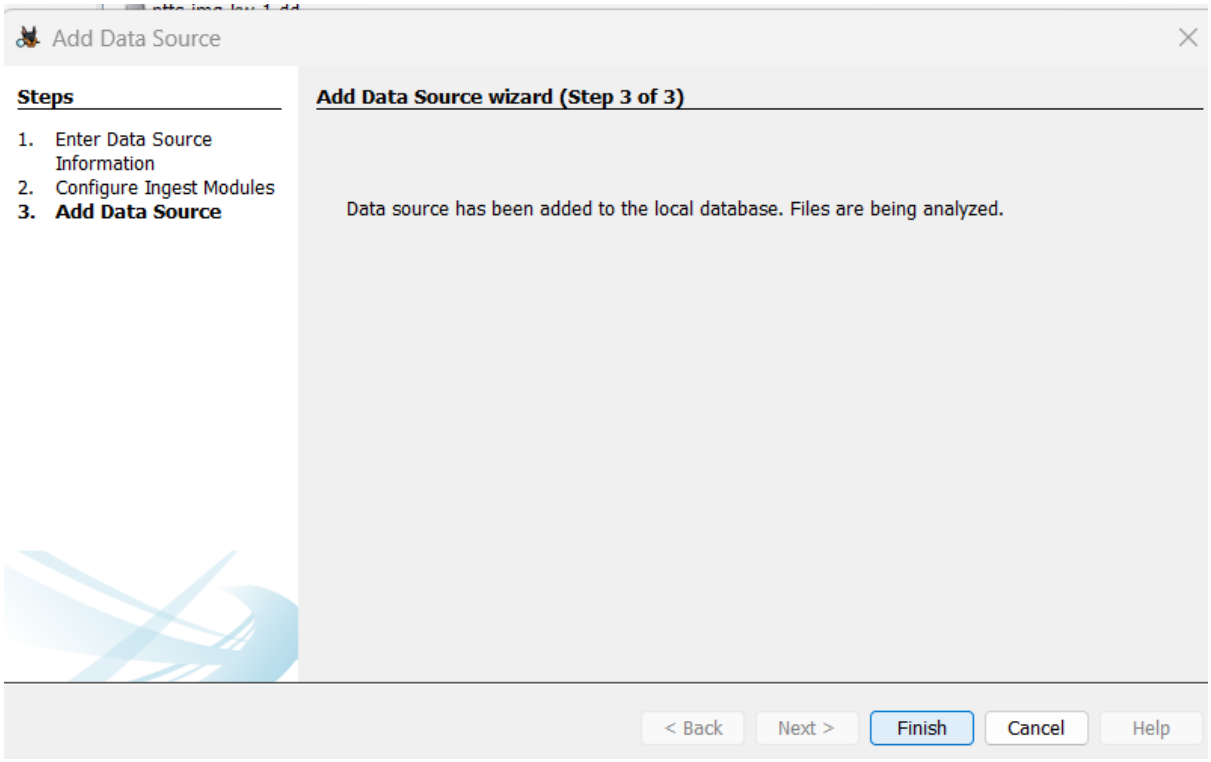


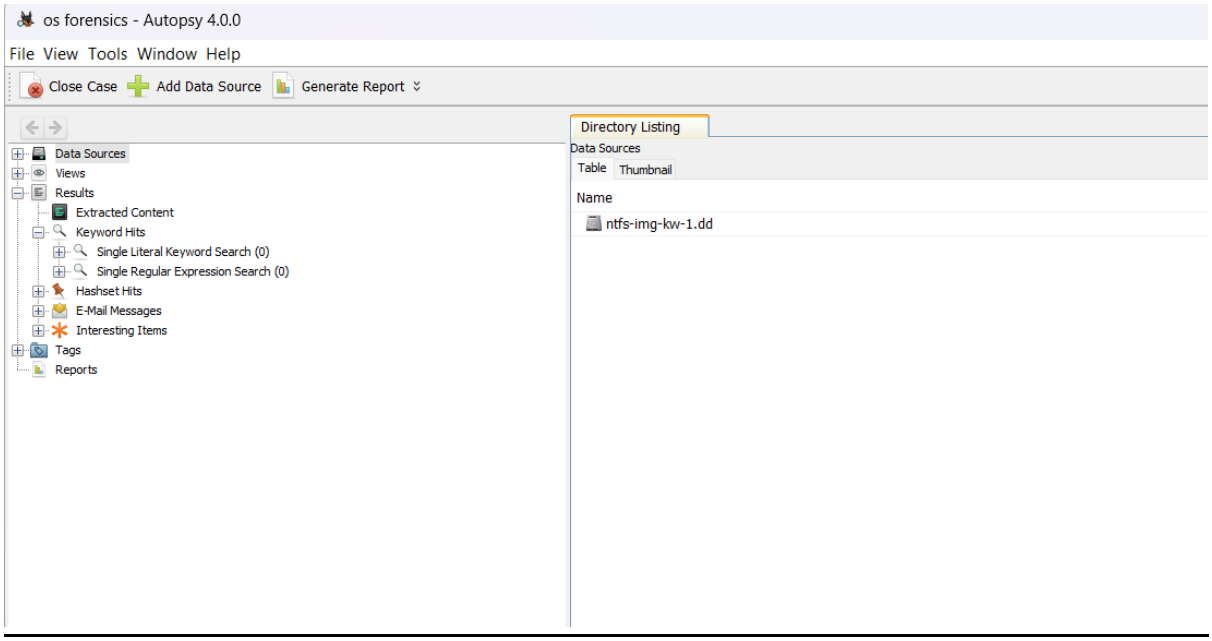


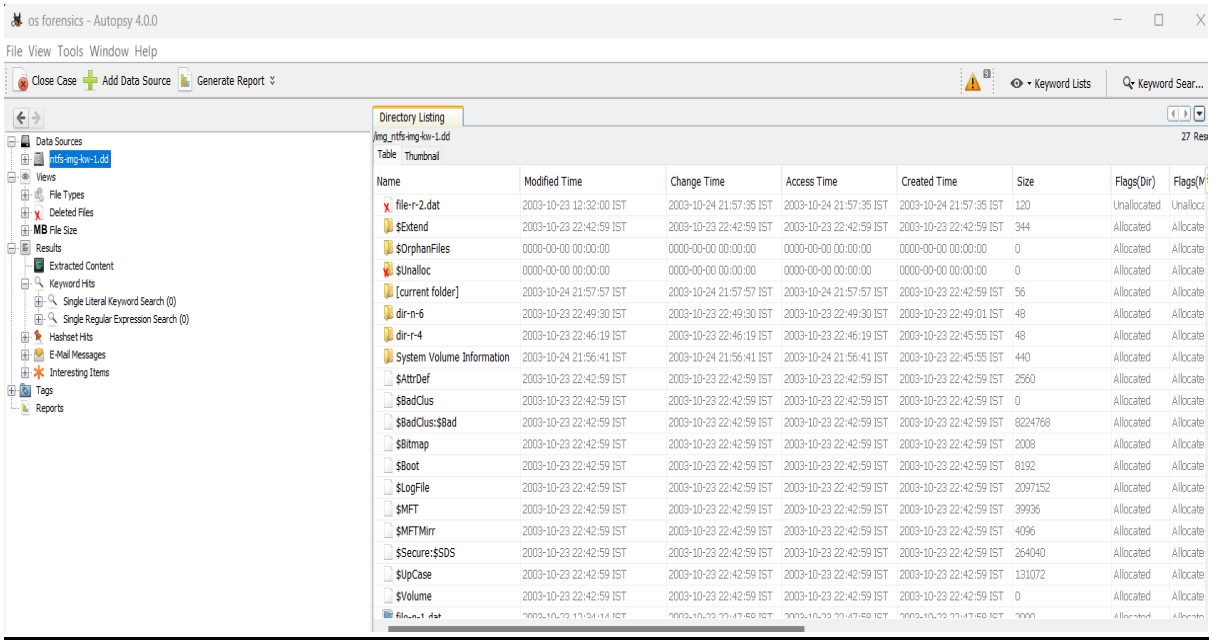
Add the evidence source, such as a disk image, physical drive, or logical files.

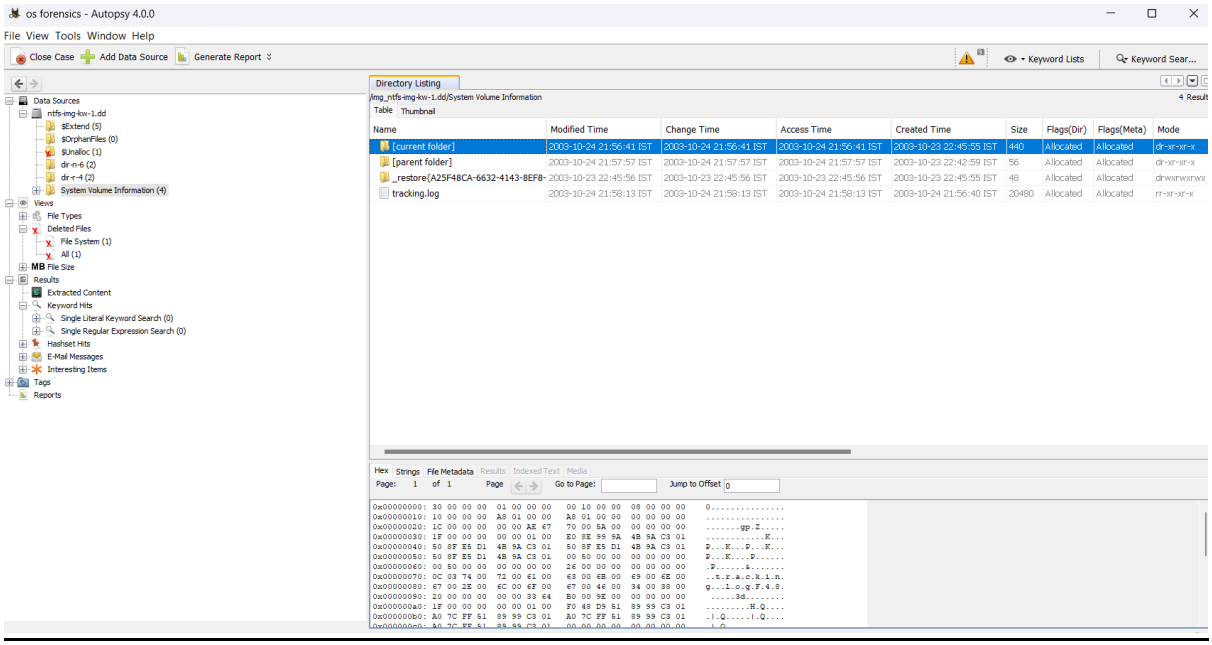

Add Data Source
Steps
1. Enter Data Source Information
2. Configure Ingest Modules
3. Add Data Source
Enter Data Source Information wizard (Step 1 of 3)
Select source type to add: Image File
Browse for an image file:
C:\Users\user\Downloads\ntfs-img-kw-1.dd
Browse
Please select the input timezone: (GMT+5:30) 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
Next >
Finish
Cancel
Help


Add Data Source
Steps
1. Enter Data Source Information
2. Configure Ingest Modules
3. 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
Extracts Android system and thir...
Advanced
Process Unallocated Space
< Back
Next >
Finish
Cancel
Help

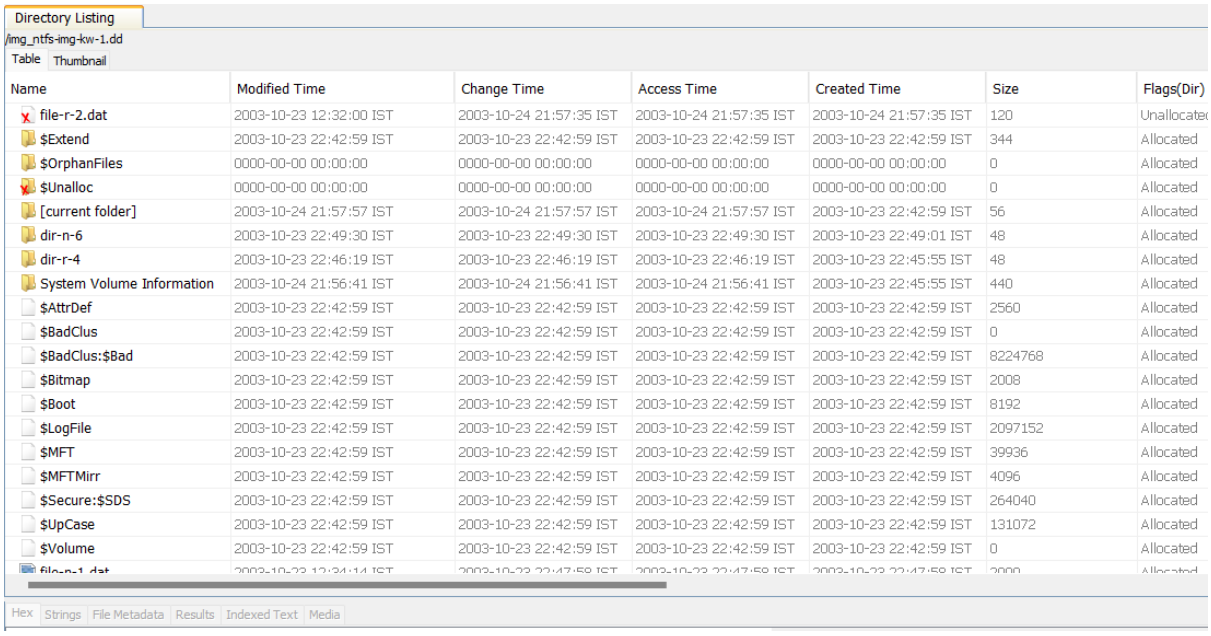

Add Data Source
Steps
1. Enter Data Source Information
2. Configure Ingest Modules
3. Add Data Source
Add Data Source wizard (Step 3 of 3)
Data source has been added to the local database. Files are being analyzed.
< Back
Next >
Finish
Cancel
Help

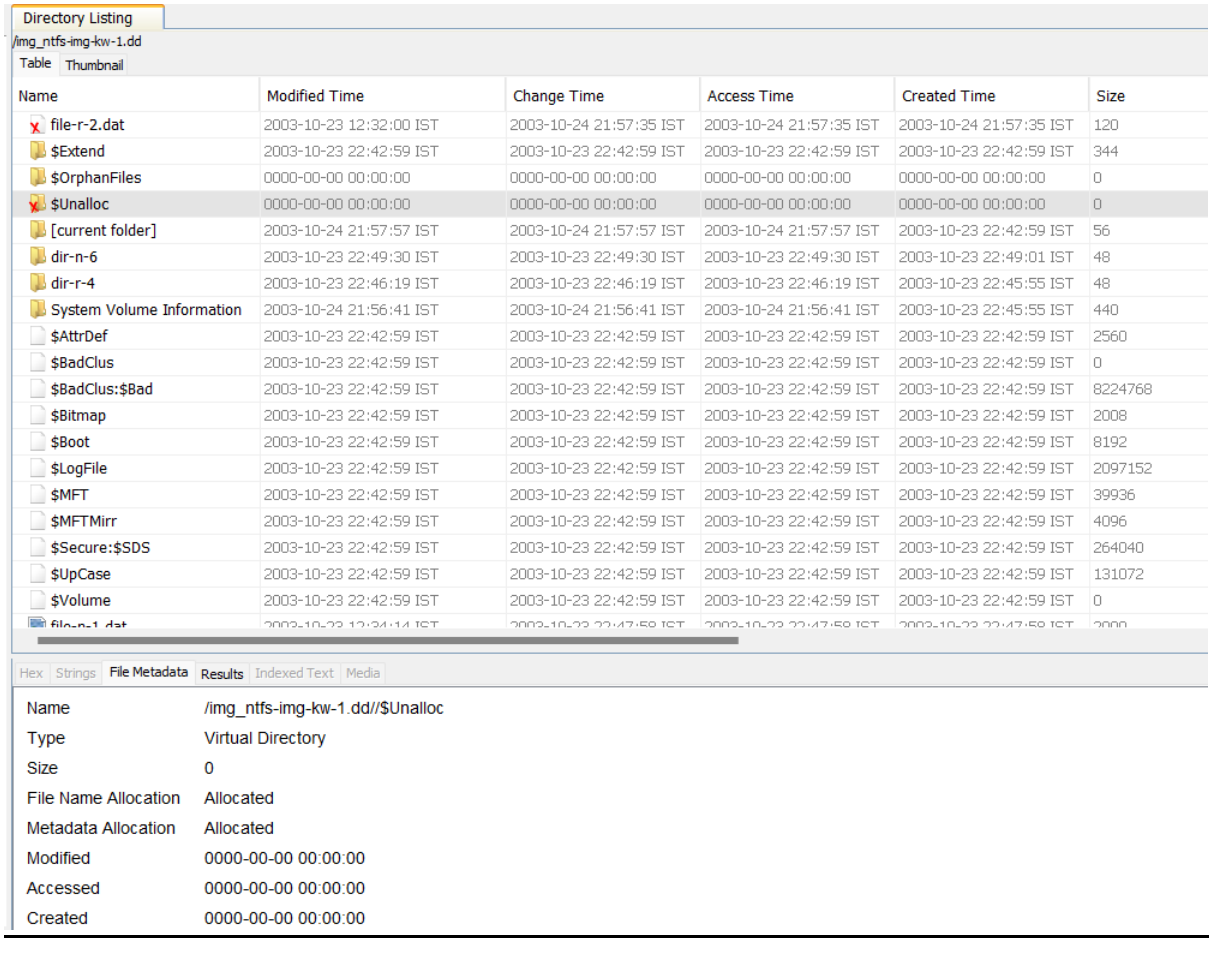

os forensics - Autopsy 4.0.0
File View Tools Window Help
Close Case
Add Data Source
Generate Report
Data Sources
Views
Results
Extracted Content
Keyword Hits
Single Literal Keyword Search (0)
Single Regular Expression Search (0)
Hashset Hits
E-Mail Messages
Interesting Items
Tags
Reports
Directory Listing
Data Sources
Table
Thumbnail
Name
ntfs-img-kw-1.dd

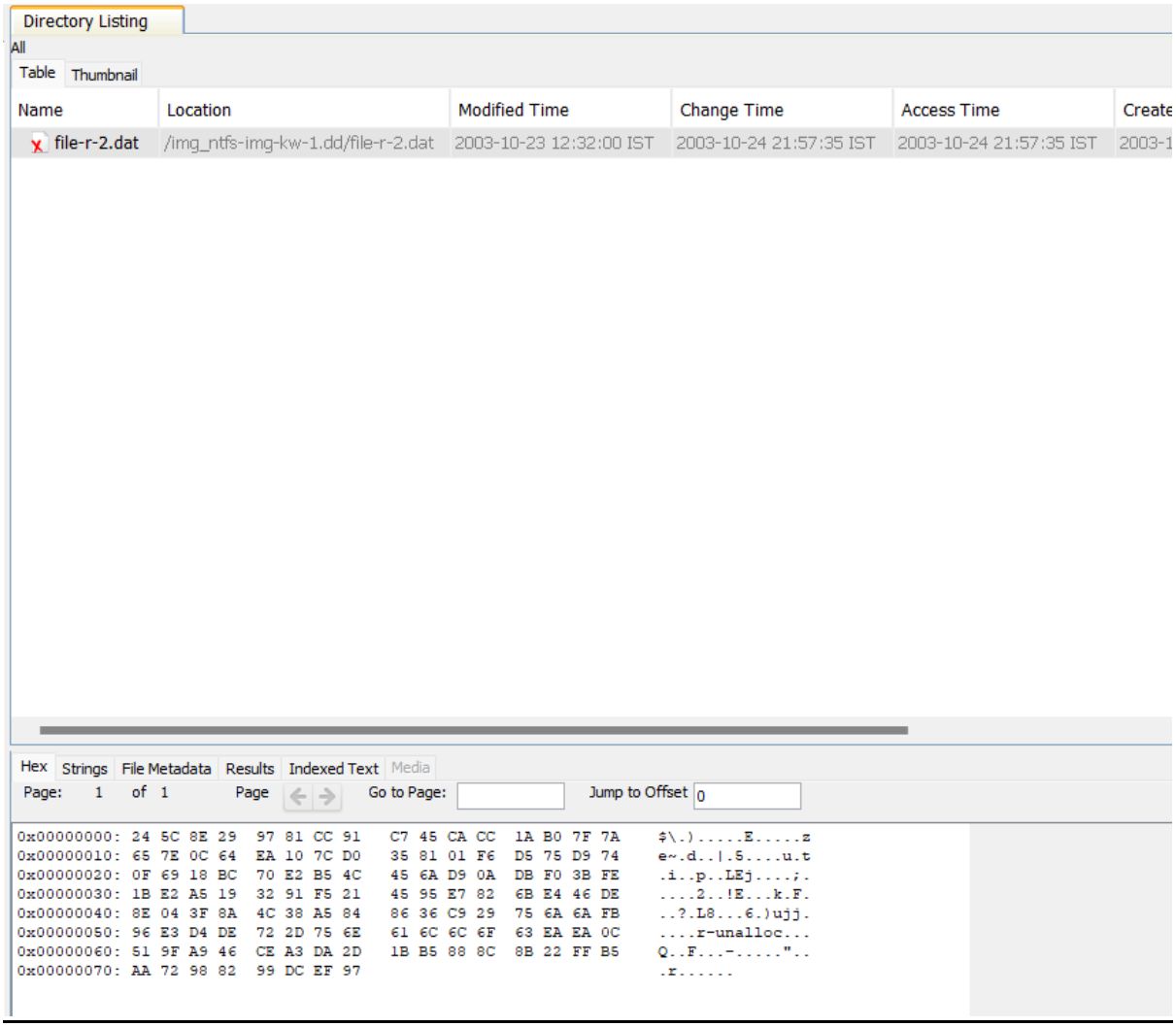




The file that are marked with a red cross are the deleted files, which have been recovered by Autopsy.


Directory Listing
/img_ntfs-img-kw-1.dd
Table
Thumbnail
Name
Modified Time
Change Time
Access Time
Created Time
Size
Flags(Dir)
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 Unallocate
$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
Hex
Strings
File Metadata
Results
Indexed Text
Media


Directory Listing
/img_ntfs-img-kw-1.dd
Table
Thumbnail
Name
Modified Time
Change Time
Access Time
Created Time
Size
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
$Volume 2003-10-23 22:42:59 IST 2003-10-23 22:42:59 IST 2003-10-23 22:42:59 IST 2003-10-23 22:42:59 IST 0
Hex
Strings
File Metadata
Results
Indexed Text
Media
Name /img_ntfs-img-kw-1.dd//$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



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.