

Cyber Forensics - 24CY611

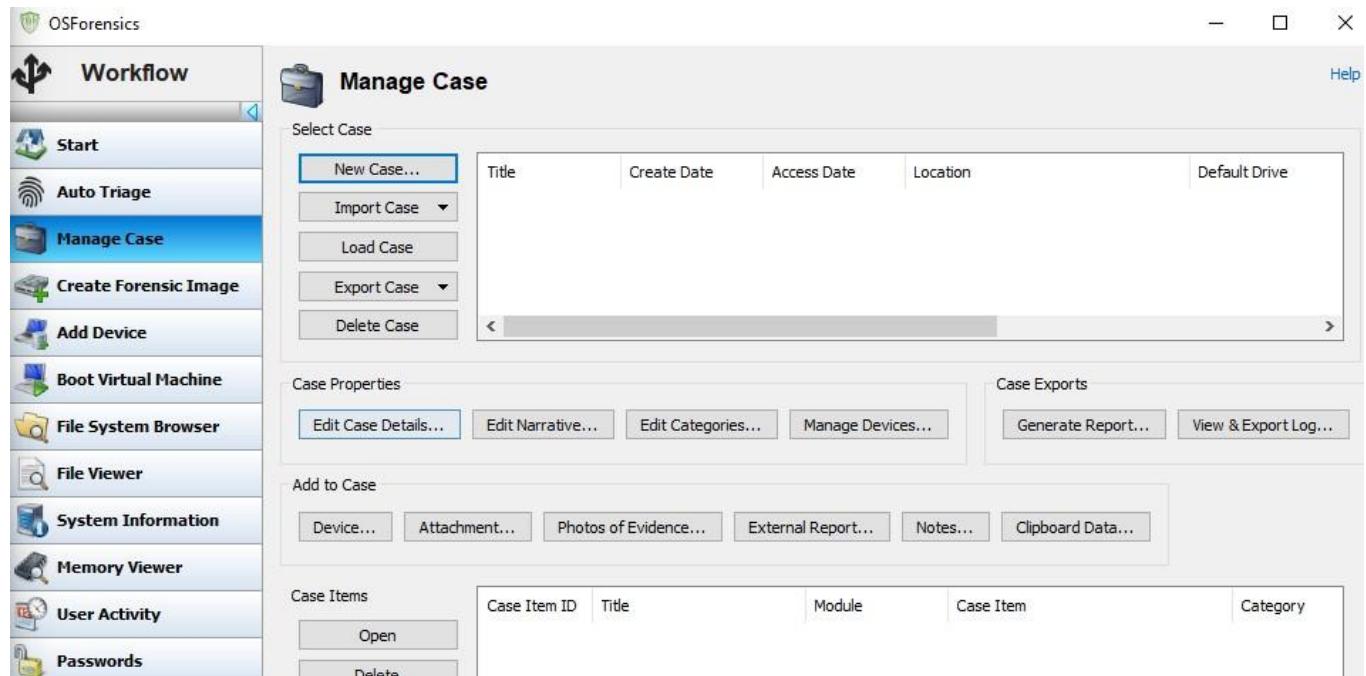
Lab 5 - Operating System Forensics

1. Discovering and Extracting Hidden forensic material on computer using OS forensics

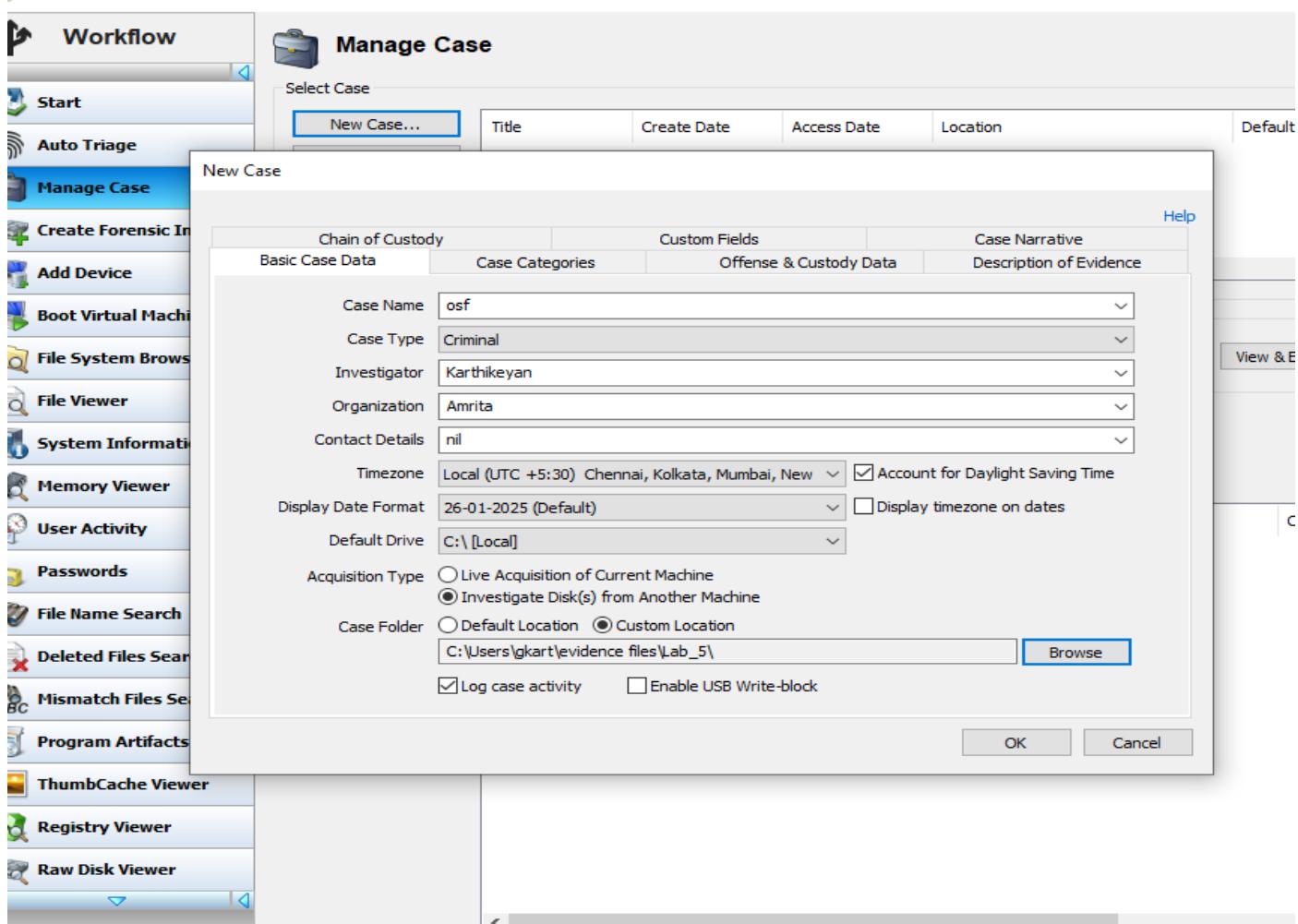
Forensics is a forensic investigation tool used to extract, analyze, and manage digital evidence from computers, including file recovery, email analysis, and disk imaging. It provides advanced search capabilities and tools for verifying data integrity, aiding in cybercrime investigations.

Steps:

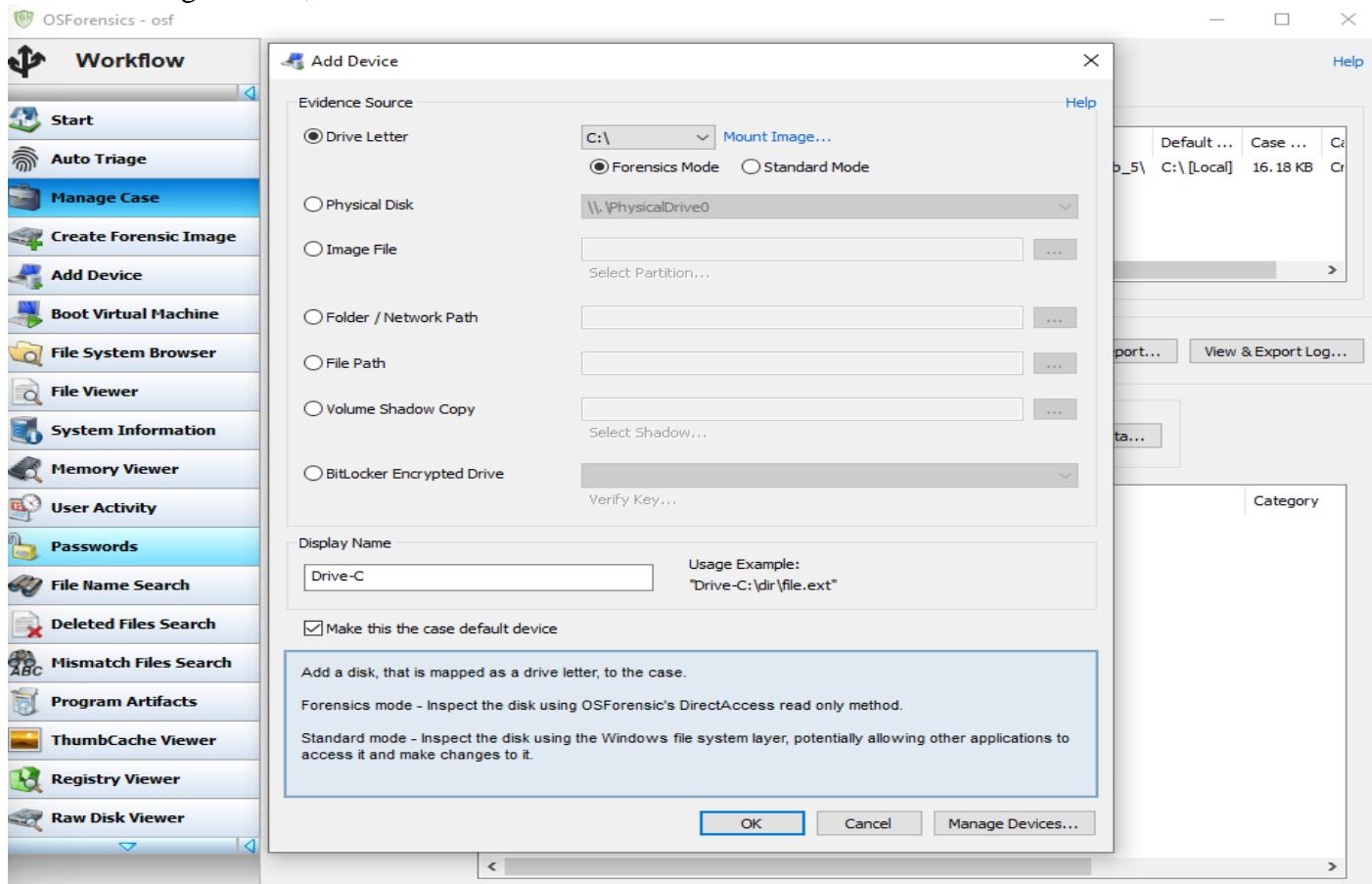
Open Forensics osftool and create a new case.



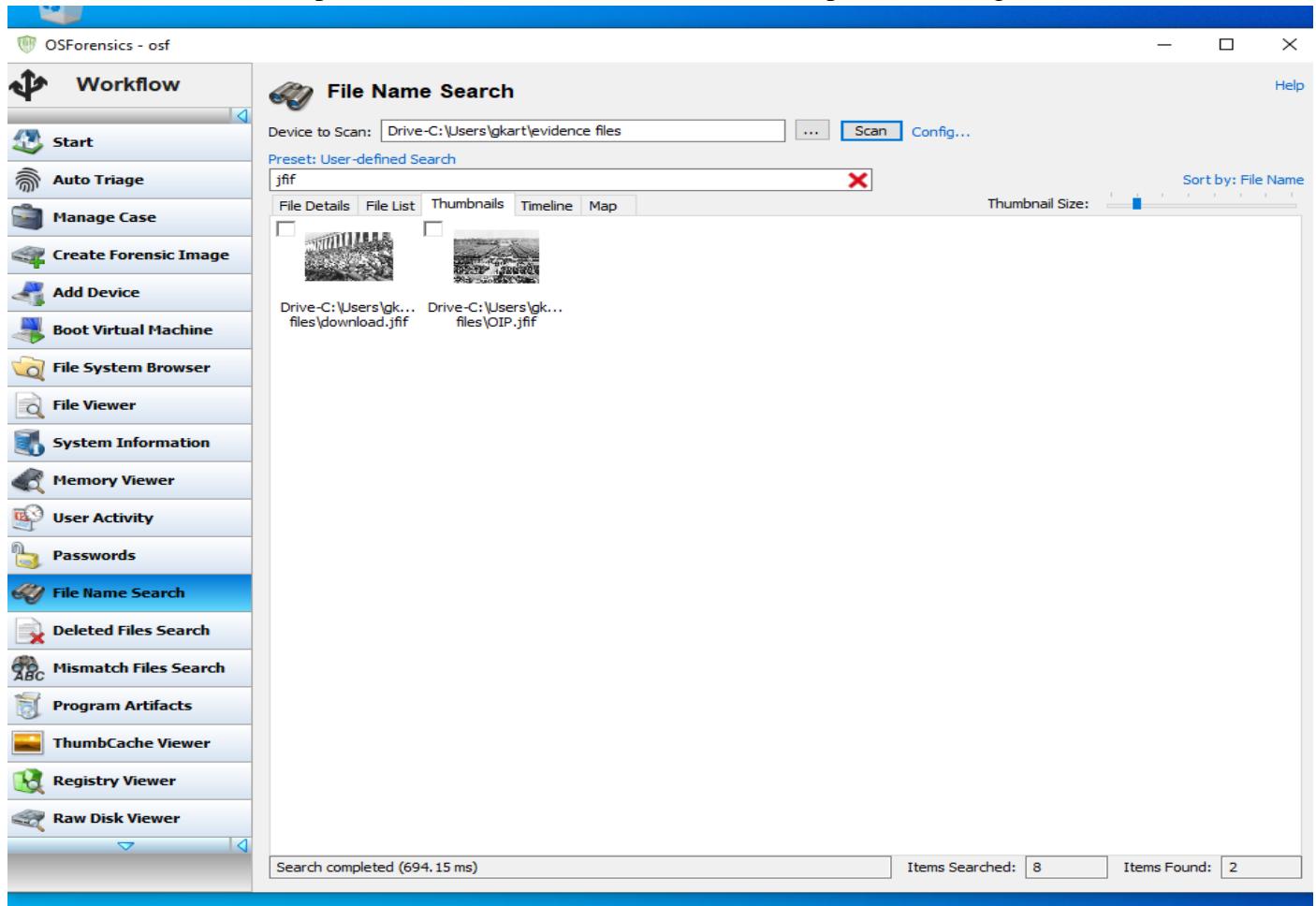
Then fill the required fields for the new case and click ok



After creating the case, add the device for evidence source



In the file name search option, select the device to scan and set the presets to images and start the scan.



The tool now displays a thumbnail of the screenshot saved in the Pictures directory, which I used as evidence, and generates an index. Creating an index involves five steps:

1. Select the desired file types for indexing using predefined options.
2. Add the specific drive or directory to be included in the index.
3. Assign an index title, include notes, and make use of memory optimization features provided in the latest version.
4. Allow the application to scan the selected path.
5. Monitor the progress and status of the indexing process as displayed by the tool.

OSForensics - osforensicslab

Workflow

- 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

Create Index | Search Index

Step 1 of 5

What types of files would you like to index?

(Use Pre-defined File Types) E-mails Attachments Executables and binary files
 Office + PDF documents Memory dump files All other supported file types
 ZIP and compressed archives Unknown files System hibernation and paging files
 Images Plain text files Use OCR for images and PDF documents Video, audio and other media Windows Event Log files

(Use previously saved configuration:)

Configuration	File Types

Next

OSForensics - osforensicslab

Workflow

- 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

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**

The screenshot shows the OSForensics - osf software interface. On the left is a vertical toolbar with various forensic tools: 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 (which is selected and highlighted in blue), Signatures, and Analyze Shadow Copies.

The main window title is "Indexing". It displays "Step 2 of 5" and asks "Which drive(s) or folder(s) would you like to index?". A table shows one entry: "File Details" (Drive-C:\Users\gkart\ evidence files) and "Type" (Folder). There are "Add..." and "Remove" buttons next to the table.

Below this, under "Advanced settings (optional)", there are six edit buttons arranged in a grid:

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

At the bottom right of the main window are "Back" and "Next" buttons.

 **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 = 10,000
 Max file size* = 4 MB

Estimated RAM required: 1,320 MB (1.3 GB)
 Available RAM: 2,202 MB (2.2 GB)

*Max file size does not apply to some file formats

Select number of threads: [Edit](#)

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

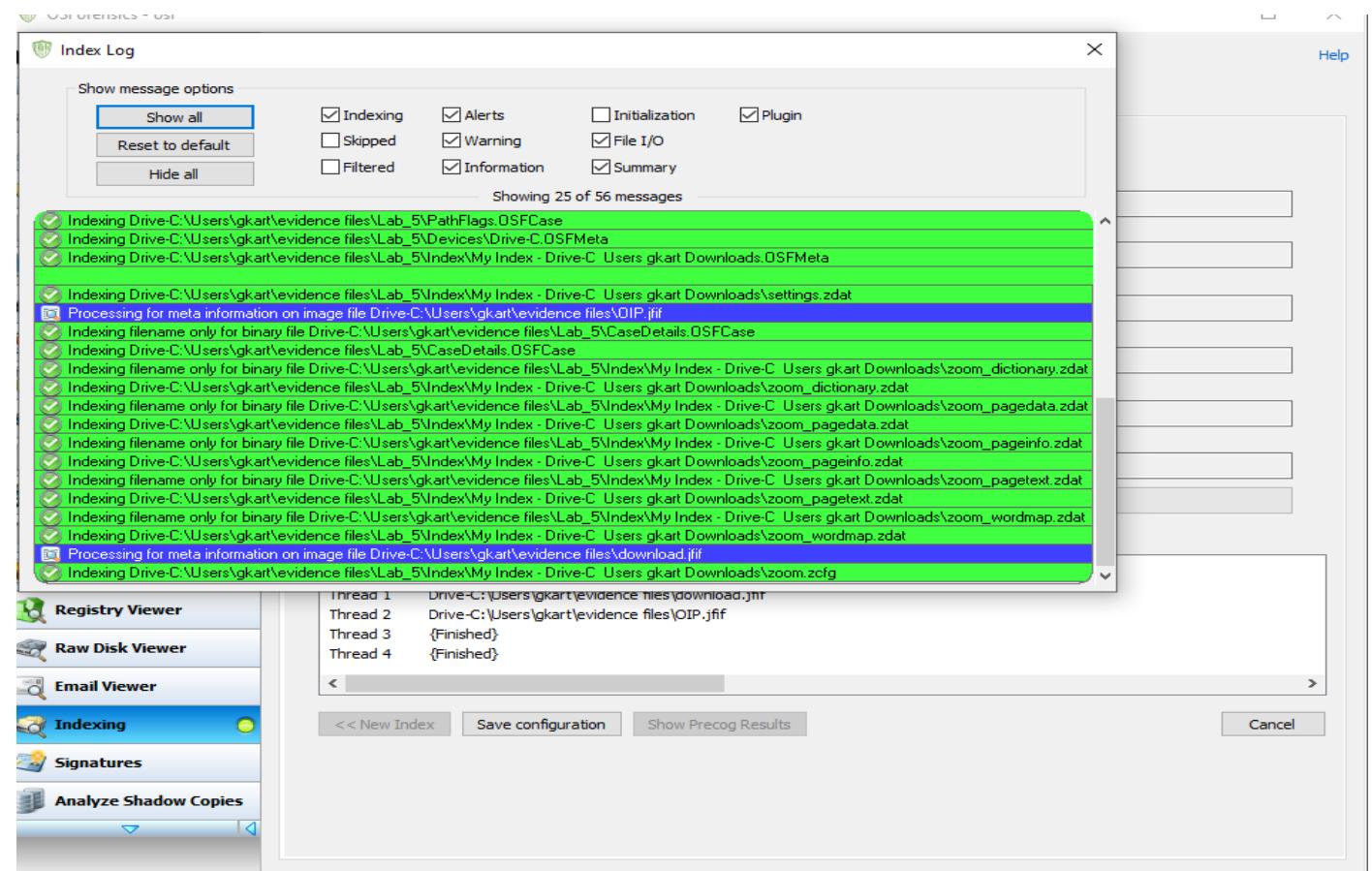
Index Title

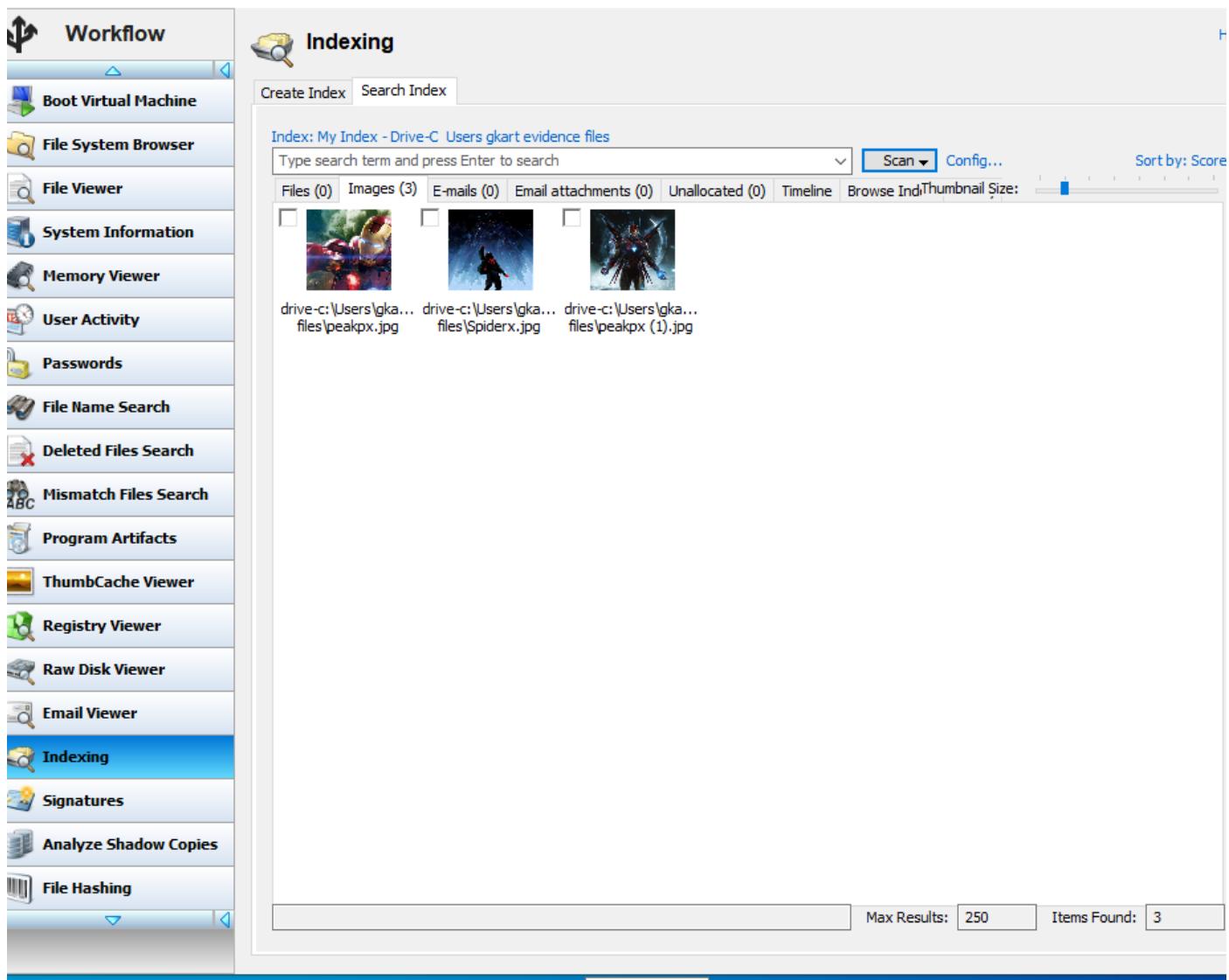
Index Notes

Index of files in:
 C:\Users\Admin\Desktop

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

[Back](#) [Start Indexing](#)

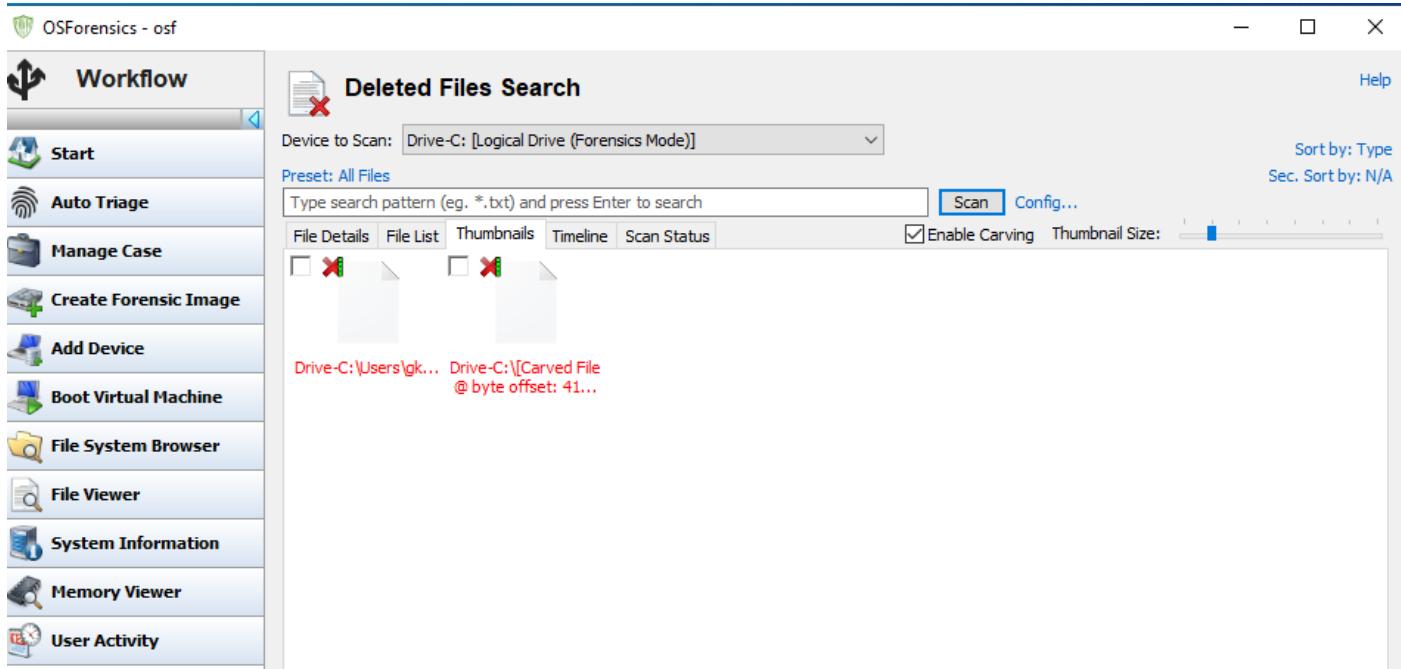




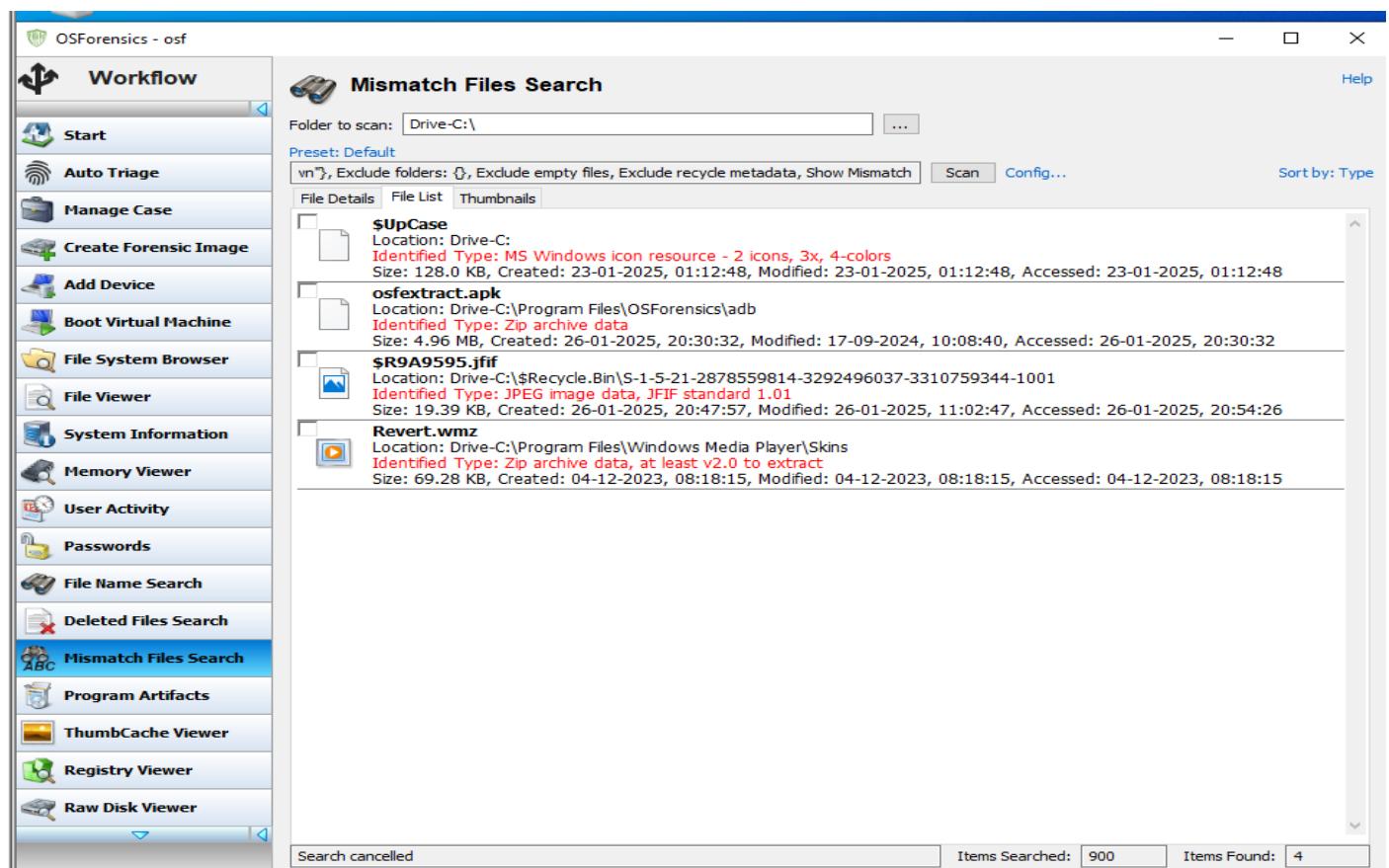
Next, select the **Recent Activity** option to scan the drive and display recent actions related to the evidence. In the latest version, this option has been renamed **User Activity**. Choose the preferred scan type to perform a detailed analysis.

Choose the device to scan, select the **C:** drive, and click **Scan** to search for evidence such as visited websites, connected USB drives, recent downloads, and wireless networks stored on the drive.

To recover deleted files, navigate to the **Deleted Files Search** option and select the desired partition.



Use the **Mismatch File Search** feature to identify files whose extensions do not match their actual content. This helps in detecting potential tampering or mislabelling of files.

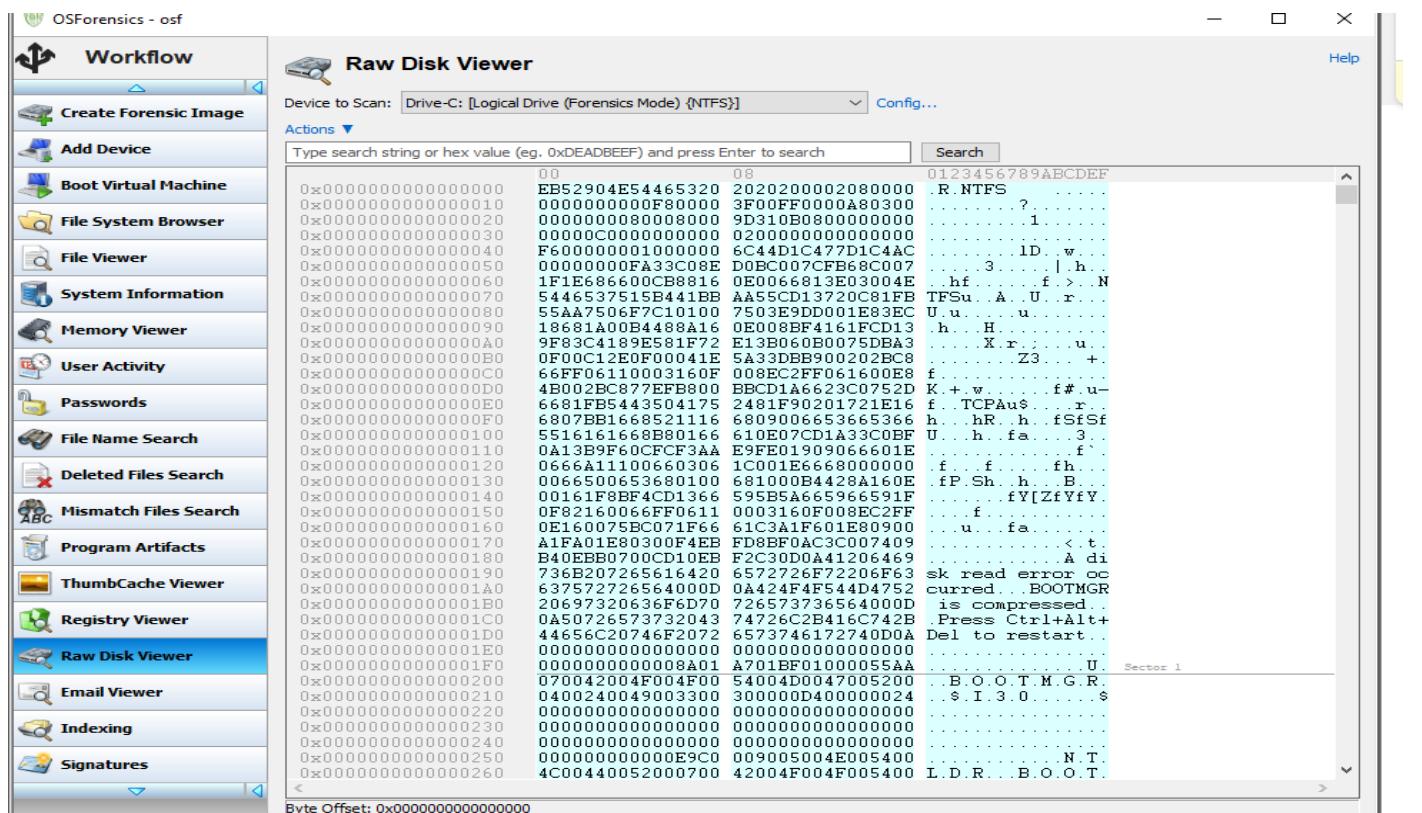


The **Memory Viewer** shows the system's memory usage and provides a detailed list of active processes, allowing for in-depth analysis.

The screenshot shows the OSForensics - osf software interface. On the left is a vertical toolbar with various forensic analysis tools: Workflow, Start, Auto Triage, Manage Case, Create Forensic Image, Add Device, Boot Virtual Machine, File System Browser, File Viewer, System Information, **Memory Viewer** (which is currently selected), User Activity, Passwords, File Name Search, Deleted Files Search, Mismatch Files Search, Program Artifacts, ThumbCache Viewer, Registry Viewer, and Raw Disk Viewer. The main window title is "Memory Viewer". It has tabs for "Live Analysis" and "Static Analysis", with "Live Analysis" selected. Below the tabs are buttons for "Refresh", "Select Window", and "Dump Physical Memory". A status bar at the top right indicates "Total Memory: 4.00 GB". The main content area is a table showing active processes. The table columns are: Process, PID, CPU %, Total CPU Time, User Time, Kernel Time, and Process Cre. The table lists several processes, with "System" highlighted. At the bottom of the main window, there is a "Process Info" section displaying details about the selected process (ntoskrnl.exe) such as Image Path, Product Name, Description, Version, User Name, Integrity Level, Digitally Signed status, and Digital Signer.

Process	PID	CPU %	Total CPU Time	User Time	Kernel Time	Process Cre
Idle	0		00:35:04.906	00:00:00.000	00:35:04.906	26-01-2025
System	4	3.08%	00:01:33.843	00:00:00.000	00:01:33.843	26-01-2025
Registry	72		00:00:00.859	00:00:00.000	00:00:00.859	26-01-2025
smss.exe	528		00:00:00.125	00:00:00.000	00:00:00.125	26-01-2025
svchost.exe	552		00:00:00.125	00:00:00.078	00:00:00.046	26-01-2025
svchost.exe	564		00:00:06.859	00:00:03.765	00:00:03.093	26-01-2025
SkypeApp.exe	572		00:00:25.156	00:00:10.421	00:00:14.734	26-01-2025
dwm.exe	596		00:00:21.593	00:00:12.796	00:00:08.796	26-01-2025
csrss.exe	632		00:00:00.546	00:00:00.093	00:00:00.453	26-01-2025
svchost.exe	696		00:00:00.609	00:00:00.296	00:00:00.312	26-01-2025
wininit.exe	700		00:00:00.093	00:00:00.015	00:00:00.078	26-01-2025
cssrs.exe	708		00:00:07.937	00:00:00.078	00:00:07.859	26-01-2025
ctfmon.exe	728		00:00:05.093	00:00:01.671	00:00:03.421	26-01-2025
winlogon.exe	760		00:00:00.265	00:00:00.062	00:00:00.203	26-01-2025

The **Raw Disk Viewer** provides direct access to view raw data on a disk at the sector level, enabling thorough analysis of disk structures and uncovering hidden information.



The **System Information** feature collects and presents comprehensive details about the system's hardware and software. It includes information such as the operating system version, installed applications, hardware specifications (e.g., CPU, memory, storage), and device configurations, providing an in-depth overview of the system's performance and setup.

OSForensics - osf

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
- ThumbCache Viewer
- Registry Viewer
- Raw Disk Viewer

System Information

Device to Scan: C:\ Scan

Command List: System Information From Registry

Type search text and press Enter

Commands Result 1 - System Information From Registry (C:\) X

Created: 26 January 2025, 21:17:24

Commands Executed

Computer Name (Registry) Timezone Info (Registry) Network Info (Registry) User Info (Registry) Printers (Registry) Shutdown Time (Registry) Windows Info (Registry)

Computer Name (Registry)

Registry File: C:\Windows\System32\Config\SYSTEM
Key Location: ControlSet001\Control\ComputerName\ComputerName

Computer Name	DESKTOP-F2LF5C3
---------------	-----------------

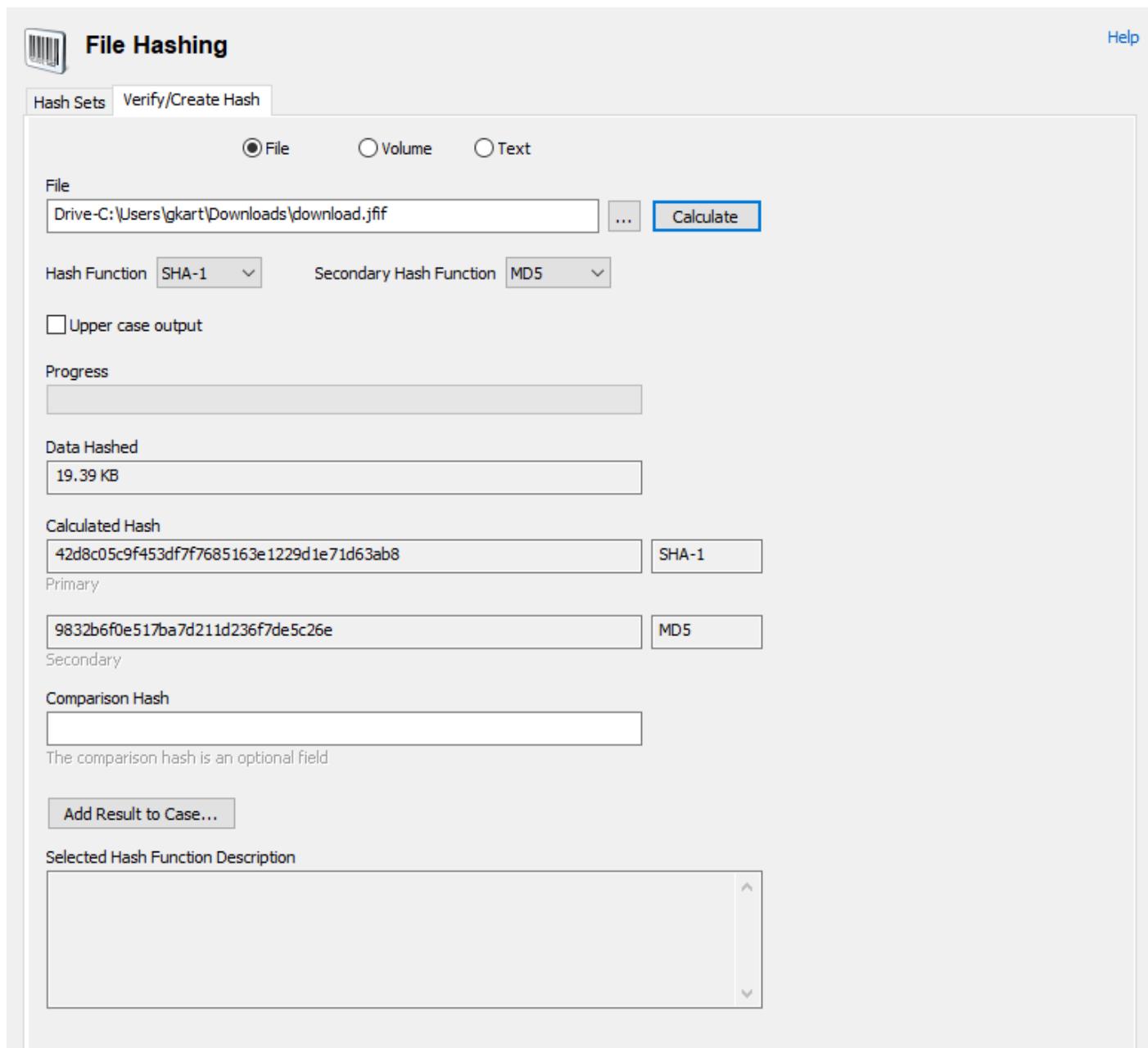
[Back to Top](#)

Timezone Info (Registry)

Registry File: C:\Windows\System32\Config\SYSTEM
Key Location: ControlSet001\Control\TimeZoneInformation

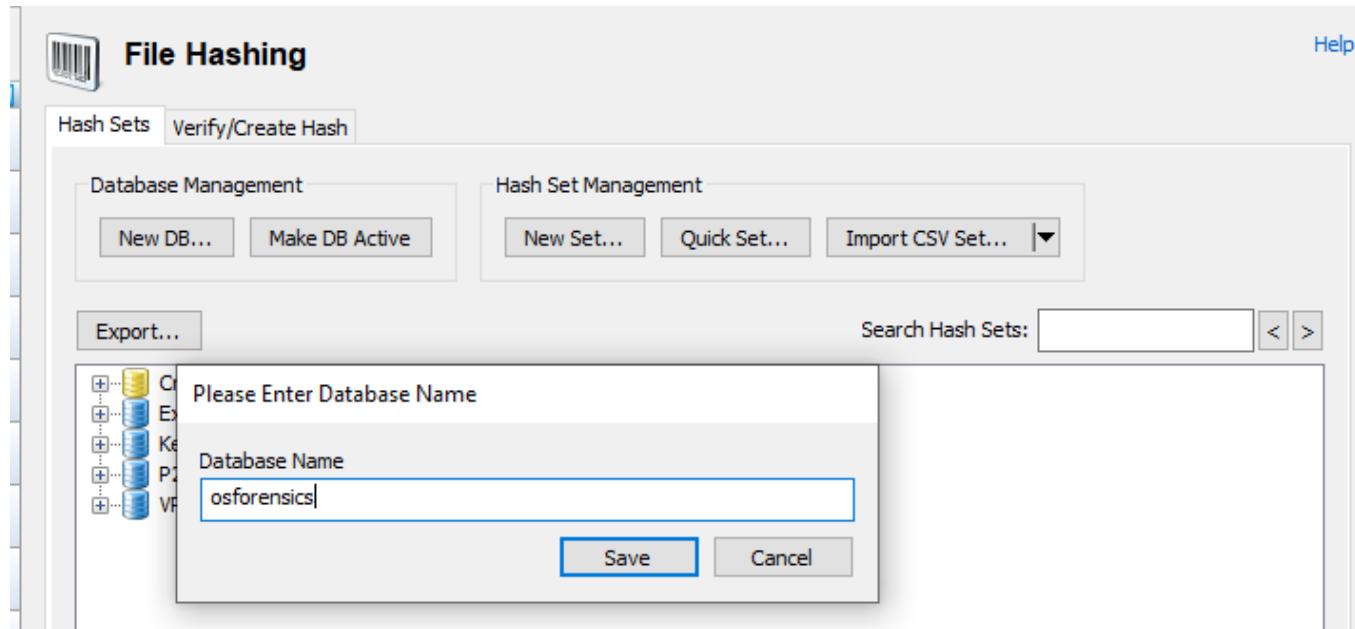
Timezone Name	India Standard Time
Bias	182
Daylight Savings Bias	196

The **File Hash** tool is used to verify the integrity of files, disks, or entire partitions. To use it, select the file you want to hash, choose the **MD5** algorithm, and the tool will calculate and display the corresponding hash value to ensure the file's authenticity and integrity.



Select the **Hash Sets** feature to identify known suspicious files, helping streamline the investigation process by minimizing the need for time-consuming manual analysis. This allows for quicker detection of potentially harmful or unauthorized files based on predefined hash values.

Create a database and set it as active. Then, create a new hash set by providing the necessary details, including the folder path. The tool will generate a new hash set based on the specified files, which can then be used for further analysis.



New Hash Set

New Hash Set

Help 

Current DB: osforensics

Origin:

Product Type:

Manufacturer:

File Set Type:

OS:

Hash Set Name:

Version:

Language:

Folder:

Skip files smaller than... bytes

Current File:

Files Hashed: Files Skipped: Time Elapsed:

Progress:

More Info:
The origin of the files. Depending on the scope of the database this could be as specific as "Bob's PC" or as broad as an entire organization.

The screenshot shows the 'File Hashing' tool interface. On the left, a sidebar lists various forensic analysis tools: Workflow, 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 (which is selected), Remote Acquisition, Customize Workflow, and Register.

The main window title is 'File Hashing'. It has tabs for 'Hash Sets' and 'Verify/Create Hash'. Below the tabs are buttons for 'Database Management' and 'Hash Set Management'. A sub-dialog titled 'osf1 1 | NA | English' is open, showing details about a hash set: Hash Set ID: 6, Hash Set Name: osf1 1 | NA | English, Hash Set Type: image, and Operating Systems: windows 10. The 'Hash Set Viewer' section displays a table of file hashes:

File Name	MD5	SHA1	SHA256	PhotoDNA	Last Updated
CASEDETAILS.O...	010D22DB2D...	D24255E3F9...	EC2776CDB7...		2025-01-26
CASELOG.OSFLOG	814627563E8...	6A795172D3...	93F2298DE8...		2025-01-26
DRIVE-C.OSFMETA	601C37FF60...	ABCFF237C9...	4D351672AA...		2025-01-26
1338237960314...	295E5F4D8B...	21C47D0FAF...	53BBBF26492...		2025-01-26
INDEXLOG.TXT	AB6864425F...	A69466190C...	CA83281656...		2025-01-26
SETTINGS.ZDAT	F643364E92...	FD43CE9AAE...	7BF647B4794...		2025-01-26
ZOOM.ZCFG	DB0CE8DC36...	6150E83070B...	7C06309968...		2025-01-26
ZOOM_DICTION...	01ED4F7FF0...	159B53107C...	B57B57E9D3...		2025-01-26
ZOOM_PAGEDA...	DE5664E955...	DB3DD4B06B...	BCE76B3C5D...		2025-01-26
ZOOM_PAGEINFO...	8B3713F0A0...	369B6642E9...	C5906E0ED9...		2025-01-26
ZOOM_PAGETEX...	B1B00DBC16...	D3982E50A9...	FAB44654E1...		2025-01-26
ZOOM_WORDM...	7C71F86F5E...	0F8BC6A96F...	1E161EDF3A...		2025-01-26
MY INDEX - DRI...	F349387D85...	771C28C567...	BDB59B2908...		2025-01-26
PATHFLAGS.OS...	0144570BE16...	3708834FA6...	708B94A6D1...		2025-01-26

Below the table, it says 'Number of files in set: 18, Total Size: 2.70 MB' and there is a 'Close' button.

The **Drive Imaging** tool creates exact copies of partitions for forensic analysis. Select the image file and specify the necessary paths to generate the partition image.

The screenshot shows two windows of the PassMark OSFMount application. The main window on the left displays a table of mounted virtual disks, with one entry highlighted:

Device	Drive	Emulation	Disk Image Path	Type	Size	Properties
\Device\OSFMDisk1	F:	Logical	C:\Users\Admin\Desktop\evidence files\image.dd	Disk	7.461 MB	Read-only

The 'Disk Image Path' column shows the path C:\Users\Admin\Desktop\image.dd. Below the table are buttons: 'Mount new...', 'Dismount', 'Dismount all & Exit', and 'Exit'. A checkbox 'Make this the case default device' is also present.

The second window, titled 'OSFMount - Mount drive', is a 'Mount Virtual Disk' dialog. It asks 'What type of virtual disk do you want to mount?' and provides two options: 'Disk image file (.img, .dd, .vmdk, .E01, ...)' (selected) and 'Empty RAM drive'. It also includes a 'Raw Image' checkbox and a 'Mount as RAM drive' checkbox. A note says 'Mouse over an item for more information.' At the bottom right is a 'Next' button.

The **Forensic Copy** tool was used to copy content while preserving timestamps for accurate data analysis. Specify the necessary paths to store the copied content. However, in the latest version of the tool, the **Forensic Copy** feature is no longer available.

Extracting Information About Loaded Processes Using Process Explorer

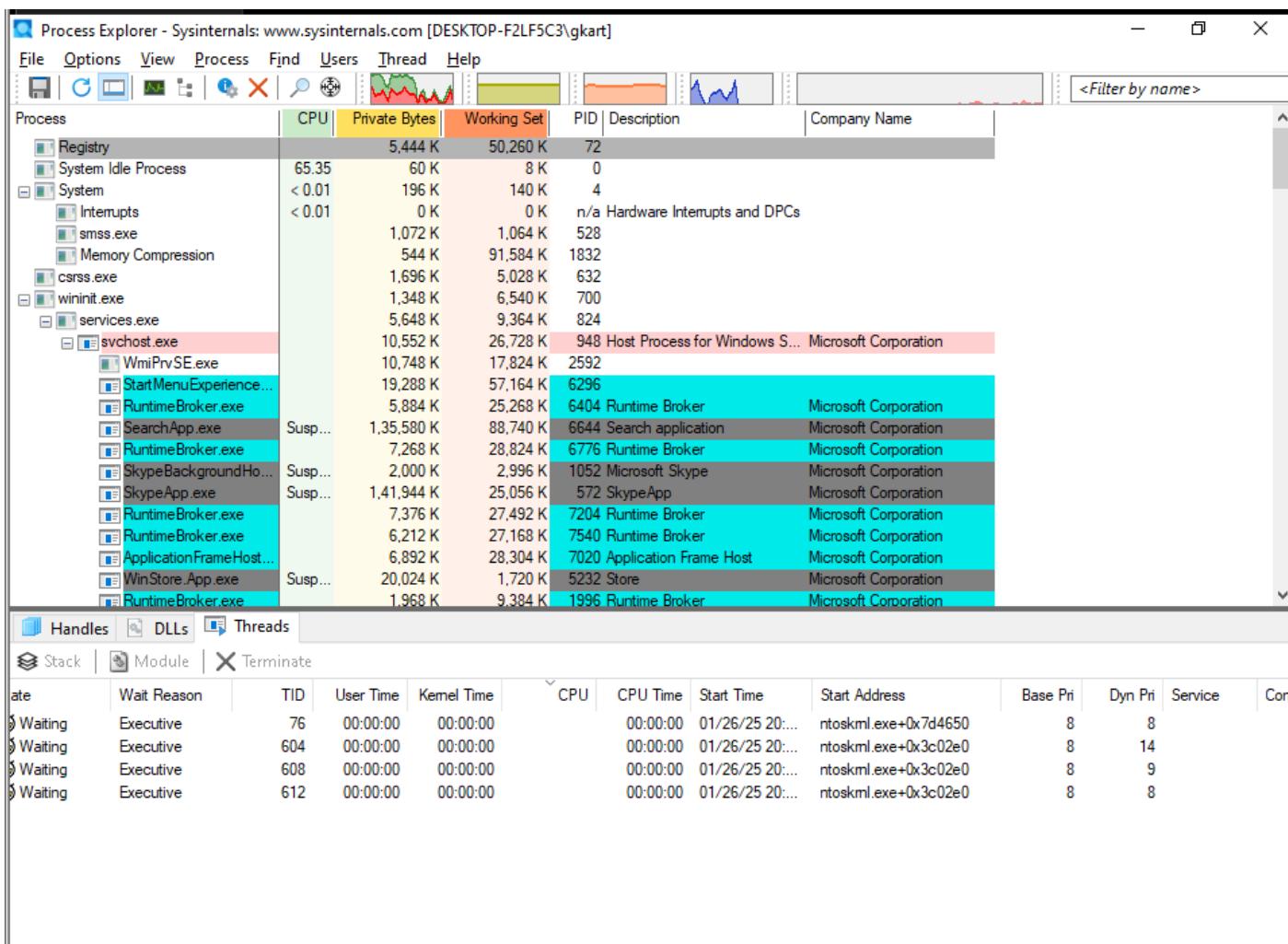
Process Explorer, developed by Microsoft, is a powerful tool used to extract detailed information about loaded processes. It provides insights such as:

- **PID (Process ID), CPU usage**, and other performance metrics for each process.
- A comprehensive list of **DLLs** (Dynamic Link Libraries) used by each process, along with their associated **strings**.
- The **Strings tab** displays **Unicode** data within the process, which is crucial for identifying potential

malware or suspicious activity.

If necessary, DLLs can be saved in a **text format** for further review. To analyze these DLL files in more depth, the **Cabinet.dll** tool can be used.

In addition to process and DLL analysis, **Process Explorer** enables management of **process handles** and **threads**, providing detailed information about the individual threads running within each process. This functionality is useful for in-depth analysis of system behavior and identifying issues or threats.



For any process, including the **Explorer process**, **Process Explorer** allows you to view and manage the following:

- DLLs (Dynamic Link Libraries):** You can see which DLLs are being used by the process. This helps in identifying any unusual or suspicious libraries that might indicate tampering or malware.
- Headers:** You can examine the headers associated with the process or DLLs, offering further insight into their structure and functionality.
- Threads:** You can view the individual threads running within the process, along with details such as their status and resource usage. This is useful for tracking down specific activities or issues related to the process.

Additionally, **Process Explorer** allows you to **manage** these components. For example, you can:

- Terminate or suspend threads or processes.
- Examine and interact with the process handles to manipulate or inspect file, registry, or synchronization objects related to the process.

This functionality is essential for performing a detailed analysis and managing processes efficiently.

Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-LA72I7T\Admin]

File Options View Process Find Users Help

View

- System Information... Ctrl+I
- Show Process Tree Ctrl+T
- Show Column Heatmaps
- Scroll to New Processes
- Show Unnamed Handles and Mappings
- Show Processes From All Users
- Opacity
- Show Lower Pane Ctrl+L
- Lower Pane View**
 - DLLs Ctrl+D**
 - Handles Ctrl+H
 - Threads Ctrl+Y
- Refresh Now F5
- Update Speed

Working Set	PID	Description	Company Name
1,300 K	1748	Host Process for Windows S...	Microsoft Corporation
1,492 K	1760	Host Process for Windows S...	Microsoft Corporation
1,560 K	1776	Host Process for Windows S...	Microsoft Corporation
1,916 K	1792	Host Process for Windows S...	Microsoft Corporation
1,180 K	1864		
1,508 K	1944	Host Process for Windows S...	Microsoft Corporation
1,544 K	2044	Host Process for Windows S...	Microsoft Corporation
1,016 K	1140	Host Process for Windows S...	Microsoft Corporation
1,400 K	2132	Host Process for Windows S...	Microsoft Corporation
1,404 K	2204	Host Process for Windows S...	Microsoft Corporation
1,696 K	2452	Host Process for Windows S...	Microsoft Corporation

To learn more about a specific DLL, you can select the running DLL in **Process Explorer** and use the **Search Online** option.

This will search online for detailed information about the DLL, helping to identify its function and legitimacy

Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-LA72I7T\Admin]

File Options View Process Find Users DLL Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
svchost.exe		3,436 K	19,216 K	2860	Host Process for Windows S...	Microsoft Corporation
taskhostw.exe		7,552 K	18,140 K	5696	Host Process for Windows T...	Microsoft Corporation
svchost.exe		1,772 K	7,700 K	288	Host Process for Windows S...	Microsoft Corporation
cfmon.exe		4,296 K	19,900 K	4952		
explorer.exe	< 0.01	64,324 K	173,564 K	1672	Windows Explorer	Microsoft Corporation
SecurityHealthSystray.exe		1,684 K	8,892 K	5284	Windows Security notificatio...	Microsoft Corporation
VBoxTray.exe	< 0.01	6,572 K	15,804 K	1952	VirtualBox Guest Additions Tr...	Oracle and/or its affiliates
msedge.exe		83,464 K	172,448 K	6860	Microsoft Edge	Microsoft Corporation
procexp64.exe	2.24	22,376 K	50,996 K	5664	Sysinternals Process Explorer	Sysinternals - www.sysinter...
svchost.exe		3,956 K	21,696 K	5292	Host Process for Windows S...	Microsoft Corporation
StartMenuExperienceHost.exe		23,616 K	62,696 K	2588		
RuntimeBroker.exe		5,716 K	26,928 K	3980	Runtime Broker	Microsoft Corporation
SearchApp.exe	Susp...	179,844 K	271,108 K	5840	Search application	Microsoft Corporation
RuntimeBroker.exe		14,684 K	45,216 K	4332	Runtime Broker	Microsoft Corporation
dllhost.exe		3,836 K	12,164 K	2540	COM Surrogate	Microsoft Corporation
RuntimeBroker.exe		10,552 K	26,848 K	4260	Runtime Broker	Microsoft Corporation
SecurityHealthService.exe		4,224 K	13,108 K	5744	Windows Security Health Se...	Microsoft Corporation

DLLs

Name	Description	Company Name	Path
zoneinfo64.res			C:\Windows\Globalization\ICU\zoneinfo64.res
zipfldr.dll.mun	Compressed (zipped) Folders	Microsoft Corporation	C:\Windows\SystemResources\zipfldr.dll.mun
zipfldr.dll.mui	Compressed (zipped) Folders	Microsoft Corporation	C:\Windows\System32\en-US\zipfldr.dll.mui
zipfldr.dll	Compressed (zipped) Folders	Microsoft Corporation	C:\Windows\System32\zipfldr.dll
xmllite.dll	Microsoft XML Lite Library	Microsoft Corporation	C:\Windows\System32\xmllite.dll
wtsapi32.dll	Windows Remote Desktop Sessio...	Microsoft Corporation	C:\Windows\System32\wtsapi32.dll
wscui.cpl.mui	Security and Maintenance	Microsoft Corporation	C:\Windows\System32\en-US\wscui.cpl.mui
wscui.cpl	Security and Maintenance	Microsoft Corporation	C:\Windows\System32\wscui.cpl
wscui.cpl	Security and Maintenance	Microsoft Corporation	C:\Windows\System32\wscui.cpl
wscinterop.dll	Windows Health Center WSC Inter...	Microsoft Corporation	C:\Windows\System32\wscinterop.dll
wscapi.dll	Windows Security Center API	Microsoft Corporation	C:\Windows\System32\wscapi.dll
ws2_32.dll	Windows Socket 2.0 32-Bit DLL	Microsoft Corporation	C:\Windows\System32\ws2_32.dll
WppRecorderUM.dll	"WppRecorderUM.DYNLINK"	Microsoft Corporation	C:\Windows\System32\WppRecorderUM.dll
wpnclient.dll	Windows Push Notifications Client	Microsoft Corporation	C:\Windows\System32\wpnclient.dll
wpnapps.dll	Windows Push Notification Apps	Microsoft Corporation	C:\Windows\System32\wpnapps.dll
WPDSHServiceObj.dll	Windows Portable Device Shell Se...	Microsoft Corporation	C:\Windows\System32\WPDSHServiceObj.dll

CPU Usage: 2.24% Commit Charge: 37.32% Processes: 124 Physical Usage: 48.84%

Properties of dlls

The screenshot shows the Process Hacker interface. On the left, the 'Handles' tab is selected, displaying a list of handles with columns for Type and Name. On the right, the 'xmllite.dll Properties' window is open, showing the 'Image' tab with the following details:

- Name:** xmllite.dll
- Description:** Microsoft XMLLite Library
- Company:** Microsoft Corporation
- Printable strings found in the scan:**
 - CDAT
 - !This program cannot be run in DOS mode.
 - Rich
 - .text
 - .rdata
 - @.data
 - .pdata
 - @.rsrc
 - @.reloc
 - tDH
 - t\$ WAVAWH
 - uQL
 - t\$H
 - D\$XH
 - FfD

At the bottom, resource usage statistics are displayed: CPU Usage: 2.24%, Commit Charge: 37.32%, Processes: 124.

The screenshot shows the Process Hacker interface with the 'Handles' tab selected. The list of handles includes various system objects such as ALPC Ports, Desktops, Directories, and Events, each with a long, complex name. At the bottom, resource usage statistics are displayed: CPU Usage: 4.49%, Commit Charge: 37.45%, Processes: 124, Physical Usage: 48.79%.

Closing a handle

The screenshot shows the Process Hacker interface with the 'Handles' tab selected. A specific handle entry in the list has a context menu open over it. The menu items shown are 'Close Handle' and 'Properties...'. The handle itself is a long string starting with '\BaseNamedObjects\...'. At the bottom, resource usage statistics are displayed: CPU Usage: 4.43%, Commit Charge: 37.48%, Processes: 123, Physical Usage: 48.77%.

Properties of handles

The screenshot shows the Windows Task Manager or similar monitoring tool. The 'Handles' tab is active, displaying a list of handles categorized by type (e.g., ALPC Port, Desktop, Directory, Event) and their corresponding names. A specific handle, '\BaseNamedObjects\[CoreUI]-PID(1672)-TID(2236) be0f25c...', is selected and shown in a detailed properties window. The properties window includes tabs for 'Details' and 'Security'. The 'Details' tab displays information such as Name, Type (ALPC Port), Description, Address (0xFFFFB18C5150A9B0), References (64973), and Quota Charges (Paged: 0, Non-Paged: 608). The bottom status bar shows CPU Usage: 5.69%, Commit Charge: 37.31%, Processes: 122, and Physical.

Running threads

The screenshot shows the 'Threads' tab in the monitoring tool. It lists 15 threads, each with a state icon (yellow circle with a black dot), wait reason, TID, user time, kernel time, and various performance metrics like CPU usage and start time. The threads are primarily in a 'Waiting' state due to UserRequest. The bottom status bar shows CPU Usage: 1.54%, Commit Charge: 37.42%, Processes: 121, and Physical Usage: 48.92%.

State	Wait Reason	TID	User Time	Kernel Time	CPU	CPU Time	Start Time	Start Address	Base Pri	Dy
Waiting	UserRequest	6016	00:00:00	00:00:01	< 0.01	00:00:02	01/25/25 21:...	shcore.dll!Ordinal172+0x...	9	
Waiting	WrUserRequest	2236	00:00:05	00:00:05		00:00:11	01/25/25 21:...	Explorer.EXE+0xa4220	8	
Waiting	UserRequest	5524	00:00:00	00:00:01		00:00:01	01/25/25 21:...	windows.immersiveshell.s...	8	
Waiting	WrAlertByThre...	2748	00:00:00	00:00:00		00:00:00	01/25/25 21:...	ucrtbase.dll!confighreadl...	8	
Waiting	WrQueue	6012	00:00:00	00:00:00		00:00:00	01/25/25 21:...	ntdll.dll!TpReleaseClean...	8	
Waiting	UserRequest	6036	00:00:00	00:00:00		00:00:00	01/25/25 21:...	shcore.dll!Ordinal172+0x...	8	
Waiting	UserRequest	4632	00:00:00	00:00:00		00:00:00	01/25/25 21:...	Explorer.EXE+0x184f0	8	
Waiting	UserRequest	880	00:00:00	00:00:00		00:00:00	01/25/25 21:...	sppc.dll!SLpVLActivateP...	8	
Waiting	UserRequest	4020	00:00:00	00:00:00		00:00:00	01/25/25 21:...	InputHost.dll!DlGetActiv...	8	
Waiting	UserRequest	4192	00:00:00	00:00:00		00:00:00	01/25/25 21:...	twinui.pcshell.dll!DlGetCl...	8	
Waiting	UserRequest	2116	00:00:00	00:00:00		00:00:00	01/25/25 21:...	twinui.pcshell.dll!DlCanU...	8	
Waiting	UserRequest	1832	00:00:00	00:00:00		00:00:00	01/25/25 21:...	ucrtbase.dll!confighreadl...	8	

Options in threads

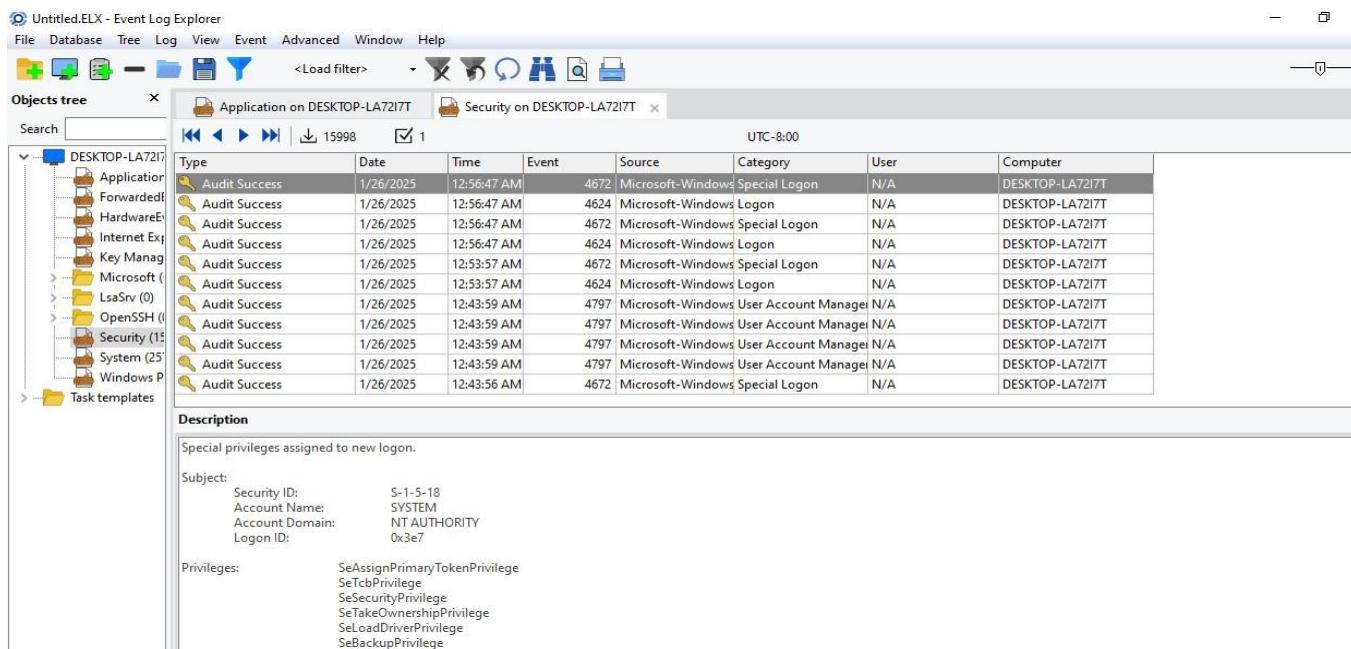
The screenshot shows the 'Threads' tab with a context menu open over a specific thread (TID 296). The menu options include Stack..., Module..., Security..., Terminate..., Suspend..., and Resume... (disabled). The bottom status bar shows CPU Usage: 0.77%, Commit Charge: 37.23%, Processes: 122, and Physical Usage: 48.39%.

Viewing, Monitoring, and Analyzing Events Using the Event Log Explorer Tool

The **Event Log Explorer** is a powerful tool designed to help you view, monitor, and analyze system events in great detail. It provides access to comprehensive logs for various system activities, including:

- **Tracking System Events:** It allows you to monitor and track all kinds of events, such as system startup and shutdown, application errors, security events, and more.
- **Detecting Anomalies:** By reviewing event logs, you can identify unusual patterns or activities that may suggest potential issues, security breaches, or malware activity.
- **Troubleshooting:** Event Log Explorer helps you diagnose and troubleshoot system issues by providing detailed event data that can highlight errors or misconfigurations within the system.

The tool allows you to filter, sort, and analyze logs, making it easier to identify and address system problems or track the history of specific activities. It is an essential tool for administrators and security professionals looking to maintain the health and security of their systems.



The screenshot shows the Event Log Explorer interface with the title bar "Untitled.ELX - Event Log Explorer". The menu bar includes File, Database, Tree, Log, View, Event, Advanced, Window, and Help. Below the menu is a toolbar with icons for file operations like Open, Save, and Filter. The main window has two tabs: "Application on DESKTOP-LA72I7T" and "Security on DESKTOP-LA72I7T". The "Security" tab is selected, showing a list of events with a total count of 15998. A search bar is present above the list. The list table has columns: Type, Date, Time, Event, Source, Category, User, and Computer. The first few rows show Audit Success events from 1/26/2025 at 12:56:47 AM, source 4672, category Microsoft-Windows Special Logon, user N/A, and computer DESKTOP-LA72I7T. Below the table is a "Description" section with details about a logon event, including Subject (Security ID: S-1-5-18, Account Name: SYSTEM, Account Domain: NT AUTHORITY, Logon ID: 0x3e7) and Privileges (SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege).

Type	Date	Time	Event	Source	Category	User	Computer
Audit Success	1/26/2025	12:56:47 AM	4672	Microsoft-Windows Special Logon	N/A	DESKTOP-LA72I7T	
Audit Success	1/26/2025	12:56:47 AM	4624	Microsoft-Windows Logon	N/A	DESKTOP-LA72I7T	
Audit Success	1/26/2025	12:56:47 AM	4672	Microsoft-Windows Special Logon	N/A	DESKTOP-LA72I7T	
Audit Success	1/26/2025	12:56:47 AM	4624	Microsoft-Windows Logon	N/A	DESKTOP-LA72I7T	
Audit Success	1/26/2025	12:53:57 AM	4672	Microsoft-Windows Special Logon	N/A	DESKTOP-LA72I7T	
Audit Success	1/26/2025	12:53:57 AM	4624	Microsoft-Windows Logon	N/A	DESKTOP-LA72I7T	
Audit Success	1/26/2025	12:43:59 AM	4797	Microsoft-Windows User Account Manager	N/A	DESKTOP-LA72I7T	
Audit Success	1/26/2025	12:43:59 AM	4797	Microsoft-Windows User Account Manager	N/A	DESKTOP-LA72I7T	
Audit Success	1/26/2025	12:43:59 AM	4797	Microsoft-Windows User Account Manager	N/A	DESKTOP-LA72I7T	
Audit Success	1/26/2025	12:43:59 AM	4797	Microsoft-Windows User Account Manager	N/A	DESKTOP-LA72I7T	
Audit Success	1/26/2025	12:43:56 AM	4672	Microsoft-Windows Special Logon	N/A	DESKTOP-LA72I7T	

This displays a description of the logs along with detailed properties of each event.

Applying filter

Filter X

Apply filter to:

Active event log view (Security on DESKTOP-LA72I7T)
 Event log view(s) on your choice

Event types <input checked="" type="checkbox"/> Verbose <input checked="" type="checkbox"/> Information <input checked="" type="checkbox"/> Warning <input checked="" type="checkbox"/> Error <input checked="" type="checkbox"/> Critical <input checked="" type="checkbox"/> Audit Success <input checked="" type="checkbox"/> Audit Failure	Source: Microsoft-Windows-Security-Auditing <input type="button" value="..."/> <input type="checkbox"/> Exclude Category: Logoff,Logon,'Security State Change','Service shutdown' <input type="button" value="..."/> <input type="checkbox"/> Exclude User: <input type="text"/> <input type="button" value="..."/> <input type="checkbox"/> Exclude Computer: DESKTOP-LA72I7T <input type="button" value="..."/> <input type="checkbox"/> Exclude
--	---

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

Text in description: RegExp Exclude

Date Time Separately Exclude
 From: 1/26/2025 12:00:00 AM To: 1/26/2025 12:00:00 AM Exclude

Display event for the last days hours Exclude

Custom columns **Description params**

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

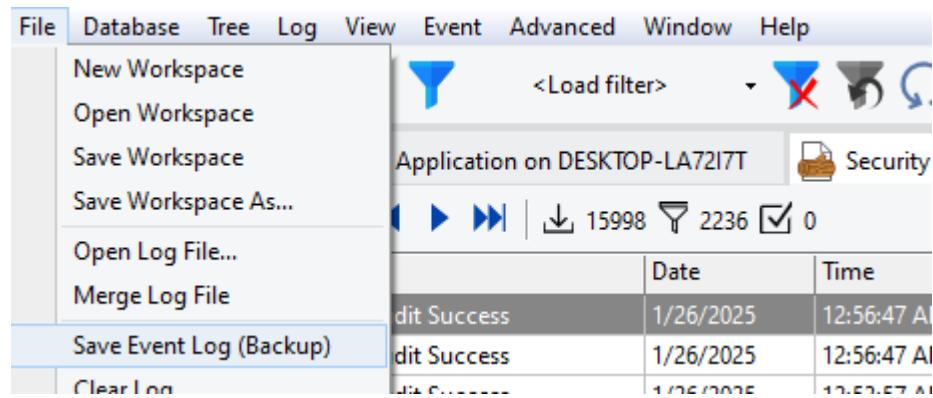
Clear **Load...** **Save...** Case sensitive **OK** **Cancel**

Filtered results

Type	Date	Time	Event	Source	Category	User	Computer
Audit Success	1/26/2025	12:56:47 AM	4624	Microsoft-Windows-Security-Auditing	Logon	N/A	DESKTOP-LA72I7T
Audit Success	1/26/2025	12:56:47 AM	4624	Microsoft-Windows-Security-Auditing	Logon	N/A	DESKTOP-LA72I7T
Audit Success	1/26/2025	12:53:57 AM	4624	Microsoft-Windows-Security-Auditing	Logon	N/A	DESKTOP-LA72I7T
Audit Success	1/26/2025	12:43:56 AM	4624	Microsoft-Windows-Security-Auditing	Logon	N/A	DESKTOP-LA72I7T
Audit Success	1/26/2025	12:40:15 AM	4624	Microsoft-Windows-Security-Auditing	Logon	N/A	DESKTOP-LA72I7T
Audit Success	1/26/2025	12:23:53 AM	4624	Microsoft-Windows-Security-Auditing	Logon	N/A	DESKTOP-LA72I7T
Audit Success	1/26/2025	12:21:27 AM	4624	Microsoft-Windows-Security-Auditing	Logon	N/A	DESKTOP-LA72I7T
Audit Success	1/26/2025	12:21:26 AM	4624	Microsoft-Windows-Security-Auditing	Logon	N/A	DESKTOP-LA72I7T
Audit Success	1/26/2025	12:21:26 AM	4624	Microsoft-Windows-Security-Auditing	Logon	N/A	DESKTOP-LA72I7T
Audit Success	1/26/2025	12:14:31 AM	4624	Microsoft-Windows-Security-Auditing	Logon	N/A	DESKTOP-LA72I7T
Audit Success	1/26/2025	12:08:51 AM	4624	Microsoft-Windows-Security-Auditing	Logon	N/A	DESKTOP-LA72I7T

Description

Save the Event Log (Backup) for later analysis

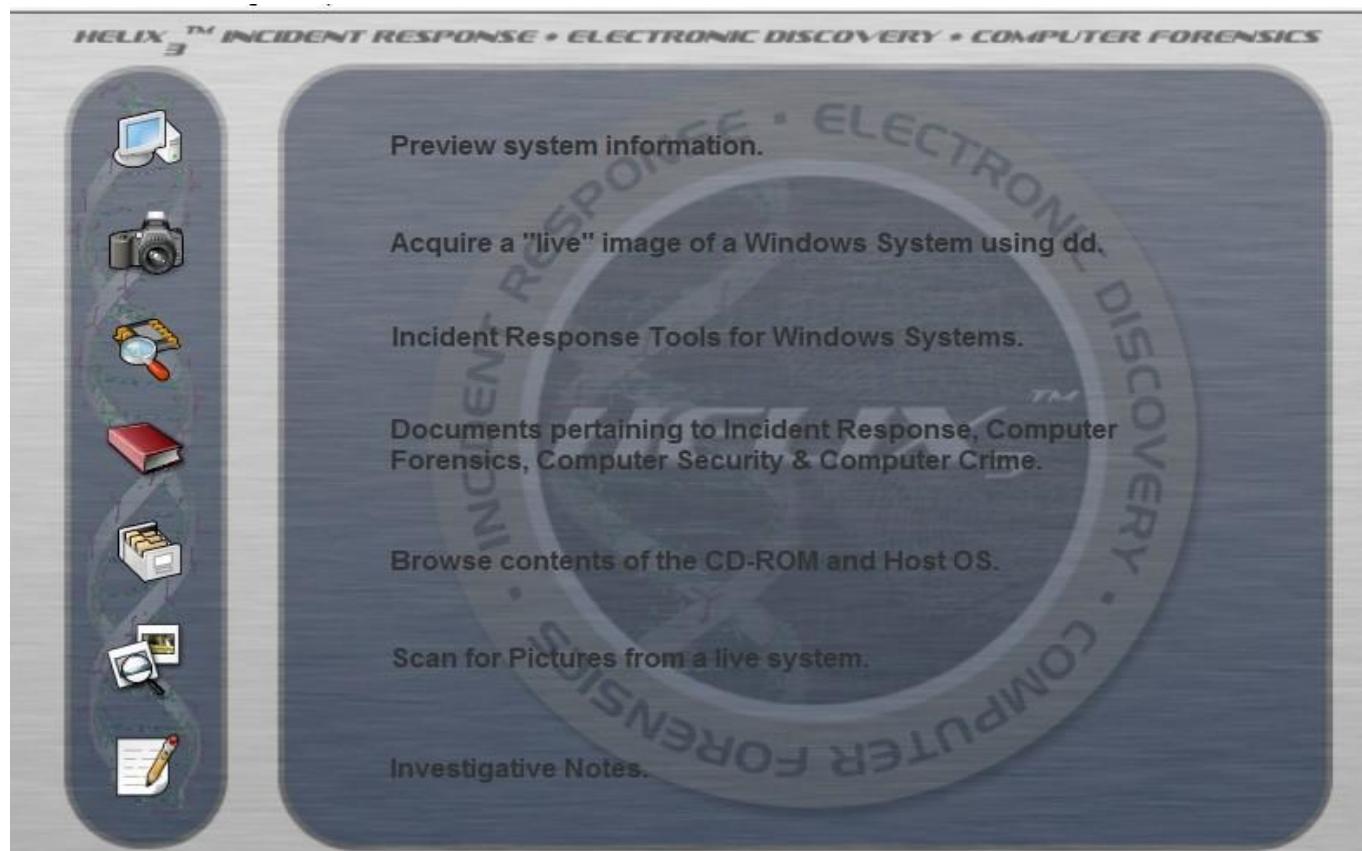


Performing a Computer Forensic Investigation Using the Helix Tool

The **Helix Tool** is an all-encompassing computer forensic platform designed for conducting thorough investigations on both live systems and disk images. It offers a wide range of features essential for digital forensics, including:

- Data Acquisition:** Helix enables the safe collection of digital evidence from live systems or disk images, ensuring that the data is preserved in a forensically sound manner without altering or damaging the original evidence.
- Analysis and Incident Response:** The tool provides capabilities for in-depth analysis, allowing investigators to examine the data and respond to incidents such as cyberattacks, data breaches, or other suspicious activities.
- Forensic Tools:** Helix includes specialized forensic utilities that ensure evidence is handled with integrity and complies with best practices for digital forensics. This helps in preserving the authenticity of the data during the investigation.
- Integration with FTK Imager:** Helix can also launch **FTK Imager**, a tool used for creating disk images and analyzing evidence. This integration facilitates detailed forensic investigations, allowing investigators to examine and process evidence from multiple sources effectively.

Overall, the Helix tool provides a complete suite of capabilities for conducting professional and thorough forensic investigations, ensuring that evidence is gathered, preserved, and analyzed properly.



System information

HELIX™ INCIDENT RESPONSE • ELECTRONIC DISCOVERY • COMPUTER FORENSICS

System Information

Operating System:

Owner Information:

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

Network Information:

- Host: DESKTOP-LA72I7T
- User: Admin
- IP: 10.0.2.15
- NIC: 0800271adb45
- Domain:

Drive:	Label:	Type:	Size:
C:\	(Logical drive)	NTFS	45479.1 MB
D:\	(CD/DVD-ROM drive)	NTFS	5119.9 MB
E:\	(Logical drive)	NTFS	700.6 MB
F:\	(CD/DVD-ROM drive)	CDFS	
G:\	(Logical drive)		

Live Acquisition

HELIX™ INCIDENT RESPONSE • ELECTRONIC DISCOVERY • COMPUTER FORENSICS

Live Acquisition

Acquire Physical Memory and/or Disk Drives

Source:
E:\ (Logical drive) - {NTFS} [5.00 GB]

Location Options: Attached/Share NetCat

Destination: \\forensics\images\

Image Name: image.dd

DD Options:

block size:	conv:	<input type="checkbox"/> Split Image
default	noerror	

Acquire

Incident Response



Select Agile Risk Management and choose the disk

The screenshot shows the Agile Risk Management Nigilant32 software interface. The title bar says "Nigilant32 - Windows Afterdark Forensic - Beta Release 0.1". The menu bar includes File, Edit, Tools, Help. The main window has a table with columns: Name, Written, Accessed, Created, Size, Inode, Type. A tooltip "Select Drive to Preview..." is shown above a preview dialog box. The dialog box contains the text "Select a physical disk partition to preview" and a table of disk partitions:

PhysicalDrive Name	Partition Number	Partition Length	Starting Offset	Drive Num..
PhysicalDrive0:Totalsize:53686402560 Bytes	Partition:1	52428800 Bytes	1048576	0
PhysicalDrive0:Totalsize:53686402560 Bytes	Partition:2	47688399872 Bytes	53477376	0
PhysicalDrive0:Totalsize:53686402560 Bytes	Partition:0	5369757696 Bytes	47742713856	0
PhysicalDrive0:Totalsize:53686402560 Bytes	Partition:3	572522496 Bytes	53112471552	0
PhysicalDrive0:Totalsize:53686402560 Bytes	Partition:4	5368709120 Bytes	47743762432	0

At the bottom of the dialog are "Cancel" and "Apply" buttons.

This shows the disk contents along with the hex of the selected file

The screenshot shows the Nigilant32 - Windows Afterdark Forensic - Beta Release 0.1 interface. The main window displays a table of file system entries and a hex dump of a selected file.

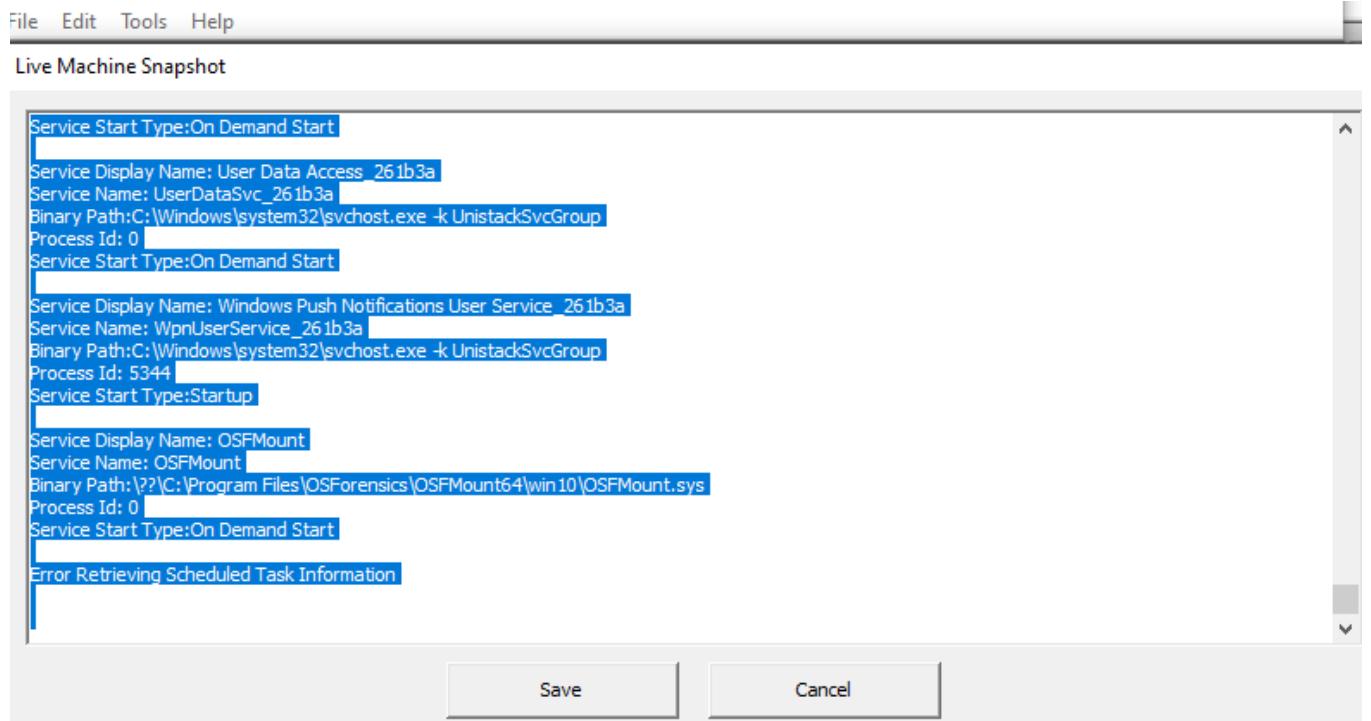
File System Entries:

Name	Written	Accessed	Created	Size	Inode	Type
pagefile.sys	Sun Jan 26 00:43:56 2025	Sun Jan 26 00:43:56 2025	Sun Jan 26 00:43:56 2025	1476395008	103718	0
\$AttrDef	Mon Dec 16 12:59:30 2024	Mon Dec 16 12:59:30 2024	Mon Dec 16 12:59:30 2024	2560	4	0
\$BadClus	Mon Dec 16 12:59:30 2024	Mon Dec 16 12:59:30 2024	Mon Dec 16 12:59:30 2024	443756544	8	0
\$Bitmap	Mon Dec 16 12:59:30 2024	Mon Dec 16 12:59:30 2024	Mon Dec 16 12:59:30 2024	1455404	6	0
\$Boot	Mon Dec 16 12:59:30 2024	Mon Dec 16 12:59:30 2024	Mon Dec 16 12:59:30 2024	8192	7	0
\$Extend	Mon Dec 16 12:59:30 2024	Mon Dec 16 12:59:30 2024	Mon Dec 16 12:59:30 2024	656	11	1
\$LogFile	Mon Dec 16 12:59:30 2024	Mon Dec 16 12:59:30 2024	Mon Dec 16 12:59:30 2024	67108864	2	0
SMFT	Mon Dec 16 12:59:30 2024	Mon Dec 16 12:59:30 2024	Mon Dec 16 12:59:30 2024	348389376	0	0
SMFTMirr	Mon Dec 16 12:59:30 2024	Mon Dec 16 12:59:30 2024	Mon Dec 16 12:59:30 2024	4096	1	0
\$Recycle.Bin	Mon Dec 23 21:15:45 2024	Sat Jan 25 21:39:51 2025	Mon Dec 23 21:15:45 2024	712	58	1
SSecure	Mon Dec 16 12:59:30 2024	Mon Dec 16 12:59:30 2024	Mon Dec 16 12:59:30 2024	2850384	9	0
SupCase	Mon Dec 16 12:59:30 2024	Mon Dec 16 12:59:30 2024	Mon Dec 16 12:59:30 2024	131104	10	0
SVolume	Mon Dec 16 12:59:30 2024	Mon Dec 16 12:59:30 2024	Mon Dec 16 12:59:30 2024	0	3	0
SWINREAgent	Mon Dec 23 21:40:17 2024	Sat Dec 29 00:20:40 2024	Mon Dec 23 21:40:17 2024	144	20014	1

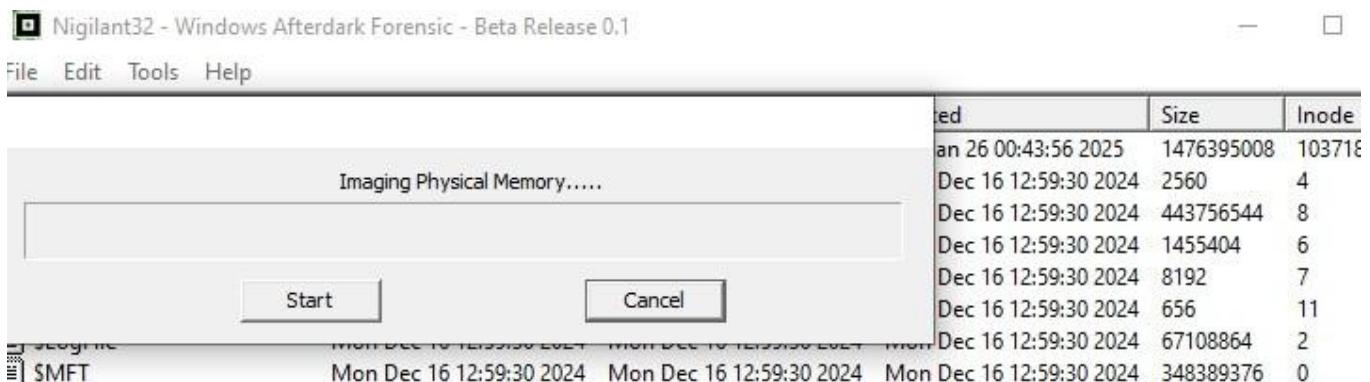
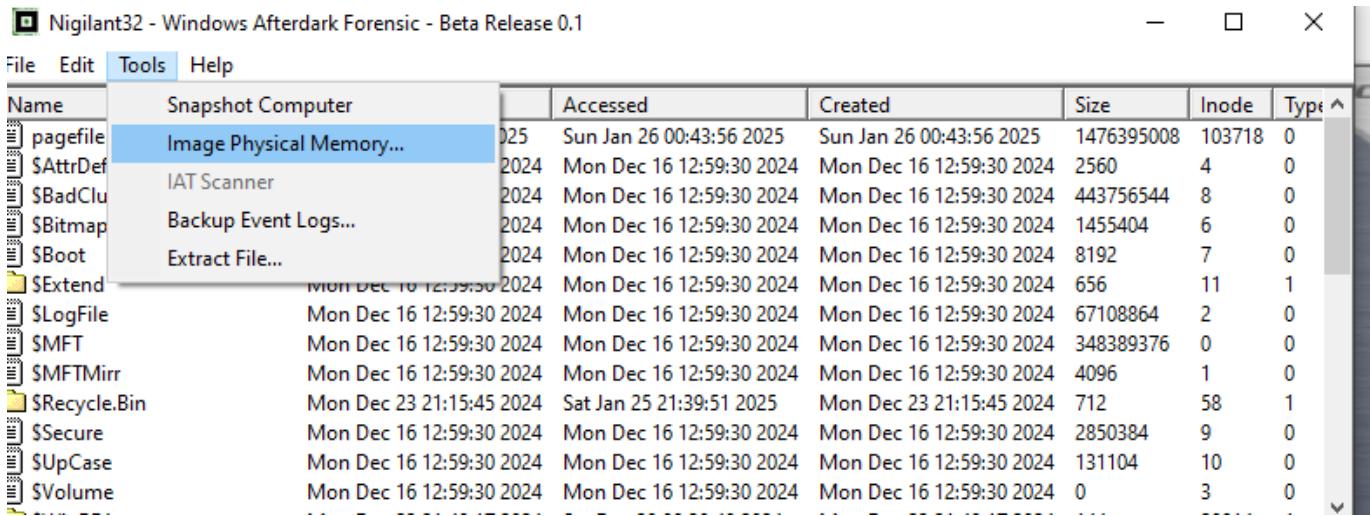
Hex Dump:

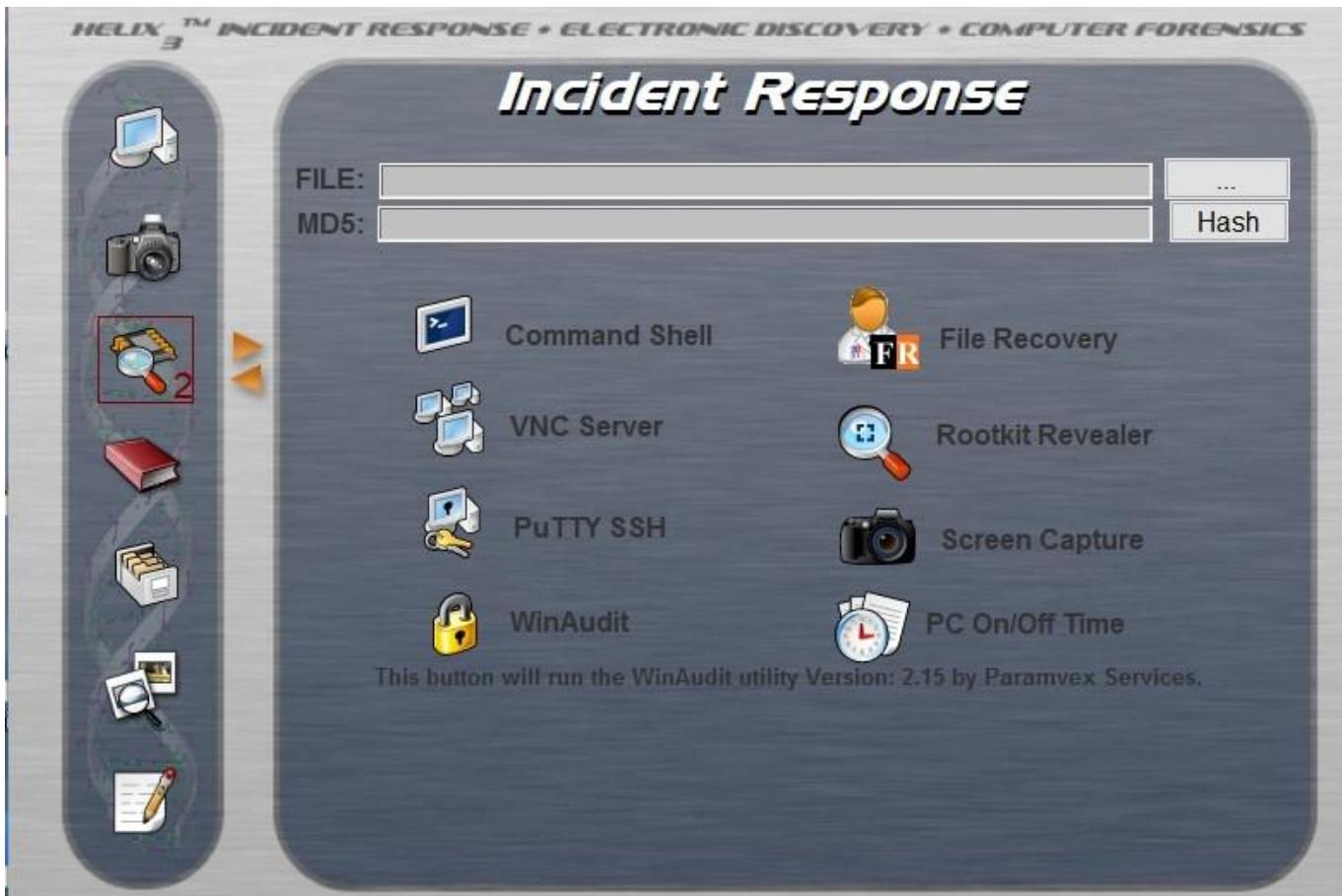
Address	Hex	ASCII	Description		
00000000	52 53 54 52	1E 00 09 00	00 00 00 00	00 00 00 00	RSTR.....
00000010	00 10 00 00	00 10 00 00	30 00 00 00	02 00 77 040....w.
00000020	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
00000030	62 D4 3E 71	00 00 00 00	01 00 FF FF	00 00 00 00	b.>q.....
00000040	28 00 00 00	E0 00 40 00	00 00 00 04	00 00 00 00	(....@.....
00000050	70 00 00 00	30 00 40 00	06 3F 22 07	00 00 00 00	p...0..@..?".
00000060	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
00000070	58 CC 3E 71	00 00 00 00	62 D4 3E 71	00 00 00 00	X.>q...b.>q...
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

Snapshot the machine by selecting tools → snapshot



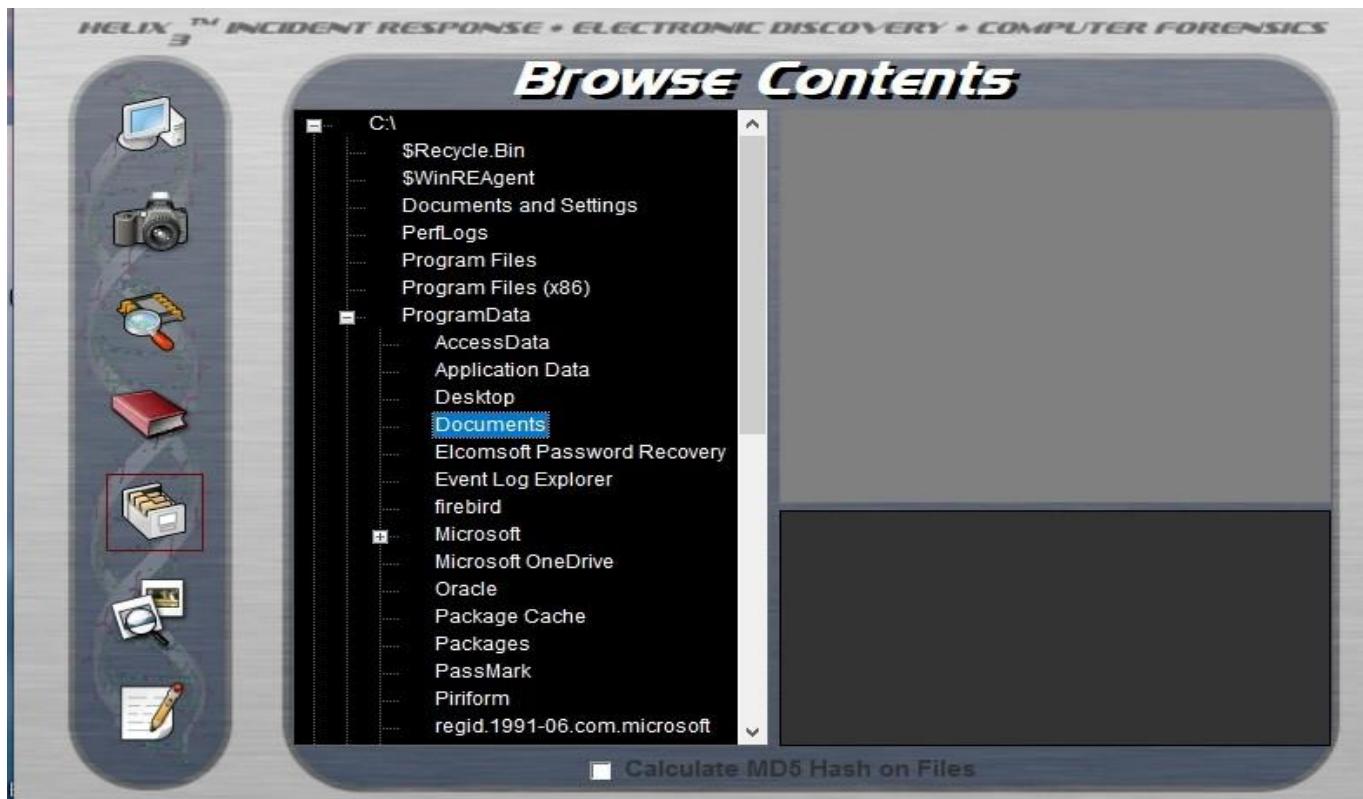
To create an image of physical memory, go to **Tools** and select **Image Physical Memory**





To generate an MD5 hash and recover files, we use the file recovery feature to retrieve deleted files. However, at the moment, the backend is not opening, and the file recovery tool is crashing

Browse Contents



Scan for pictures - It scans for pictures, in what directory we are loading.



4) Acquiring volatile data in Linux

In Linux, volatile data, such as user and session-related information, is stored in RAM when the system is live.

This data can include active user sessions, running processes, network connections, and other runtime information, which can be crucial for forensic investigations.

```
(kartikeyan㉿kali)-[~]
$ uname -a
Linux kali 6.11.2-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.11.2-1kali1 (2024-10-15) x86_64 GNU/Lin
ux
```

The **uname** command displays detailed system information about the Linux operating system, such as kernel version, architecture, and hostname.

```
(root㉿kali)-[/home/kartikeyan]
# lshw -short
H/W path          Device      Class      Description
=====
/0                  system      VMware Virtual Platform
/0/0                 bus        440BX Desktop Reference Platform
/0/0/0               memory     86KiB BIOS
/0/1                 processor   Intel(R) Core(TM) i7-10510U CPU @ 1.80GHz
/0/1/0               memory     16KiB L1 cache
/0/1/1               memory     16KiB L1 cache
/0/2                 processor   Intel(R) Core(TM) i7-10510U CPU @ 1.80GHz
/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/a/9a              memory     16KiB L1 cache
/0/b                 processor   CPU
/0/b/9b              memory     16KiB L1 cache
/0/c                 processor   CPU
/0/c/9c              memory     16KiB L1 cache
/0/d                 processor   CPU
/0/d/9d              memory     16KiB L1 cache
/0/e                 processor   CPU
/0/e/9e              memory     16KiB L1 cache
/0/f                 processor   CPU
sudo
```

The **lshw -short** command provides a summary of the hardware details, including CPU, memory, disk, and network devices, offering a concise overview of the system's physical components.

```
(root㉿kali)-[/home/kartikeyan]
# w
21:48:49 up 5 min,  4 users,  load average: 0.16, 0.31, 0.18
USER   TTY      FROM           LOGIN@    IDLE    JCPU   PCPU WHAT
kartikeyan  pts/2      -          21:43    5:20   7.52s  0.03s /usr/libexec/gnome-session-b
kartikeyan  pts/1      -          21:43    5:14   0.00s  0.34s /usr/lib/systemd/systemd --u
root    pts/1      -          21:47    0.00s  0.99s  0.04s w
root    pts/1      -          21:47    5:14   0.00s  0.12s /usr/lib/systemd/systemd --u
```

The **w** command displays uptime details, including system load, the number of users, and their current activity.

```
[sudo] password for Karthikeyan:
└─(root㉿kali)-[~/home/karthikeyan]
└─# last -a
root      pts/1          Sun Jan 26 22:02 - still logged in
karthike  tty2          Sun Jan 26 22:00 - still logged in
Debian-g  tty1          Sun Jan 26 22:00 - 22:01  (00:00)
Debian-g  tty1          Sun Jan 26 21:59 - 21:59  (00:00)

/var/lib/wtmpdb/wtmp.db begins Sun Jan 26 21:59:00 2025
```

The **last -a** command shows the details of the last login sessions, including the user, login time, and IP address.

```
└─(root㉿kali)-[~/home/karthikeyan]
└─# netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address          Foreign Address        State
udp      0      0 kali:bootpc            192.168.133.254:bootps ESTABLISHED

Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type      State      I-Node    Path
unix     3      [ ]      STREAM   CONNECTED  15755
unix     3      [ ]      STREAM   CONNECTED  15574    /run/user/1000/at-spi/bus_1
unix     3      [ ]      STREAM   CONNECTED  14221
unix     3      [ ]      STREAM   CONNECTED  14681
unix     3      [ ]      DGRAM    CONNECTED  17804
unix     3      [ ]      STREAM   CONNECTED  15828    /run/user/1000/pulse/native
unix     2      [ ]      DGRAM    CONNECTED  15703
unix     3      [ ]      STREAM   CONNECTED  15502    /run/systemd/journal/stdout
unix     3      [ ]      STREAM   CONNECTED  8821     /run/dbus/system_bus_socket
unix     3      [ ]      STREAM   CONNECTED  14222    /run/user/1000/bus
unix     3      [ ]      STREAM   CONNECTED  15688
unix     3      [ ]      STREAM   CONNECTED  15641
unix     3      [ ]      STREAM   CONNECTED  15647
unix     3      [ ]      STREAM   CONNECTED  12120
unix     3      [ ]      STREAM   CONNECTED  9420     /run/systemd/journal/stdout
unix     3      [ ]      DGRAM    CONNECTED  17805
unix     3      [ ]      STREAM   CONNECTED  15917
unix     3      [ ]      STREAM   CONNECTED  14297    /run/user/1000/pipewire-0
unix     3      [ ]      STREAM   CONNECTED  14084    /run/user/1000/bus
unix     3      [ ]      STREAM   CONNECTED  8983     /run/systemd/journal/stdout
unix     3      [ ]      STREAM   CONNECTED  8688
```

The **netstat** command provides network status information, including active connections, listening ports, and network interface statistics.

```
└─(root㉿kali)-[~/home/karthikeyan]
└─# ifconfig -a
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.133.130 netmask 255.255.255.0 broadcast 192.168.133.255
        inet6 fe80::20c:29ff:fe1e:a579 prefixlen 64 scopeid 0x20<link>
            ether 00:0c:29:1e:a5:79 txqueuelen 1000 (Ethernet)
            RX packets 24 bytes 8803 (8.5 KiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 47 bytes 5751 (5.6 KiB)
            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 24 bytes 1440 (1.4 KiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 24 bytes 1440 (1.4 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

The **ipconfig** command lists the current network settings, including IP address, subnet mask, and default gateway.

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

[root@kali]# lsmod
Module           Size  Used by
snd_seq_dummy    12288  0
snd_hrtimer      12288  2
snd_seq_midi     20480  0
snd_seq_midi_event 16384  1 snd_seq_midi
snd_seq          110592 15 snd_seq_midi,snd_seq_midi_event,snd_seq_dummy
rfkill            40960  4
qrtr              57344  2
intel_rapl_msr   20480  0
intel_rapl_common 53248  1 intel_rapl_msr
sunrpc            872448 1
intel_uncore_frequency_common 16384  0
```

The **lsof** command lists all open files, including those associated with ports, services, and processes, helping to identify active network connections and resource usage.

Install auditd

```
[root@kali]# apt install auditd
Upgrading:
  libaudit-common  libaudit1

Installing:
  auditd

Installing dependencies:
  libauparse0t64

Suggested packages:
  audispd-plugins

Summary:
  Upgrading: 2, Installing: 2, Removing: 0, Not Upgrading: 1146
  Download size: 354 kB
  Space needed: 957 kB / 30.9 GB available
```

```
[root@kali]~[~/home/karthikeyan]
# aureport

Summary Report
=====
Range of time in logs: 26/01/25 22:13:32.957 - 26/01/25 22:13:32.955
Selected time for report: 26/01/25 22:13:32 - 26/01/25 22:13:32.955
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: 2
Number of terminals: 2
Number of host names: 1
Number of executables: 2
Number of commands: 1
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
Number of integrity events: 0
Number of virt events: 0
Number of keys: 0
Number of process IDs: 3
```

The **aureport** command is used in Linux to generate audit reports from the **auditd** daemon.

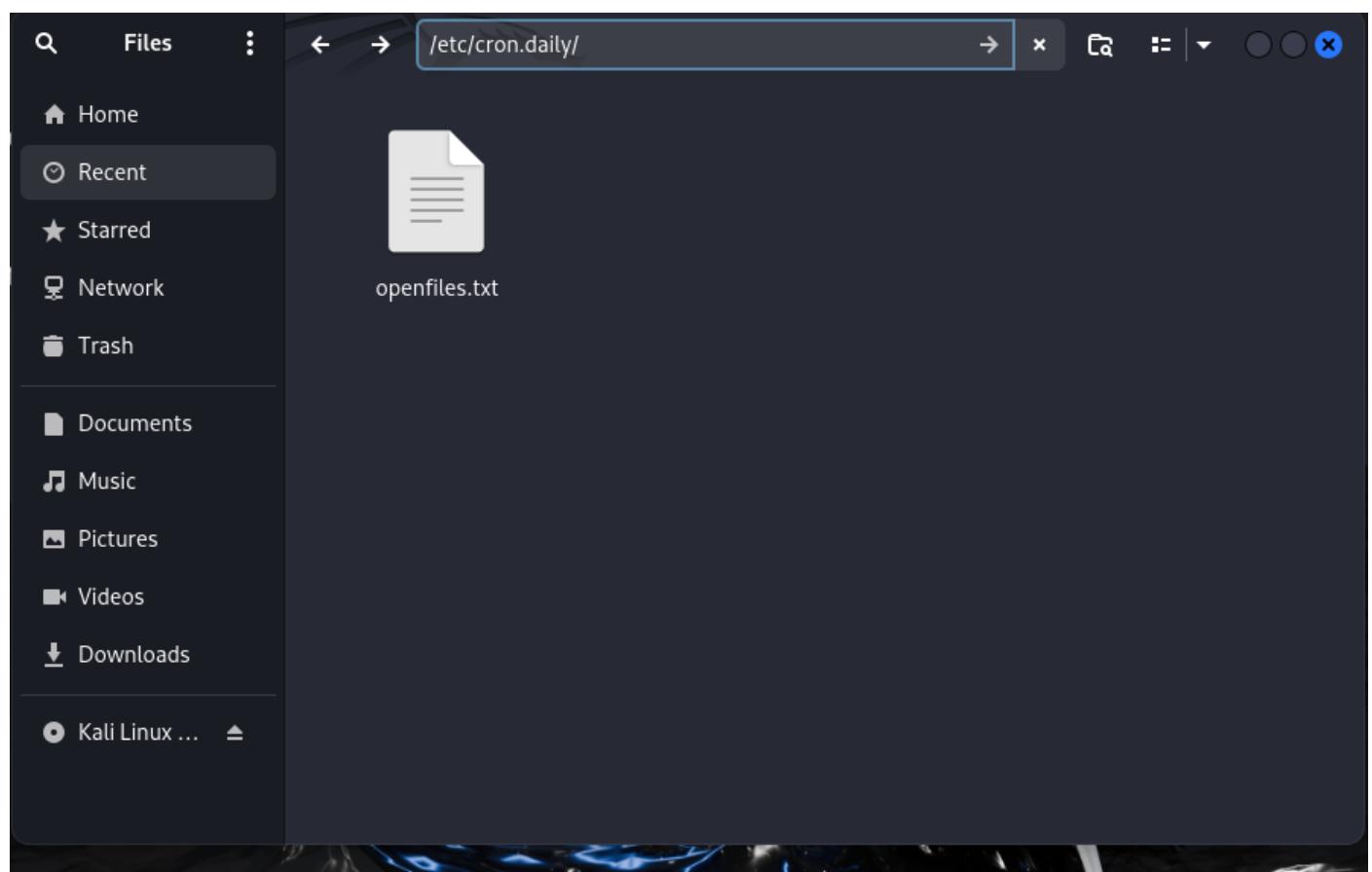
```
[root@kali]~[/home/karthikeyan]
# id root
uid=0(root) gid=0(root) groups=0(root)

[root@kali]~[/home/karthikeyan]
# ausearch -ui 0 --interpret
-----
type=DAEMON_START msg=audit(26/01/25 22:13:32.957:7212) : op=start ver=4.0.2 format=enriched kernel=6.11.2-amd64 auid	unset pid=4073 uid=root ses	unset subj=unconfined res=success
-----
type=SERVICE_START msg=audit(26/01/25 22:13:32.955:3) : 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(26/01/25 22:13:32.955:4) : pid=4045 uid=root auid=kartikeyan ses=3 subj=unconfined msg='op=PAM:session_close grantors=pam_limits,pam_permit,pam_umask,pam_unix,pam_winbind acct=root exe=/usr/bin/sudo hostname=? addr=? terminal=/dev/pts/1 res=success'
-----
type=CRED_DISP msg=audit(26/01/25 22:13:32.955:5) : pid=4045 uid=root auid=kartikeyan ses=3 subj=unconfined msg='op=PAM:setcred grantors=pam_permit acct=root exe=/usr/bin/sudo hostname=? addr=? terminal=/dev/pts/1 res=success'
```

The **ausearch -ui 0 --interpret** command in Linux is used to search audit logs for events related to the user ID 0 (root user).

/var/spool/cron directory is used in Linux to store **crontab files** for individual users. These files define scheduled tasks that the system executes at specified times.

Each user has their own crontab file within this directory, and the system reads these files to execute the scheduled jobs.



The `/etc/cron.daily` directory in Linux contains scripts or tasks that are scheduled to run once daily.

A screenshot of a terminal window on a Linux desktop. The terminal session starts with the user's login information: `[karthikeyan@kali)-[~]`. The user then runs the command `$ cat .zsh_history`, which outputs several commands related to network scanning and file manipulation:

```

└─$ cat .zsh_history
metasploit
ls
/usr/share/nmap/scripts
ls
sudo nano My_scan.nse
ls
cd ..
ping 192.168.133.13\
/usr/share/nmap/scripts
nano My_scan.nse\
sudo nano My_scan.nse\
suod rm My_scan.nse\
sudo rm My_scan.nse\
sudo nano My_scan.nse\
sudo mv My_scan.nse /usr/share/nmap/scripts/\
sudo nmap --script-updatedb\

```

In the background, a file named 'openfiles.txt' is visible in a file manager window.

The `.bash_history` file is located in a user's home directory (e.g., `~/.bash_history`) and stores the command history of the `bash` shell.

```
(kartikeyan㉿kali)-[~]
$ arp
Address          HWtype  HWaddress          Flags Mask   Iface
192.168.133.254  ether    00:50:56:fe:18:55  C      eth0
_gateway         ether    00:50:56:eb:95:ed  C      eth0
```

The **arp** command is used to view and manage the **Address Resolution Protocol (ARP)** cache on a system.

The **ps auxww** command in Linux provides a detailed list of all running processes on the system.

- **a:** Shows processes for all users.
- **u:** Displays process information in a user-friendly format, including the user, CPU, and memory usage.
- **x:** Includes processes without a controlling terminal.
- **ww:** Ensures the full command line of each process is displayed without truncation.

```
root@kali: /home/kartikeyan
# ps auxww
USER        PID %CPU %MEM    VSZ   RSS TTY      STAT START  TIME COMMAND
root          1  0.1  0.3 23392 14456 ?        Ss   22:00  0:02 /sbin/init splash
root          2  0.0  0.0     0     0 ?        S    22:00  0:00 [kthreadd]
root          3  0.0  0.0     0     0 ?        S    22:00  0:00 [pool_workqueue_release]
root          4  0.0  0.0     0     0 ?        I<  22:00  0:00 [kworker/R-rcu_gp]
root          5  0.0  0.0     0     0 ?        I<  22:00  0:00 [kworker/R-sync_wq]
root          6  0.0  0.0     0     0 ?        I<  22:00  0:00 [kworker/R-slub_flushwq]
root          7  0.0  0.0     0     0 ?        I<  22:00  0:00 [kworker/R-netns]
root          8  0.0  0.0     0     0 ?        I    22:00  0:00 [kworker/0:0-events]
root         11  0.0  0.0     0     0 ?        I    22:00  0:00 [kworker/u512:0-ipv6_addrco
nf]
root         12  0.0  0.0     0     0 ?        I<  22:00  0:00 [kworker/R-mm_percpu_wq]
root         13  0.0  0.0     0     0 ?        I    22:00  0:00 [rcu_tasks_kthread]
root         14  0.0  0.0     0     0 ?        I    22:00  0:00 [rcu_tasks_rude_kthread]
root         15  0.0  0.0     0     0 ?        I    22:00  0:00 [rcu_tasks_trace_kthread]
root         16  0.0  0.0     0     0 ?        S    22:00  0:00 [ksoftirqd/0]
root         17  0.0  0.0     0     0 ?        I    22:00  0:00 [rcu_preempt]
root         18  0.0  0.0     0     0 ?        S    22:00  0:00 [rcu_exp_par_gp_kthread_wor
ker/1]
root         19  0.0  0.0     0     0 ?        S    22:00  0:00 [rcu_exp_gp_kthread_worker]
root         20  0.0  0.0     0     0 ?        S    22:00  0:00 [migration/0]
root         21  0.0  0.0     0     0 ?        S    22:00  0:00 [idle_inject/0]
root         22  0.0  0.0     0     0 ?        S    22:00  0:00 [cpuhp/0]
root         23  0.0  0.0     0     0 ?        S    22:00  0:00 [cpuhp/1]
root         24  0.0  0.0     0     0 ?        S    22:00  0:00 [idle_inject/1]
root         25  0.0  0.0     0     0 ?        S    22:00  0:00 [migration/1]
root         26  0.0  0.0     0     0 ?        S    22:00  0:00 [ksoftirqd/1]
root         28  0.0  0.0     0     0 ?        I<  22:00  0:00 [kworker/1:0H-events_highpr
i]
root         33  0.0  0.0     0     0 ?        S    22:00  0:00 [kdevtmpfs]
root         34  0.0  0.0     0     0 ?        I<  22:00  0:00 [kworker/R-inet_frag_wq]
root         36  0.0  0.0     0     0 ?        S    22:00  0:00 [kauditfd]
root         37  0.0  0.0     0     0 ?        S    22:00  0:00 [khungtaskd]
root         38  0.0  0.0     0     0 ?        S    22:00  0:00 [oom_reaper]
```

The **ss -l -p -n | grep 4793** command is used to inspect network sockets and filter results for a specific process or port (in this case, 4793):

- **ss:** Displays detailed socket statistics.
- **-l:** Lists listening sockets.
- **-p:** Shows the processes using the sockets.
- **-n:** Displays addresses and ports in numeric form to avoid DNS lookups.
- **| grep 4793:** Filters the output to show only lines containing "4793," which could be a port number or process ID.

```
[root@kali]~# ss -l -p -n | grep 4793
```

X clip command stores the details of text copied.

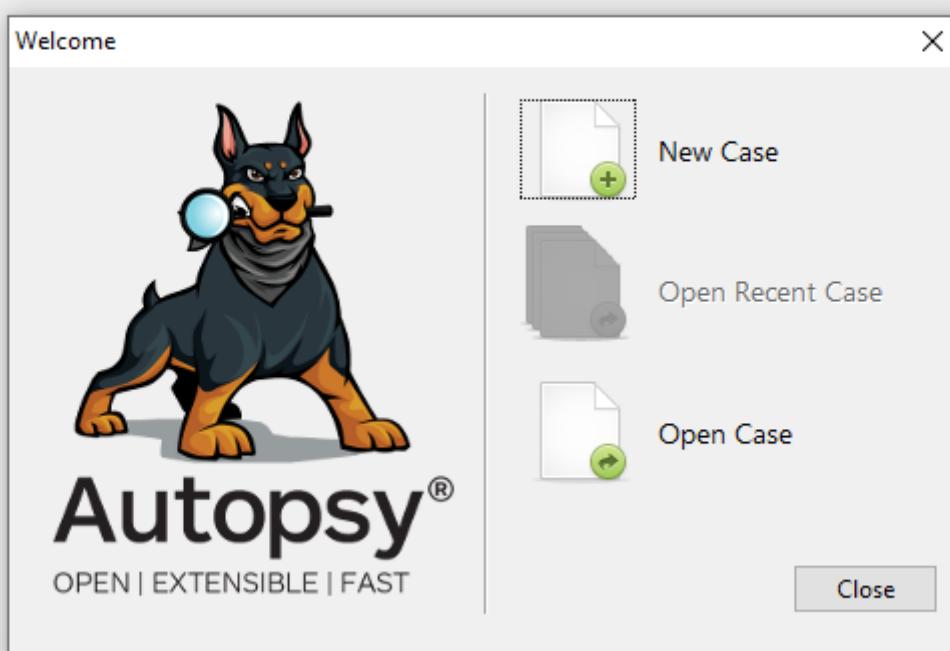
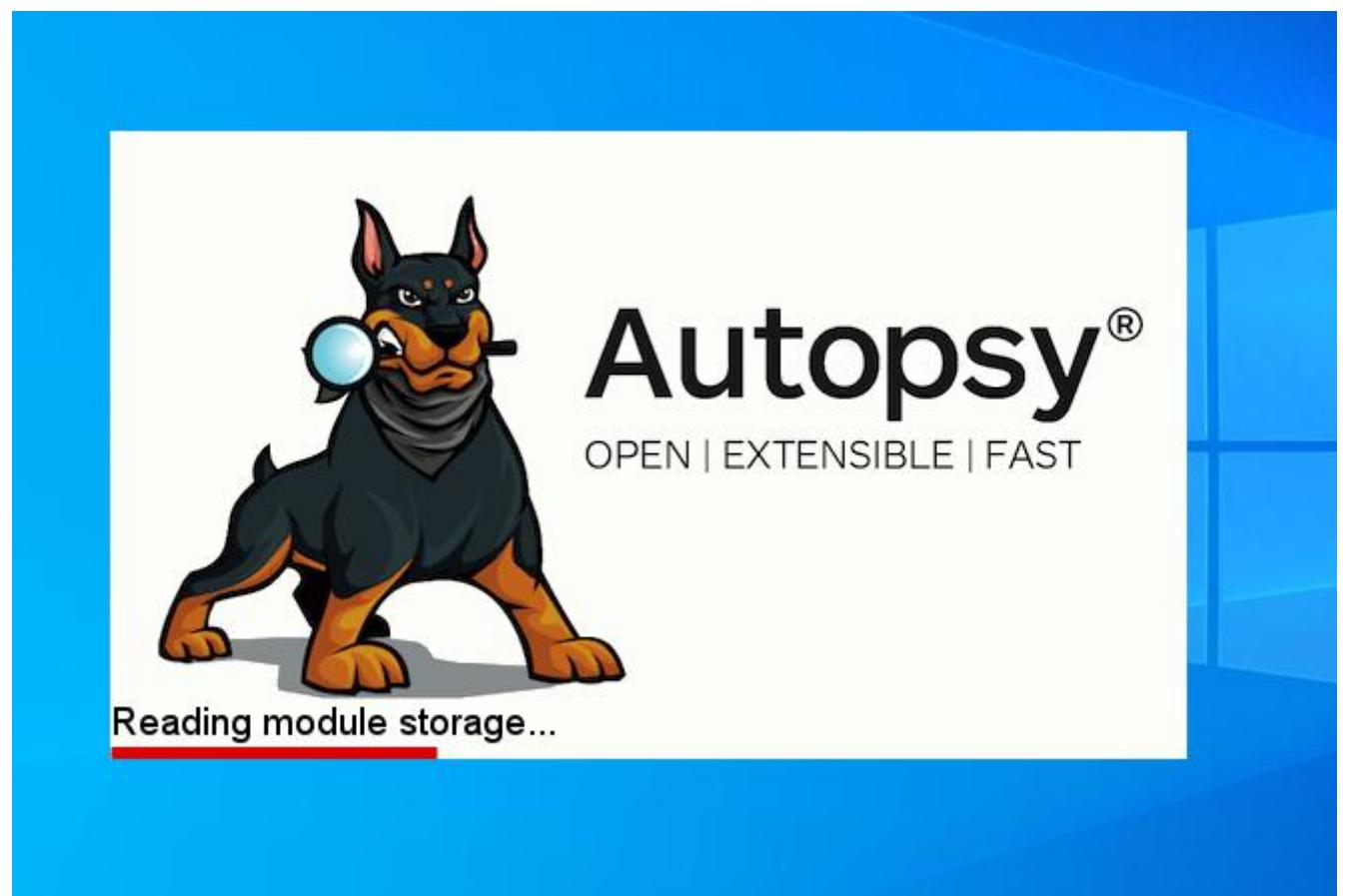
```
(karthikeyan㉿kali)-[~] $ cat .zsh_history | xclip  
  
(karthikeyan㉿kali)-[~] $ xclip -o  
metasploit  
ls  
/usr ★ Starred  
/usr/share/nmap/scripts  
ls  
sudo nano My_scan.nse  
ls  
cd ..  
ping 192.168.133.13\  
  
/usr/share/nmap/scripts  
nano My_scan.nse\  
sudo nano My_scan.nse\  
sudo rm My_scan.nse\  
sudo rm My_scan.nse\  
sudo nano My_scan.nse\  
  
sudo mv My_scan.nse /usr/share/nmap/scripts/\  
  
openfiles.txt
```

6. Analyzing Non-Volatile Data in a Linux System

To begin analyzing non-volatile data on a Linux system:

1. Open **Autopsy**, a digital forensics tool.
2. Create a **new case** by selecting the appropriate option.
3. Provide the required details for the case, such as the case name, description, and investigator information.

Once the case is set up, you can begin analysing non-volatile data from the Linux system, such as file systems, logs, and other stored data.



nsics

New Case Information

Steps

1. Case Information
2. Optional Information

Case Information

Case Name:

Base Directory:

Case Type: Single-User Multi-User

Case data will be stored in the following directory:

New Case Information

Steps

1. Case Information
2. Optional Information

Optional Information

Case

Number:

Examiner

Name:

Phone:

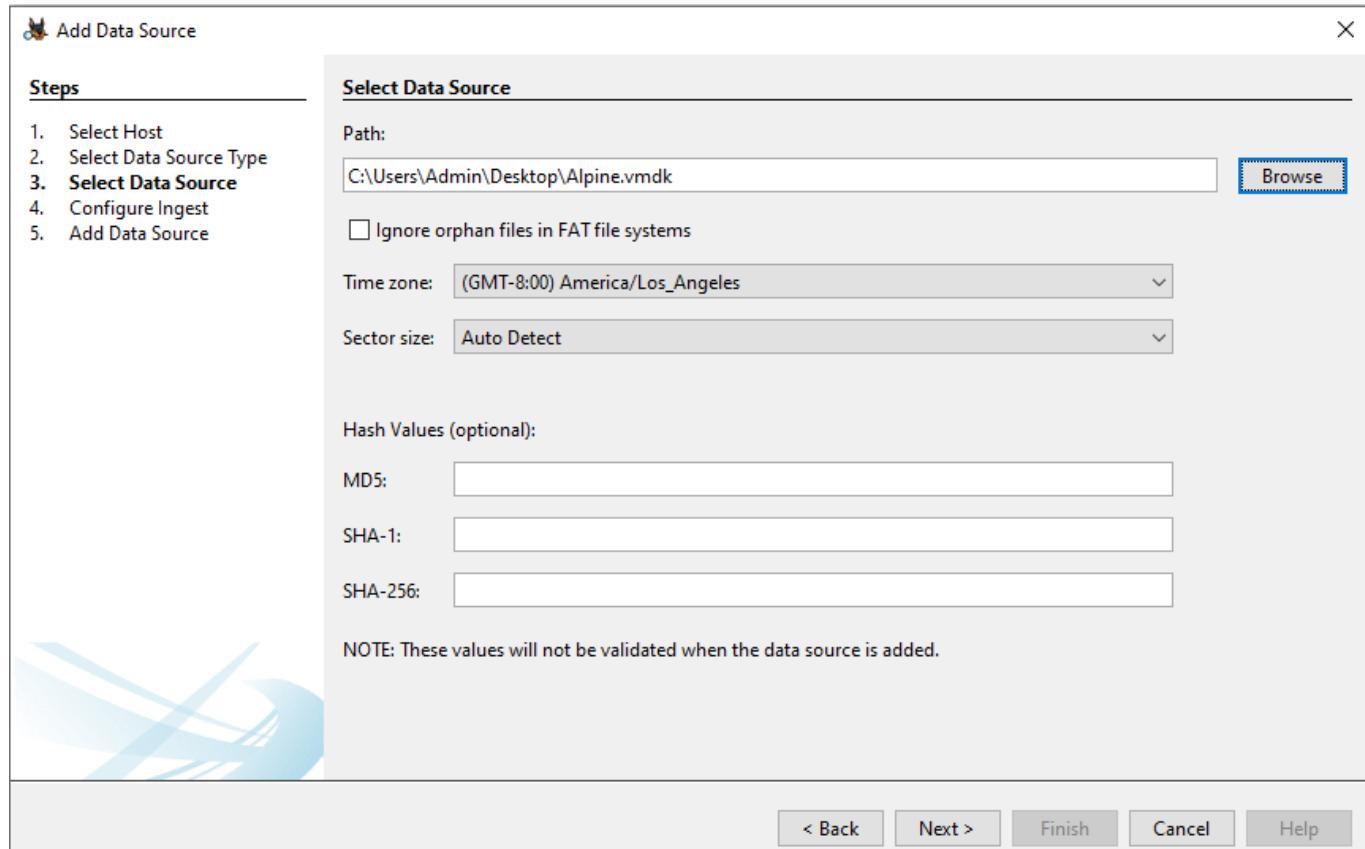
Email:

Notes:

Organization

Organization analysis is being done for:

After creating the case select add data source to mount the evidence image. Select the vmdk file



The tool will display the results after analysis. Expand the Data Sources. Click the image name, here

Table Thumbnail Summary Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time
\$OrphanFiles				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
\$Unalloc				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
[current folder]				2025-01-26 04:17:46 PST	2025-01-26 04:17:46 PST	2025-01-26 04:17:59 PST
[parent folder]				2025-01-26 04:17:46 PST	2025-01-26 04:17:46 PST	2025-01-26 04:17:59 PST
bin				2025-01-26 04:17:58 PST	2025-01-26 04:17:58 PST	2025-01-26 04:17:45 PST
boot				2025-01-26 04:17:43 PST	2025-01-26 04:17:43 PST	2025-01-26 04:17:43 PST
dev				2025-01-26 04:17:43 PST	2025-01-26 04:17:43 PST	2025-01-26 04:17:43 PST
etc				2025-01-26 04:17:58 PST	2025-01-26 04:17:58 PST	2025-01-26 04:17:43 PST
home				2025-01-26 04:17:43 PST	2025-01-26 04:17:43 PST	2025-01-26 04:17:43 PST
lib				2025-01-26 04:17:51 PST	2025-01-26 04:17:51 PST	2025-01-26 04:17:43 PST
lost+found				2025-01-26 04:17:43 PST	2025-01-26 04:17:43 PST	2025-01-26 04:17:43 PST
media				2025-01-26 04:17:46 PST	2025-01-26 04:17:46 PST	2025-01-26 04:17:46 PST
mnt				2025-01-26 04:17:46 PST	2025-01-26 04:17:46 PST	2025-01-26 04:17:46 PST
opt				2025-01-26 04:17:46 PST	2025-01-26 04:17:46 PST	2025-01-26 04:17:46 PST
proc				2025-01-26 04:17:43 PST	2025-01-26 04:17:43 PST	2025-01-26 04:17:43 PST
root				2025-01-26 04:17:46 PST	2025-01-26 04:17:46 PST	2025-01-26 04:17:46 PST
run				2025-01-26 04:17:46 PST	2025-01-26 04:17:46 PST	2025-01-26 04:17:46 PST
sbin				2025-01-26 04:17:58 PST	2025-01-26 04:17:58 PST	2025-01-26 04:17:45 PST
srv				2025-01-26 04:17:46 PST	2025-01-26 04:17:46 PST	2025-01-26 04:17:46 PST

Data Artifacts Analysis Results Context Annotations Other Occurrences

home folder stores the details of the user home directory

Table Thumbnail Summary Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time
[current folder]				2025-01-26 04:17:43 PST	2025-01-26 04:17:43 PST	2025-01-26 04:17:43 PST
[parent folder]				2025-01-26 04:17:46 PST	2025-01-26 04:17:46 PST	2025-01-26 04:17:59 PST
admin				2025-01-26 04:17:13 PST	2025-01-26 04:17:43 PST	2025-01-26 04:17:13 PST

File views option has the deleted files option to view all the deleted files.

The screenshot shows the 'File Views' section of a software interface. Under 'File Types', 'Deleted Files' is selected, which is highlighted in blue. This selection leads to a table titled 'Deleted Files' with 2 results. The table includes columns for 'Type' and 'Source'. The data shows two entries: 'File System (62)' and 'All (300)'. A 'Save Table as CSV' button is located at the top right of the table area.

Select the results folder . It contains encrypted content.

The screenshot shows the 'File Views' section of a software interface. Under 'Analysis Results', 'Encryption Programs (3)' is selected, which is highlighted in blue. This selection leads to a table titled 'Encryption Programs' with 3 results. The table includes columns for 'Source Name', 'S', 'C', 'O', 'Source Type', 'Score', 'Conclusion', 'Configuration', and 'Justification'. The data shows three entries: 'cryptpts', 'cryptpts.ko.gz', and 'cryptpts.ko', all categorized as 'Likely Notable' and associated with 'Encryption Programs'.

/var/log will have the syslog

The screenshot shows the 'Data Sources' interface. A specific volume, 'Alpine.vmdk_1 Host', is selected. Inside this volume, the 'vol4' partition is mounted. The path '/img_Alpine.vmdk/vol_vol4/var/log' is selected, which is highlighted in blue. This selection leads to a table titled '/img_Alpine.vmdk/vol_vol4/var/log' with 3 results. The table includes columns for 'Name', 'S', 'C', 'O', 'Modified Time', 'Change Time', and 'Access Time'. The data shows three entries: '[current folder]', '[parent folder]', and 'chrony'. All three entries were modified and changed on 2025-01-26 at 04:17:46 PST, and accessed on 2025-01-26 at 04:17:46 PST.

/lib folder contains library files that are used by the system to run commands and boot the system

The screenshot shows a forensic analysis interface with two main panes. The left pane, titled 'Data Sources', displays a hierarchical file tree for 'Alpine.vmdk_1 Host' and 'Alpine.vmdk'. The 'Alpine.vmdk' tree includes volumes 'vol1', 'vol2', 'vol3', and 'vol4'. 'vol4' is expanded to show sub-directories like '\$OrphanFiles', '\$CarvedFiles', '\$Unalloc', 'bin', 'boot', 'dev', 'etc', 'home', 'lib', and 'apk'. The 'lib' directory is selected and highlighted in blue. The right pane shows a table titled '/img_Alpine.vmdk/vol_vol4/lib' with 10 results. The table has columns: Name, S, C, O, Modified Time, Change Time, and Access Time. The data is as follows:

Name	S	C	O	Modified Time	Change Time	Access Time
libc.musl-x86_64.so.1		2		2025-01-26 04:17:45 PST	2025-01-26 04:17:45 PST	2025-01-26 04:17:5
[current folder]				2025-01-26 04:17:51 PST	2025-01-26 04:17:51 PST	2025-01-26 04:17:4
[parent folder]				2025-01-26 04:17:46 PST	2025-01-26 04:17:46 PST	2025-01-26 04:17:5
apk				2025-01-26 04:17:45 PST	2025-01-26 04:17:45 PST	2025-01-26 04:17:4
firmware				2025-01-26 04:17:46 PST	2025-01-26 04:17:46 PST	2025-01-26 04:17:4
mdev				2025-01-26 04:17:46 PST	2025-01-26 04:17:46 PST	2025-01-26 04:17:5
modules				2025-01-26 04:17:51 PST	2025-01-26 04:17:51 PST	2025-01-26 04:17:5
modules-load.d				2025-01-26 04:17:46 PST	2025-01-26 04:17:46 PST	2025-01-26 04:17:4
sysctl.d				2025-01-26 04:17:46 PST	2025-01-26 04:17:46 PST	2025-01-26 04:17:4
ld-musl-x86_64.so.1	0			2024-12-03 08:17:55 PST	2025-01-26 04:17:45 PST	2025-01-26 04:17:4