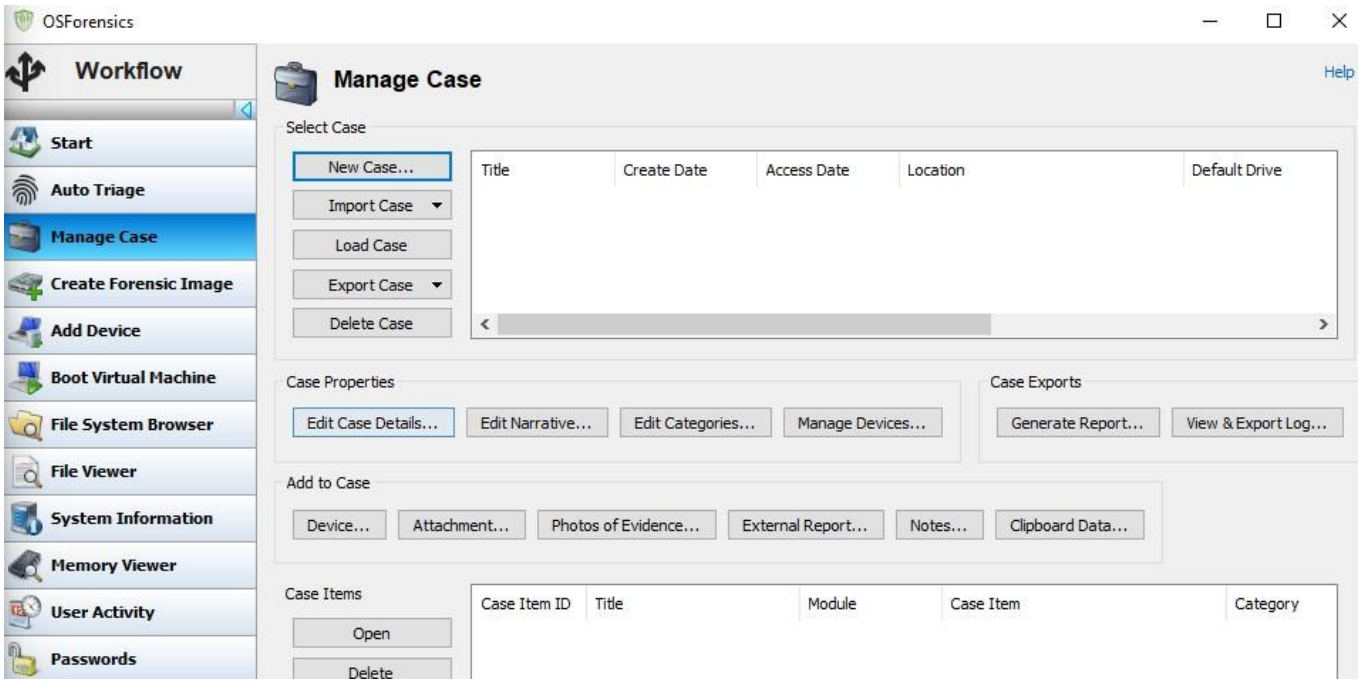
Cyber Forensics - 24CY611
Lab 5 - Operating System Forensics

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

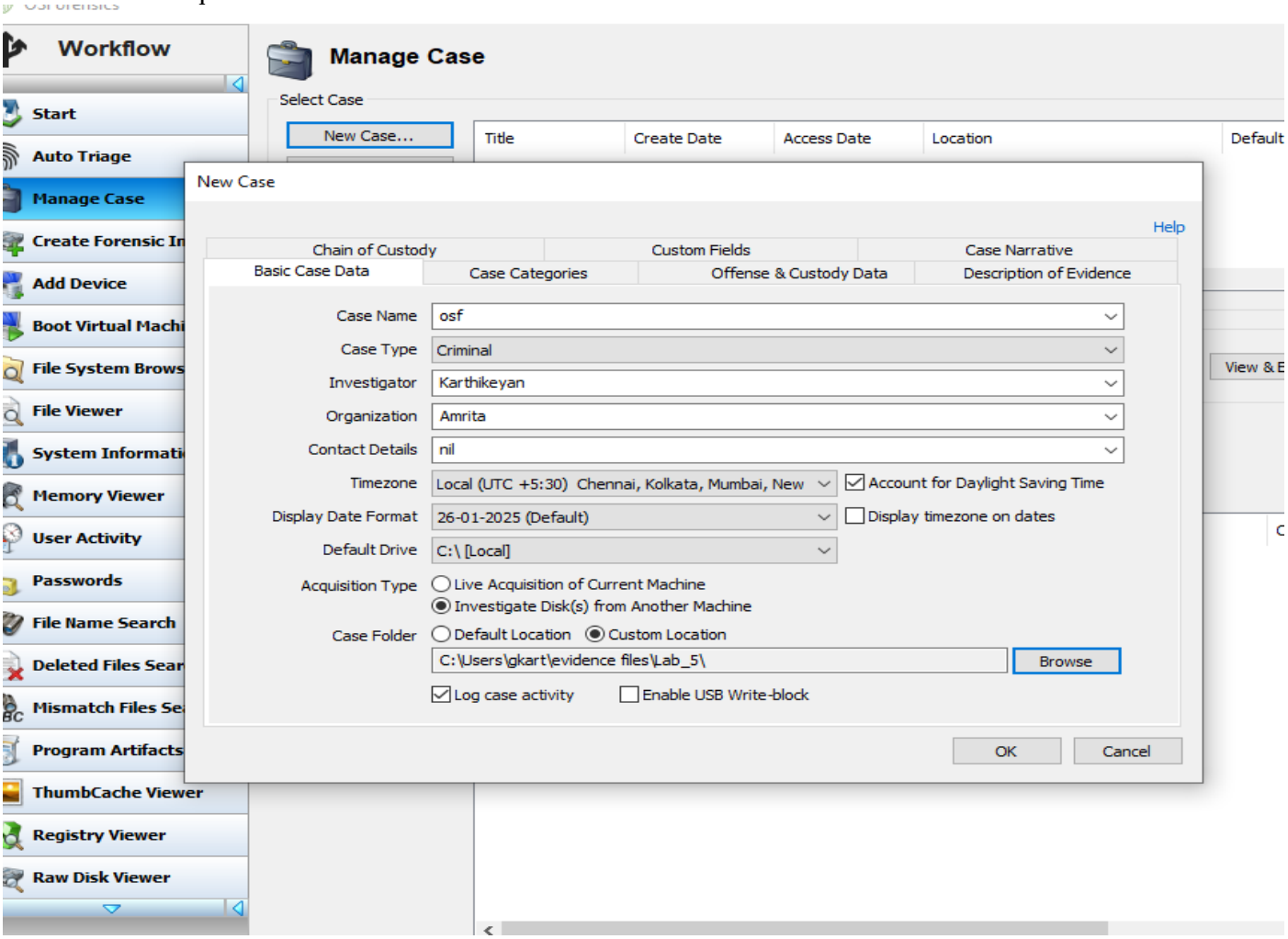
Forensics is a forensic investigation tool used to extract, analyze, and manage digital evidence from computers, including file recovery, email analysis, and disk imaging. It provides advanced search capabilities and tools for verifying data integrity, aiding in cybercrime investigations.

Steps:

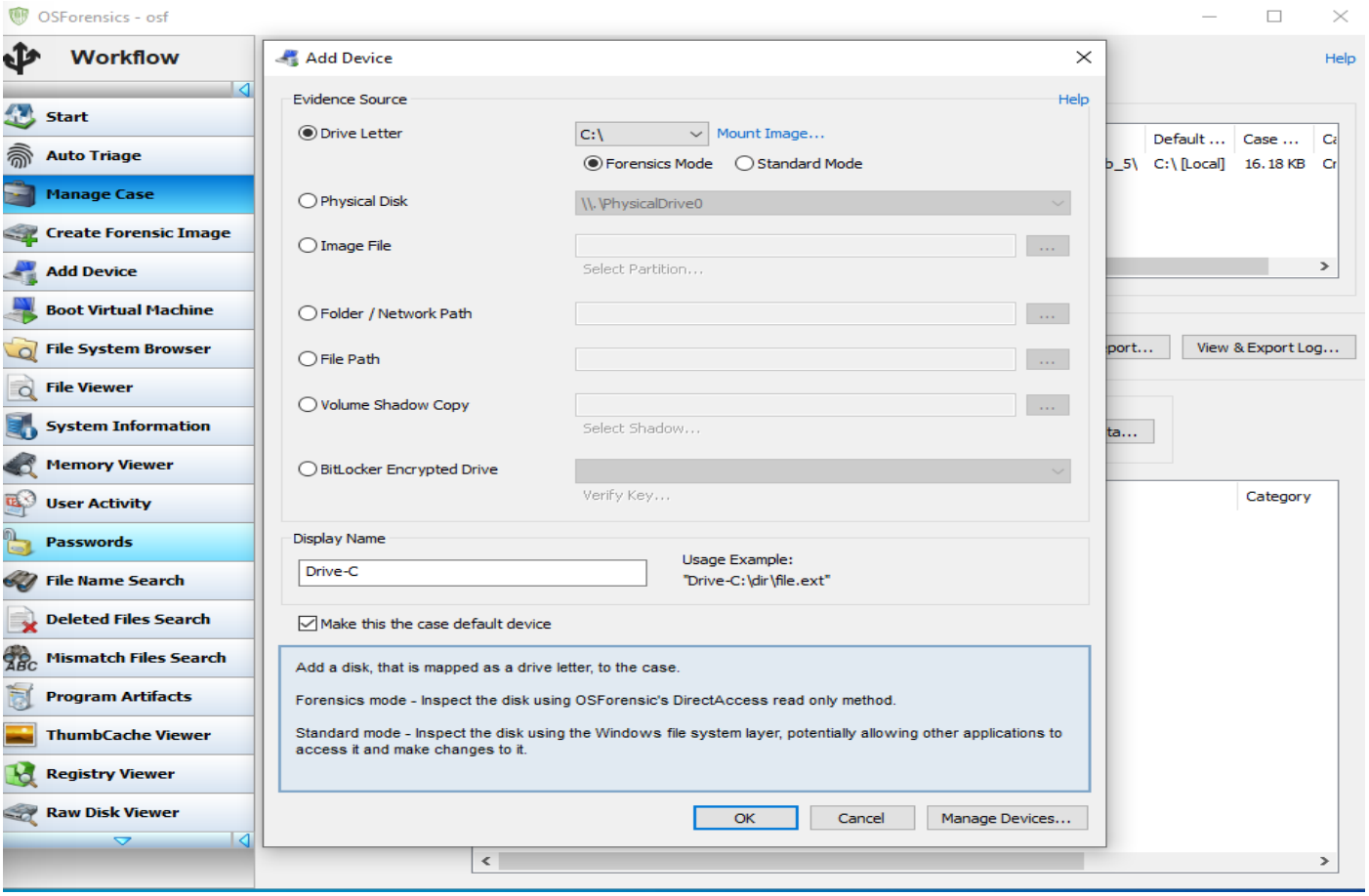
Open Forensics osftool and create a new case.



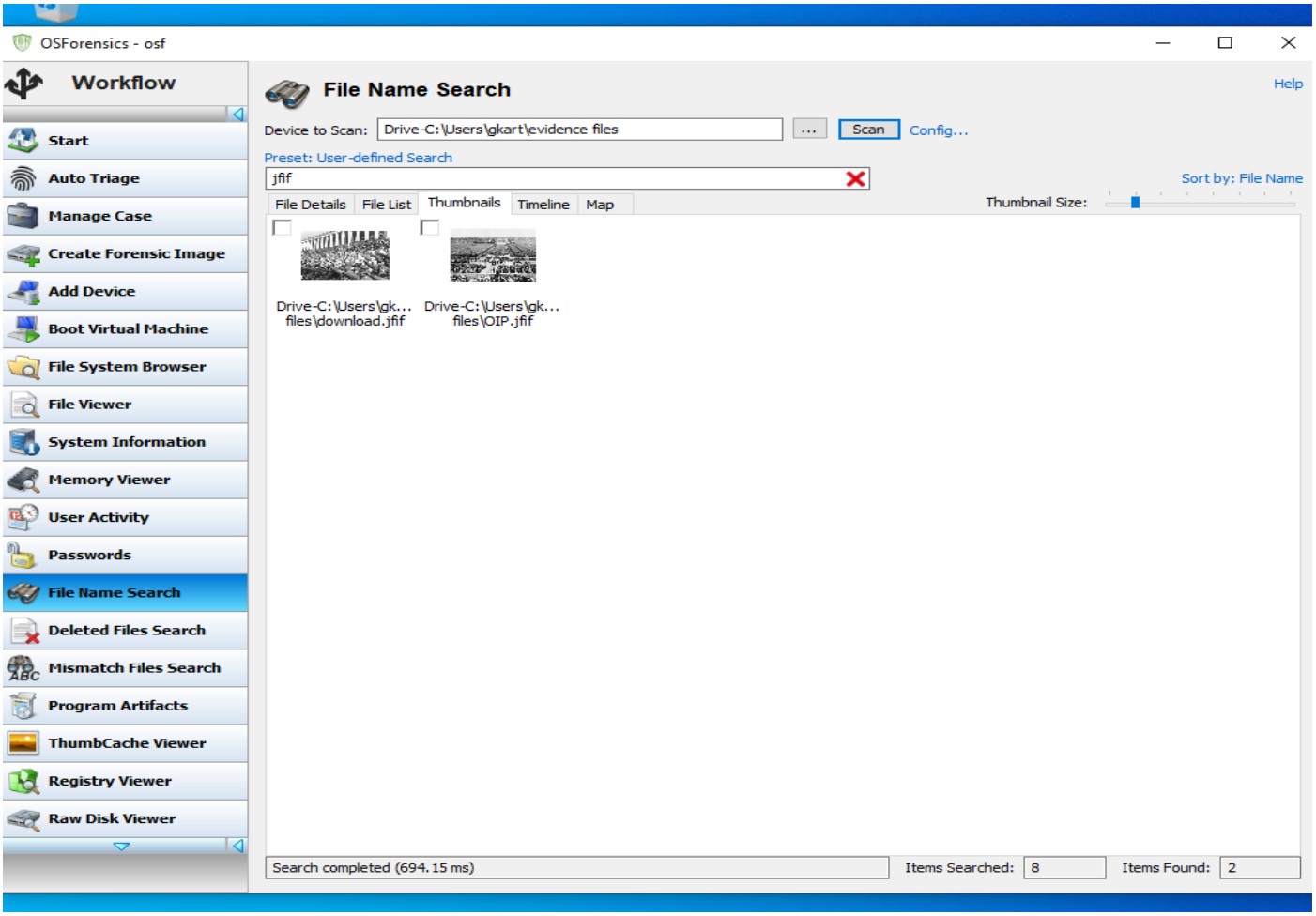
Then fill the required fields for the new case and click ok



After creating the case, add the device for evidence source

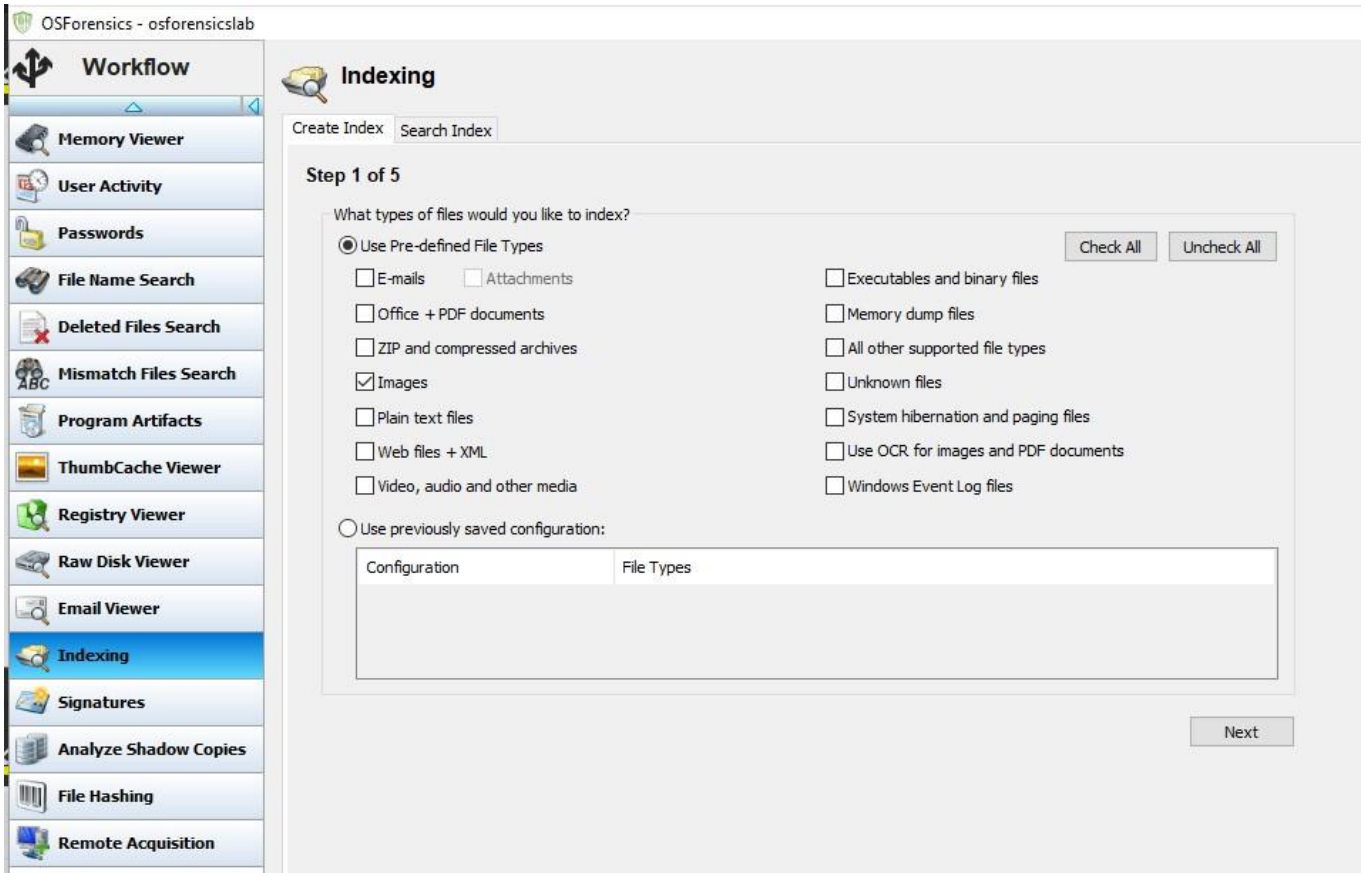


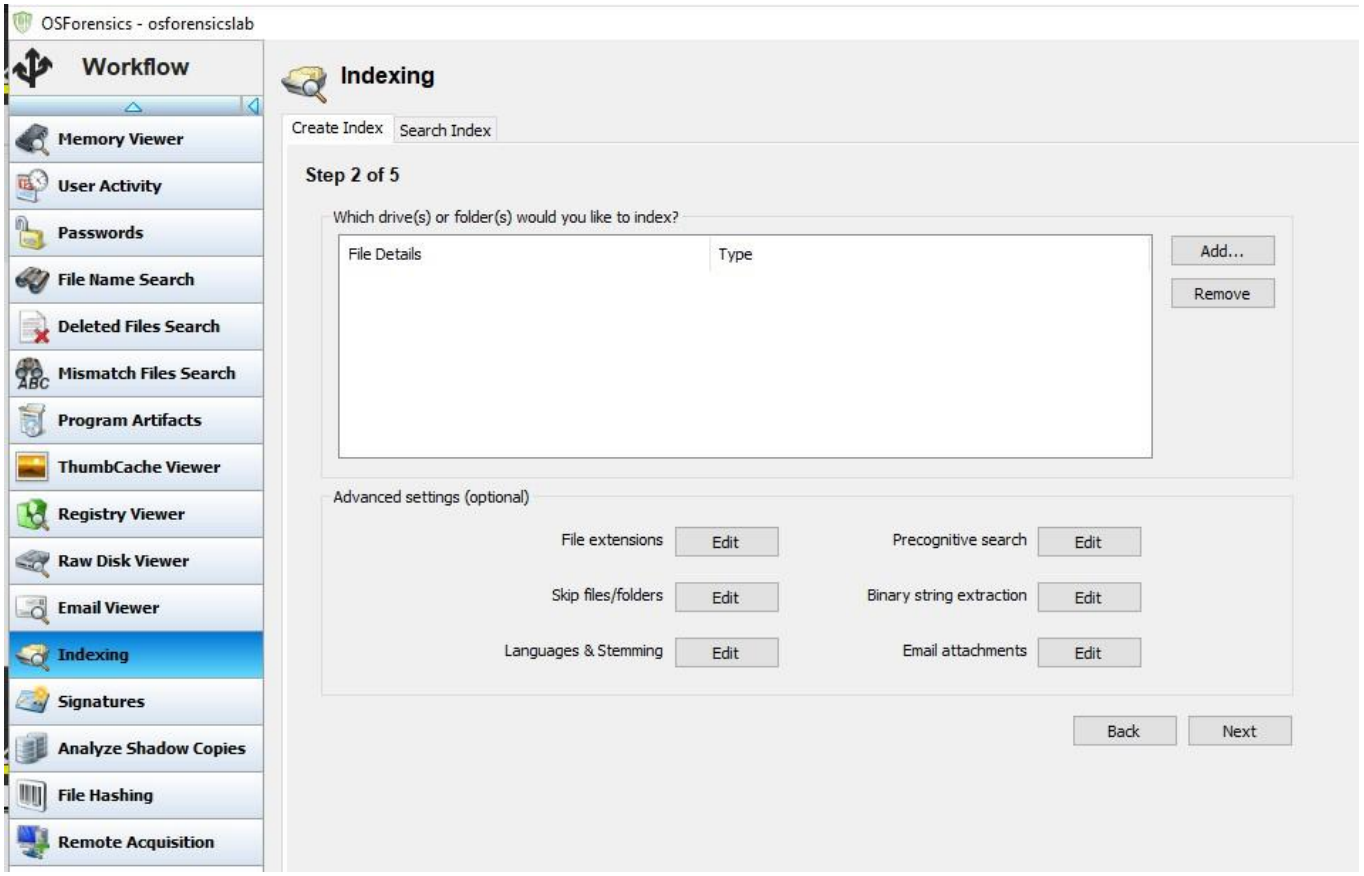
In the file name search option, select the device to scan and set the presets to images and start the scan.

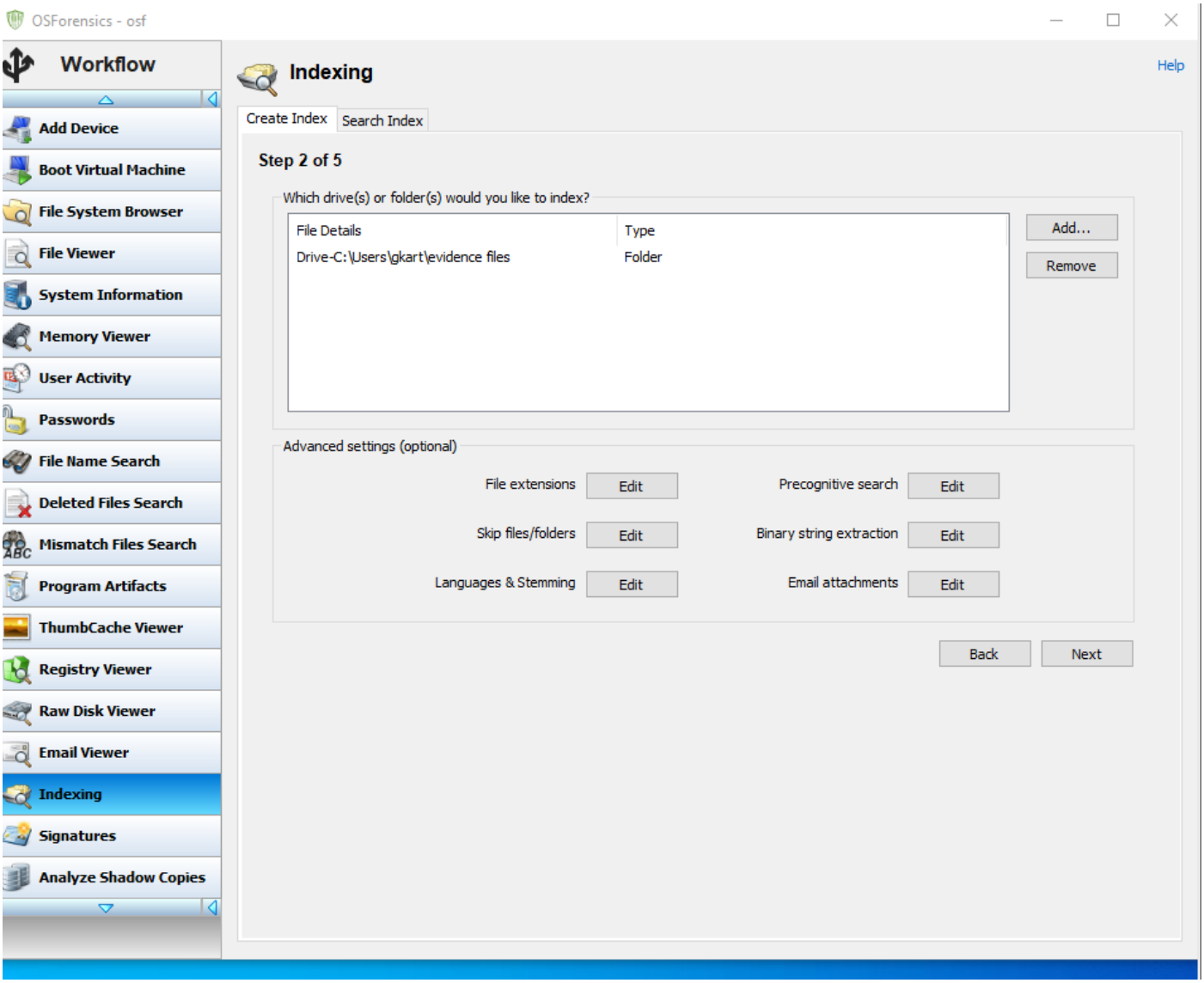


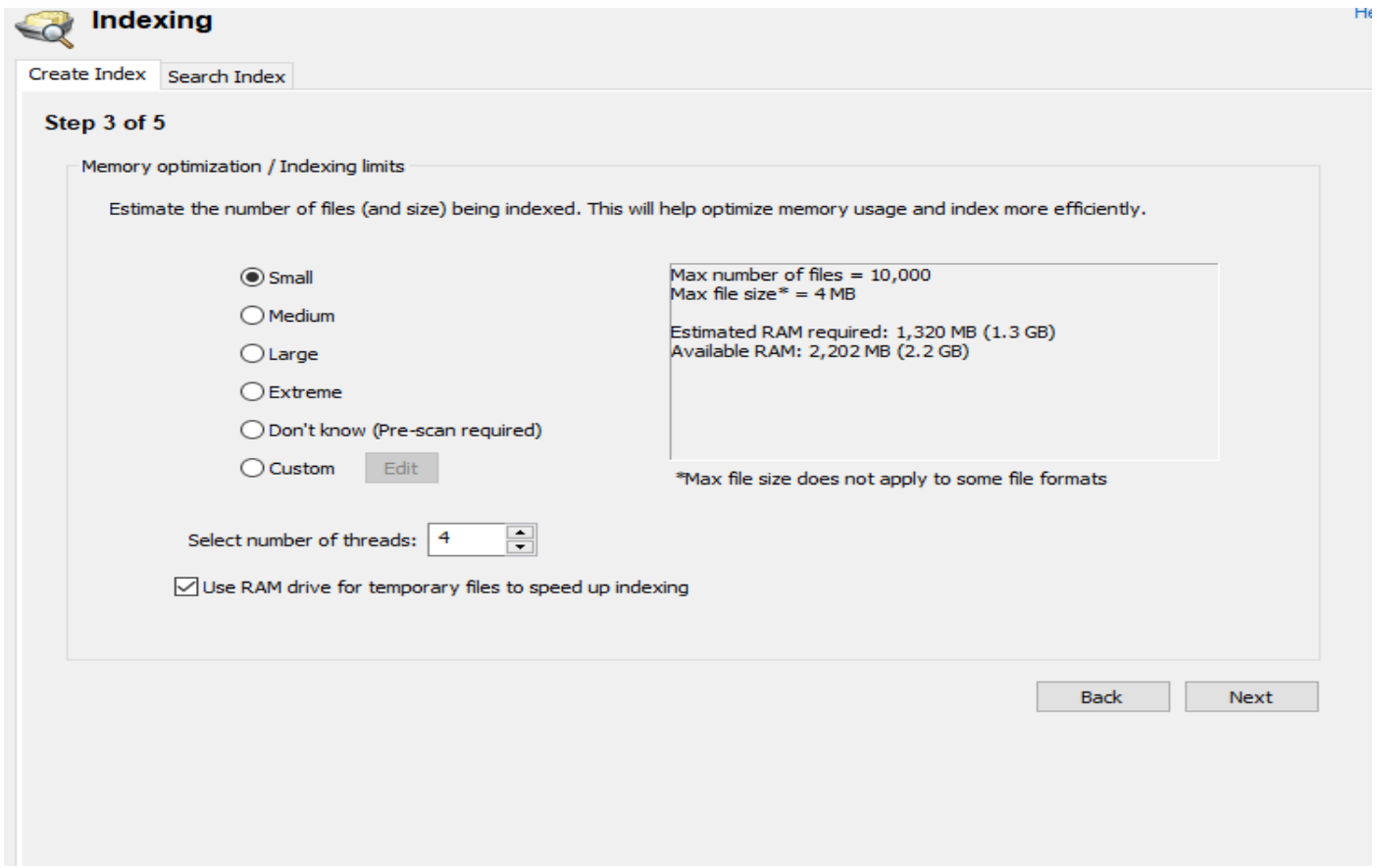
The tool now displays a thumbnail of the screenshot saved in the Pictures directory, which I used as evidence, and generates an index. Creating an index involves five steps:

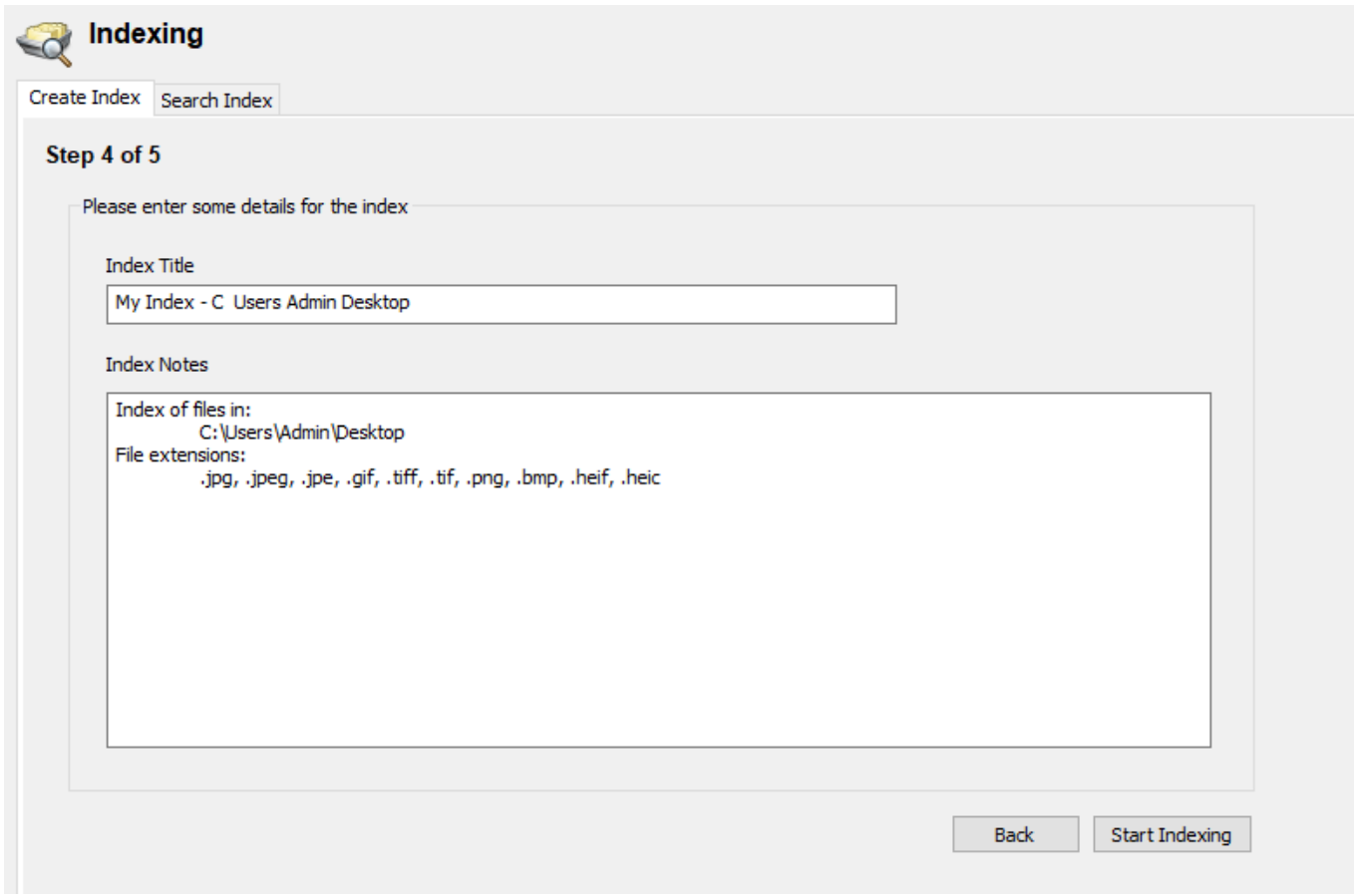
1. Select the desired file types for indexing using predefined options.
2. Add the specific drive or directory to be included in the index.
3. Assign an index title, include notes, and make use of memory optimization features provided in the latest version.
4. Allow the application to scan the selected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

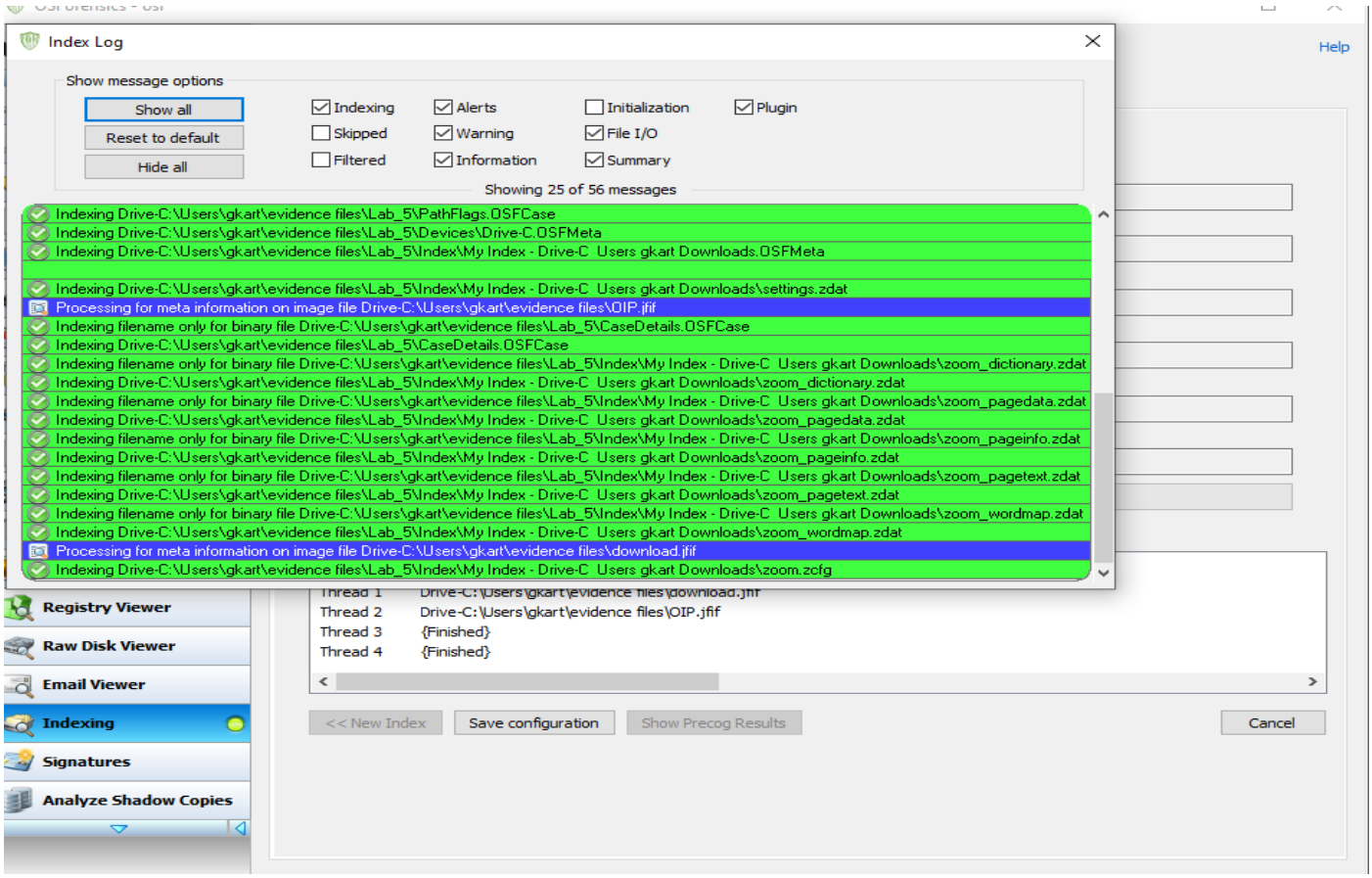

OSForensics - osforensicslab
Workflow
Memory Viewer
User Activity
Passwords
File Name Search
Deleted Files Search
Mismatch Files Search
Program Artifacts
ThumbCache Viewer
Registry Viewer
Raw Disk Viewer
Email Viewer
Indexing
Signatures
Analyze Shadow Copies
File Hashing
Remote Acquisition
Indexing
Create Index
Search Index
Step 1 of 5
What types of files would you like to index?
Use Pre-defined File Types
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

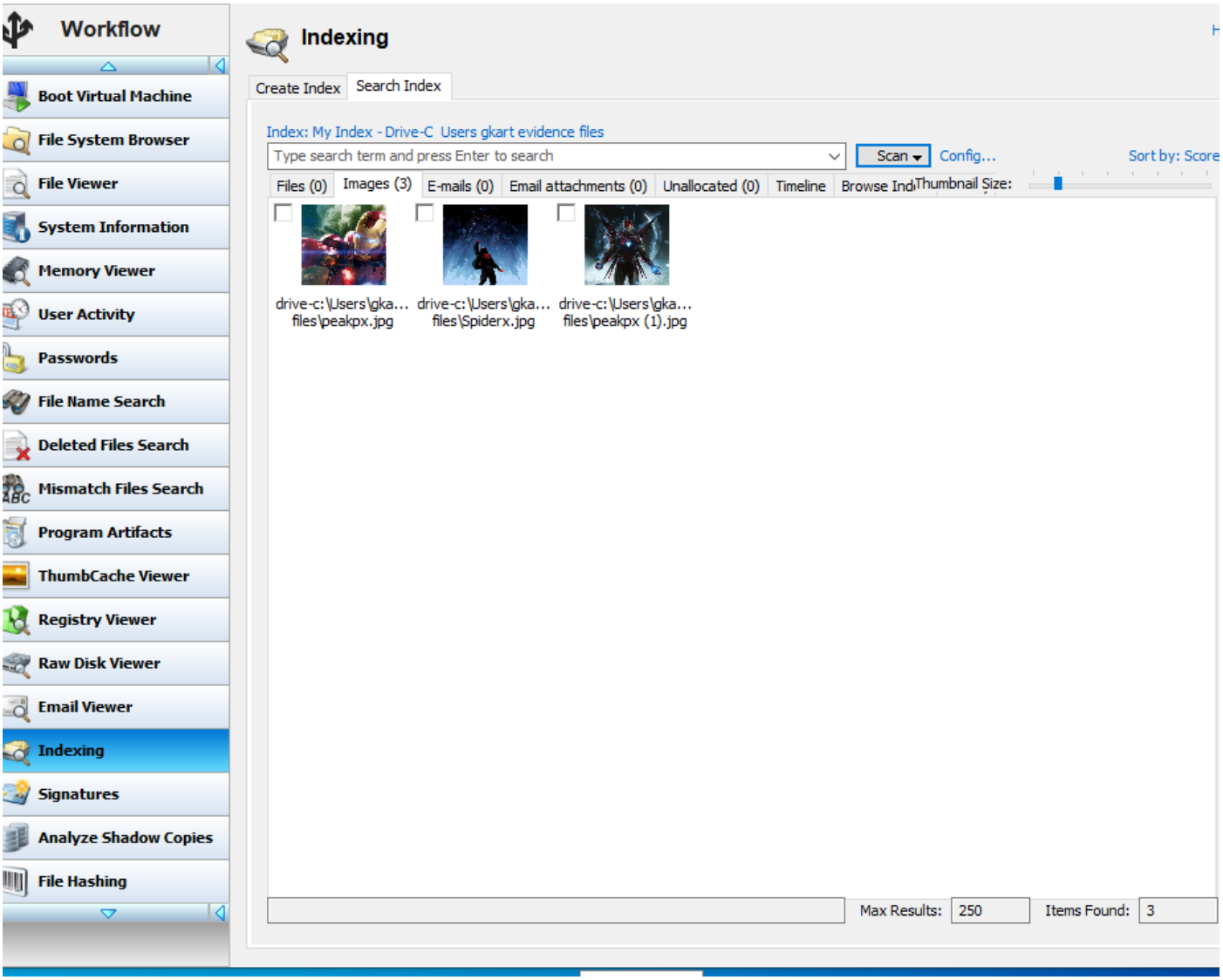

OSForensics - osforensicslab
Workflow
Memory Viewer
User Activity
Passwords
File Name Search
Deleted Files Search
Mismatch Files Search
Program Artifacts
ThumbCache Viewer
Registry Viewer
Raw Disk Viewer
Email Viewer
Indexing
Signatures
Analyze Shadow Copies
File Hashing
Remote Acquisition
Indexing
Create 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


OSForensics - osf
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
Indexing
Help
Create Index
Search Index
Step 2 of 5
Which drive(s) or folder(s) would you like to index?
File Details
Type
Drive-C:\Users\gkart\evidence files
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

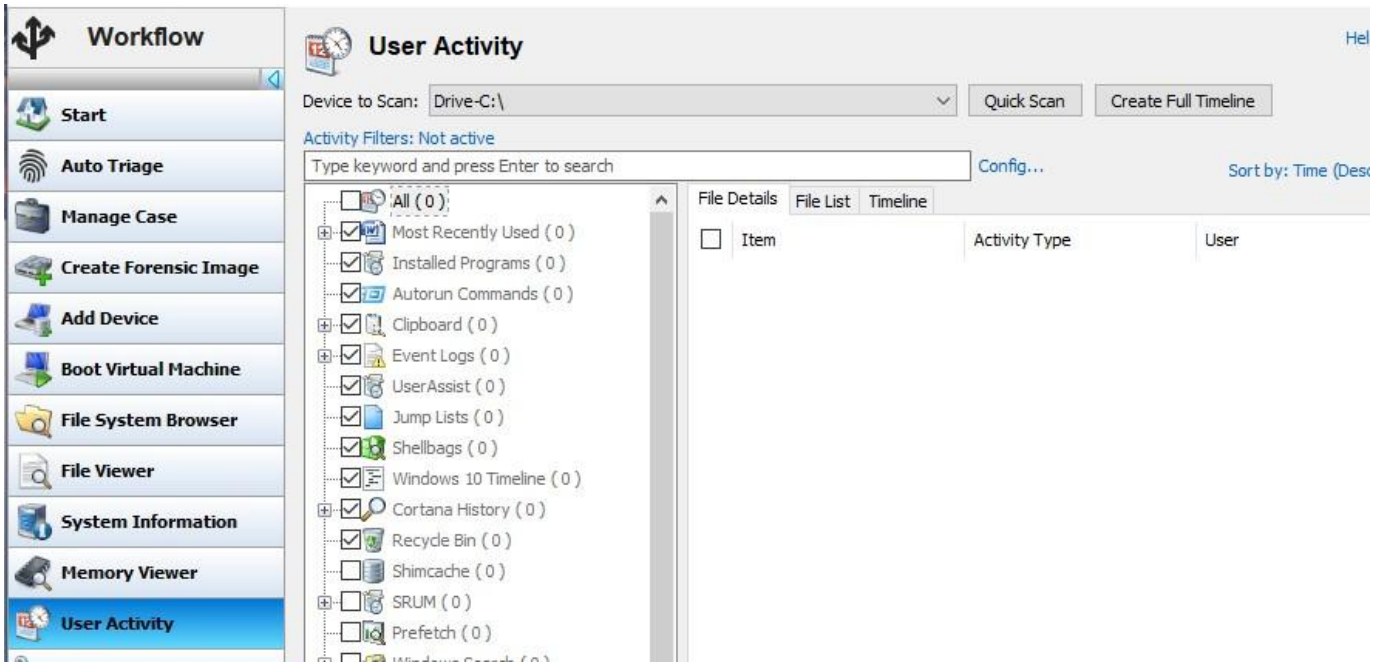

Indexing
Create Index
Search Index
Step 3 of 5
Memory optimization / Indexing limits
Estimate the number of files (and size) being indexed. This will help optimize memory usage and index more efficiently.
Small
Medium
Large
Extreme
Don't know (Pre-scan required)
Custom
Edit
Max number of files = 10,000
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: 4
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
My Index - C Users Admin Desktop
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

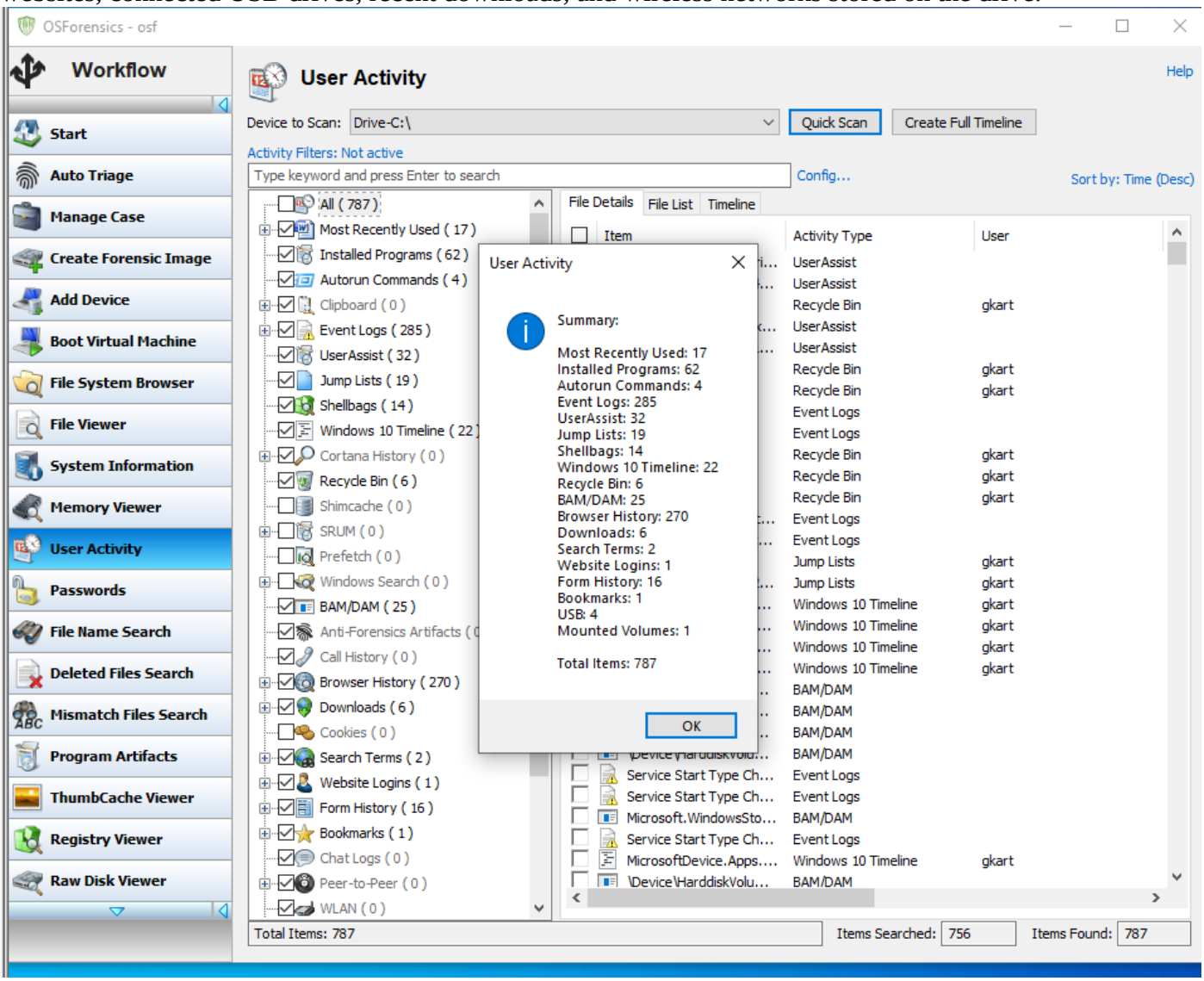

Index Log
Show message options
Show all
Reset to default
Hide all
Indexing
Alerts
Initialization
Plugin
Skipped
Warning
File I/O
Filtered
Information
Summary
Showing 25 of 56 messages
Indexing Drive-C:\Users\gkart\evidence files\Lab_5\PathFlags.OSFCase
Indexing Drive-C:\Users\gkart\evidence files\Lab_5\Devices\Drive-C.OSFMeta
Indexing Drive-C:\Users\gkart\evidence files\Lab_5\Index\My Index - Drive-C_Users gkart Downloads.OSFMeta
Indexing Drive-C:\Users\gkart\evidence files\Lab_5\Index\My Index - Drive-C_Users gkart Downloads\settings.zdat
Processing for meta information on image file Drive-C:\Users\gkart\evidence files\OIP.jfif
Indexing filename only for binary file Drive-C:\Users\gkart\evidence files\Lab_5\CaseDetails.OSFCase
Indexing Drive-C:\Users\gkart\evidence files\Lab_5\CaseDetails.OSFCase
Indexing filename only for binary file Drive-C:\Users\gkart\evidence files\Lab_5\Index\My Index - Drive-C_Users gkart Downloads\zoom_dictionary.zdat
Indexing Drive-C:\Users\gkart\evidence files\Lab_5\Index\My Index - Drive-C_Users gkart Downloads\zoom_dictionary.zdat
Indexing filename only for binary file Drive-C:\Users\gkart\evidence files\Lab_5\Index\My Index - Drive-C_Users gkart Downloads\zoom_pagedata.zdat
Indexing Drive-C:\Users\gkart\evidence files\Lab_5\Index\My Index - Drive-C_Users gkart Downloads\zoom_pagedata.zdat
Indexing filename only for binary file Drive-C:\Users\gkart\evidence files\Lab_5\Index\My Index - Drive-C_Users gkart Downloads\zoom_pageinfo.zdat
Indexing Drive-C:\Users\gkart\evidence files\Lab_5\Index\My Index - Drive-C_Users gkart Downloads\zoom_pageinfo.zdat
Indexing filename only for binary file Drive-C:\Users\gkart\evidence files\Lab_5\Index\My Index - Drive-C_Users gkart Downloads\zoom_pagetext.zdat
Indexing Drive-C:\Users\gkart\evidence files\Lab_5\Index\My Index - Drive-C_Users gkart Downloads\zoom_pagetext.zdat
Indexing filename only for binary file Drive-C:\Users\gkart\evidence files\Lab_5\Index\My Index - Drive-C_Users gkart Downloads\zoom_wordmap.zdat
Indexing Drive-C:\Users\gkart\evidence files\Lab_5\Index\My Index - Drive-C_Users gkart Downloads\zoom_wordmap.zdat
Processing for meta information on image file Drive-C:\Users\gkart\evidence files\download.jfif
Indexing Drive-C:\Users\gkart\evidence files\Lab_5\Index\My Index - Drive-C_Users gkart Downloads\zoom.zcfg
Help
Registry Viewer
Raw Disk Viewer
Email Viewer
Indexing
Signatures
Analyze Shadow Copies
Thread 2 Drive-C:\Users\gkart\evidence files\OIP.jfif
Thread 3 {Finished}
Thread 4 {Finished}
<< New Index
Save configuration
Show Precog Results
Cancel



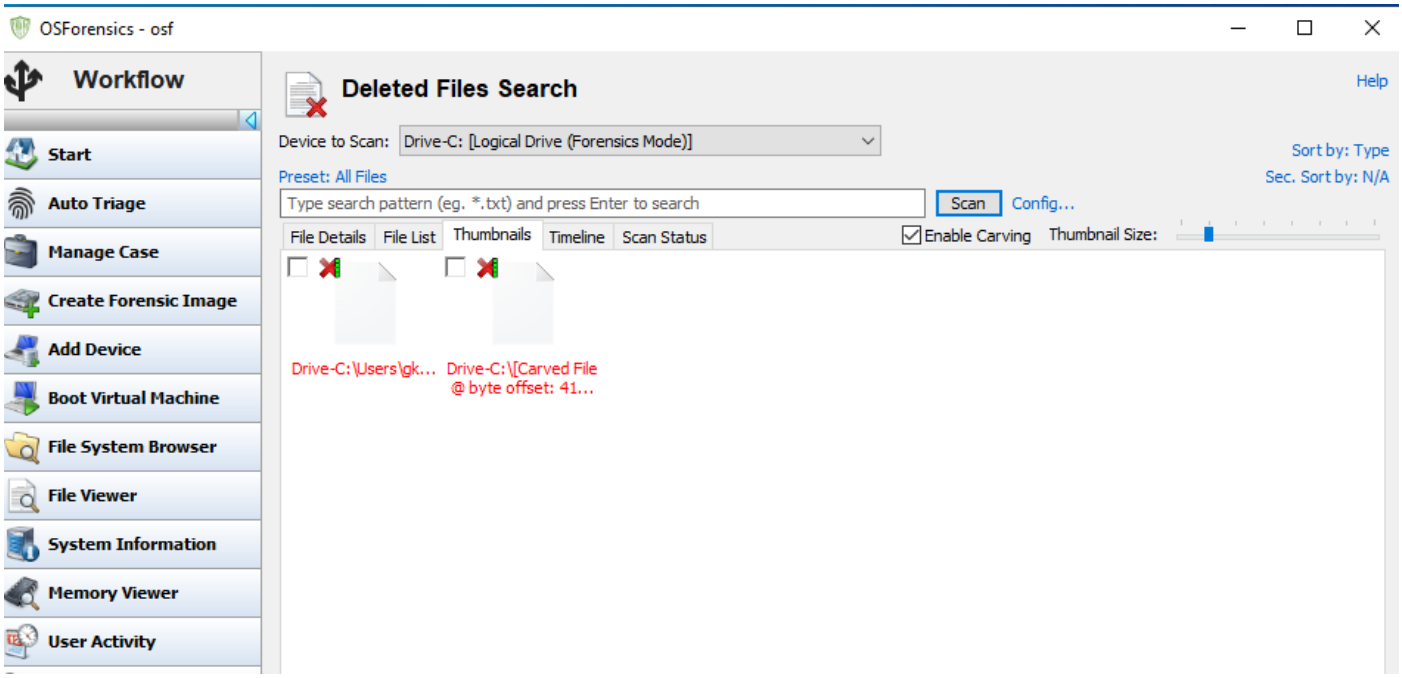
Next, select the **Recent Activity** option to scan the drive and display recent actions related to the evidence. In the latest version, this option has been renamed **User Activity**. Choose the preferred scan type to perform a detailed analysis.



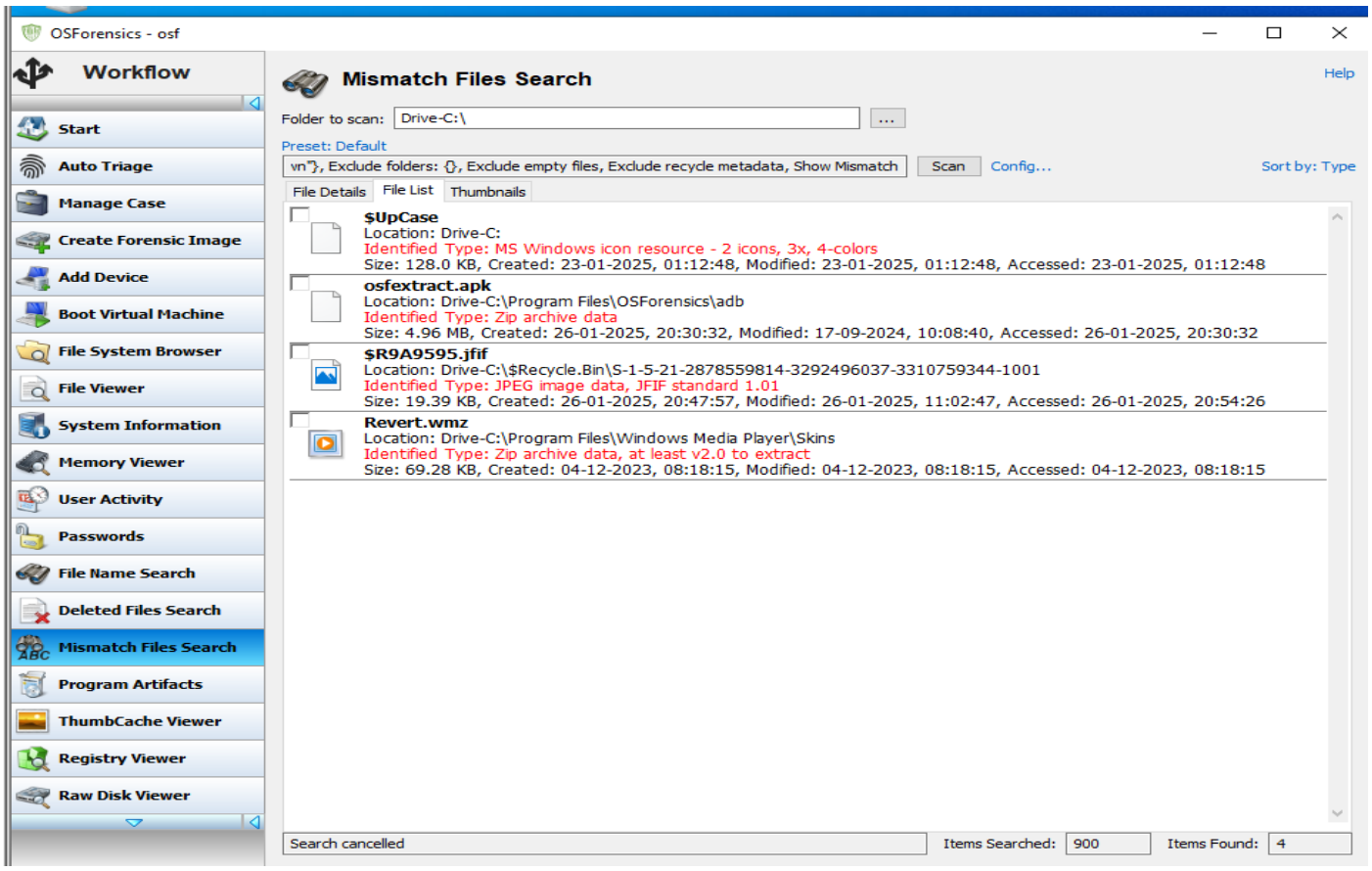
Choose the device to scan, select the **C:** drive, and click **Scan** to search for evidence such as visited websites, connected USB drives, recent downloads, and wireless networks stored on the drive.



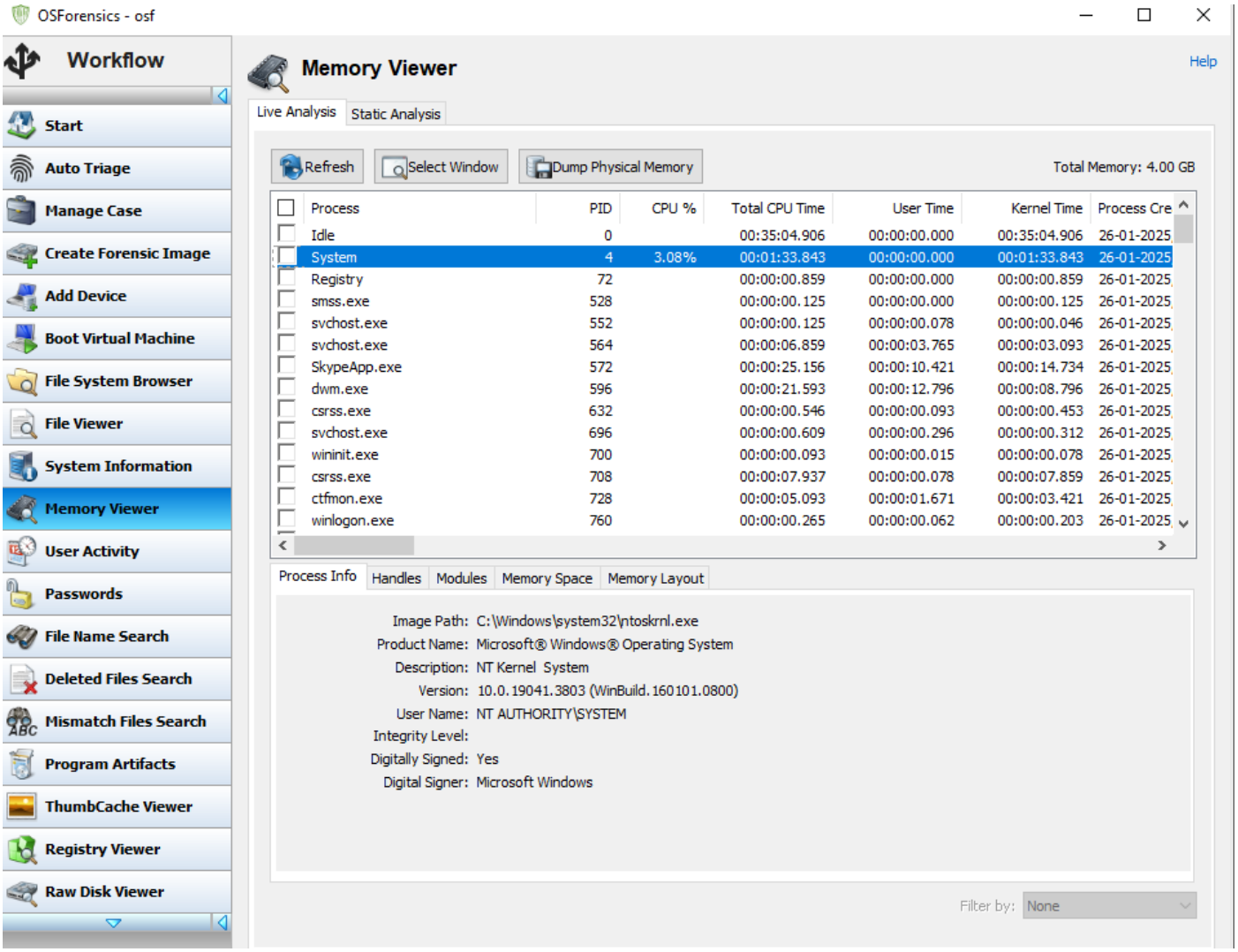
To recover deleted files, navigate to the **Deleted Files Search** option and select the desired partition.



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.

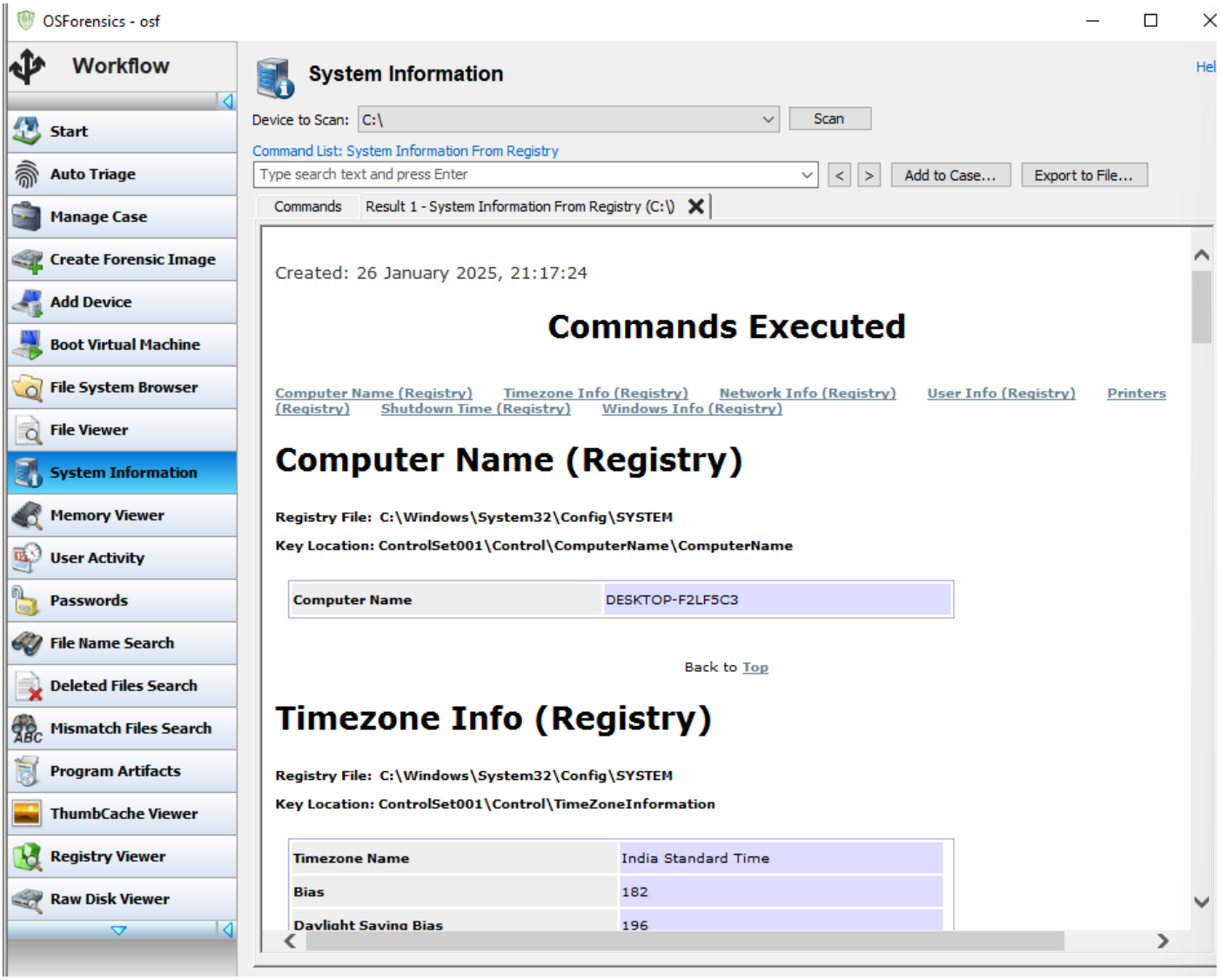


The **Memory Viewer** shows the system's memory usage and provides a detailed list of active processes, allowing for in-depth analysis.

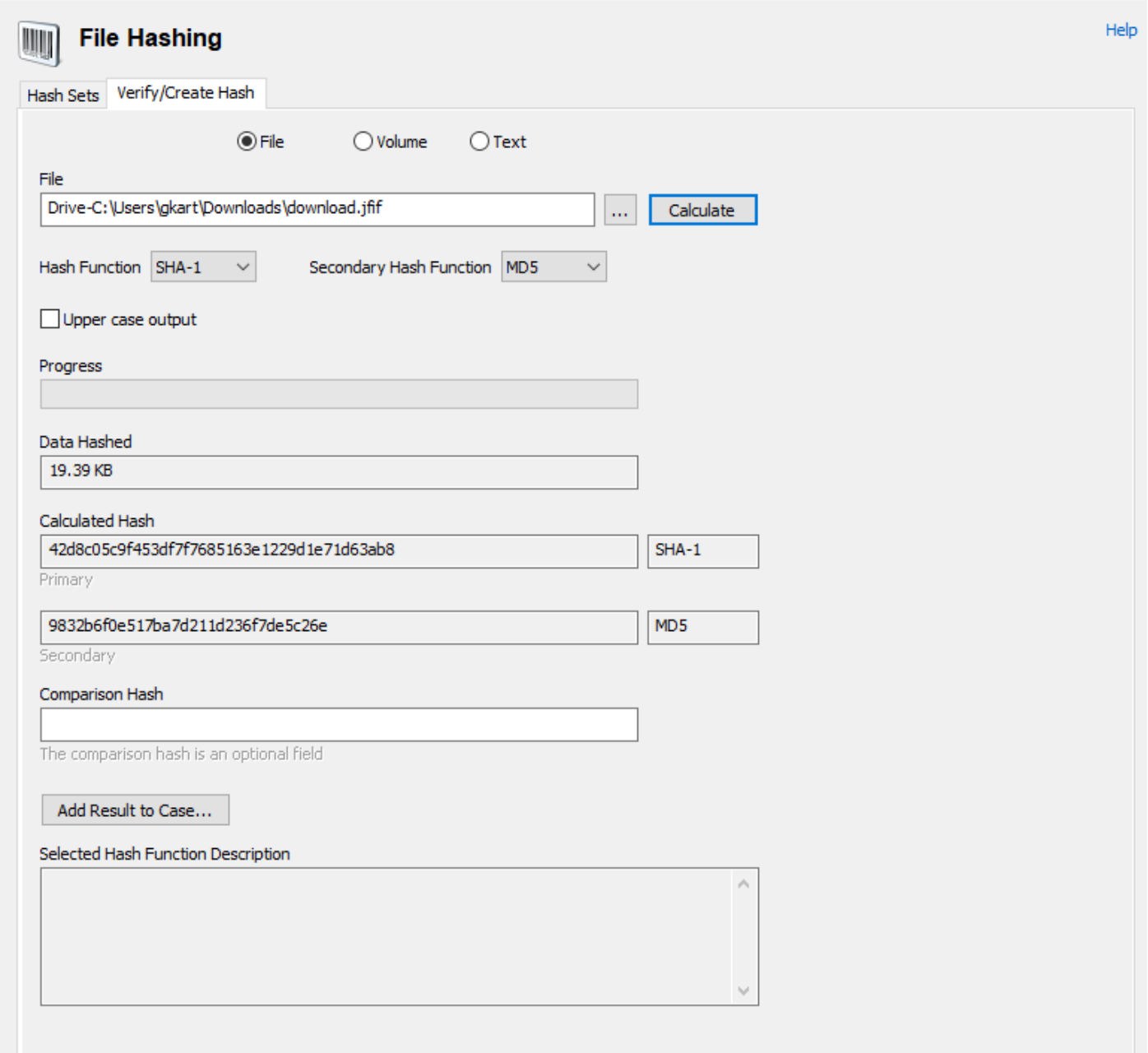


The **Raw Disk Viewer** provides direct access to view raw data on a disk at the sector level, enabling thorough analysis of disk structures and uncovering hidden information.

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.

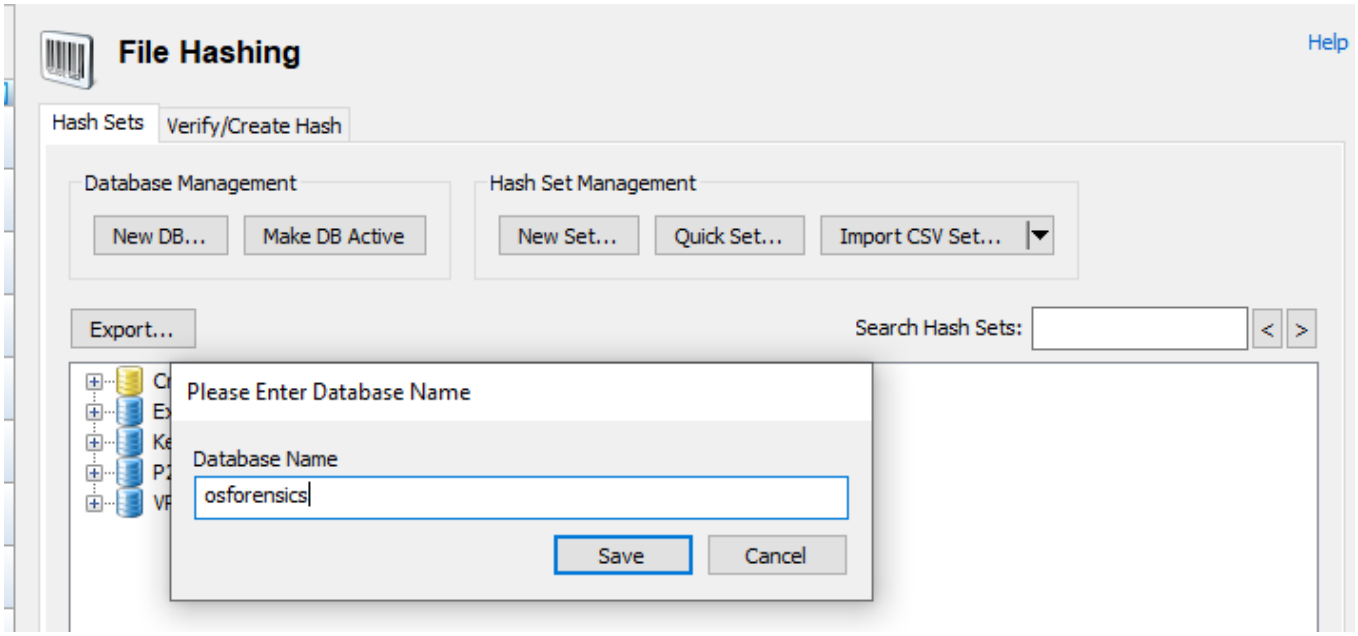

OSForensics - osf
Workflow
Start
Auto Triage
Manage Case
Create Forensic Image
Add Device
Boot Virtual Machine
File System Browser
File Viewer
System Information
Memory Viewer
User Activity
Passwords
File Name Search
Deleted Files Search
Mismatch Files Search
Program Artifacts
ThumbCache Viewer
Registry Viewer
Raw Disk Viewer
System Information
Device to Scan: C:\
Scan
Command List: System Information From Registry
Type search text and press Enter
Add to Case...
Export to File...
Commands
Result 1 - System Information From Registry (C:\)
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 Saving Bias
196

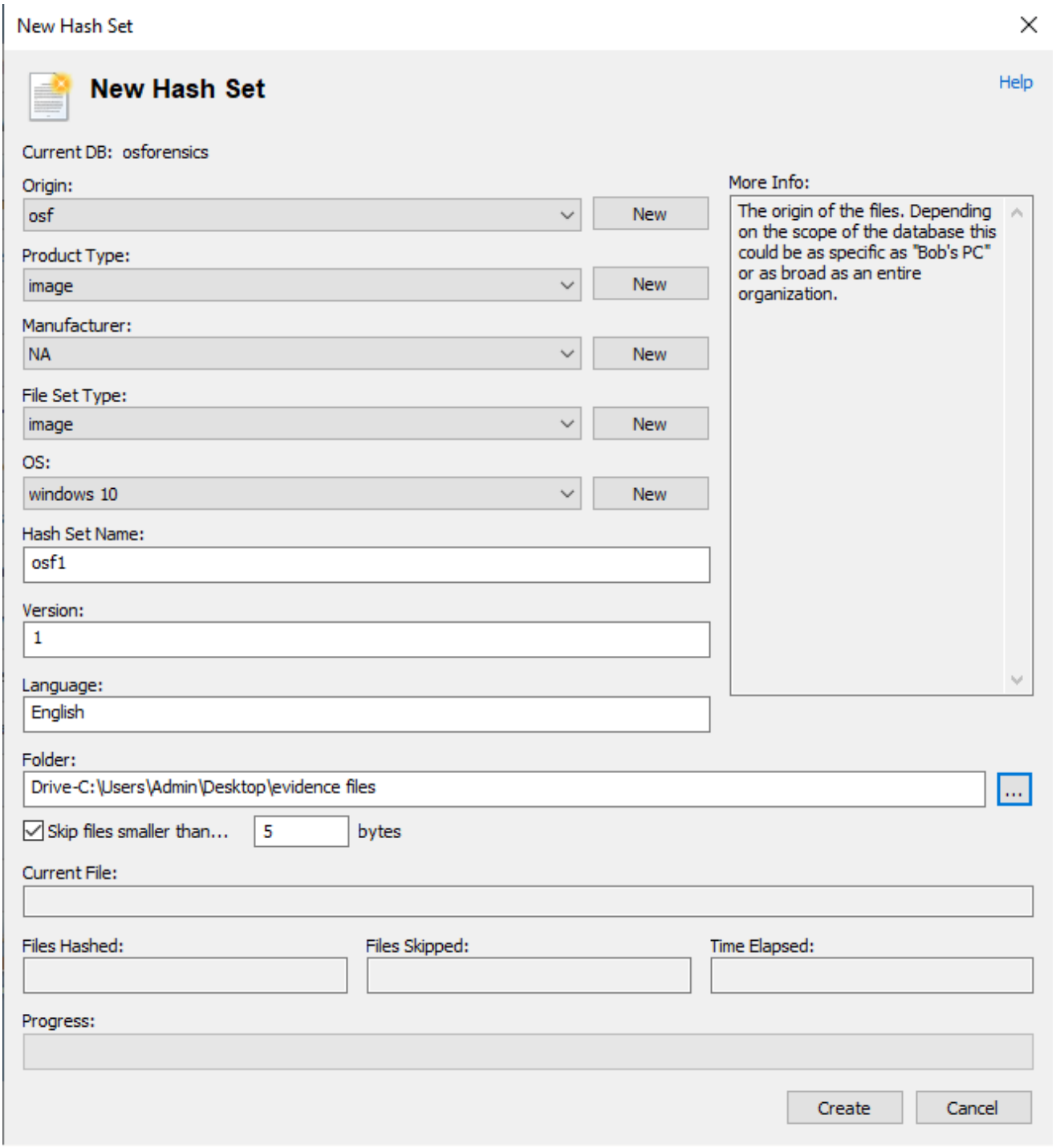
The **File Hash** tool is used to verify the integrity of files, disks, or entire partitions. To use it, select the file you want to hash, choose the **MD5** algorithm, and the tool will calculate and display the corresponding hash value to ensure the file's authenticity and integrity.

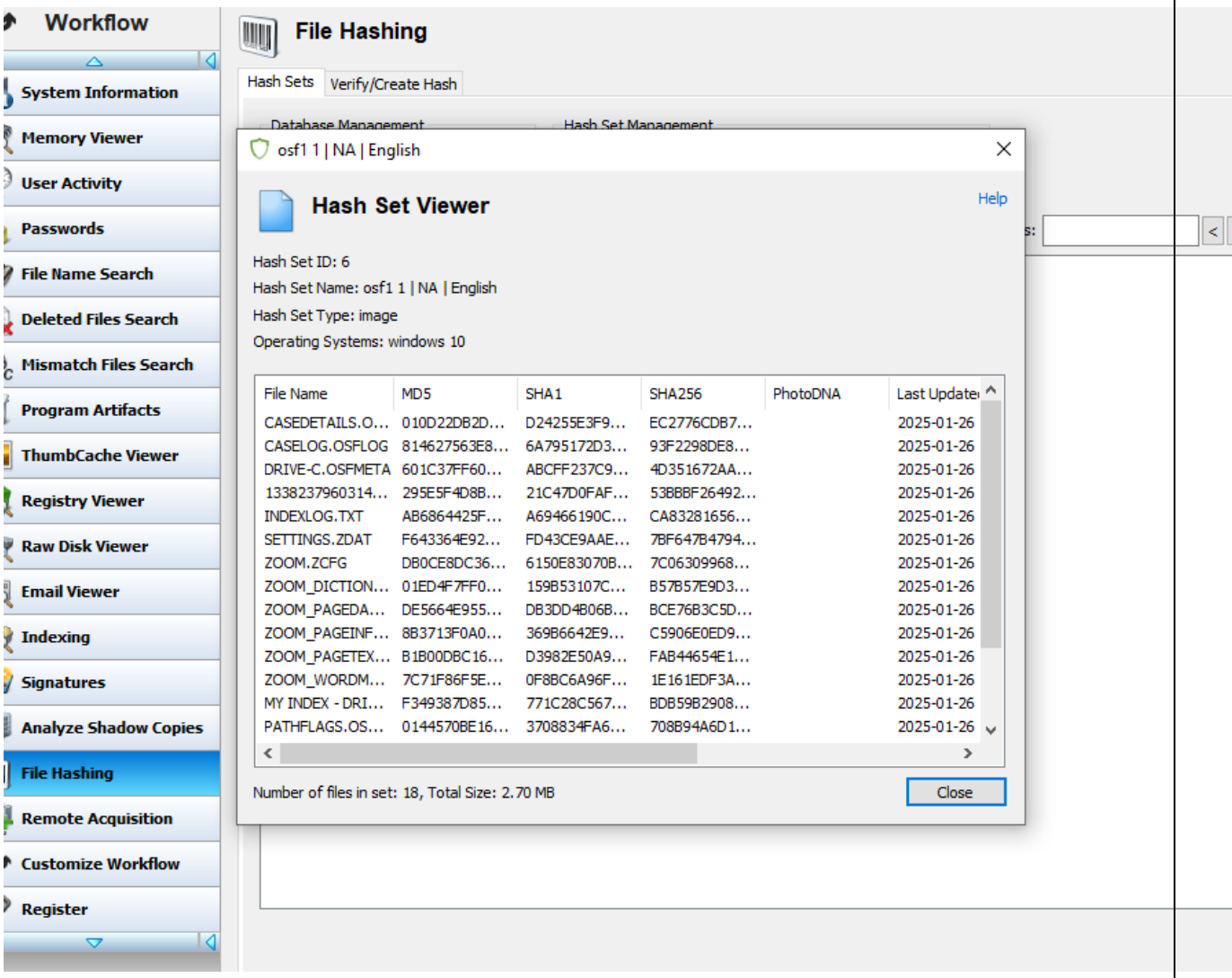


Select the **Hash Sets** feature to identify known suspicious files, helping streamline the investigation process by minimizing the need for time-consuming manual analysis. This allows for quicker detection of potentially harmful or unauthorized files based on predefined hash values.

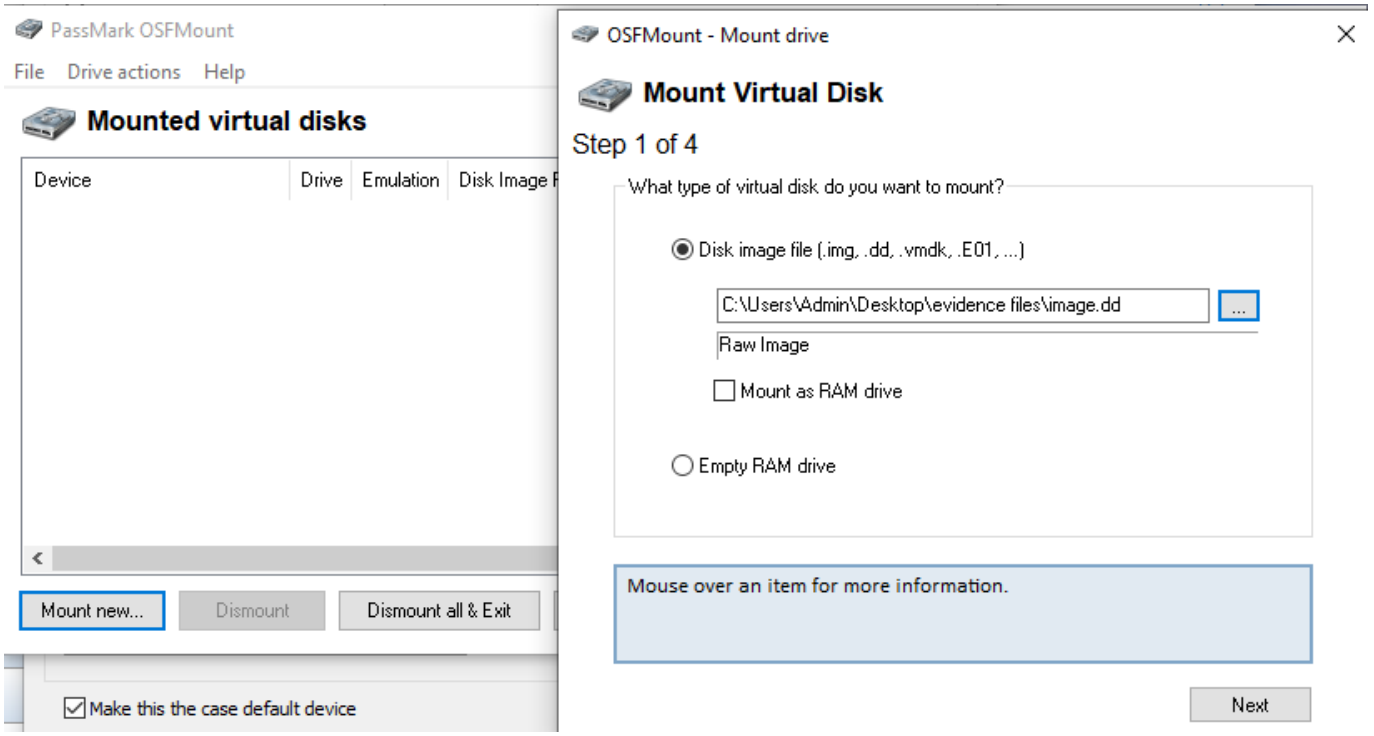
Create a database and set it as active. Then, create a new hash set by providing the necessary details, including the folder path. The tool will generate a new hash set based on the specified files, which can then be used for further analysis.

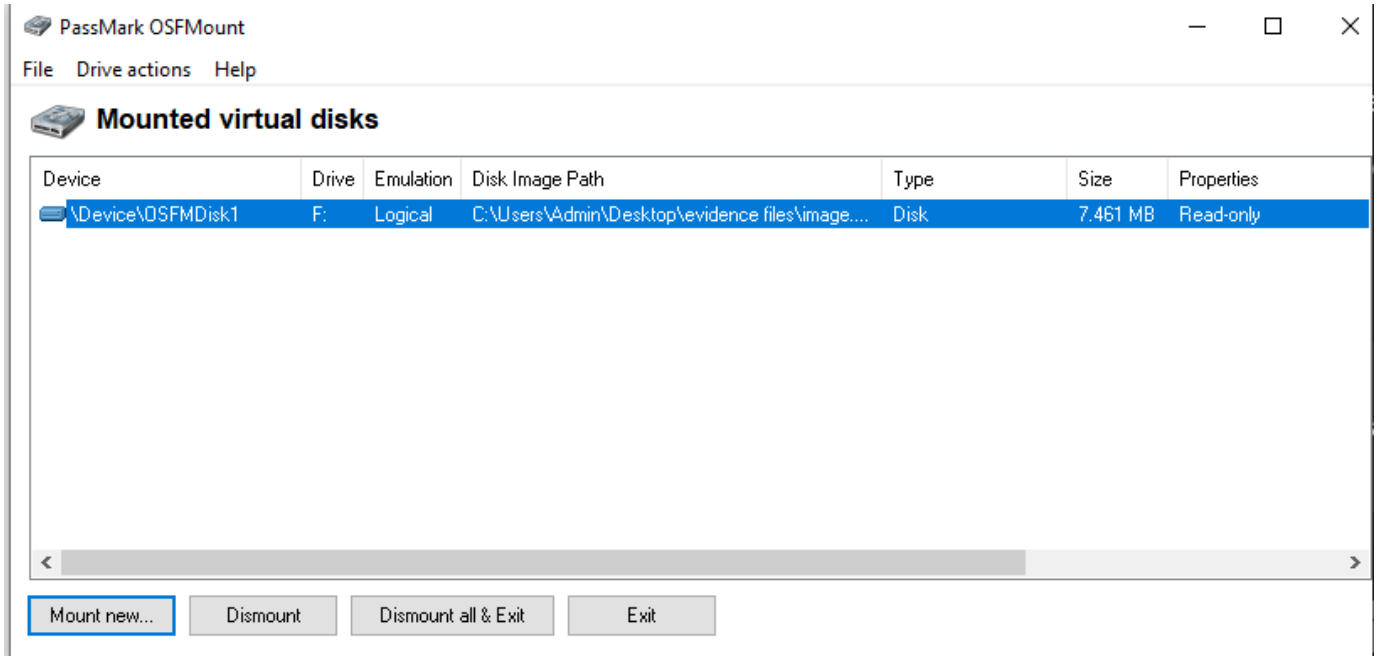

File Hashing
Help
Hash Sets
Verify/Create Hash
Database Management
New DB...
Make DB Active
Hash Set Management
New Set...
Quick Set...
Import CSV Set...
Export...
Search Hash Sets:
Please Enter Database Name
Database Name
osforensics
Save
Cancel


New Hash Set
New Hash Set
Help
Current DB: osforensics
Origin:
osf
New
Product Type:
image
New
Manufacturer:
NA
New
File Set Type:
image
New
OS:
windows 10
New
Hash Set Name:
osf1
Version:
1
Language:
English
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.
Folder:
Drive-C:\Users\Admin\Desktop\evidence files
...
Skip files smaller than...
5
bytes
Current File:
Files Hashed:
Files Skipped:
Time Elapsed:
Progress:
Create
Cancel



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 **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

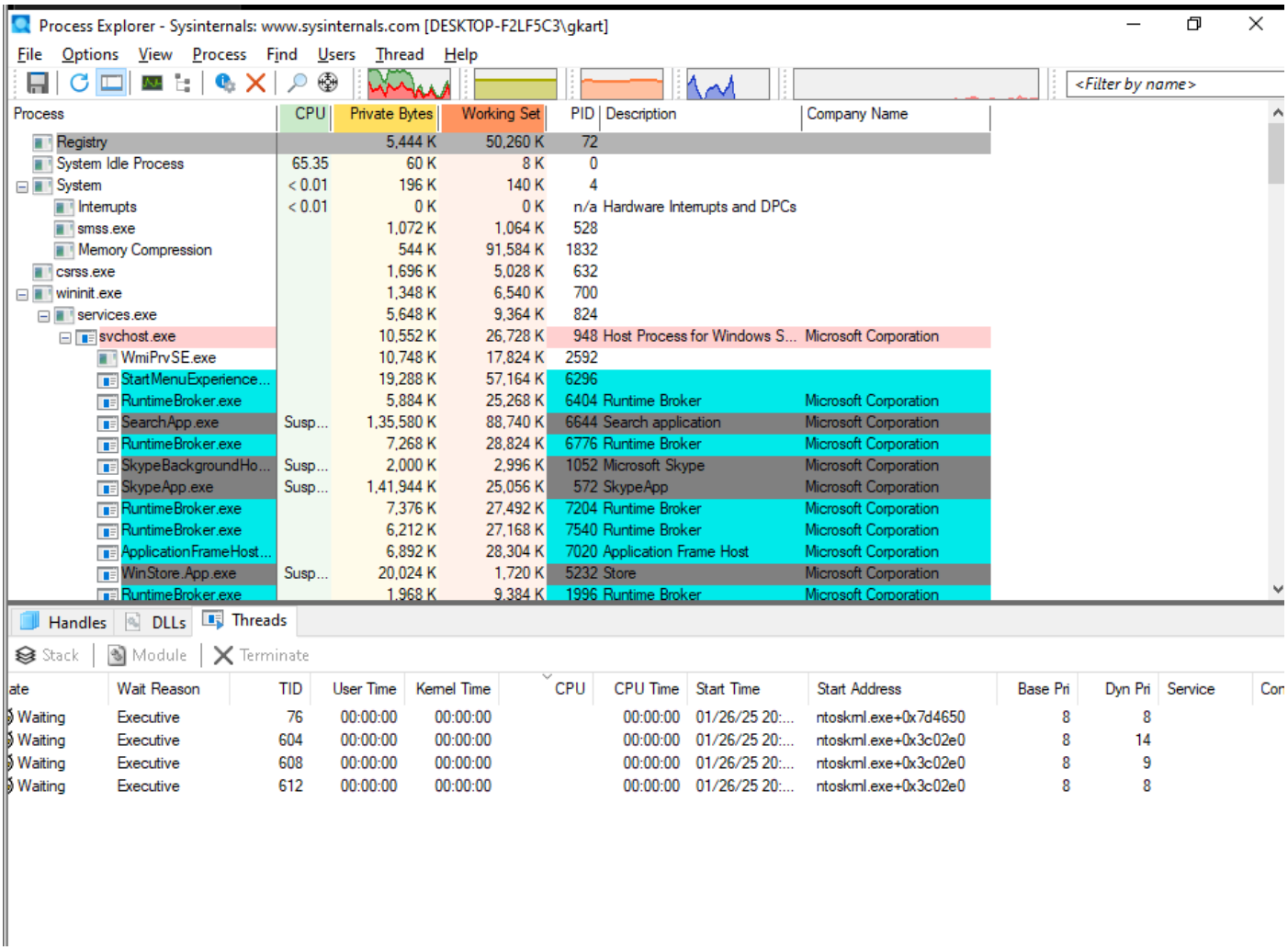
Process Explorer, developed by Microsoft, is a powerful tool used to extract detailed information about loaded processes. It provides insights such as:

- **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.



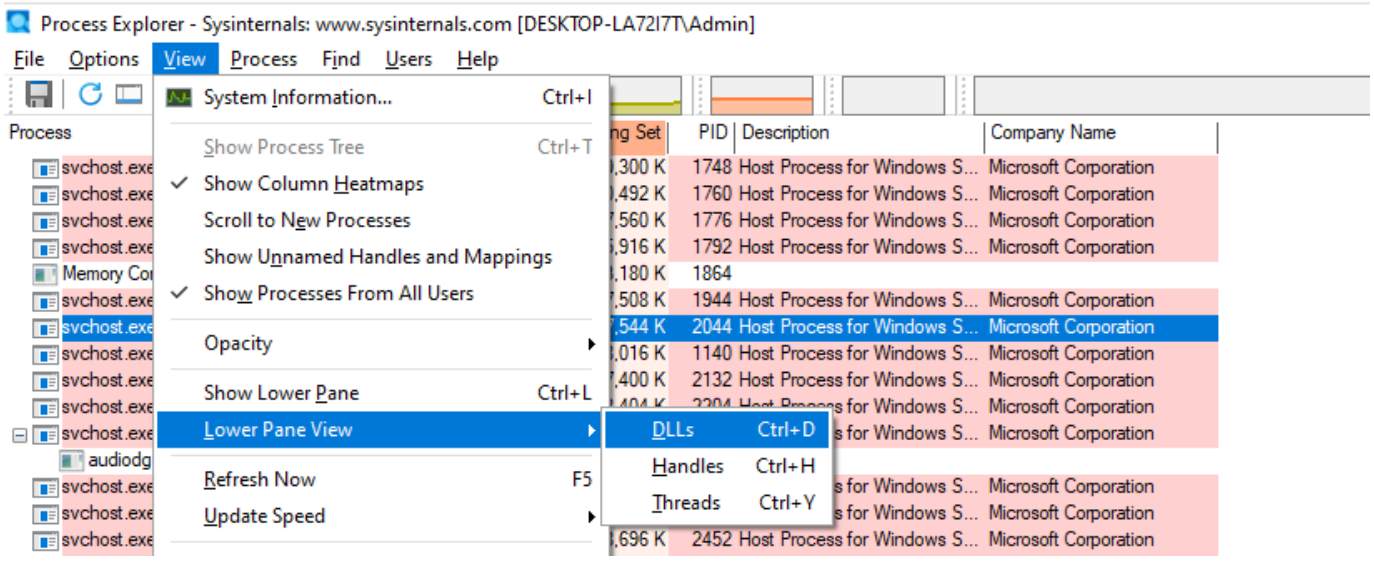
For any process, including the **Explorer process**, **Process Explorer** allows you to view and manage the following:

- **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:

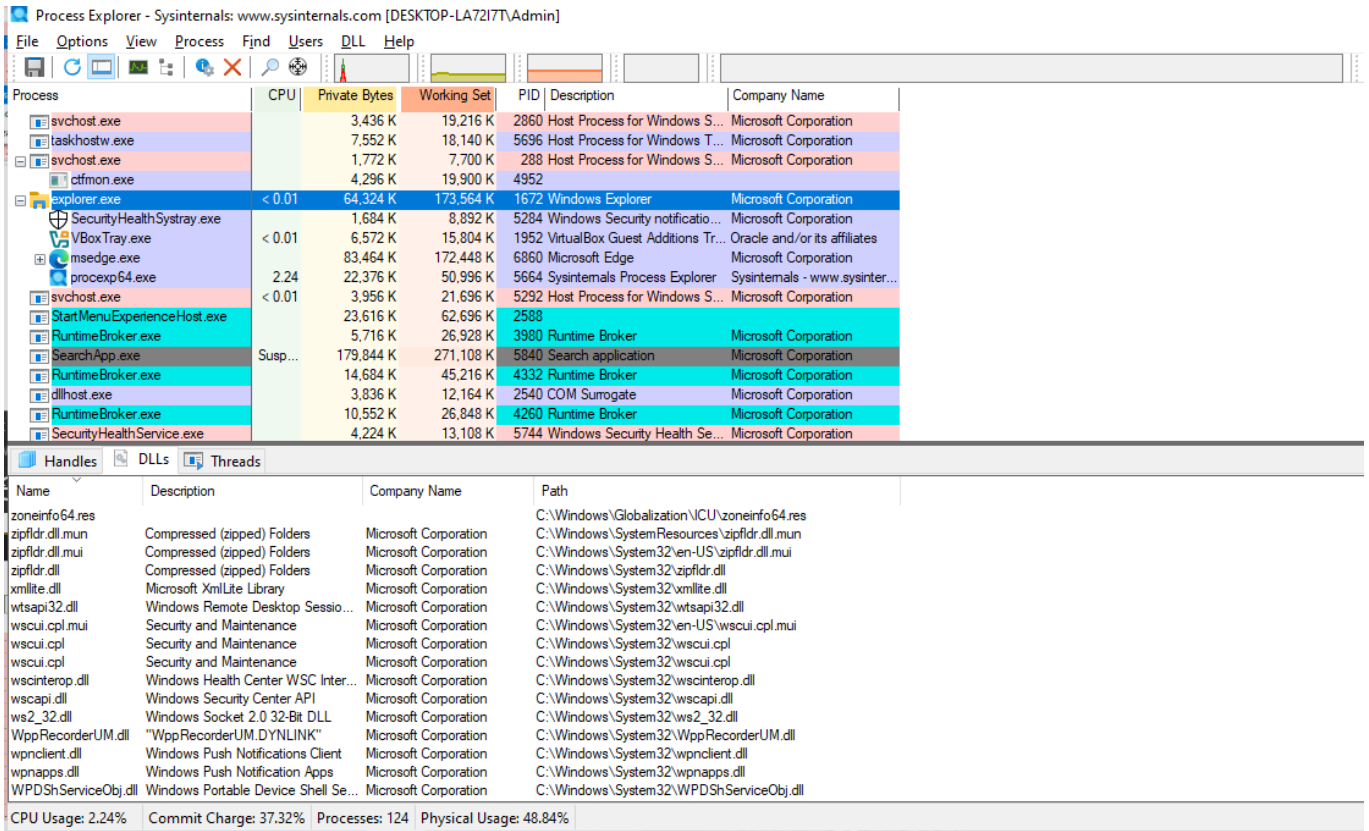
- Terminate or suspend threads or processes.
- Examine and interact with the process handles to manipulate or inspect file, registry, or synchronization objects related to the process.

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

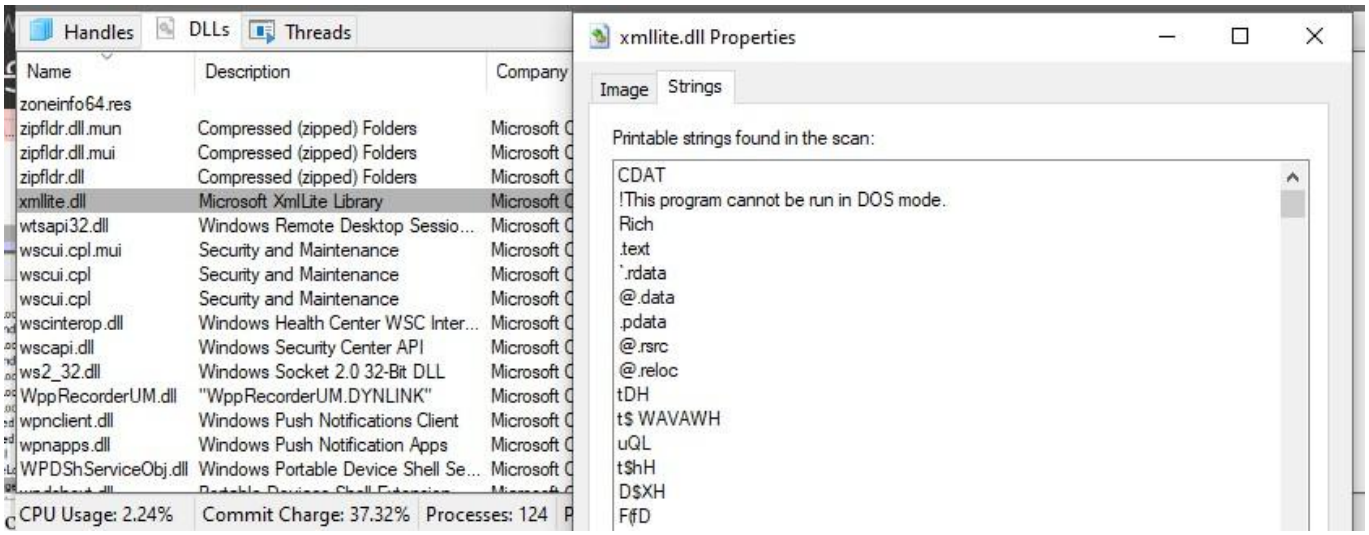


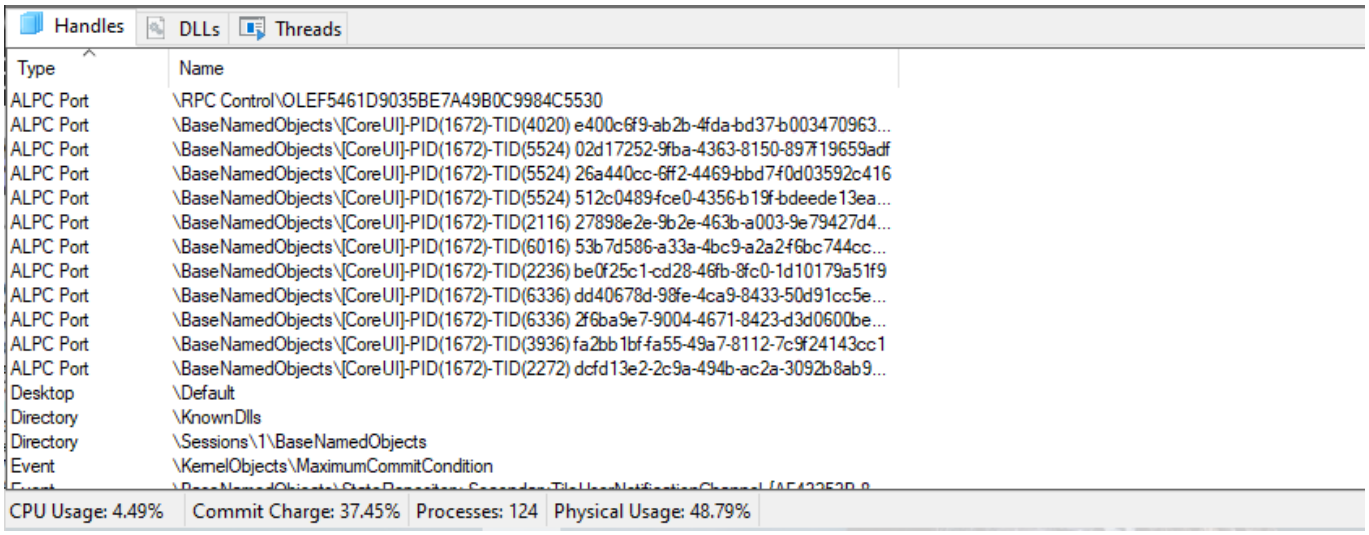
To learn more about a specific DLL, you can select the running DLL in **Process Explorer** and use the **Search Online** option.

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

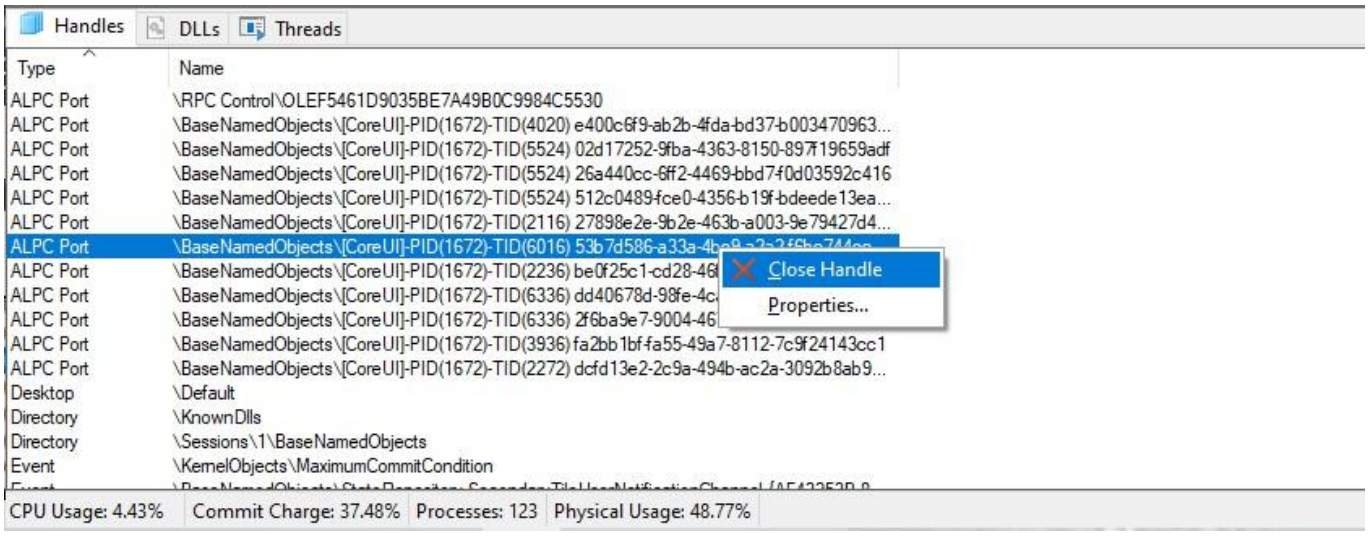


Properties of dlls

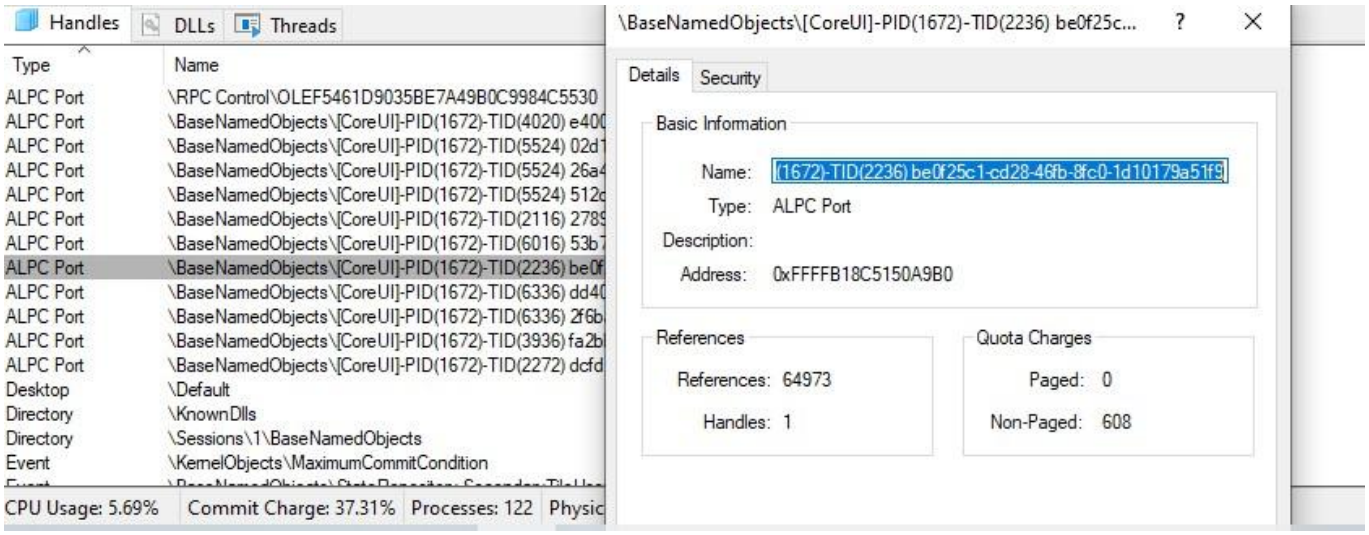




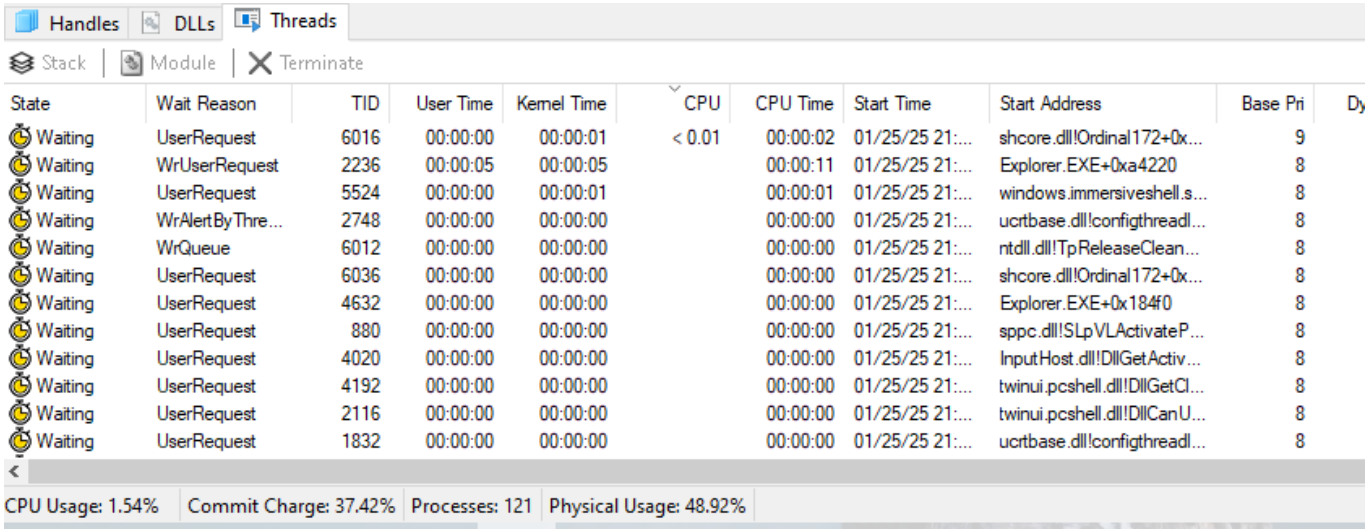
Closing a handle



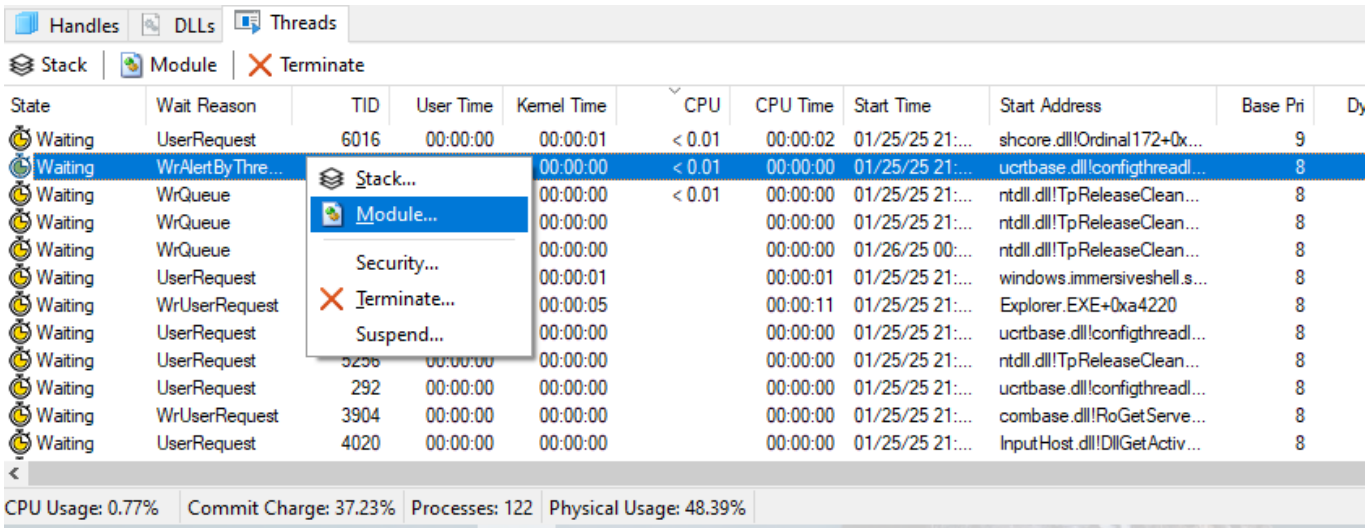
Properties of handles



Running threads



Options in threads

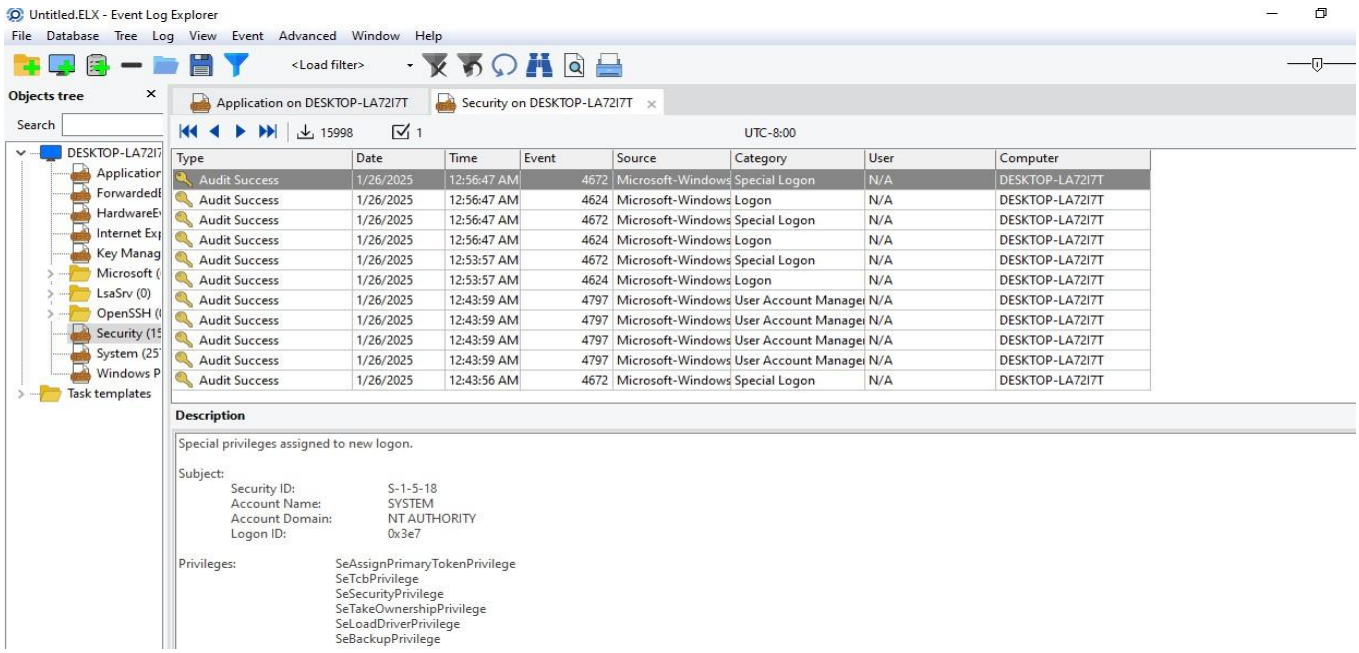


Viewing, Monitoring, and Analyzing Events Using the Event Log Explorer Tool

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:

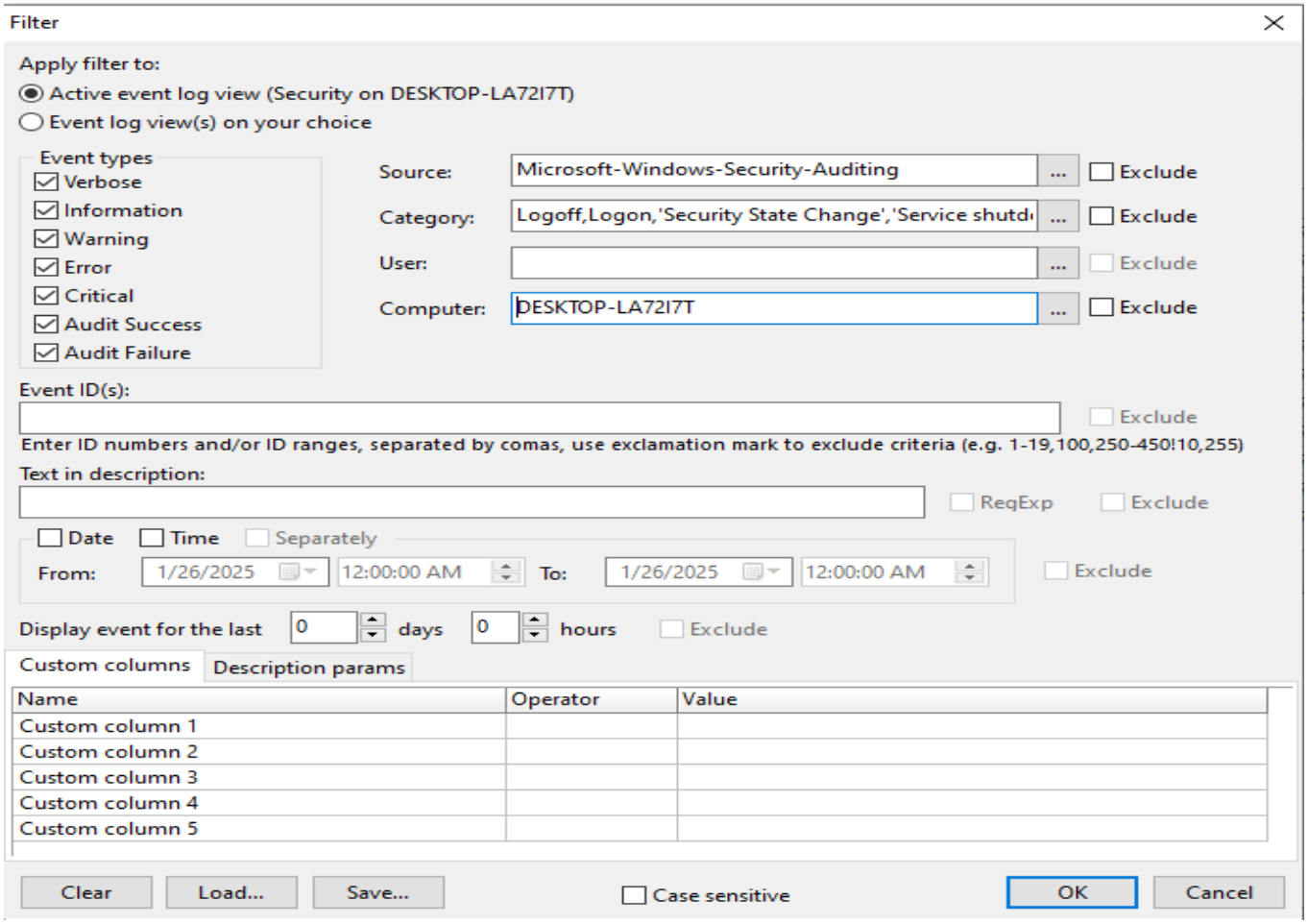
- **Tracking System Events**: It allows you to monitor and track all kinds of events, such as system startup and shutdown, application errors, security events, and more.
- **Detecting Anomalies**: By reviewing event logs, you can identify unusual patterns or activities that may suggest potential issues, 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.

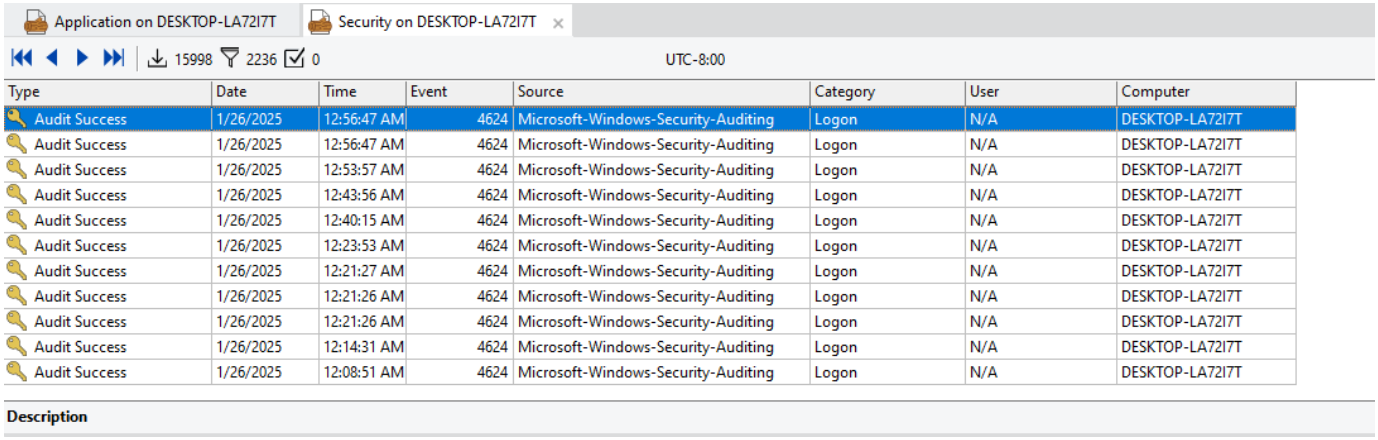


This displays a description of the logs along with detailed properties of each event.

Applying filter

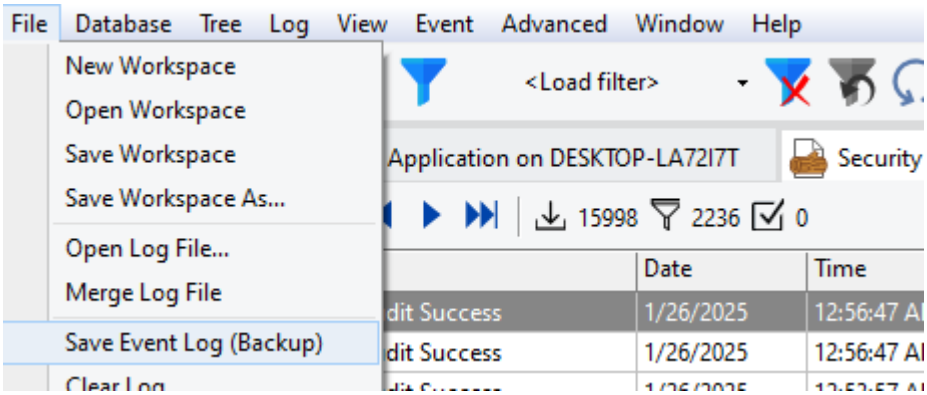

Filter
Apply filter to:
Active event log view (Security on DESKTOP-LA72I7T)
Event log view(s) on your choice
Event types
Verbose
Information
Warning
Error
Critical
Audit Success
Audit Failure
Source: Microsoft-Windows-Security-Auditing
Category: Logoff,Logon,'Security State Change','Service shutd
User:
Computer: DESKTOP-LA72I7T
Exclude
Event ID(s):
Enter ID numbers and/or ID ranges, separated by comas, use exclamation mark to exclude criteria (e.g. 1-19,100,250-450!10,255)
Text in description:
RegExp
Date
Time
Separately
From: 1/26/2025 12:00:00 AM
To: 1/26/2025 12:00:00 AM
Display event for the last 0 days 0 hours
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

Save the Event Log (Backup) for later analysis



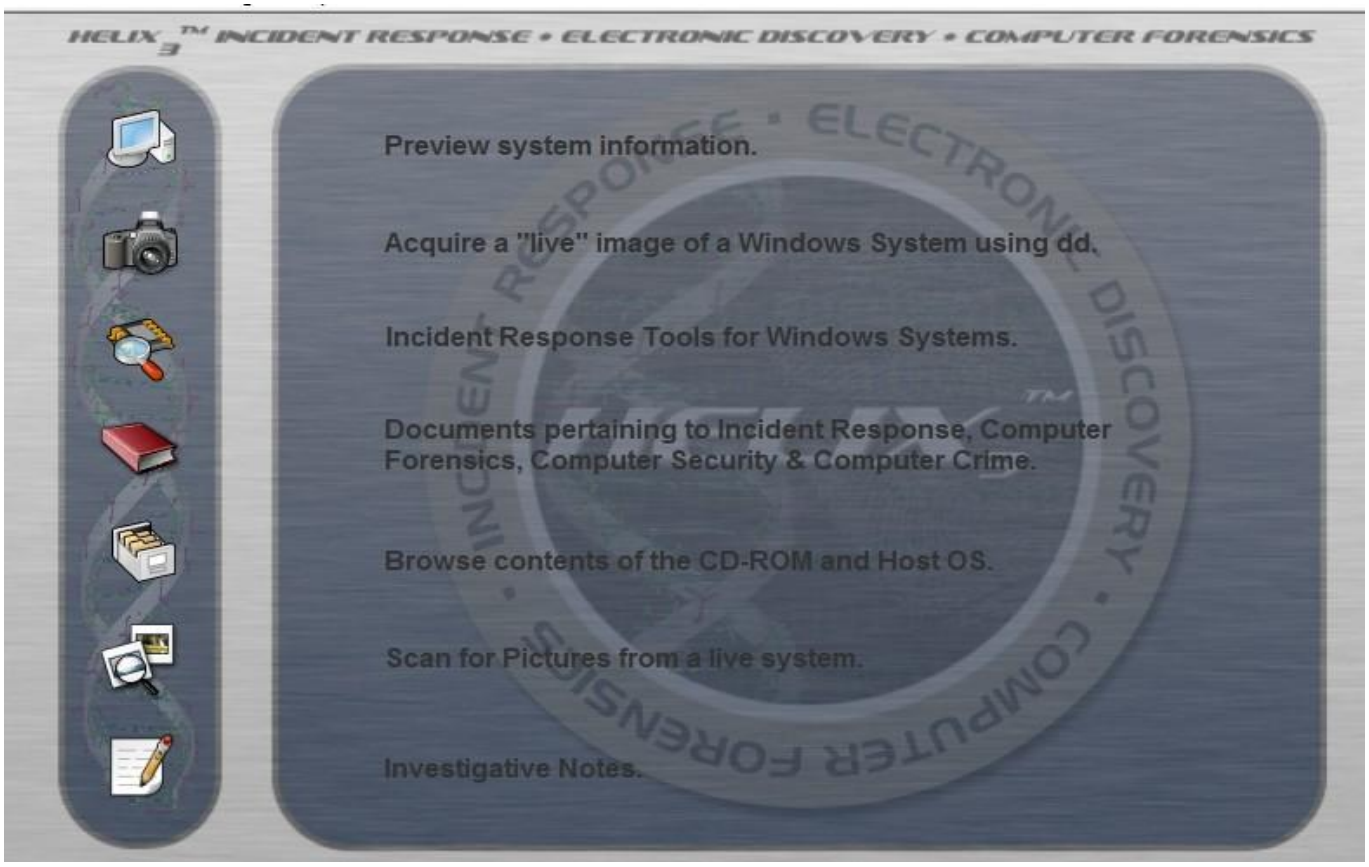
Performing a Computer Forensic Investigation Using the Helix Tool

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:

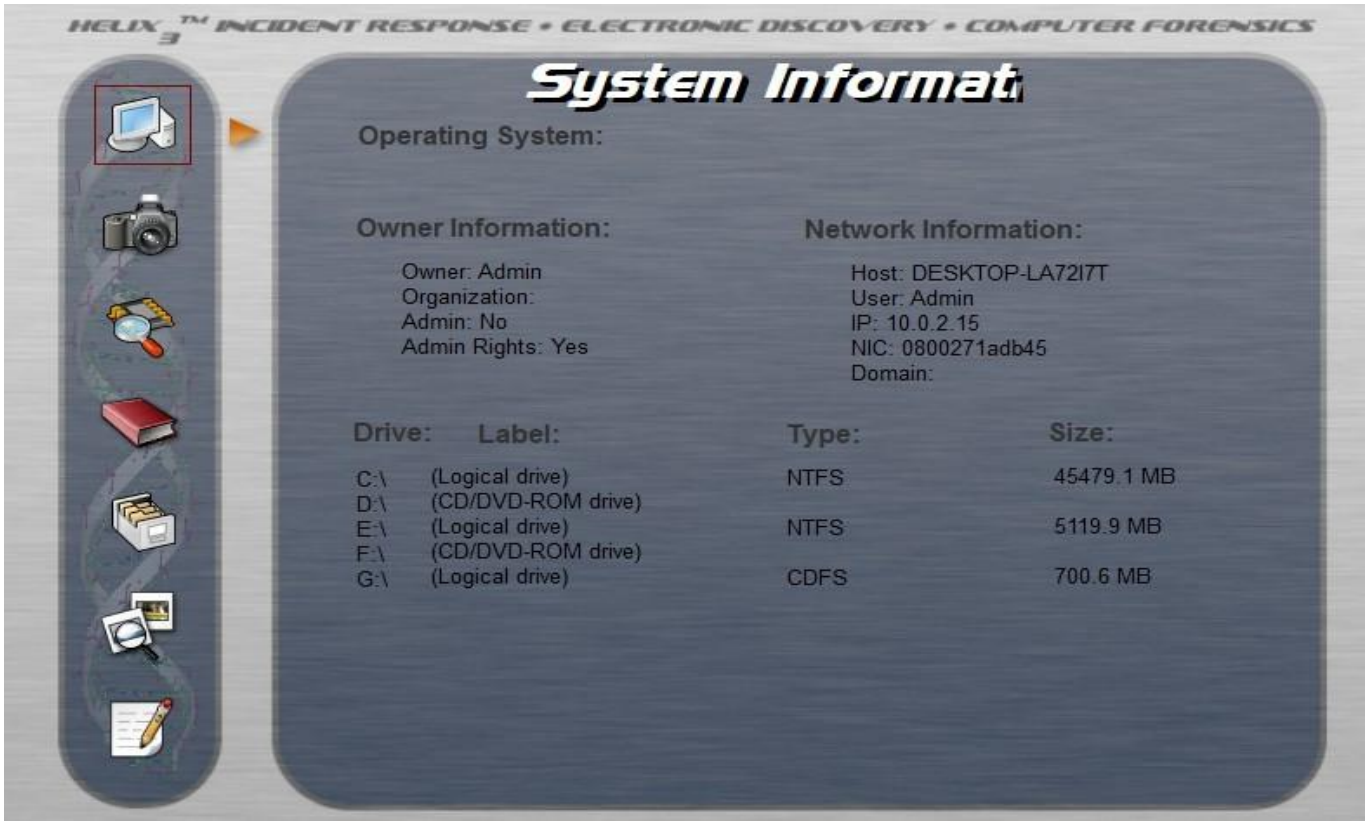
- **Data Acquisition**: Helix enables the safe collection of digital evidence from live systems or disk images, ensuring that the data is preserved in a forensically sound manner without altering or damaging the original evidence.
- **Analysis and Incident Response**: The tool provides capabilities for 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.


HELIX v1.9 (07/13/2007)
INCIDENT RESPONSE • ELECTRONIC DISCOVERY • COMPUTER FORENSICS
HELIX 3
WARNING
You are running this application in a LIVE Windows environment. There is ABSOLUTELY NO WAY to protect this live environment from changing.
This application WILL make changes to the running system. This is an accepted risk you must be willing to take.
If you are not willing to accept this risk or do not understand what you are doing then exit now, otherwise agree and proceed at your own risk....
Brought to you by:
e-fense
http://www.e-fense.com
helix@e-fense.com
Choose Your Language:
English
Accept
Exit


HELIX 3 INCIDENT RESPONSE • ELECTRONIC DISCOVERY • COMPUTER FORENSICS
Preview system information.
Acquire a "live" image of a Windows System using dd.
Incident Response Tools for Windows Systems.
Documents pertaining to Incident Response, Computer Forensics, Computer Security & Computer Crime.
Browse contents of the CD-ROM and Host OS.
Scan for Pictures from a live system.
Investigative Notes.

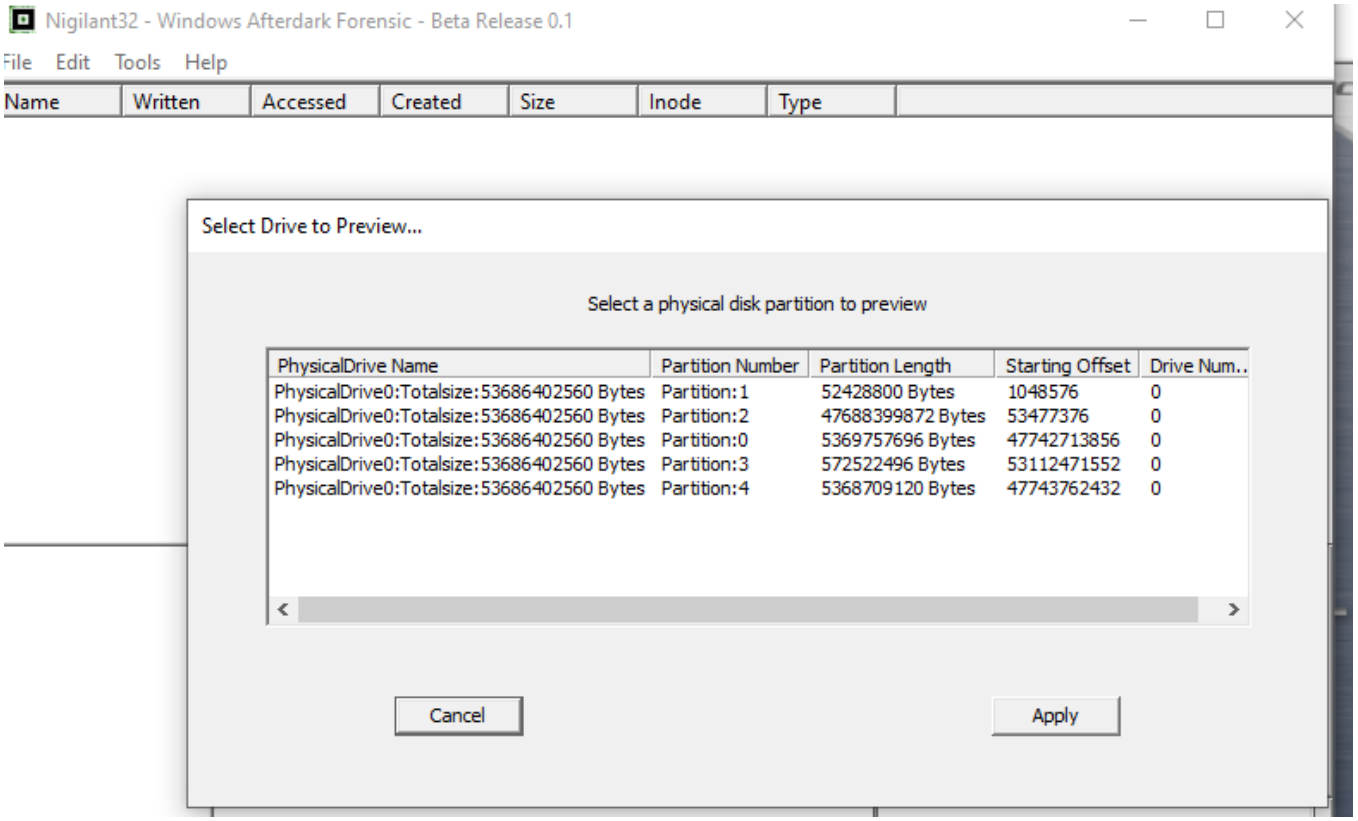
System information



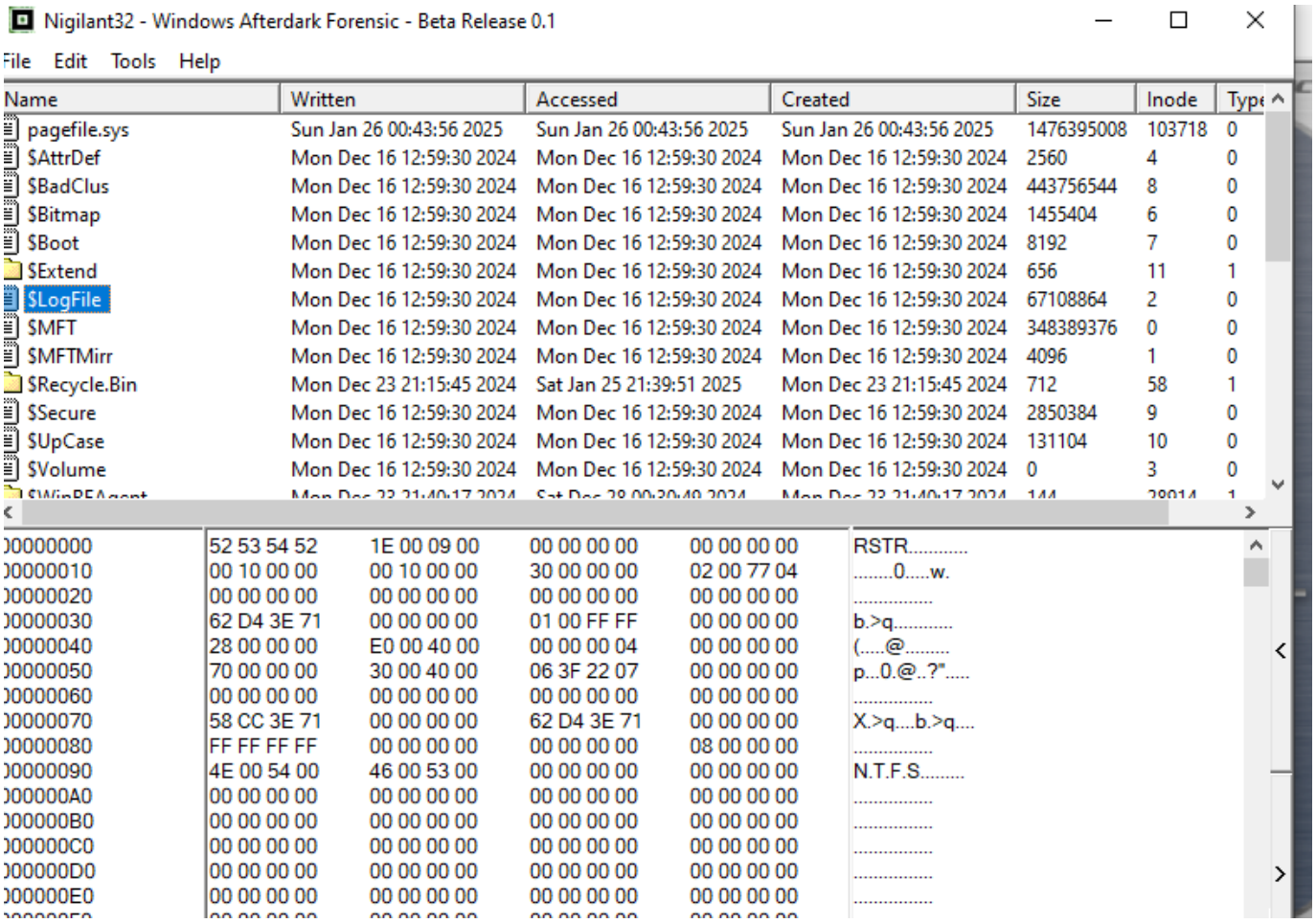
Live Acquisition

Incident Response

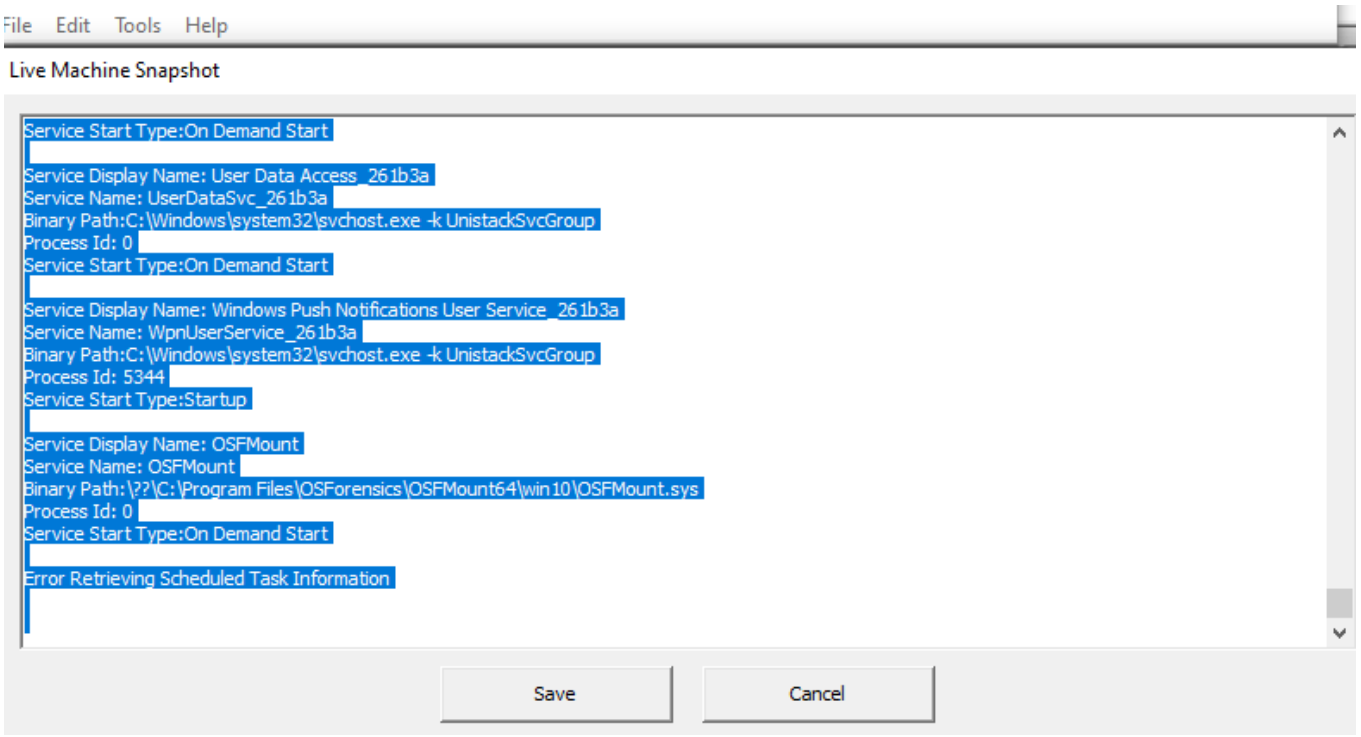
Select Agile Risk Management and choose the disk



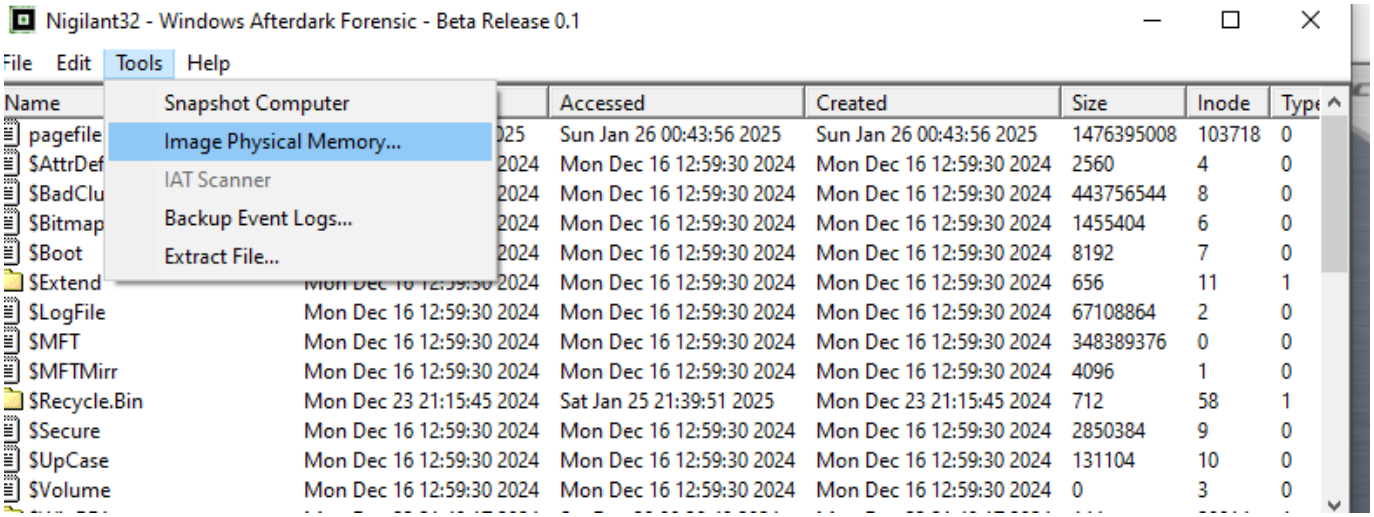
This shows the disk contents along with the hex of the selected file

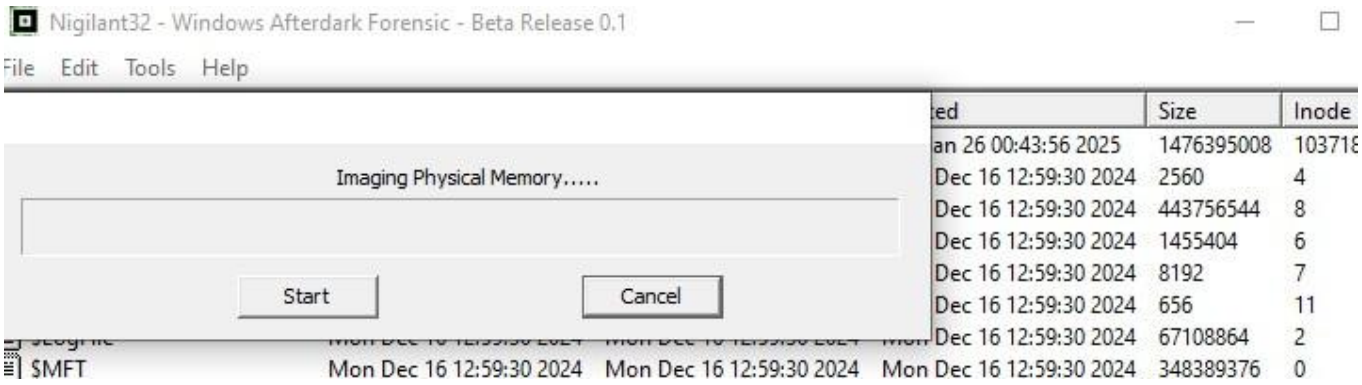


Snapshot the machine by selecting tools → snapshot


File Edit Tools Help
Live Machine Snapshot
Service Start Type:On Demand Start
Service Display Name: User Data Access_261b3a
Service Name: UserDataSvc_261b3a
Binary Path:C:\Windows\system32\svchost.exe -k UnistackSvcGroup
Process Id: 0
Service Start Type:On Demand Start
Service Display Name: Windows Push Notifications User Service_261b3a
Service Name: WpnUserService_261b3a
Binary Path:C:\Windows\system32\svchost.exe -k UnistackSvcGroup
Process Id: 5344
Service Start Type:Startup
Service Display Name: OSFMount
Service Name: OSFMount
Binary Path:\??\C:\Program Files\OSForensics\OSFMount64\win10\OSFMount.sys
Process Id: 0
Service Start Type:On Demand Start
Error Retrieving Scheduled Task Information
Save
Cancel

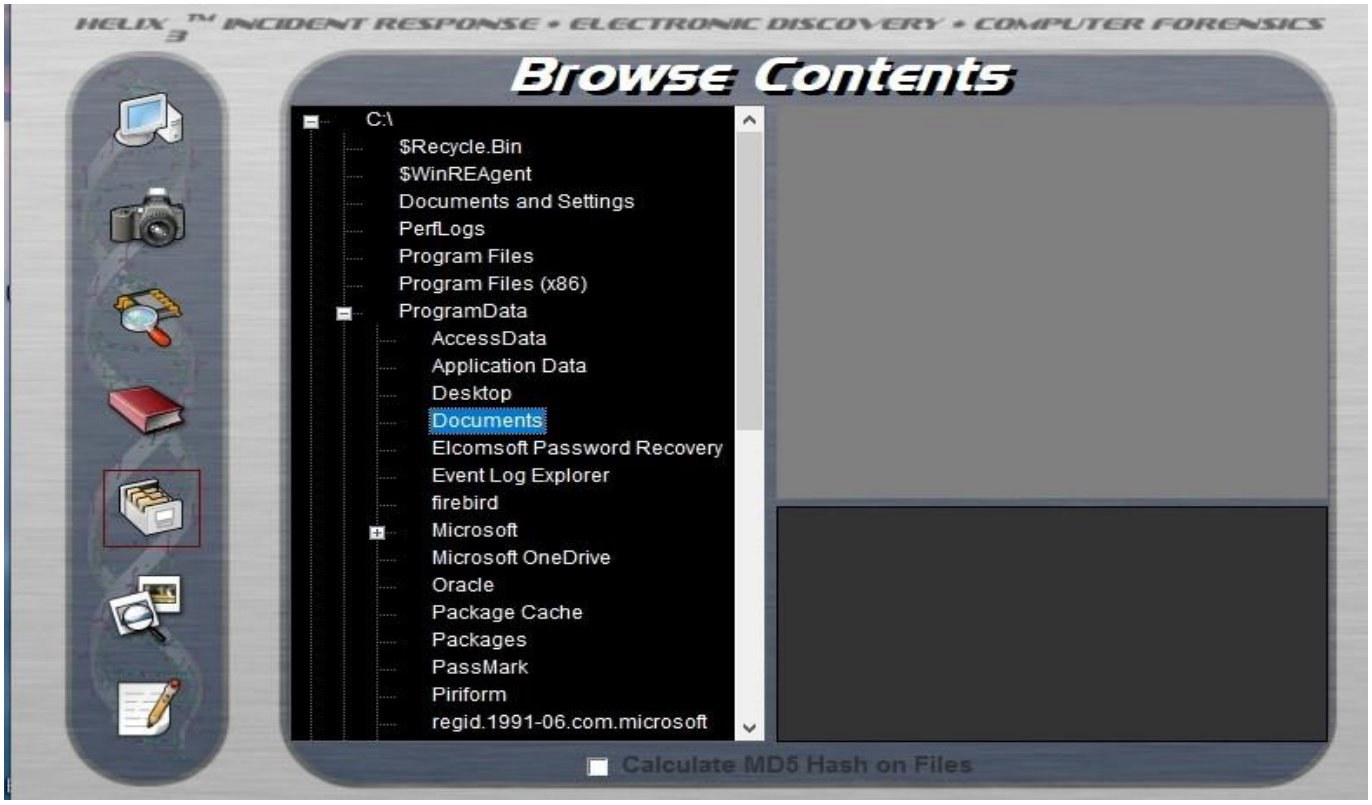
To create an image of physical memory, go to **Tools** and select **Image Physical Memory**





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.

```
┌──(karthikeyan㉿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/karthikeyan]
└─# 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   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/karthikeyan]
└─# 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
karthike tty2     -                21:43    5:20   7.52s  0.03s /usr/libexec/gnome-session-b
karthike          -                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              -                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.

```
┌──(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                    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)-[/home/karthikeyan]
└─# 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)-[/home/karthikeyan]
└─# 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

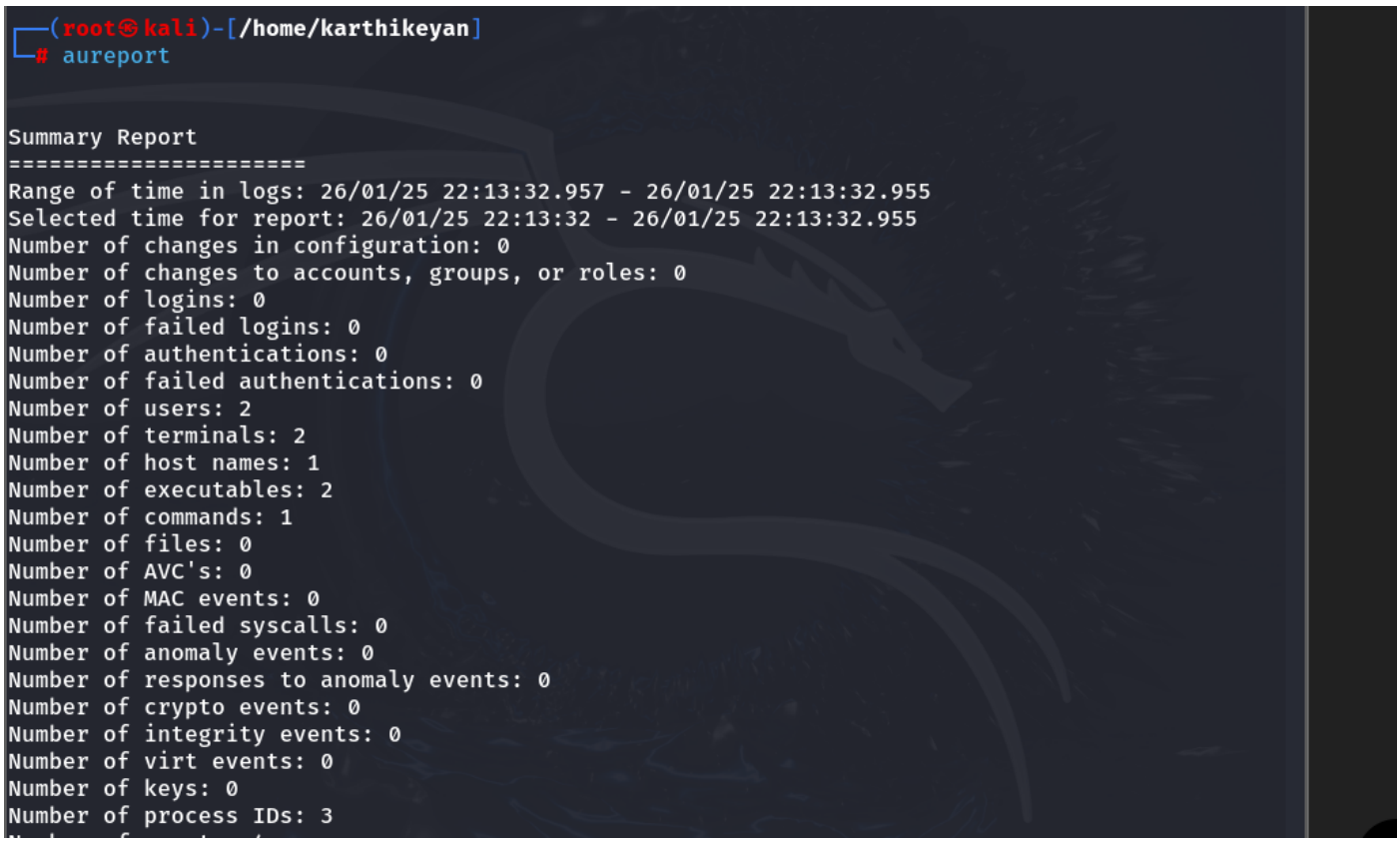
```
┌──(root㉿kali)-[/home/karthikeyan]
└─# apt install auditd
Upgrading:
  libaudit-common  libaudit1

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
```



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

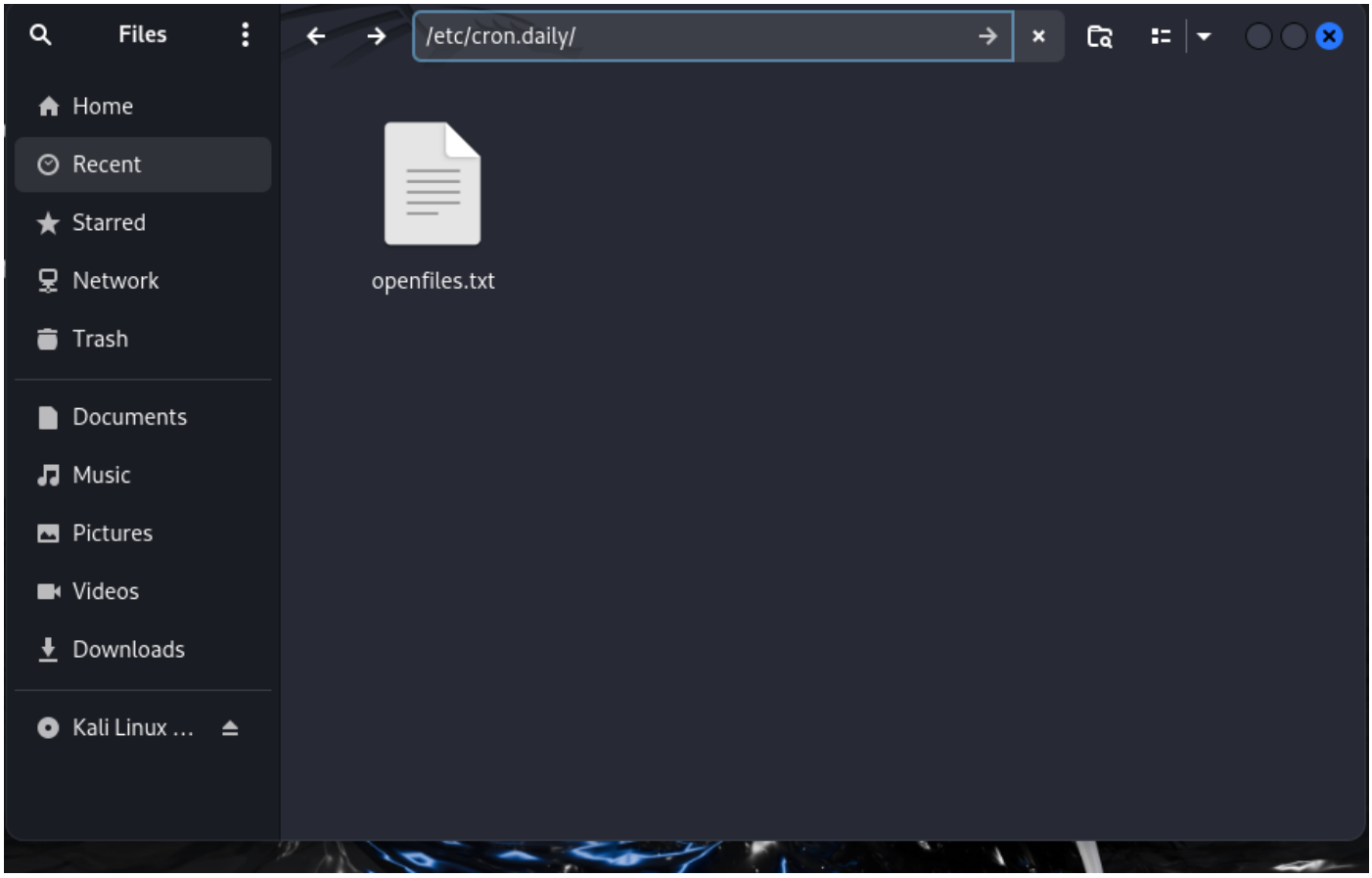
```
┌──(root㉿kali)-[/home/karthikeyan]
└─# id root
uid=0(root) gid=0(root) groups=0(root)

┌──(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 k
ernel=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 su
bj=unconfined msg='unit=auditd comm=systemd exe=/usr/lib/systemd/systemd hostname=? addr=? ter
minal=? res=success'
----
type=USER_END msg=audit(26/01/25 22:13:32.955:4) : pid=4045 uid=root auid=karthikeyan ses=3 su
bj=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=karthikeyan ses=3 s
ubj=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.

```
┌──(karthikeyan㉿kali)-[~]
└─$ cat .zsh_history
metasploit
ls
/usr
/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\
```

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.

```
┌──(karthikeyan㉿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.

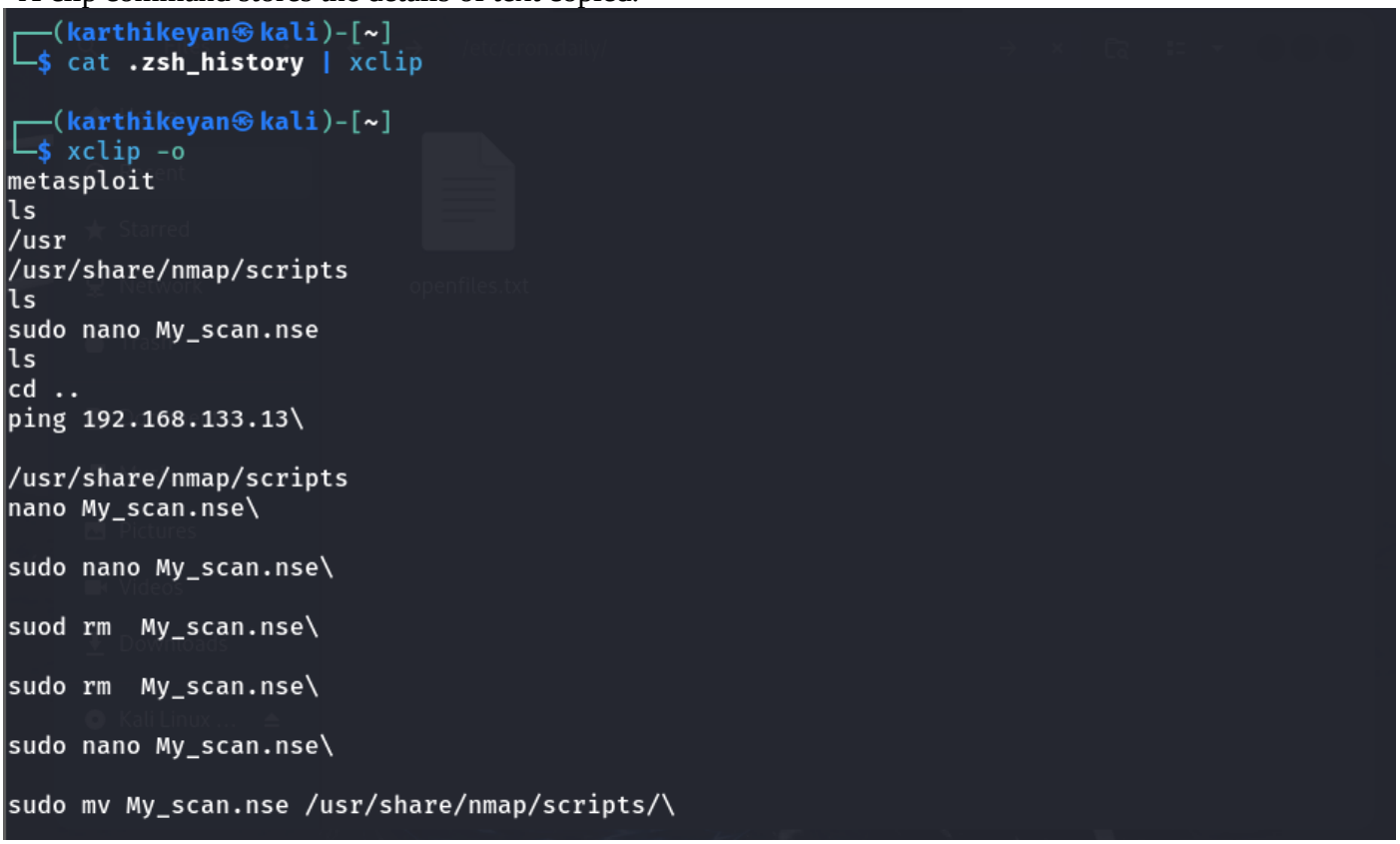
```
root@kali: /home/karthikeyan
┌──(root㉿kali)-[/home/karthikeyan]
└─# ps auxww
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.1  0.3  23392 14456 ?        Ss   22:00   0:02 /sbin/init splash
root           2  0.0  0.0      0     0 ?        S    22:00   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 [kauditd]
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)-[/home/karthikeyan]
└─# ss -l -p -n | grep 4793
```

X clip command stores the details of text copied.



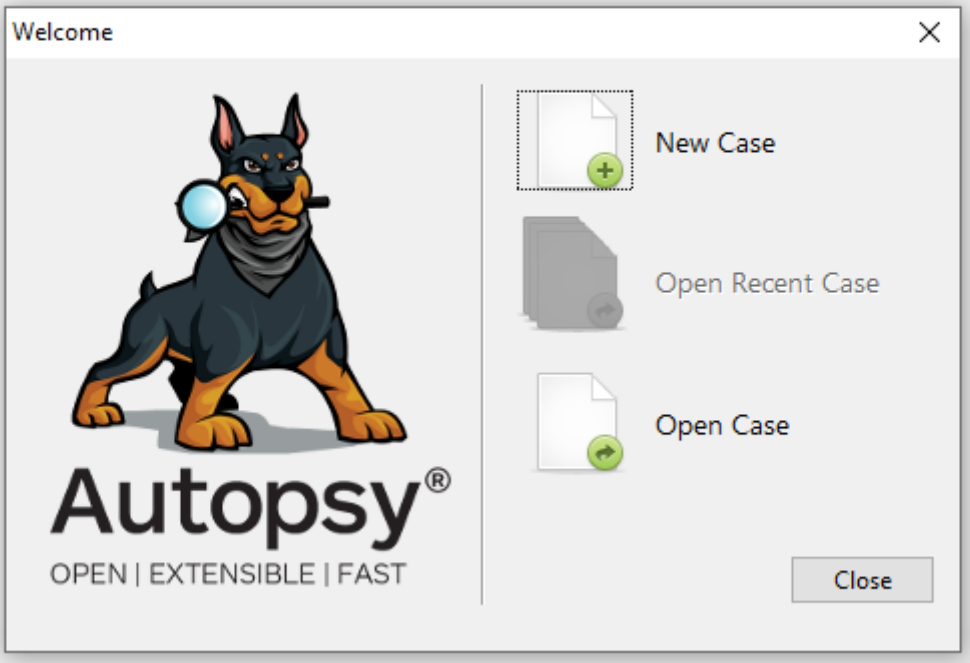
6. Analyzing Non-Volatile Data in a Linux System

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

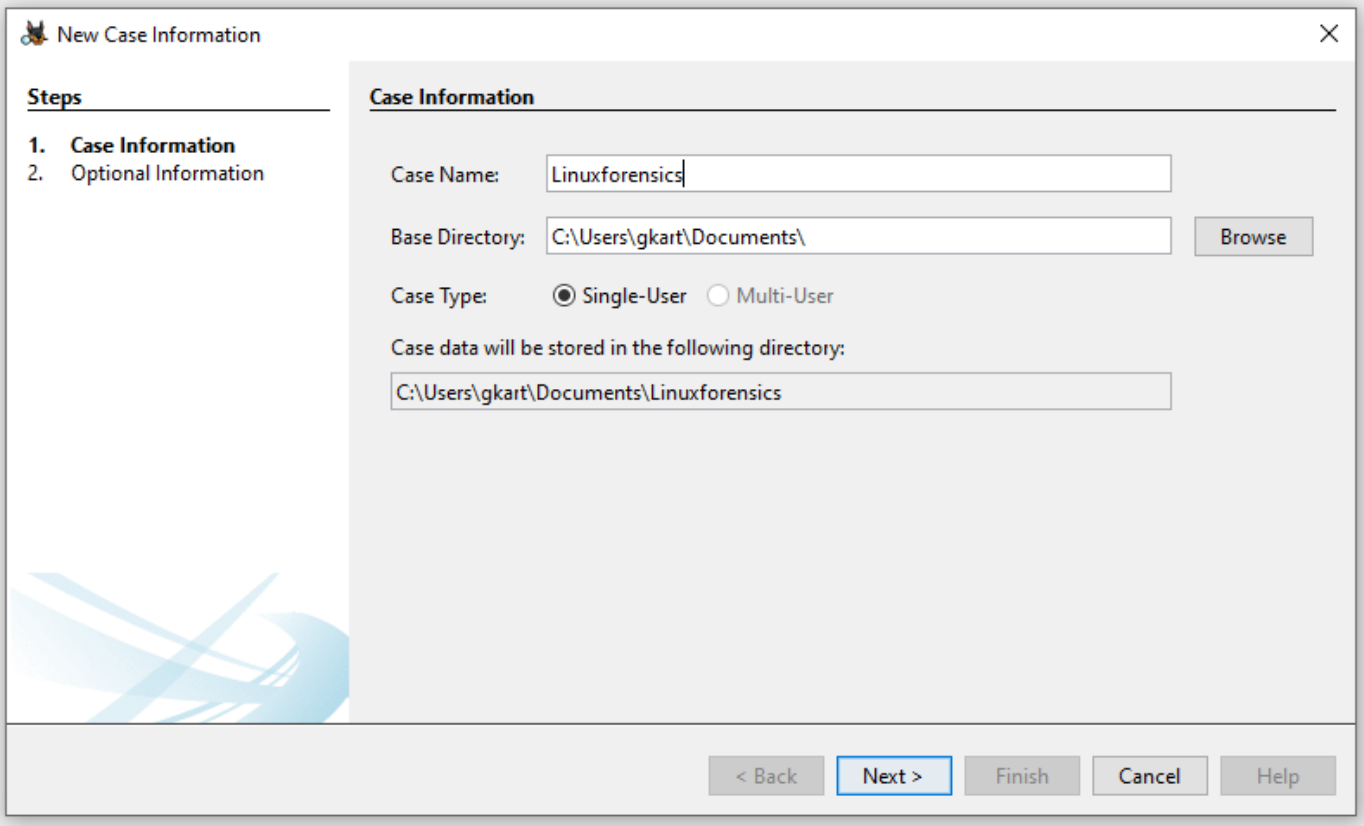
1. Open **Autopsy**, a digital forensics tool.
2. Create a **new case** by selecting the appropriate option.
3. Provide the required details for the case, such as the case name, description, and investigator information.

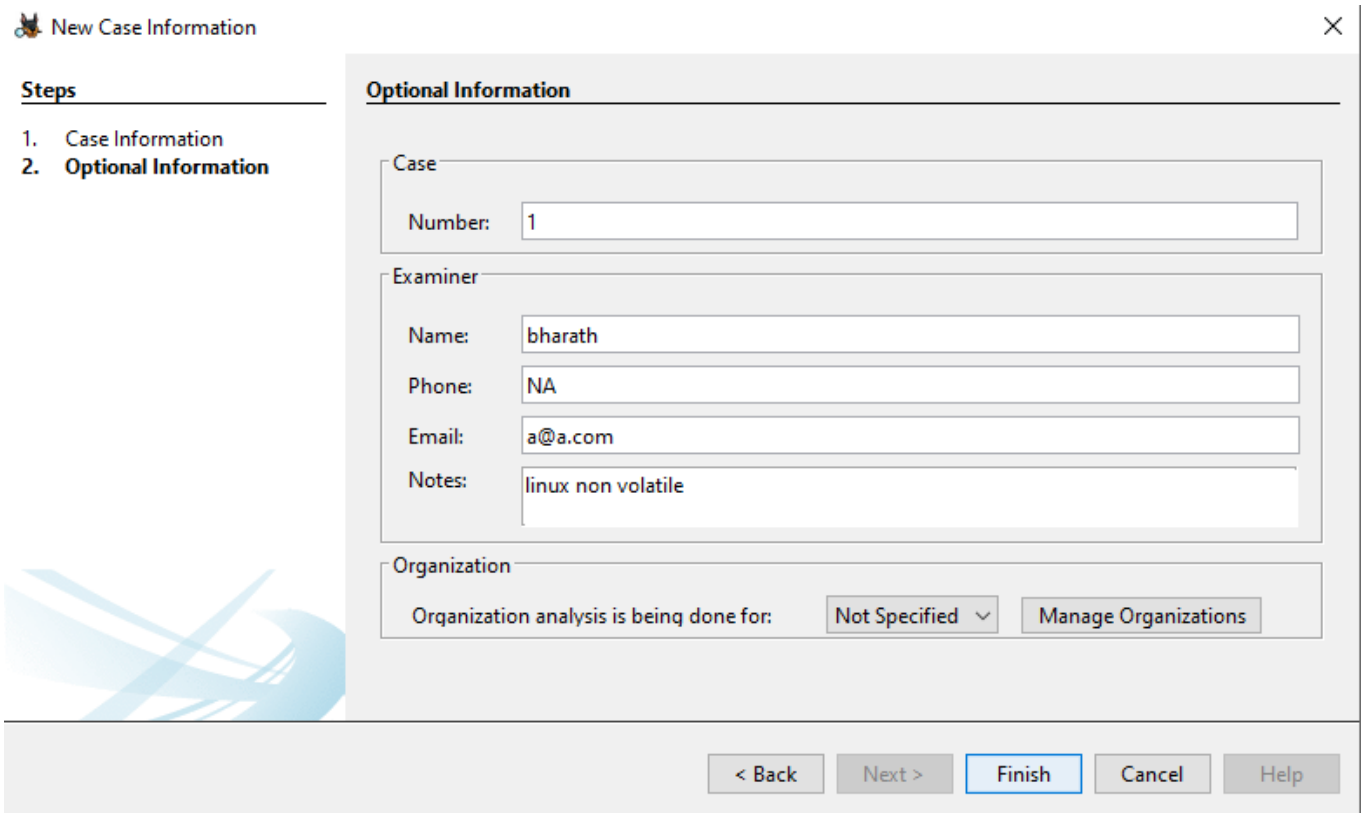
Once the case is set up, you can begin analysing non-volatile data from the Linux system, such as file systems, logs, and other stored data.


Autopsy®
OPEN | EXTENSIBLE | FAST
Reading module storage...

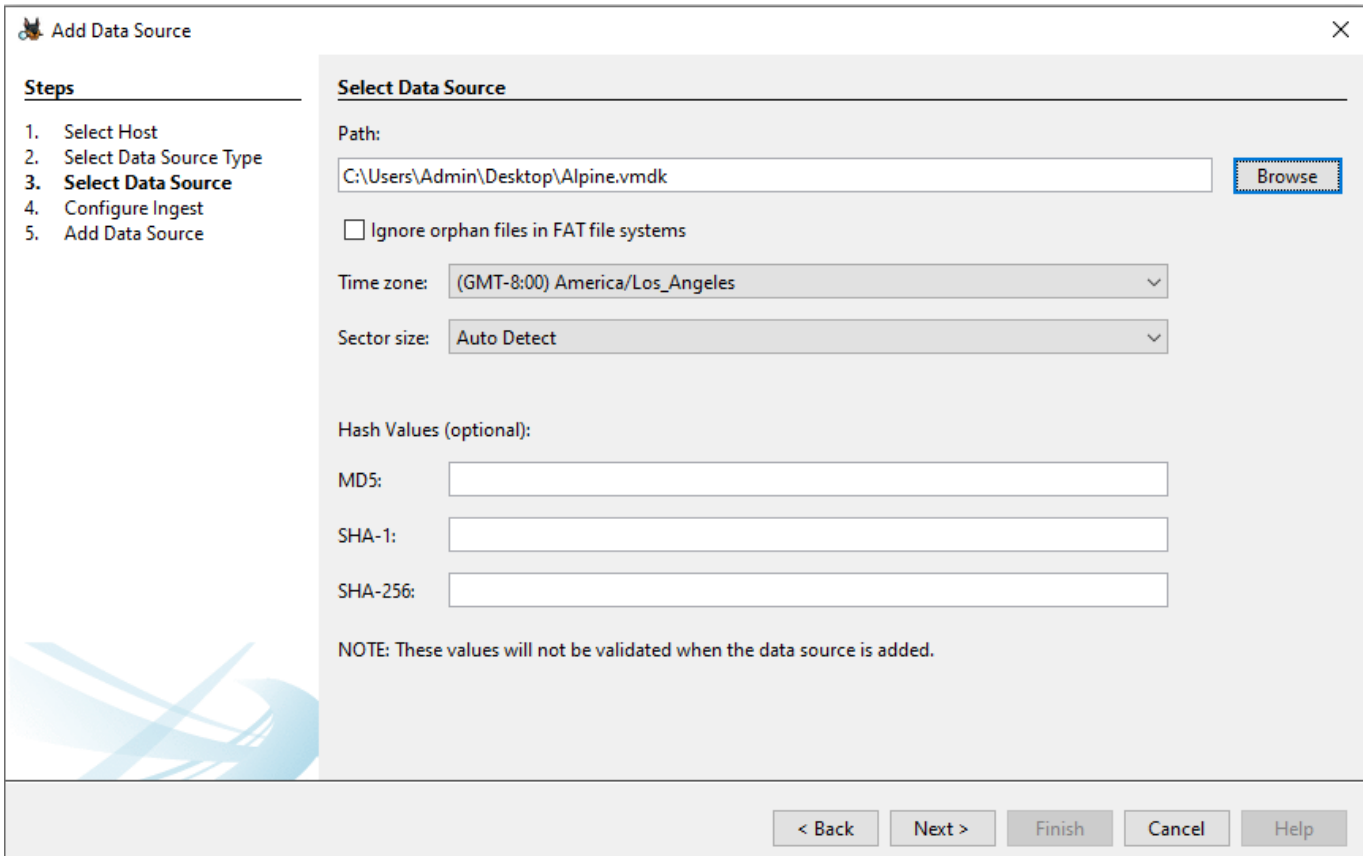

Welcome
New Case
Open Recent Case
Open Case
Close
Autopsy®
OPEN | EXTENSIBLE | FAST

nsics

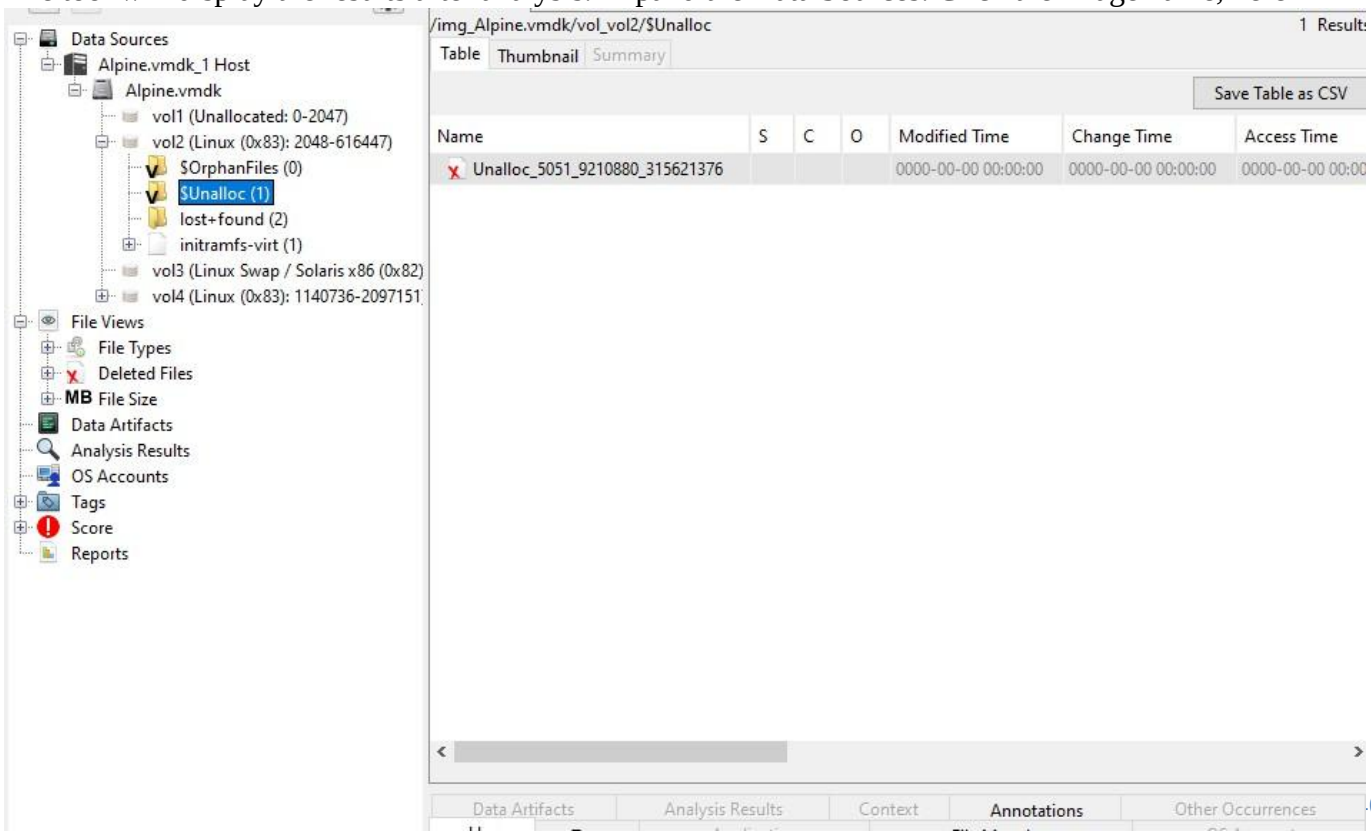

New Case Information
Steps
1. Case Information
2. Optional Information
Case Information
Case Name: Linuxforensics
Base Directory: C:\Users\gkart\Documents\
Browse
Case Type: Single-User Multi-User
Case data will be stored in the following directory:
C:\Users\gkart\Documents\Linuxforensics
< Back
Next >
Finish
Cancel
Help

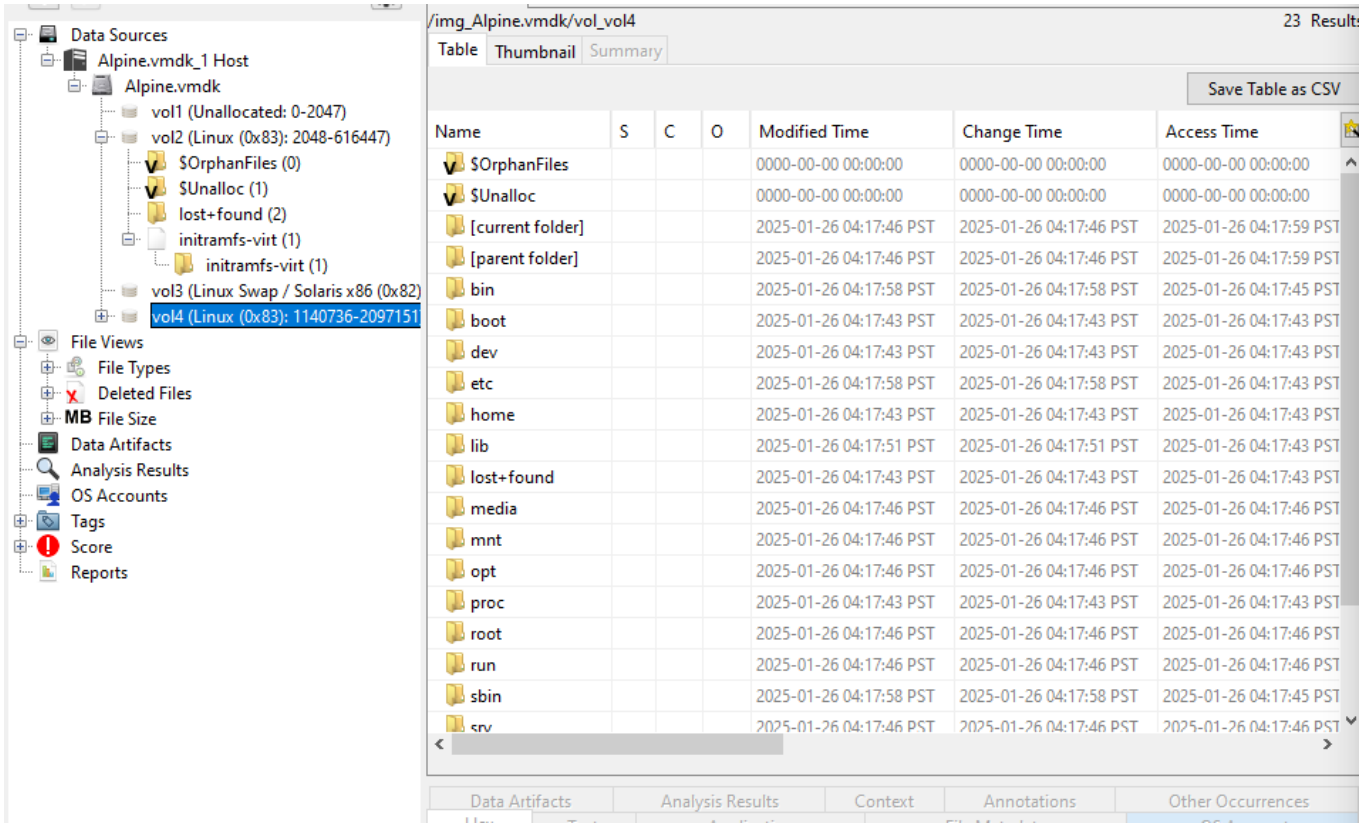

New Case Information
Steps
1. Case Information
2. Optional Information
Optional Information
Case
Number: 1
Examiner
Name: bharath
Phone: NA
Email: a@a.com
Notes: linux non volatile
Organization
Organization analysis is being done for: Not Specified
Manage Organizations
< Back
Next >
Finish
Cancel
Help

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

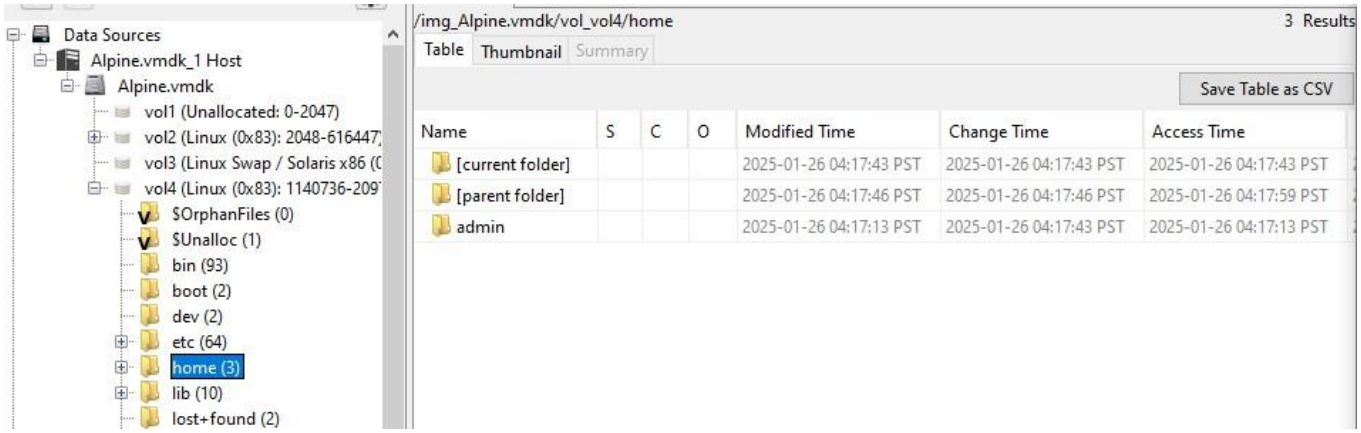


The tool will display the results after analysis. Expand the Data Sources. Click the image name, here

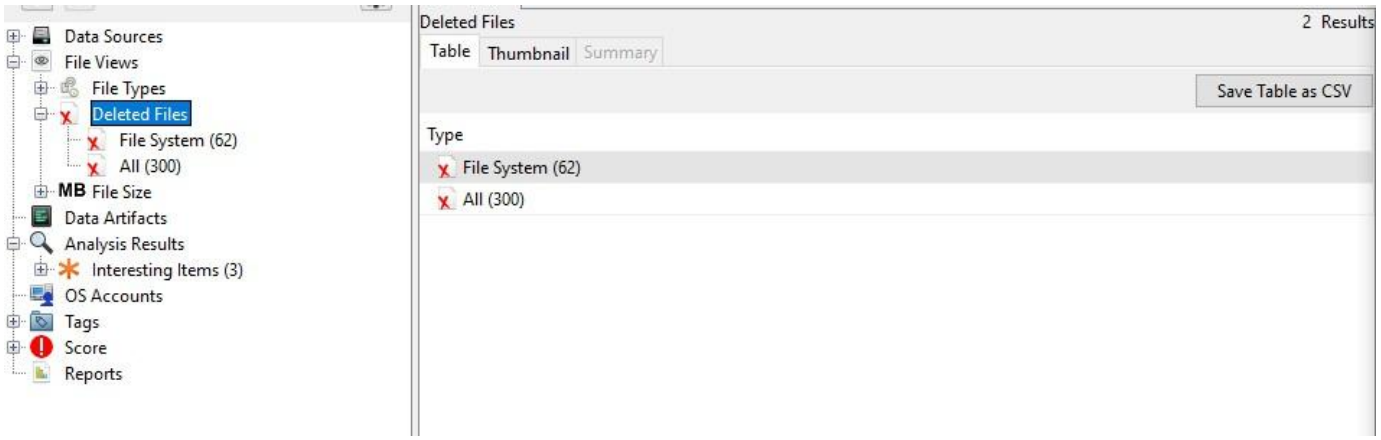




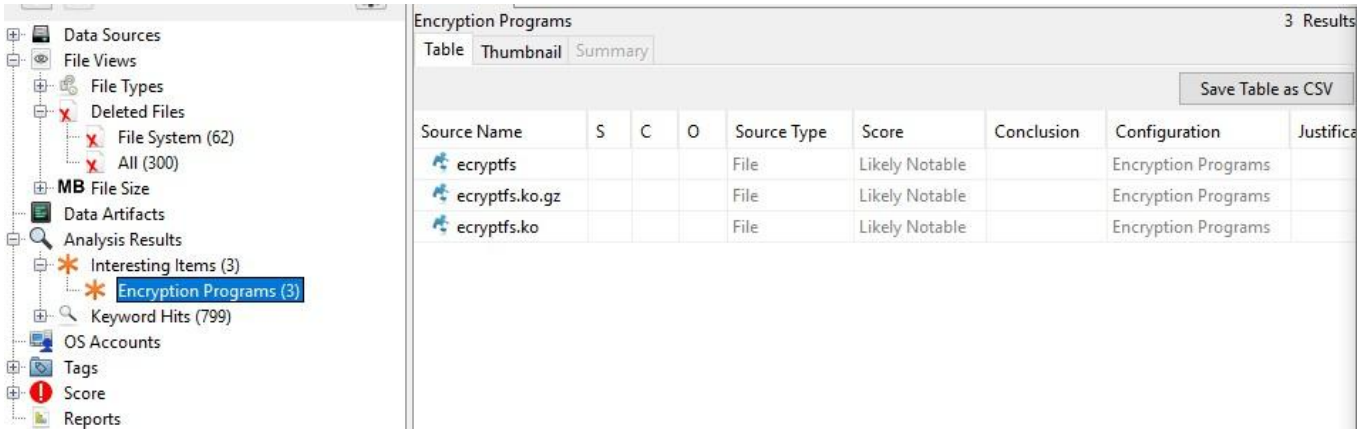
home folder stores the details of the user home directory



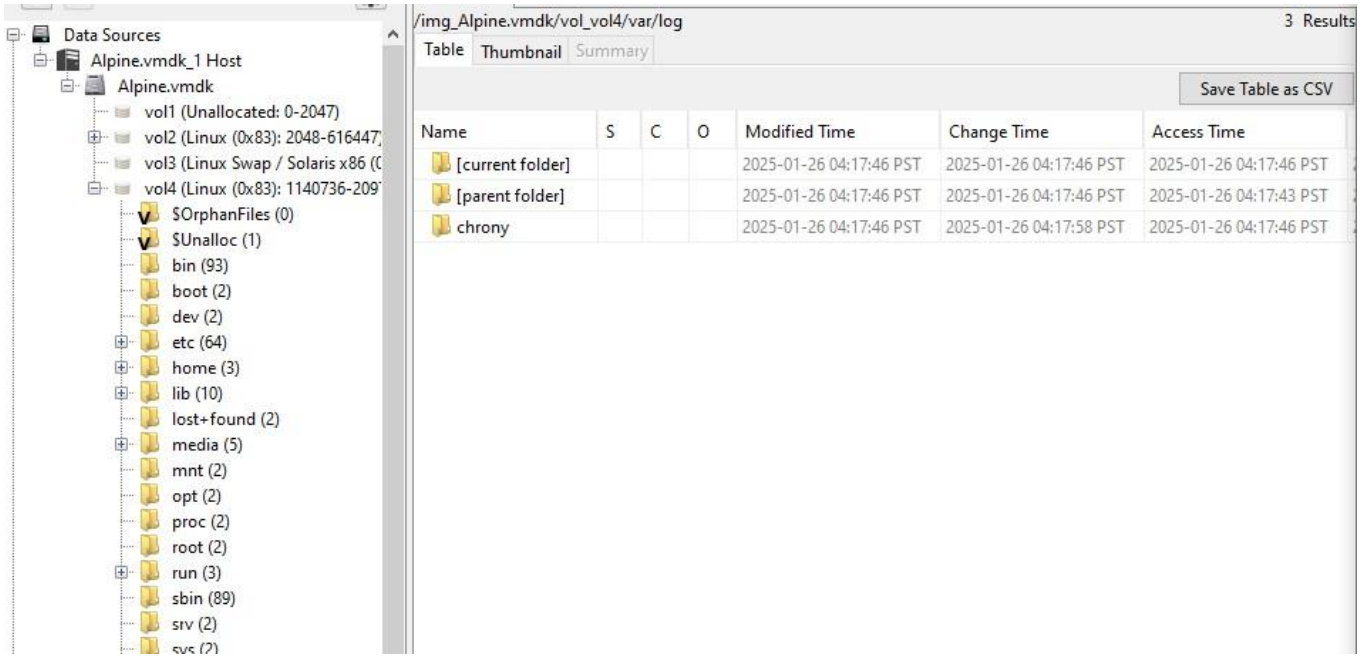
File views option has the deleted files option to view all the deleted files.



Select the results folder . It contains encrypted content.



/var/log will have the syslog



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