UNIVERSITY OF SCIENCE AND TECHNOLOGY OF HANOI

Information and Communication Technology Department

Lab Work Day 6

Digital Forensic

Name - ID: Đào Ngọc Tùng BA12-185

Trần Đức Trung BA12-179

Phạm Phú Hưng BA12-081

Nguyễn Tiến Ngọc BA12-140

Ha Noi, November 2024

Lab 1: Acquiring Volatile Information from a Live Windows System

To collect information about logged-on users, opened files, and running processes on a live Windows system.

Tools Required: PsLoggedon, LogonSessions, NetworkOpenedFiles.

Steps1: Identify Logged-On Users

Open Command Prompt with Administrator privileges.

`PsLoggedon64.exe`

This will display:

Locally logged-on users.

Users connected via shared resources.

Steps 2: List Active Login Sessions

Navigate to the directory containing the LogonSessions tool.

`LogonSessions64.exe -p`

This will show active login sessions, their types, and processes associated with each session.

Check Files Opened Over the Network

Launch the `NetworkOpenedFiles.exe` tool.

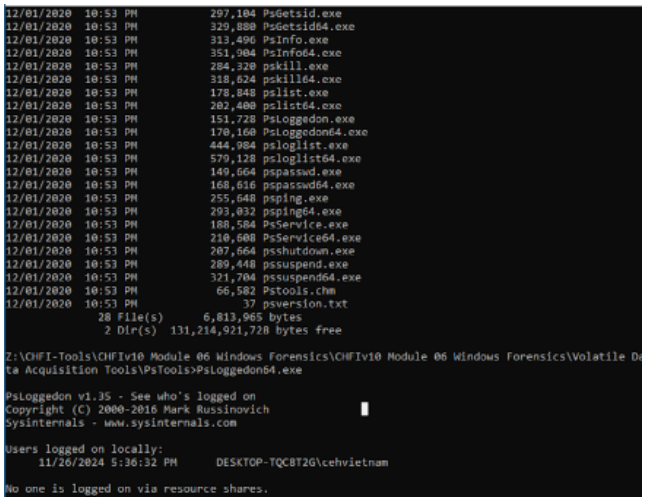
This displays details about shared files and folders accessed remotely, including:

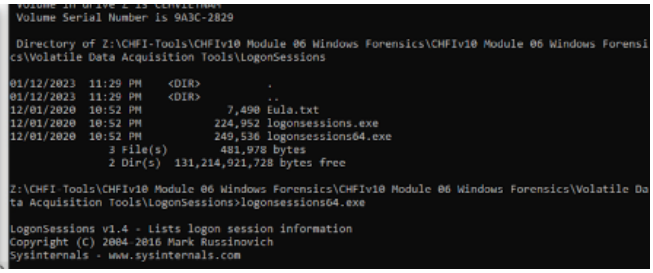
File paths.

IP addresses of remote computers.

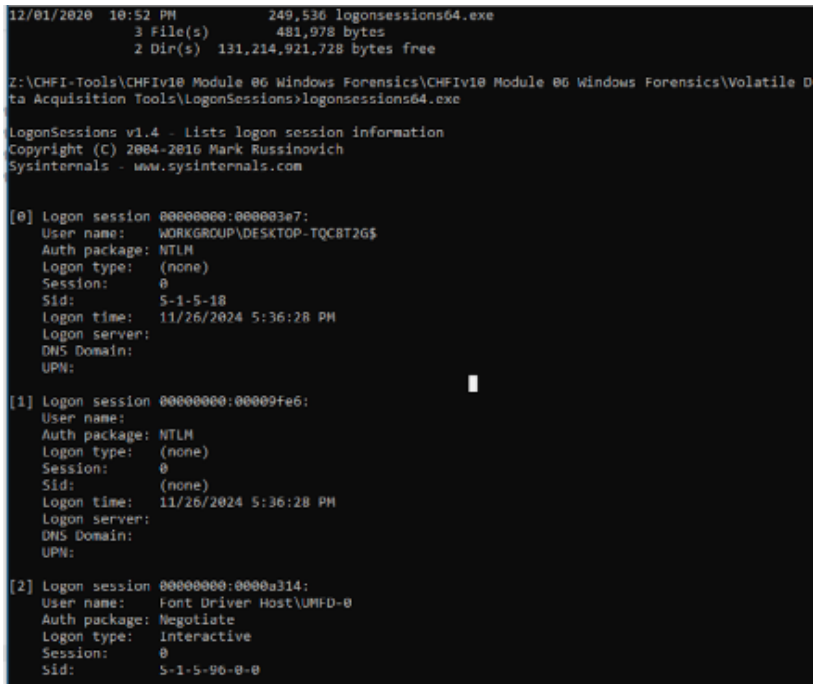
Usernames and permissions.

The Command Prompt window will display that the local user is logged in as the Administrator of the local machine.

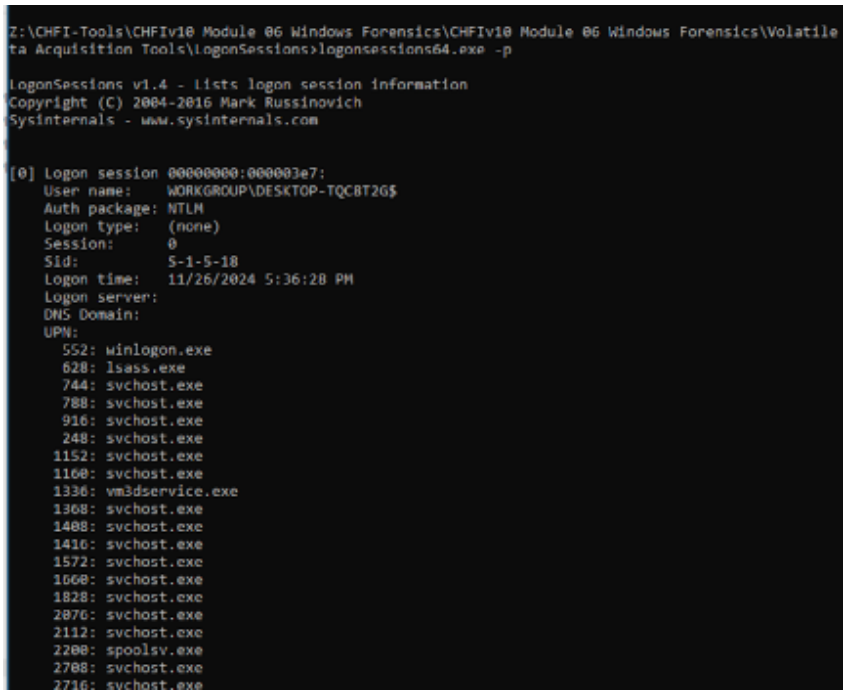




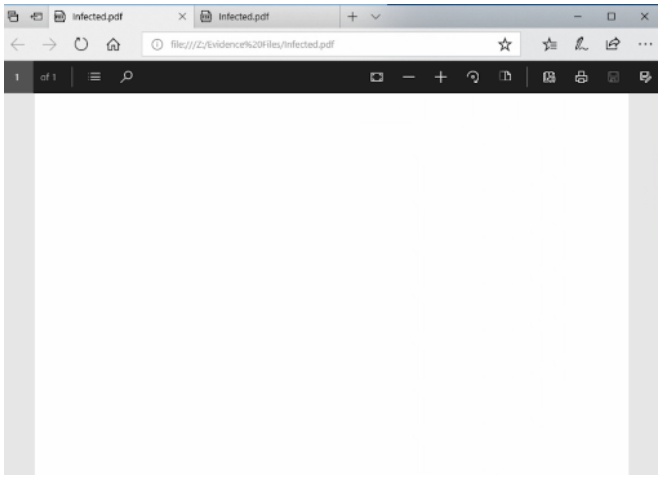
Open Command Prompt, navigate to the directory containing LogonSessions, type `LogonSessions64.exe`, and press Enter.



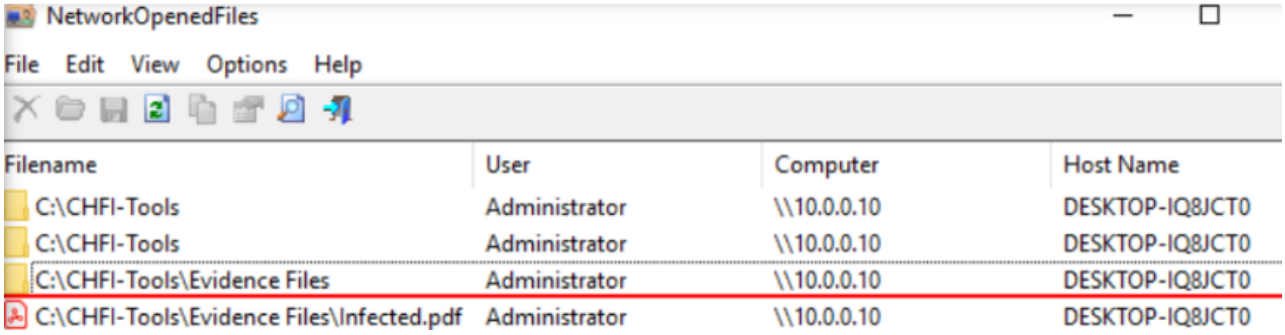
LList the currently active login sessions

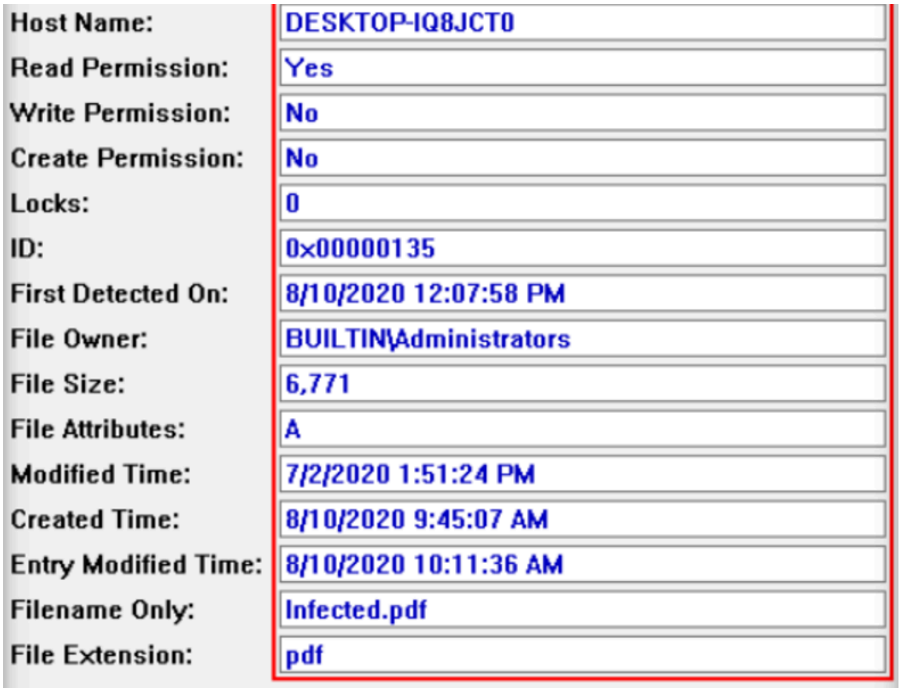


All running processes associated with each session will be listed under the UPN (User Principal Name) section.



Open file infected.pdf





Host Name:	DESKTOP-IQ8JCT0
Read Permission:	Yes
Write Permission:	No
Create Permission:	No
Locks:	0
ID:	0x00000135
First Detected On:	8/10/2020 12:07:58 PM
File Owner:	BUILTIN\Administrators
File Size:	6,771
File Attributes:	A
Modified Time:	7/2/2020 1:51:24 PM
Created Time:	8/10/2020 9:45:07 AM
Entry Modified Time:	8/10/2020 10:11:36 AM
Filename Only:	Infected.pdf
File Extension:	pdf

To run NetworkOpenedFiles, switch to the Windows Server 2016 virtual machine. Navigate to `C:\CHFI-Tools\CHFIv10 Module 06 Windows Forensics\Volatile Data Acquisition Tools\NetworkOpenedFiles` and double-click `NetworkOpenedFiles.exe`. This will display the shared folders and files that have been accessed (e.g., CHFI-Tools, Evidence Files, and Infected.pdf), along with details such as the IP address of the remote computer and the user accessing them. Double-clicking on a file, such as `Infected.pdf`, will open the Properties window, revealing all associated details of the file.

Lab 2: Investigating RAM Using Redline and Volatility

Objective

To analyze memory dumps to identify malicious activities or suspicious processes.

Tools Required

Redline

Volatility

Steps

1. **Analyze Memory with Redline**

   Install and launch Redline.

   Choose the option *From a Saved Memory File*, and select the RAM dump file (`Windows_RAM.mem`).

   Allow the tool to complete its analysis.

   Review results, focusing on:

      Process hierarchy to identify parent-child relationships.

      Suspicious network connections, such as `rundll32.exe`.

2. **Analyze Memory with Volatility**

Open Command Prompt and navigate to the Volatility folder.

Use the `imageinfo` command to determine the appropriate profile:

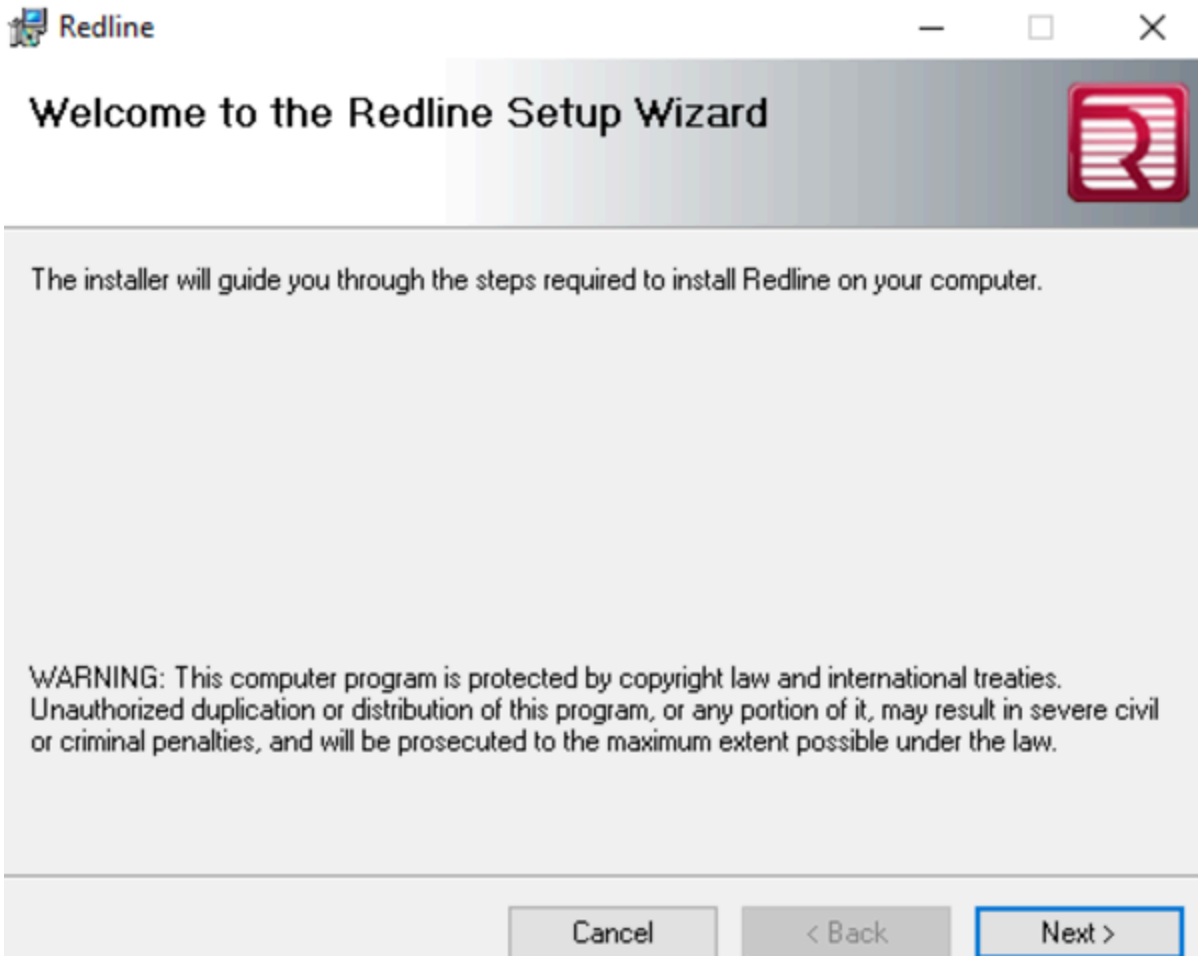
```
volatility_2.6_win64_standalone.exe -f
"C:\path\to\Windows_RAM.mem" imageinfo
```

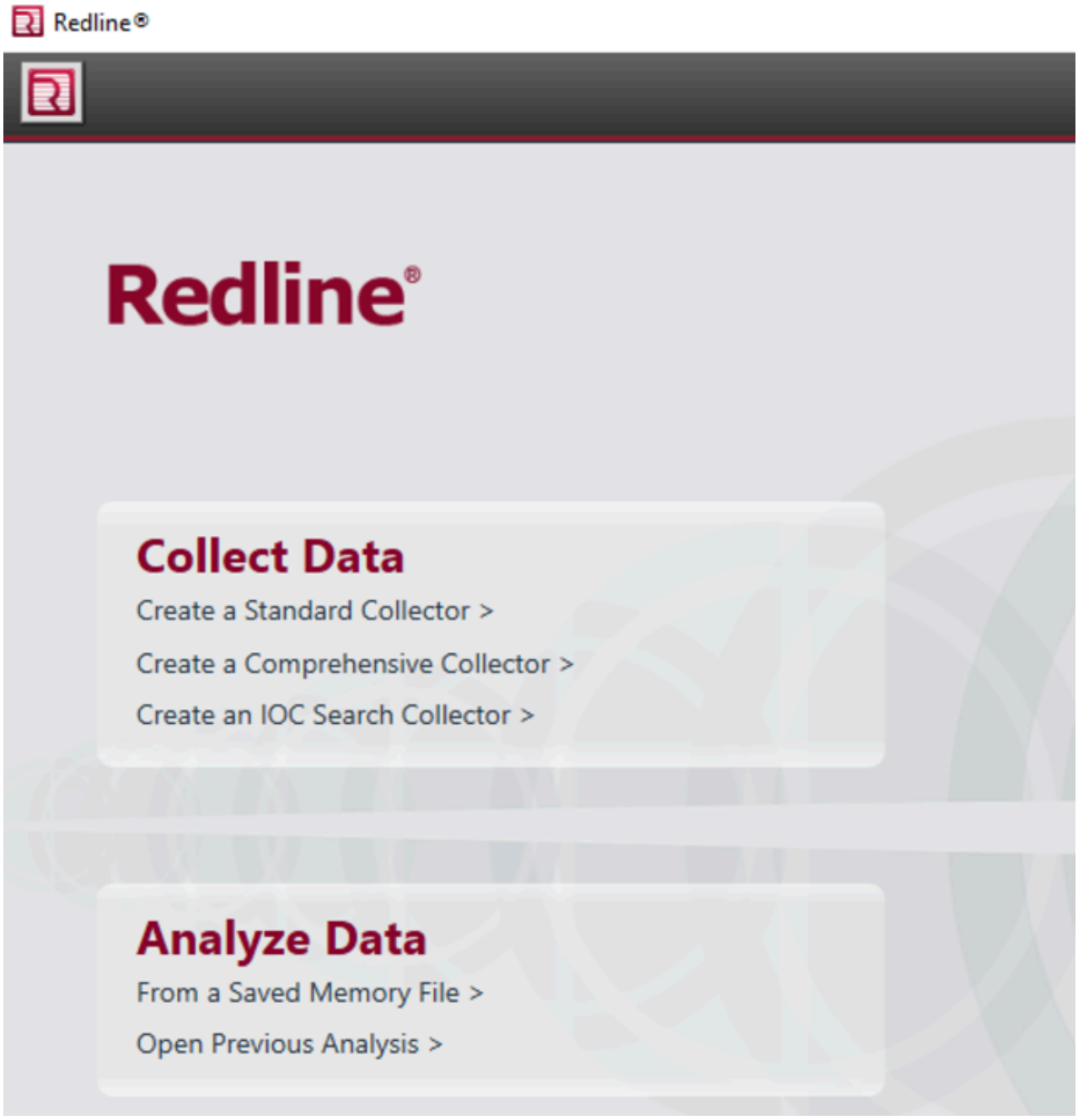
Use plugins like:

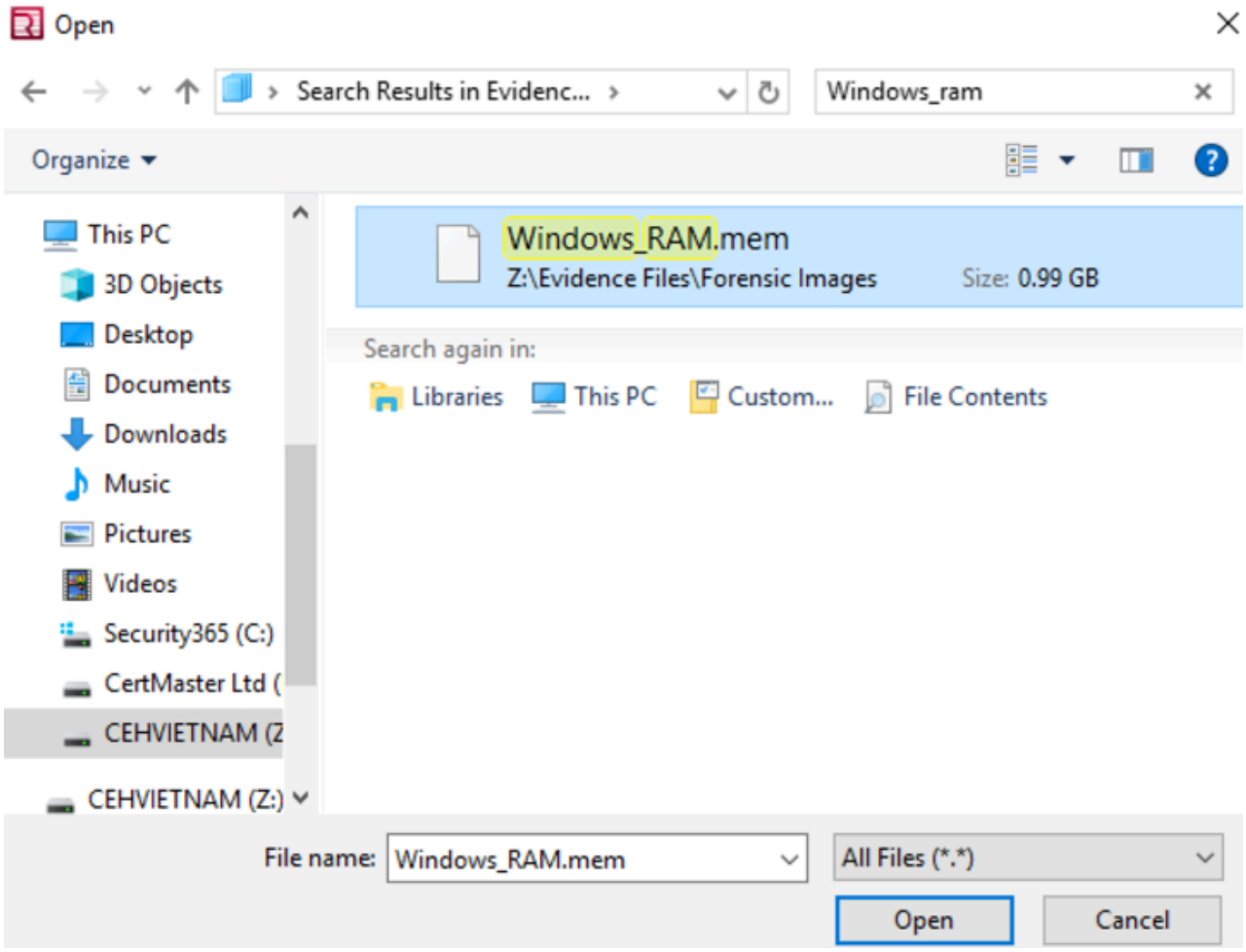
`netscan` to identify network connections.

`pstree` to view process trees.

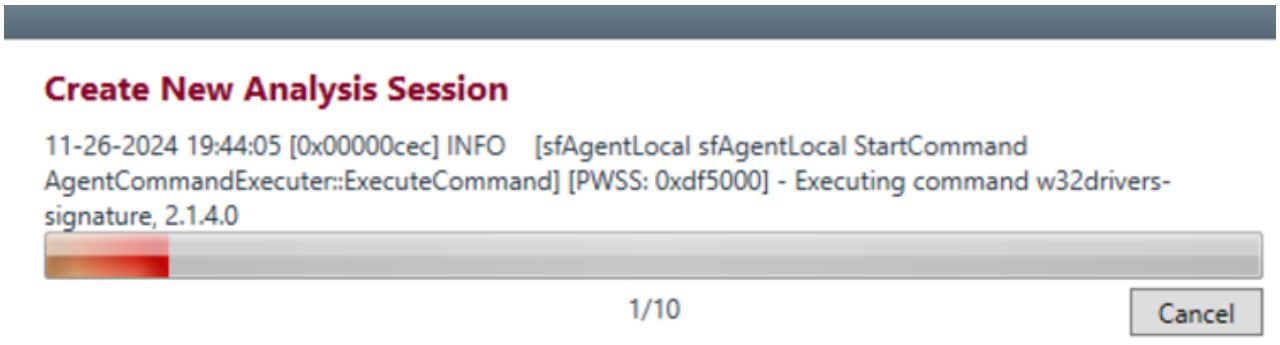
Investigate suspicious processes by their PID.

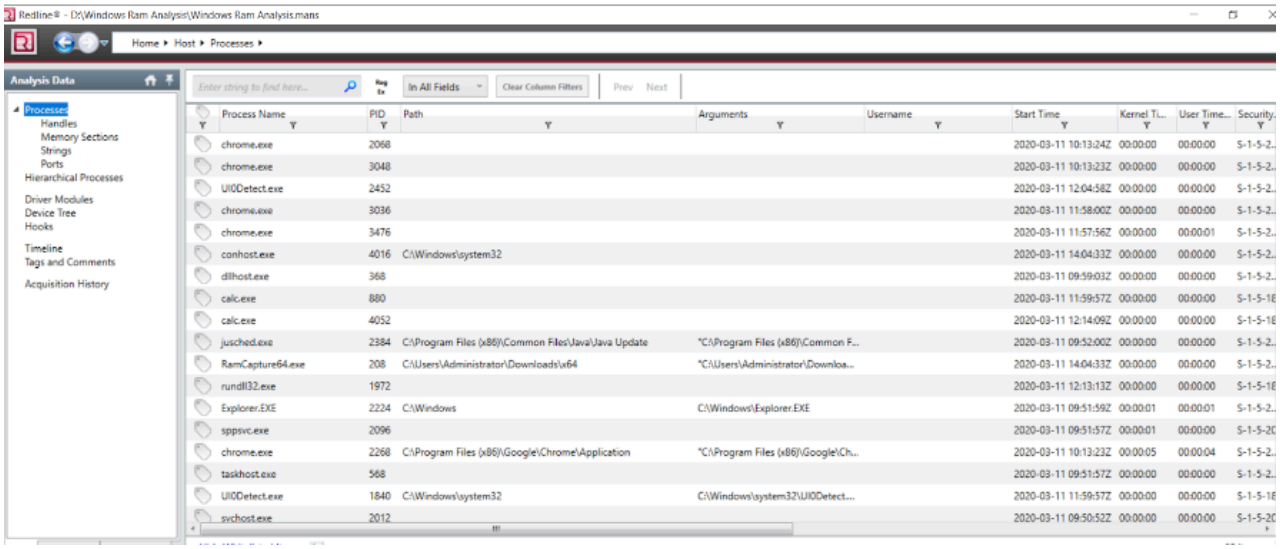

Redline
Welcome to the Redline Setup Wizard
The installer will guide you through the steps required to install Redline on your computer.
WARNING: This computer program is protected by copyright law and international treaties. Unauthorized duplication or distribution of this program, or any portion of it, may result in severe civil or criminal penalties, and will be prosecuted to the maximum extent possible under the law.
Cancel
< Back
Next >

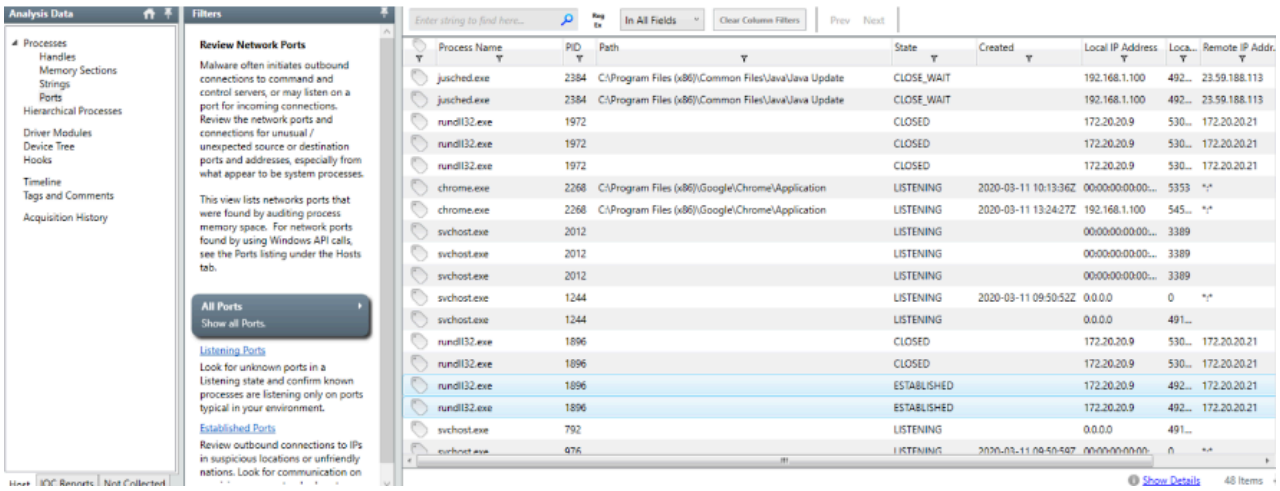

Redline®
Redline®
Collect Data
Create a Standard Collector >
Create a Comprehensive Collector >
Create an IOC Search Collector >
Analyze Data
From a Saved Memory File >
Open Previous Analysis >

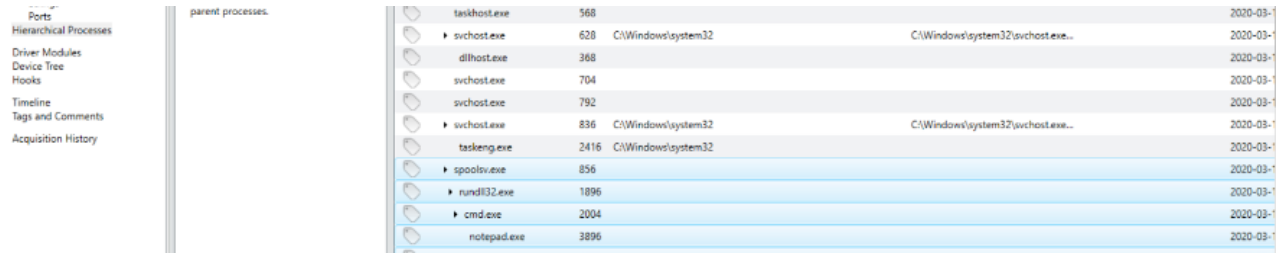

Open
Search Results in Evidenc...
Windows_ram
Organize
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Security365 (C:)
CertMaster Ltd (
CEHVIETNAM (Z
CEHVIETNAM (Z:)
Windows_RAM.mem
Z:\Evidence Files\Forensic Images
Size: 0.99 GB
Search again in:
Libraries
This PC
Custom...
File Contents
File name: Windows_RAM.mem
All Files (*.*)
Open
Cancel

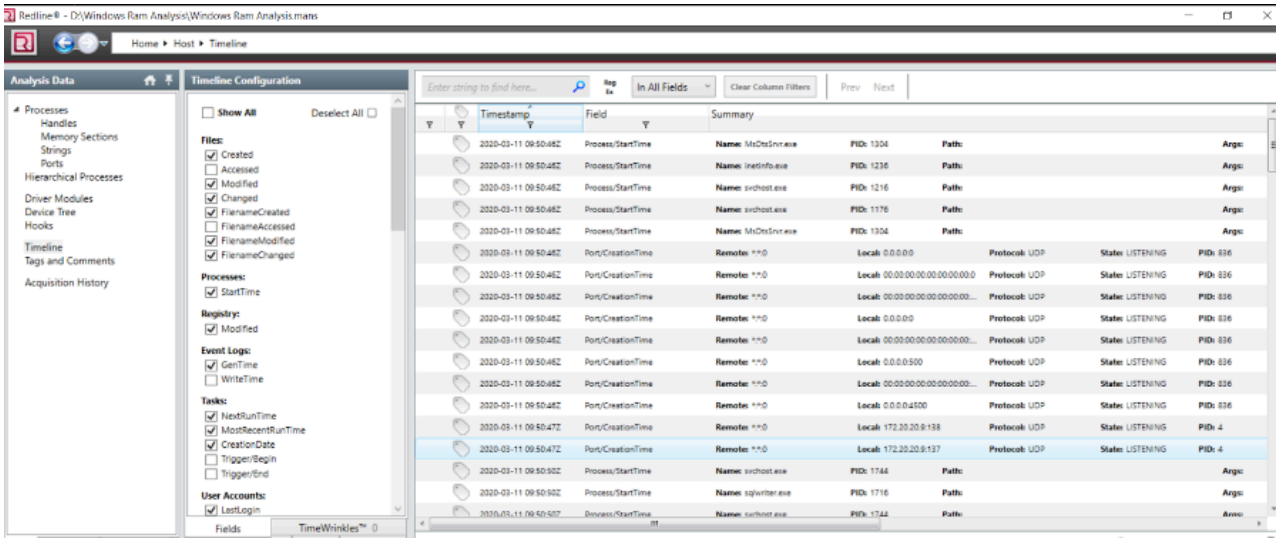

Save Your Analysis Session To:
Name: Windows Ram Analysis
Location: C:\Users\cehvietnam\Documents
Browse
Cancel
Back
OK


Create New Analysis Session
11-26-2024 19:44:05 [0x00000cec] INFO [sfAgentLocal sfAgentLocal StartCommand AgentCommandExecuter::ExecuteCommand] [PWSS: 0xdf5000] - Executing command w32drivers-signature, 2.1.4.0
1/10
Cancel


Redline® - D:\Windows Ram Analysis\Windows Ram Analysis.mans
Home ▸ Host ▸ Processes ▸
Analysis Data
Processes
Handles
Memory Sections
Strings
Ports
Hierarchical Processes
Driver Modules
Device Tree
Hooks
Timeline
Tags and Comments
Acquisition History
Enter string to find here...
In All Fields
Clear Column Filters
Prev
Next
Process Name | PID | Path | Arguments | Username | Start Time | Kernel Ti... | User Time... | Security...
chrome.exe 2068 2020-03-11 10:13:24Z 00:00:00 00:00:00 S-1-5-2..
chrome.exe 3048 2020-03-11 10:13:23Z 00:00:00 00:00:00 S-1-5-2..
UI0Detect.exe 2452 2020-03-11 12:04:58Z 00:00:00 00:00:00 S-1-5-2..
chrome.exe 3036 2020-03-11 11:58:00Z 00:00:00 00:00:00 S-1-5-2..
chrome.exe 3476 2020-03-11 11:57:56Z 00:00:00 00:00:01 S-1-5-2..
conhost.exe 4016 C:\Windows\system32 2020-03-11 14:04:33Z 00:00:00 00:00:00 S-1-5-2..
dllhost.exe 368 2020-03-11 09:59:03Z 00:00:00 00:00:00 S-1-5-2..
calc.exe 880 2020-03-11 11:59:57Z 00:00:00 00:00:00 S-1-5-18
calc.exe 4052 2020-03-11 12:14:09Z 00:00:00 00:00:00 S-1-5-18
jusched.exe 2384 C:\Program Files (x86)\Common Files\Java\Java Update "C:\Program Files (x86)\Common F... 2020-03-11 09:52:00Z 00:00:00 00:00:00 S-1-5-2..
RamCapture64.exe 208 C:\Users\Administrator\Downloads\x64 "C:\Users\Administrator\Downloa... 2020-03-11 14:04:33Z 00:00:00 00:00:00 S-1-5-2..
rundll32.exe 1972 2020-03-11 12:13:13Z 00:00:00 00:00:00 S-1-5-18
Explorer.EXE 2224 C:\Windows C:\Windows\Explorer.EXE 2020-03-11 09:51:59Z 00:00:01 00:00:01 S-1-5-2..
sppsvc.exe 2096 2020-03-11 09:51:57Z 00:00:01 00:00:00 S-1-5-20
chrome.exe 2268 C:\Program Files (x86)\Google\Chrome\Application "C:\Program Files (x86)\Google\Ch... 2020-03-11 10:13:23Z 00:00:05 00:00:04 S-1-5-2..
taskhost.exe 568 2020-03-11 09:51:57Z 00:00:00 00:00:00 S-1-5-2..
UI0Detect.exe 1840 C:\Windows\system32 C:\Windows\system32\UI0Detect... 2020-03-11 11:59:57Z 00:00:00 00:00:00 S-1-5-18
svchost.exe 2012 2020-03-11 09:50:52Z 00:00:00 00:00:00 S-1-5-20


Analysis Data
Processes
Handles
Memory Sections
Strings
Ports
Hierarchical Processes
Driver Modules
Device Tree
Hooks
Timeline
Tags and Comments
Acquisition History
Filters
Review Network Ports
Malware often initiates outbound connections to command and control servers, or may listen on a port for incoming connections. Review the network ports and connections for unusual / unexpected source or destination ports and addresses, especially from what appear to be system processes.
This view lists networks ports that were found by auditing process memory space. For network ports found by using Windows API calls, see the Ports listing under the Hosts tab.
All Ports
Show all Ports.
Listening Ports
Look for unknown ports in a Listening state and confirm known processes are listening only on ports typical in your environment.
Established Ports
Review outbound connections to IPs in suspicious locations or unfriendly nations. Look for communication on
Enter string to find here...
In All Fields
Clear Column Filters
Prev
Next
Process Name | PID | Path | State | Created | Local IP Address | Loca... | Remote IP Addr...
jusched.exe 2384 C:\Program Files (x86)\Common Files\Java\Java Update CLOSE_WAIT 192.168.1.100 492... 23.59.188.113
jusched.exe 2384 C:\Program Files (x86)\Common Files\Java\Java Update CLOSE_WAIT 192.168.1.100 492... 23.59.188.113
rundll32.exe 1972 CLOSED 172.20.20.9 530... 172.20.20.21
rundll32.exe 1972 CLOSED 172.20.20.9 530... 172.20.20.21
rundll32.exe 1972 CLOSED 172.20.20.9 530... 172.20.20.21
chrome.exe 2268 C:\Program Files (x86)\Google\Chrome\Application LISTENING 2020-03-11 10:13:36Z 5353 *:*
chrome.exe 2268 C:\Program Files (x86)\Google\Chrome\Application LISTENING 2020-03-11 13:24:27Z 192.168.1.100 545... *:*
svchost.exe 2012 LISTENING 3389
svchost.exe 2012 LISTENING 3389
svchost.exe 2012 LISTENING 3389
svchost.exe 1244 LISTENING 2020-03-11 09:50:52Z 0.0.0.0 0 *:*
svchost.exe 1244 LISTENING 0.0.0.0 491...
rundll32.exe 1896 CLOSED 172.20.20.9 530... 172.20.20.21
rundll32.exe 1896 CLOSED 172.20.20.9 530... 172.20.20.21
rundll32.exe 1896 ESTABLISHED 172.20.20.9 492... 172.20.20.21
rundll32.exe 1896 ESTABLISHED 172.20.20.9 492... 172.20.20.21
svchost.exe 792 LISTENING 0.0.0.0 491...
Show Details
48 Items


Ports
Hierarchical Processes
Driver Modules
Device Tree
Hooks
Timeline
Tags and Comments
Acquisition History
parent processes.
taskhost.exe 568 2020-03-1
svchost.exe 628 C:\Windows\system32 C:\Windows\system32\svchost.exe... 2020-03-1
dllhost.exe 368 2020-03-1
svchost.exe 704 2020-03-1
svchost.exe 792 2020-03-1
svchost.exe 836 C:\Windows\system32 C:\Windows\system32\svchost.exe... 2020-03-1
taskeng.exe 2416 C:\Windows\system32 2020-03-1
spoolsv.exe 856 2020-03-1
rundll32.exe 1896 2020-03-1
cmd.exe 2004 2020-03-1
notepad.exe 3896 2020-03-1




```
Z:\CHFI-Tools\CHFIv10 Module 06 Windows Forensics\CHFIv10 Module 06 Windows Forensics\Memo
ry Forensics Tools\Volatility>volatility_2.6_win64_standalone.exe -f "Z:\Evidence Files\Fo
rensic Images\Windows_Ram.mem" imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_
23418, Win2008R2SP1x64, Win7SP1x64_23418
                     AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (Z:\Evidence Files\Forensic Images\Windo
ws_Ram.mem)
                      PAE type : No PAE
                           DTB : 0x187000L
                          KDBG : 0xf8000164e0a0L
          Number of Processors : 1
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0xfffff8000164fd00L
             KUSER_SHARED_DATA : 0xfffff78000000000L
           Image date and time : 2020-03-11 14:04:34 UTC+0000
     Image local date and time : 2020-03-11 07:04:34 -0700
```

```
Z:\CHFI-Tools\CHFIv10 Module 06 Windows Forensics\CHFIv10 Module 06 Windows Forensics\Memory
 Forensics Tools\Volatility>volatility_2.6_win64_standalone.exe -f "Z:\Evidence Files\Forens
ic Images\Windows_Ram.mem" kdbgscan
Volatility Foundation Volatility Framework 2.6
**************************************************
Instantiating KDBG using: Z:\Evidence Files\Forensic Images\Windows_Ram.mem WinXPSP2x86 (5.1
.0 32bit)
Offset (P)                    : 0x164e0a0
KDBG owner tag check          : True
Profile suggestion (KDBGHeader): Win7SP1x64
PsActiveProcessHead           : 0x1684370
PsLoadedModuleList            : 0x16a2670
KernelBase                    : 0xfffff8000145e000

**************************************************
Instantiating KDBG using: Z:\Evidence Files\Forensic Images\Windows_Ram.mem WinXPSP2x86 (5.1
.0 32bit)
Offset (P)                    : 0x164e0a0
KDBG owner tag check          : True
Profile suggestion (KDBGHeader): Win2008R2SP1x64
PsActiveProcessHead           : 0x1684370
PsLoadedModuleList            : 0x16a2670
KernelBase                    : 0xfffff8000145e000
```

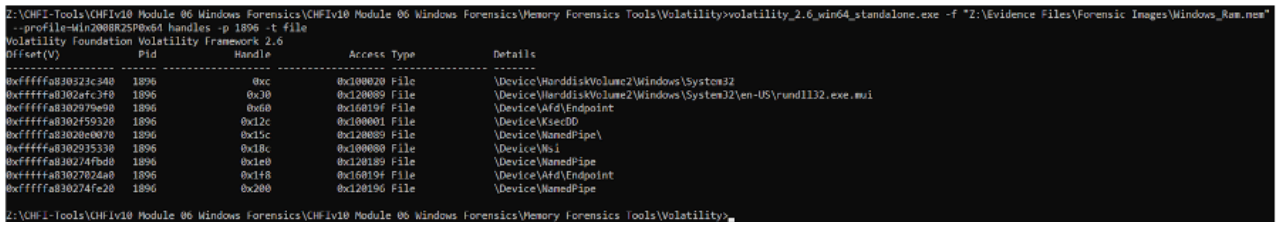
Administrator: Command Prompt

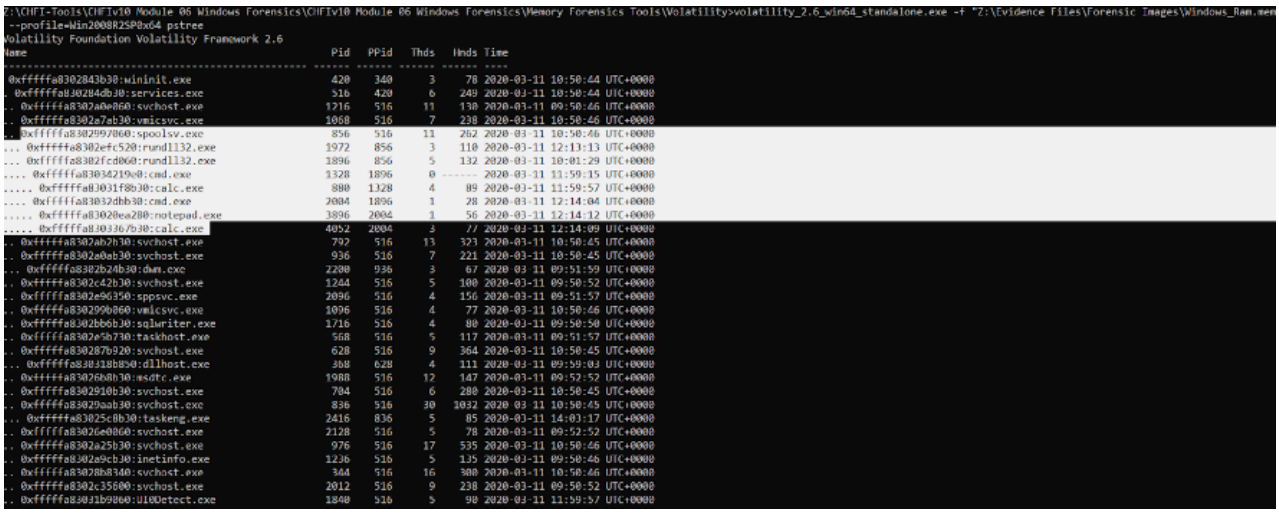
```
Z:\CHFI-Tools\CHFIv10 Module 06 Windows Forensics\CHFIv10 Module 06 Windows Forensics\Memory Forensics Tools\Volatili
ty>volatility_2.6_win64_standalone.exe -f "Z:\Evidence Files\Forensic Images\Windows_Ram.mem" --profile=Win2008R2SP0x
64 netscan
Volatility Foundation Volatility Framework 2.6
Offset(P)          Proto    Local Address                  Foreign Address      State          Pid      Owner
    Created
0xb3f9ec0          UDPv4    0.0.0.0:5353                   *:*                                 2268     chrome.exe
    2020-03-11 10:13:36 UTC+0000
0xb3f9ec0          UDPv6    :::5353                        *:*                                 2268     chrome.exe
    2020-03-11 10:13:36 UTC+0000
0xd2447e0          TCPv4    172.20.20.9:53073              172.20.20.21:4444    CLOSED         1896     rundll32.ex
e
0xd3877e0          TCPv4    172.20.20.9:53073              172.20.20.21:4444    CLOSED         1896     rundll32.ex
e
0xd55b8c0          TCPv4    192.168.1.100:53082            52.237.132.211:443   ESTABLISHED    2140     chrome.exe
0xd6951f0          TCPv4    172.20.20.9:53074              172.20.20.21:4444    CLOSED         1972     rundll32.ex
e
0x10adc3a0         TCPv4    192.168.1.100:53083            52.237.132.211:443   ESTABLISHED    2140     chrome.exe
0x11cbe010         TCPv4    -:52978                        52.237.132.211:443   CLOSED         2140     chrome.exe
0x12277010         TCPv4    192.168.1.100:49200            23.59.188.113:80     CLOSE_WAIT     2384     jusched.exe

0x14781a90         TCPv4    192.168.1.100:49201            23.59.188.113:80     CLOSE_WAIT     2436     jucheck.exe

0x14c53ec0         UDPv4    0.0.0.0:5353                   *:*                                 2140     chrome.exe
    2020-03-11 11:58:18 UTC+0000
0x14c53ec0         UDPv6    :::5353                        *:*                                 2140     chrome.exe
    2020-03-11 11:58:18 UTC+0000
0x15fa11f0         TCPv4    172.20.20.9:53074              172.20.20.21:4444    CLOSED         1972     rundll32.ex
e
```

```
0x30ad5cf0       TCPv4    172.20.20.9:49227              172.20.20.21:4444    ESTABLISHED    1896     rundll32.exe
0x32254ec0       UDPv4    192.168.1.100:137              *:*                                 4        System         2020-03-11 09:50:59 UTC+0000
0x331f6cf0       TCPv4    :0                             56.171.154.2:0       CLOSED         976      svchost.exe
0x3422a810       TCPv4    0.0.0.0:49157                  0.0.0.0:0            LISTENING      524      lsass.exe
0x3422a810       TCPv6    :::49157                       :::0                 LISTENING      524      lsass.exe
0x3422a930       TCPv4    0.0.0.0:49157                  0.0.0.0:0            LISTENING      524      lsass.exe
0x34cb08d0       TCPv6    -:0                            38ab:9a02:83fa:ffff:38ab:9a02:83fa:ffff:0 CLOSED          976      svchost.exe
0x35420ec0       UDPv4    0.0.0.0:0                      *:*                                 33619969                  2020-03-11 09:52:15 UTC+0000
0x35420ec0       UDPv6    :::0                           *:*                                 33619969                  2020-03-11 09:52:15 UTC+0000
0x362ab970       TCPv4    0.0.0.0:49155                  0.0.0.0:0            LISTENING      516      services.exe
0x362ab970       TCPv6    :::49155                       :::0                 LISTENING      516      services.exe
0x37765010       TCPv4    :53000                         52.237.132.211:443   CLOSED         2140     chrome.exe
0x38381010       UDPv4    0.0.0.0:0                      *:*                                 976      svchost.exe    2020-03-11 09:50:59 UTC+0000
0x38381010       UDPv6    :::0                           *:*                                 976      svchost.exe    2020-03-11 09:50:59 UTC+0000
0x37b3a6e0       TCPv4    192.168.1.100:53085            52.114.75.79:443     CLOSED         2140     chrome.exe
0x37ed3cf0       TCPv4    -:0                            56.171.154.2:0       CLOSED         976      svchost.exe
```





Lab 3: Examining Web Browser Artifacts

Objective

To retrieve browsing history, cookies, and cache data from web browsers.

Tools Required

- ChromeCacheView, ChromeHistoryView, ChromeCookiesView
- MZCacheView, MZHistoryView, MZCookiesView

Steps

1. **Analyze Chrome Artifacts**
    - Use the following tools:
        - `ChromeCacheView` for cache data.
        - `ChromeHistoryView` for browsing history.

        - `ChromeCookiesView` for cookies.
2. **Analyze Firefox Artifacts**
    - Use the following tools:
        - `MZCacheView` for cache data.
        - `MZHistoryView` for browsing history.
        - `MZCookiesView` for cookies.

Lab 4: Discovering and Extracting Forensic Data

Objective

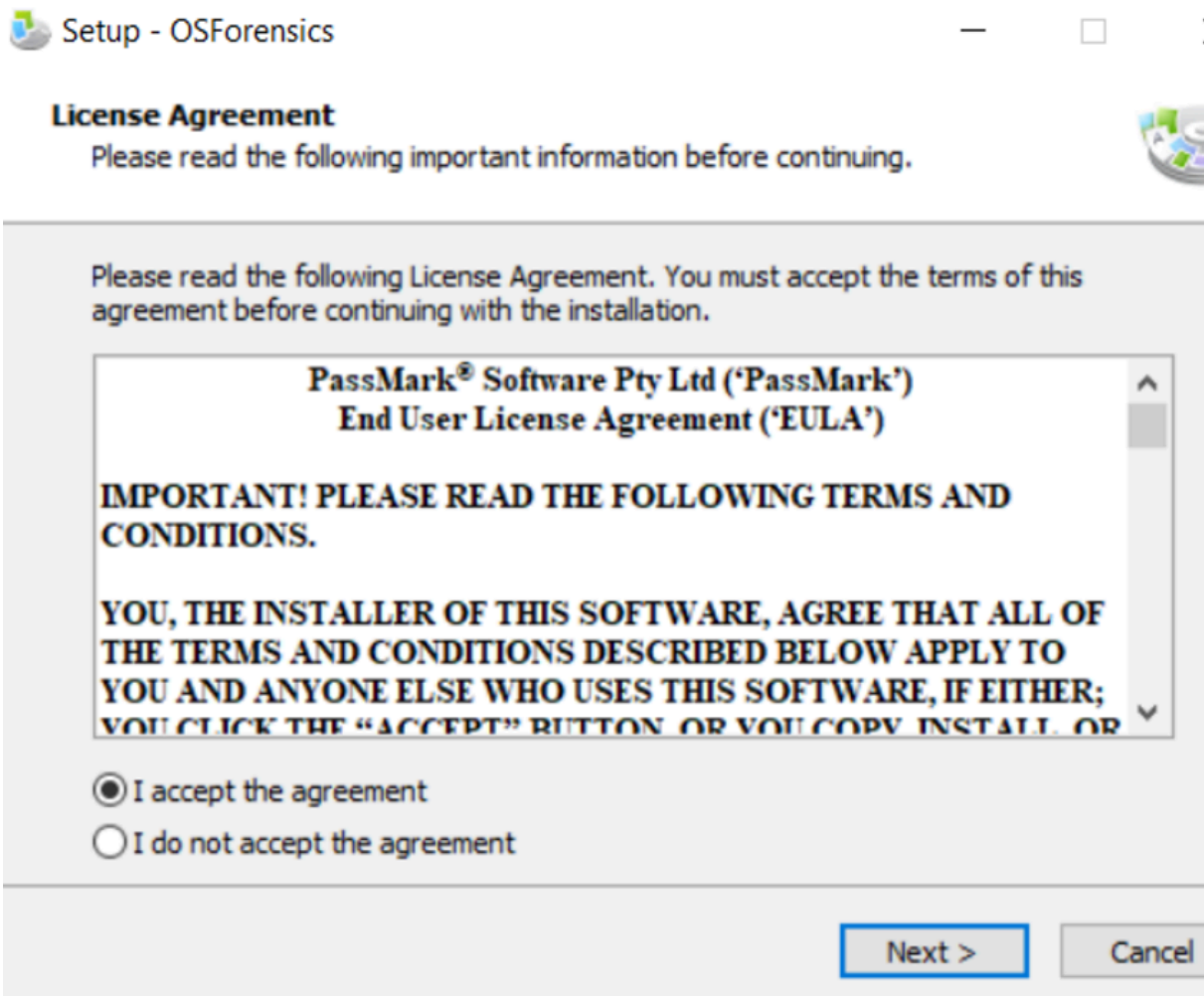
To locate evidence on a suspect's computer using OSForensics.

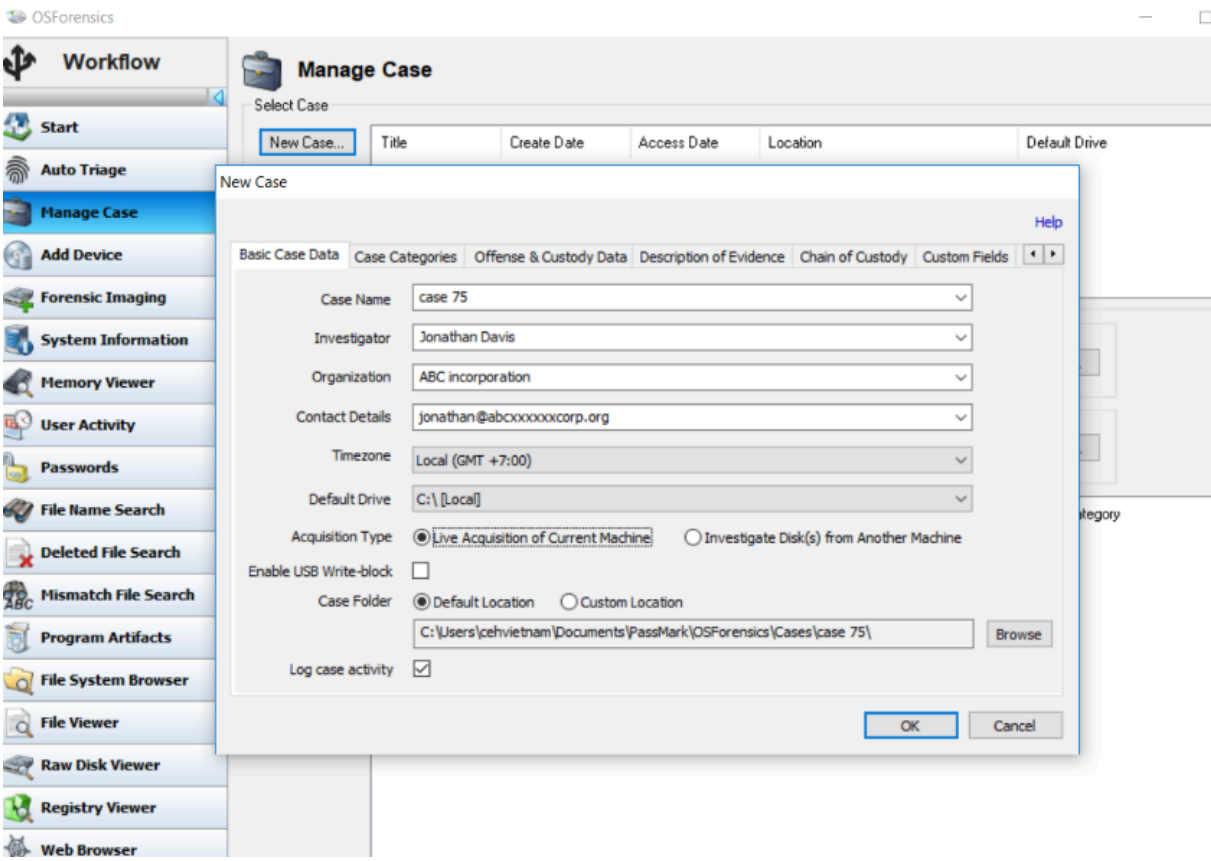
Tools Required

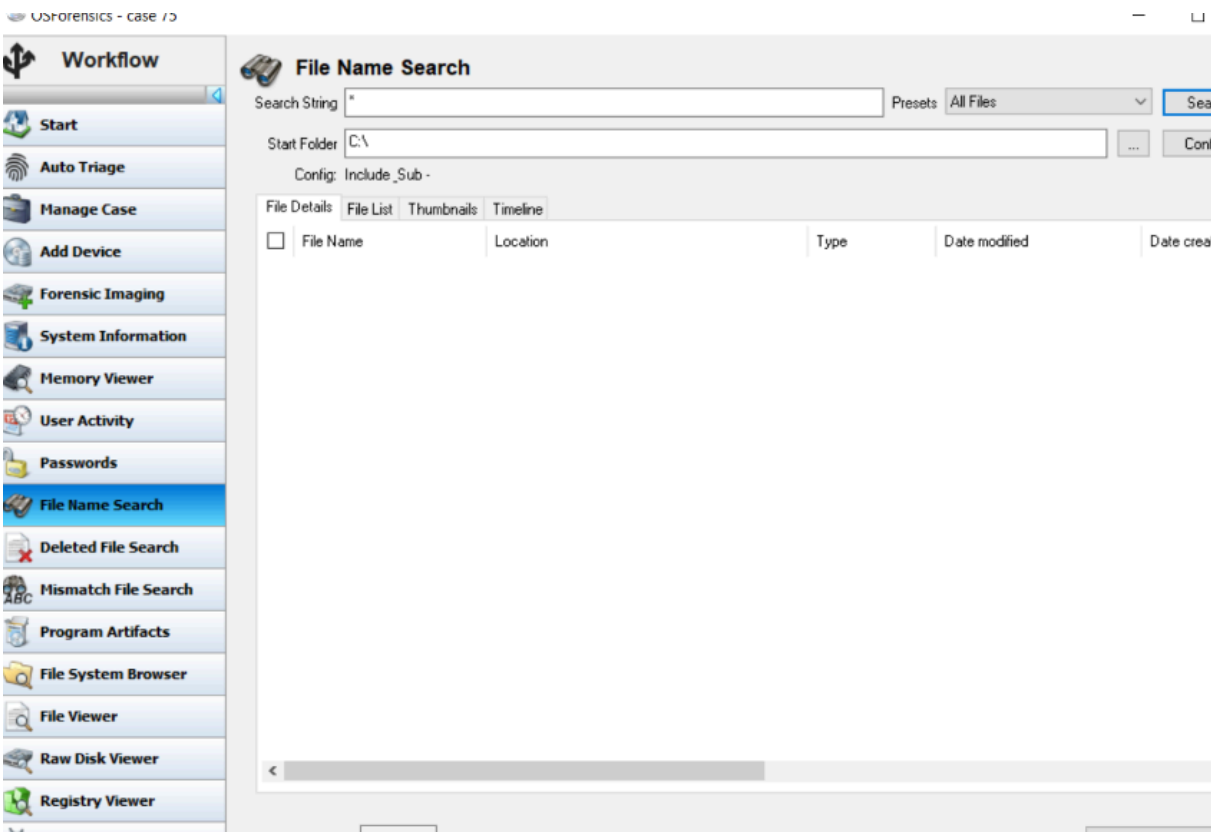
- OSForensics

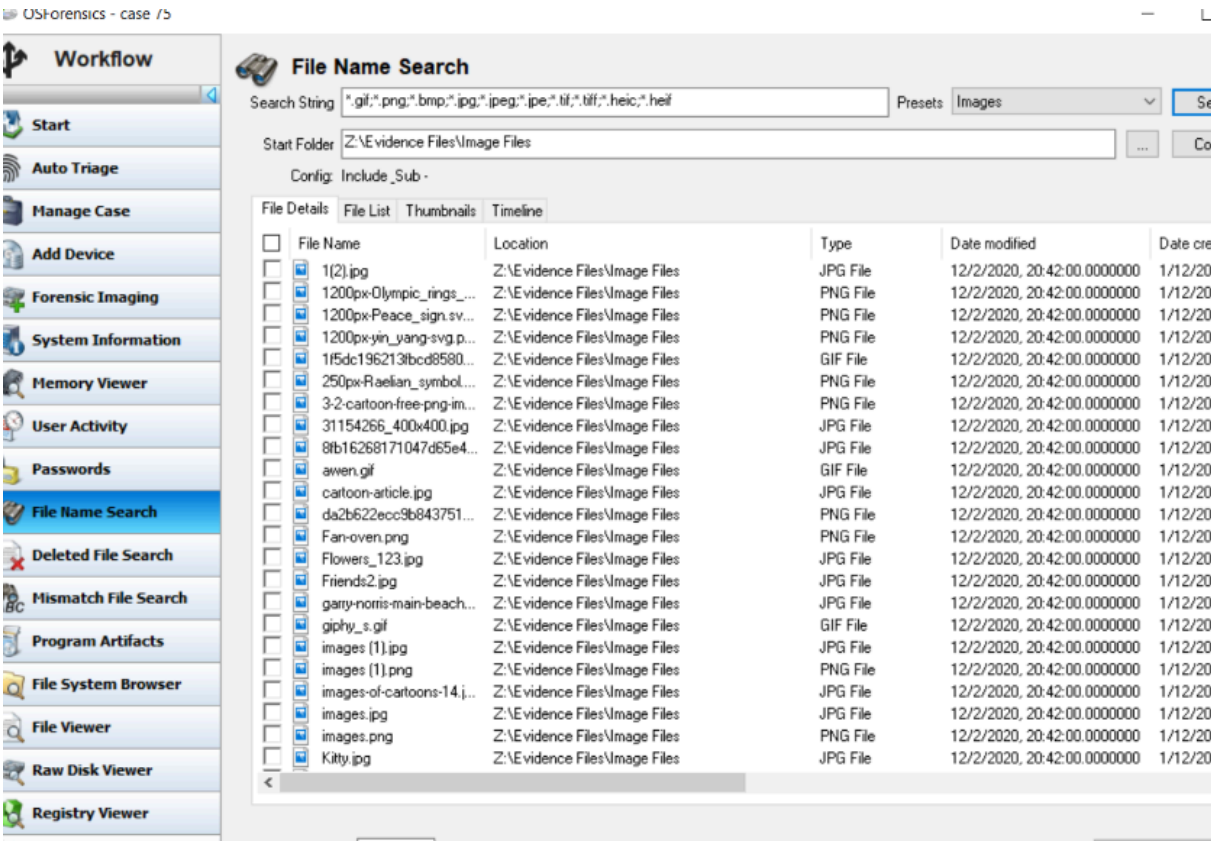
Steps

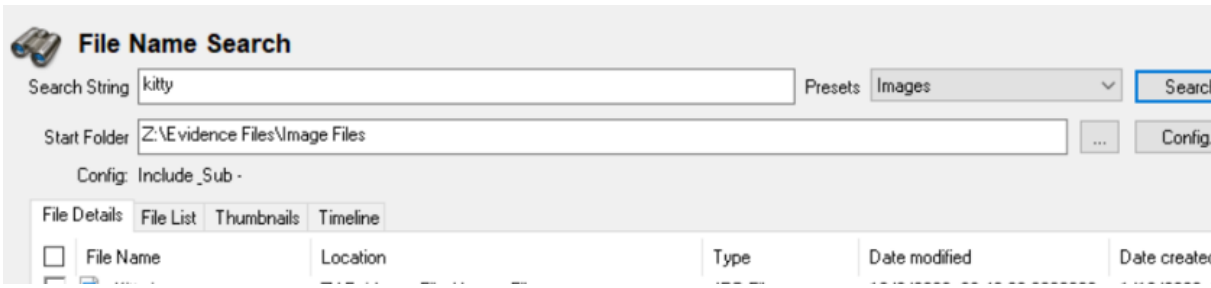
1. **Create a Case**
    - Launch OSForensics and create a new case, selecting *Live Acquisition*.
2. **Search for Files**
    - Use the `File Name Search` feature to locate specific files (e.g., images, documents).
3. **Create and Search Indexes**
    - Use `Create Index` to index files, then search the index using `Search Index`.
4. **Recover Deleted Files**
    - Use `Deleted File Search` to find and recover deleted files from the disk.

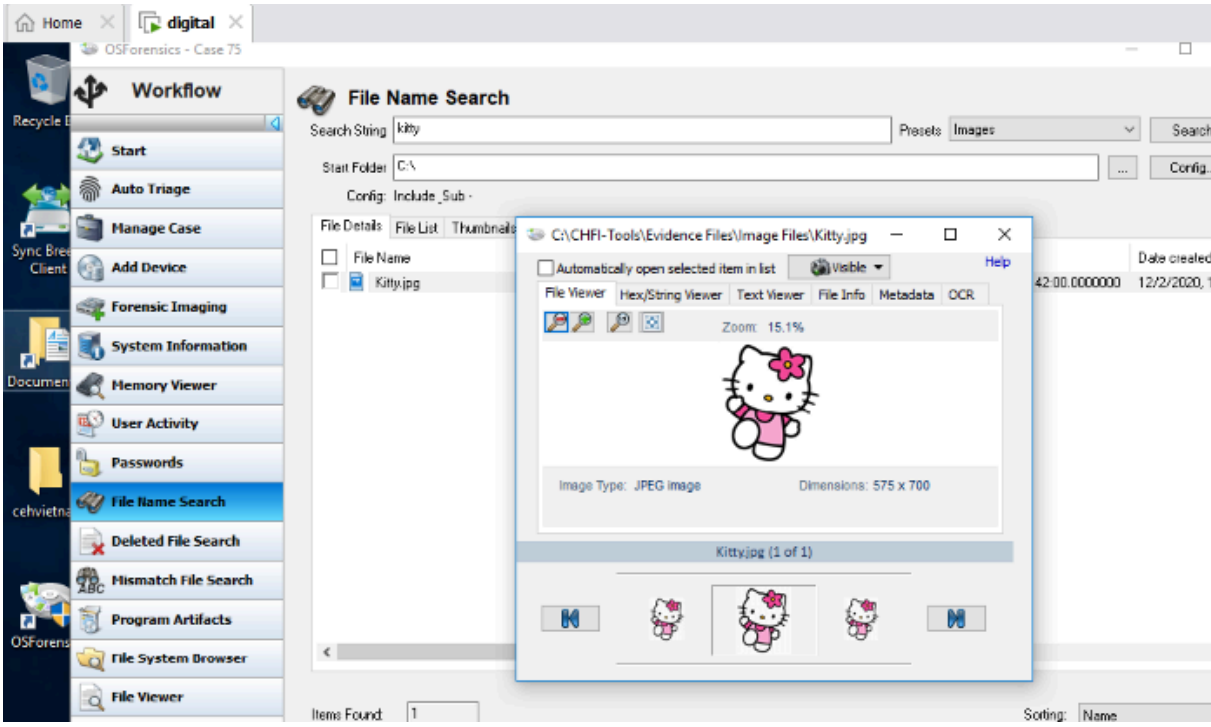

Setup - OSForensics
License Agreement
Please read the following important information before continuing.
Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.
PassMark® Software Pty Ltd ('PassMark')
End User License Agreement ('EULA')
IMPORTANT! PLEASE READ THE FOLLOWING TERMS AND CONDITIONS.
YOU, THE INSTALLER OF THIS SOFTWARE, AGREE THAT ALL OF THE TERMS AND CONDITIONS DESCRIBED BELOW APPLY TO YOU AND ANYONE ELSE WHO USES THIS SOFTWARE, IF EITHER;
I accept the agreement
I do not accept the agreement
Next >
Cancel

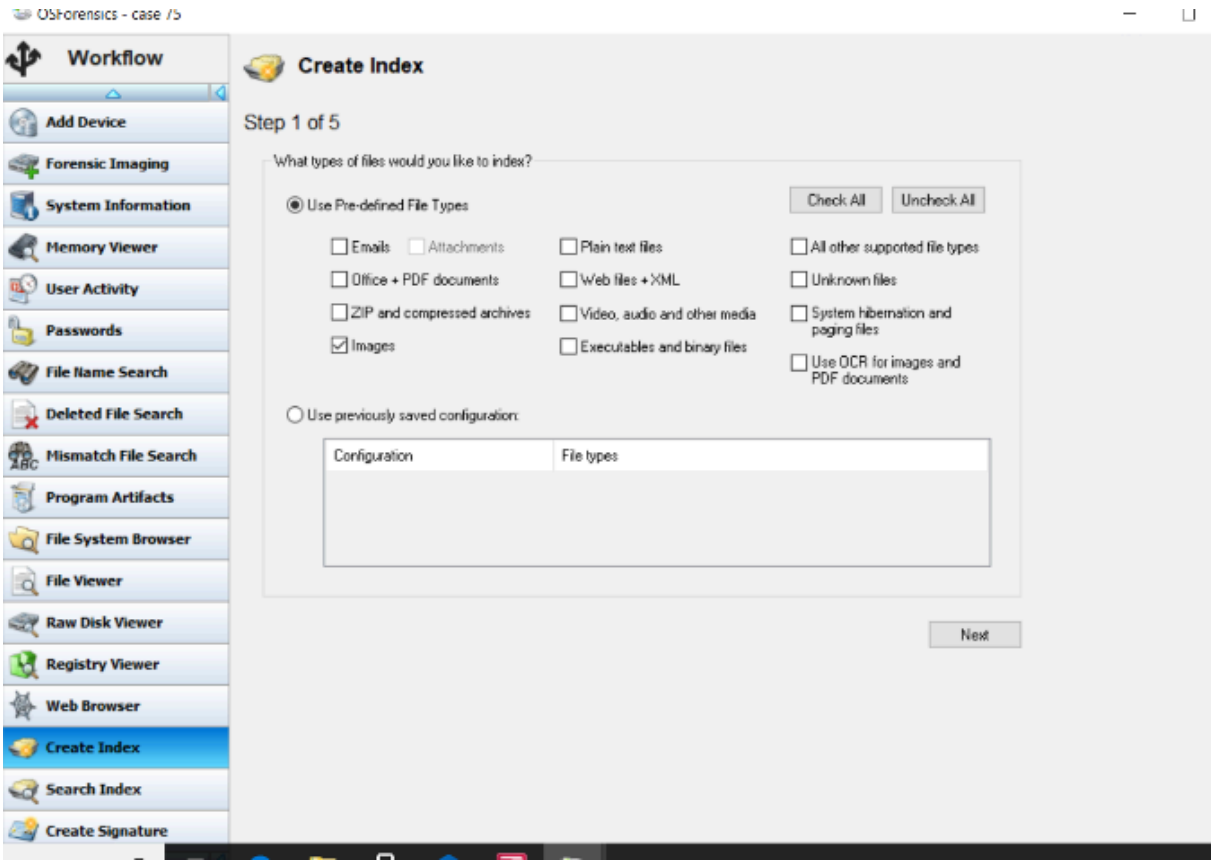

OSForensics
Workflow
Start
Auto Triage
Manage Case
Add Device
Forensic Imaging
System Information
Memory Viewer
User Activity
Passwords
File Name Search
Deleted File Search
Mismatch File Search
Program Artifacts
File System Browser
File Viewer
Raw Disk Viewer
Registry Viewer
Web Browser
Manage Case
Select Case
New Case...
Title
Create Date
Access Date
Location
Default Drive
New Case
Help
Basic Case Data
Case Categories
Offense & Custody Data
Description of Evidence
Chain of Custody
Custom Fields
Case Name
case 75
Investigator
Jonathan Davis
Organization
ABC incorporation
Contact Details
jonathan@abcxxxxxxcorp.org
Timezone
Local (GMT +7:00)
Default Drive
C:\ [Local]
Acquisition Type
Live Acquisition of Current Machine
Investigate Disk(s) from Another Machine
Enable USB Write-block
Case Folder
Default Location
Custom Location
C:\Users\cehvietnam\Documents\PassMark\OSForensics\Cases\case 75\
Browse
Log case activity
OK
Cancel

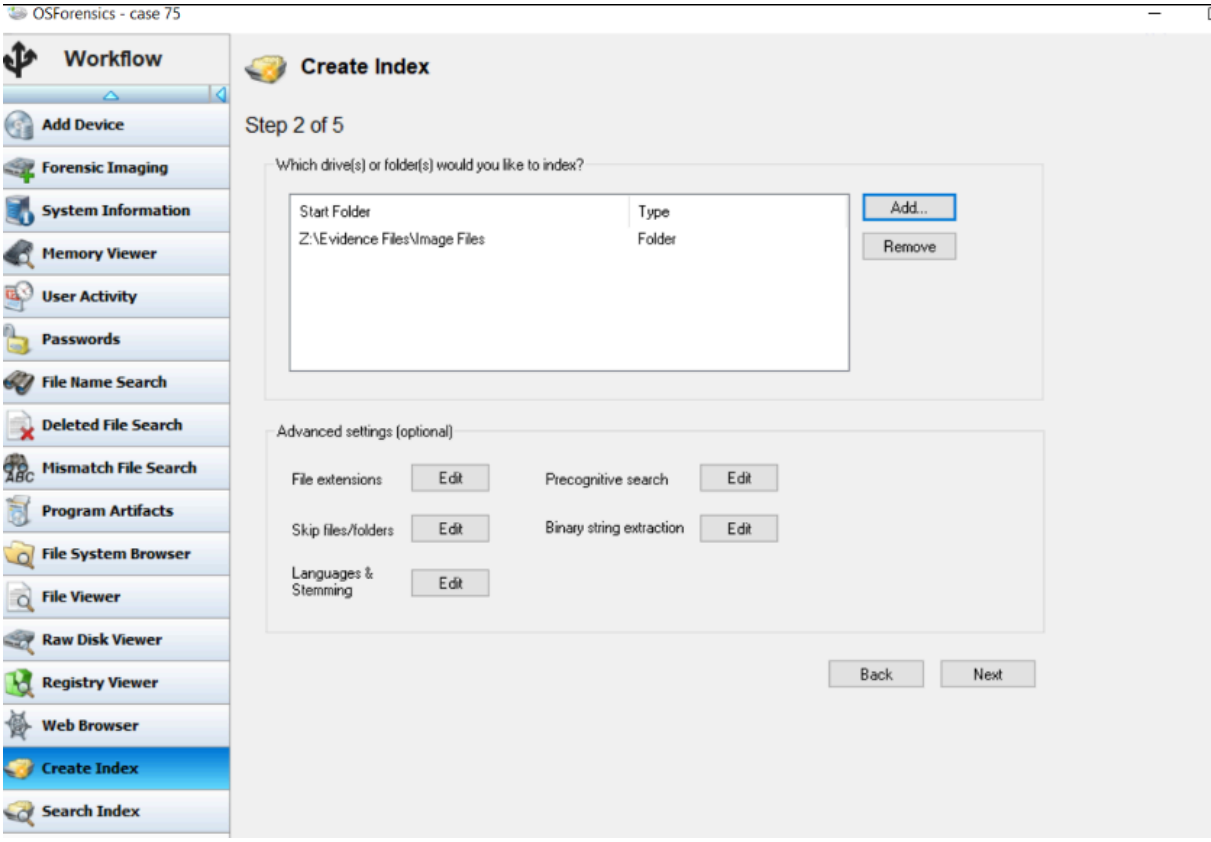

OSForensics - case 75
Workflow
Start
Auto Triage
Manage Case
Add Device
Forensic Imaging
System Information
Memory Viewer
User Activity
Passwords
File Name Search
Deleted File Search
Mismatch File Search
Program Artifacts
File System Browser
File Viewer
Raw Disk Viewer
Registry Viewer
File Name Search
Search String
*
Presets
All Files
Start Folder
C:\
Config: Include _Sub -
File Details
File List
Thumbnails
Timeline
File Name
Location
Type
Date modified

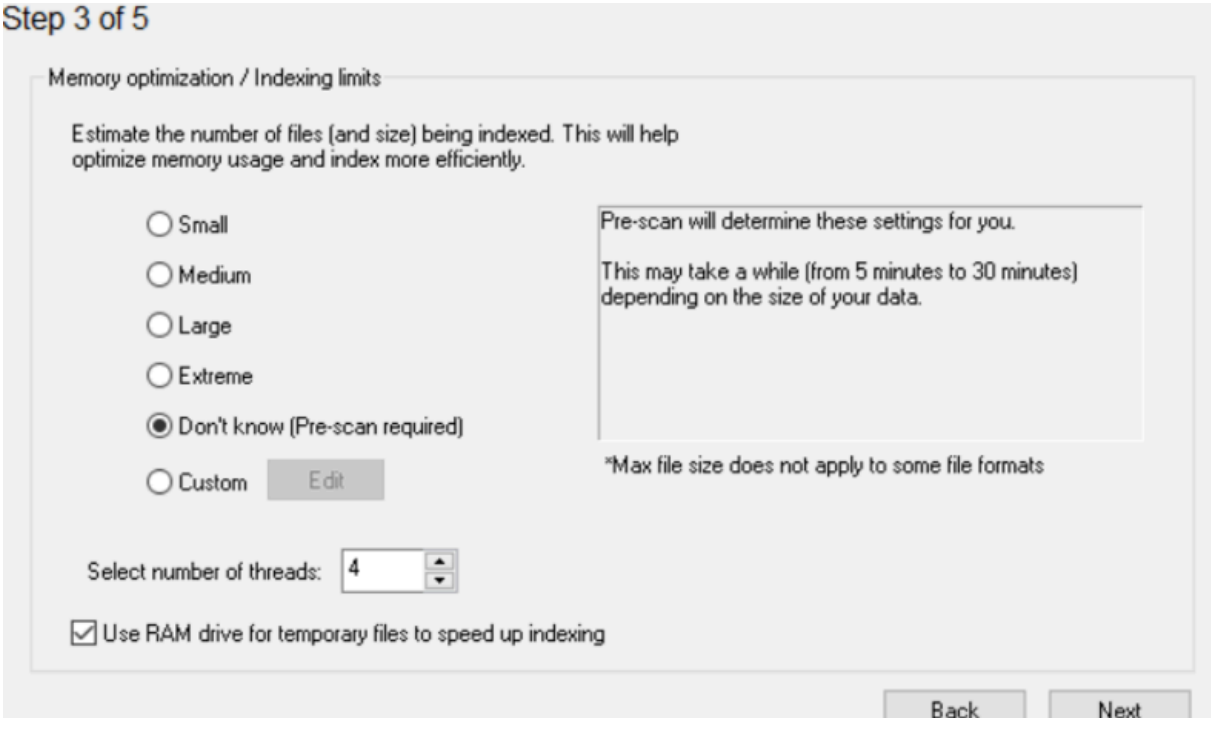

OSForensics - case 75
Workflow
Start
Auto Triage
Manage Case
Add Device
Forensic Imaging
System Information
Memory Viewer
User Activity
Passwords
File Name Search
Deleted File Search
Mismatch File Search
Program Artifacts
File System Browser
File Viewer
Raw Disk Viewer
Registry Viewer
File Name Search
Search String *.gif;*.png;*.bmp;*.jpg;*.jpeg;*.jpe;*.tif;*.tiff;*.heic;*.heif
Presets Images
Start Folder Z:\Evidence Files\Image Files
Config: Include _Sub -
File Details
File List
Thumbnails
Timeline
File Name
Location
Type
Date modified
1(2).jpg Z:\Evidence Files\Image Files JPG File 12/2/2020, 20:42:00.0000000
1200px-Olympic_rings_... Z:\Evidence Files\Image Files PNG File 12/2/2020, 20:42:00.0000000
1200px-Peace_sign.sv... Z:\Evidence Files\Image Files PNG File 12/2/2020, 20:42:00.0000000
1200px-yin_yang-svg.p... Z:\Evidence Files\Image Files PNG File 12/2/2020, 20:42:00.0000000
1f5dc196213fbcd8580... Z:\Evidence Files\Image Files GIF File 12/2/2020, 20:42:00.0000000
250px-Raelian_symbol.... Z:\Evidence Files\Image Files PNG File 12/2/2020, 20:42:00.0000000
3-2-cartoon-free-png-im... Z:\Evidence Files\Image Files PNG File 12/2/2020, 20:42:00.0000000
31154266_400x400.jpg Z:\Evidence Files\Image Files JPG File 12/2/2020, 20:42:00.0000000
8fb16268171047d65e4... Z:\Evidence Files\Image Files JPG File 12/2/2020, 20:42:00.0000000
awen.gif Z:\Evidence Files\Image Files GIF File 12/2/2020, 20:42:00.0000000
cartoon-article.jpg Z:\Evidence Files\Image Files JPG File 12/2/2020, 20:42:00.0000000
da2b622ecc9b843751... Z:\Evidence Files\Image Files PNG File 12/2/2020, 20:42:00.0000000
Fan-oven.png Z:\Evidence Files\Image Files PNG File 12/2/2020, 20:42:00.0000000
Flowers_123.jpg Z:\Evidence Files\Image Files JPG File 12/2/2020, 20:42:00.0000000
Friends2.jpg Z:\Evidence Files\Image Files JPG File 12/2/2020, 20:42:00.0000000
garry-norris-main-beach... Z:\Evidence Files\Image Files JPG File 12/2/2020, 20:42:00.0000000
giphy_s.gif Z:\Evidence Files\Image Files GIF File 12/2/2020, 20:42:00.0000000
images (1).jpg Z:\Evidence Files\Image Files JPG File 12/2/2020, 20:42:00.0000000
images (1).png Z:\Evidence Files\Image Files PNG File 12/2/2020, 20:42:00.0000000
images-of-cartoons-14.j... Z:\Evidence Files\Image Files JPG File 12/2/2020, 20:42:00.0000000
images.jpg Z:\Evidence Files\Image Files JPG File 12/2/2020, 20:42:00.0000000
images.png Z:\Evidence Files\Image Files PNG File 12/2/2020, 20:42:00.0000000
Kitty.jpg Z:\Evidence Files\Image Files JPG File 12/2/2020, 20:42:00.0000000

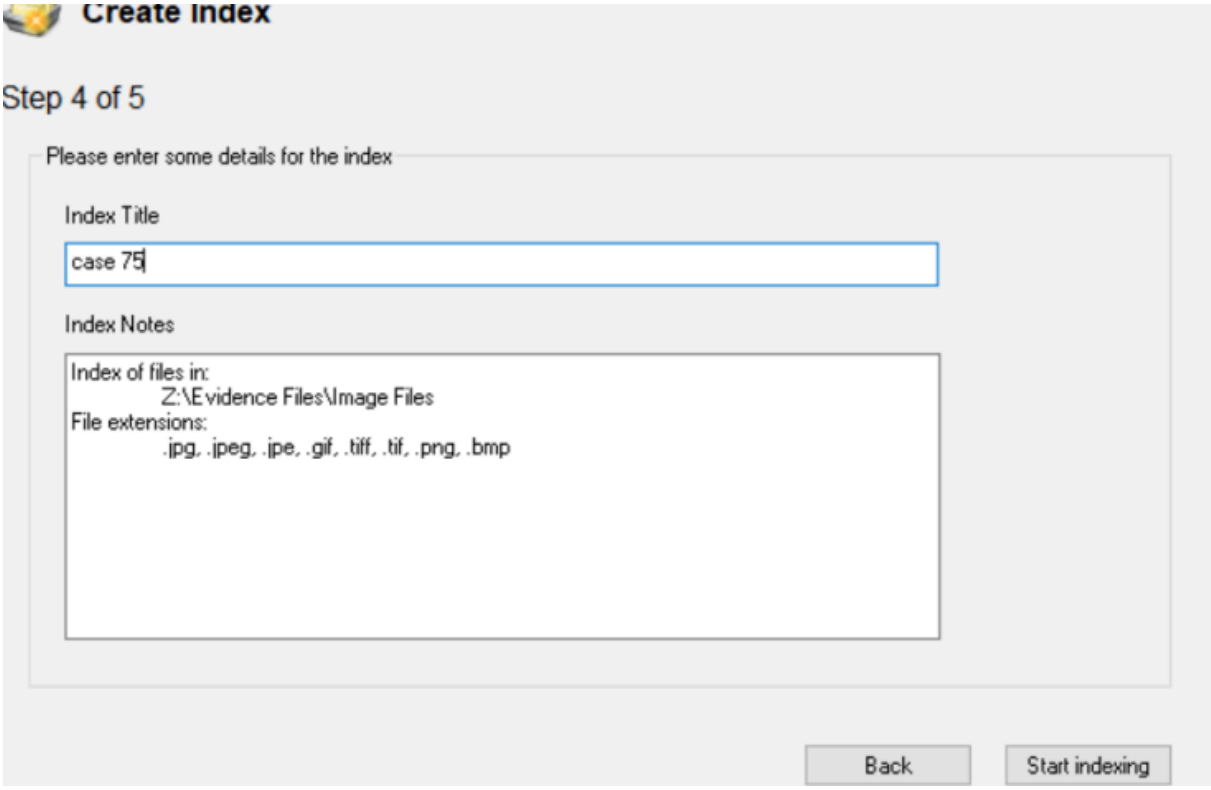

File Name Search
Search String kitty
Presets Images
Start Folder Z:\Evidence Files\Image Files
Config: Include _Sub -
File Details
File List
Thumbnails
Timeline
File Name
Location
Type
Date modified

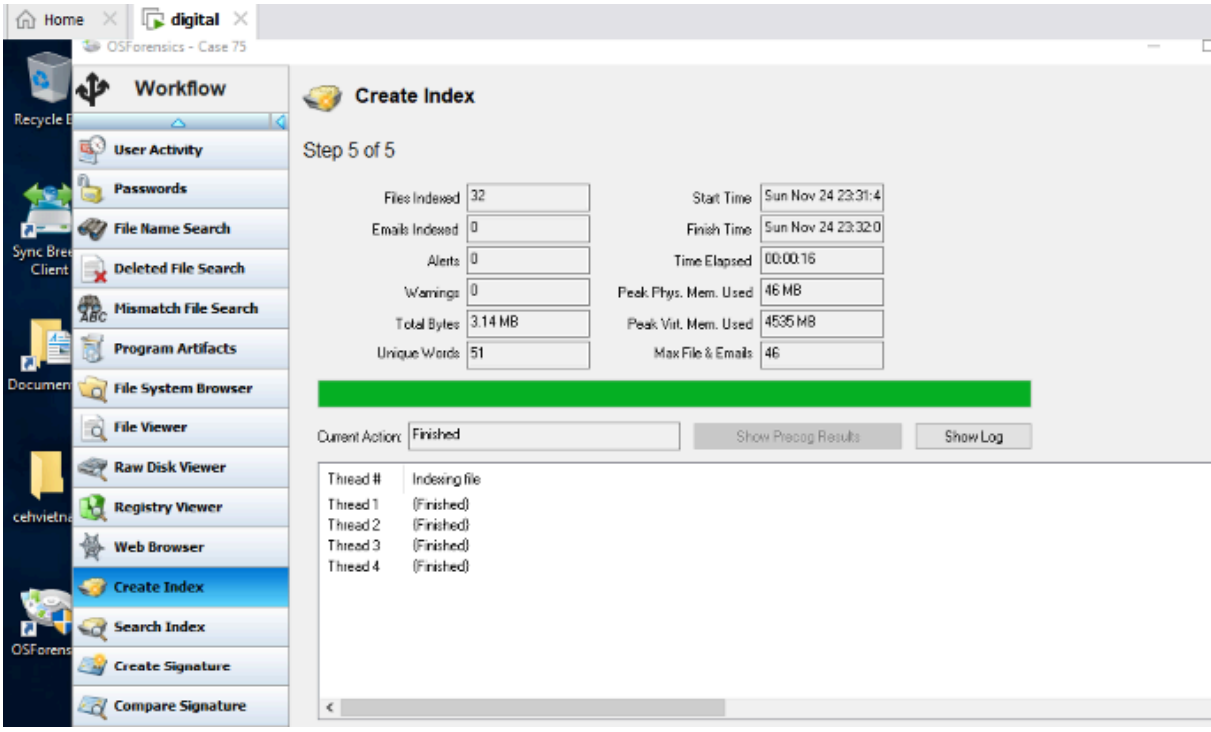

Home
digital
OSForensics - Case 75
Workflow
Start
Auto Triage
Manage Case
Add Device
Forensic Imaging
System Information
Memory Viewer
User Activity
Passwords
File Name Search
Deleted File Search
Mismatch File Search
Program Artifacts
File System Browser
File Viewer
File Name Search
Search String
kitty
Presets
Images
Start Folder
C:\
Config: Include_Sub -
File Details
File List
Thumbnails
File Name
Kitty.jpg
C:\CHFI-Tools\Evidence Files\Image Files\Kitty.jpg
Automatically open selected item in list
Visible
Help
File Viewer
Hex/String Viewer
Text Viewer
File Info
Metadata
OCR
Zoom: 15.1%
Image Type: JPEG image
Dimensions: 575 x 700
Kitty.jpg (1 of 1)
Items Found:
Sorting:
Name

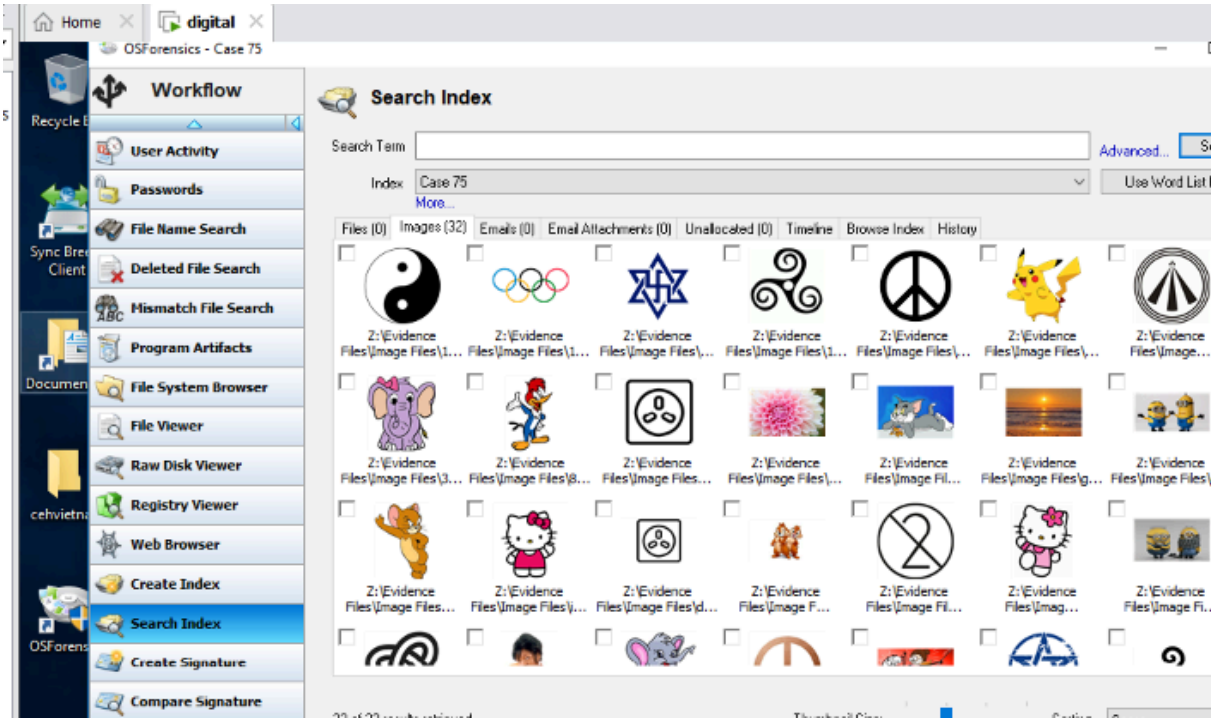

OSForensics - case 75
Workflow
Add Device
Forensic Imaging
System Information
Memory Viewer
User Activity
Passwords
File Name Search
Deleted File Search
Mismatch File Search
Program Artifacts
File System Browser
File Viewer
Raw Disk Viewer
Registry Viewer
Web Browser
Create Index
Search Index
Create Signature
Create Index
Step 1 of 5
What types of files would you like to index?
Use Pre-defined File Types
Check All
Uncheck All
Emails
Attachments
Plain text files
All other supported file types
Office + PDF documents
Web files + XML
Unknown files
ZIP and compressed archives
Video, audio and other media
System hibernation and paging files
Images
Executables and binary files
Use OCR for images and PDF documents
Use previously saved configuration:
Configuration
File types
Next

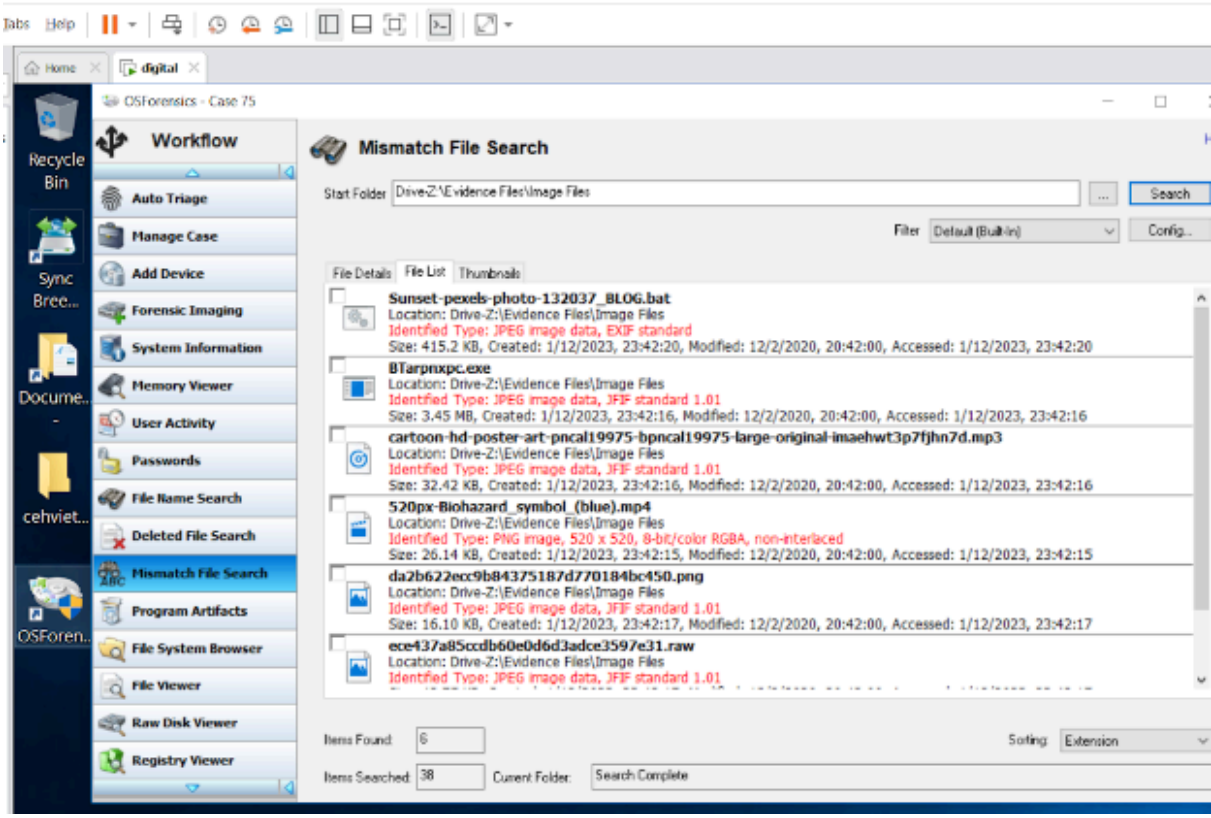

OSForensics - case 75
Workflow
Add Device
Forensic Imaging
System Information
Memory Viewer
User Activity
Passwords
File Name Search
Deleted File Search
Mismatch File Search
Program Artifacts
File System Browser
File Viewer
Raw Disk Viewer
Registry Viewer
Web Browser
Create Index
Search Index
Create Index
Step 2 of 5
Which drive(s) or folder(s) would you like to index?
Start Folder
Type
Z:\Evidence Files\Image Files
Folder
Add...
Remove
Advanced settings (optional)
File extensions
Edit
Precognitive search
Edit
Skip files/folders
Edit
Binary string extraction
Edit
Languages & Stemming
Edit
Back
Next

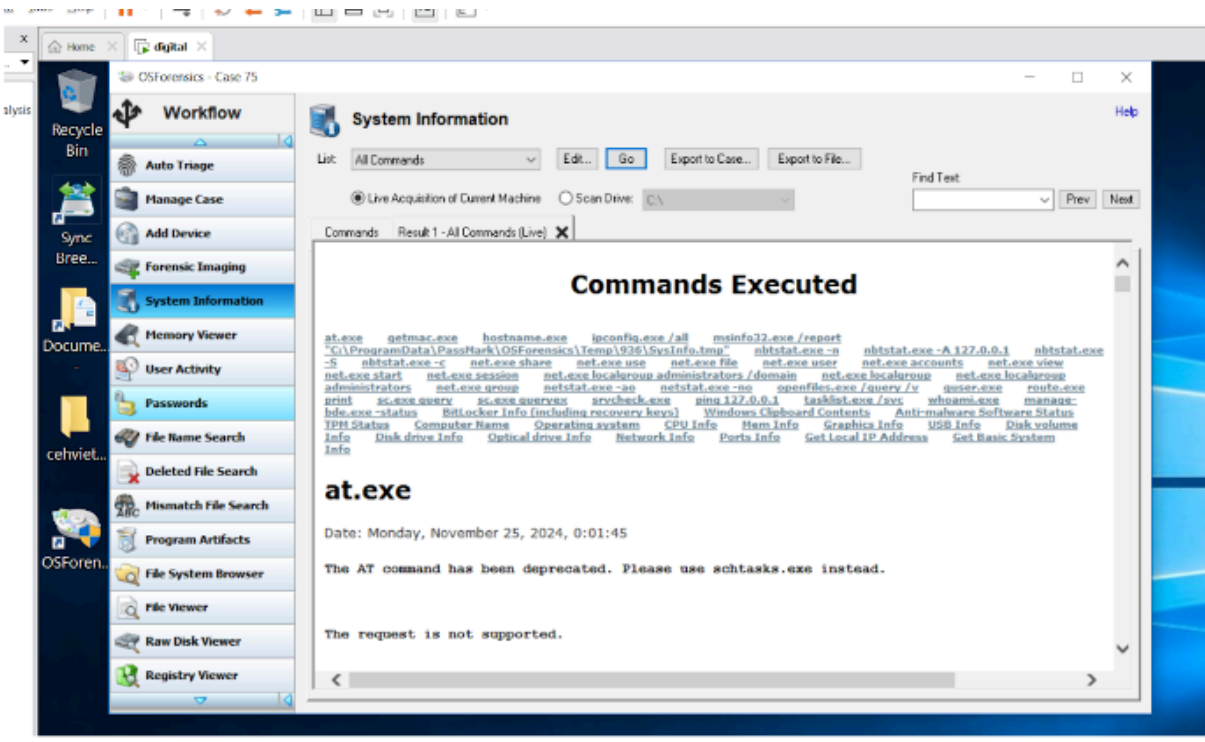

Step 3 of 5
Memory optimization / Indexing limits
Estimate the number of files (and size) being indexed. This will help optimize memory usage and index more efficiently.
Small
Medium
Large
Extreme
Don't know (Pre-scan required)
Custom
Edit
Pre-scan will determine these settings for you.
This may take a while (from 5 minutes to 30 minutes) depending on the size of your data.
*Max file size does not apply to some file formats
Select number of threads:
4
Use RAM drive for temporary files to speed up indexing
Back
Next

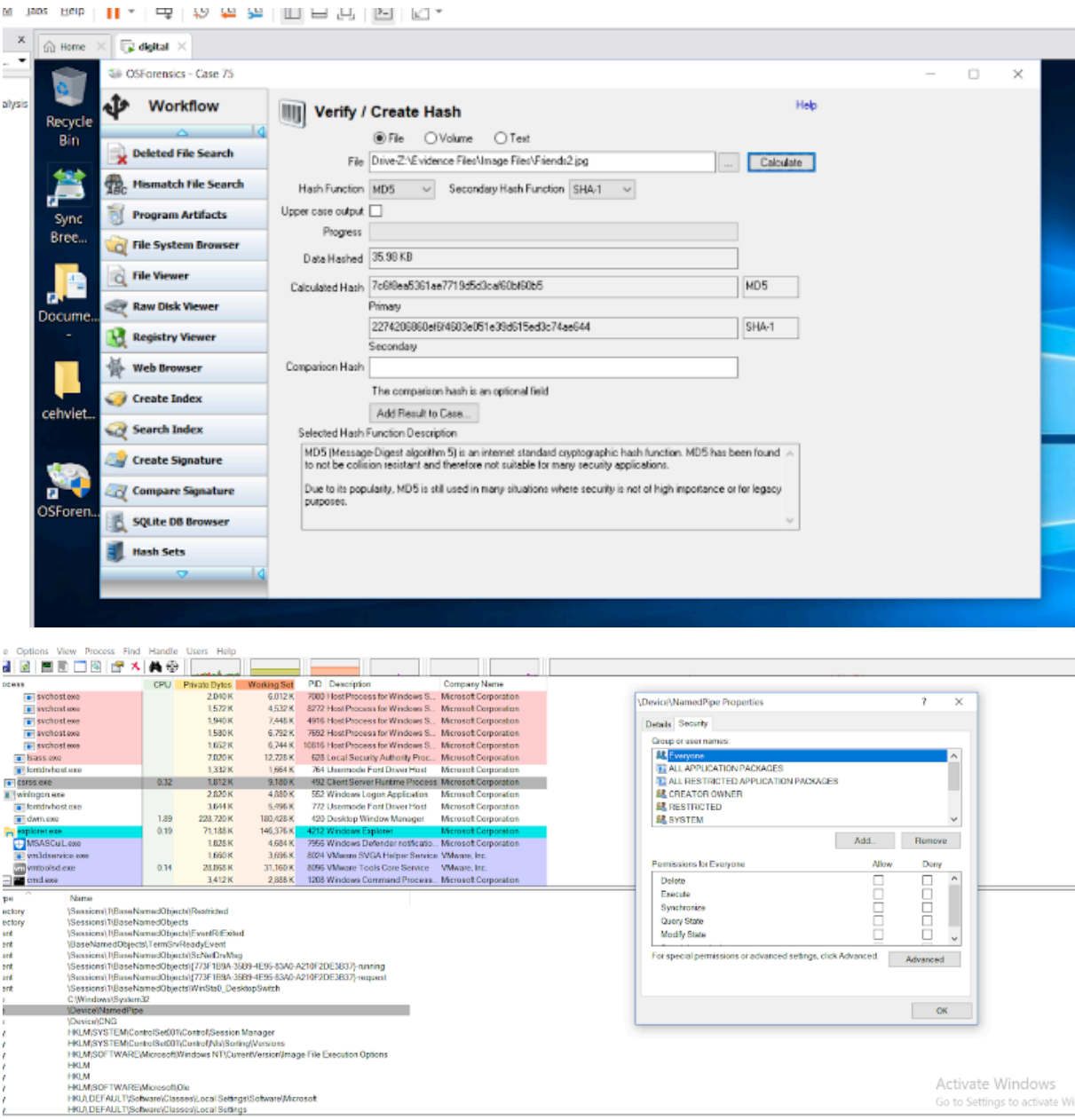

Create Index
Step 4 of 5
Please enter some details for the index
Index Title
case 75
Index Notes
Index of files in:
Z:\Evidence Files\Image Files
File extensions:
.jpg, .jpeg, .jpe, .gif, .tiff, .tif, .png, .bmp
Back
Start indexing


Home
digital
OSForensics - Case 75
Workflow
User Activity
Passwords
File Name Search
Deleted File Search
Mismatch File Search
Program Artifacts
File System Browser
File Viewer
Raw Disk Viewer
Registry Viewer
Web Browser
Create Index
Search Index
Create Signature
Compare Signature
Create Index
Step 5 of 5
Files Indexed 32
Emails Indexed 0
Alerts 0
Warnings 0
Total Bytes 3.14 MB
Unique Words 51
Start Time Sun Nov 24 23:31:4
Finish Time Sun Nov 24 23:32:0
Time Elapsed 00:00:16
Peak Phys. Mem. Used 46 MB
Peak Virt. Mem. Used 4535 MB
Max File & Emails 46
Current Action: Finished
Show Precog Results
Show Log
Thread # Indexing file
Thread 1 (Finished)
Thread 2 (Finished)
Thread 3 (Finished)
Thread 4 (Finished)


Home
digital
OSForensics - Case 75
Workflow
User Activity
Passwords
File Name Search
Deleted File Search
Mismatch File Search
Program Artifacts
File System Browser
File Viewer
Raw Disk Viewer
Registry Viewer
Web Browser
Create Index
Search Index
Create Signature
Compare Signature
Search Index
Search Term
Advanced...
Index
Case 75
More...
Use Word List
Files (0)
Images (32)
Emails (0)
Email Attachments (0)
Unallocated (0)
Timeline
Browse Index
History


Tabs
Help
Home
digital
OSForensics - Case 75
Workflow
Auto Triage
Manage Case
Add Device
Forensic Imaging
System Information
Memory Viewer
User Activity
Passwords
File Name Search
Deleted File Search
Mismatch File Search
Program Artifacts
File System Browser
File Viewer
Raw Disk Viewer
Registry Viewer
Mismatch File Search
Start Folder
Drive-Z:\Evidence Files\Image Files
Search
Filter
Default (Built-in)
Config...
File Details
File List
Thumbnails
Sunset-pexels-photo-132037_BLOG.bat
Location: Drive-Z:\Evidence Files\Image Files
Identified Type: JPEG image data, EXIF standard
Size: 415.2 KB, Created: 1/12/2023, 23:42:20, Modified: 12/2/2020, 20:42:00, Accessed: 1/12/2023, 23:42:20
BTarpnxpc.exe
Location: Drive-Z:\Evidence Files\Image Files
Identified Type: JPEG image data, JFIF standard 1.01
Size: 3.45 MB, Created: 1/12/2023, 23:42:16, Modified: 12/2/2020, 20:42:00, Accessed: 1/12/2023, 23:42:16
cartoon-hd-poster-art-pncal19975-bpncal19975-large-original-imaehwt3p7fjhn7d.mp3
Location: Drive-Z:\Evidence Files\Image Files
Identified Type: JPEG image data, JFIF standard 1.01
Size: 32.42 KB, Created: 1/12/2023, 23:42:16, Modified: 12/2/2020, 20:42:00, Accessed: 1/12/2023, 23:42:16
520px-Biohazard_symbol_(blue).mp4
Location: Drive-Z:\Evidence Files\Image Files
Identified Type: PNG image, 520 x 520, 8-bit/color RGBA, non-interlaced
Size: 26.14 KB, Created: 1/12/2023, 23:42:15, Modified: 12/2/2020, 20:42:00, Accessed: 1/12/2023, 23:42:15
da2b622ecc9b84375187d770184bc450.png
Location: Drive-Z:\Evidence Files\Image Files
Identified Type: JPEG image data, JFIF standard 1.01
Size: 16.10 KB, Created: 1/12/2023, 23:42:17, Modified: 12/2/2020, 20:42:00, Accessed: 1/12/2023, 23:42:17
ece437a85ccdb60e0d6d3adce3597e31.raw
Location: Drive-Z:\Evidence Files\Image Files
Identified Type: JPEG image data, JFIF standard 1.01
Items Found
6
Sorting
Extension
Items Searched
38
Current Folder
Search Complete


Home
digital
OSForensics - Case 75
Recycle Bin
Sync Bree...
Docume...
cehviet...
OSForen...
Workflow
Auto Triage
Manage Case
Add Device
Forensic Imaging
System Information
Memory Viewer
User Activity
Passwords
File Name Search
Deleted File Search
Mismatch File Search
Program Artifacts
File System Browser
File Viewer
Raw Disk Viewer
Registry Viewer
System Information
Help
List: All Commands
Edit...
Go
Export to Case...
Export to File...
Find Text:
Prev
Next
Live Acquisition of Current Machine
Scan Drive: C:\
Commands
Result 1 - All Commands (Live)
Commands Executed
at.exe getmac.exe hostname.exe ipconfig.exe /all msinfo32.exe /report "C:\ProgramData\PassMark\OSForensics\Temp\936\SysInfo.tmp" nbtstat.exe -n nbtstat.exe -A 127.0.0.1 nbtstat.exe -S nbtstat.exe -c net.exe share net.exe use net.exe file net.exe user net.exe accounts net.exe view net.exe start net.exe session net.exe localgroup administrators /domain net.exe localgroup net.exe localgroup administrators net.exe group netstat.exe -ao netstat.exe -no openfiles.exe /query /v qwinsta.exe route.exe print sc.exe query sc.exe queryex srvcheck.exe ping 127.0.0.1 tasklist.exe /svc whoami.exe manage-bde.exe -status BitLocker Info (including recovery keys) Windows Clipboard Contents Anti-malware Software Status TPM Status Computer Name Operating system CPU Info Mem Info Graphics Info USB Info Disk volume Info Disk drive Info Optical drive Info Network Info Ports Info Get Local IP Address Get Basic System Info
at.exe
Date: Monday, November 25, 2024, 0:01:45
The AT command has been deprecated. Please use schtasks.exe instead.
The request is not supported.



Lab 5: Extracting Information About Running Processes

Objective

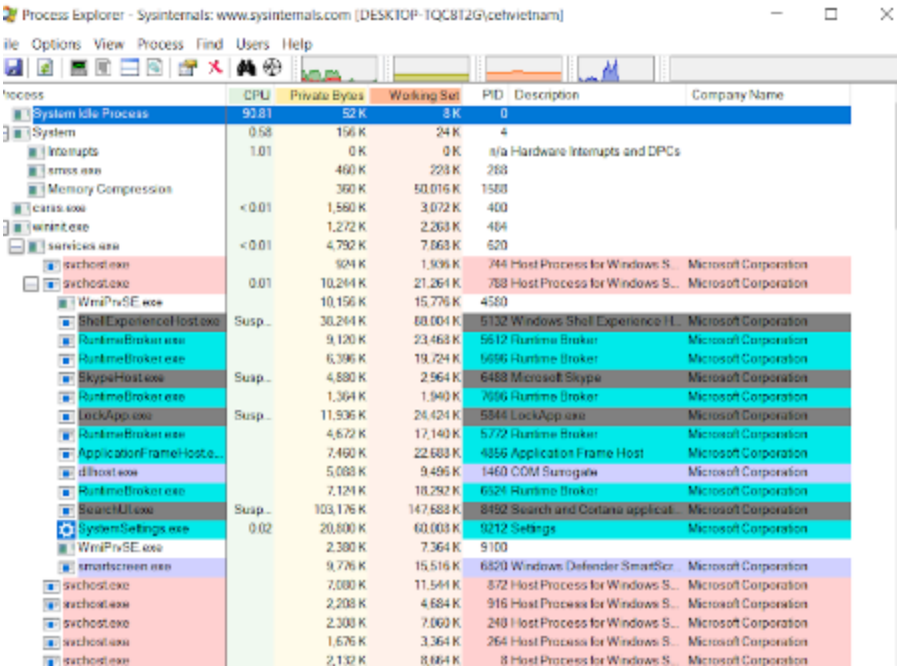
To analyze loaded DLLs and verify processes using Process Explorer.

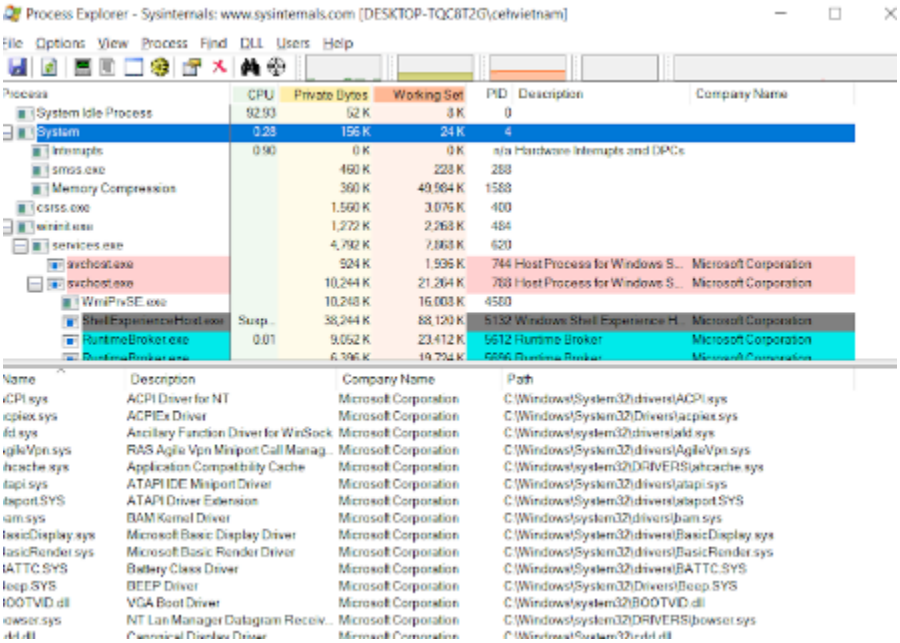
Tools Required

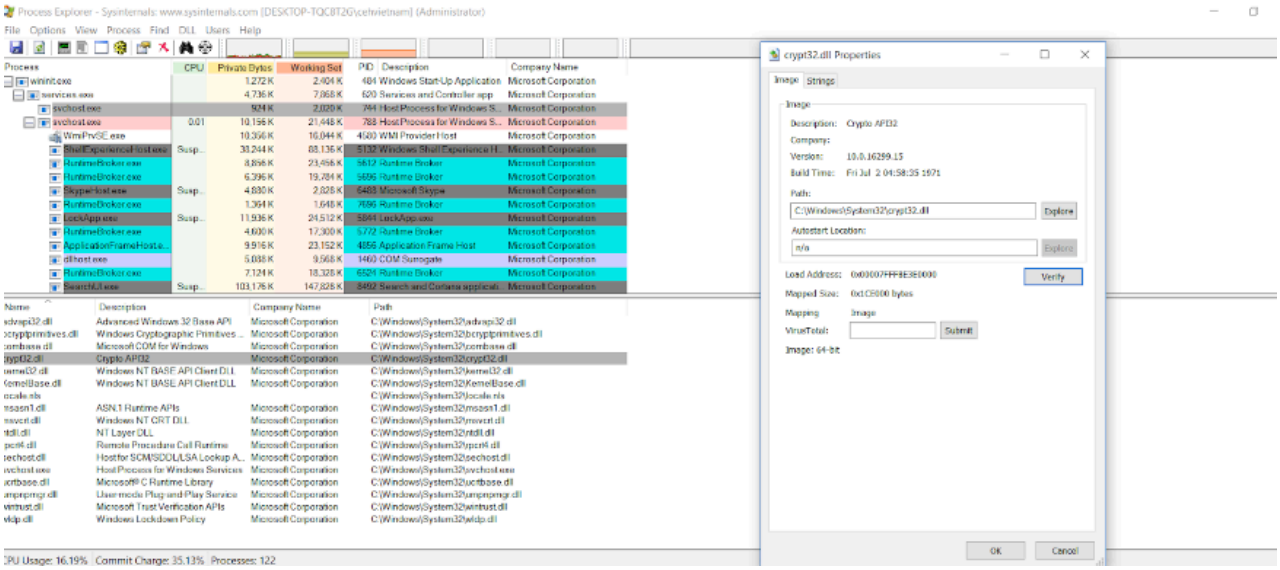
- Process Explorer

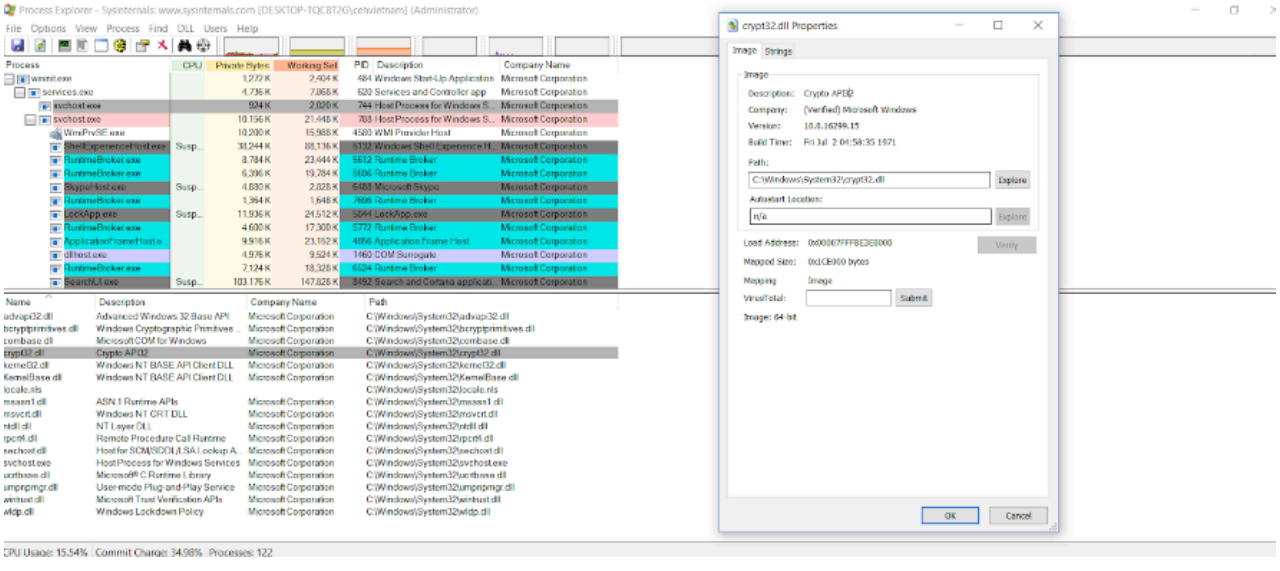
Steps

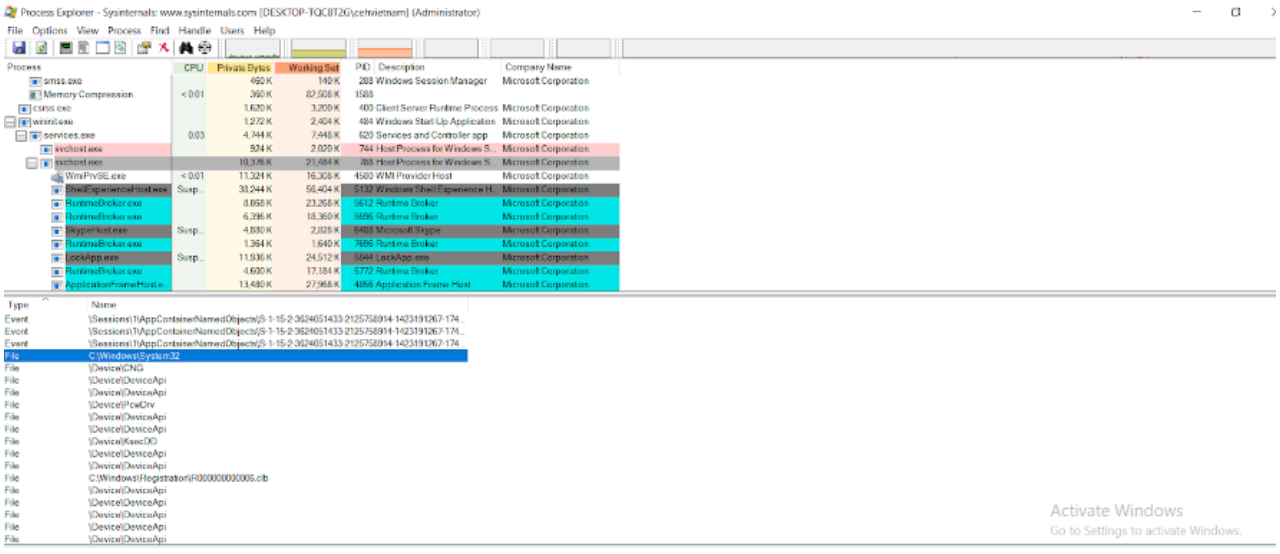
1. Open `Process Explorer`.
2. View DLLs loaded by a process:
    - Select a process.
    - Navigate to `View -> Lower Pane View -> DLLs`.
3. Verify process legitimacy:
    - Right-click a DLL and choose `Properties` to check its signature.

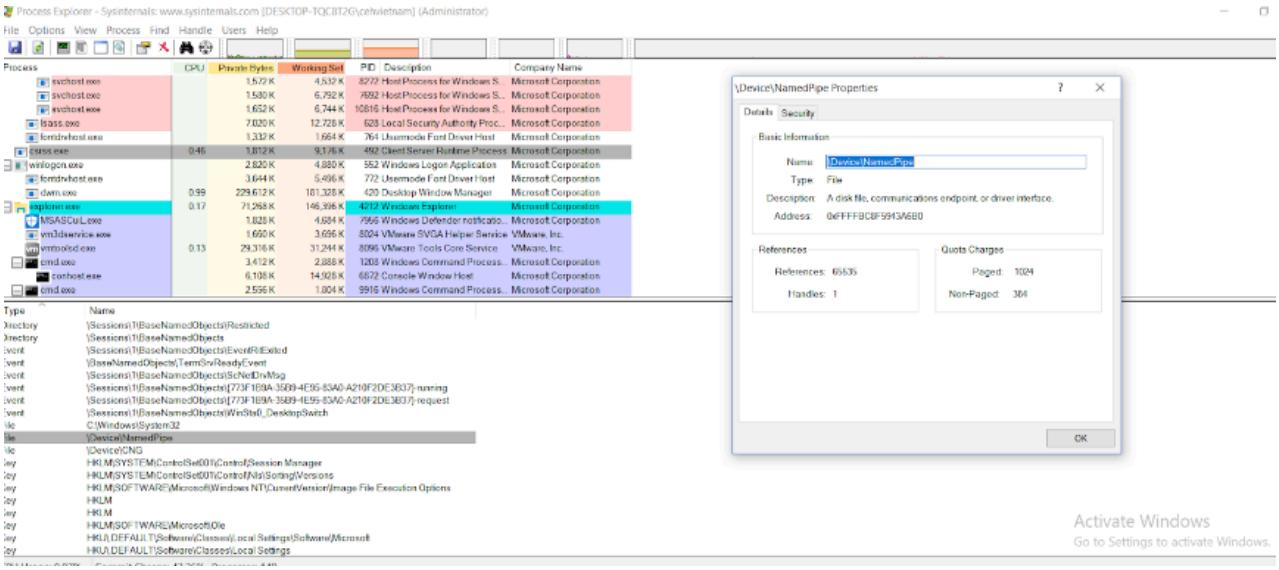

Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-TQC8T2G\cehvietnam]
ile Options View Process Find Users Help
rocess CPU Private Bytes Working Set PID Description Company Name
System Idle Process 93.81 52 K 8 K 0
System 0.58 156 K 24 K 4
Interrupts 1.01 0 K 0 K n/a Hardware Interrupts and DPCs
smss.exe 460 K 228 K 288
Memory Compression 360 K 50,016 K 1588
csrss.exe < 0.01 1,560 K 3,072 K 400
wininit.exe 1,272 K 2,268 K 484
services.exe < 0.01 4,792 K 7,868 K 620
svchost.exe 924 K 1,936 K 744 Host Process for Windows S... Microsoft Corporation
svchost.exe 0.01 10,244 K 21,264 K 788 Host Process for Windows S... Microsoft Corporation
WmiPrvSE.exe 10,156 K 15,776 K 4580
ShellExperienceHost.exe Susp... 30,244 K 68,004 K 5132 Windows Shell Experience H... Microsoft Corporation
RuntimeBroker.exe 9,120 K 23,468 K 5612 Runtime Broker Microsoft Corporation
RuntimeBroker.exe 6,396 K 19,724 K 6696 Runtime Broker Microsoft Corporation
SkypeHost.exe Susp... 4,880 K 2,964 K 6488 Microsoft Skype Microsoft Corporation
RuntimeBroker.exe 1,364 K 1,940 K 7696 Runtime Broker Microsoft Corporation
LockApp.exe Susp... 11,936 K 24,424 K 5844 LockApp.exe Microsoft Corporation
RuntimeBroker.exe 4,672 K 17,140 K 5772 Runtime Broker Microsoft Corporation
ApplicationFrameHoste... 7,460 K 22,688 K 4856 Application Frame Host Microsoft Corporation
dllhost.exe 5,088 K 9,496 K 1460 COM Surrogate Microsoft Corporation
RuntimeBroker.exe 7,124 K 18,292 K 6524 Runtime Broker Microsoft Corporation
SearchUI.exe Susp... 103,176 K 147,688 K 8492 Search and Cortana applicat... Microsoft Corporation
SystemSettings.exe 0.02 20,800 K 60,008 K 9212 Settings Microsoft Corporation
WmiPrvSE.exe 2,380 K 7,364 K 9100
smartscreen.exe 9,776 K 15,516 K 6820 Windows Defender SmartScr... Microsoft Corporation
svchost.exe 7,080 K 11,544 K 872 Host Process for Windows S... Microsoft Corporation
svchost.exe 2,208 K 4,684 K 916 Host Process for Windows S... Microsoft Corporation
svchost.exe 2,308 K 7,060 K 240 Host Process for Windows S... Microsoft Corporation
svchost.exe 1,676 K 3,364 K 264 Host Process for Windows S... Microsoft Corporation
svchost.exe 2,132 K 8,864 K 8 Host Process for Windows S... Microsoft Corporation

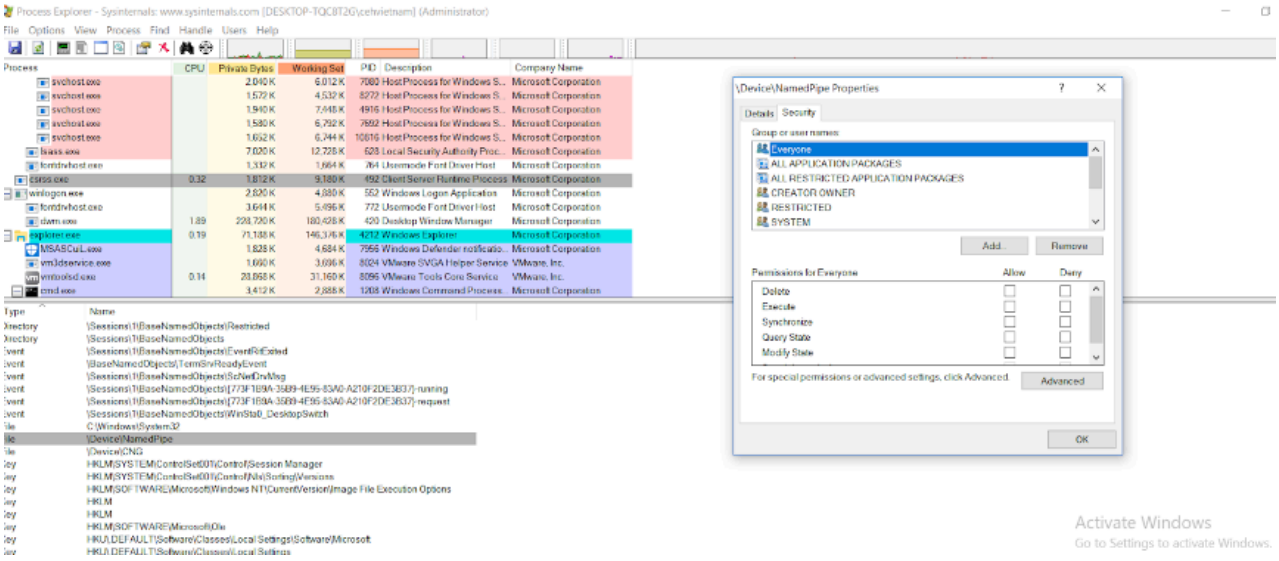

Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-TQC8T2G\cehvietnam]
File Options View Process Find DLL Users Help
Process CPU Private Bytes Working Set PID Description Company Name
System Idle Process 92.93 52 K 8 K 0
System 0.28 156 K 24 K 4
Interrupts 0.90 0 K 0 K n/a Hardware Interrupts and DPCs
smss.exe 460 K 228 K 288
Memory Compression 360 K 49,584 K 1588
csrss.exe 1,560 K 3,076 K 400
wininit.exe 1,272 K 2,268 K 484
services.exe 4,792 K 7,868 K 620
svchost.exe 924 K 1,936 K 744 Host Process for Windows S... Microsoft Corporation
svchost.exe 10,244 K 21,264 K 788 Host Process for Windows S... Microsoft Corporation
WmiPrvSE.exe 10,248 K 16,008 K 4580
ShellExperienceHost.exe Susp... 38,244 K 88,120 K 5132 Windows Shell Experience H... Microsoft Corporation
RuntimeBroker.exe 0.01 9,052 K 23,412 K 5612 Runtime Broker Microsoft Corporation
Name Description Company Name Path
ACPI.sys ACPI Driver for NT Microsoft Corporation C:\Windows\System32\drivers\ACPI.sys
acpiex.sys ACPIEx Driver Microsoft Corporation C:\Windows\System32\Drivers\acpiex.sys
afd.sys Ancillary Function Driver for WinSock Microsoft Corporation C:\Windows\system32\drivers\afd.sys
AgileVpn.sys RAS Agile Vpn Miniport Call Manag... Microsoft Corporation C:\Windows\System32\drivers\AgileVpn.sys
ahcache.sys Application Compatibility Cache Microsoft Corporation C:\Windows\system32\DRIVERS\ahcache.sys
atapi.sys ATAPI IDE Miniport Driver Microsoft Corporation C:\Windows\System32\drivers\atapi.sys
bxport.SYS ATAPI Driver Extension Microsoft Corporation C:\Windows\System32\drivers\bxport.SYS
bam.sys BAM Kernel Driver Microsoft Corporation C:\Windows\system32\drivers\bam.sys
BasicDisplay.sys Microsoft Basic Display Driver Microsoft Corporation C:\Windows\System32\drivers\BasicDisplay.sys
BasicRender.sys Microsoft Basic Render Driver Microsoft Corporation C:\Windows\System32\drivers\BasicRender.sys
BATTC.SYS Battery Class Driver Microsoft Corporation C:\Windows\System32\drivers\BATTC.SYS
Beep.SYS BEEP Driver Microsoft Corporation C:\Windows\System32\Drivers\Beep.SYS
BOOTVID.dll VGA Boot Driver Microsoft Corporation C:\Windows\system32\BOOTVID.dll
bowser.sys NT Lan Manager Datagram Receiv... Microsoft Corporation C:\Windows\system32\DRIVERS\bowser.sys


Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-TQC8T2G\cehvietnam] (Administrator)
File Options View Process Find DLL Users Help
crypt32.dll Properties
Image Strings
Description: Crypto API32
Company:
Version: 10.0.16299.15
Build Time: Fri Jul 2 04:58:35 1971
Path: C:\Windows\System32\crypt32.dll
Autostart Location: n/a
Load Address: 0x00007FF8E8E80000
Mapped Size: 0x1CE000 bytes
Mapping: Image
VirusTotal:
Submit
Image: 64-bit
OK
Cancel
CPU Usage: 16.19% Commit Charge: 35.13% Processes: 122


Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-TQC8T2G\cehvietnam] (Administrator)
File Options View Process Find DLL Users Help
crypt32.dll Properties
Image Strings
Description: Crypto API32
Company: (Verified) Microsoft Windows
Version: 10.0.16299.15
Build Time: Fri Jul 2 04:58:35 1971
Path: C:\Windows\System32\crypt32.dll
Autostart Location: n/a
Load Address: 0x00007FF8E8E80000
Mapped Size: 0x1CE000 bytes
Mapping: Image
VirusTotal:
Submit
Image: 64-bit
OK
Cancel
CPU Usage: 15.54% Commit Charge: 34.98% Processes: 122


Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-TQC8T2G\cehvietnam] (Administrator)
File Options View Process Find Handle Users Help
C:\Windows\System32
Activate Windows
Go to Settings to activate Windows.





Lab 6: Analyzing Windows Logs

Objective

To investigate security logs for signs of unauthorized activity.

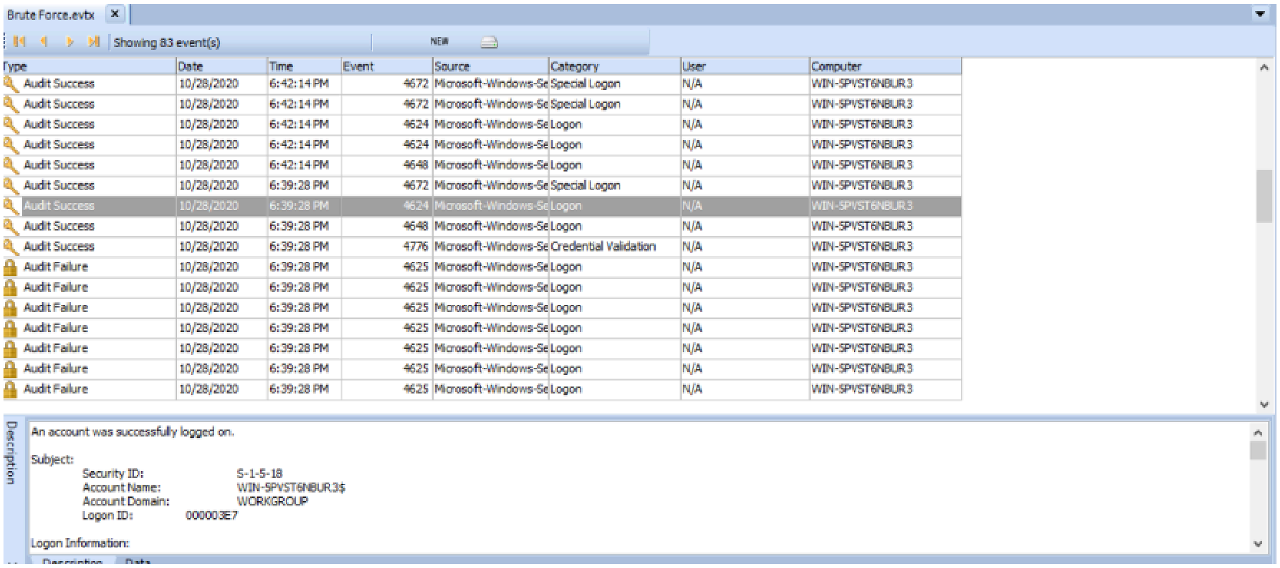
Tools Required

- EventLog Explorer

Steps

1. Open the log file in EventLog Explorer.

2. Filter logs to focus on specific events, such as `Audit Failure`.
3. Analyze logs to identify:
    - Failed login attempts, potentially indicating brute force attacks.
    - Events showing successful logins following failures.



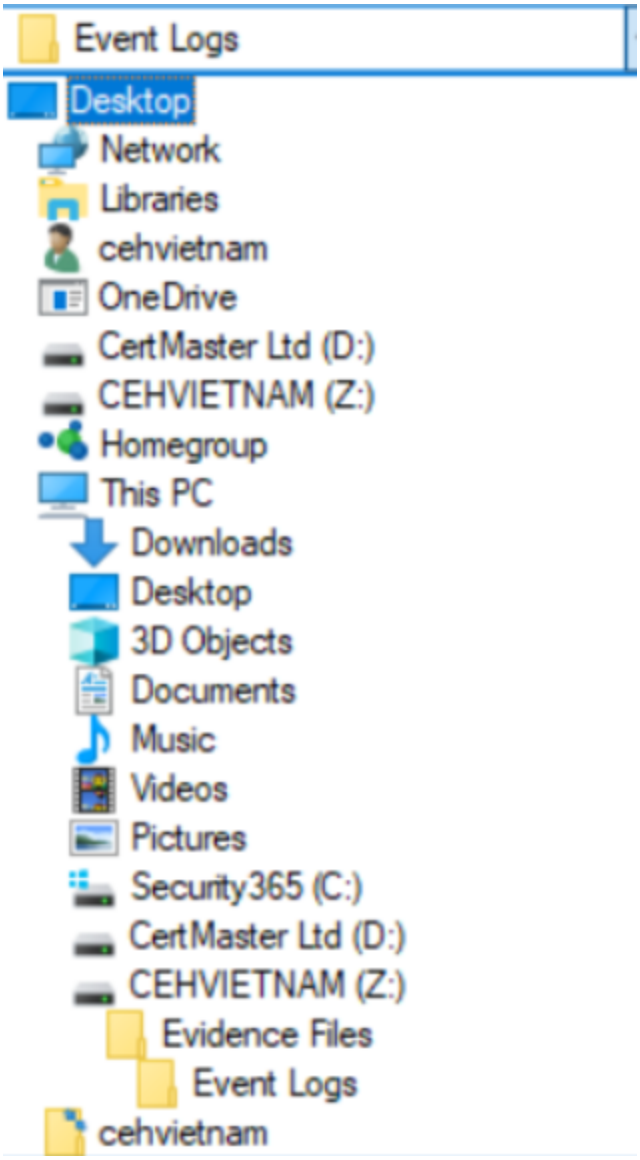
Type	Date	Time	Event	Source	Category	User	Computer
Audit Success	10/28/2020	6:42:14 PM	4672	Microsoft-Windows-Se	Special Logon	N/A	WIN-5PVST6NBUR3
Audit Success	10/28/2020	6:42:14 PM	4672	Microsoft-Windows-Se	Special Logon	N/A	WIN-5PVST6NBUR3
Audit Success	10/28/2020	6:42:14 PM	4624	Microsoft-Windows-Se	Logon	N/A	WIN-5PVST6NBUR3
Audit Success	10/28/2020	6:42:14 PM	4624	Microsoft-Windows-Se	Logon	N/A	WIN-5PVST6NBUR3
Audit Success	10/28/2020	6:42:14 PM	4648	Microsoft-Windows-Se	Logon	N/A	WIN-5PVST6NBUR3
Audit Success	10/28/2020	6:39:28 PM	4672	Microsoft-Windows-Se	Special Logon	N/A	WIN-5PVST6NBUR3
Audit Success	10/28/2020	6:39:28 PM	4624	Microsoft-Windows-Se	Logon	N/A	WIN-5PVST6NBUR3
Audit Success	10/28/2020	6:39:28 PM	4648	Microsoft-Windows-Se	Logon	N/A	WIN-5PVST6NBUR3
Audit Success	10/28/2020	6:39:28 PM	4776	Microsoft-Windows-Se	Credential Validation	N/A	WIN-5PVST6NBUR3
Audit Failure	10/28/2020	6:39:28 PM	4625	Microsoft-Windows-Se	Logon	N/A	WIN-5PVST6NBUR3
Audit Failure	10/28/2020	6:39:28 PM	4625	Microsoft-Windows-Se	Logon	N/A	WIN-5PVST6NBUR3
Audit Failure	10/28/2020	6:39:28 PM	4625	Microsoft-Windows-Se	Logon	N/A	WIN-5PVST6NBUR3
Audit Failure	10/28/2020	6:39:28 PM	4625	Microsoft-Windows-Se	Logon	N/A	WIN-5PVST6NBUR3
Audit Failure	10/28/2020	6:39:28 PM	4625	Microsoft-Windows-Se	Logon	N/A	WIN-5PVST6NBUR3
Audit Failure	10/28/2020	6:39:28 PM	4625	Microsoft-Windows-Se	Logon	N/A	WIN-5PVST6NBUR3
Audit Failure	10/28/2020	6:39:28 PM	4625	Microsoft-Windows-Se	Logon	N/A	WIN-5PVST6NBUR3

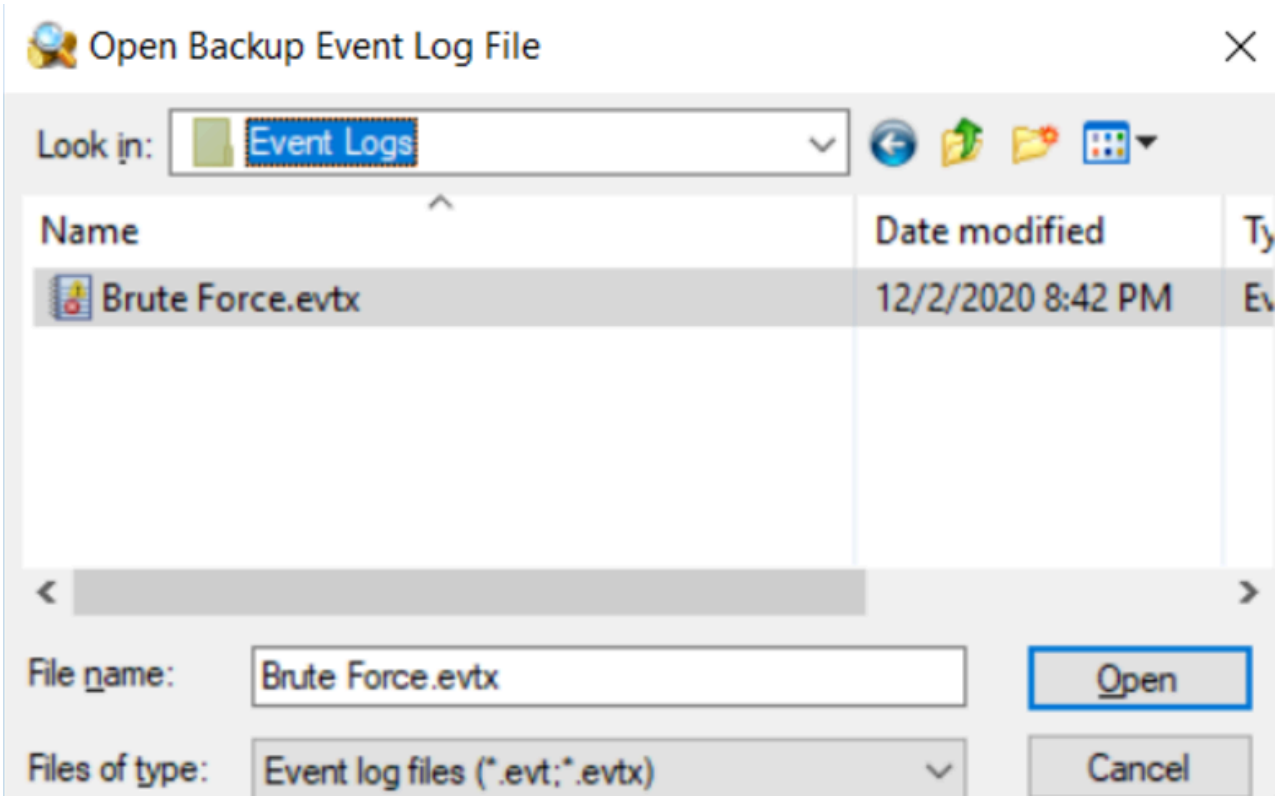
Description

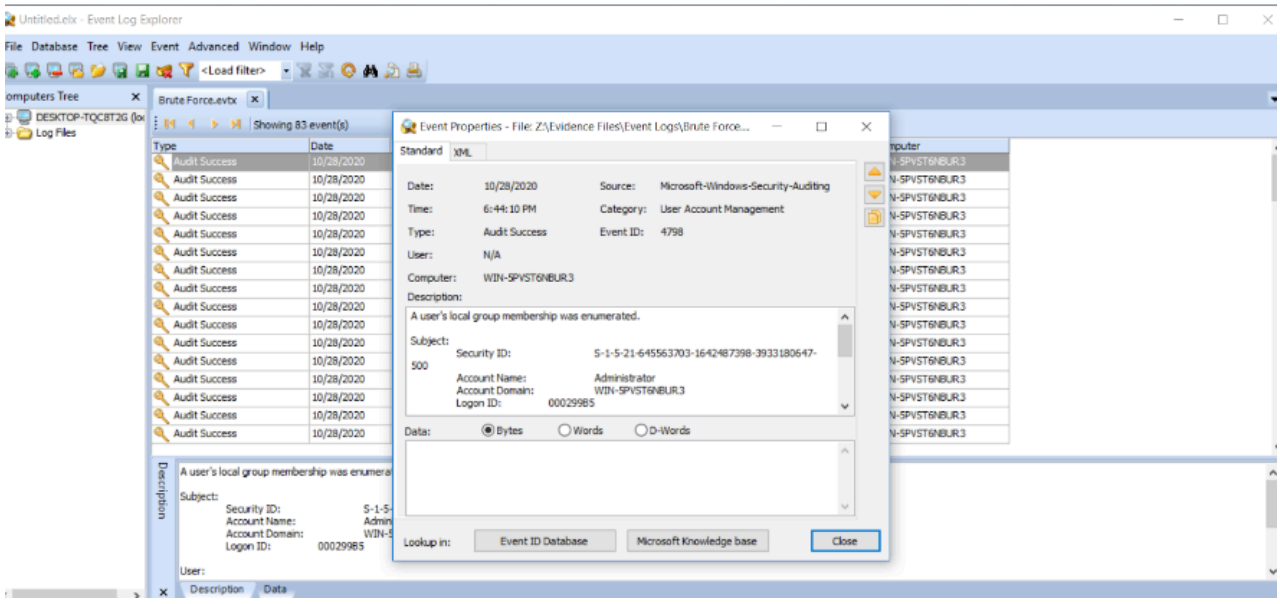
An account was successfully logged on.

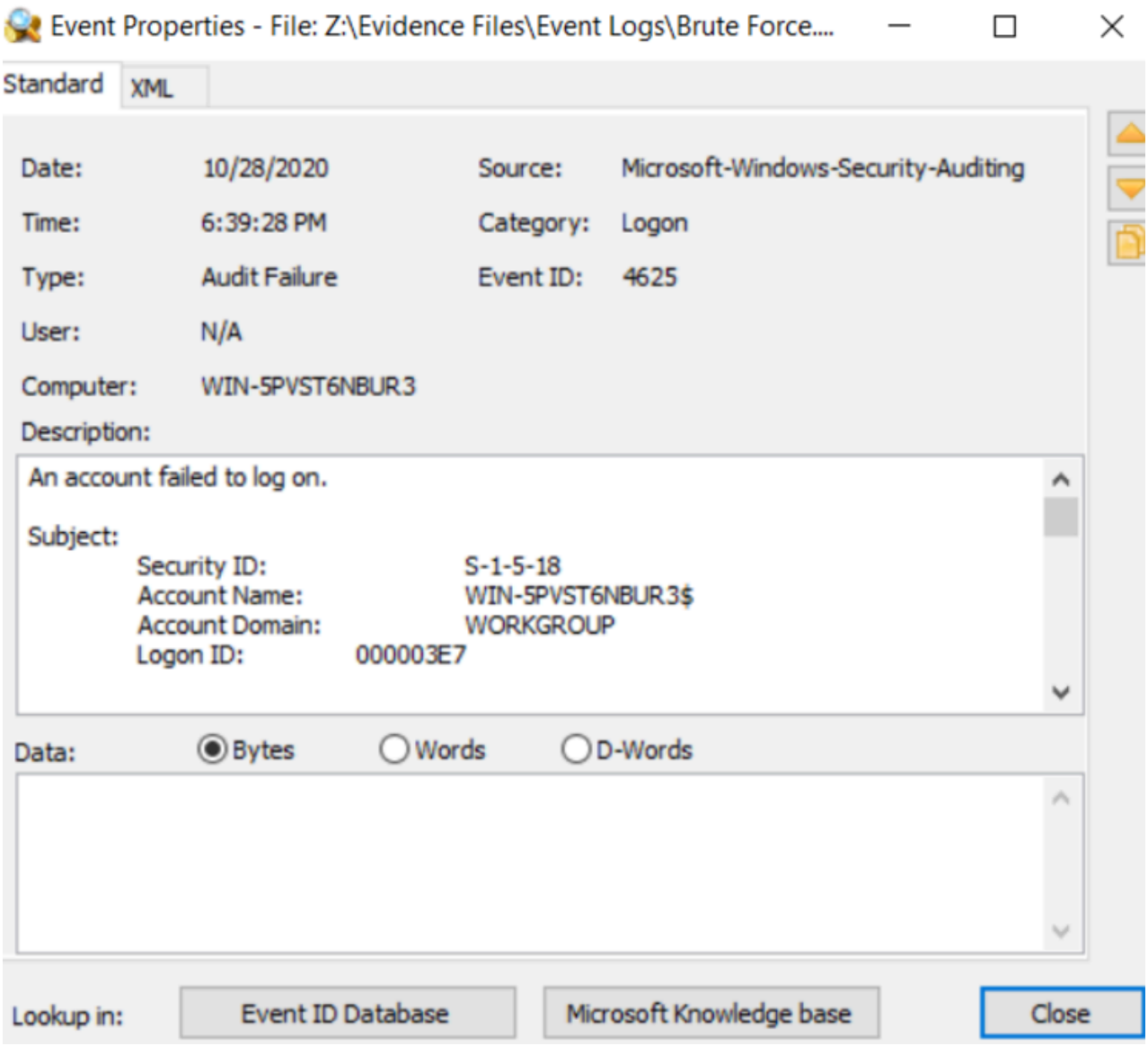
Subject:
Security ID: S-1-5-18
Account Name: WIN-5PVST6NBUR3$
Account Domain: WORKGROUP
Logon ID: 000003E7

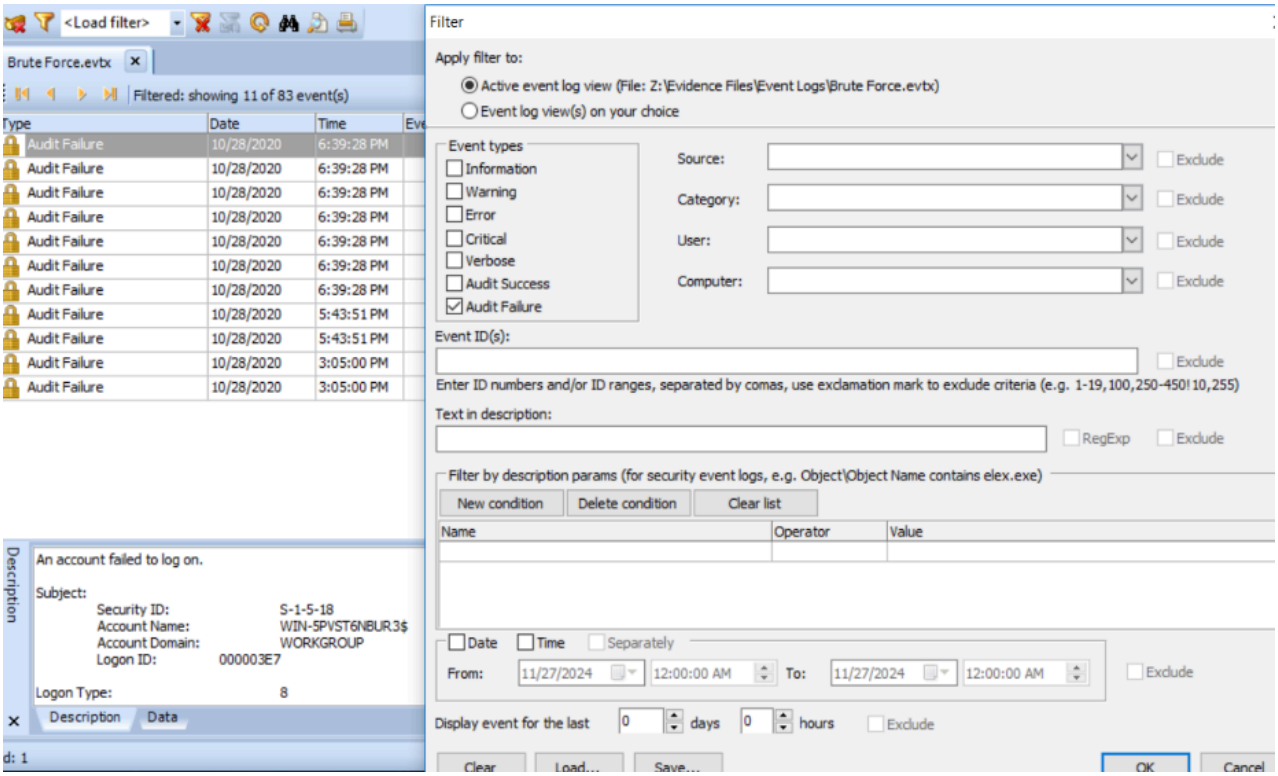
Logon Information:

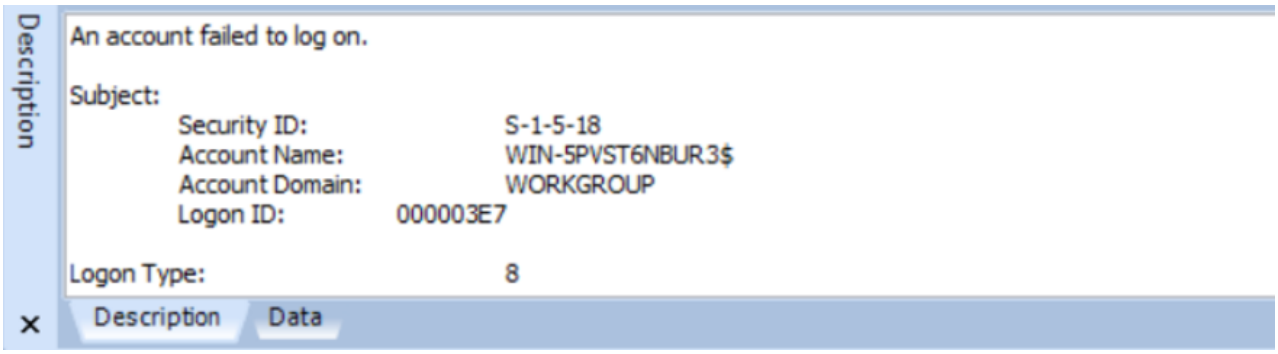

Event Logs
Desktop
Network
Libraries
cehvietnam
OneDrive
CertMaster Ltd (D:)
CEHVIETNAM (Z:)
Homegroup
This PC
Downloads
Desktop
3D Objects
Documents
Music
Videos
Pictures
Security365 (C:)
CertMaster Ltd (D:)
CEHVIETNAM (Z:)
Evidence Files
Event Logs
cehvietnam


Open Backup Event Log File
Look in:
Event Logs
Name
Date modified
Brute Force.evtx
12/2/2020 8:42 PM
File name:
Brute Force.evtx
Open
Files of type:
Event log files (*.evt;*.evtx)
Cancel

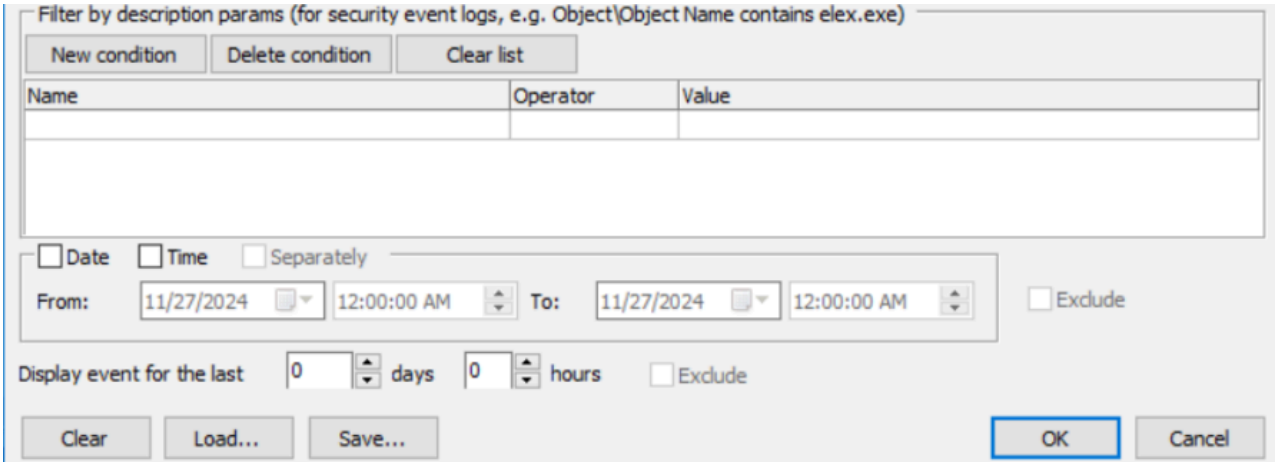

Untitled.elx - Event Log Explorer
File Database Tree View Event Advanced Window Help
Brute Force.evtx
Showing 83 event(s)
Event Properties - File: Z:\Evidence Files\Event Logs\Brute Force...
Standard
XML
Date: 10/28/2020
Time: 6:44:10 PM
Type: Audit Success
User: N/A
Computer: WIN-5PVST6NBUR3
Source: Microsoft-Windows-Security-Auditing
Category: User Account Management
Event ID: 4798
Description:
A user's local group membership was enumerated.
Subject:
Security ID: S-1-5-21-645563703-1642487398-3933180647-500
Account Name: Administrator
Account Domain: WIN-5PVST6NBUR3
Logon ID: 00029985
Data:
Bytes
Words
D-Words
Lookup in:
Event ID Database
Microsoft Knowledge base
Close
Description
Data

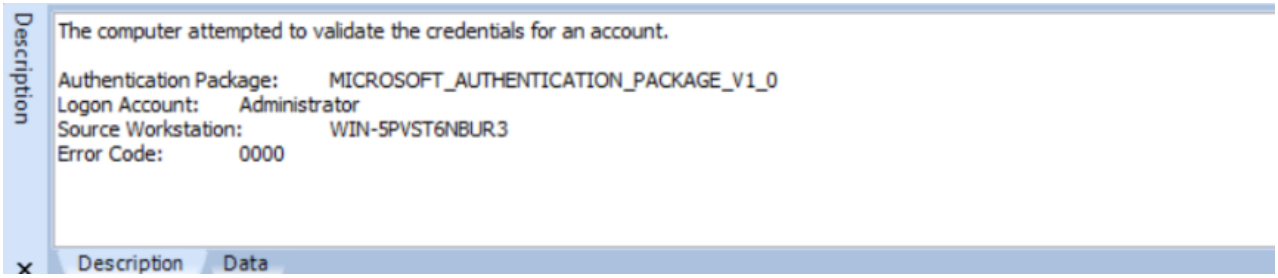

Event Properties - File: Z:\Evidence Files\Event Logs\Brute Force....
Standard
XML
Date: 10/28/2020
Source: Microsoft-Windows-Security-Auditing
Time: 6:39:28 PM
Category: Logon
Type: Audit Failure
Event ID: 4625
User: N/A
Computer: WIN-5PVST6NBUR3
Description:
An account failed to log on.
Subject:
Security ID: S-1-5-18
Account Name: WIN-5PVST6NBUR3$
Account Domain: WORKGROUP
Logon ID: 000003E7
Data:
Bytes
Words
D-Words
Lookup in:
Event ID Database
Microsoft Knowledge base
Close

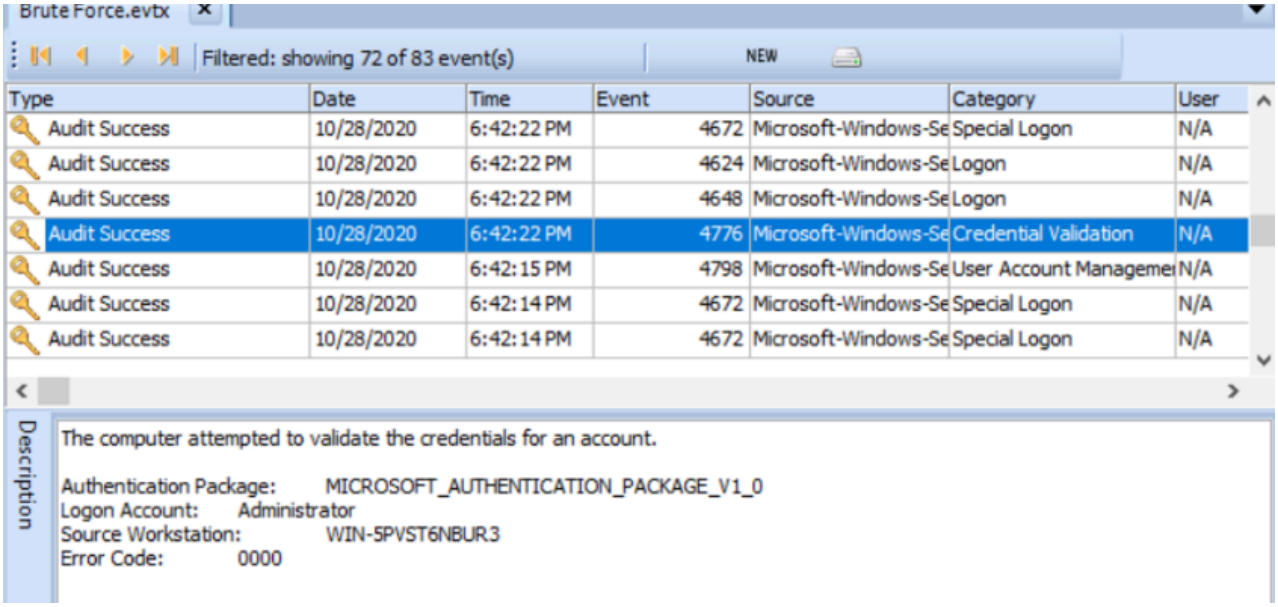

<Load filter>
Brute Force.evtx
Filtered: showing 11 of 83 event(s)
Type Date Time
Audit Failure 10/28/2020 6:39:28 PM
Audit Failure 10/28/2020 6:39:28 PM
Audit Failure 10/28/2020 6:39:28 PM
Audit Failure 10/28/2020 6:39:28 PM
Audit Failure 10/28/2020 6:39:28 PM
Audit Failure 10/28/2020 6:39:28 PM
Audit Failure 10/28/2020 6:39:28 PM
Audit Failure 10/28/2020 5:43:51 PM
Audit Failure 10/28/2020 5:43:51 PM
Audit Failure 10/28/2020 3:05:00 PM
Audit Failure 10/28/2020 3:05:00 PM
Description
An account failed to log on.
Subject:
Security ID: S-1-5-18
Account Name: WIN-5PVST6NBUR3$
Account Domain: WORKGROUP
Logon ID: 000003E7
Logon Type: 8
Description Data
d: 1
Filter
Apply filter to:
Active event log view (File: Z:\Evidence Files\Event Logs\Brute Force.evtx)
Event log view(s) on your choice
Event types
Information
Warning
Error
Critical
Verbose
Audit Success
Audit Failure
Source:
Category:
User:
Computer:
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
Filter by description params (for security event logs, e.g. Object\Object Name contains elex.exe)
New condition
Delete condition
Clear list
Name
Operator
Value
Date
Time
Separately
From: 11/27/2024 12:00:00 AM
To: 11/27/2024 12:00:00 AM
Display event for the last 0 days 0 hours
Clear
Load...
Save...
OK
Cancel


Description
An account failed to log on.
Subject:
Security ID: S-1-5-18
Account Name: WIN-5PVST6NBUR3$
Account Domain: WORKGROUP
Logon ID: 000003E7
Logon Type: 8
Description
Data

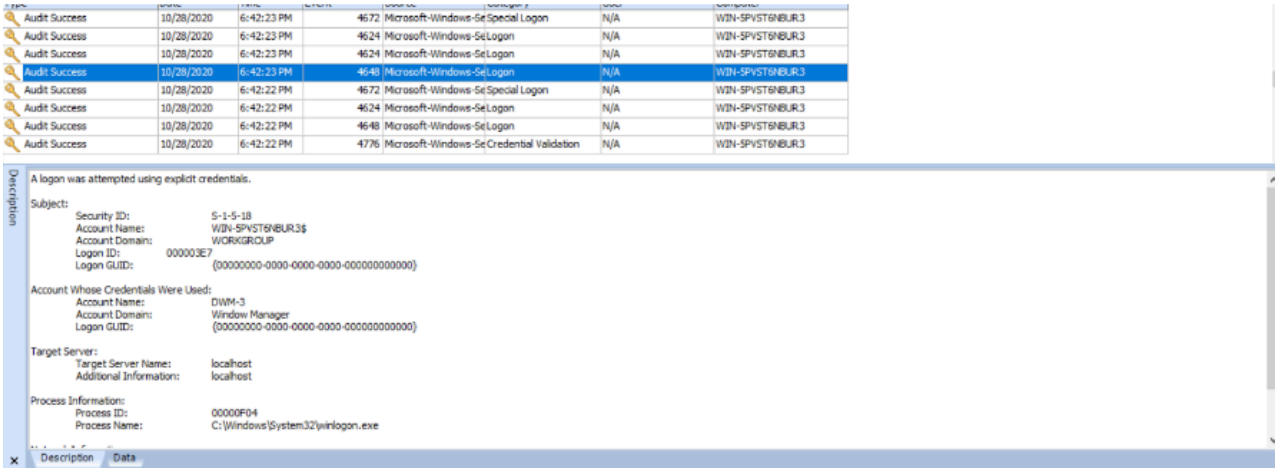

Account For Which Logon Failed:
Security ID: S-1-0-0
Account Name: Administrator
Account Domain:


Filter by description params (for security event logs, e.g. Object\Object Name contains elex.exe)
New condition
Delete condition
Clear list
Name
Operator
Value
Date
Time
Separately
From:
11/27/2024
12:00:00 AM
To:
11/27/2024
12:00:00 AM
Exclude
Display event for the last
0
days
0
hours
Exclude
Clear
Load...
Save...
OK
Cancel

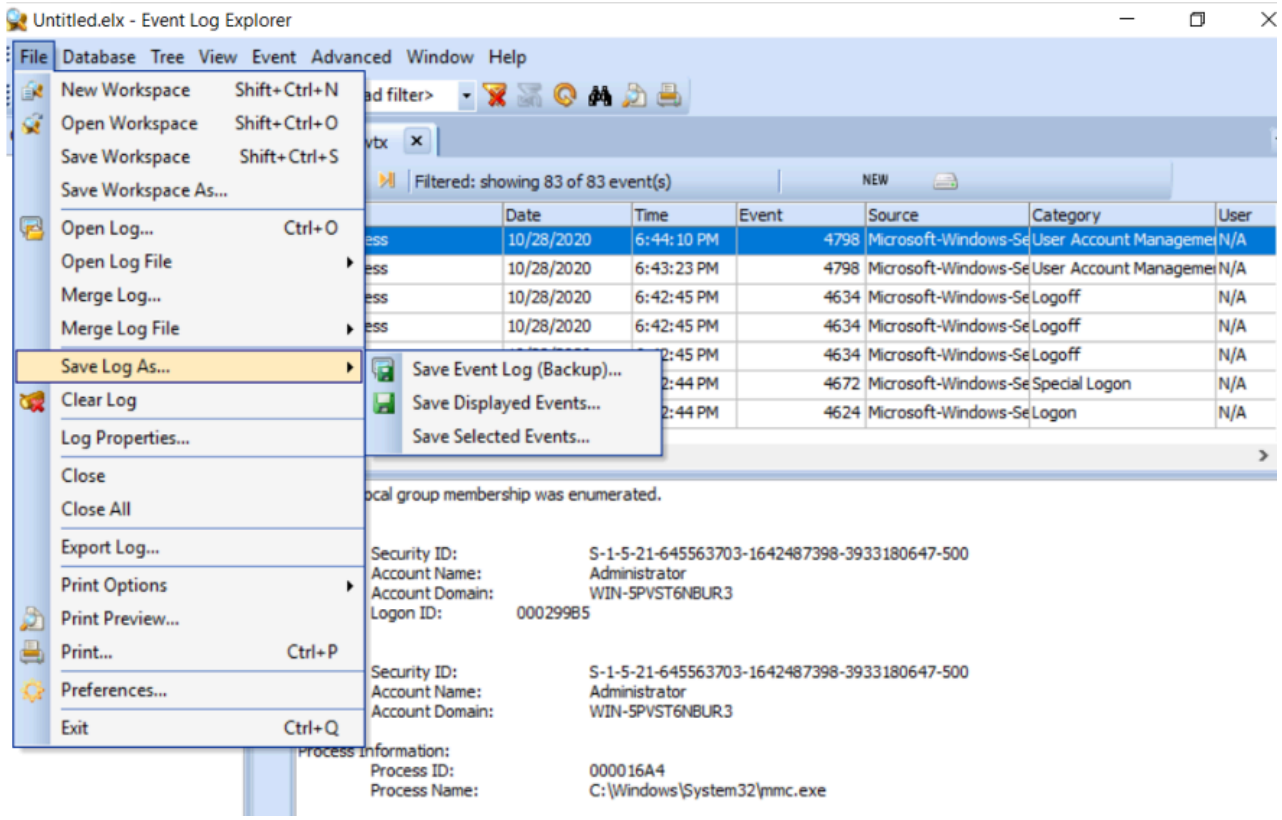

Description
The computer attempted to validate the credentials for an account.
Authentication Package: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
Logon Account: Administrator
Source Workstation: WIN-5PVST6NBUR3
Error Code: 0000
Description
Data

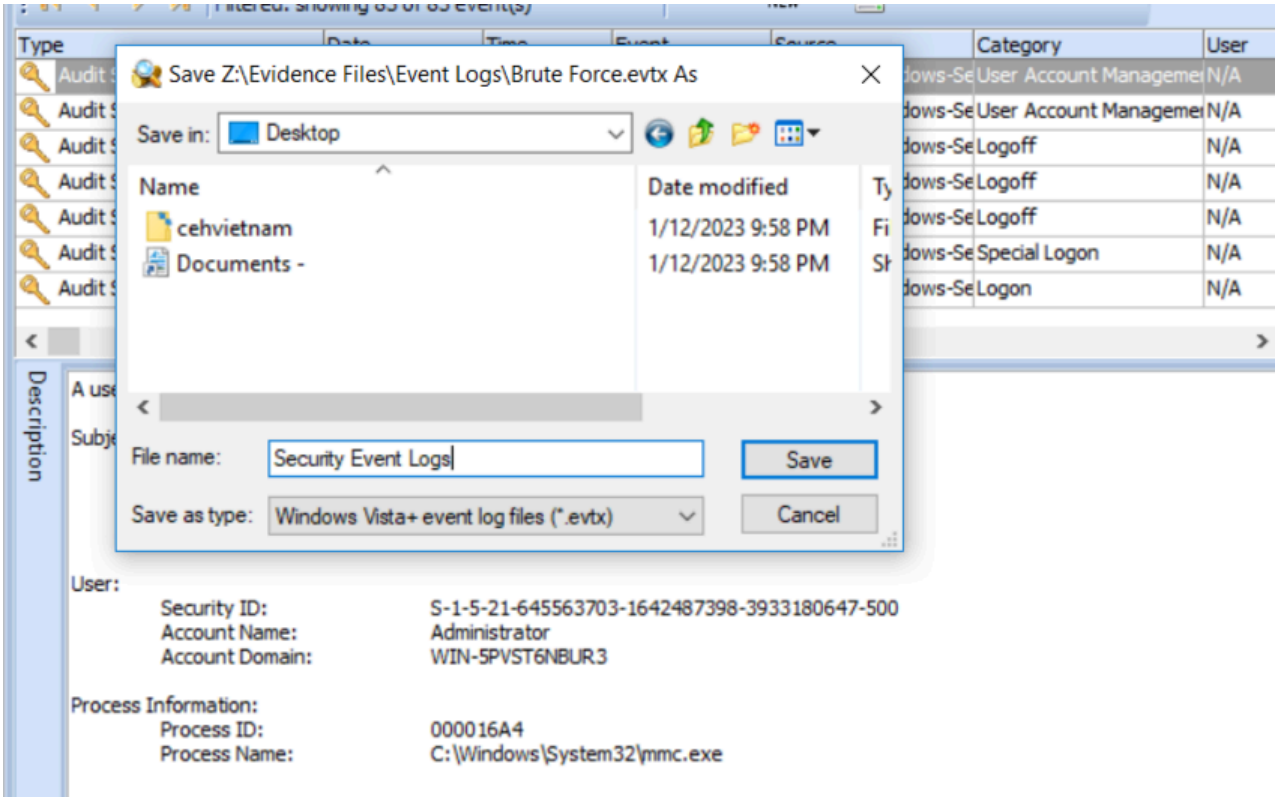

Brute Force.evtx
Filtered: showing 72 of 83 event(s)
NEW
Type
Date
Time
Event
Source
Category
User
Audit Success 10/28/2020 6:42:22 PM 4672 Microsoft-Windows-Se Special Logon N/A
Audit Success 10/28/2020 6:42:22 PM 4624 Microsoft-Windows-Se Logon N/A
Audit Success 10/28/2020 6:42:22 PM 4648 Microsoft-Windows-Se Logon N/A
Audit Success 10/28/2020 6:42:22 PM 4776 Microsoft-Windows-Se Credential Validation N/A
Audit Success 10/28/2020 6:42:15 PM 4798 Microsoft-Windows-Se User Account Manageme N/A
Audit Success 10/28/2020 6:42:14 PM 4672 Microsoft-Windows-Se Special Logon N/A
Audit Success 10/28/2020 6:42:14 PM 4672 Microsoft-Windows-Se Special Logon N/A
Description
The computer attempted to validate the credentials for an account.
Authentication Package: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
Logon Account: Administrator
Source Workstation: WIN-5PVST6NBUR3
Error Code: 0000

This implies that a logon attempt using clear, plaintext login credentials might have been made on the local machine. This might occur when an attacker/malicious user has got hold of the login credentials for a local machine.



Audit Success	10/28/2020	6:42:23 PM	4672	Microsoft-Windows-Se	Special Logon	N/A	WIN-SPVST6NBUR3
Audit Success	10/28/2020	6:42:23 PM	4624	Microsoft-Windows-Se	Logon	N/A	WIN-SPVST6NBUR3
Audit Success	10/28/2020	6:42:23 PM	4624	Microsoft-Windows-Se	Logon	N/A	WIN-SPVST6NBUR3
Audit Success	10/28/2020	6:42:23 PM	4648	Microsoft-Windows-Se	Logon	N/A	WIN-SPVST6NBUR3
Audit Success	10/28/2020	6:42:22 PM	4672	Microsoft-Windows-Se	Special Logon	N/A	WIN-SPVST6NBUR3
Audit Success	10/28/2020	6:42:22 PM	4624	Microsoft-Windows-Se	Logon	N/A	WIN-SPVST6NBUR3
Audit Success	10/28/2020	6:42:22 PM	4648	Microsoft-Windows-Se	Logon	N/A	WIN-SPVST6NBUR3
Audit Success	10/28/2020	6:42:22 PM	4776	Microsoft-Windows-Se	Credential Validation	N/A	WIN-SPVST6NBUR3





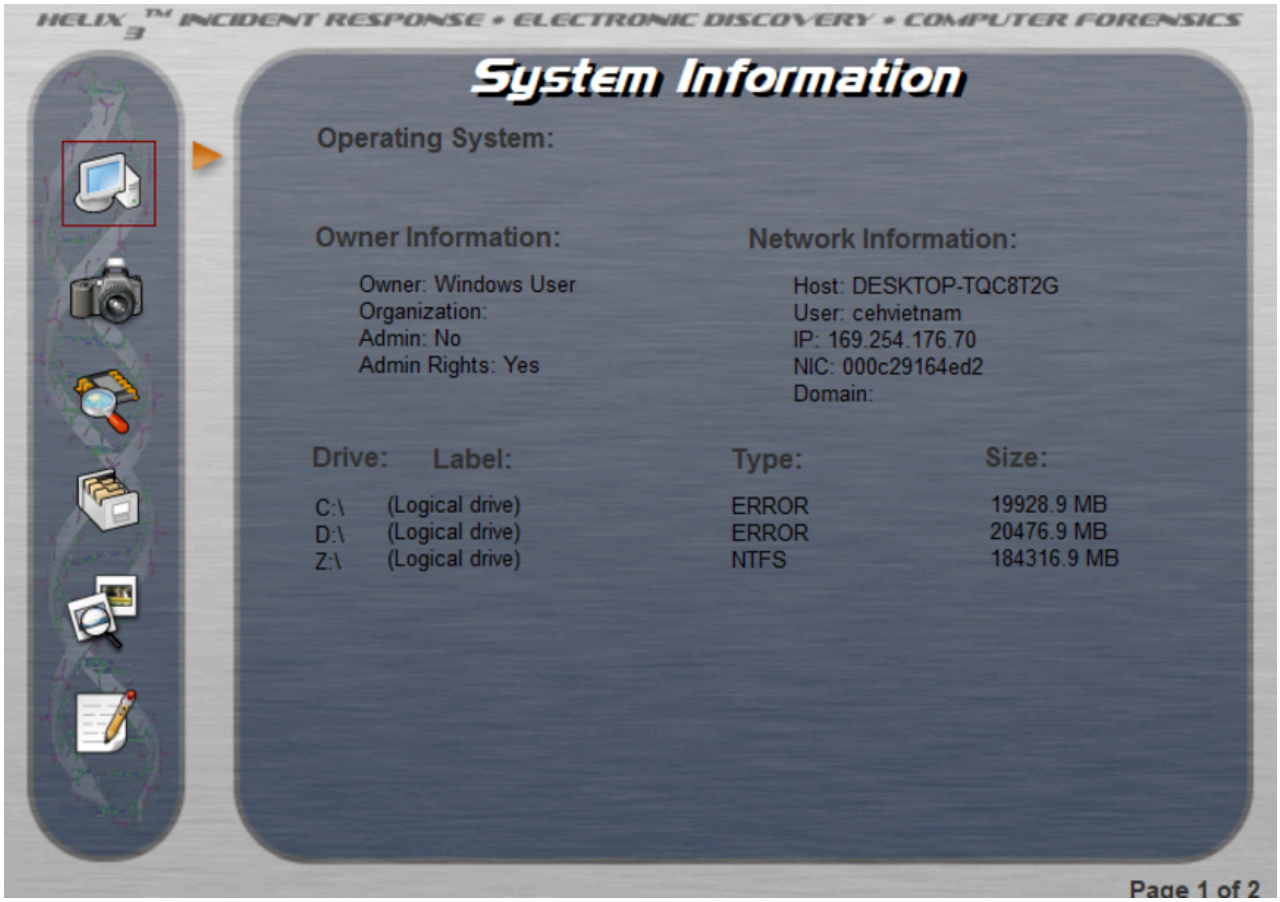
Lab 7: Performing a Digital Forensic Investigation

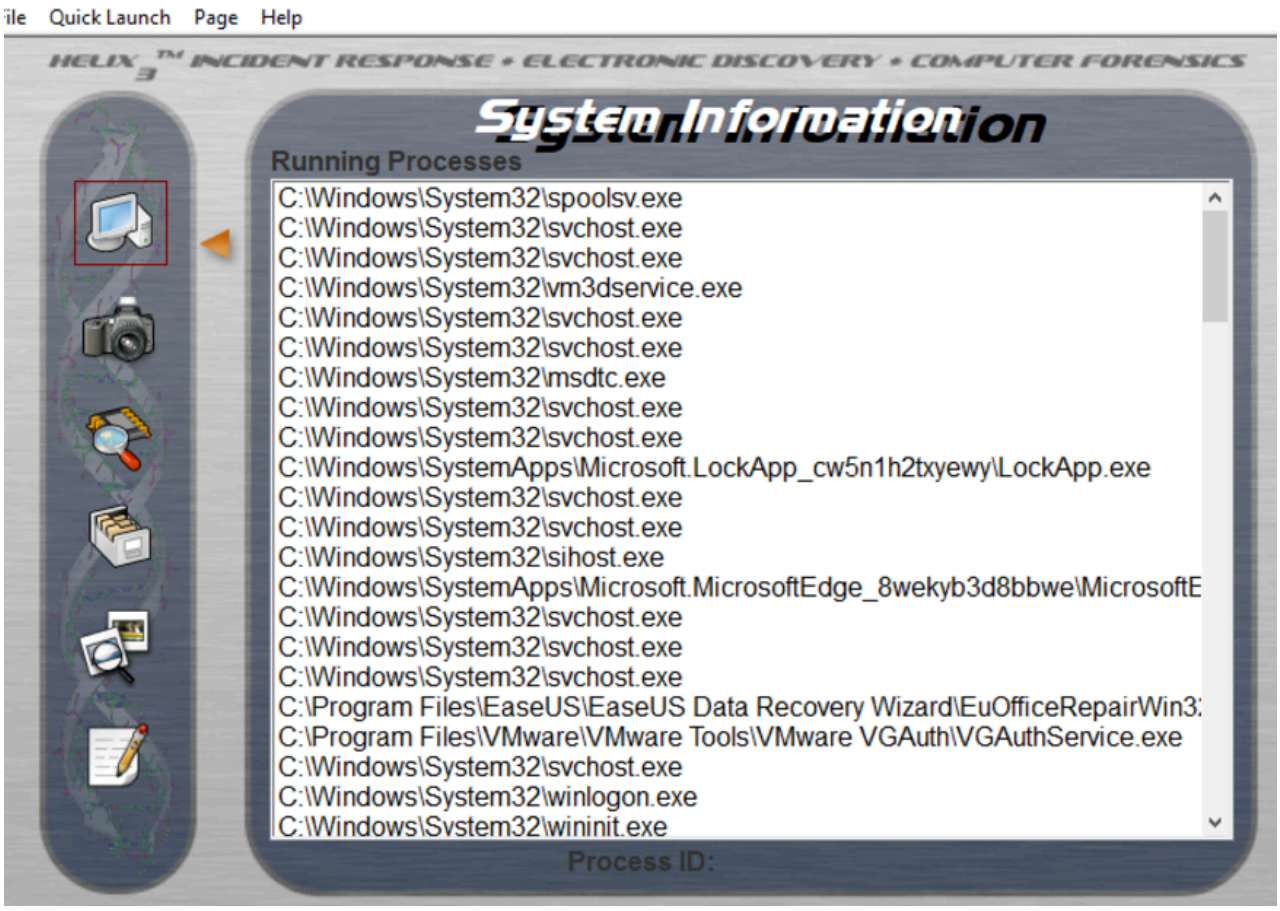
Objective

To examine system details, analyze files, and recover deleted data.

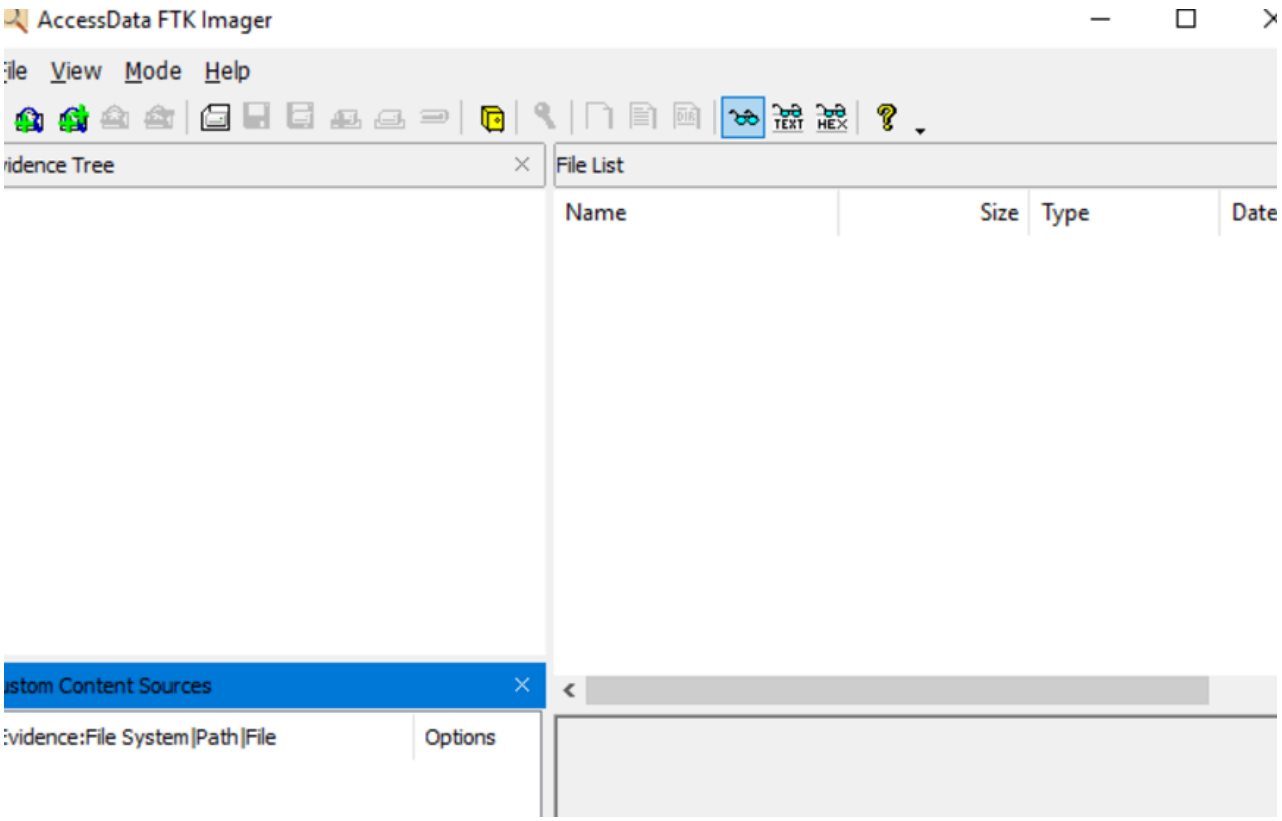
Steps

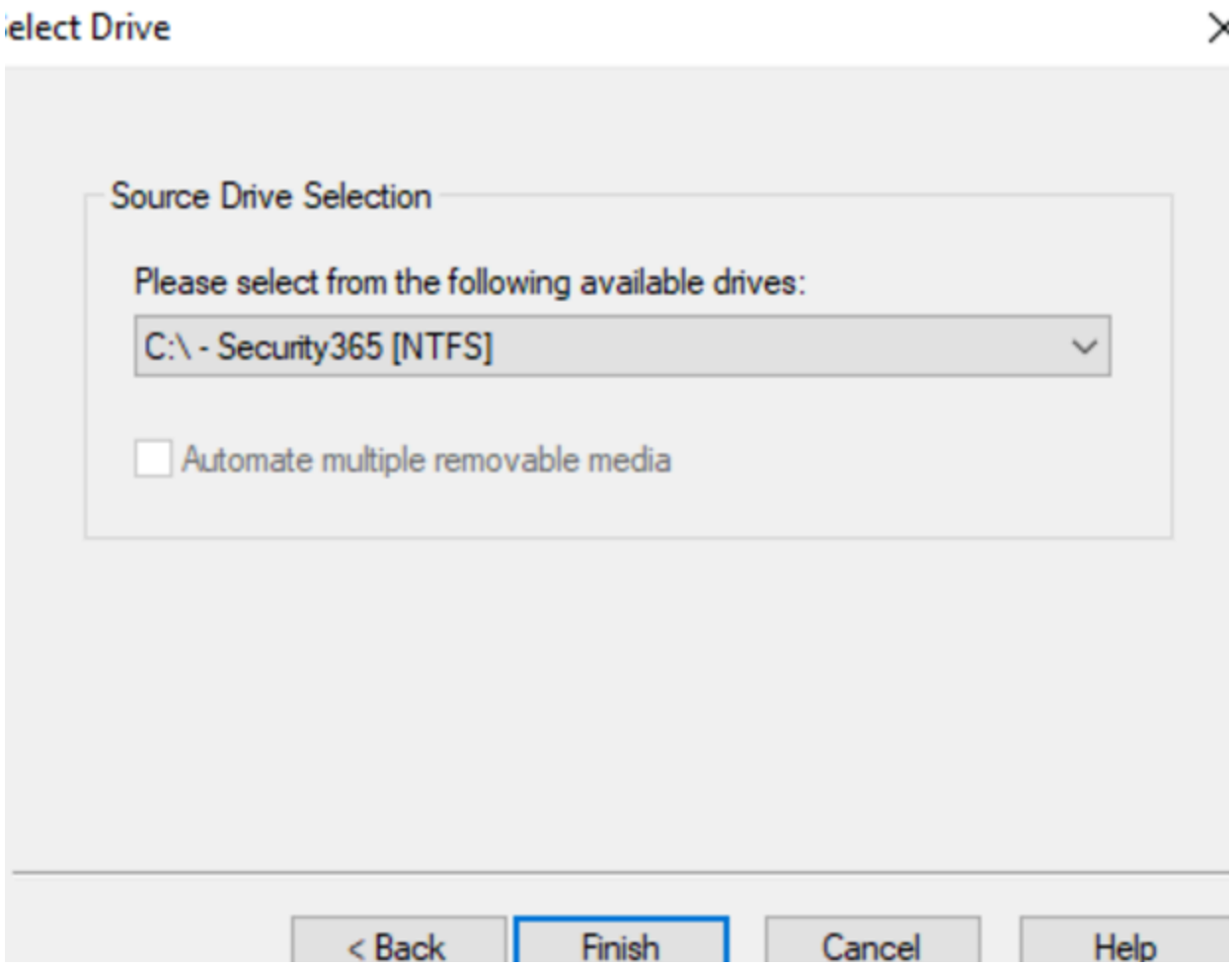
1. **View System Information**
    - Use tools like FTK Imager to create a disk image of the system.
2. **Analyze Files**
    - Select suspicious files and calculate their MD5 hash to verify integrity.
3. **Recover Deleted Files**
    - Use file recovery tools to restore deleted files and inspect their contents.

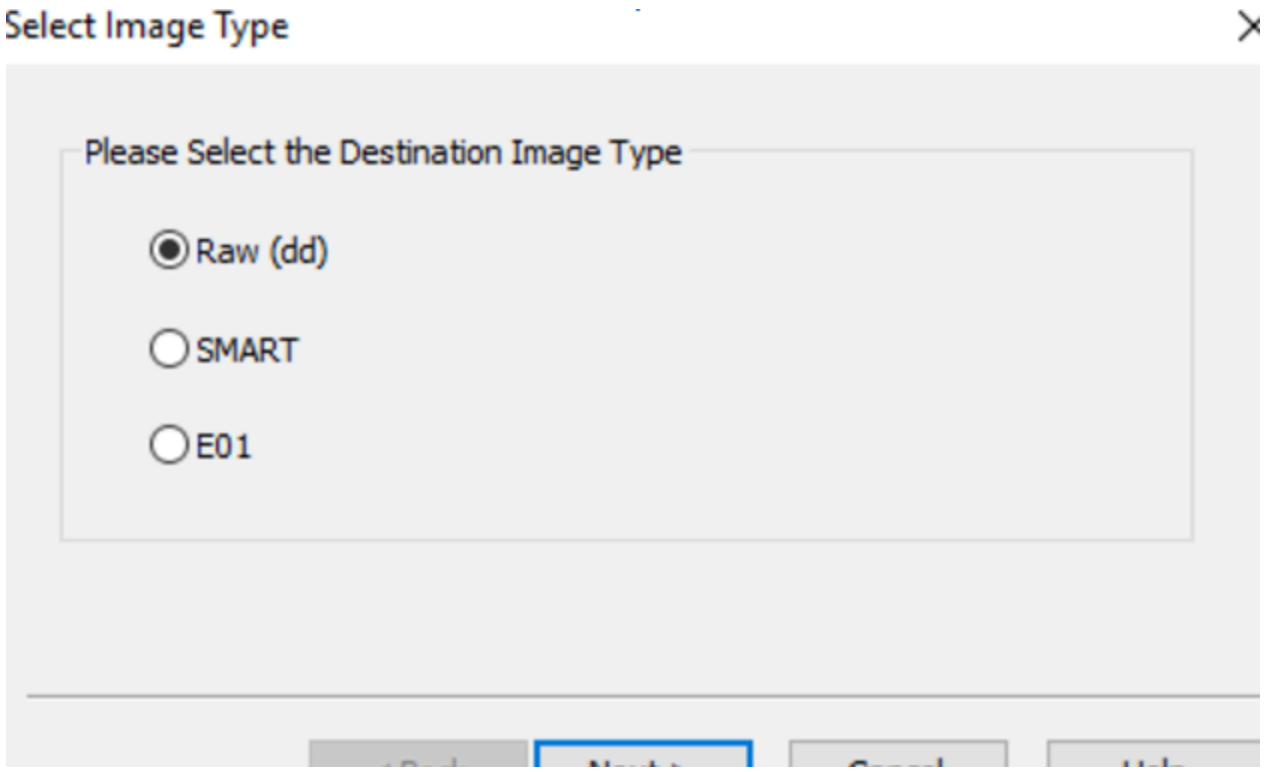

HELIX 3 ™ INCIDENT RESPONSE • ELECTRONIC DISCOVERY • COMPUTER FORENSICS
System Information
Operating System:
Owner Information:
Owner: Windows User
Organization:
Admin: No
Admin Rights: Yes
Network Information:
Host: DESKTOP-TQC8T2G
User: cehvietnam
IP: 169.254.176.70
NIC: 000c29164ed2
Domain:
Drive: Label: Type: Size:
C:\ (Logical drive) ERROR 19928.9 MB
D:\ (Logical drive) ERROR 20476.9 MB
Z:\ (Logical drive) NTFS 184316.9 MB
Page 1 of 2

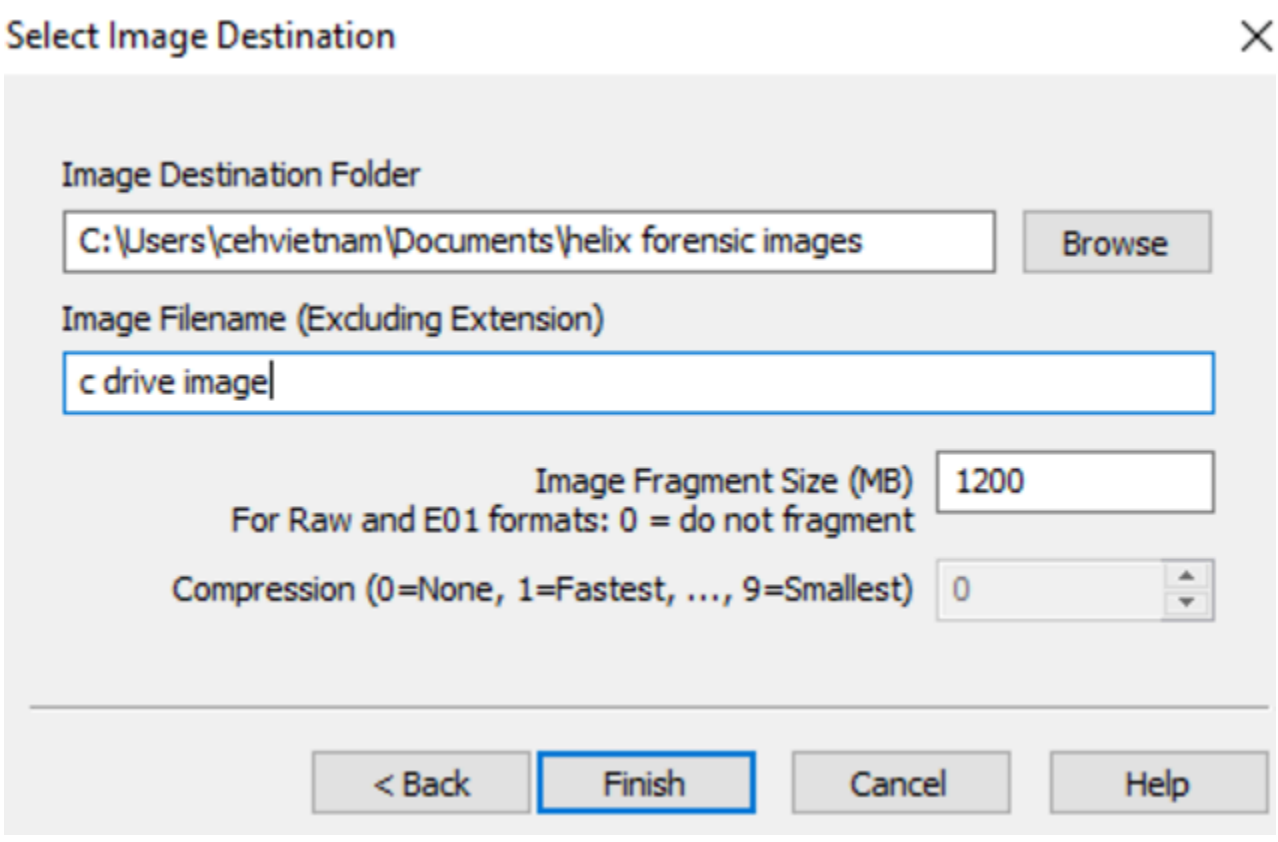

ile Quick Launch Page Help
HELIX 3 INCIDENT RESPONSE • ELECTRONIC DISCOVERY • COMPUTER FORENSICS
System Information
Running Processes
C:\Windows\System32\spoolsv.exe
C:\Windows\System32\svchost.exe
C:\Windows\System32\svchost.exe
C:\Windows\System32\vm3dservice.exe
C:\Windows\System32\svchost.exe
C:\Windows\System32\svchost.exe
C:\Windows\System32\msdtc.exe
C:\Windows\System32\svchost.exe
C:\Windows\System32\svchost.exe
C:\Windows\SystemApps\Microsoft.LockApp_cw5n1h2txyewy\LockApp.exe
C:\Windows\System32\svchost.exe
C:\Windows\System32\svchost.exe
C:\Windows\System32\sihost.exe
C:\Windows\SystemApps\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\MicrosoftE
C:\Windows\System32\svchost.exe
C:\Windows\System32\svchost.exe
C:\Windows\System32\svchost.exe
C:\Program Files\EaseUS\EaseUS Data Recovery Wizard\EuOfficeRepairWin3
C:\Program Files\VMware\VMware Tools\VMware VGAuth\VGAuthService.exe
C:\Windows\System32\svchost.exe
C:\Windows\System32\winlogon.exe
C:\Windows\System32\wininit.exe
Process ID:


File Quick Launch Page Help
HELIX 3 ™ INCIDENT RESPONSE • ELECTRONIC DISCOVERY • COMPUTER FORENSICS
Live Acquisition
AccessData
FTK Imager
Version 2.5.3
FTK Imager allows you to acquire physical device images and logically view data from FAT, NTFS, EXT 2 and 3 as well as HFS and HPFS file systems.
Additionally, FTK Imager allows you to truly multi-task by creating multiple images from a single source and / or multiple images simultaneously. FTK Imager generates DD, SMART and Encase® images and reads several other industry standard formats.
With Isobuster technology built in, FTK Imager provides ready access to CDFS and DVD file systems - to include multi and open session CDs.
Additional functionality of Imager:
* Acquire locked system files (such as SAM / SYSTEM / NTUSER)
* Hash physically or logically for verification (MD5 and SHA1)
* Preview media (thumbnail views, keyword searches, properties)
Imager
Page 2 of 3


AccessData FTK Imager
File View Mode Help
Evidence Tree
File List
Name
Size
Type
Date
Custom Content Sources
Evidence:File System|Path|File
Options


elect Drive
Source Drive Selection
Please select from the following available drives:
C:\ - Security365 [NTFS]
Automate multiple removable media
< Back
Finish
Cancel
Help


Select Image Type
Please Select the Destination Image Type
Raw (dd)
SMART
E01


Select Image Destination
Image Destination Folder
C:\Users\cehvietnam\Documents\helix forensic images
Browse
Image Filename (Excluding Extension)
c drive image
Image Fragment Size (MB)
For Raw and E01 formats: 0 = do not fragment
1200
Compression (0=None, 1=Fastest, ..., 9=Smallest)
0
< Back
Finish
Cancel
Help

c drive image.001	11/26/2024 2:13 PM	001 File	1,024,000 KB
c drive image.001	11/26/2024 2:23 PM	Text Document	2 KB
c drive image.002	11/26/2024 2:14 PM	002 File	1,024,000 KB
c drive image.003	11/26/2024 2:14 PM	003 File	1,024,000 KB
c drive image.004	11/26/2024 2:14 PM	004 File	1,024,000 KB
c drive image.005	11/26/2024 2:15 PM	005 File	1,024,000 KB
c drive image.006	11/26/2024 2:15 PM	006 File	1,024,000 KB
c drive image.007	11/26/2024 2:15 PM	007 File	1,024,000 KB

Select Drive to Preview...

Select a physical disk partition to preview

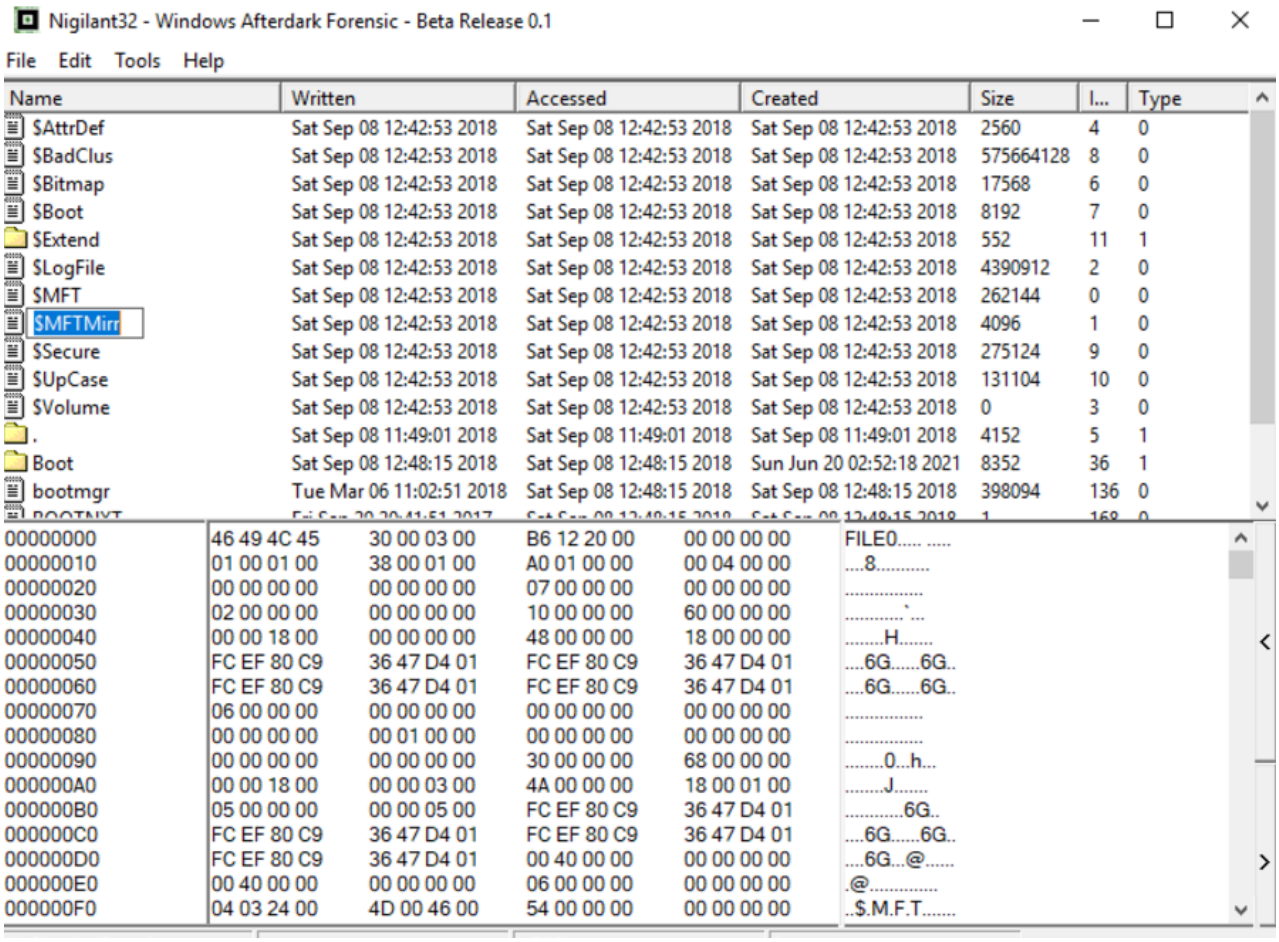
PhysicalDrive Name	Partition Number	Partition Length	Starting Offset	Drive Nur
PhysicalDrive0:Totalsize:21467980800 Bytes	Partition:1	575668224 Bytes	1048576	0
PhysicalDrive0:Totalsize:21467980800 Bytes	Partition:2	20897071104 Bytes	576716800	0
PhysicalDrive1:Totalsize:193269404160 Bytes	Partition:1	193270382592 Bytes	1048576	1
PhysicalDrive2:Totalsize:21467980800 Bytes	Partition:1	21471690752 Bytes	1048576	2

Cancel Apply

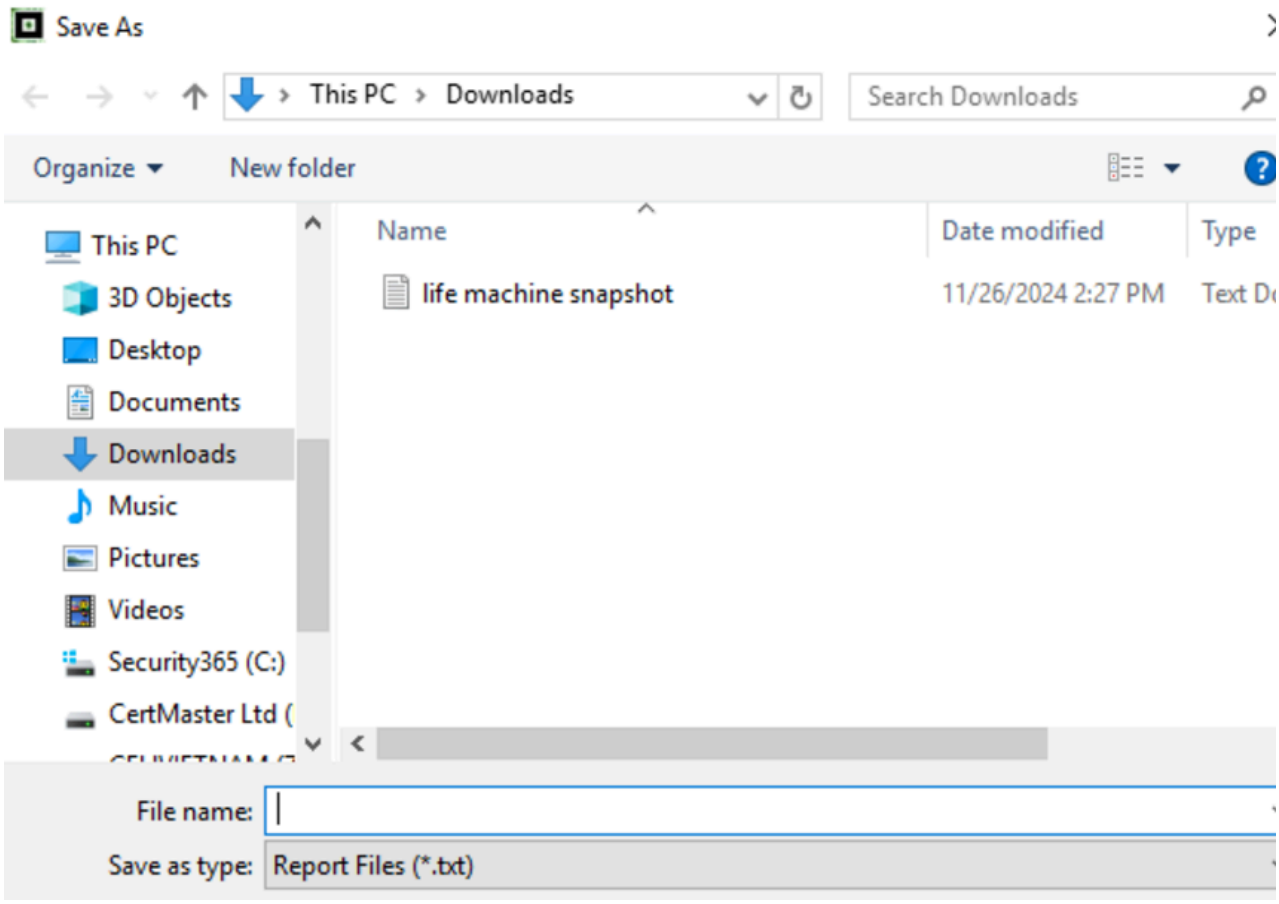
Nigilant32 - Windows Afterdark Forensic - Beta Release 0.1

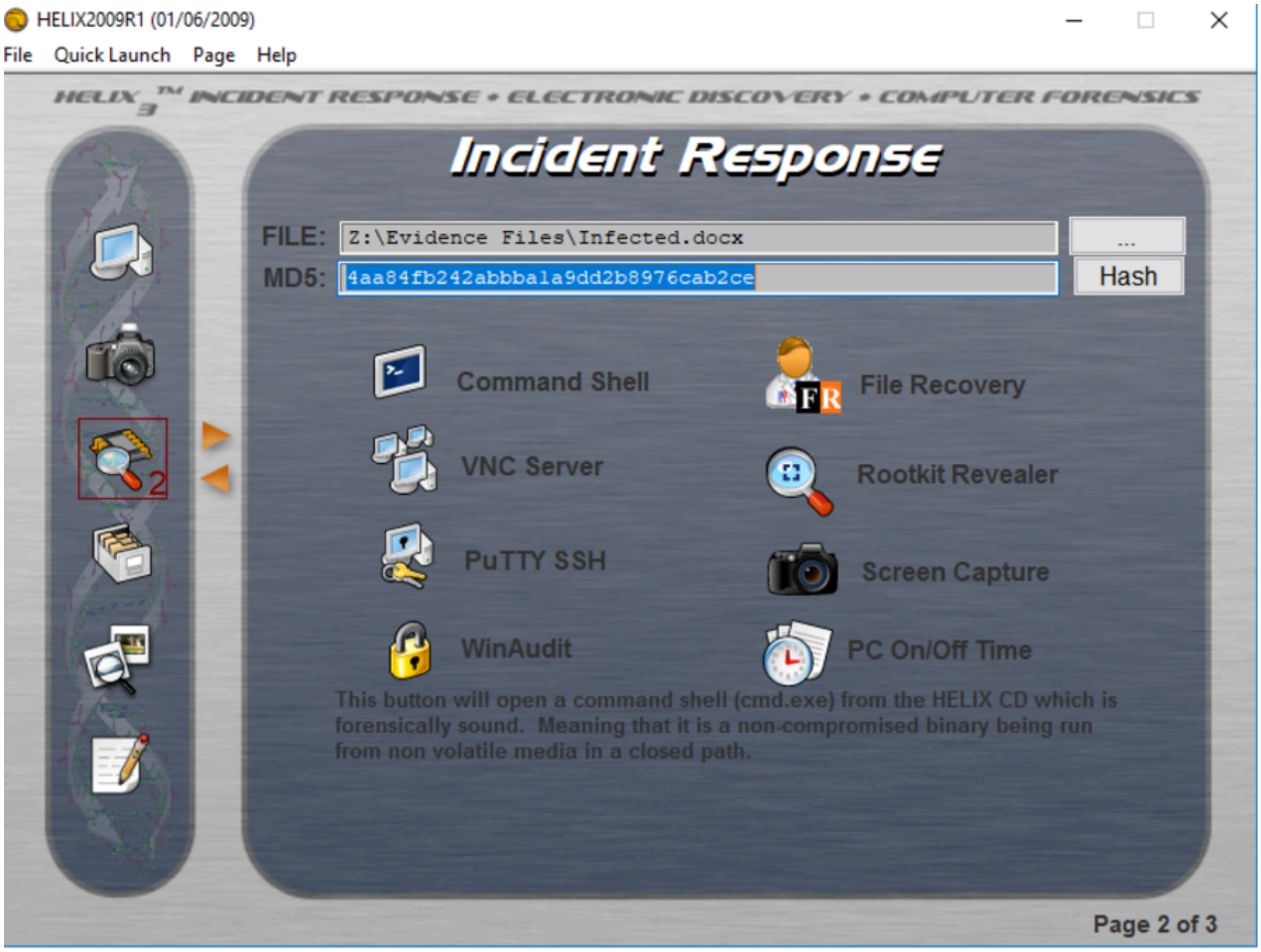
File Edit Tools Help

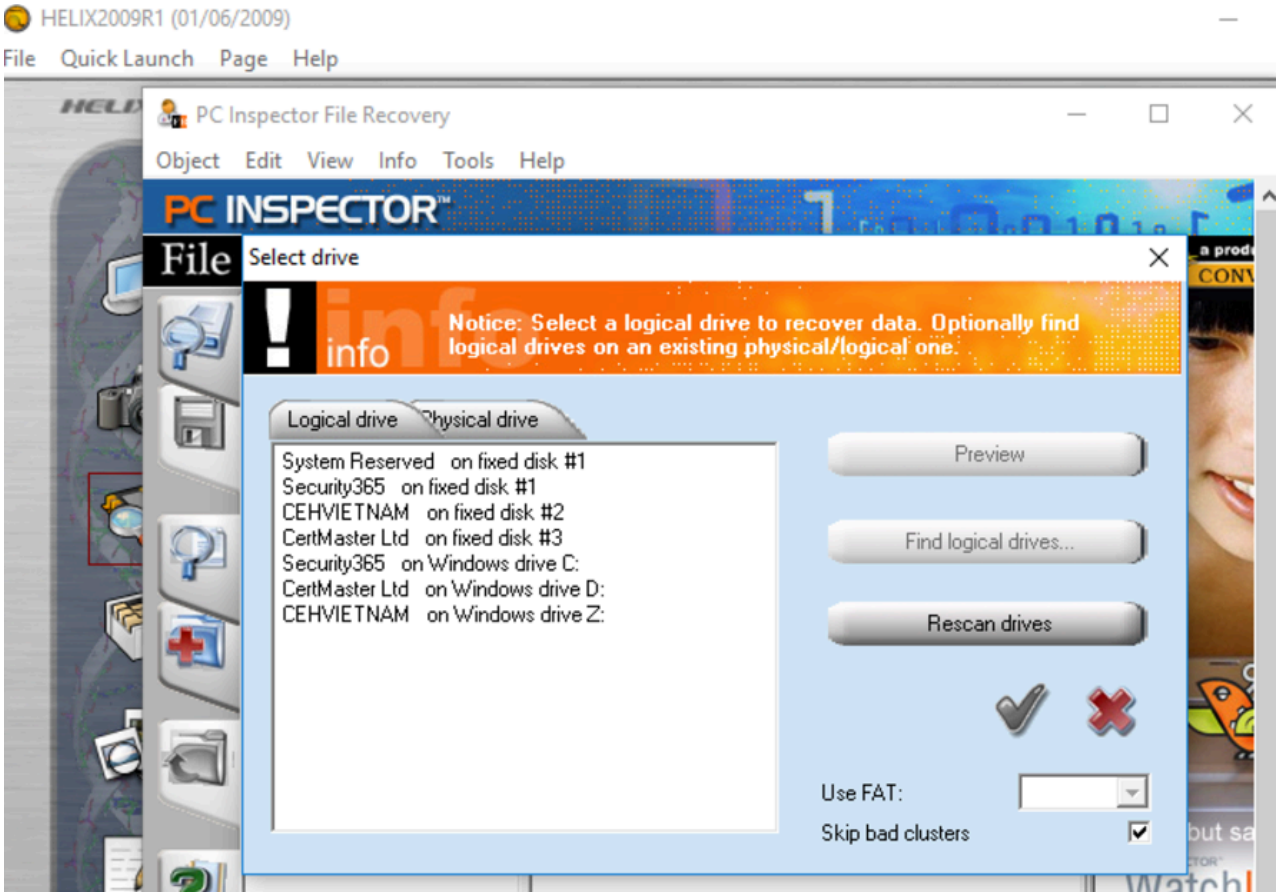
Name	Written	Accessed	Created	Size	I...	Type
$AttrDef	Sat Sep 08 12:42:53 2018	Sat Sep 08 12:42:53 2018	Sat Sep 08 12:42:53 2018	2560	4	0
$BadClus	Sat Sep 08 12:42:53 2018	Sat Sep 08 12:42:53 2018	Sat Sep 08 12:42:53 2018	575664128	8	0
$Bitmap	Sat Sep 08 12:42:53 2018	Sat Sep 08 12:42:53 2018	Sat Sep 08 12:42:53 2018	17568	6	0
$Boot	Sat Sep 08 12:42:53 2018	Sat Sep 08 12:42:53 2018	Sat Sep 08 12:42:53 2018	8192	7	0
$Extend	Sat Sep 08 12:42:53 2018	Sat Sep 08 12:42:53 2018	Sat Sep 08 12:42:53 2018	552	11	1
$LogFile	Sat Sep 08 12:42:53 2018	Sat Sep 08 12:42:53 2018	Sat Sep 08 12:42:53 2018	4390912	2	0
$MFT	Sat Sep 08 12:42:53 2018	Sat Sep 08 12:42:53 2018	Sat Sep 08 12:42:53 2018	262144	0	0
$MFTMirr	Sat Sep 08 12:42:53 2018	Sat Sep 08 12:42:53 2018	Sat Sep 08 12:42:53 2018	4096	1	0
$Secure	Sat Sep 08 12:42:53 2018	Sat Sep 08 12:42:53 2018	Sat Sep 08 12:42:53 2018	275124	9	0
$UpCase	Sat Sep 08 12:42:53 2018	Sat Sep 08 12:42:53 2018	Sat Sep 08 12:42:53 2018	131104	10	0
$Volume	Sat Sep 08 12:42:53 2018	Sat Sep 08 12:42:53 2018	Sat Sep 08 12:42:53 2018	0	3	0
.	Sat Sep 08 11:49:01 2018	Sat Sep 08 11:49:01 2018	Sat Sep 08 11:49:01 2018	4152	5	1
Boot	Sat Sep 08 12:48:15 2018	Sat Sep 08 12:48:15 2018	Sun Jun 20 02:52:18 2021	8352	36	1
bootmgr	Tue Mar 06 11:02:51 2018	Sat Sep 08 12:48:15 2018	Sat Sep 08 12:48:15 2018	398094	136	0

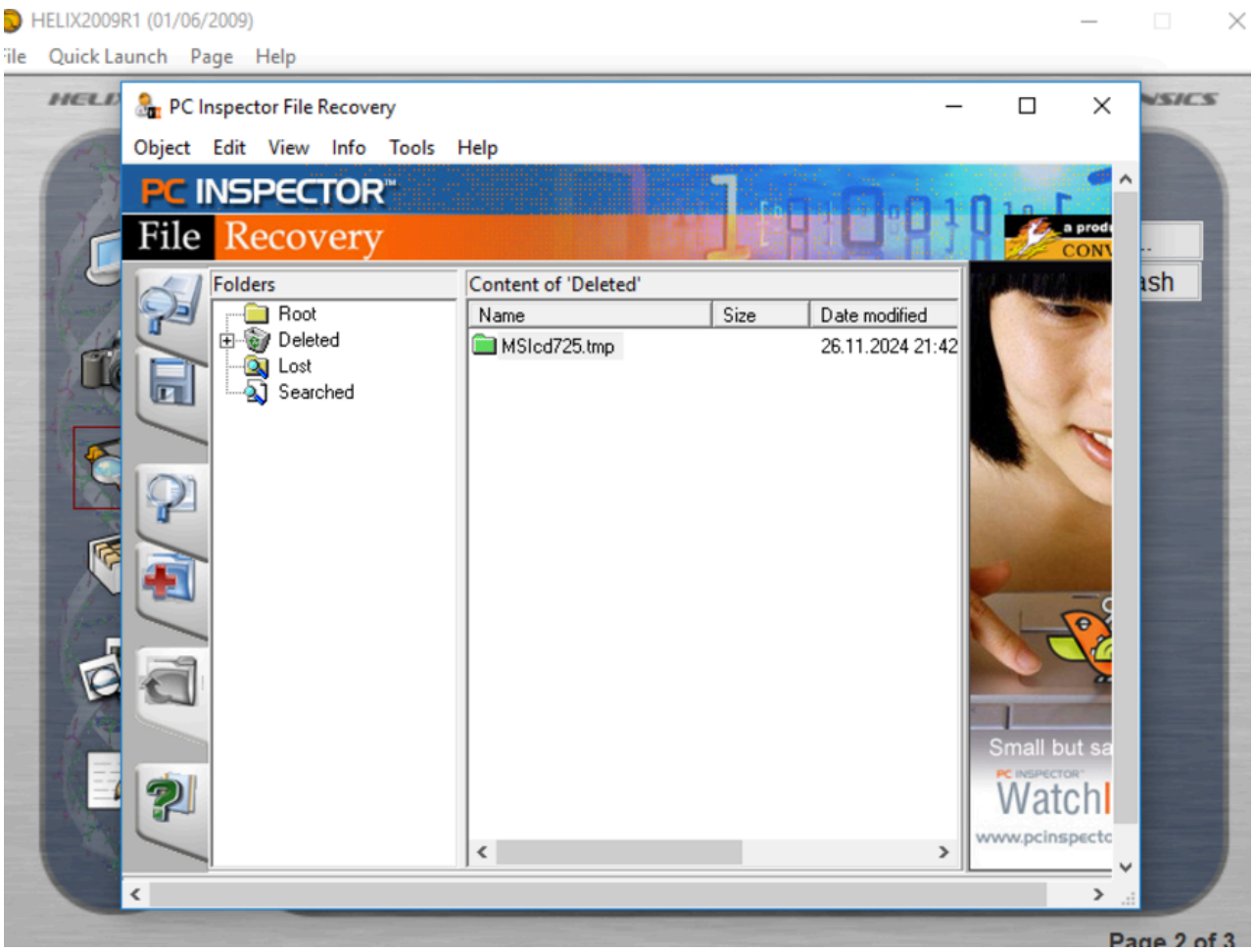

Nigilant32 - Windows Afterdark Forensic - Beta Release 0.1
File Edit Tools Help
Name Written Accessed Created Size I... Type
$AttrDef Sat Sep 08 12:42:53 2018 Sat Sep 08 12:42:53 2018 Sat Sep 08 12:42:53 2018 2560 4 0
$BadClus Sat Sep 08 12:42:53 2018 Sat Sep 08 12:42:53 2018 Sat Sep 08 12:42:53 2018 575664128 8 0
$Bitmap Sat Sep 08 12:42:53 2018 Sat Sep 08 12:42:53 2018 Sat Sep 08 12:42:53 2018 17568 6 0
$Boot Sat Sep 08 12:42:53 2018 Sat Sep 08 12:42:53 2018 Sat Sep 08 12:42:53 2018 8192 7 0
$Extend Sat Sep 08 12:42:53 2018 Sat Sep 08 12:42:53 2018 Sat Sep 08 12:42:53 2018 552 11 1
$LogFile Sat Sep 08 12:42:53 2018 Sat Sep 08 12:42:53 2018 Sat Sep 08 12:42:53 2018 4390912 2 0
$MFT Sat Sep 08 12:42:53 2018 Sat Sep 08 12:42:53 2018 Sat Sep 08 12:42:53 2018 262144 0 0
$MFTMirr Sat Sep 08 12:42:53 2018 Sat Sep 08 12:42:53 2018 Sat Sep 08 12:42:53 2018 4096 1 0
$Secure Sat Sep 08 12:42:53 2018 Sat Sep 08 12:42:53 2018 Sat Sep 08 12:42:53 2018 275124 9 0
$UpCase Sat Sep 08 12:42:53 2018 Sat Sep 08 12:42:53 2018 Sat Sep 08 12:42:53 2018 131104 10 0
$Volume Sat Sep 08 12:42:53 2018 Sat Sep 08 12:42:53 2018 Sat Sep 08 12:42:53 2018 0 3 0
. Sat Sep 08 11:49:01 2018 Sat Sep 08 11:49:01 2018 Sat Sep 08 11:49:01 2018 4152 5 1
Boot Sat Sep 08 12:48:15 2018 Sat Sep 08 12:48:15 2018 Sun Jun 20 02:52:18 2021 8352 36 1
bootmgr Tue Mar 06 11:02:51 2018 Sat Sep 08 12:48:15 2018 Sat Sep 08 12:48:15 2018 398094 136 0
00000000 46 49 4C 45 30 00 03 00 B6 12 20 00 00 00 00 00 FILE0..... .....
00000010 01 00 01 00 38 00 01 00 A0 01 00 00 00 04 00 00 ....8.....
00000020 00 00 00 00 00 00 00 00 07 00 00 00 00 00 00 00 ....
00000030 02 00 00 00 00 00 00 00 10 00 00 00 60 00 00 00 ....`...
00000040 00 00 18 00 00 00 00 00 48 00 00 00 18 00 00 00 ....H.......
00000050 FC EF 80 C9 36 47 D4 01 FC EF 80 C9 36 47 D4 01 ....6G......6G..
00000060 FC EF 80 C9 36 47 D4 01 FC EF 80 C9 36 47 D4 01 ....6G......6G..
00000070 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00000080 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 ....
00000090 00 00 00 00 00 00 00 00 30 00 00 00 68 00 00 00 ....0...h...
000000A0 00 00 18 00 00 00 03 00 4A 00 00 00 18 00 01 00 ....J.......
000000B0 05 00 00 00 00 00 05 00 FC EF 80 C9 36 47 D4 01 ....6G..
000000C0 FC EF 80 C9 36 47 D4 01 FC EF 80 C9 36 47 D4 01 ....6G......6G..
000000D0 FC EF 80 C9 36 47 D4 01 00 40 00 00 00 00 00 00 ....6G...@......
000000E0 00 40 00 00 00 00 00 00 06 00 00 00 00 00 00 00 .@..............
000000F0 04 03 24 00 4D 00 46 00 54 00 00 00 00 00 00 00 ..$.M.F.T.......

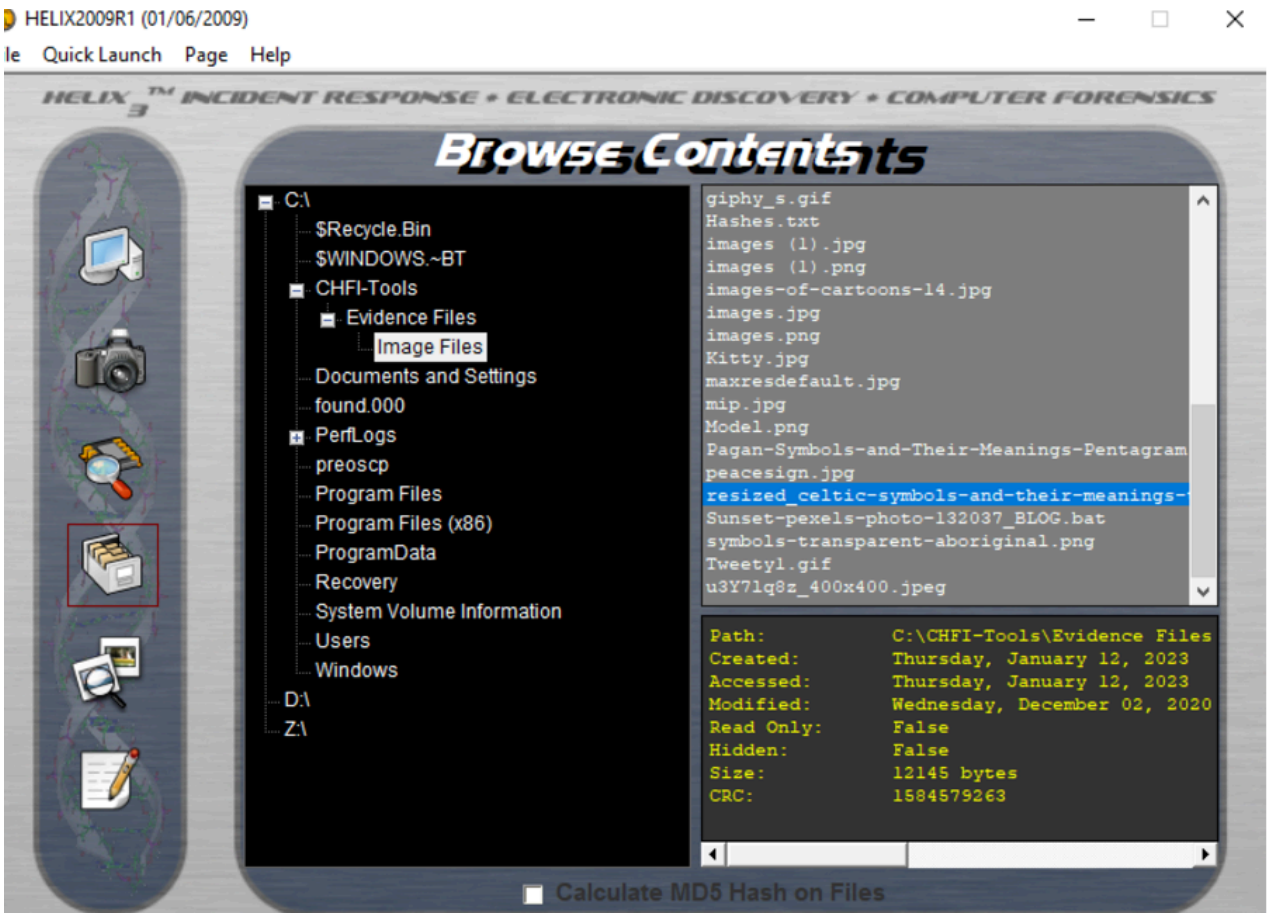

Nigilant32 - Windows Afterdark Forensic - Beta Release 0.1
File Edit Tools Help
Live Machine Snapshot
Service Start Type:On Demand Start
Service Display Name: User Data Access_43a72
Service Name: UserDataSvc_43a72
Binary Path:C:\Windows\system32\svchost.exe -k UnistackSvcGroup
Process Id: 0
Service Start Type:On Demand Start
Service Display Name: Windows Push Notifications User Service_43a72
Service Name: WpnUserService_43a72
Binary Path:C:\Windows\system32\svchost.exe -k UnistackSvcGroup
Process Id: 4676
Service Start Type:Startup
Service Display Name: MpKsl76f6d81b
Service Name: MpKsl76f6d81b
Binary Path:\??\C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{8153AB58-14D9-4AD2-A32A-6273DB51576B}\MpKsl76f6d81b.sys
Process Id: 0
Service Start Type:Service Start on IoInitSystem (Driver)
Error Retrieving Scheduled Task Information

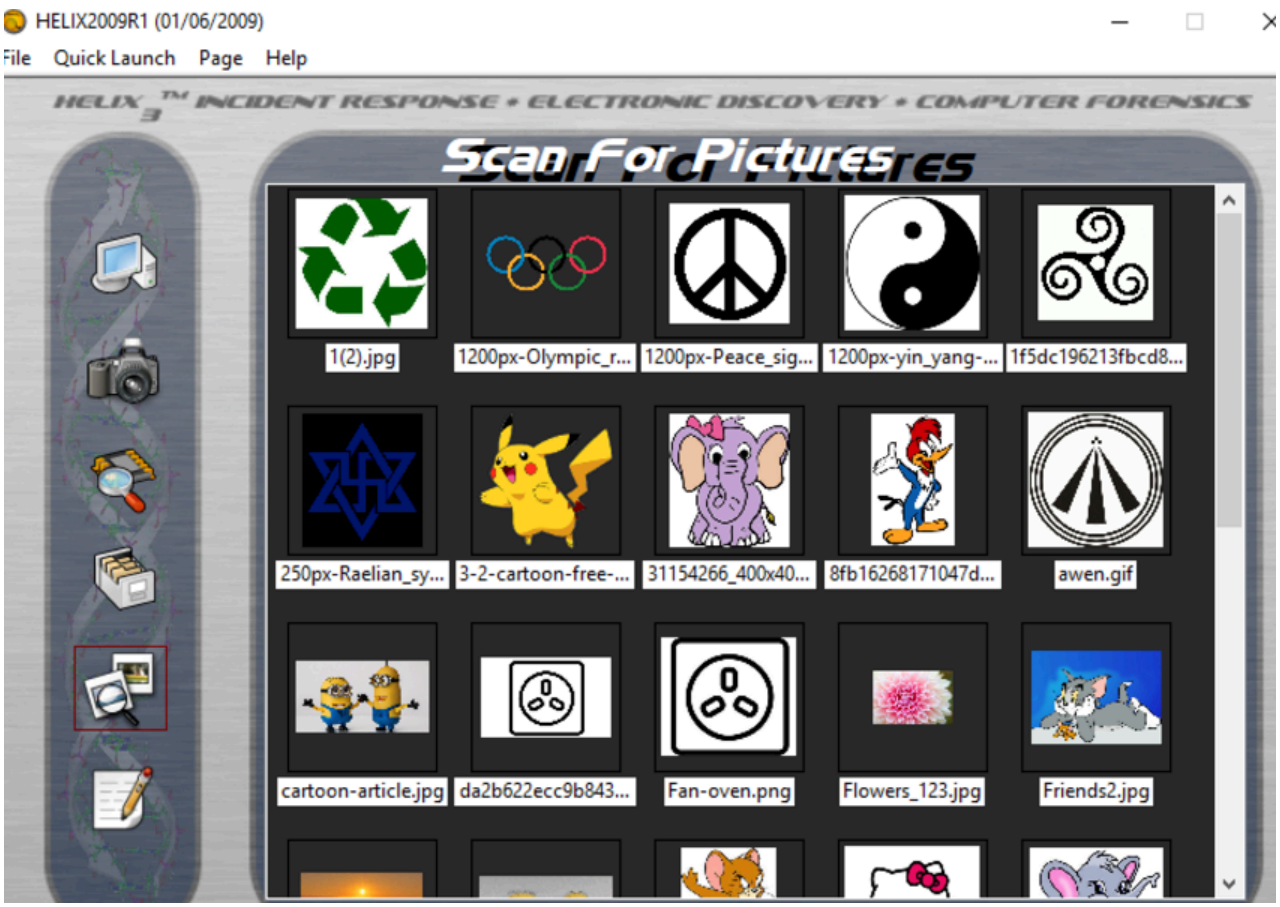

Save As
This PC
Downloads
Search Downloads
Organize
New folder
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Security365 (C:)
CertMaster Ltd (
Name
Date modified
Type
life machine snapshot
11/26/2024 2:27 PM
File name:
Save as type:
Report Files (*.txt)

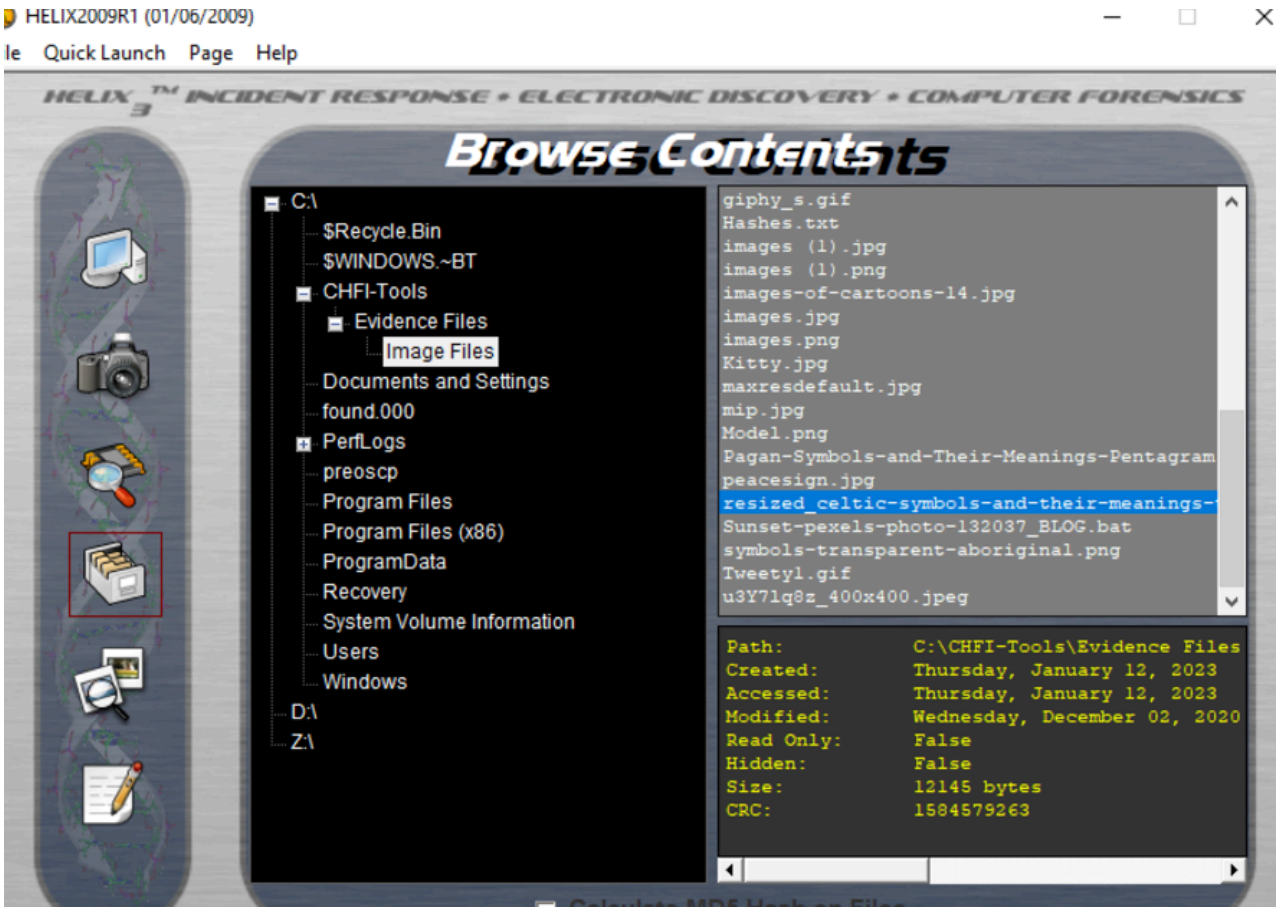

HELIX2009R1 (01/06/2009)
File Quick Launch Page Help
HELIX 3 INCIDENT RESPONSE • ELECTRONIC DISCOVERY • COMPUTER FORENSICS
Incident Response
FILE: Z:\Evidence Files\Infected.docx
...
MD5: 4aa84fb242abbbala9dd2b8976cab2ce
Hash
Command Shell
File Recovery
VNC Server
Rootkit Revealer
PuTTY SSH
Screen Capture
WinAudit
PC On/Off Time
This button will open a command shell (cmd.exe) from the HELIX CD which is forensically sound. Meaning that it is a non-compromised binary being run from non volatile media in a closed path.
Page 2 of 3

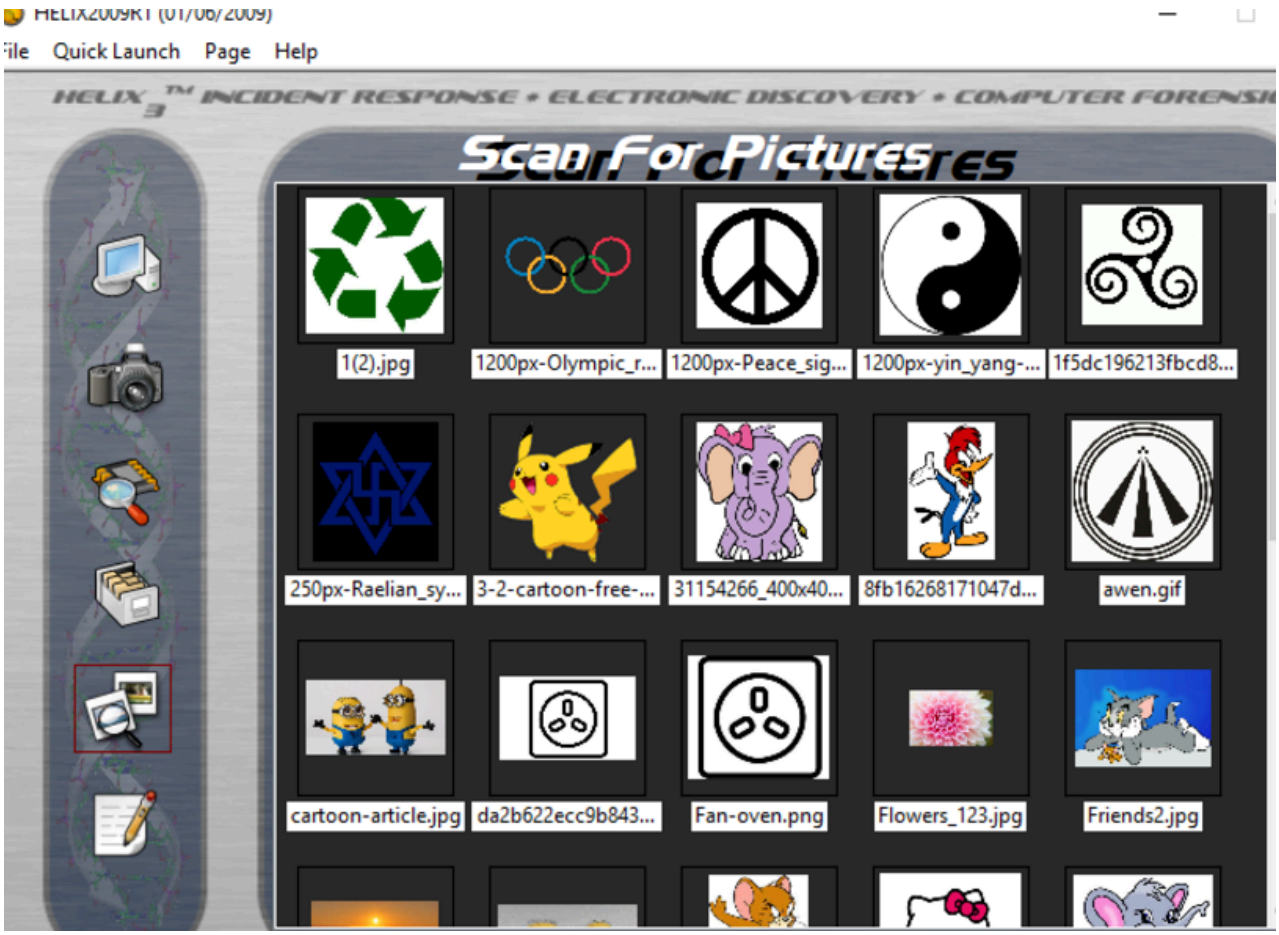

HELIX2009R1 (01/06/2009)
File Quick Launch Page Help
PC Inspector File Recovery
Object Edit View Info Tools Help
PC INSPECTOR
File
Select drive
Notice: Select a logical drive to recover data. Optionally find logical drives on an existing physical/logical one.
Logical drive
Physical drive
System Reserved on fixed disk #1
Security365 on fixed disk #1
CEHVIETNAM on fixed disk #2
CertMaster Ltd on fixed disk #3
Security365 on Windows drive C:
CertMaster Ltd on Windows drive D:
CEHVIETNAM on Windows drive Z:
Preview
Find logical drives...
Rescan drives
Use FAT:
Skip bad clusters


HELIX2009R1 (01/06/2009)
File Quick Launch Page Help
PC Inspector File Recovery
Object Edit View Info Tools Help
PC INSPECTOR
File Recovery
Folders
Root
Deleted
Lost
Searched
Content of 'Deleted'
Name
Size
Date modified
MSIcd725.tmp
26.11.2024 21:42
Small but sa
Watchl
www.pcinspecto
Page 2 of 3


HELIX2009R1 (01/06/2009)
le Quick Launch Page Help
HELIX 3 INCIDENT RESPONSE • ELECTRONIC DISCOVERY • COMPUTER FORENSICS
Browse Contents
C:\
$Recycle.Bin
$WINDOWS.~BT
CHFI-Tools
Evidence Files
Image Files
Documents and Settings
found.000
PerfLogs
preoscp
Program Files
Program Files (x86)
ProgramData
Recovery
System Volume Information
Users
Windows
D:\
Z:\
giphy_s.gif
Hashes.txt
images (1).jpg
images (1).png
images-of-cartoons-14.jpg
images.jpg
images.png
Kitty.jpg
maxresdefault.jpg
mip.jpg
Model.png
Pagan-Symbols-and-Their-Meanings-Pentagram
peacesign.jpg
resized_celtic-symbols-and-their-meanings-
Sunset-pexels-photo-132037_BLOG.bat
symbols-transparent-aboriginal.png
Tweety1.gif
u3Y7lq8z_400x400.jpeg
Path: C:\CHFI-Tools\Evidence Files
Created: Thursday, January 12, 2023
Accessed: Thursday, January 12, 2023
Modified: Wednesday, December 02, 2020
Read Only: False
Hidden: False
Size: 12145 bytes
CRC: 1584579263
Calculate MD5 Hash on Files


HELIX2009R1 (01/06/2009)
File Quick Launch Page Help
HELIX 3 INCIDENT RESPONSE • ELECTRONIC DISCOVERY • COMPUTER FORENSICS
Scan For Pictures
1(2).jpg
1200px-Olympic_r...
1200px-Peace_sig...
1200px-yin_yang-...
1f5dc196213fbcd8...
250px-Raelian_sy...
3-2-cartoon-free-...
31154266_400x40...
8fb162681710 47d...
awen.gif
cartoon-article.jpg
da2b622ecc9b843...
Fan-oven.png
Flowers_123.jpg
Friends2.jpg


HELIX2009R1 (01/06/2009)
le Quick Launch Page Help
HELIX 3 INCIDENT RESPONSE • ELECTRONIC DISCOVERY • COMPUTER FORENSICS
Browse Contents
C:\
$Recycle.Bin
$WINDOWS.~BT
CHFI-Tools
Evidence Files
Image Files
Documents and Settings
found.000
PerfLogs
preoscp
Program Files
Program Files (x86)
ProgramData
Recovery
System Volume Information
Users
Windows
D:\
Z:\
giphy_s.gif
Hashes.txt
images (1).jpg
images (1).png
images-of-cartoons-14.jpg
images.jpg
images.png
Kitty.jpg
maxresdefault.jpg
mip.jpg
Model.png
Pagan-Symbols-and-Their-Meanings-Pentagram
peacesign.jpg
resized_celtic-symbols-and-their-meanings-
Sunset-pexels-photo-132037_BLOG.bat
symbols-transparent-aboriginal.png
Tweety1.gif
u3Y71q8z_400x400.jpeg
Path: C:\CHFI-Tools\Evidence Files
Created: Thursday, January 12, 2023
Accessed: Thursday, January 12, 2023
Modified: Wednesday, December 02, 2020
Read Only: False
Hidden: False
Size: 12145 bytes
CRC: 1584579263



Lab 8: Collecting and Parsing Forensic Artifacts

Objective

> To gather forensic artifacts from a live Windows system using KAPE.

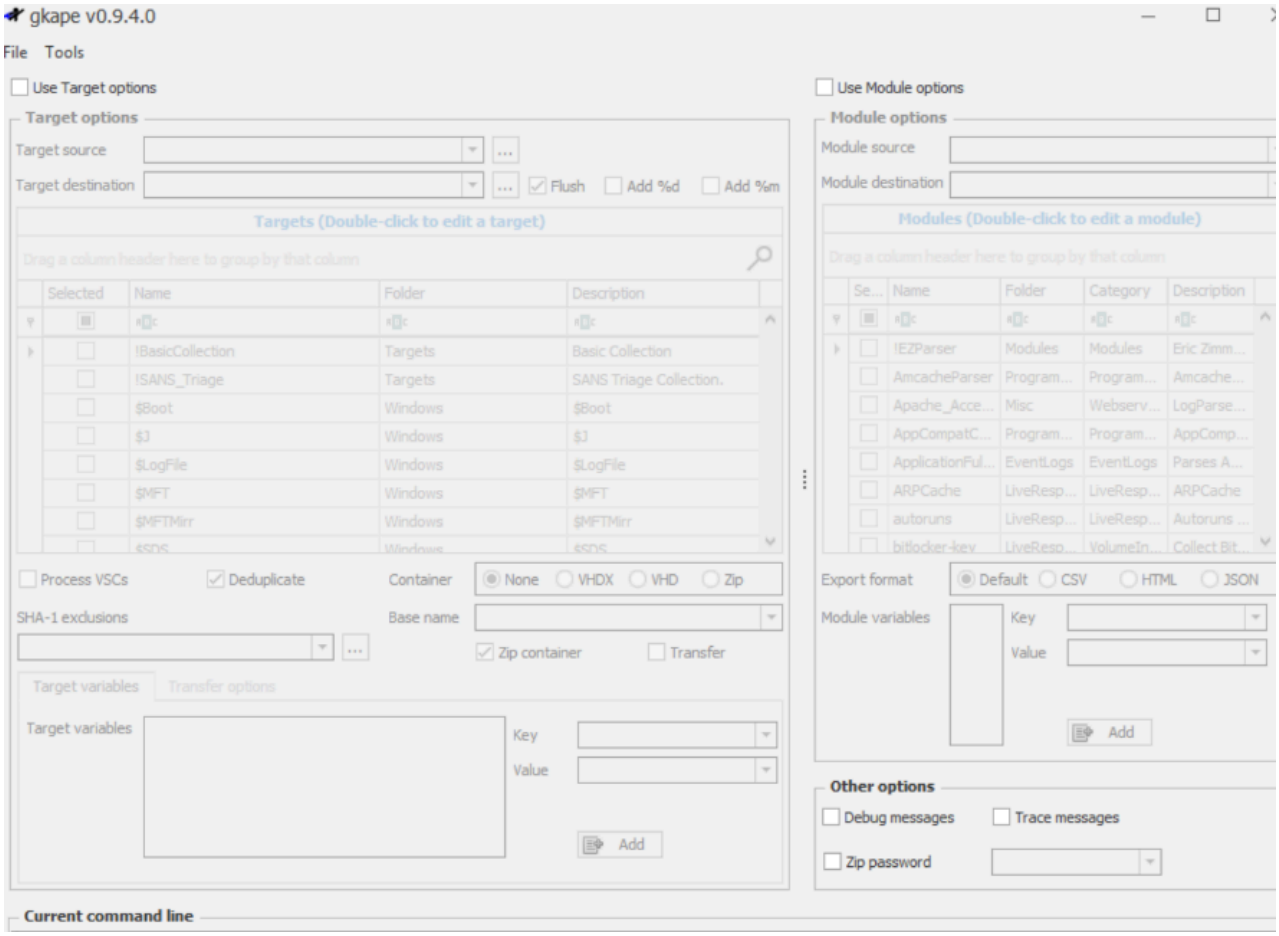
Tools Required

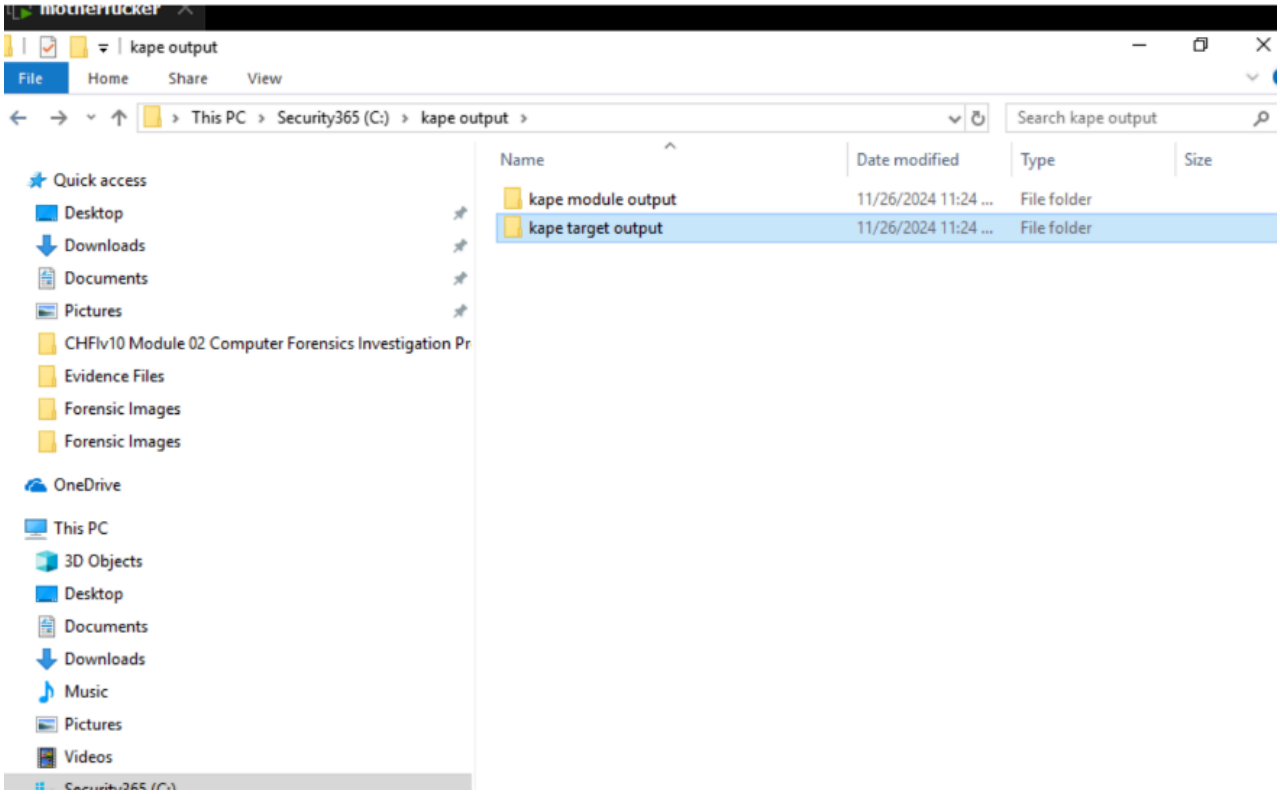
- KAPE

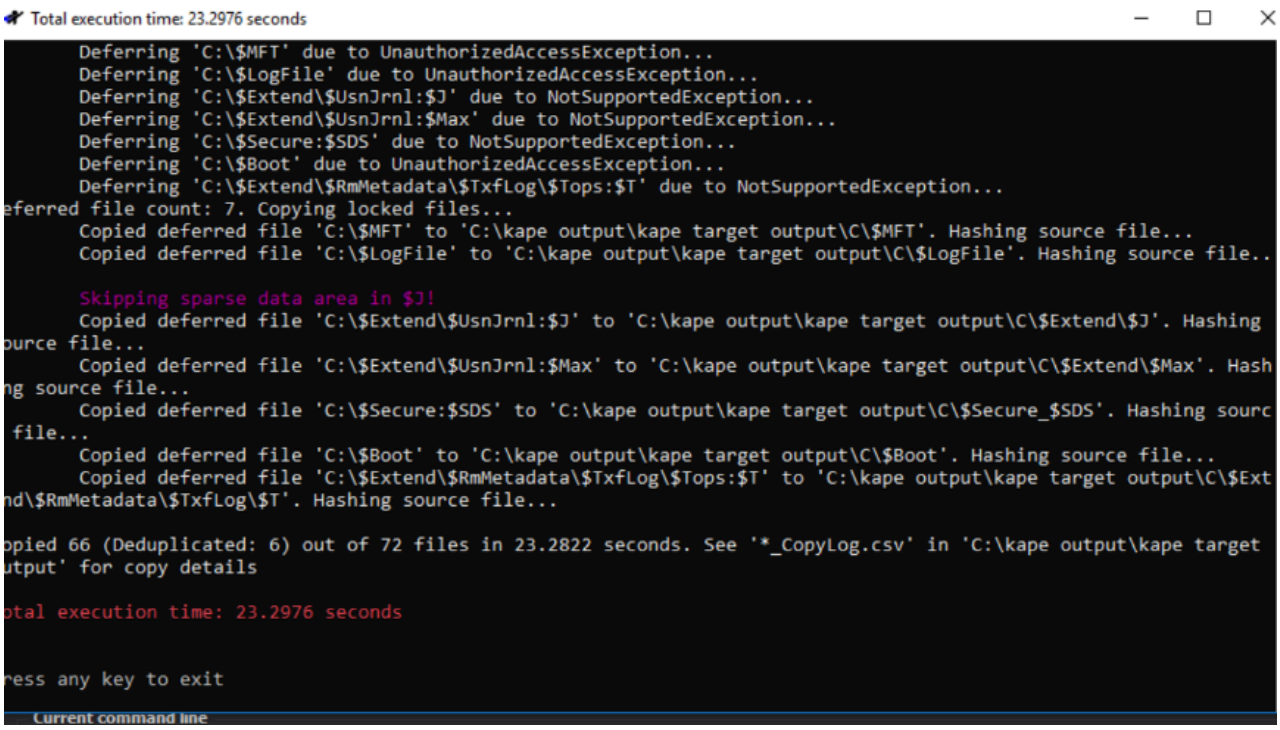
Steps

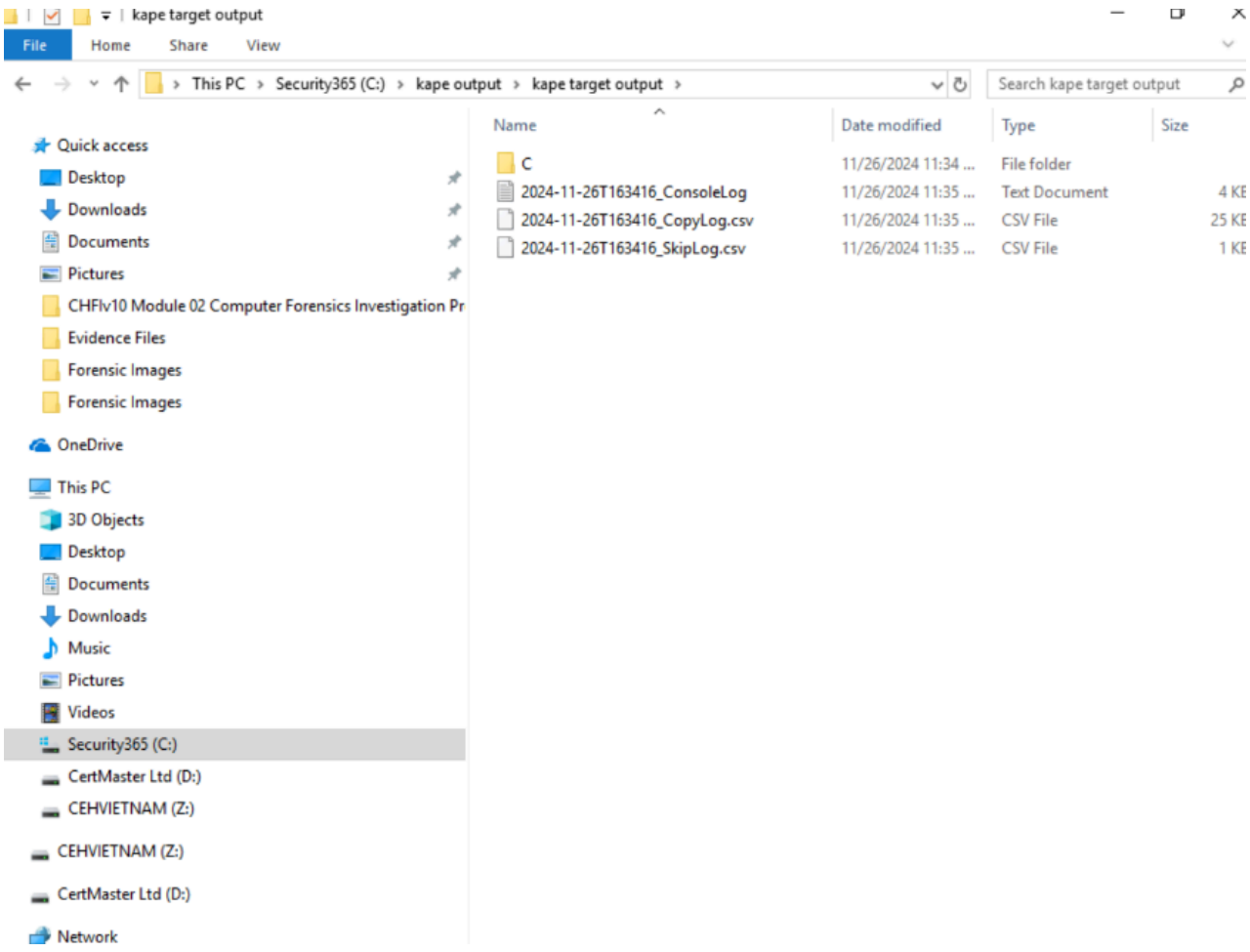
1. **Configure KAPE**
   - Set target and module directories.
   - Select relevant artifacts for acquisition.
2. **Collect and Parse Data**

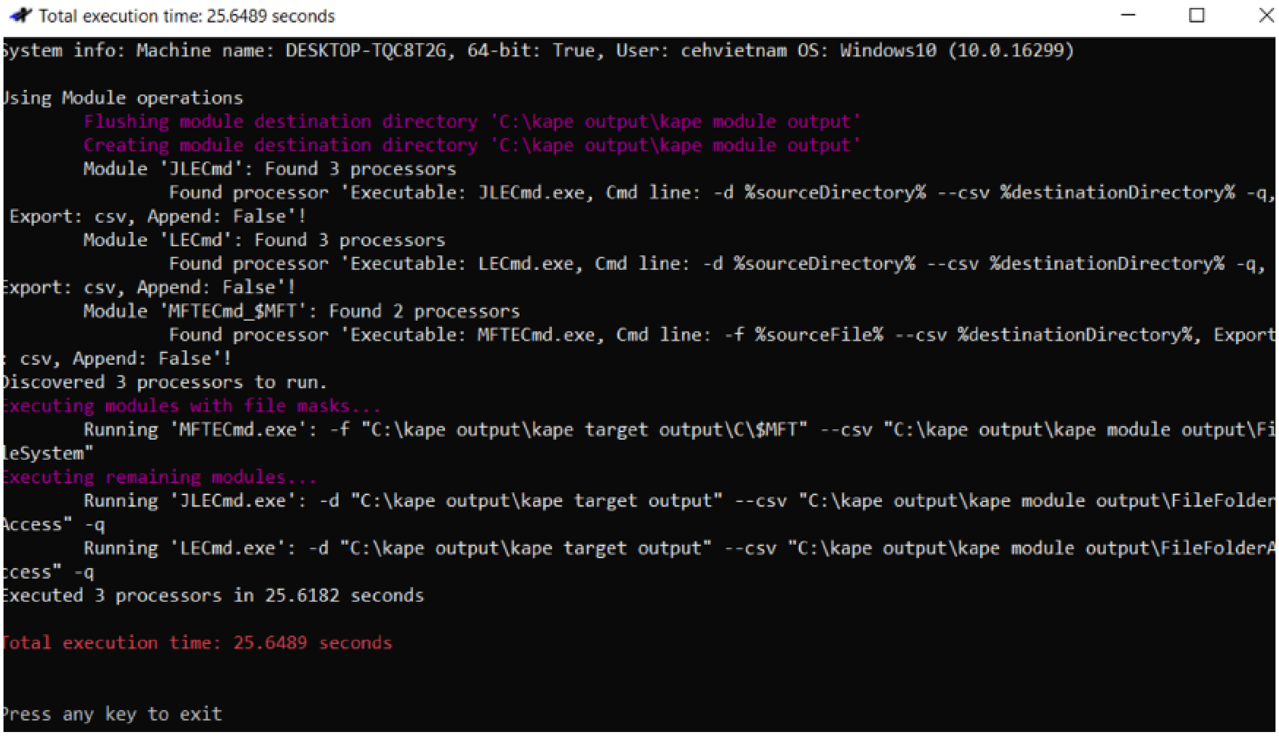
- Execute KAPE to acquire target files.
- Parse the collected files and review them in the module directory.

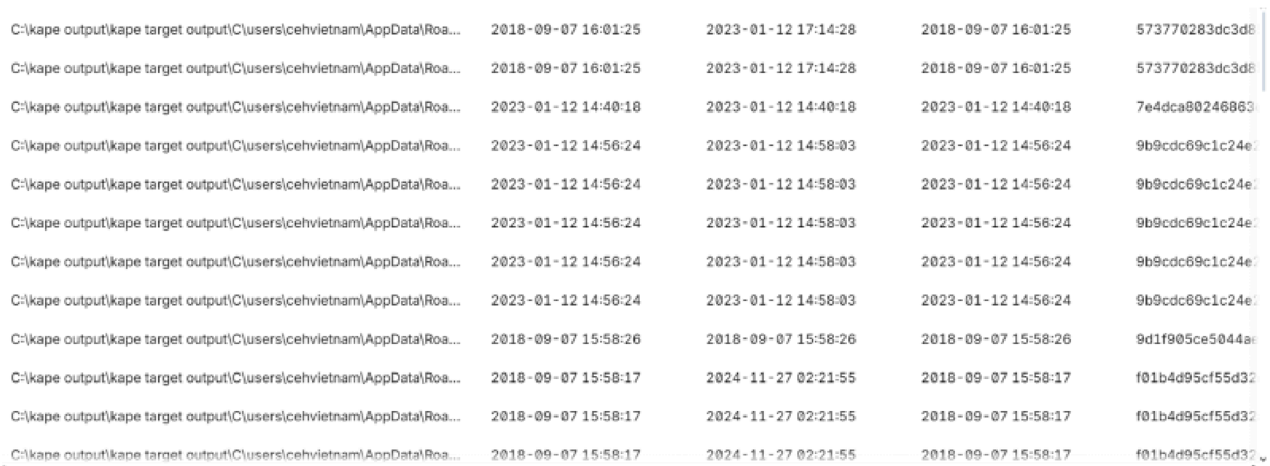

gkape v0.9.4.0
File
Tools
Use Target options
Target options
Target source
Target destination
Flush
Add %d
Add %m
Targets (Double-click to edit a target)
Drag a column header here to group by that column
Selected
Name
Folder
Description
!BasicCollection
Targets
Basic Collection
!SANS_Triage
Targets
SANS Triage Collection.
$Boot
Windows
$Boot
$J
Windows
$J
$LogFile
Windows
$LogFile
$MFT
Windows
$MFT
$MFTMirr
Windows
$MFTMirr
Process VSCs
Deduplicate
Container
None
VHDX
VHD
Zip
SHA-1 exclusions
Base name
Zip container
Transfer
Target variables
Transfer options
Target variables
Key
Value
Add
Use Module options
Module options
Module source
Module destination
Modules (Double-click to edit a module)
Drag a column header here to group by that column
Se...
Name
Folder
Category
Description
!EZParser
Modules
Modules
Eric Zimm...
AmcacheParser
Program...
Program...
Amcache...
Apache_Acce...
Misc
Webserv...
LogParse...
AppCompatC...
Program...
Program...
AppComp...
ApplicationFul...
EventLogs
EventLogs
Parses A...
ARPCache
LiveResp...
LiveResp...
ARPCache
autoruns
LiveResp...
LiveResp...
Autoruns ...
bitlocker-key
LiveReso...
VolumeIn...
Collect Bit...
Export format
Default
CSV
HTML
JSON
Module variables
Key
Value
Add
Other options
Debug messages
Trace messages
Zip password
Current command line


motherfucker
kape output
File
Home
Share
View
This PC › Security365 (C:) › kape output ›
Search kape output
Quick access
Desktop
Downloads
Documents
Pictures
CHFIv10 Module 02 Computer Forensics Investigation Pr
Evidence Files
Forensic Images
Forensic Images
OneDrive
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Name
Date modified
Type
Size
kape module output
11/26/2024 11:24 ...
File folder
kape target output
11/26/2024 11:24 ...
File folder


Total execution time: 23.2976 seconds
Deferring 'C:\$MFT' due to UnauthorizedAccessException...
Deferring 'C:\$LogFile' due to UnauthorizedAccessException...
Deferring 'C:\$Extend\$UsnJrnl:$J' due to NotSupportedException...
Deferring 'C:\$Extend\$UsnJrnl:$Max' due to NotSupportedException...
Deferring 'C:\$Secure:$SDS' due to NotSupportedException...
Deferring 'C:\$Boot' due to UnauthorizedAccessException...
Deferring 'C:\$Extend\$RmMetadata\$TxfLog\$Tops:$T' due to NotSupportedException...
eferred file count: 7. Copying locked files...
Copied deferred file 'C:\$MFT' to 'C:\kape output\kape target output\C\$MFT'. Hashing source file...
Copied deferred file 'C:\$LogFile' to 'C:\kape output\kape target output\C\$LogFile'. Hashing source file..
Skipping sparse data area in $J!
Copied deferred file 'C:\$Extend\$UsnJrnl:$J' to 'C:\kape output\kape target output\C\$Extend\$J'. Hashing
ource file...
Copied deferred file 'C:\$Extend\$UsnJrnl:$Max' to 'C:\kape output\kape target output\C\$Extend\$Max'. Hash
g source file...
Copied deferred file 'C:\$Secure:$SDS' to 'C:\kape output\kape target output\C\$Secure_$SDS'. Hashing sourc
file...
Copied deferred file 'C:\$Boot' to 'C:\kape output\kape target output\C\$Boot'. Hashing source file...
Copied deferred file 'C:\$Extend\$RmMetadata\$TxfLog\$Tops:$T' to 'C:\kape output\kape target output\C\$Ext
d\$RmMetadata\$TxfLog\$T'. Hashing source file...
pied 66 (Deduplicated: 6) out of 72 files in 23.2822 seconds. See '*_CopyLog.csv' in 'C:\kape output\kape target
tput' for copy details
tal execution time: 23.2976 seconds
ess any key to exit
Current command line


kape target output
File
Home
Share
View
This PC
Security365 (C:)
kape output
kape target output
Search kape target output
Quick access
Desktop
Downloads
Documents
Pictures
CHFIv10 Module 02 Computer Forensics Investigation Pr
Evidence Files
Forensic Images
Forensic Images
OneDrive
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Security365 (C:)
CertMaster Ltd (D:)
CEHVIETNAM (Z:)
CEHVIETNAM (Z:)
CertMaster Ltd (D:)
Network
Name
Date modified
Type
Size
C
11/26/2024 11:34 ...
File folder
2024-11-26T163416_ConsoleLog
11/26/2024 11:35 ...
Text Document
4 KB
2024-11-26T163416_CopyLog.csv
11/26/2024 11:35 ...
CSV File
25 KB
2024-11-26T163416_SkipLog.csv
11/26/2024 11:35 ...
CSV File
1 KB





C:\kape output\kape target output\C\users\cehvietnam\AppData\Roa...	2018-09-07 16:01:25	2023-01-12 17:14:28	2018-09-07 16:01:25	573770283dc3d8
C:\kape output\kape target output\C\users\cehvietnam\AppData\Roa...	2018-09-07 16:01:25	2023-01-12 17:14:28	2018-09-07 16:01:25	573770283dc3d8
C:\kape output\kape target output\C\users\cehvietnam\AppData\Roa...	2023-01-12 14:40:18	2023-01-12 14:40:18	2023-01-12 14:40:18	7e4dca80246863
C:\kape output\kape target output\C\users\cehvietnam\AppData\Roa...	2023-01-12 14:56:24	2023-01-12 14:58:03	2023-01-12 14:56:24	9b9cdc69c1c24e
C:\kape output\kape target output\C\users\cehvietnam\AppData\Roa...	2023-01-12 14:56:24	2023-01-12 14:58:03	2023-01-12 14:56:24	9b9cdc69c1c24e
C:\kape output\kape target output\C\users\cehvietnam\AppData\Roa...	2023-01-12 14:56:24	2023-01-12 14:58:03	2023-01-12 14:56:24	9b9cdc69c1c24e
C:\kape output\kape target output\C\users\cehvietnam\AppData\Roa...	2023-01-12 14:56:24	2023-01-12 14:58:03	2023-01-12 14:56:24	9b9cdc69c1c24e
C:\kape output\kape target output\C\users\cehvietnam\AppData\Roa...	2023-01-12 14:56:24	2023-01-12 14:58:03	2023-01-12 14:56:24	9b9cdc69c1c24e
C:\kape output\kape target output\C\users\cehvietnam\AppData\Roa...	2018-09-07 15:58:26	2018-09-07 15:58:26	2018-09-07 15:58:26	9d1f905ce5044a
C:\kape output\kape target output\C\users\cehvietnam\AppData\Roa...	2018-09-07 15:58:17	2024-11-27 02:21:55	2018-09-07 15:58:17	f01b4d95cf55d3
C:\kape output\kape target output\C\users\cehvietnam\AppData\Roa...	2018-09-07 15:58:17	2024-11-27 02:21:55	2018-09-07 15:58:17	f01b4d95cf55d3
C:\kape output\kape target output\C\users\cehvietnam\AppData\Roa...	2018-09-07 15:58:17	2024-11-27 02:21:55	2018-09-07 15:58:17	f01b4d95cf55d3

THANK!