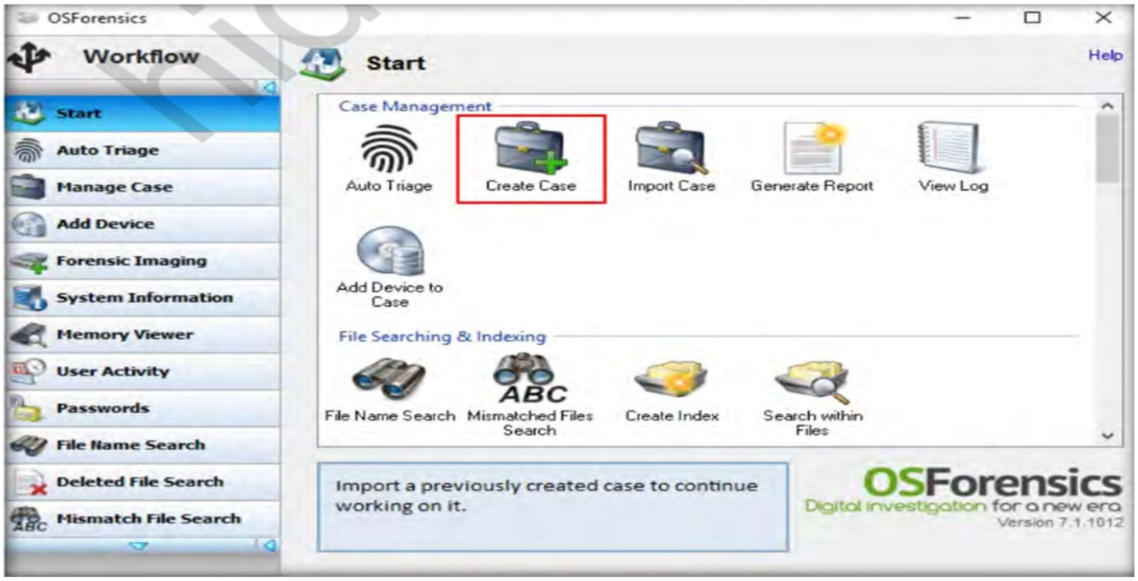
PRACTICAL NO. 02

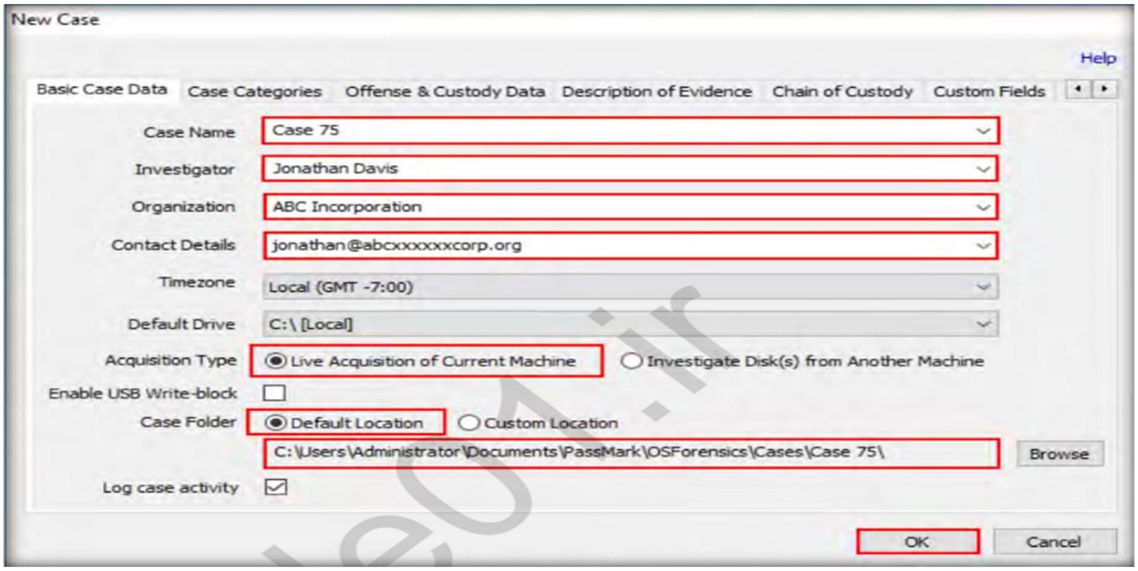
a. Explore Windows forensic tools (OSForensics)

Navigate to C:\CHFI-Tools\CHFIv10Module 06 Windows Forensics\Windows Forensics Tools\OS Forensics, double-clickosf.exe to launch the steup. In the final step of installation, check the Launch OSForensics option and click Finish. OSForensics GUI appears, along with PassMark OSForensics pop-up. In the pop-up, click Continue Using Trial Version. Our first task is to create a case using this tool. Click the Create Case icon in the tool's main window to create a new case.

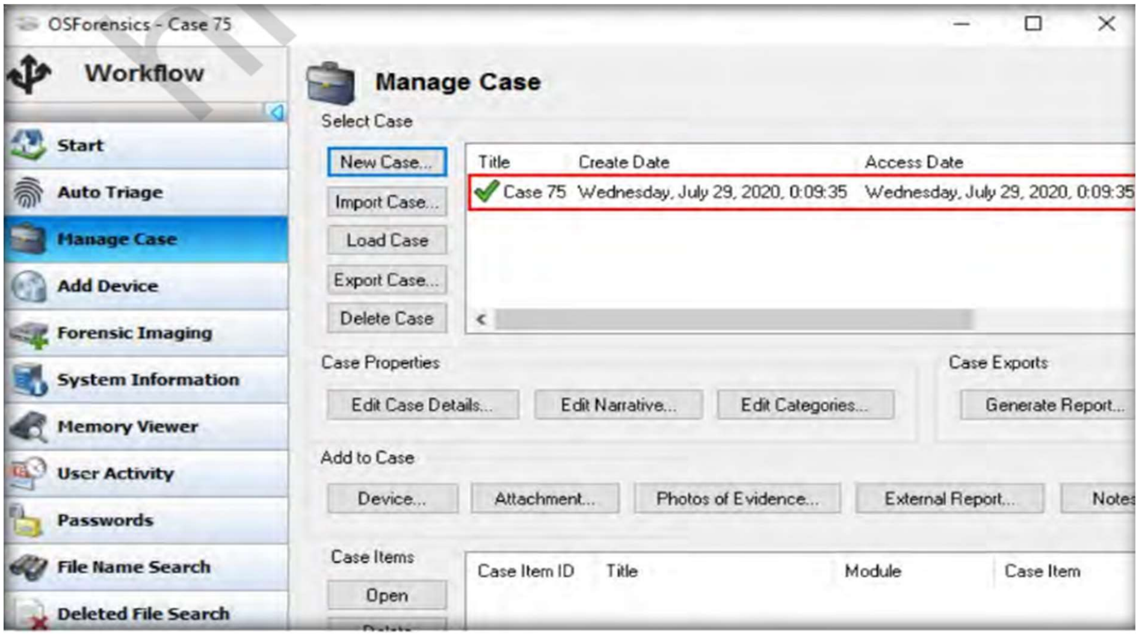


Import a previously created case to continue working on it.

A New Case window appears; fill out the required fields in the window. Ensure that you select the radio button for the Live Acquisition of Current Machine option in the Acquisition Type category. You may choose to save the new case folder either in Default or Custom locations. Click OK

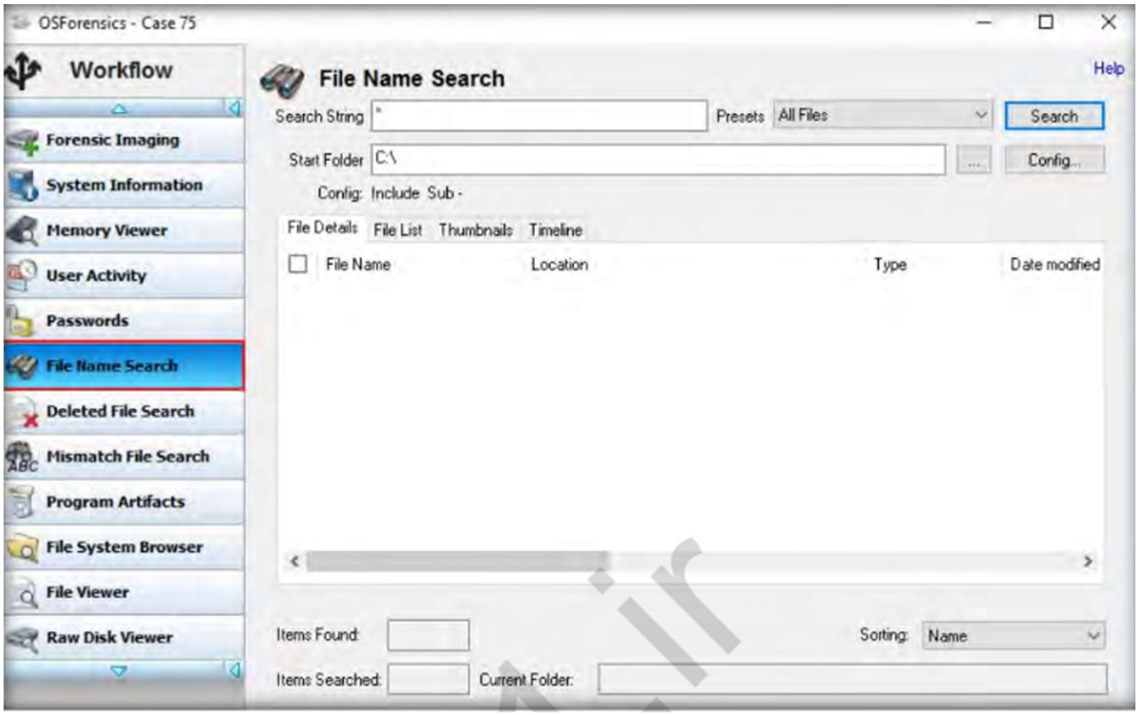


Case Name	Case 75
Investigator	Jonathan Davis
Organization	ABC Incorporation
Contact Details	jonathan@abcxxxxxxcorp.org
Timezone	Local (GMT -7:00)
Default Drive	C:\ [Local]
Acquisition Type	● Live Acquisition of Current Machine ○ Investigate Disk(s) from Another Machine
Enable USB Write-block	□
Case Folder	● Default Location ○ Custom Location
	C:\Users\Administrator\Documents\PassMark\OSForensics\Cases\Case 75\
Log case activity	☑



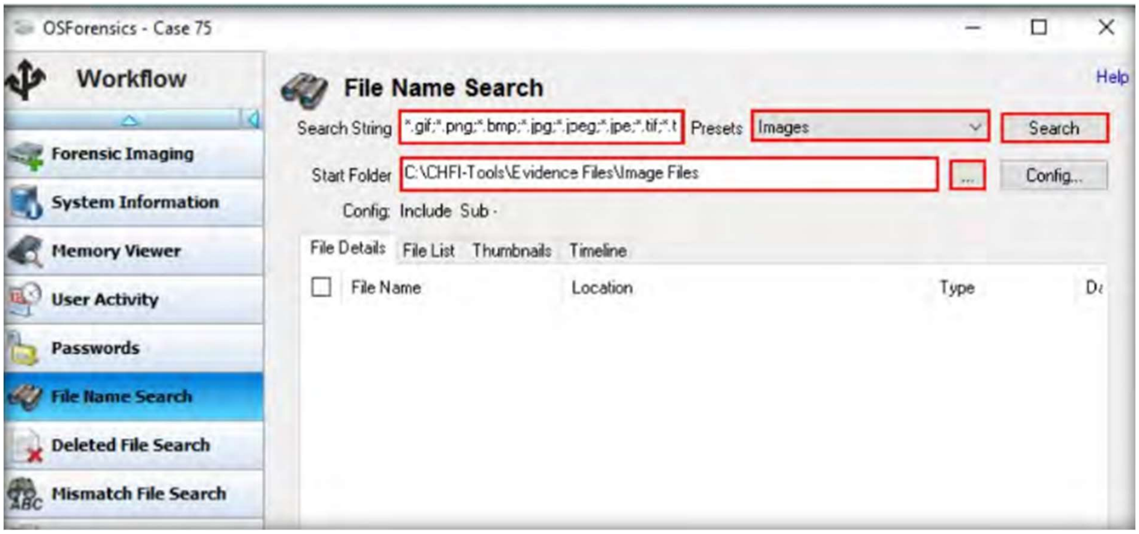
Title	Create Date	Access Date
✓ Case 75	Wednesday, July 29, 2020, 0:09:35	Wednesday, July 29, 2020, 0:09:35

The OSForensics tool can help investigators in searching and locating files on a system. To start searching for files, click File Name Search in the left pane of the window.



Search String: *
Presets: All Files
Start Folder: C:\
Config: Include Sub -
Sorting: Name

In the Start Folder field, specify the path to search for image files by clicking the ellipsis button and choosing the location (here, we are specifying the location C:\CHFI-Tools\EvidenceFiles\Image Files to search for images in it). Then, click the Search button.



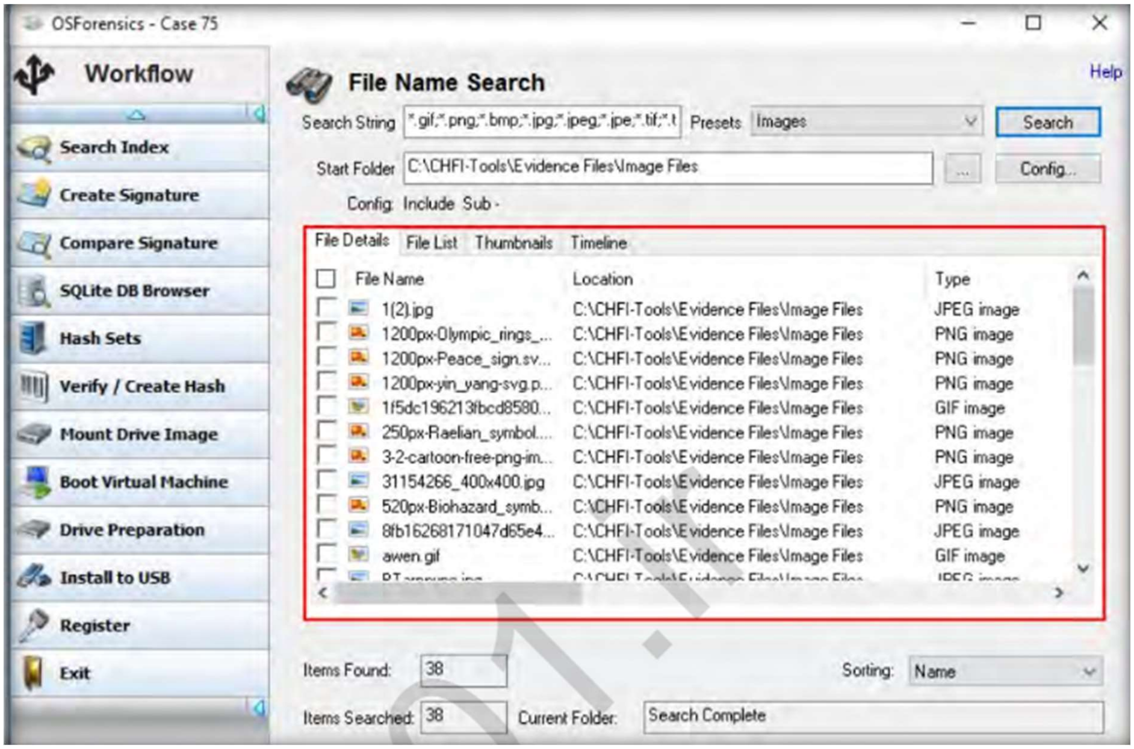
Search String: *.gif;*.png;*.bmp;*.jpg;*.jpeg;*.jpe;*.tif;*.t

Presets: Images

Start Folder: C:\CHFI-Tools\Evidence Files\Image Files

Config: Include Sub -

File Name	Location	Type	Da



Search String: *.gif;*.png;*.bmp;*.jpg;*.jpeg;*.jpe;*.tif;*.t

Presets: Images

Start Folder: C:\CHFI-Tools\Evidence Files\Image Files

Config: Include Sub -

File Name	Location	Type
1(2).jpg	C:\CHFI-Tools\Evidence Files\Image Files	JPEG image
1200px-Olympic_rings_...	C:\CHFI-Tools\Evidence Files\Image Files	PNG image
1200px-Peace_sign.sv...	C:\CHFI-Tools\Evidence Files\Image Files	PNG image
1200px-yin_yang-svg.p...	C:\CHFI-Tools\Evidence Files\Image Files	PNG image
1f5dc196213fbcd8580...	C:\CHFI-Tools\Evidence Files\Image Files	GIF image
250px-Raelian_symbol....	C:\CHFI-Tools\Evidence Files\Image Files	PNG image
3-2-cartoon-free-png-im...	C:\CHFI-Tools\Evidence Files\Image Files	PNG image
31154266_400x400.jpg	C:\CHFI-Tools\Evidence Files\Image Files	JPEG image
520px-Biohazard_symb...	C:\CHFI-Tools\Evidence Files\Image Files	PNG image
8fb16268171047d65e4...	C:\CHFI-Tools\Evidence Files\Image Files	JPEG image
awen.gif	C:\CHFI-Tools\Evidence Files\Image Files	GIF image

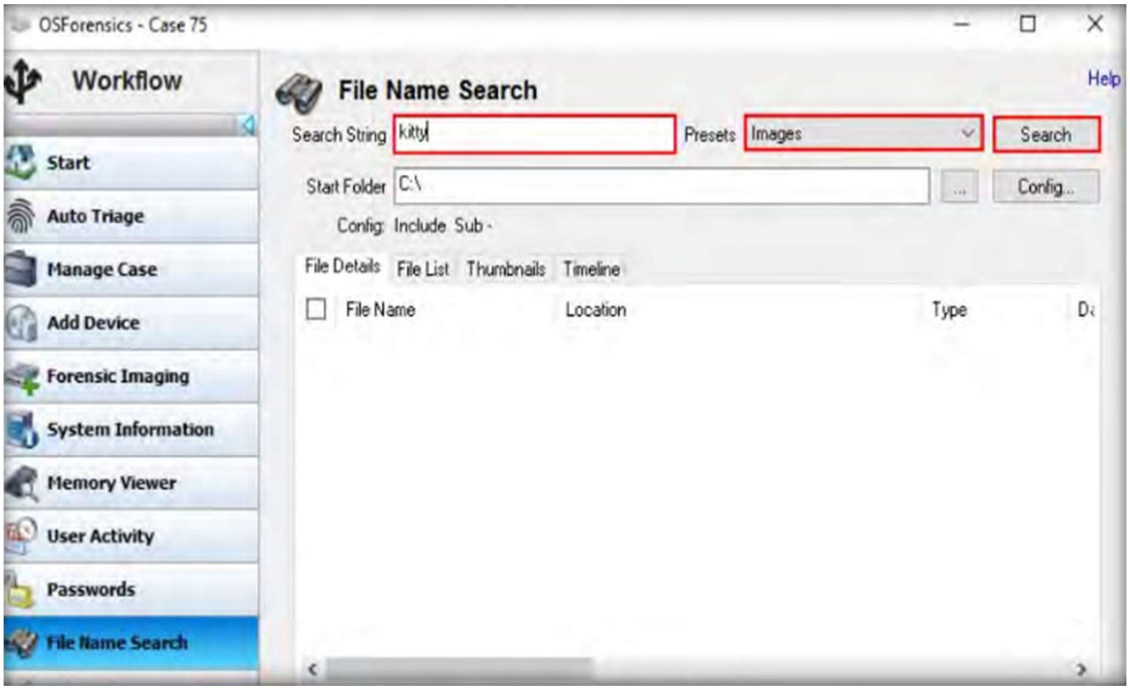
Items Found: 38

Sorting: Name

Items Searched: 38

Current Folder: Search Complete

Alternatively, if you wish to search only for a single image on the entire system, select Images from the Pre-sets drop-down menu, enter the name of the desired image file in the Search String field, and then click Search, as shown in the screenshot below. Here, we are searching for the JPEG image file named Kitty.



File Name Search

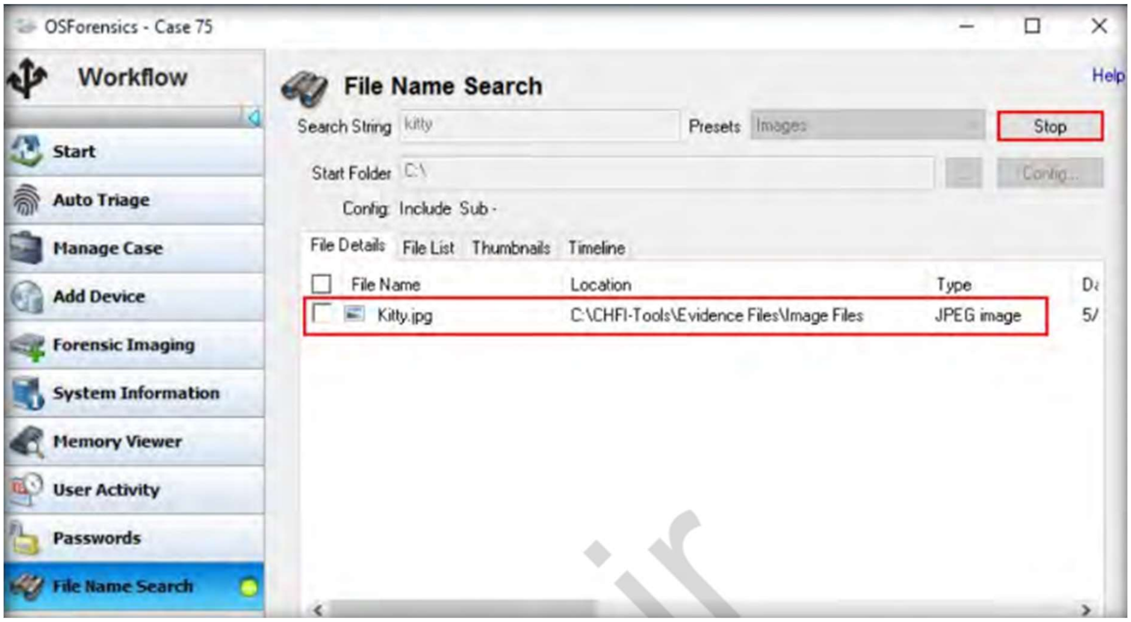
Search String: kitty

Presets: Images

Start Folder: C:\

Config: Include Sub -

□ File Name	Location	Type	Da



File Name Search

Search String: kitty

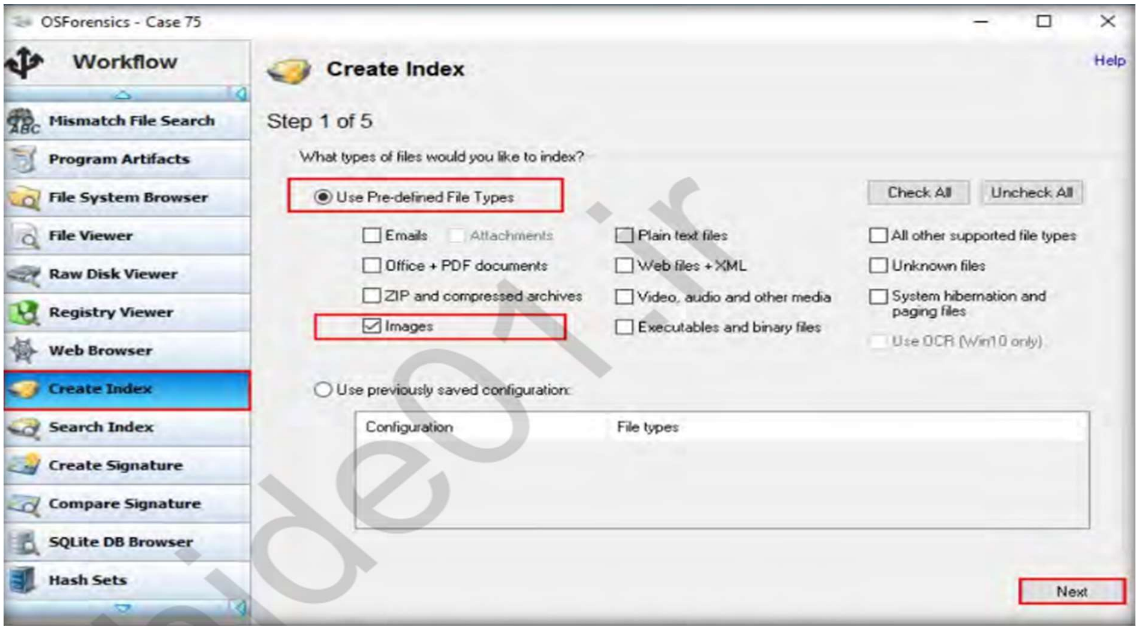
Presets: Images

Start Folder: C:\

Config: Include Sub -

□ File Name	Location	Type	Da
□ Kitty.jpg	C:\CHFI-Tools\Evidence Files\Image Files	JPEG image	5/

The Create Index section appears in the right pane. In this section, select the Use Pre-defined File Types option for creating the index and check the required options listed under it for selecting the file types that you wish to index (here, we have selected the Images option). Then, click Next.



Create Index

Step 1 of 5

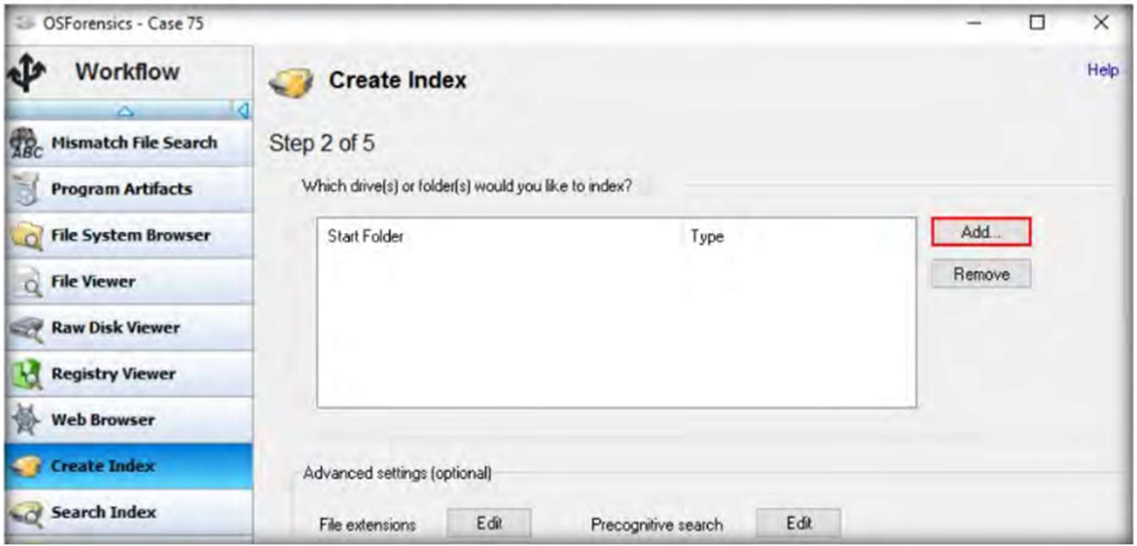
What types of files would you like to index?

● Use Pre-defined File Types

□ 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 (Win10 only)

○ Use previously saved configuration:

Configuration	File types



Create Index

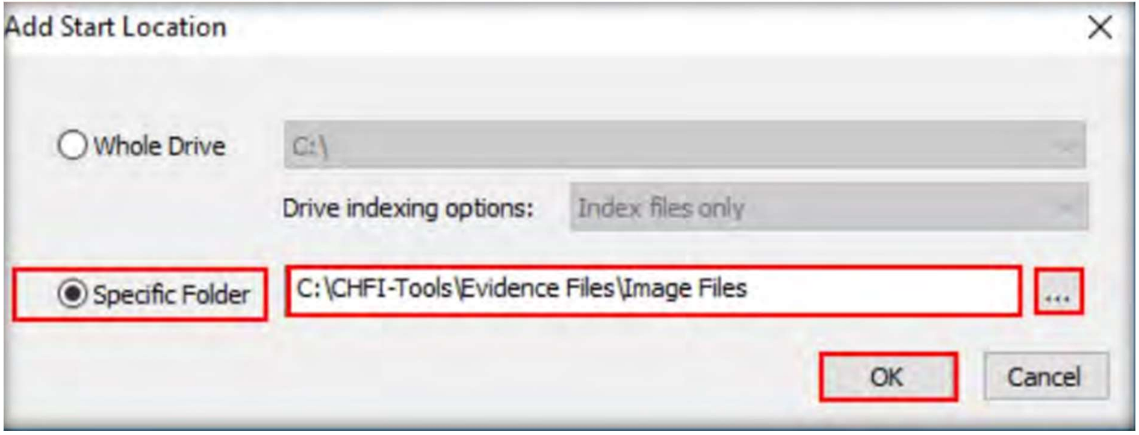
Step 2 of 5

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

Start Folder	Type

Advanced settings (optional)

File extensions   Precognitive search

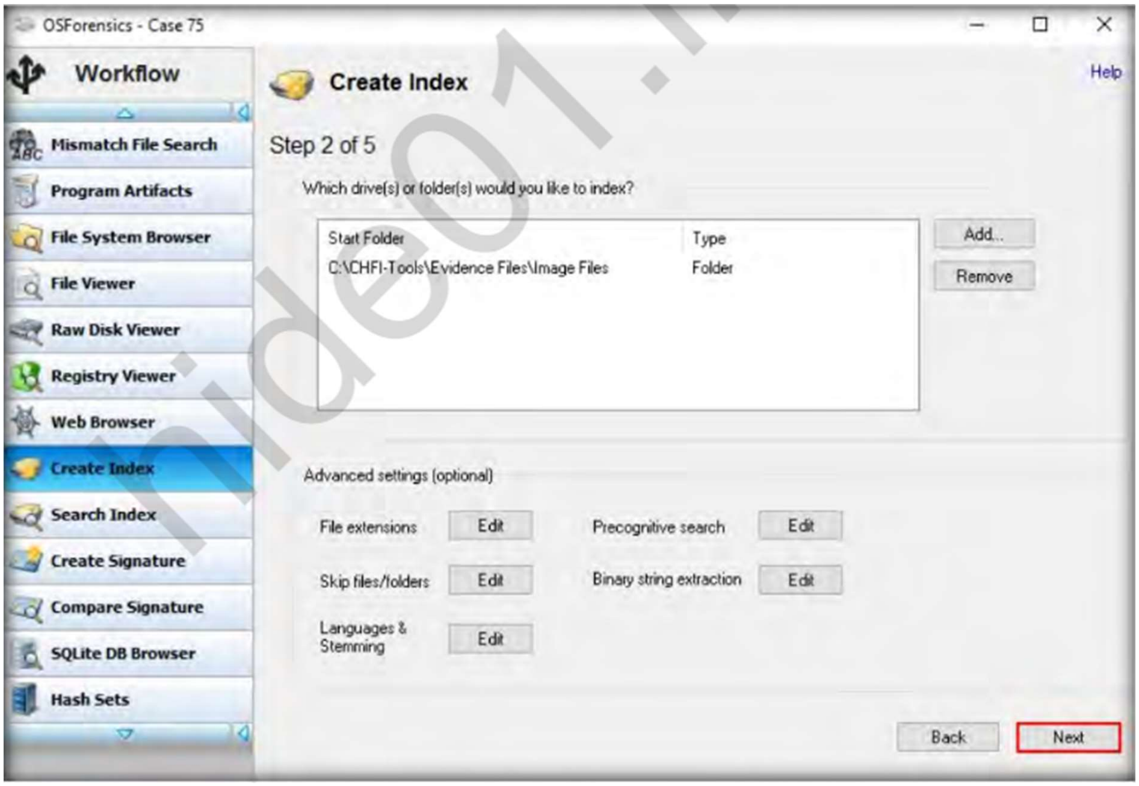


Add Start Location

○ Whole Drive   C:\

Drive indexing options: Index files only

● Specific Folder   C:\CHFI-Tools\Evidence Files\Image Files



Create Index

Step 2 of 5

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

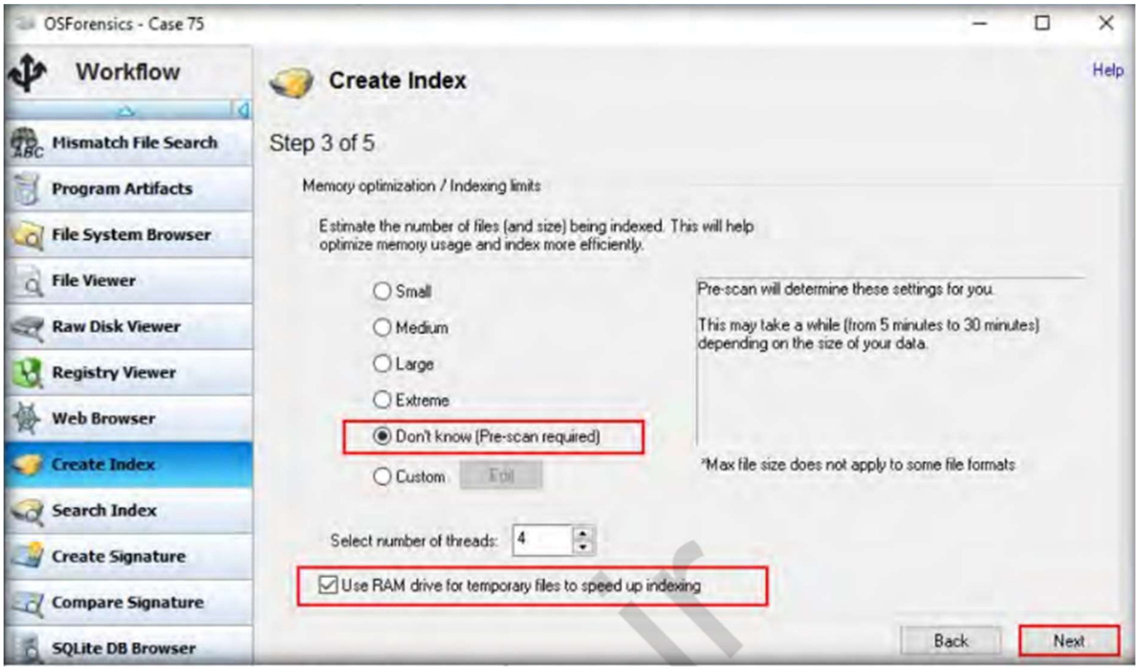
Start Folder	Type
C:\CHFI-Tools\Evidence Files\Image Files	Folder

Advanced settings (optional)

File extensions [Edit] Precognitive search [Edit]

Skip files/folders [Edit] Binary string extraction [Edit]

Languages & Stemming [Edit]



Create Index

Step 3 of 5

Memory optimization / Indexing limits

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

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

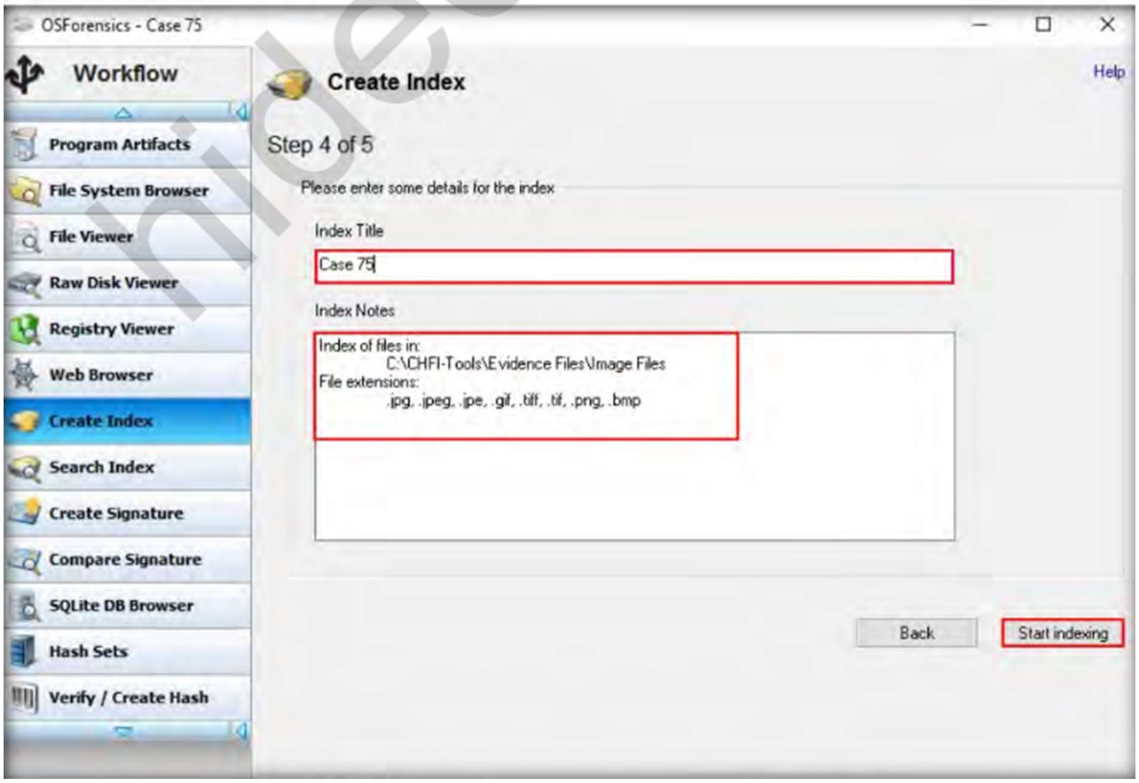
Pre-scan will determine these settings for you.

This may take a while (from 5 minutes to 30 minutes) depending on the size of your data.

*Max file size does not apply to some file formats

Select number of threads: 4

☑ Use RAM drive for temporary files to speed up indexing



Create Index

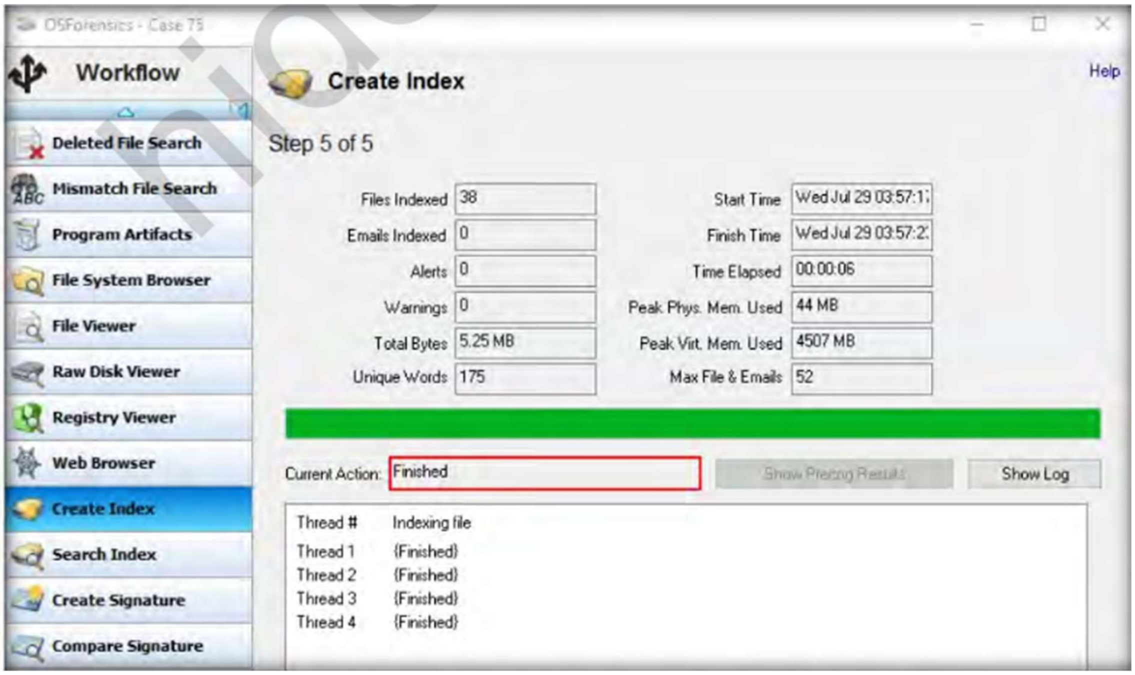
Step 4 of 5

Please enter some details for the index

Index Title: Case 75

Index Notes:

```
Index of files in:
          C:\CHFI-Tools\Evidence Files\Image Files
File extensions:
          .jpg, .jpeg, .jpe, .gif, .tiff, .tif, .png, .bmp
```



Create Index

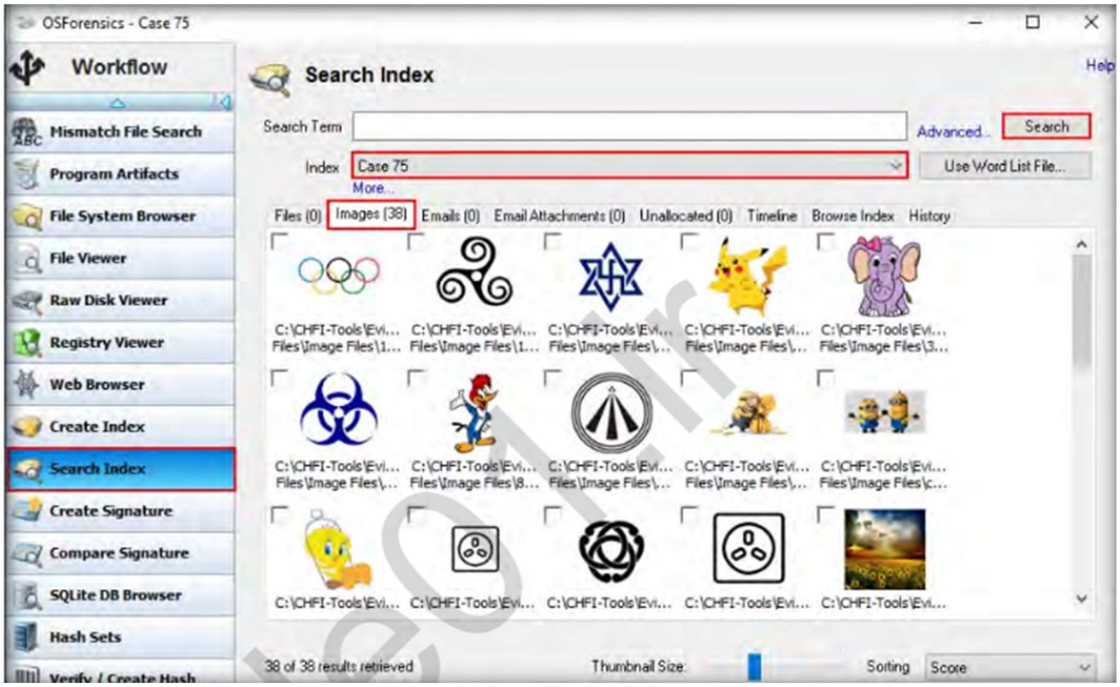
Step 5 of 5

Files Indexed	38	Start Time	Wed Jul 29 03:57:1
Emails Indexed	0	Finish Time	Wed Jul 29 03:57:2
Alerts	0	Time Elapsed	00:00:06
Warnings	0	Peak Phys. Mem. Used	44 MB
Total Bytes	5.25 MB	Peak Virt. Mem. Used	4507 MB
Unique Words	175	Max File & Emails	52

Current Action: Finished

```
Thread #     Indexing file
Thread 1     (Finished)
Thread 2     (Finished)
Thread 3     (Finished)
Thread 4     (Finished)
```

We will now search the indexed files. To search for the indexed files, select Search Index from the left pane of the tool window. The Search Index section now appears in the tool window. The index field at the top displays the name of the case we created (i.e., Case 75). Click Search. The tool will load the image files that you have indexed under the Images tab.



Search Term:

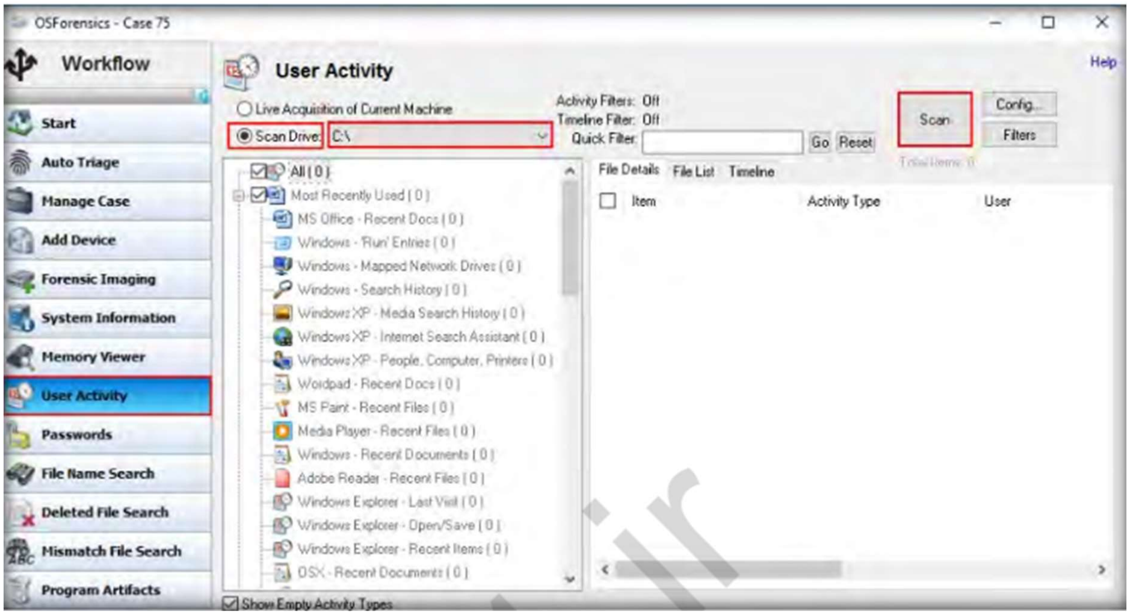
Index: Case 75

C:\CHFI-Tools\Evi... Files\Image Files\1...

38 of 38 results retrieved

Sorting: Score

Click User Activity in the left pane to scan for evidence such as browsed websites, USB drives, recent downloads and wireless networks.

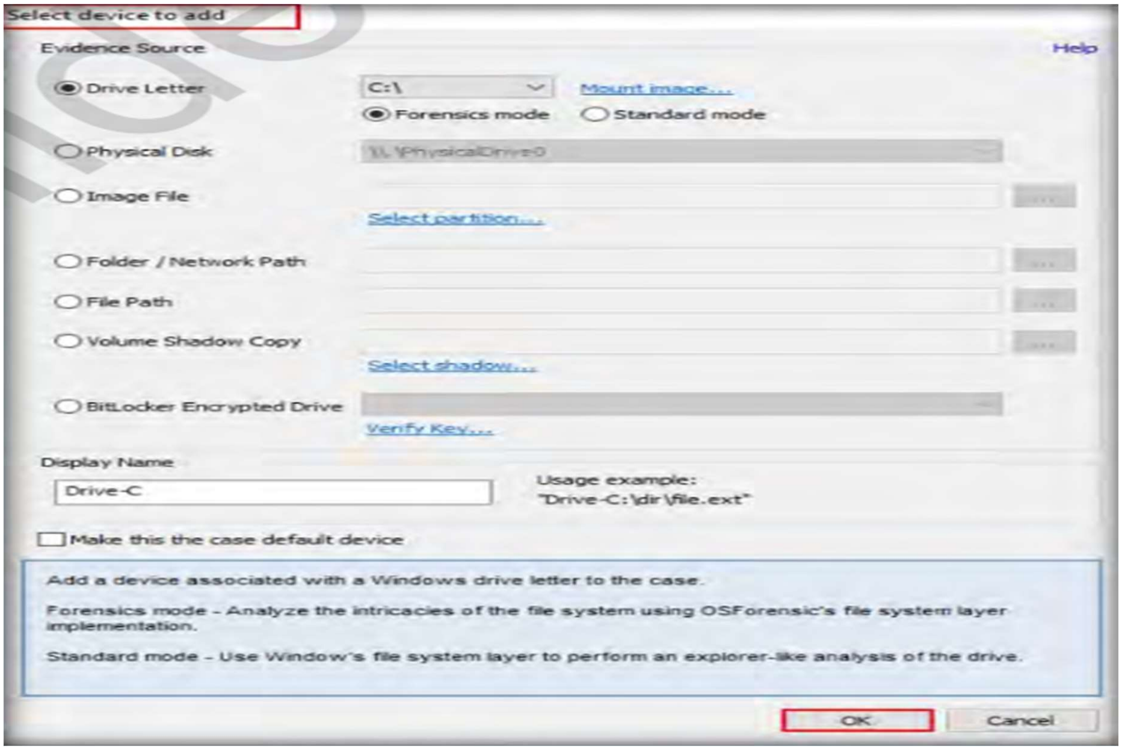


○ Live Acquisition of Current Machine
● Scan Drive: C:\

Activity Filters: Off
Timeline Filter: Off
Quick Filter:

All (0)
Most Recently Used (0)
MS Office - Recent Docs (0)
Windows - 'Run' Entries (0)
Windows - Mapped Network Drives (0)
Windows - Search History (0)
Windows XP - Media Search History (0)
Windows XP - Internet Search Assistant (0)
Windows XP - People, Computer, Printers (0)
Wordpad - Recent Docs (0)
MS Paint - Recent Files (0)
Media Player - Recent Files (0)
Windows - Recent Documents (0)
Adobe Reader - Recent Files (0)
Windows Explorer - Last Visit (0)
Windows Explorer - Open/Save (0)
Windows Explorer - Recent Items (0)
OSX - Recent Documents (0)

☑ Show Empty Activity Types



Select device to add

Evidence Source

● Drive Letter C:\ Mount image...

● Forensics mode ○ Standard mode

○ Physical Disk \\.\PhysicalDrive0

○ Image File

Select partition...

○ Folder / Network Path

○ File Path

○ Volume Shadow Copy

Select shadow...

○ BitLocker Encrypted Drive

Verify Key...

Display Name: Drive-C

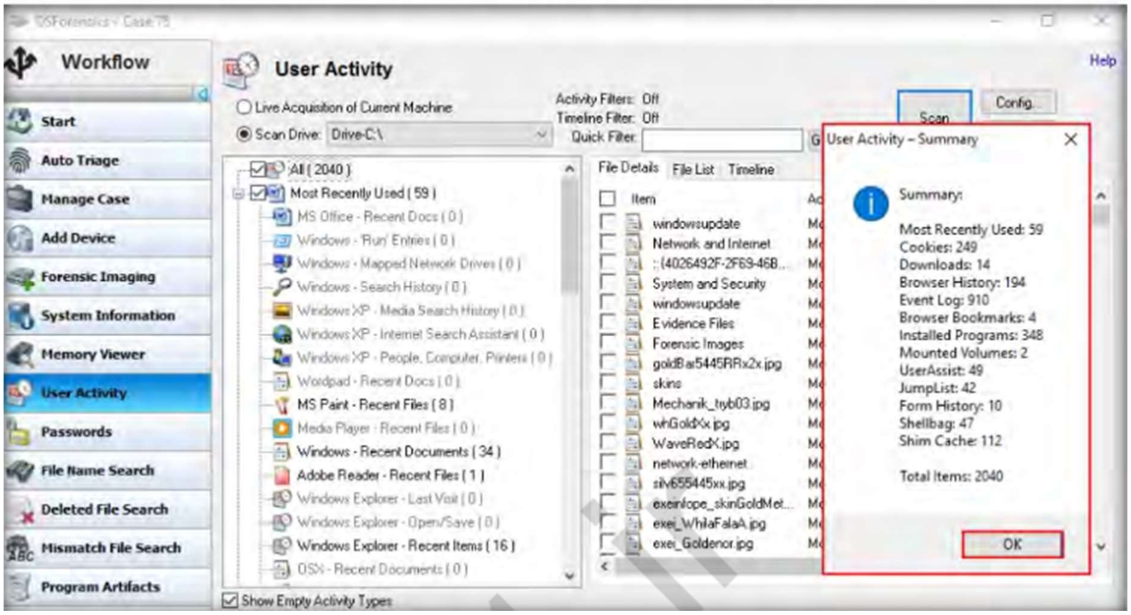
Usage example: "Drive-C:\dir\file.ext"

□ Make this the case default device

Add a device associated with a Windows drive letter to the case.

Forensics mode - Analyze the intricacies of the file system using OSForensic's file system layer implementation.

Standard mode - Use Window's file system layer to perform an explorer-like analysis of the drive.



○ Live Acquisition of Current Machine

● Scan Drive: Drive-C:\

Activity Filters: Off

Timeline Filter: Off

Quick Filter:

☑ All (2040)

☑ Most Recently Used (59)

- MS Office - Recent Docs (0)
- Windows - 'Run' Entries (0)
- Windows - Mapped Network Drives (0)
- Windows - Search History (0)
- Windows XP - Media Search History (0)
- Windows XP - Internet Search Assistant (0)
- Windows XP - People, Computer, Printers (0)
- Wordpad - Recent Docs (0)
- MS Paint - Recent Files (8)
- Media Player - Recent Files (0)
- Windows - Recent Documents (34)
- Adobe Reader - Recent Files (1)
- Windows Explorer - Last Visit (0)
- Windows Explorer - Open/Save (0)
- Windows Explorer - Recent Items (16)
- OSX - Recent Documents (0)

☑ Show Empty Activity Types

windowsupdate
Network and Internet
::{4026492F-2F69-46B...
System and Security
windowsupdate
Evidence Files
Forensic Images
goldBar5445RRx2x.jpg
skins
Mechanik_tryb03.jpg
whGoldXx.jpg
WaveRedX.jpg
network-ethernet
silv655445xx.jpg
exeinfope_skinGoldMet...
exe_WhilaFalaA.jpg
exe_Goldenor.jpg

User Activity – Summary

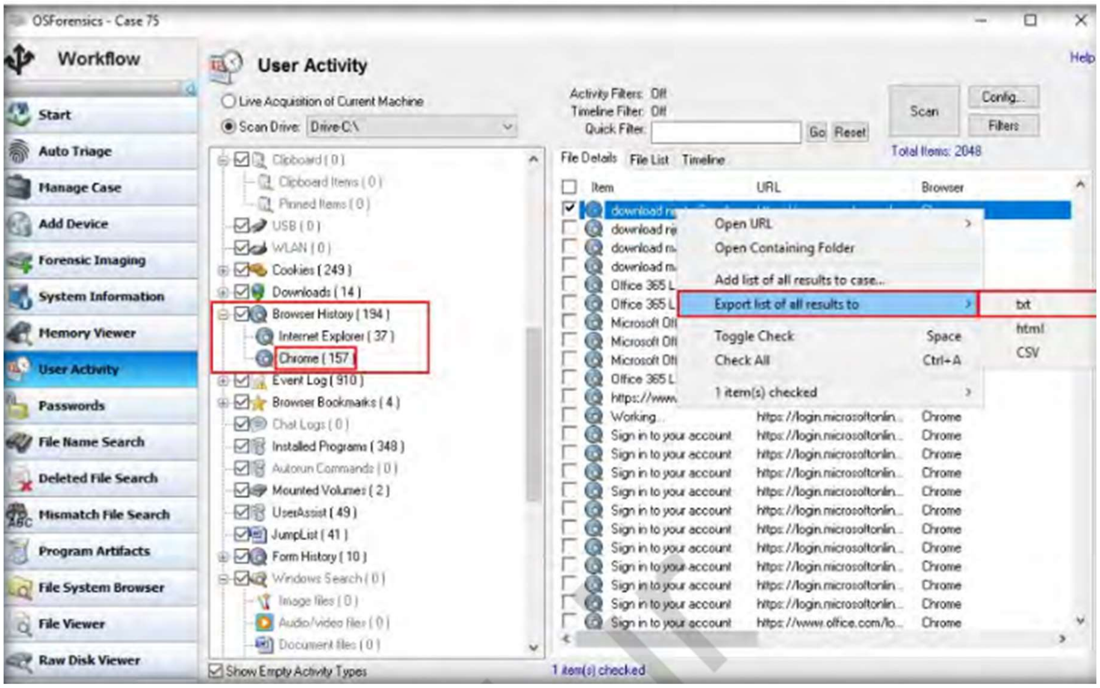
Summary:

Most Recently Used: 59
Cookies: 249
Downloads: 14
Browser History: 194
Event Log: 910
Browser Bookmarks: 4
Installed Programs: 348
Mounted Volumes: 2
UserAssist: 49
JumpList: 42
Form History: 10
Shellbag: 47
Shim Cache: 112

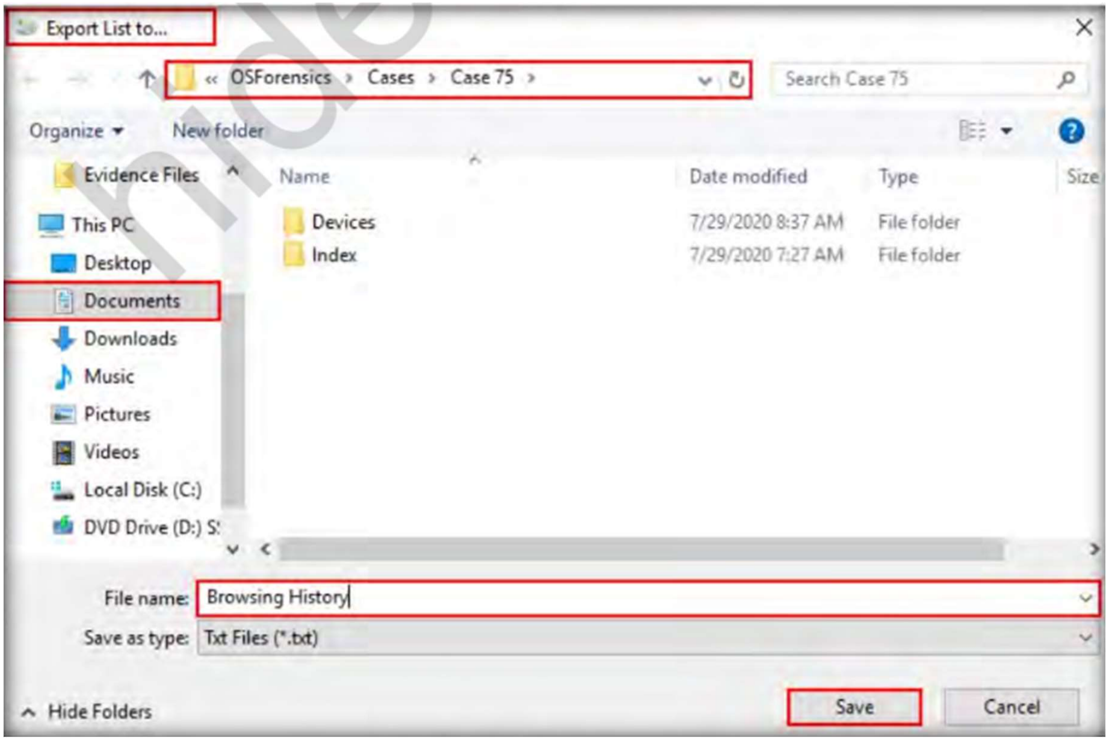
Total Items: 2040

OK

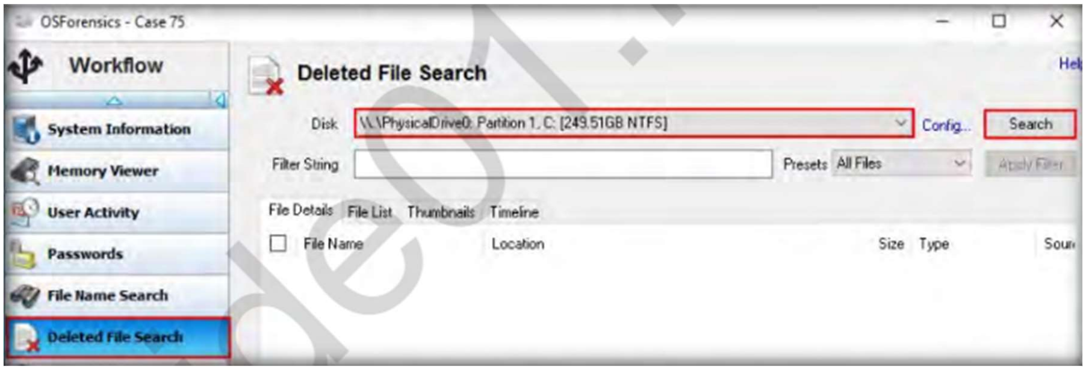
If you wish to save any of the above user-activity information on your system, such as Browser History, then scroll down the items list in the left pane below the Scan Drive option and expand the Browser History node. Select the browser for which you wish to retrieve the history (Here, we are selecting Chrome). The browser history pertaining to this browser will be displayed in the right pane of the tool window.



An Export List to. Window will appear. Navigate to C:\Users\Administrator\Documents\PassMark\OSForensics\Cases\Case 75, name the file (here, we are naming it as Browsing History), and click Save to export the browsing history.



To recover deleted files from the file system, click Deleted File Search in the left pane, select a disk on which you wish to perform the deleted file search from the Disk drop-down menu, and click the search button.

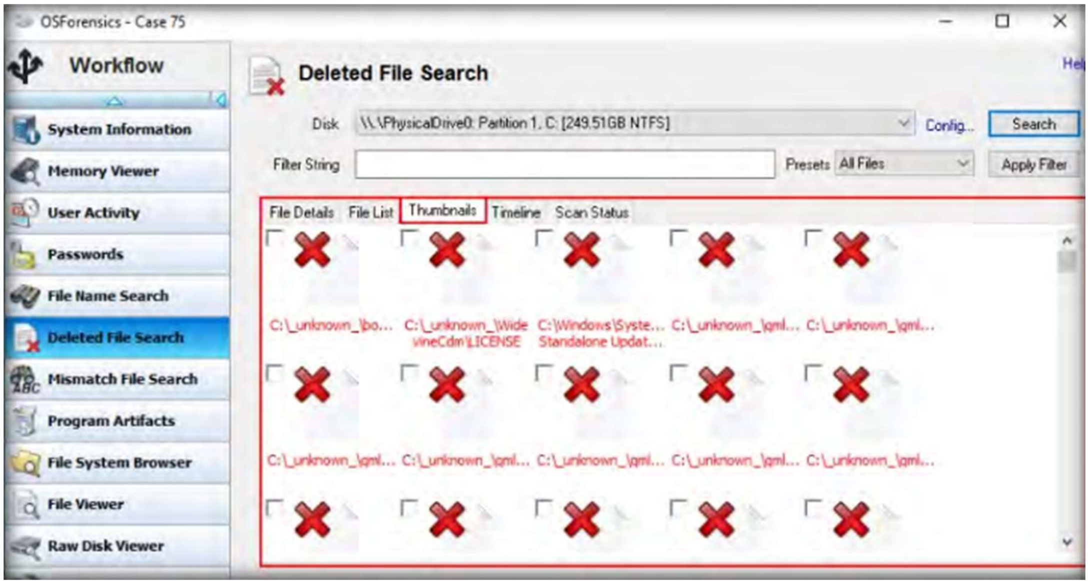


Deleted File Search

Disk \\.\PhysicalDrive0: Partition 1, C: [249.51GB NTFS]

Filter String

Presets All Files



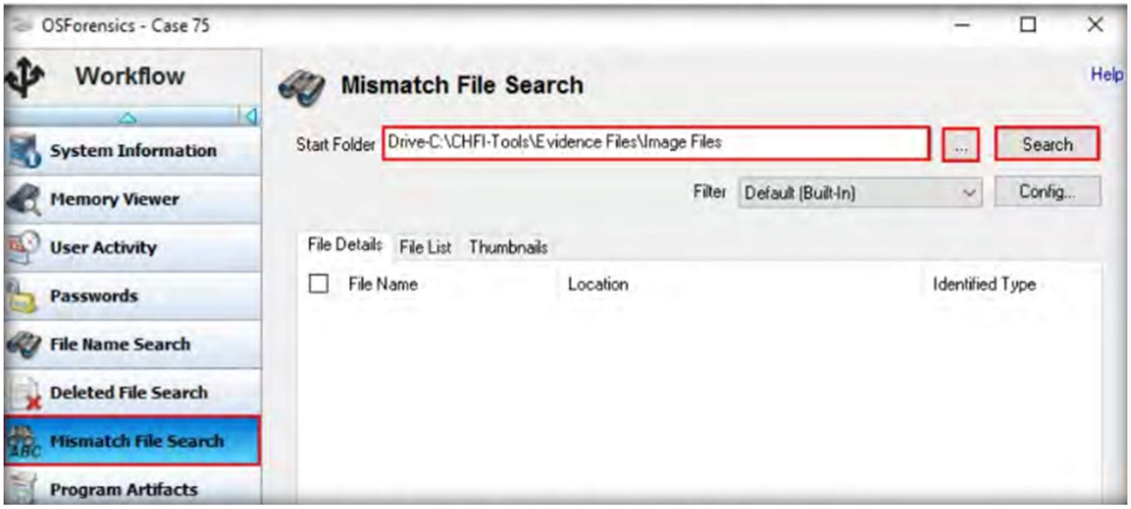
Deleted File Search

Disk \\.\PhysicalDrive0: Partition 1, C: [249.51GB NTFS]

Filter String

Presets All Files

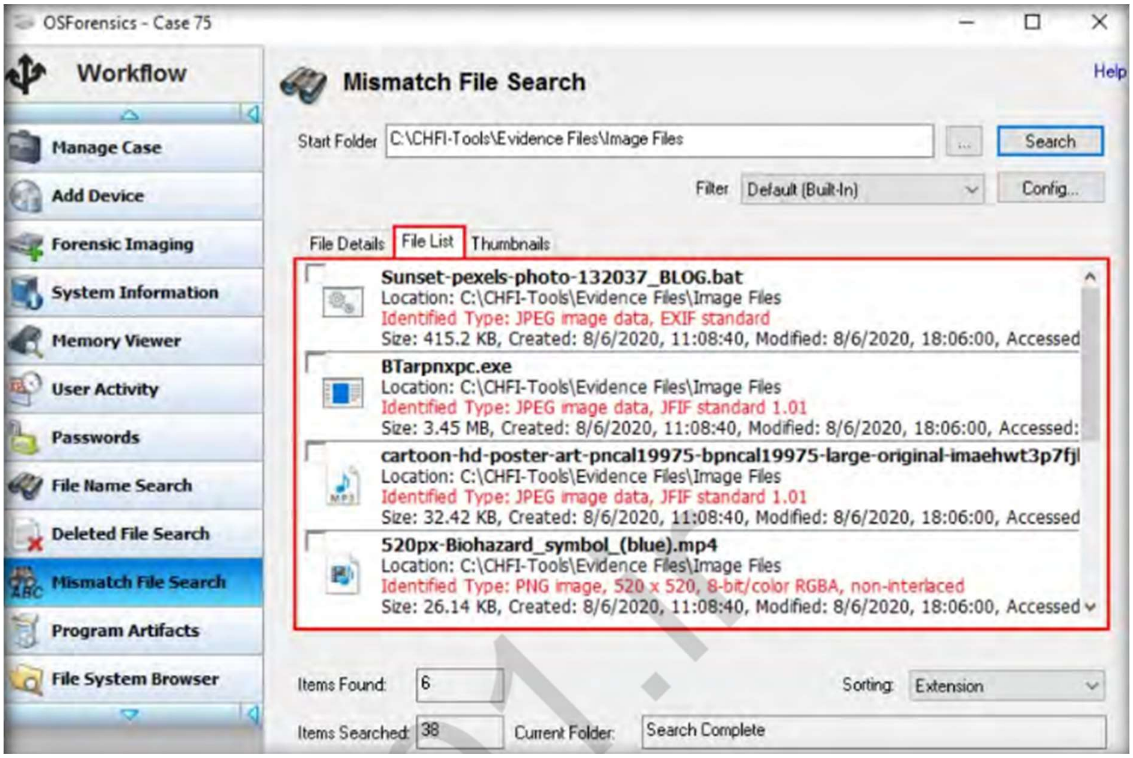
To locate files having contents that do not match the file extensions, click Mismatch File Search in the left pane of the tool window. The tool will display the Mismatch File Search section in the right pane, as shown in the screenshot:



Mismatch File Search

Start Folder Drive-C:\CHFI-Tools\Evidence Files\Image Files

Filter Default (Built-In)



Start Folder: C:\CHFI-Tools\Evidence Files\Image Files

Filter: Default (Built-In)

Sunset-pexels-photo-132037_BLOG.bat
Location: C:\CHFI-Tools\Evidence Files\Image Files
Identified Type: JPEG image data, EXIF standard
Size: 415.2 KB, Created: 8/6/2020, 11:08:40, Modified: 8/6/2020, 18:06:00, Accessed

BTarpnxpc.exe
Location: C:\CHFI-Tools\Evidence Files\Image Files
Identified Type: JPEG image data, JFIF standard 1.01
Size: 3.45 MB, Created: 8/6/2020, 11:08:40, Modified: 8/6/2020, 18:06:00, Accessed:

cartoon-hd-poster-art-pncal19975-bpncal19975-large-original-imaehwt3p7fjl
Location: C:\CHFI-Tools\Evidence Files\Image Files
Identified Type: JPEG image data, JFIF standard 1.01
Size: 32.42 KB, Created: 8/6/2020, 11:08:40, Modified: 8/6/2020, 18:06:00, Accessed

520px-Biohazard_symbol_(blue).mp4
Location: C:\CHFI-Tools\Evidence Files\Image Files
Identified Type: PNG image, 520 x 520, 8-bit/color RGBA, non-interlaced
Size: 26.14 KB, Created: 8/6/2020, 11:08:40, Modified: 8/6/2020, 18:06:00, Accessed

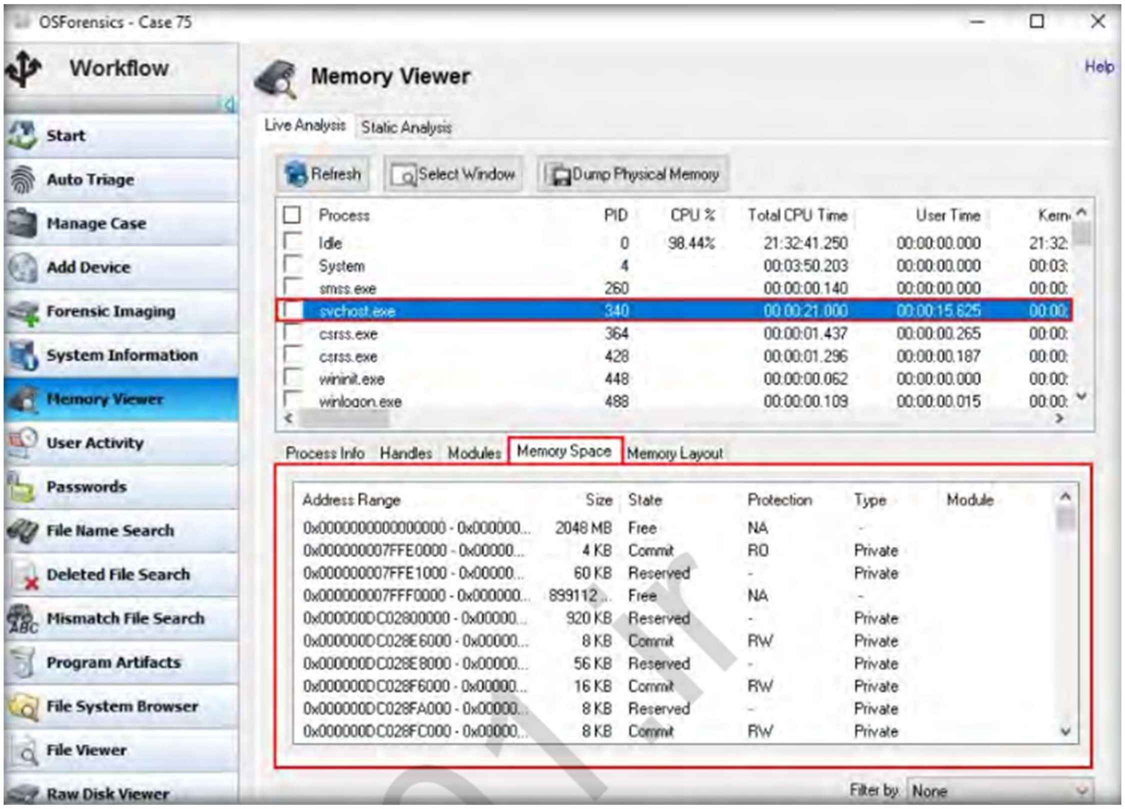
Items Found: 6

Sorting: Extension

Items Searched: 38

Current Folder: Search Complete

To view the processes running on the system, click Memory Viewer

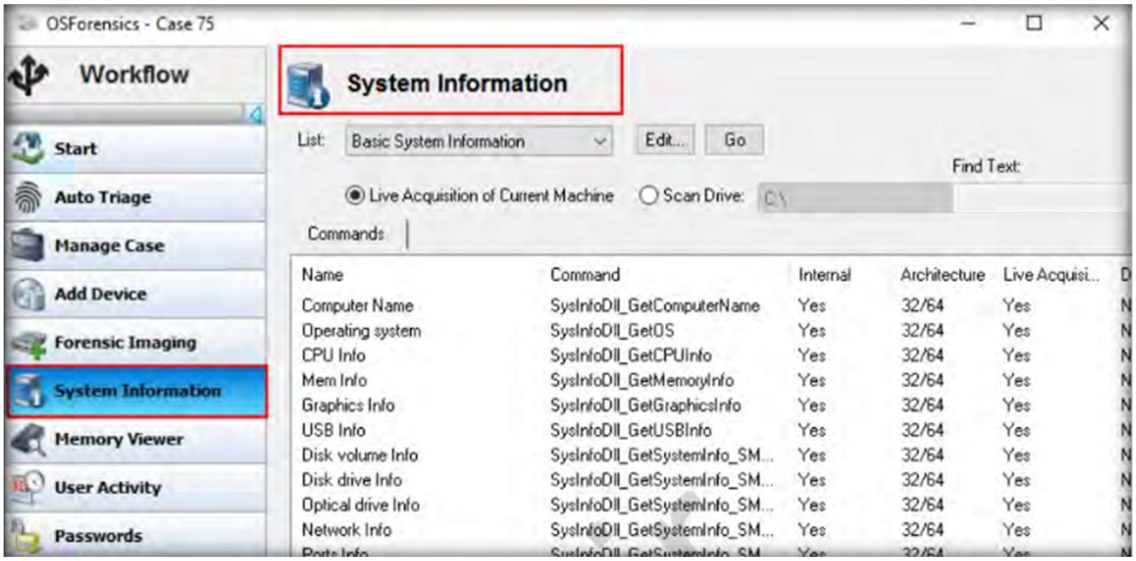


Process	PID	CPU %	Total CPU Time	User Time	Kern
Idle	0	98.44%	21:32:41.250	00:00:00.000	21:32:
System	4		00:03:50.203	00:00:00.000	00:03:
smss.exe	260		00:00:00.140	00:00:00.000	00:00:
svchost.exe	340		00:00:21.000	00:00:15.625	00:00:
csrss.exe	364		00:00:01.437	00:00:00.265	00:00:
csrss.exe	428		00:00:01.296	00:00:00.187	00:00:
wininit.exe	448		00:00:00.062	00:00:00.000	00:00:
winlogon.exe	488		00:00:00.109	00:00:00.015	00:00:

Address Range	Size	State	Protection	Type	Module
0x0000000000000000 - 0x000000...	2048 MB	Free	NA	-	
0x000000007FFE0000 - 0x00000...	4 KB	Commit	RO	Private	
0x000000007FFE1000 - 0x00000...	60 KB	Reserved	-	Private	
0x000000007FFF0000 - 0x000000...	899112...	Free	NA	-	
0x000000DC02800000 - 0x00000...	920 KB	Reserved	-	Private	
0x000000DC028E6000 - 0x00000...	8 KB	Commit	RW	Private	
0x000000DC028E8000 - 0x00000...	56 KB	Reserved	-	Private	
0x000000DC028F6000 - 0x00000...	16 KB	Commit	RW	Private	
0x000000DC028FA000 - 0x00000...	8 KB	Reserved	-	Private	
0x000000DC028FC000 - 0x00000...	8 KB	Commit	RW	Private	

Filter by: None

To retrieve detailed information about the core components of the system, click System Information. The tool will display the System Information section.



List: Basic System Information

● Live Acquisition of Current Machine ○ Scan Drive: C:\

Name	Command	Internal	Architecture	Live Acquisi...	D
Computer Name	SysInfoDll_GetComputerName	Yes	32/64	Yes	N
Operating system	SysInfoDll_GetOS	Yes	32/64	Yes	N
CPU Info	SysInfoDll_GetCPUInfo	Yes	32/64	Yes	N
Mem Info	SysInfoDll_GetMemoryInfo	Yes	32/64	Yes	N
Graphics Info	SysInfoDll_GetGraphicsInfo	Yes	32/64	Yes	N
USB Info	SysInfoDll_GetUSBInfo	Yes	32/64	Yes	N
Disk volume Info	SysInfoDll_GetSystemInfo_SM...	Yes	32/64	Yes	N
Disk drive Info	SysInfoDll_GetSystemInfo_SM...	Yes	32/64	Yes	N
Optical drive Info	SysInfoDll_GetSystemInfo_SM...	Yes	32/64	Yes	N
Network Info	SysInfoDll_GetSystemInfo_SM...	Yes	32/64	Yes	N
Ports Info	SysInfoDll_GetSystemInfo_SM...	Yes	32/64	Yes	N

In this manner, you can perform investigation on a system or the folders and partitions within the system to gather data of interest to the forensic investigation.