Access Machines 7

Cyber Defense > Incident Response and Forensics > Windows Forensics 2

Windows Forensics 2

Learn about common Windows file systems and forensic artifacts in the file systems.

Medium 70 min

Start AttackBox | Help | Save Room | 481

Options

Room completed (100%)

Task 1 ✓ Introduction

Task 2 ✓ The FAT file systems

Task 3 ✓ The NTFS File System

Task 4 ✓ Recovering deleted files

Deleted files and Data recovery:

Understanding the file systems makes it easier to know how files are deleted, recovered, and wiped. As we learned in the previous two tasks, a file system stores the location of a file on the disk in a table or a database. When we delete a file from the file system, the file system deletes the entries that store the file's location on the disk. For the file system, the location where the file existed is now available for writing or unallocated. However, the file contents on disk are still there, as long as they are not overwritten by the file system while copying another file or by the disk firmware while performing maintenance on the disk.

Similarly, there is data on the disk in different unallocated clusters, which can possibly be recovered. To recover this data, we have to understand the file structure of different file types to identify the specific file through the data we see in a hex editor. However, we will not cover that in this room. What we will do, is to use a tool that does this work for us and identifies deleted files in a disk image file. But what is a disk image file?

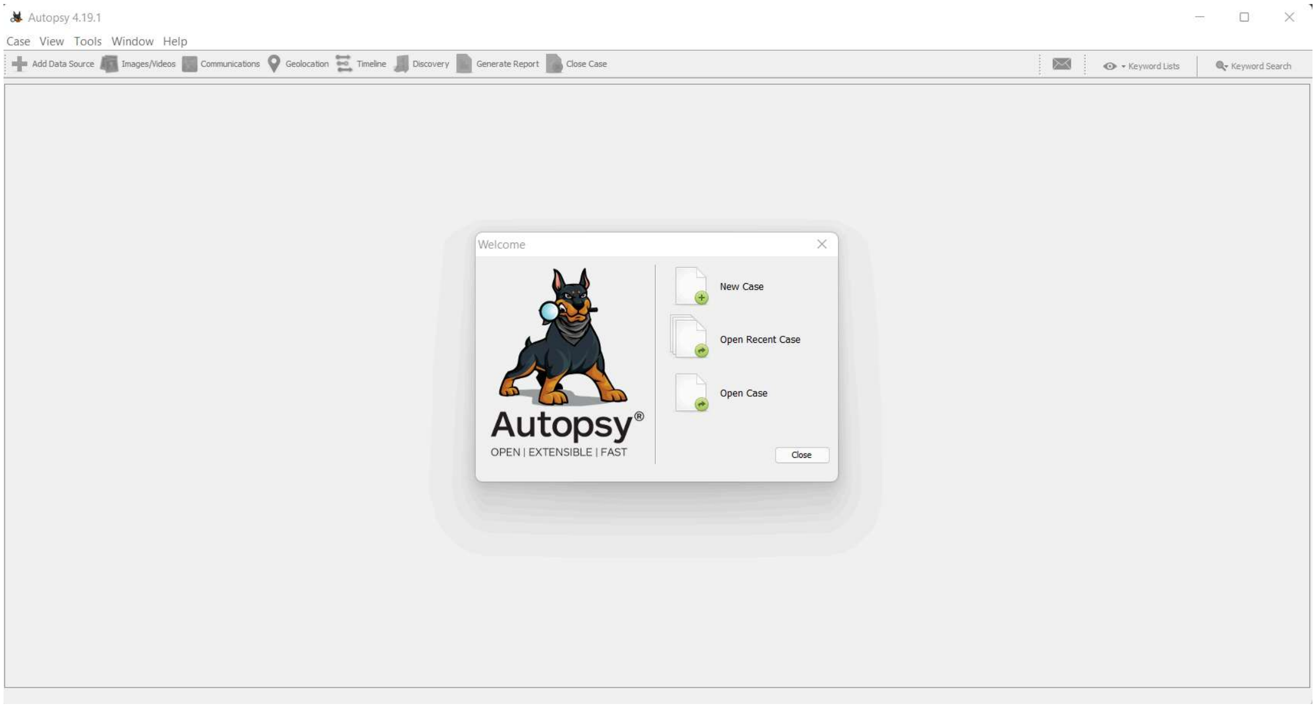
Disk Image:

A disk image file is a file that contains a bit-by-bit copy of a disk drive. A bit-by-bit copy saves all the data in a disk image file, including the metadata, in a single file. Thus, while performing forensics, one can make several copies of the physical evidence, i.e., the disk, and use them for investigation. This helps in two ways. 1) The original evidence is not contaminated while performing forensics, and 2) The disk image file can be copied to another disk and analyzed without using specialized hardware.

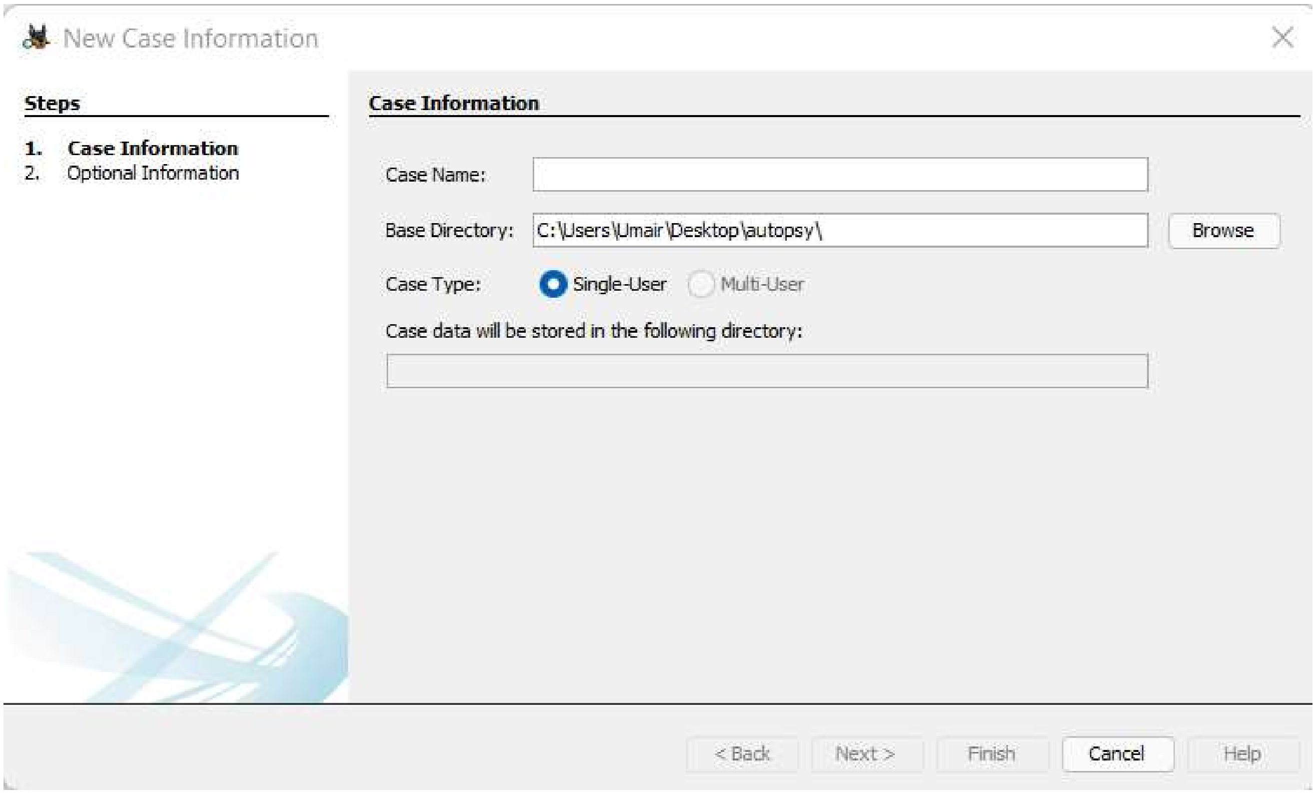
Recovering files using Autopsy

With that out of the way, let's see how we can recover deleted files from a disk. We will use Autopsy for recovering deleted files. For a room dedicated to Autopsy, you can go here.

On the attached VM, you will find an icon for Autopsy on the Desktop. Double-click it to run Autopsy. You will be greeted with the following screen:



Click on the 'New Case' Option. You will find a window similar to the following:



Case Information

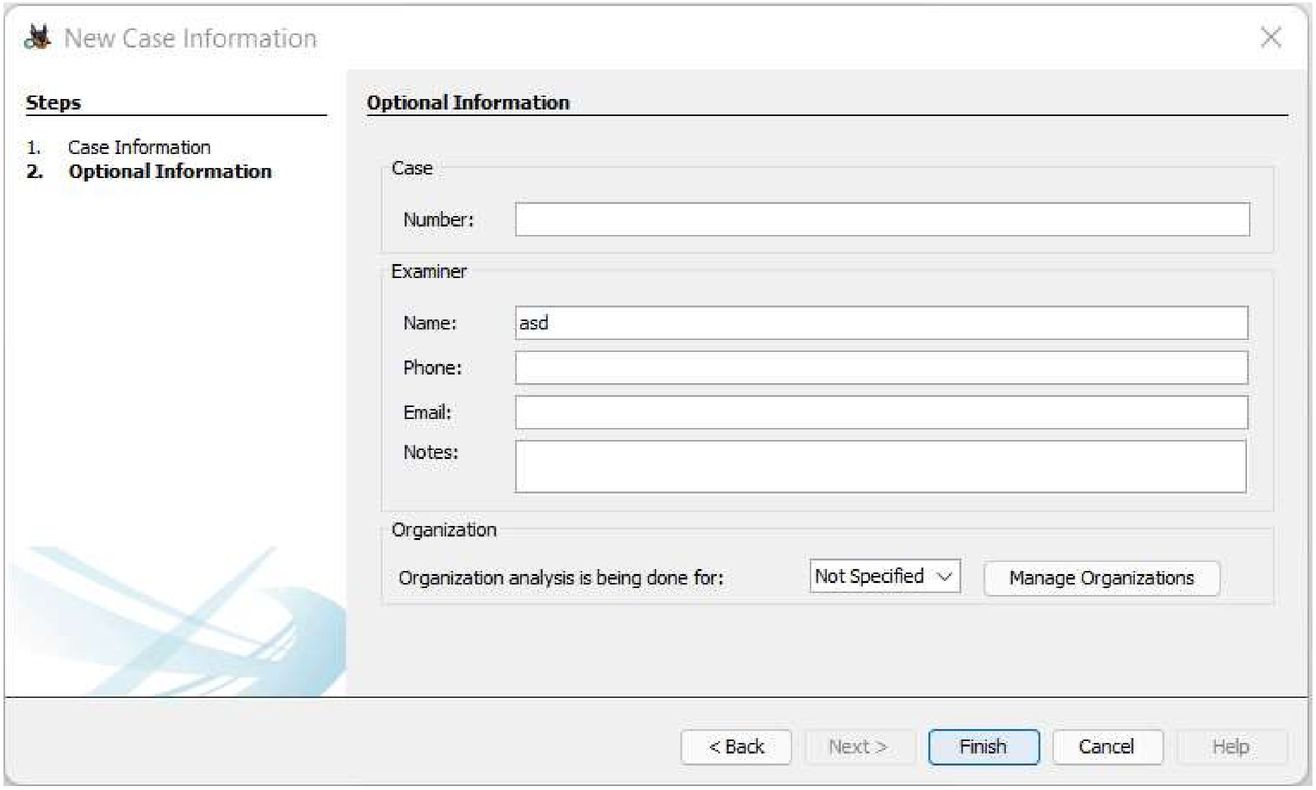
Case Name:

Base Directory: C:\Users\Umair\Desktop\autopsy\

Case Type: ● Single-User ○ Multi-User

Case data will be stored in the following directory:

Enter a name to save your case by, and click Next.



Optional Information

Case

Number:

Examiner

Name: asd

Phone:

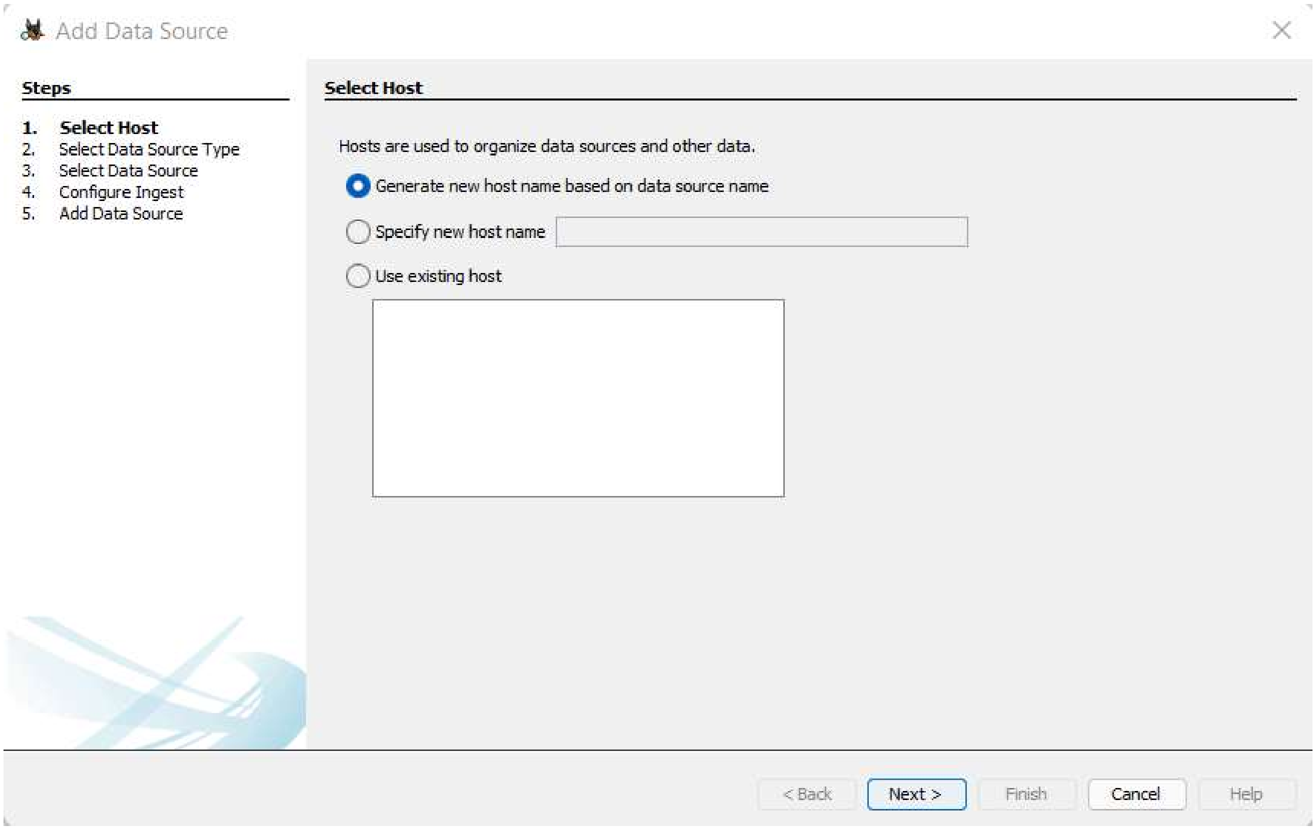
Email:

Notes:

Organization

Organization analysis is being done for: Not Specified

You can add the required details here. For now, we can click Finish to move forward. Autopsy will perform some processing and then show the following screen. Click Next to move forward.



Add Data Source

Steps

1. **Select Host**
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source

Select Host

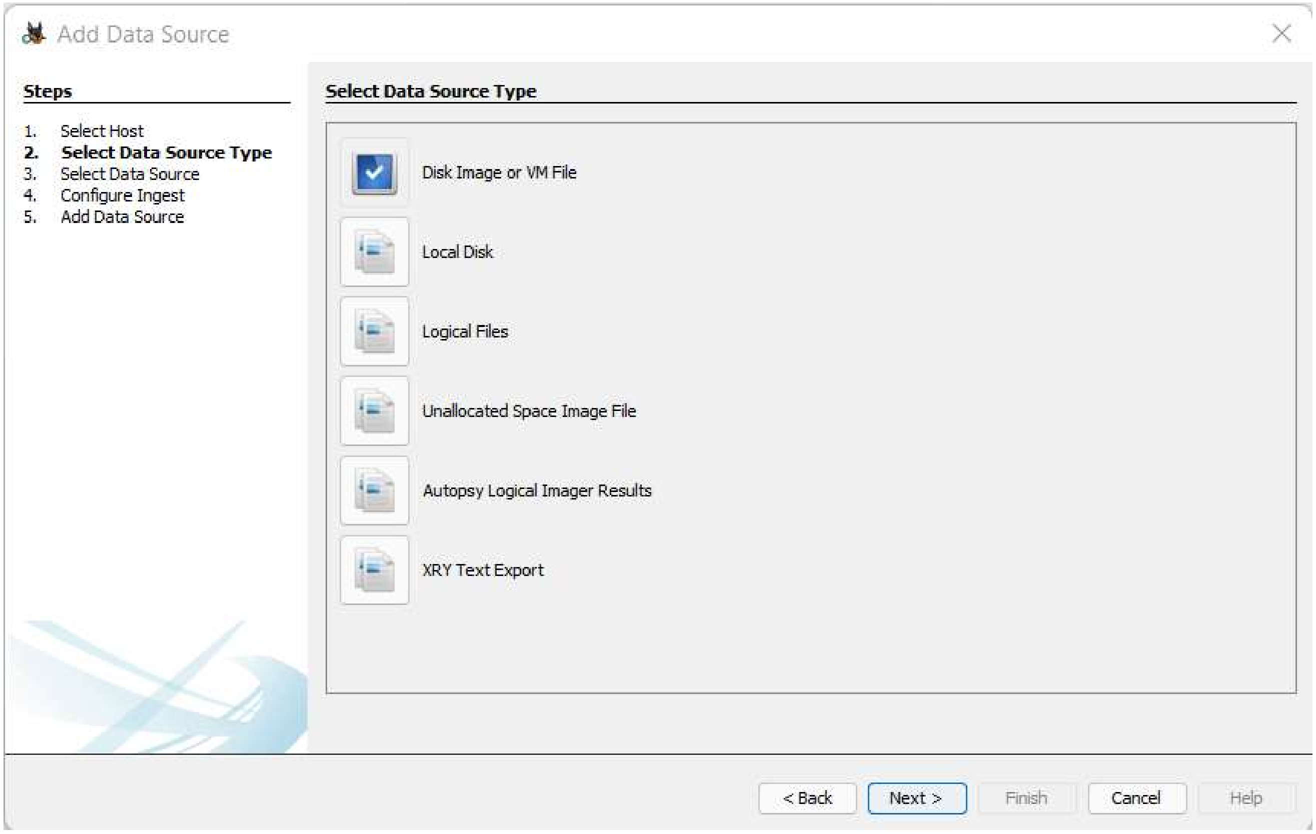
Hosts are used to organize data sources and other data.

● Generate new host name based on data source name

○ Specify new host name

○ Use existing host

You will see this screen. Since we will be performing analysis on a disk image, select the topmost option, Disk Image or VM File.



Add Data Source

Steps

1. Select Host
2. **Select Data Source Type**
3. Select Data Source
4. Configure Ingest
5. Add Data Source

Select Data Source Type

☑ Disk Image or VM File

Local Disk

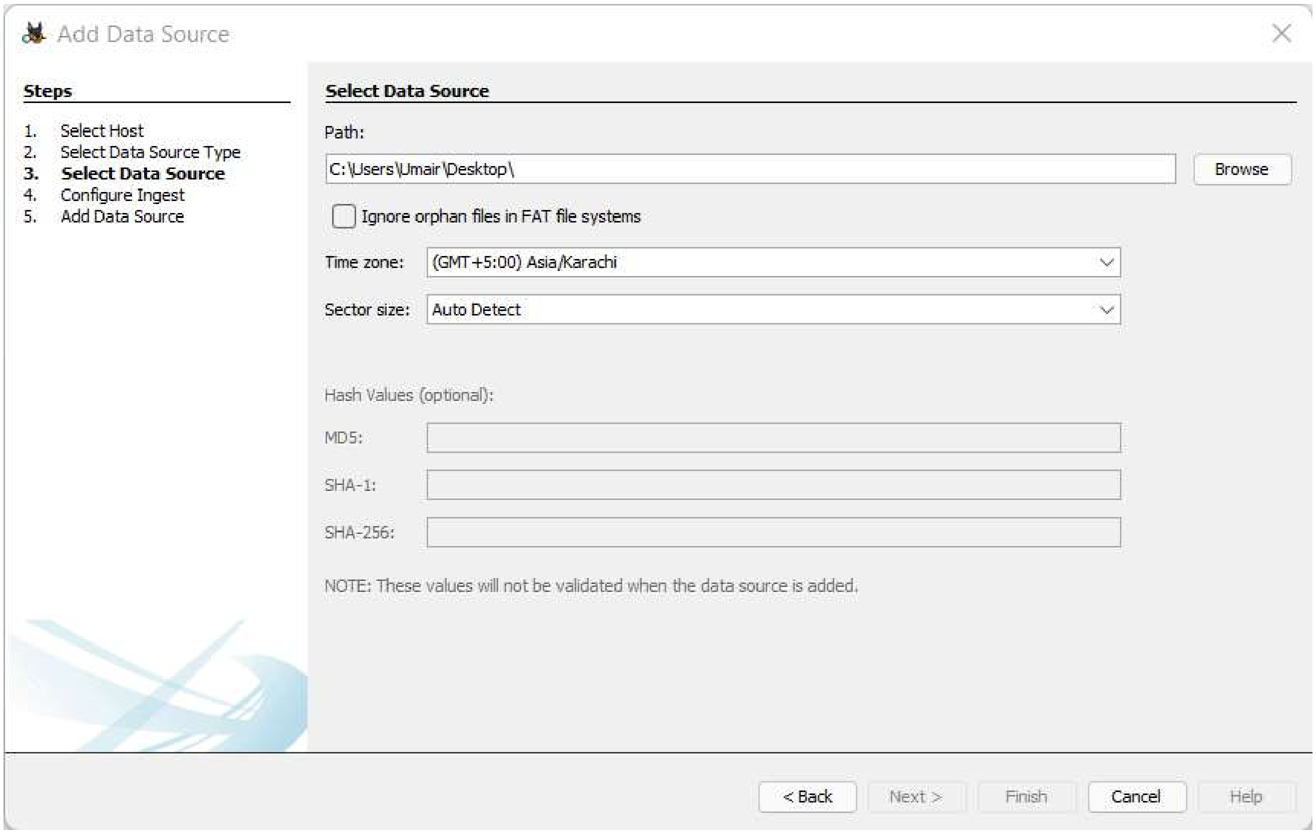
Logical Files

Unallocated Space Image File

Autopsy Logical Imager Results

XRY Text Export

It will ask you for the location of the data source.



Add Data Source

Steps

1. Select Host
2. Select Data Source Type
3. **Select Data Source**
4. Configure Ingest
5. Add Data Source

Select Data Source

Path: C:\Users\Umair\Desktop\

□ Ignore orphan files in FAT file systems

Time zone: (GMT+5:00) Asia/Karachi

Sector size: Auto Detect

Hash Values (optional):

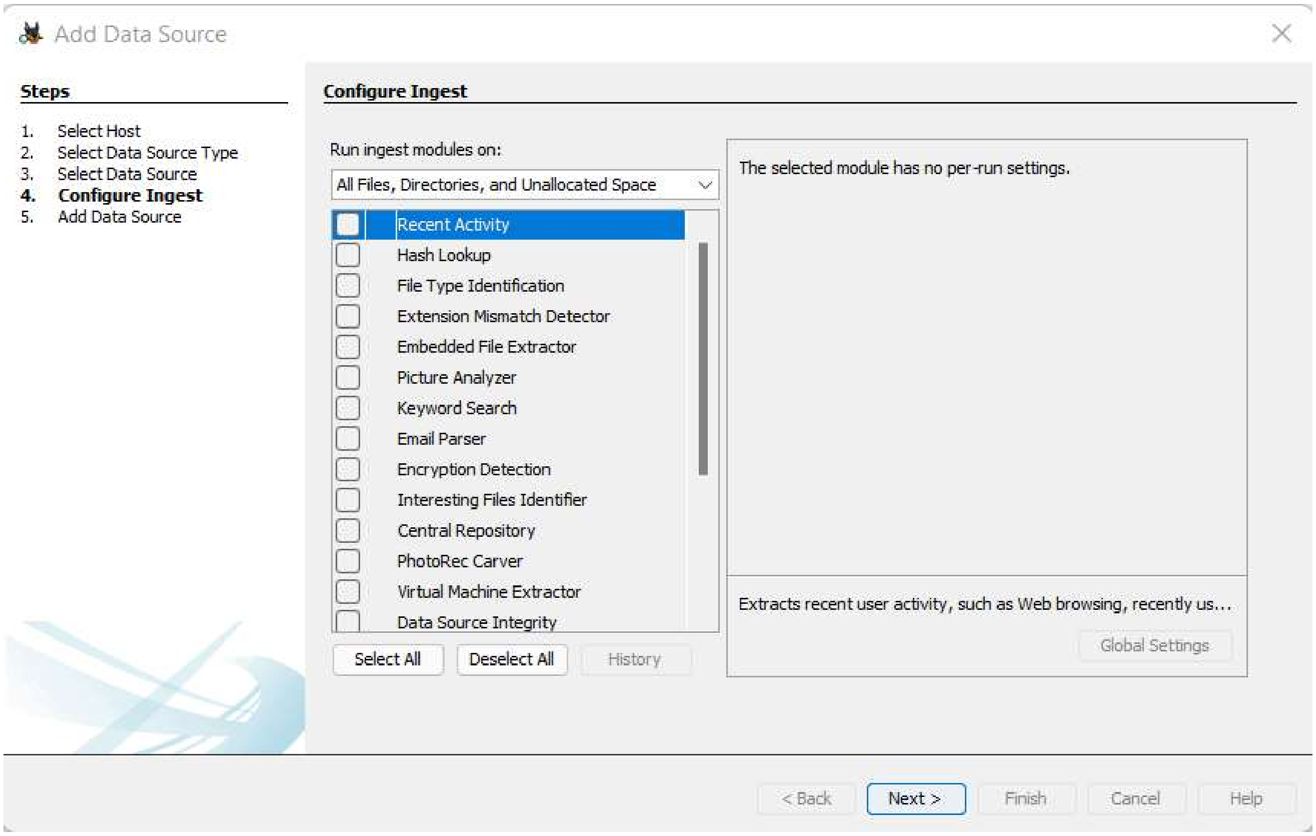
MD5:

SHA-1:

SHA-256:

NOTE: These values will not be validated when the data source is added.

Provide the location of the data source. You will find a disk image named 'usb.001' on the Desktop. Provide the path to that file in the above window and click next. You will see the following window:



Add Data Source

Steps

1. Select Host
2. Select Data Source Type
3. Select Data Source
4. **Configure Ingest**
5. Add Data Source

Configure Ingest

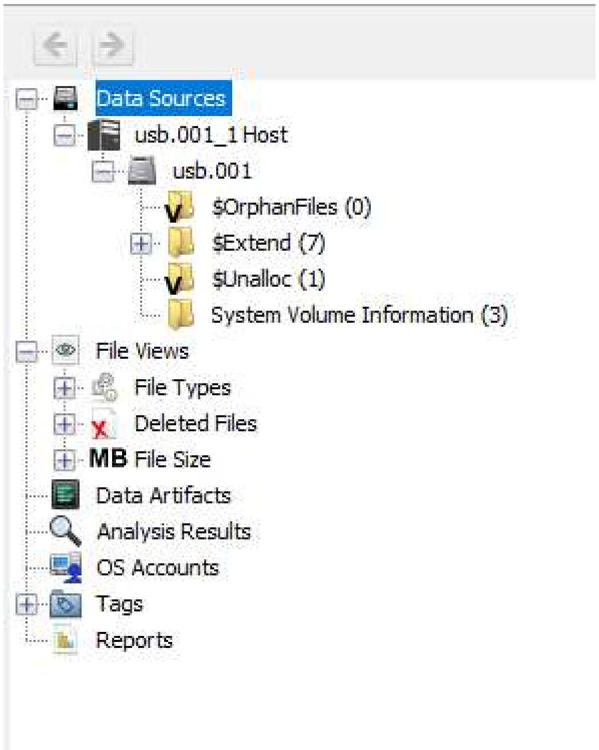
Run ingest modules on: All Files, Directories, and Unallocated Space

- □ Recent Activity
- □ Hash Lookup
- □ File Type Identification
- □ Extension Mismatch Detector
- □ Embedded File Extractor
- □ Picture Analyzer
- □ Keyword Search
- □ Email Parser
- □ Encryption Detection
- □ Interesting Files Identifier
- □ Central Repository
- □ PhotoRec Carver
- □ Virtual Machine Extractor
- □ Data Source Integrity

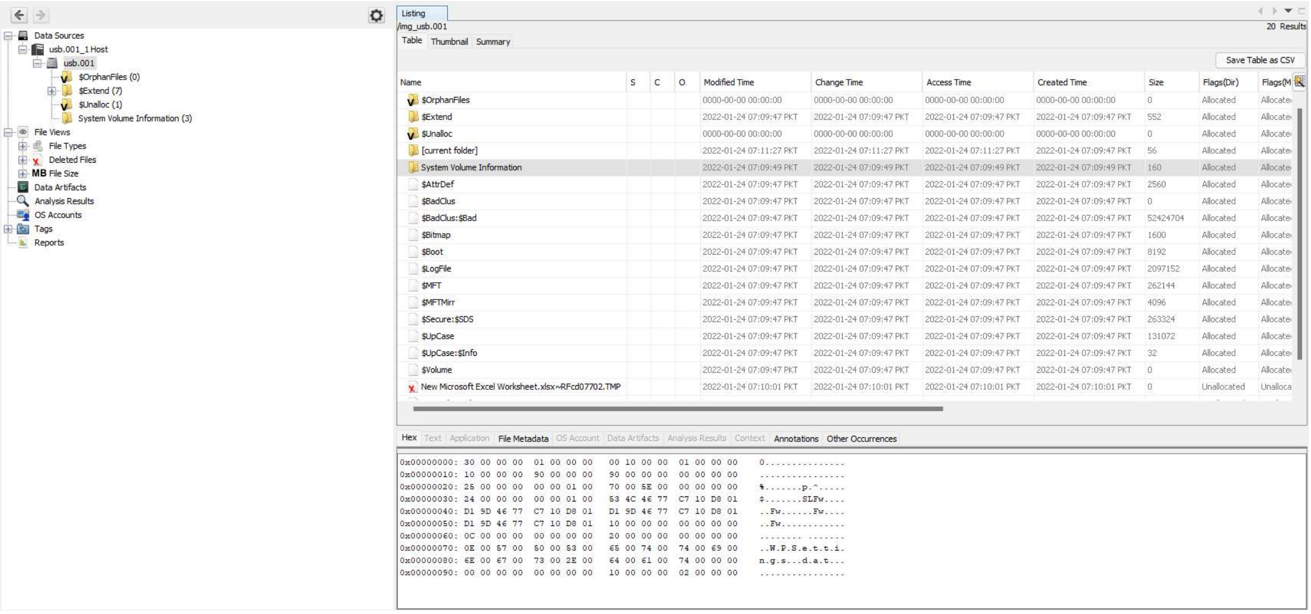
The selected module has no per-run settings.

Extracts recent user activity, such as Web browsing, recently us...

Here, click Deselect All. These are different modules that Autopsy runs on the data for processing. For this task, we don't need any of these. If enabled, they take a lot of time to run. Click Next after clicking Deselect All. Autopsy will load the disk image. You will see the following in the left panel.



The Data Sources show the data sources that we have added to Autopsy. We can add more sources as well. The File Views and Tags menus show what Autopsy has found after processing the data. Expand the Data Sources, and click on the usb.001 device. Autopsy will show the contents of the disk image in the following way:



/img_usb.001

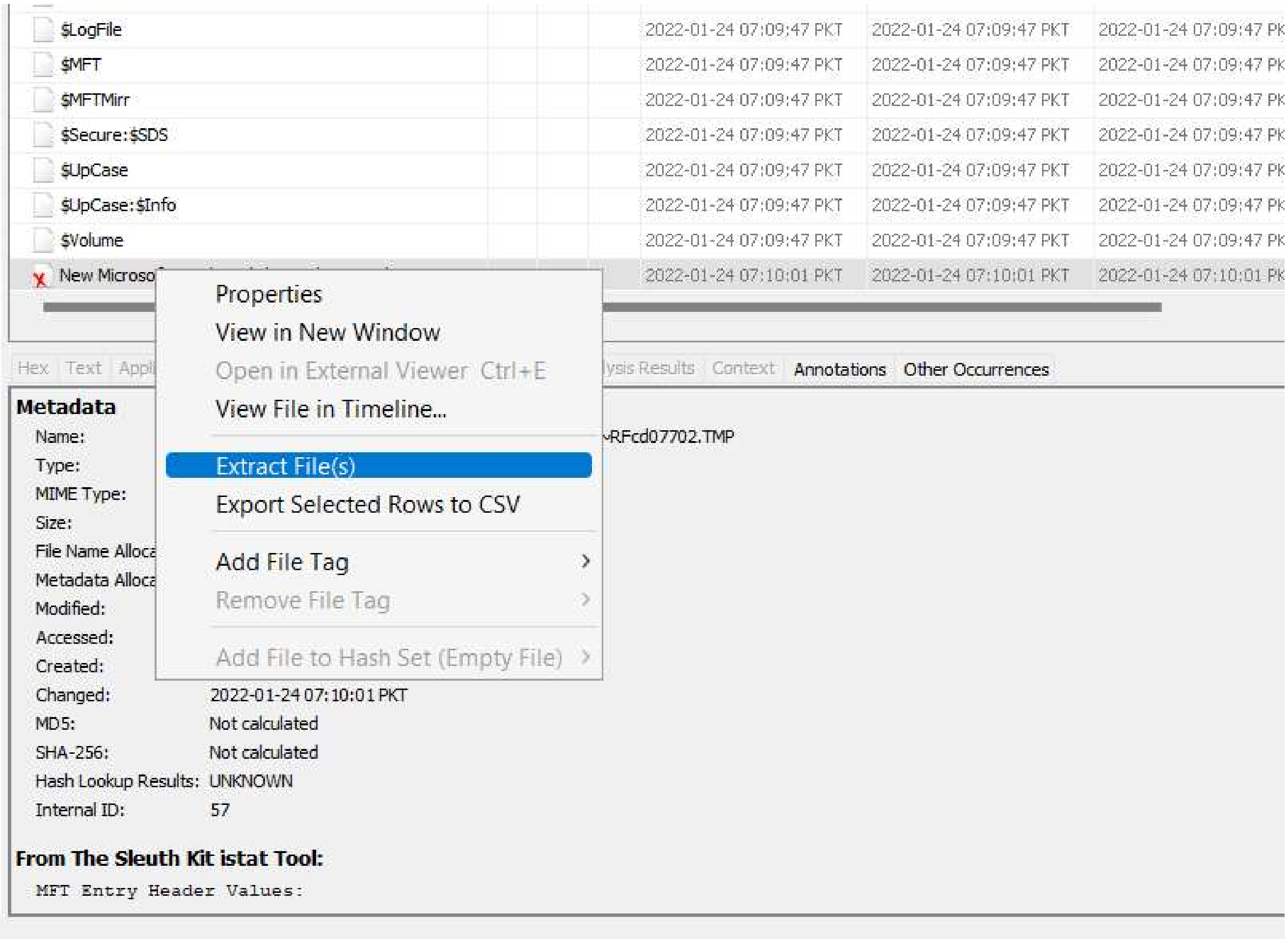
20 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(M
$OrphanFiles				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocate
$Extend				2022-01-24 07:09:47 PKT	2022-01-24 07:09:47 PKT	2022-01-24 07:09:47 PKT	2022-01-24 07:09:47 PKT	552	Allocated	Allocate
$Unalloc				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocate
[current folder]				2022-01-24 07:11:27 PKT	2022-01-24 07:11:27 PKT	2022-01-24 07:11:27 PKT	2022-01-24 07:09:47 PKT	56	Allocated	Allocate
System Volume Information				2022-01-24 07:09:49 PKT	2022-01-24 07:09:49 PKT	2022-01-24 07:09:49 PKT	2022-01-24 07:09:49 PKT	160	Allocated	Allocate
$AttrDef				2022-01-24 07:09:47 PKT	2022-01-24 07:09:47 PKT	2022-01-24 07:09:47 PKT	2022-01-24 07:09:47 PKT	2560	Allocated	Allocate
$BadClus				2022-01-24 07:09:47 PKT	2022-01-24 07:09:47 PKT	2022-01-24 07:09:47 PKT	2022-01-24 07:09:47 PKT	0	Allocated	Allocate
$BadClus:$Bad				2022-01-24 07:09:47 PKT	2022-01-24 07:09:47 PKT	2022-01-24 07:09:47 PKT	2022-01-24 07:09:47 PKT	52424704	Allocated	Allocate
$Bitmap				2022-01-24 07:09:47 PKT	2022-01-24 07:09:47 PKT	2022-01-24 07:09:47 PKT	2022-01-24 07:09:47 PKT	1600	Allocated	Allocate
$Boot				2022-01-24 07:09:47 PKT	2022-01-24 07:09:47 PKT	2022-01-24 07:09:47 PKT	2022-01-24 07:09:47 PKT	8192	Allocated	Allocate
$LogFile				2022-01-24 07:09:47 PKT	2022-01-24 07:09:47 PKT	2022-01-24 07:09:47 PKT	2022-01-24 07:09:47 PKT	2097152	Allocated	Allocate
$MFT				2022-01-24 07:09:47 PKT	2022-01-24 07:09:47 PKT	2022-01-24 07:09:47 PKT	2022-01-24 07:09:47 PKT	262144	Allocated	Allocate
$MFTMirr				2022-01-24 07:09:47 PKT	2022-01-24 07:09:47 PKT	2022-01-24 07:09:47 PKT	2022-01-24 07:09:47 PKT	4096	Allocated	Allocate
$Secure:$SDS				2022-01-24 07:09:47 PKT	2022-01-24 07:09:47 PKT	2022-01-24 07:09:47 PKT	2022-01-24 07:09:47 PKT	263324	Allocated	Allocate
$UpCase				2022-01-24 07:09:47 PKT	2022-01-24 07:09:47 PKT	2022-01-24 07:09:47 PKT	2022-01-24 07:09:47 PKT	131072	Allocated	Allocate
$UpCase:$Info				2022-01-24 07:09:47 PKT	2022-01-24 07:09:47 PKT	2022-01-24 07:09:47 PKT	2022-01-24 07:09:47 PKT	32	Allocated	Allocate
$Volume				2022-01-24 07:09:47 PKT	2022-01-24 07:09:47 PKT	2022-01-24 07:09:47 PKT	2022-01-24 07:09:47 PKT	0	Allocated	Allocate
New Microsoft Excel Worksheet.xlsx~RFcd07702.TMP				2022-01-24 07:10:01 PKT	2022-01-24 07:10:01 PKT	2022-01-24 07:10:01 PKT	2022-01-24 07:10:01 PKT	0	Unallocated	Unalloca

```
0x00000000: 30 00 00 00  01 00 00 00   00 10 00 00  01 00 00 00    0...............
0x00000010: 10 00 00 00  90 00 00 00   90 00 00 00  00 00 00 00    ................
0x00000020: 25 00 00 00  00 00 01 00   70 00 5E 00  00 00 00 00    %.......p.^.....
0x00000030: 24 00 00 00  00 00 01 00   53 4C 46 77  C7 10 D8 01    $.......SLFw....
0x00000040: D1 9D 46 77  C7 10 D8 01   D1 9D 46 77  C7 10 D8 01    ..Fw......Fw....
0x00000050: D1 9D 46 77  C7 10 D8 01   10 00 00 00  00 00 00 00    ..Fw............
0x00000060: 0C 00 00 00  00 00 00 00   20 00 00 00  00 00 00 00    ........ .......
0x00000070: 0E 00 57 00  50 00 53 00   65 00 74 00  74 00 69 00    ..W.P.S.e.t.t.i.
0x00000080: 6E 00 67 00  73 00 2E 00   64 00 61 00  74 00 00 00    n.g.s...d.a.t...
0x00000090: 00 00 00 00  00 00 00 00   10 00 00 00  02 00 00 00    ................
```

The contents of the disk are shown on the right side. All the files and folders present in the disk are listed in the upper tab. In the lower tab, details about the selected files are shown. There are different options to see the details here. You can check them out to find interesting information.

Notice the X mark on the last file in the screenshot above, named New Microsoft Excel Worksheet.xlsx~RFcd07702.TMP. This indicates that this is a deleted file. Deleted files will have this X mark on them. To recover a deleted file, right-click on it, and select the Extract File(s) option.



$LogFile	2022-01-24 07:09:47 PKT	2022-01-24 07:09:47 PKT	2022-01-24 07:09:47 PK
$MFT	2022-01-24 07:09:47 PKT	2022-01-24 07:09:47 PKT	2022-01-24 07:09:47 PK
$MFTMirr	2022-01-24 07:09:47 PKT	2022-01-24 07:09:47 PKT	2022-01-24 07:09:47 PK
$Secure:$SDS	2022-01-24 07:09:47 PKT	2022-01-24 07:09:47 PKT	2022-01-24 07:09:47 PK
$UpCase	2022-01-24 07:09:47 PKT	2022-01-24 07:09:47 PKT	2022-01-24 07:09:47 PK
$UpCase:$Info	2022-01-24 07:09:47 PKT	2022-01-24 07:09:47 PKT	2022-01-24 07:09:47 PK
$Volume	2022-01-24 07:09:47 PKT	2022-01-24 07:09:47 PKT	2022-01-24 07:09:47 PK
New Microso	2022-01-24 07:10:01 PKT	2022-01-24 07:10:01 PKT	2022-01-24 07:10:01 PK

Metadata

Name: ~RFcd07702.TMP
Type:
MIME Type:
Size:
File Name Alloca
Metadata Alloca
Modified:
Accessed:
Created:
Changed: 2022-01-24 07:10:01 PKT
MD5: Not calculated
SHA-256: Not calculated
Hash Lookup Results: UNKNOWN
Internal ID: 57

From The Sleuth Kit istat Tool:

```
MFT Entry Header Values:
```

Provide the path to save the extracted file, and you will have your deleted file recovered. Now let's see what other deleted files you can find on this disk image and answer the following questions.

Answer the questions below

There is another xlsx file that was deleted. What is the full name of that file?

Tryhackme.xlsx ✓ Correct Answer

What is the name of the TXT file that was deleted from the disk?

TryHackMe2.txt

✓ Correct Answer

Recover the TXT file from Question #2. What was written in this txt file?

thm-4n6-2-4

✓ Correct Answer

Task 5 ✓ Evidence of Execution

Task 6 ✓ File/folder knowledge

Task 7 ✓ External Devices/USB device forensics

Task 8 ✓ Conclusion and Further material

Created by

tryhackme umairalizafar

Room Type	Users in Room	Created
Only subscribers can deploy virtual machines in this room! Go to your profile page to subscribe (if you have not already).	23,000	932 days ago