

Deleted File Recovery. Part 1.

Presenter: Dr. S. Roy, Dept. of CS, BGSU

Event: 2024 CyberGuardians Camp

Date: June 24-28, 2024

Outline

- A motivation video
- The Gist of Part 1 of the Module
- What Part 1 of the Module contains
- Let's run the lab activity: Lab 1.1 and Lab 1.2

The Gist of Part 1 of the Module

- A free GUI-based tool (Autopsy) on a Windows computer is used
- We demonstrate that we can recover deleted files in many scenarios
- We experience that there are two types of recovery mechanisms: metadata-based recovery and file carving
 - Metadata-based recovery works for any type of file as long as metadata is present
 - File carving works only for the file types that have a header signature and a footer signature

What Part 1 of the Module contains

- Item 1. a motivation video
- Item 2. a lecture ppt
- Item 3. two lessons
- Item 4. labs
 - Lab 1.1
 - Lab 1.2
 - a resource folder containing sample artifacts
- Item 5. exercises
 - exercise 1.1
 - exercise 1.2
 - a resource folder containing sample artifacts
- Item 6. An endnote

Now let's start Part 1

A common scenario in real-life Digital Forensics

- The court orders a suspect to hand over his thumb drive
- The suspect deletes files in his thumb drive before handing it over to the law enforcement



A common scenario in real-life (Contd.)

- A digital forensics analyst uses some “magic” tools on the thumb drive to recover the deleted files
- The recovered files help the analyst connect the dots in making the case against the suspect



In this module, we will learn about those “magic” tools that recover deleted files.

The driving
question for
us in this
module

- How can we recover deleted files?

Let's discover via hands-on experiments

Experiment and discover

- We use a free popular tool named **Autopsy** to recover deleted files
 - Autopsy runs on a Windows computer
 - Get the tool from <https://www.autopsy.com/download/>
- The case story: A thumb drive is seized from a suspect, which had bunch of files (e.g., some text, some documents, some photos, etc.); however, those files are now deleted
- We experiment with two scenarios
 - Lab 1.1: the suspect has simply deleted the files in the thumb drive
 - Lab 1.2: the suspect has done “quick format” of the thumb drive
- The detailed instructions for the labs are available to us in the corresponding folder.

Lab 1.1

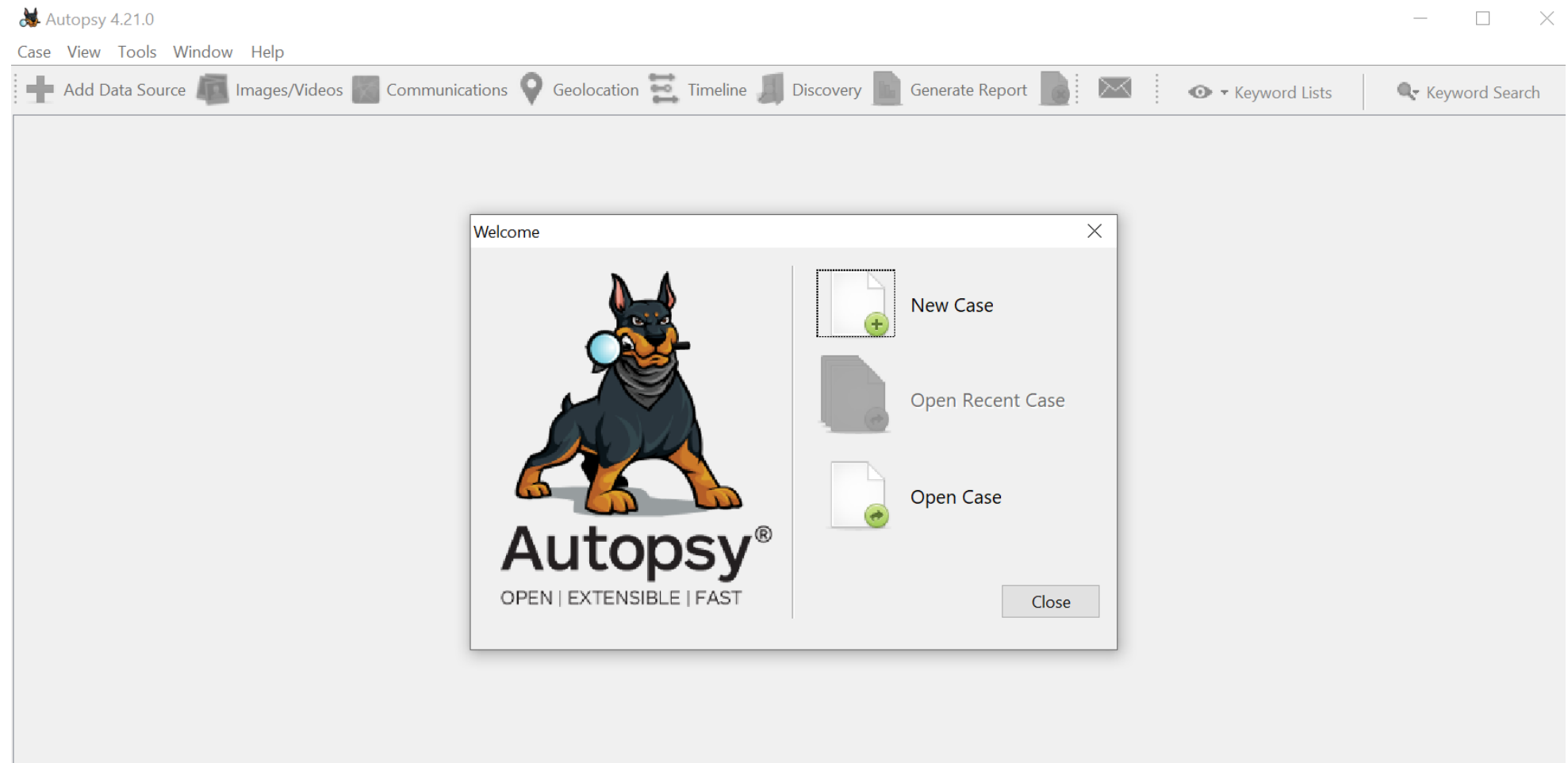
- The suspect deleted files and folder in the thumb drive
- Can we recover the files and folders?

Setting up the lab: The instructor prepares the thumb drive

- Create a small *partition* in the thumb drive
 - Use the *disk management* tool on a Windows computer (refer to Appendix, if necessary)
 - Make the size of the partition 1 GB
 - Create a FAT32 file system
 - Uncheck the “quick format” option so that everything is erased
- The lab has a *resource* folder that contains a few artifacts
 - Copy the content of *collection1* to the newly created partition of the thumb drive
 - Note that we do not copy the *collection1* folder, but copy only what is inside
- Apply the usual “delete” operation to delete the whole content
- The thumb drive is ready now
- Let’s start the Autopsy tool

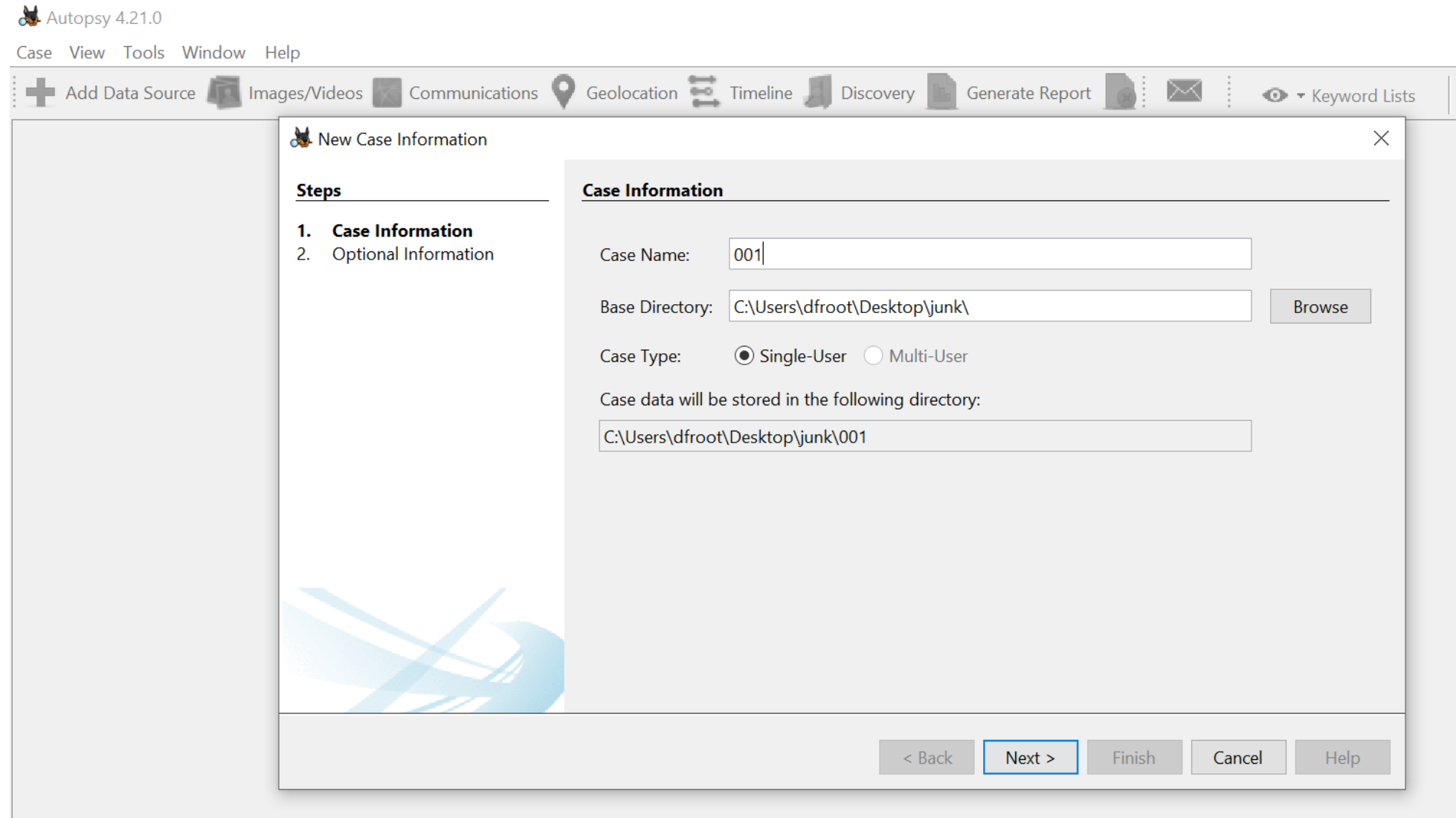
Starting Autopsy

- Start Autopsy on a Windows computer
- Start a **New Case** and proceed



Putting down case information

- Choose a name for the case
- Choose a directory to store information about the case



The screenshot shows the Autopsy 4.21.0 application window with the 'New Case Information' dialog box open. The dialog box has a title bar with the Autopsy logo and the text 'New Case Information'. It features a 'Steps' panel on the left with two steps: '1. Case Information' (selected) and '2. Optional Information'. The main area is titled 'Case Information' and contains the following fields and controls:

- Case Name:** A text input field containing '001'.
- Base Directory:** A text input field containing 'C:\Users\dfroot\Desktop\junk\'. To its right is a 'Browse' button.
- Case Type:** Two radio buttons: 'Single-User' (selected) and 'Multi-User'.
- Case data will be stored in the following directory:** A text input field containing 'C:\Users\dfroot\Desktop\junk\001'.

At the bottom of the dialog box, there are five buttons: '< Back' (disabled), 'Next >' (active/highlighted), 'Finish' (disabled), 'Cancel', and 'Help'.

Give case number and proceed

Autopsy 4.21.0

Case View Tools Window Help

+ Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Keyword Lists

New Case Information

Steps

1. Case Information
2. **Optional Information**

Optional Information

Case

Number:

Examiner

Name:

Phone:

Email:

Notes:

Organization

Organization analysis is being done for: Not Specified Manage Organizations

< Back Next > Finish Cancel Help

Choose default options and proceed

001 - Autopsy 4.21.0

Case View Tools Window Help

+ Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Keyword Lists Keyword Search

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

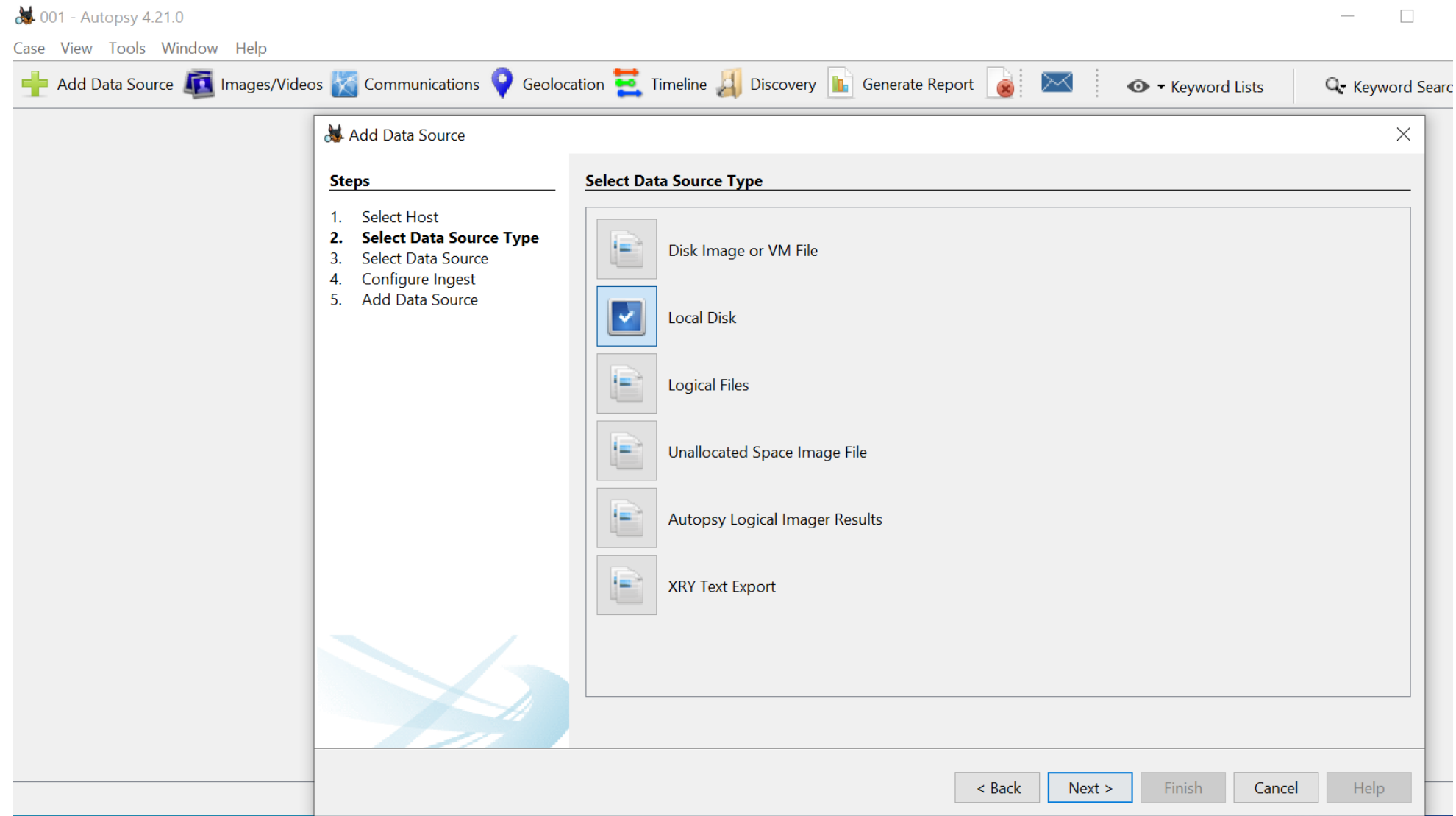
☐ Specify new host name

☐ Use existing host

< Back Next > Finish Cancel Help

Select data source

- Select the thumb drive as the source



Select data source (contd.)

001 - Autopsy 4.21.0

Case View Tools Window Help

+ Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Keyword Lists Keyword Search

Steps

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

Select Data Source

Local Disk: FORENSICS (D:) Select Disk

Timezone: (GMT-5:00) America/New_York

☐ Ignore orphan files in FAT file systems
(faster results, although some data will not be searched)

☐ Make a VHD image of the drive while it is being analyzed

oduleOutput\Image Writer\FORENSICS (D) 1717287739277.vhd Browse

☐ Update case to use VHD file upon completion

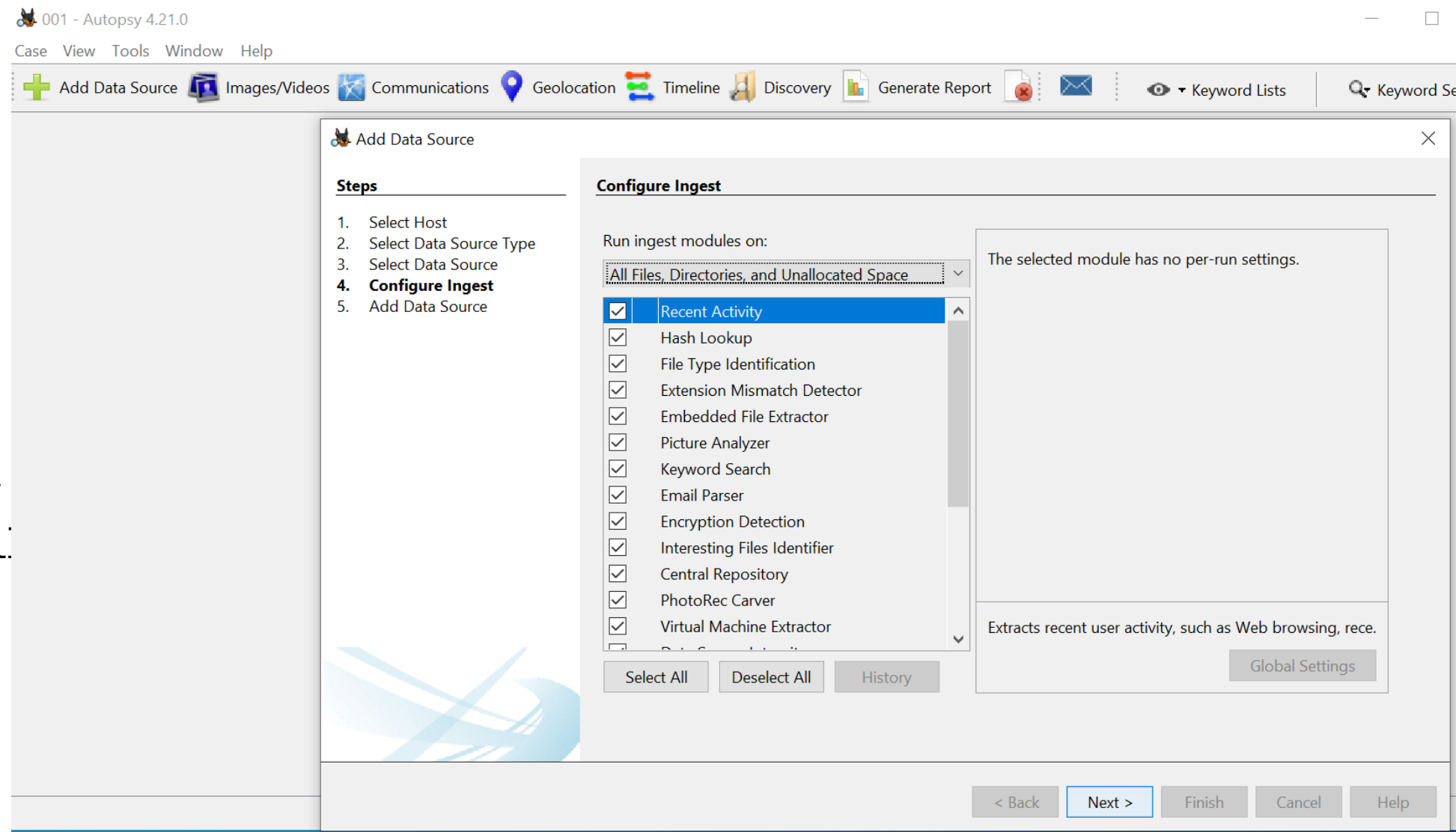
Note that at least one ingest module must be run to create a complete copy

Sector Size: Auto Detect

< Back Next > Finish Cancel Help

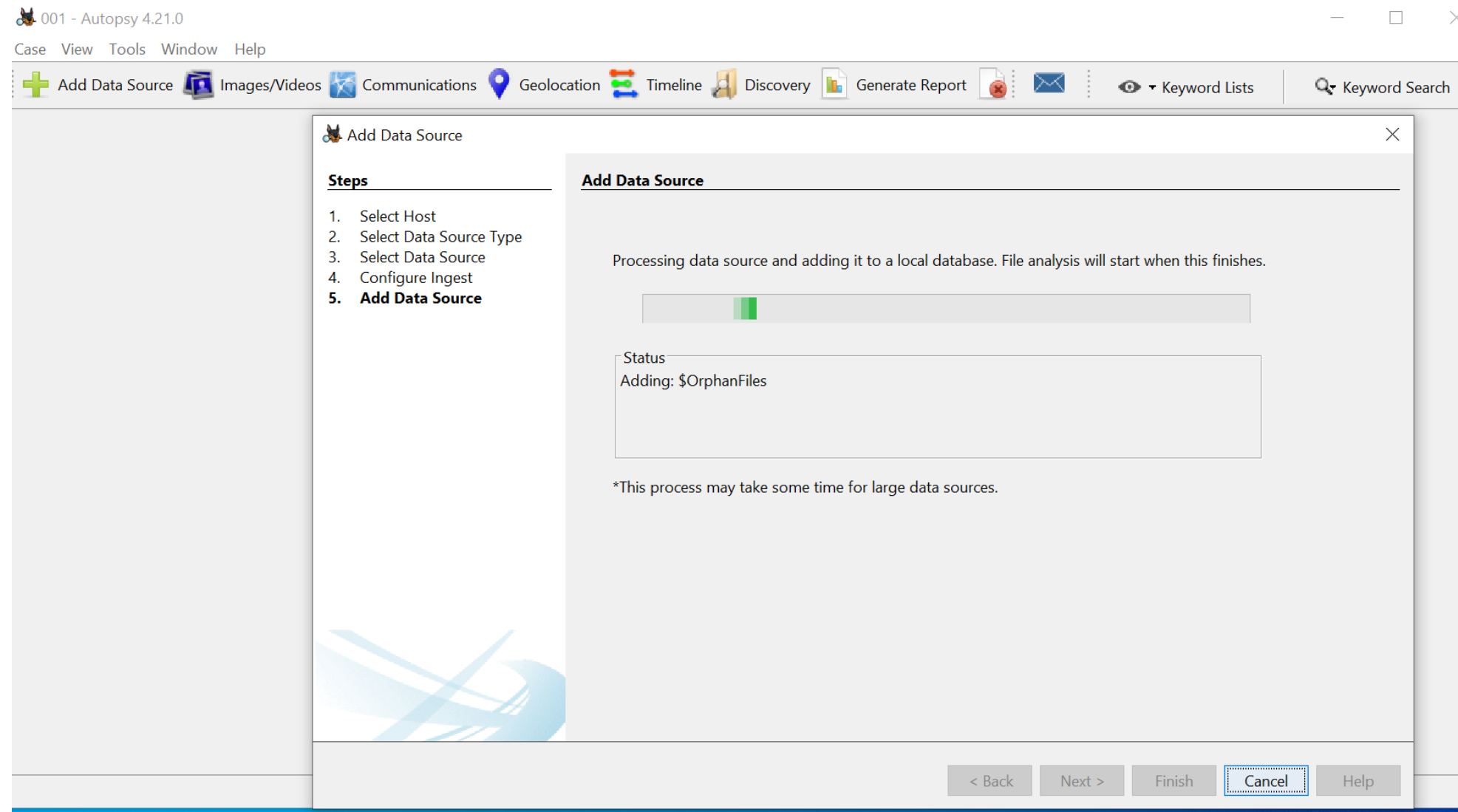
Choose Autopsy modules to run

- We may uncheck irrelevant modules such as virtual machine extractor, Android analyzer, iOS analyzer, and more to save time
- However, it is ok to check ALL (the default option) if your thumb drive is not big



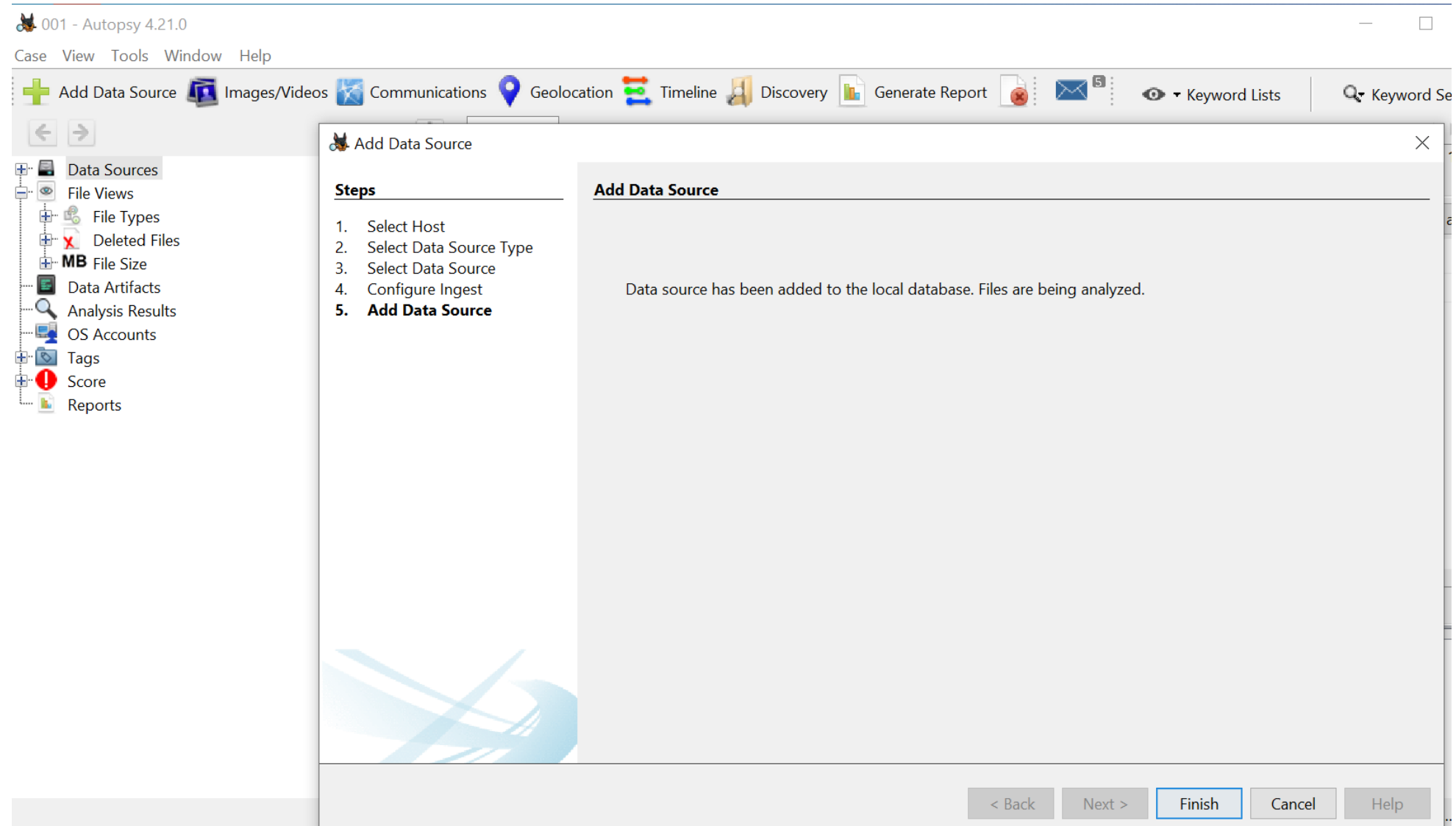
Proceed through the next step

- Wait for the process to complete and click “Finish”



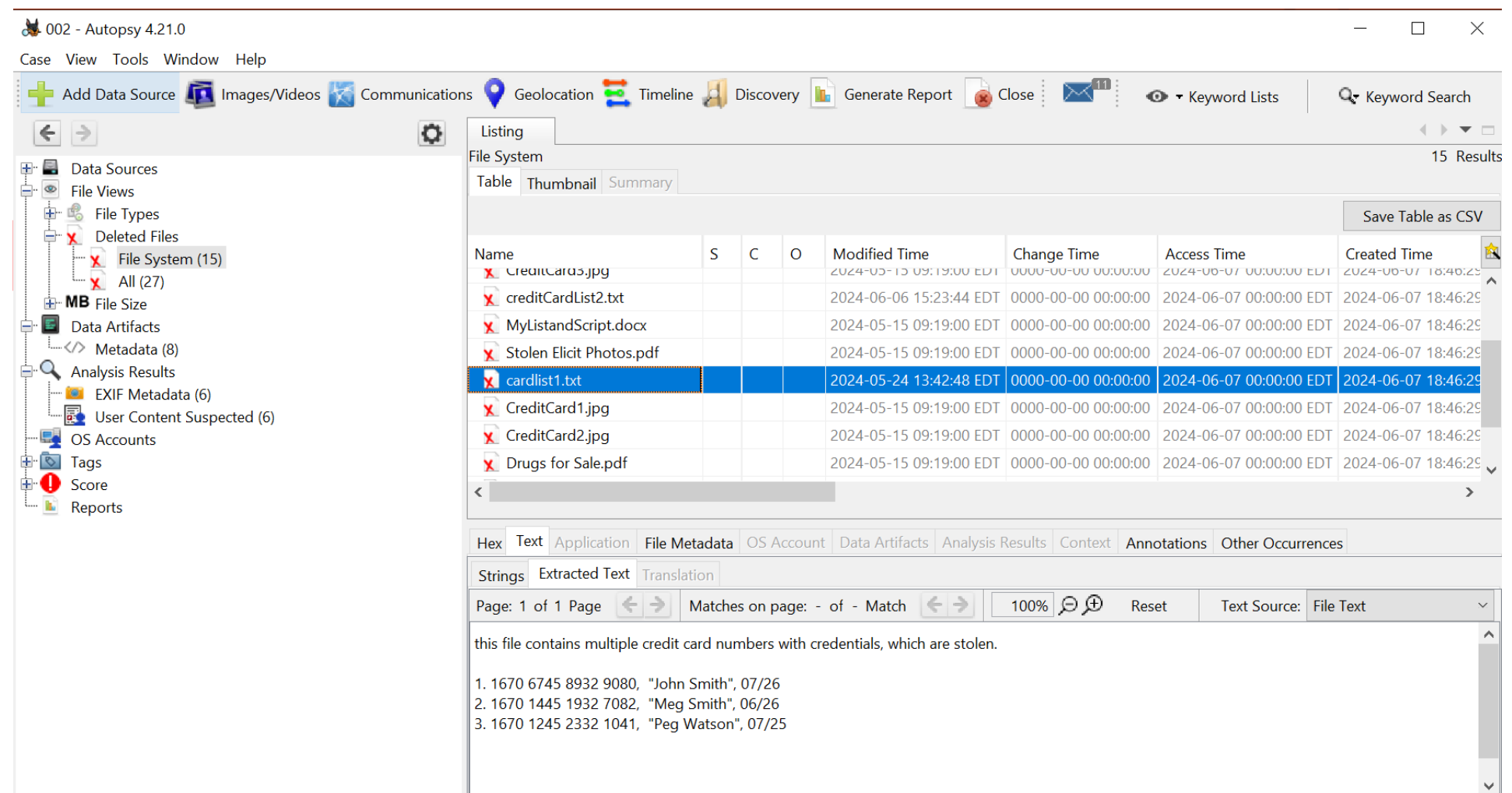
Proceed through the next step (contd.)

- Wait for the process to complete and click “Finish”



Lab 1.1 outcome

- Autopsy lists the recovered items under “Deleted Files” tab on the left column
 - Items listed under “File System” sub-tab are items recovered using metadata. We see all files and folder are listed there.
 - cardlist1.txt (highlighted on the right column) is one such recovered file. At the bottom of the right column, we see the real data of this file.



The screenshot shows the Autopsy 4.21.0 interface. On the left, the 'Deleted Files' tab is selected, showing a tree view with 'File System (15)' and 'All (27)'. The main pane displays a table of recovered files. The file 'cardlist1.txt' is highlighted in blue. Below the table, the 'Text' tab is selected, showing the extracted text of the file.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
creditCard1.jpg				2024-05-15 09:19:00 EDT	0000-00-00 00:00:00	2024-06-07 00:00:00 EDT	2024-06-07 18:46:29
creditCardList2.txt				2024-06-06 15:23:44 EDT	0000-00-00 00:00:00	2024-06-07 00:00:00 EDT	2024-06-07 18:46:29
MyListandScript.docx				2024-05-15 09:19:00 EDT	0000-00-00 00:00:00	2024-06-07 00:00:00 EDT	2024-06-07 18:46:29
Stolen Elicit Photos.pdf				2024-05-15 09:19:00 EDT	0000-00-00 00:00:00	2024-06-07 00:00:00 EDT	2024-06-07 18:46:29
cardlist1.txt				2024-05-24 13:42:48 EDT	0000-00-00 00:00:00	2024-06-07 00:00:00 EDT	2024-06-07 18:46:29
CreditCard1.jpg				2024-05-15 09:19:00 EDT	0000-00-00 00:00:00	2024-06-07 00:00:00 EDT	2024-06-07 18:46:29
CreditCard2.jpg				2024-05-15 09:19:00 EDT	0000-00-00 00:00:00	2024-06-07 00:00:00 EDT	2024-06-07 18:46:29
Drugs for Sale.pdf				2024-05-15 09:19:00 EDT	0000-00-00 00:00:00	2024-06-07 00:00:00 EDT	2024-06-07 18:46:29

Page: 1 of 1 Page Matches on page: - of - Match 100% Reset Text Source: File Text

this file contains multiple credit card numbers with credentials, which are stolen.

- 1670 6745 8932 9080, "John Smith", 07/26
- 1670 1445 1932 7082, "Meg Smith", 06/26
- 1670 1245 2332 1041, "Peg Watson", 07/25

Lab 1.1 outcome (contd.)

- cardlist1.txt is one such recovered file.
- On the right column at the bottom, we now see the **metadata** of this file
- The previous slide and this slide prove that the “deletion” operation neither erase the **metadata** nor the **real data** of cardlist1.txt

The screenshot displays the Autopsy 4.21.0 interface. The left sidebar shows the 'Data Sources' tree with 'File System (15)' selected. The main window shows a 'File System' listing of 15 results. The file 'cardlist1.txt' is highlighted in the listing table. Below the listing, the 'File Metadata' tab is active, showing details for 'cardlist1.txt'.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
creditCard1.jpg				2024-05-15 09:19:00 EDT	0000-00-00 00:00:00	2024-06-07 00:00:00 EDT	2024-06-07 18:46:29
creditCardList2.txt				2024-06-06 15:23:44 EDT	0000-00-00 00:00:00	2024-06-07 00:00:00 EDT	2024-06-07 18:46:29
MyListandScript.docx				2024-05-15 09:19:00 EDT	0000-00-00 00:00:00	2024-06-07 00:00:00 EDT	2024-06-07 18:46:29
Stolen Elicit Photos.pdf				2024-05-15 09:19:00 EDT	0000-00-00 00:00:00	2024-06-07 00:00:00 EDT	2024-06-07 18:46:29
cardlist1.txt				2024-05-24 13:42:48 EDT	0000-00-00 00:00:00	2024-06-07 00:00:00 EDT	2024-06-07 18:46:29
CreditCard1.jpg				2024-05-15 09:19:00 EDT	0000-00-00 00:00:00	2024-06-07 00:00:00 EDT	2024-06-07 18:46:29

Hex	Text	Application	File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences
Metadata									
Name:	/img_D/cardlist1.txt								
Type:	File System								
MIME Type:	text/plain								
Size:	226								
File Name Allocation:	Unallocated								
Metadata Allocation:	Unallocated								
Modified:	2024-05-24 13:42:48 EDT								
Accessed:	2024-06-07 00:00:00 EDT								
Created:	2024-06-07 18:46:29 EDT								

Lab 1.1 outcome (contd.)

- File **_ource.txt** is another recovered file.
- On the right column at the bottom, we see the metadata of this file. We observe that the first character of the original name (source.txt) is replaced by an underscore('_')
- However, we see the other part of the metadata (e.g., modification timestamp, and more) and the real data of the file are fully recovered.

The screenshot displays the Autopsy 4.21.0 interface. The left sidebar shows a tree view of data sources, with 'File System (15)' selected. The main pane shows a table of files in the file system. The file '_ource.txt' is highlighted. Below the table, the 'File Metadata' tab is active, showing details for the selected file.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
CreditCard1.jpg				2024-05-15 09:19:00 EDT	0000-00-00 00:00:00	2024-06-07 00:00:00 EDT	2024-06-07 18:46:29
CreditCard2.jpg				2024-05-15 09:19:00 EDT	0000-00-00 00:00:00	2024-06-07 00:00:00 EDT	2024-06-07 18:46:29
Drugs for Sale.pdf				2024-05-15 09:19:00 EDT	0000-00-00 00:00:00	2024-06-07 00:00:00 EDT	2024-06-07 18:46:29
FavWebsite.url				2024-05-15 09:19:00 EDT	0000-00-00 00:00:00	2024-06-07 00:00:00 EDT	2024-06-07 18:46:29
_ource.txt				2024-05-24 13:38:36 EDT	0000-00-00 00:00:00	2024-06-07 00:00:00 EDT	2024-06-07 18:46:29
Stolen Elicit Photos.docx				2024-05-15 09:19:00 EDT	0000-00-00 00:00:00	2024-06-07 00:00:00 EDT	2024-06-07 18:46:29

Metadata

Name:	/img_D:/_ource.txt
Type:	File System
MIME Type:	text/plain
Size:	78
File Name Allocation:	Unallocated
Metadata Allocation:	Unallocated
Modified:	2024-05-24 13:38:36 EDT
Accessed:	2024-06-07 00:00:00 EDT
Created:	2024-06-07 18:46:29 EDT

Lab 1.1 outcome (contd.)

- **CreditCard1.jpg** is one of the recovered files.
- On the right column at the bottom, we see the real data of this file.
- We also see that the metadata (e.g., modification timestamp, and more) of the file is fully recovered.

002 - Autopsy 4.21.0

Case View Tools Window Help







+ Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Keyword Lists Keyword Search

Listing

File System 15 Results

Table Thumbnail Summary

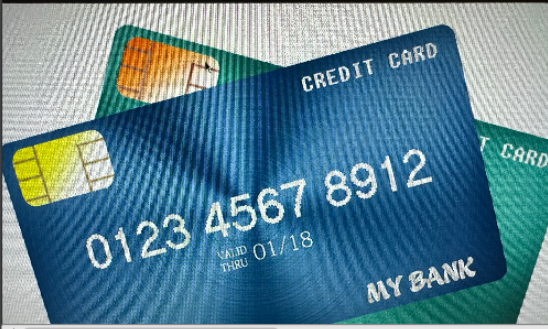
Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
 CreditCard1.jpg				2024-05-15 09:19:00 EDT	0000-00-00 00:00:00	2024-06-07 00:00:00 EDT	2024-06-07 18:46:29
 CreditCard2.jpg				2024-05-15 09:19:00 EDT	0000-00-00 00:00:00	2024-06-07 00:00:00 EDT	2024-06-07 18:46:29
 Drugs for Sale.pdf				2024-05-15 09:19:00 EDT	0000-00-00 00:00:00	2024-06-07 00:00:00 EDT	2024-06-07 18:46:29
 FavWebsite.url				2024-05-15 09:19:00 EDT	0000-00-00 00:00:00	2024-06-07 00:00:00 EDT	2024-06-07 18:46:29
 _ource.txt				2024-05-24 13:38:36 EDT	0000-00-00 00:00:00	2024-06-07 00:00:00 EDT	2024-06-07 18:46:29
 Stolen Flirt Photos.docx				2024-05-15 09:19:00 EDT	0000-00-00 00:00:00	2024-06-07 00:00:00 EDT	2024-06-07 18:46:29

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

0° 8% Reset

Tags Menu



Summary of our findings in Lab 1.1

- Autopsy uses both mechanisms (metadata-based recovery and file carving) to recover deleted files.
- Therefore, we get two copies of the deleted files, except the text files on which file carving doesn't work.

Lab 1.2

- The suspect did a “quick format” of the thumb drive
- Can we recover the files and folders?

Setting up the lab: The instructor prepares the thumb drive

- “format” the thumb drive
 - It should be *full format*, so do not check the “quick format” option
- The lab has a *resource* folder that contains a few artifacts
 - Copy the content of *collection1* to the the thumb drive
 - Note that we do not copy the *collection1* folder, but copy only what is inside
- Now do a “quick format” of the thumb drive
- The thumb drive is ready now
- Let’s start the Autopsy tool

Lab 1.2 outcome

- Autopsy lists the recovered items under “**Deleted Files**” tab on the left column
- Overall, a smaller number of files are recovered compared to Lab 1.1
 - Items listed under “File System” sub-tab are items recovered using **metadata**. This only includes files which were in folder1 but not the files which were in the root folder
 - CreditCardlist2.txt is one such recovered file. On the right column at the bottom, we see that this filename was only partially recovered.

The screenshot displays the Autopsy 4.21.0 interface. On the left, the 'Deleted Files' tab is selected, showing a tree view with 'File System (4)' and 'All (16)'. The main pane shows a table of recovered files. Below the table, the 'File Metadata' tab is selected, displaying detailed information for the file 'CREDIT~1.TXT'.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
CREDIT~1.JPG				2024-05-15 09:19:00 EDT	0000-00-00 00:00:00	2024-06-07 00:00:00 EDT	2024-06-07 18:34:28 EDT	710472
CREDIT~1.TXT				2024-06-06 15:23:44 EDT	0000-00-00 00:00:00	2024-06-07 00:00:00 EDT	2024-06-07 18:34:28 EDT	226
MYLIST~1.DOC				2024-05-15 09:19:00 EDT	0000-00-00 00:00:00	2024-06-07 00:00:00 EDT	2024-06-07 18:34:28 EDT	22493
STOLEN~1.PDF				2024-05-15 09:19:00 EDT	0000-00-00 00:00:00	2024-06-07 00:00:00 EDT	2024-06-07 18:34:28 EDT	261728

Metadata

Name: /img_D/\$OrphanFiles/CREDIT~1.TXT
Type: File System
MIME Type: text/plain
Size: 226
File Name Allocation: Unallocated
Metadata Allocation: Unallocated
Modified: 2024-06-06 15:23:44 EDT
Accessed: 2024-06-07 00:00:00 EDT
Created: 2024-06-07 18:34:28 EDT
Changed: 0000-00-00 00:00:00
MD5: Not calculated
SHA-256: Not calculated

Lab 1.2 outcome (contd.)

- Items listed under “All” sub-tab include items recovered using **file carving**.
- The text files (e.g., source.txt) in the root folder are not recovered. However, pdf files, docx files, jpg files in root folder or folder1 are recovered.
- f0015184.pdf is one such recovered file. On the right column at the bottom, we see that the metadata of the file is not recovered. Even the original filename is erased, and Autopsy assigns a new name.

The screenshot displays the Autopsy 4.21.0 interface. The left sidebar shows a tree view of data sources, including 'Deleted Files' and 'All (16)'. The main window is divided into two panes. The top pane, titled 'Listing', shows a table of recovered files. The bottom pane, titled 'Metadata', shows the details for the selected file, f0015184.pdf.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
f0015136.docx			6	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	224
f0015184.pdf			6	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	261
f0026952.jpg			5	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	811
f0015704.jpg			5	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	552

Metadata

Name: /img_D:/CarvedFiles/1/f0015184.pdf
Type: Carved
MIME Type: application/pdf
Size: 261728
File Name Allocation: Unallocated
Metadata Allocation: Unallocated
Modified: 0000-00-00 00:00:00
Accessed: 0000-00-00 00:00:00
Created: 0000-00-00 00:00:00
Changed: 0000-00-00 00:00:00

Lab 1.2 outcome (contd.)

- However, the real data of the pdf file is fully recovered as we see at the bottom on the right column.

001 - Autopsy 4.21.0

Case View Tools Window Help

+ Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Keyword Lists Keyword Search


Listing All 16 Results

Table Thumbnail Summary Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
f0015136.docx			6	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	224
f0015184.pdf			6	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	261
f0026952.jpg			5	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	811
f0015704.jpg			5	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	552

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

1 of 3 100%



Summary of our findings in Lab 1.2

- Since *quick formatting* removes the content of the root directory's metadata (while metadata for the subfolders aren't affected), only file carving could work for the files in the root directory.
- File Carving uses file signatures (special identifiers for a file type which are stored alongside the data). Since .txt does not have a signature, file carving doesn't recover .txt files in the root folder.

References

- The following book is considered as the authority of file recovery
 - File System Forensic Analysis by Brian Carrier
- If you need help on how to install Autopsy on a Windows computer, check out youtube tutorials
 - As an example, <https://www.youtube.com/watch?v=h23fGpCk76A>

Happy Learning

THANK YOU!