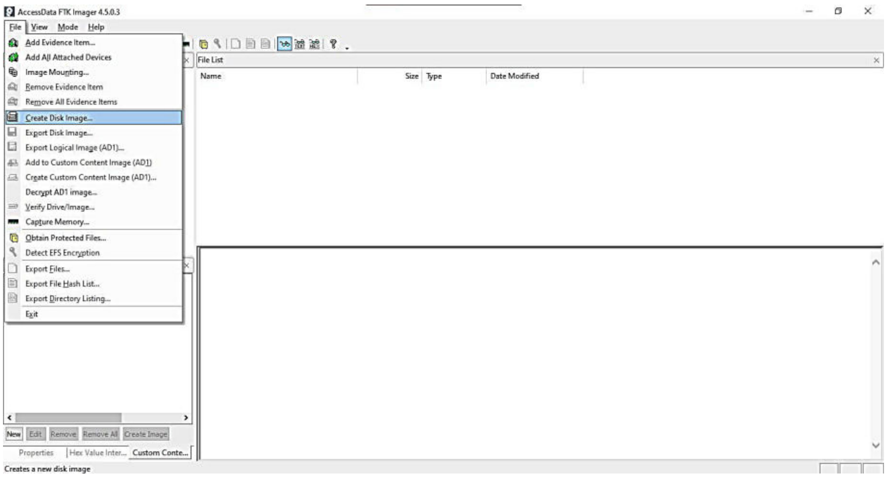
PRACTICAL NO: 07

Aim: Recovering and Inspecting deleted files

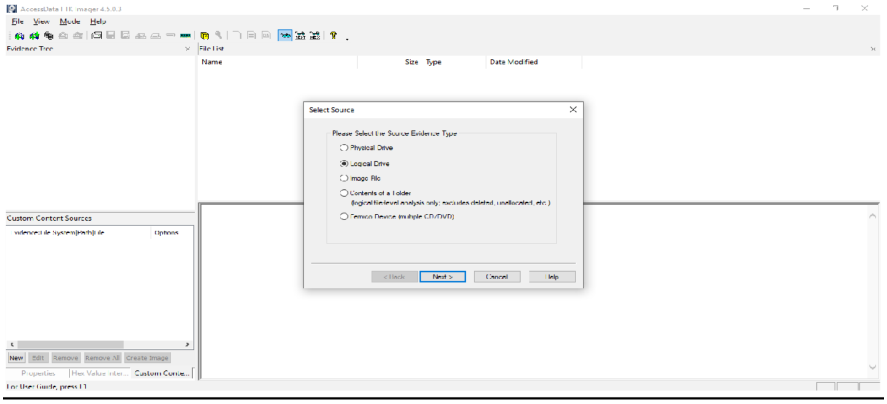
- Check for Deleted Files
- Recover the Deleted Files
- Analysing and Inspecting the recovered file0073

CREATING DISK IMAGE FILE:

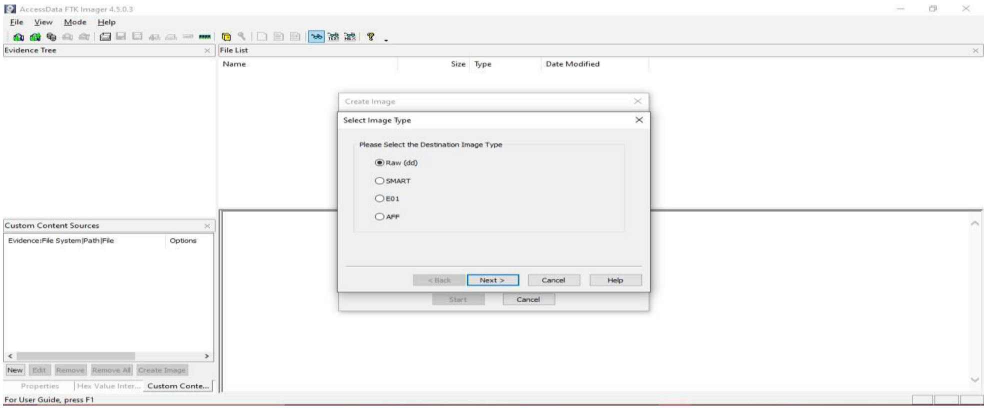
Step 1: Open AccessData FTK Imager, Click File, and then Create Disk Image.


AccessData FTK Imager 4.5.0.3
File View Mode Help
Add Evidence Item...
Add All Attached Devices
Image Mounting...
Remove Evidence Item
Remove All Evidence Items
Create Disk Image...
Export Disk Image...
Export Logical Image (AD1)...
Add to Custom Content Image (AD1)
Create Custom Content Image (AD1)...
Decrypt AD1 image...
Verify Drive/Image...
Capture Memory...
Obtain Protected Files...
Detect EFS Encryption
Export Files...
Export File Hash List...
Export Directory Listing...
Exit
File List
Name Size Type Date Modified
New Edit Remove Remove All Create Image
Properties Hex Value Inter... Custom Conte...
Creates a new disk image

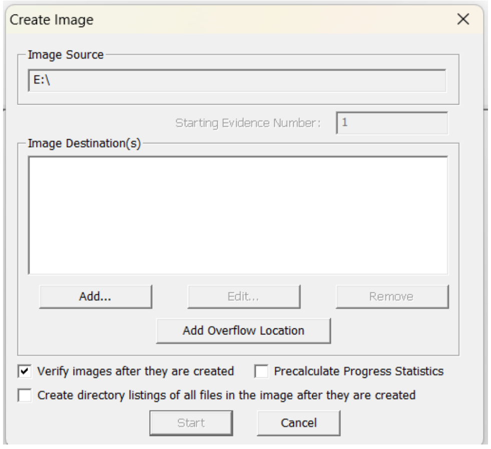
Step 2: Select the source evidence type you want to make an image of and click Next.


Select Source
Please Select the Source Evidence Type
○ Physical Drive
● Logical Drive
○ Image File
○ Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)
○ Femico Device (multiple CD/DVD)
< Back Next > Cancel Help
Custom Content Sources
Evidence:File System|Path|File Options
For User Guide, press F1

Step3: Select the source evidence drive with path.


AccessData FTK Imager 4.5.0.3
File View Mode Help
Evidence Tree
File List
Name Size Type Date Modified
Create Image
Select Image Type
Please Select the Destination Image Type
● Raw (dd)
○ SMART
○ E01
○ AFF
< Back Next > Cancel Help
Start Cancel
Custom Content Sources
Evidence:File System|Path|File Options
For User Guide, press F1

Click on “add” to add image destination



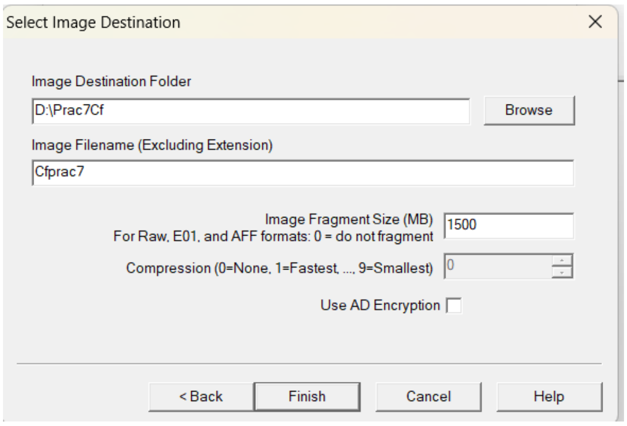
Create Image

Image Source: E:\

Starting Evidence Number: 1

Image Destination(s)

☑ Verify images after they are created
□ Precalculate Progress Statistics
□ Create directory listings of all files in the image after they are created



Select Image Destination

Image Destination Folder: D:\Prac7Cf

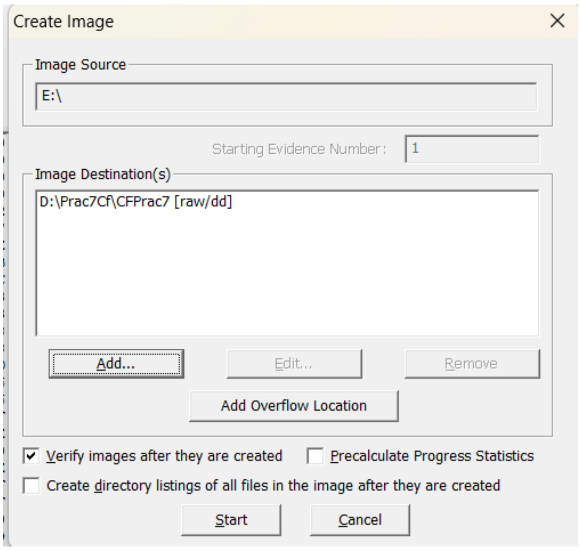
Image Filename (Excluding Extension): Cfprac7

Image Fragment Size (MB) For Raw, E01, and AFF formats: 0 = do not fragment: 1500

Compression (0=None, 1=Fastest, ..., 9=Smallest): 0

Use AD Encryption □

Step4: In the Image Destination Folder field, type the location path where you want to save the image file, or click Browse to find to the desired location.



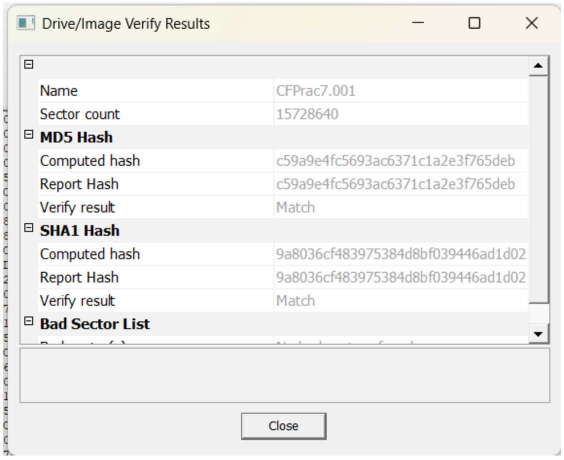
Create Image

Image Source: E:\

Starting Evidence Number: 1

Image Destination(s): D:\Prac7Cf\CFPrac7 [raw/dd]

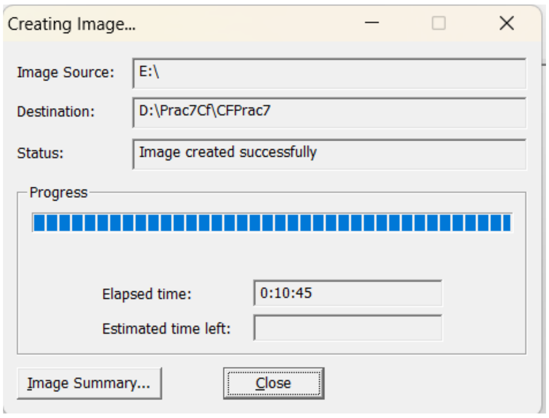
☑ Verify images after they are created
□ Precalculate Progress Statistics
□ Create directory listings of all files in the image after they are created



Drive/Image Verify Results

Name	CFPrac7.001
Sector count	15728640
MD5 Hash	
Computed hash	c59a9e4fc5693ac6371c1a2e3f765deb
Report Hash	c59a9e4fc5693ac6371c1a2e3f765deb
Verify result	Match
SHA1 Hash	
Computed hash	9a8036cf483975384d8bf039446ad1d02
Report Hash	9a8036cf483975384d8bf039446ad1d02
Verify result	Match
Bad Sector List	

Step 5: After adding the image destination path click on finish and start the image processing. The images are successfully created



Creating Image...

Image Source: E:\

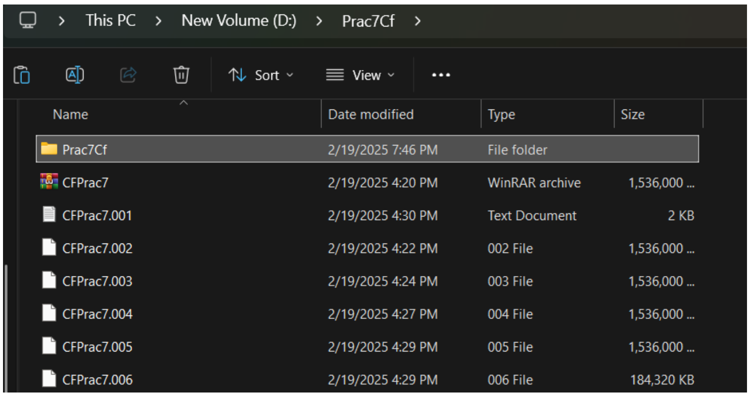
Destination: D:\Prac7Cf\CFPrac7

Status: Image created successfully

Progress

Elapsed time: 0:10:45

Estimated time left:

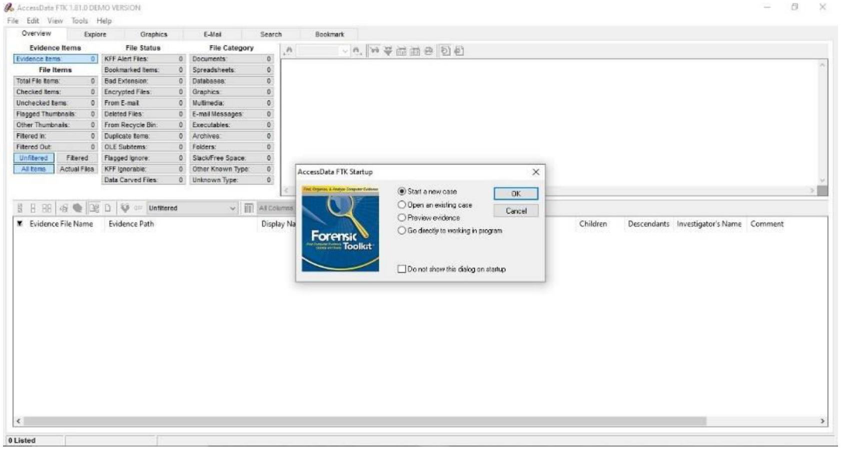


This PC > New Volume (D:) > Prac7Cf >

Name	Date modified	Type	Size
Prac7Cf	2/19/2025 7:46 PM	File folder	
CFPrac7	2/19/2025 4:20 PM	WinRAR archive	1,536,000 ...
CFPrac7.001	2/19/2025 4:30 PM	Text Document	2 KB
CFPrac7.002	2/19/2025 4:22 PM	002 File	1,536,000 ...
CFPrac7.003	2/19/2025 4:24 PM	003 File	1,536,000 ...
CFPrac7.004	2/19/2025 4:27 PM	004 File	1,536,000 ...
CFPrac7.005	2/19/2025 4:29 PM	005 File	1,536,000 ...
CFPrac7.006	2/19/2025 4:29 PM	006 File	184,320 KB

RECOVERING THE DELETED FILES:

Step 1: Open Forensic Toolkit and click on "Start a new case".

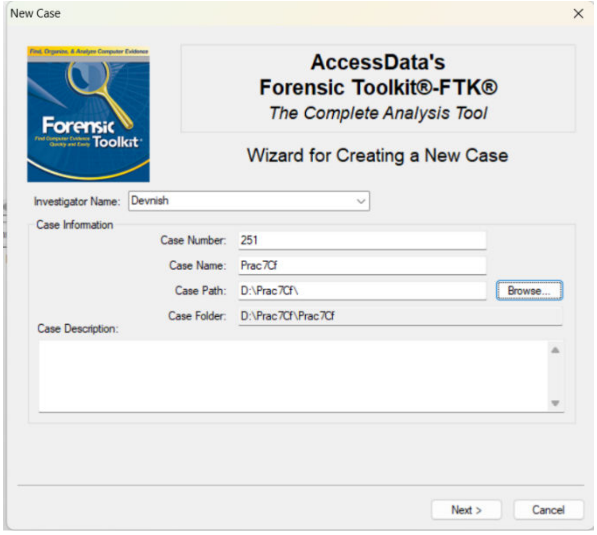


AccessData FTK Startup

● Start a new case
○ Open an existing case
○ Preview evidence
○ Go directly to working in program

□ Do not show this dialog on startup

Step 2: Fill the following details and click next.



New Case

AccessData's Forensic Toolkit®-FTK®
The Complete Analysis Tool

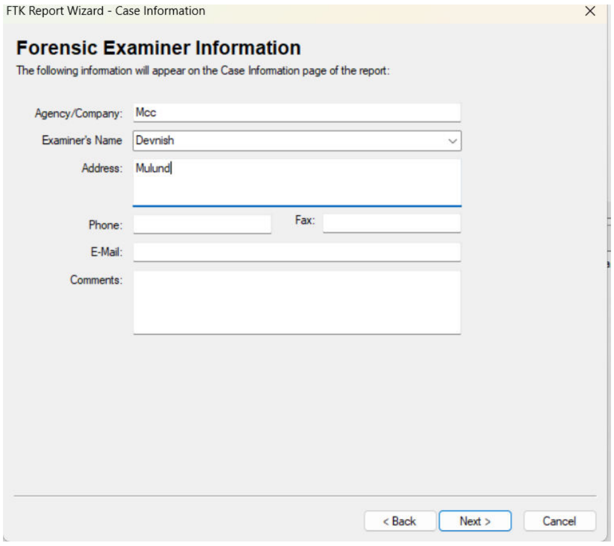
Wizard for Creating a New Case

Investigator Name: Devnish

Case Information

Case Number: 251
Case Name: Prac7Cf
Case Path: D:\Prac7Cf\
Case Folder: D:\Prac7Cf\Prac7Cf

Case Description:



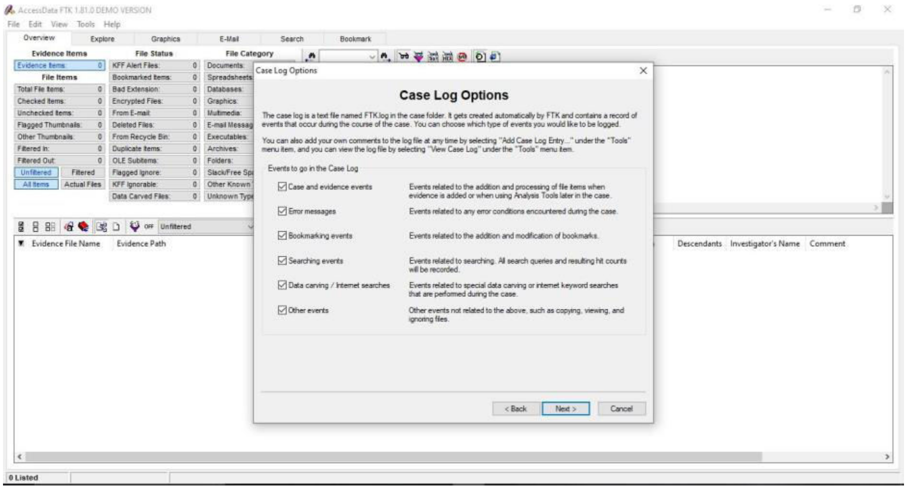
FTK Report Wizard - Case Information

Forensic Examiner Information

The following information will appear on the Case Information page of the report:

Agency/Company: Mcc
Examiner's Name: Devnish
Address: Mulund
Phone:
Fax:
E-Mail:
Comments:

Step 3: Click next.



Case Log Options

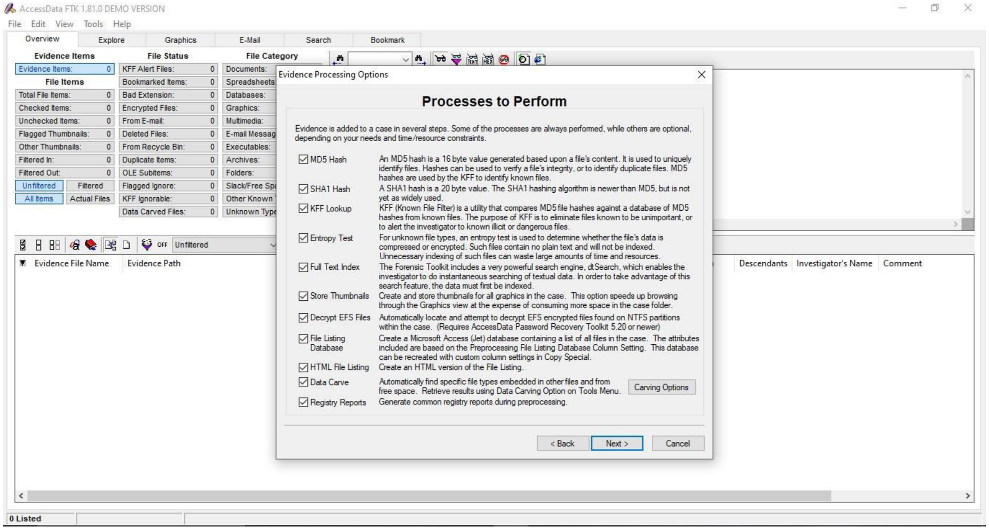
The case log is a text file named FTK.log in the case folder. It gets created automatically by FTK and contains a record of events that occur during the course of the case. You can choose which type of events you would like to be logged.

You can also add your own comments to the log file at any time by selecting "Add Case Log Entry..." under the "Tools" menu item, and you can view the log file by selecting "View Case Log" under the "Tools" menu item.

Events to go in the Case Log

☑ Case and evidence events — Events related to the addition and processing of file items when evidence is added or when using Analysis Tools later in the case.
☑ Error messages — Events related to any error conditions encountered during the case.
☑ Bookmarking events — Events related to the addition and modification of bookmarks.
☑ Searching events — Events related to searching. All search queries and resulting hit counts will be recorded.
☑ Data carving / Internet searches — Events related to special data carving or internet keyword searches that are performed during the case.
☑ Other events — Other events not related to the above, such as copying, viewing, and ignoring files.

Step 4: Click next.



Evidence Processing Options

Processes to Perform

Evidence is added to a case in several steps. Some of the processes are always perfomed, while others are optional, depending on your needs and time/resource constraints.

☑ MD5 Hash — An MD5 hash is a 16 byte value generated based upon a file's content. It is used to uniquely identify files. Hashes can be used to verify a file's integrity, or to identify duplicate files. MD5 hashes are used by the KFF to identify known files.

☑ SHA1 Hash — A SHA1 hash is a 20 byte value. The SHA1 hashing algorithm is newer than MD5, but is not yet as widely used.

☑ KFF Lookup — KFF (Known File Filter) is a utility that compares MD5 file hashes against a database of MD5 hashes from known files. The purpose of KFF is to eliminate files known to be unimportant, or to alert the investigator to known illicit or dangerous files.

☑ Entropy Test — For unknown file types, an entropy test is used to determine whether the file's data is compressed or encrypted. Such files contain no plain text and will not be indexed. Unnecessary indexing of such files can waste large amounts of time and resources.

☑ Full Text Index — The Forensic Toolkit includes a very powerful search engine, dtSearch, which enables the investigator to do instantaneous searching of textual data. In order to take advantage of this search feature, the data must first be indexed.

☑ Store Thumbnails — Create and store thumbnails for all graphics in the case. This option speeds up browsing through the Graphics view at the expense of consuming more space in the case folder.

☑ Decrypt EFS Files — Automatically locate and attempt to decrypt EFS encrypted files found on NTFS partitions within the case. (Requires AccessData Password Recovery Toolkit 5.20 or newer)

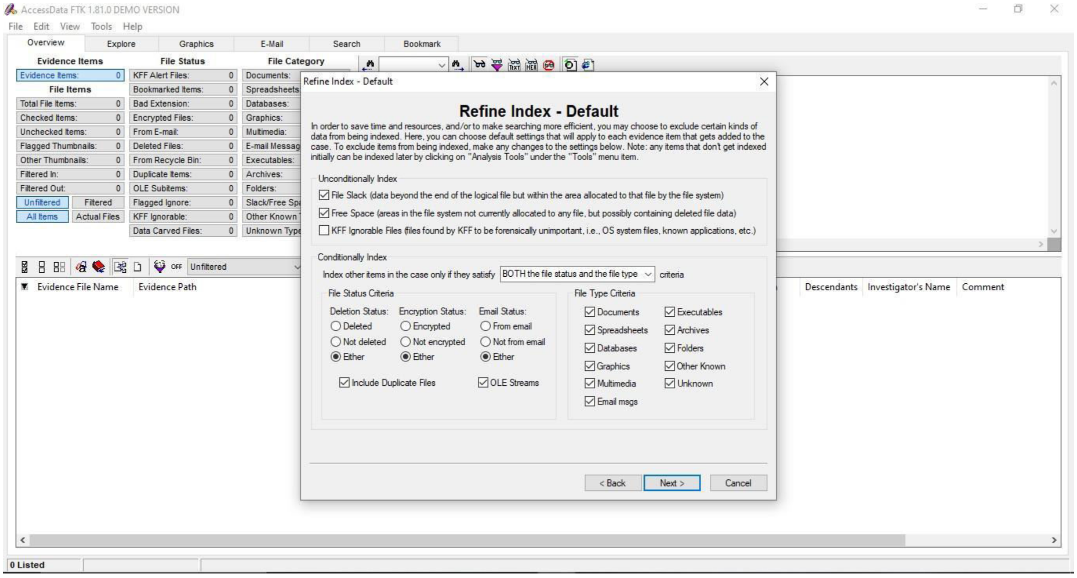
☑ File Listing Database — Create a Microsoft Access (Jet) database containing a list of all files in the case. The attributes included are based on the Preprocessing File Listing Database Column Setting. This database can be recreated with custom column settings in Copy Special.

☑ HTML File Listing — Create an HTML version of the File Listing.

☑ Data Carve — Automatically find specific file types embedded in other files and from free space. Retrieve results using Data Carving Option on Tools Menu.

☑ Registry Reports — Generate common registry reports during preprocessing.

Step 6: Click Next.



Refine Index - Default

In order to save time and resources, and/or to make searching more efficient, you may choose to exclude certain kinds of data from being indexed. Here, you can choose default settings that will apply to each evidence item that gets added to the case. To exclude items from being indexed, make any changes to the settings below. Note: any items that don't get indexed initially can be indexed later by clicking on "Analysis Tools" under the "Tools" menu item.

Unconditionally Index

☑ File Slack (data beyond the end of the logical file but within the area allocated to that file by the file system)

☑ Free Space (areas in the file system not currently allocated to any file, but possibly containing deleted file data)

☐ KFF Ignorable Files (files found by KFF to be forensically unimportant, i.e., OS system files, known applications, etc.)

Conditionally Index

Index other items in the case only if they satisfy BOTH the file status and the file type criteria

File Status Criteria

Deletion Status: ○ Deleted ○ Not deleted ● Either

Encryption Status: ○ Encrypted ○ Not encrypted ● Either

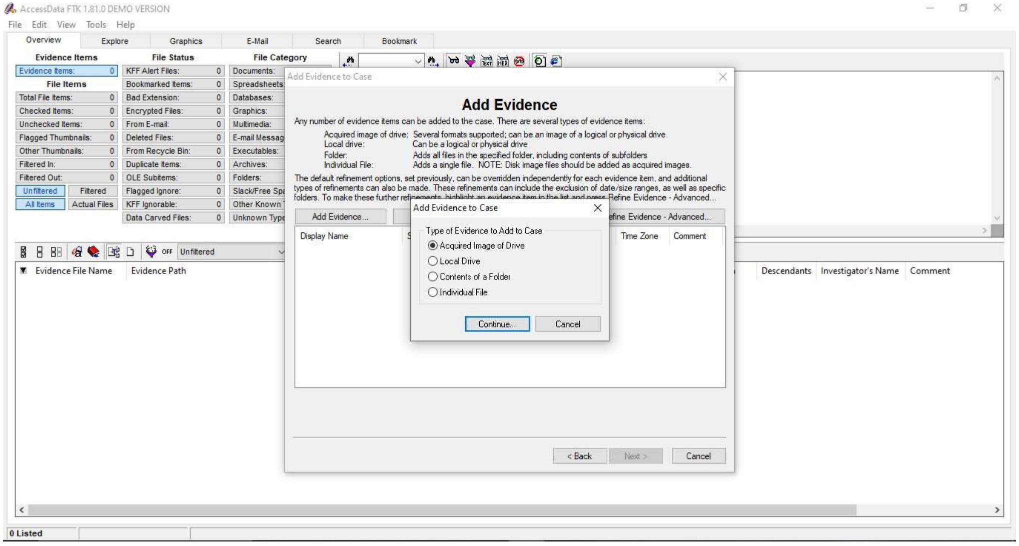
Email Status: ○ From email ○ Not from email ● Either

☑ Include Duplicate Files ☑ OLE Streams

File Type Criteria

☑ Documents ☑ Executables ☑ Spreadsheets ☑ Archives ☑ Databases ☑ Folders ☑ Graphics ☑ Other Known ☑ Multimedia ☑ Unknown ☑ Email msgs

Step 7: Add evidence, and select Acquired Image of Drive.



Add Evidence to Case

Add Evidence

Any number of evidence items can be added to the case. There are several types of evidence items:

Acquired image of drive: Several formats supported; can be an image of a logical or physical drive
Local drive: Can be a logical or physical drive
Folder: Adds all files in the specified folder, including contents of subfolders
Individual File: Adds a single file. NOTE: Disk image files should be added as acquired images.

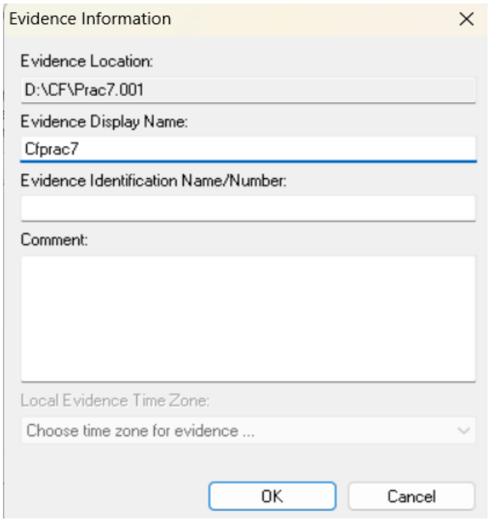
The default refinement options, set previously, can be overridden independently for each evidence item, and additional types of refinements can also be made. These refinements can include the exclusion of date/size ranges, as well as specific folders. To make these further refinements, highlight an evidence item in the list and press Refine Evidence - Advanced...

Add Evidence to Case

Type of Evidence to Add to Case

● Acquired Image of Drive
○ Local Drive
○ Contents of a Folder
○ Individual File

Step 8: Fill the following and click OK.



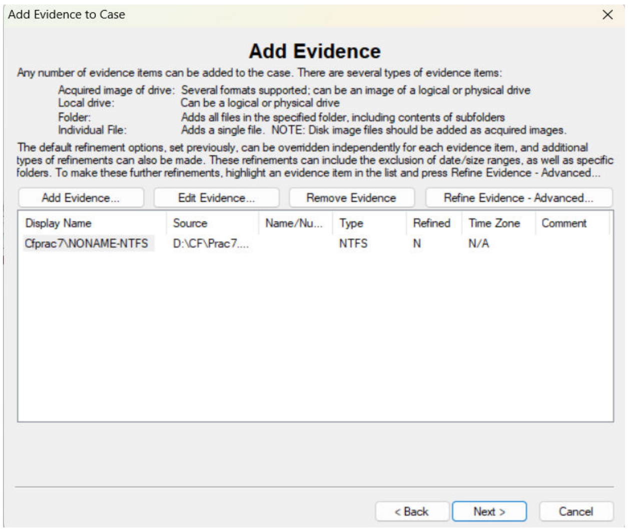
Evidence Location: D:\CF\Prac7.001

Evidence Display Name: Cfprac7

Evidence Identification Name/Number:

Comment:

Local Evidence Time Zone: Choose time zone for evidence ...



Add Evidence

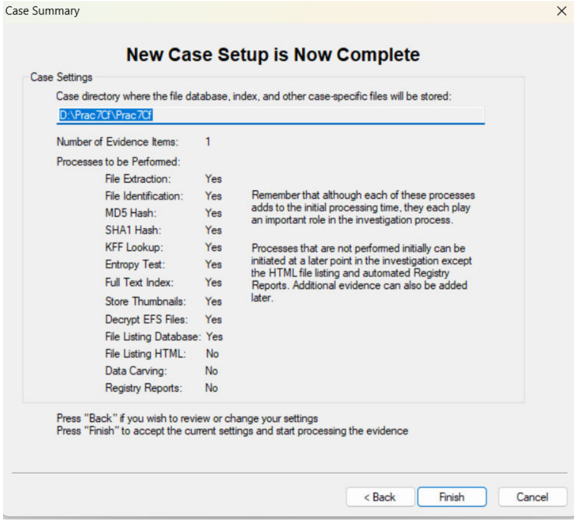
Any number of evidence items can be added to the case. There are several types of evidence items:

Acquired image of drive:	Several formats supported; can be an image of a logical or physical drive
Local drive:	Can be a logical or physical drive
Folder:	Adds all files in the specified folder, including contents of subfolders
Individual File:	Adds a single file. NOTE: Disk image files should be added as acquired images.

The default refinement options, set previously, can be overridden independently for each evidence item, and additional types of refinements can also be made. These refinements can include the exclusion of date/size ranges, as well as specific folders. To make these further refinements, highlight an evidence item in the list and press Refine Evidence - Advanced...

Display Name	Source	Name/Nu...	Type	Refined	Time Zone	Comment
Cfprac7\NONAME-NTFS	D:\CF\Prac7....		NTFS	N	N/A	

Step 9: Click finish.



New Case Setup is Now Complete

Case Settings

Case directory where the file database, index, and other case-specific files will be stored:

D:\Prac7Cf\Prac7Cf

Number of Evidence Items: 1

Processes to be Performed:

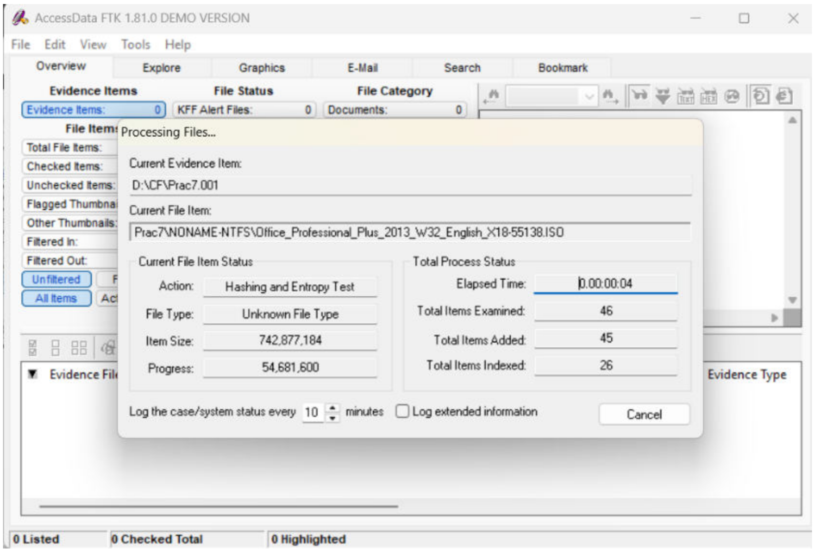
File Extraction:	Yes
File Identification:	Yes
MD5 Hash:	Yes
SHA1 Hash:	Yes
KFF Lookup:	Yes
Entropy Test:	Yes
Full Text Index:	Yes
Store Thumbnails:	Yes
Decrypt EFS Files:	Yes
File Listing Database:	Yes
File Listing HTML:	No
Data Carving:	No
Registry Reports:	No

Remember that although each of these processes adds to the initial processing time, they each play an important role in the investigation process.

Processes that are not performed initially can be initiated at a later point in the investigation except the HTML file listing and automated Registry Reports. Additional evidence can also be added later.

Press "Back" if you wish to review or change your settings
Press "Finish" to accept the current settings and start processing the evidence

Let the process complete.



Processing Files...

Current Evidence Item: D:\CF\Prac7.001

Current File Item: Prac7\NONAME-NTFS\Office_Professional_Plus_2013_W32_English_X18-55138.ISO

Current File Item Status

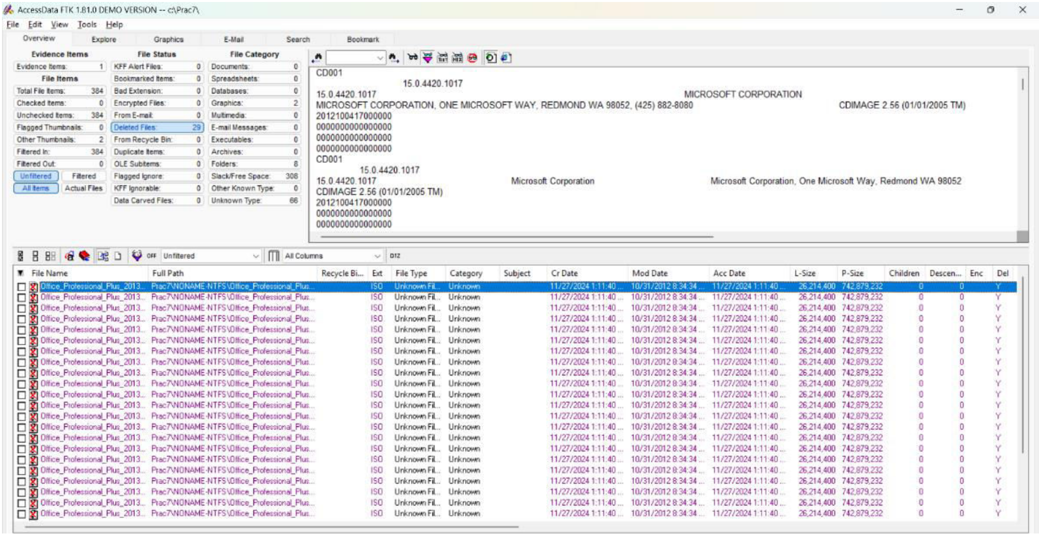
Action:	Hashing and Entropy Test
File Type:	Unknown File Type
Item Size:	742,877,184
Progress:	54,681,600

Total Process Status

Elapsed Time:	0:00:00:04
Total Items Examined:	46
Total Items Added:	45
Total Items Indexed:	26

Log the case/system status every 10 minutes □ Log extended information

Step 10: Find deleted files.



AccessData FTK 1.81.0 DEMO VERSION -- c:\Prac7\

File Edit View Tools Help
Overview Explore Graphics E-Mail Search Bookmark

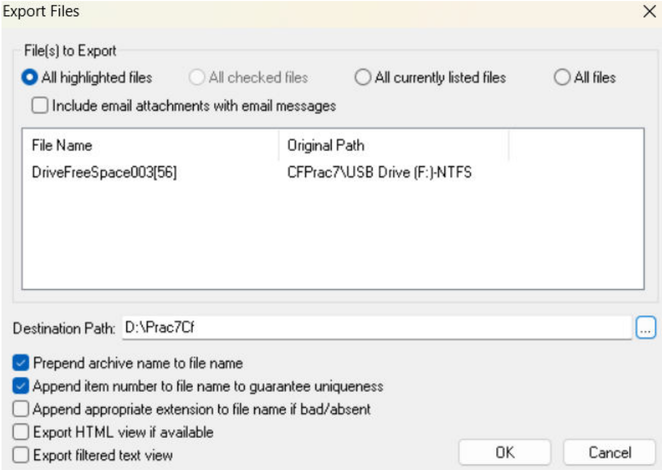
Evidence Items		File Status		File Category	
Evidence Items:	1	KFF Alert Files:	0	Documents:	0
File Items		Bookmarked Items:	0	Spreadsheets:	0
Total File Items:	384	Bad Extension:	0	Databases:	0
Checked Items:	0	Encrypted Files:	0	Graphics:	2
Unchecked Items:	384	From E-mail:	0	Multimedia:	0
Flagged Thumbnails:	0	Deleted Files:	29	E-mail Messages:	0
Other Thumbnails:	2	From Recycle Bin:	0	Executables:	0
Filtered In:	384	Duplicate Items:	0	Archives:	0
Filtered Out:	0	OLE Subitems:	0	Folders:	8
Unfiltered	Filtered	Flagged Ignore:	0	Slack/Free Space:	308
All Items	Actual Files	KFF Ignorable:	0	Other Known Type:	0
		Data Carved Files:	0	Unknown Type:	66

```
CD001
                15.0.4420.1017
15.0.4420.1017                                                  MICROSOFT CORPORATION
MICROSOFT CORPORATION, ONE MICROSOFT WAY, REDMOND WA 98052, (425) 882-8080          CDIMAGE 2.56 (01/01/2005 TM)
2012100417000000
0000000000000000
0000000000000000
0000000000000000
CD001
            15.0.4420.1017
15.0.4420.1017                    Microsoft Corporation                 Microsoft Corporation, One Microsoft Way, Redmond WA 98052
CDIMAGE 2.56 (01/01/2005 TM)
2012100417000000
0000000000000000
0000000000000000
```

File Name	Full Path	Recycle Bi...	Ext	File Type	Category	Subject	Cr Date	Mod Date	Acc Date	L-Size	P-Size	Children	Descen...	Enc	Del
Office_Professional_Plus_2013...	Prac7\NONAME-NTFS\Office_Professional_Plus...		ISO	Unknown Fil...	Unknown		11/27/2024 1:11:40 ...	10/31/2012 8:34:34 ...	11/27/2024 1:11:40 ...	26,214,400	742,879,232	0	0		Y
Office_Professional_Plus_2013...	Prac7\NONAME-NTFS\Office_Professional_Plus...		ISO	Unknown Fil...	Unknown		11/27/2024 1:11:40 ...	10/31/2012 8:34:34 ...	11/27/2024 1:11:40 ...	26,214,400	742,879,232	0	0		Y
Office_Professional_Plus_2013...	Prac7\NONAME-NTFS\Office_Professional_Plus...		ISO	Unknown Fil...	Unknown		11/27/2024 1:11:40 ...	10/31/2012 8:34:34 ...	11/27/2024 1:11:40 ...	26,214,400	742,879,232	0	0		Y
Office_Professional_Plus_2013...	Prac7\NONAME-NTFS\Office_Professional_Plus...		ISO	Unknown Fil...	Unknown		11/27/2024 1:11:40 ...	10/31/2012 8:34:34 ...	11/27/2024 1:11:40 ...	26,214,400	742,879,232	0	0		Y
Office_Professional_Plus_2013...	Prac7\NONAME-NTFS\Office_Professional_Plus...		ISO	Unknown Fil...	Unknown		11/27/2024 1:11:40 ...	10/31/2012 8:34:34 ...	11/27/2024 1:11:40 ...	26,214,400	742,879,232	0	0		Y
Office_Professional_Plus_2013...	Prac7\NONAME-NTFS\Office_Professional_Plus...		ISO	Unknown Fil...	Unknown		11/27/2024 1:11:40 ...	10/31/2012 8:34:34 ...	11/27/2024 1:11:40 ...	26,214,400	742,879,232	0	0		Y
Office_Professional_Plus_2013...	Prac7\NONAME-NTFS\Office_Professional_Plus...		ISO	Unknown Fil...	Unknown		11/27/2024 1:11:40 ...	10/31/2012 8:34:34 ...	11/27/2024 1:11:40 ...	26,214,400	742,879,232	0	0		Y
Office_Professional_Plus_2013...	Prac7\NONAME-NTFS\Office_Professional_Plus...		ISO	Unknown Fil...	Unknown		11/27/2024 1:11:40 ...	10/31/2012 8:34:34 ...	11/27/2024 1:11:40 ...	26,214,400	742,879,232	0	0		Y
Office_Professional_Plus_2013...	Prac7\NONAME-NTFS\Office_Professional_Plus...		ISO	Unknown Fil...	Unknown		11/27/2024 1:11:40 ...	10/31/2012 8:34:34 ...	11/27/2024 1:11:40 ...	26,214,400	742,879,232	0	0		Y
Office_Professional_Plus_2013...	Prac7\NONAME-NTFS\Office_Professional_Plus...		ISO	Unknown Fil...	Unknown		11/27/2024 1:11:40 ...	10/31/2012 8:34:34 ...	11/27/2024 1:11:40 ...	26,214,400	742,879,232	0	0		Y
Office_Professional_Plus_2013...	Prac7\NONAME-NTFS\Office_Professional_Plus...		ISO	Unknown Fil...	Unknown		11/27/2024 1:11:40 ...	10/31/2012 8:34:34 ...	11/27/2024 1:11:40 ...	26,214,400	742,879,232	0	0		Y
Office_Professional_Plus_2013...	Prac7\NONAME-NTFS\Office_Professional_Plus...		ISO	Unknown Fil...	Unknown		11/27/2024 1:11:40 ...	10/31/2012 8:34:34 ...	11/27/2024 1:11:40 ...	26,214,400	742,879,232	0	0		Y
Office_Professional_Plus_2013...	Prac7\NONAME-NTFS\Office_Professional_Plus...		ISO	Unknown Fil...	Unknown		11/27/2024 1:11:40 ...	10/31/2012 8:34:34 ...	11/27/2024 1:11:40 ...	26,214,400	742,879,232	0	0		Y
Office_Professional_Plus_2013...	Prac7\NONAME-NTFS\Office_Professional_Plus...		ISO	Unknown Fil...	Unknown		11/27/2024 1:11:40 ...	10/31/2012 8:34:34 ...	11/27/2024 1:11:40 ...	26,214,400	742,879,232	0	0		Y
Office_Professional_Plus_2013...	Prac7\NONAME-NTFS\Office_Professional_Plus...		ISO	Unknown Fil...	Unknown		11/27/2024 1:11:40 ...	10/31/2012 8:34:34 ...	11/27/2024 1:11:40 ...	26,214,400	742,879,232	0	0		Y
Office_Professional_Plus_2013...	Prac7\NONAME-NTFS\Office_Professional_Plus...		ISO	Unknown Fil...	Unknown		11/27/2024 1:11:40 ...	10/31/2012 8:34:34 ...	11/27/2024 1:11:40 ...	26,214,400	742,879,232	0	0		Y
Office_Professional_Plus_2013...	Prac7\NONAME-NTFS\Office_Professional_Plus...		ISO	Unknown Fil...	Unknown		11/27/2024 1:11:40 ...	10/31/2012 8:34:34 ...	11/27/2024 1:11:40 ...	26,214,400	742,879,232	0	0		Y
Office_Professional_Plus_2013...	Prac7\NONAME-NTFS\Office_Professional_Plus...		ISO	Unknown Fil...	Unknown		11/27/2024 1:11:40 ...	10/31/2012 8:34:34 ...	11/27/2024 1:11:40 ...	26,214,400	742,879,232	0	0		Y
Office_Professional_Plus_2013...	Prac7\NONAME-NTFS\Office_Professional_Plus...		ISO	Unknown Fil...	Unknown		11/27/2024 1:11:40 ...	10/31/2012 8:34:34 ...	11/27/2024 1:11:40 ...	26,214,400	742,879,232	0	0		Y
Office_Professional_Plus_2013...	Prac7\NONAME-NTFS\Office_Professional_Plus...		ISO	Unknown Fil...	Unknown		11/27/2024 1:11:40 ...	10/31/2012 8:34:34 ...	11/27/2024 1:11:40 ...	26,214,400	742,879,232	0	0		Y
Office_Professional_Plus_2013...	Prac7\NONAME-NTFS\Office_Professional_Plus...		ISO	Unknown Fil...	Unknown		11/27/2024 1:11:40 ...	10/31/2012 8:34:34 ...	11/27/2024 1:11:40 ...	26,214,400	742,879,232	0	0		Y
Office_Professional_Plus_2013...	Prac7\NONAME-NTFS\Office_Professional_Plus...		ISO	Unknown Fil...	Unknown		11/27/2024 1:11:40 ...	10/31/2012 8:34:34 ...	11/27/2024 1:11:40 ...	26,214,400	742,879,232	0	0		Y

Step 11: Extract deleted files.

Click on File Which you want to recover -> Right Click on that file and Select Export File Select Destination path-> Click on Ok



Export Files

File(s) to Export

● All highlighted files ○ All checked files ○ All currently listed files ○ All files

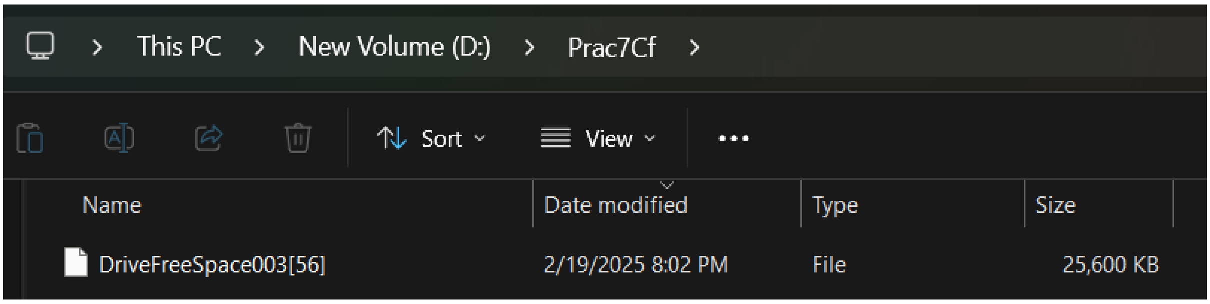
□ Include email attachments with email messages

File Name	Original Path
DriveFreeSpace003[56]	CFPrac7\USB Drive (F:)-NTFS

Destination Path: D:\Prac7Cf

☑ Prepend archive name to file name
☑ Append item number to file name to guarantee uniqueness
□ Append appropriate extension to file name if bad/absent
□ Export HTML view if available
□ Export filtered text view

Step 12: Deleted files are recovered at the specified location.



Name	Date modified	Type	Size
DriveFreeSpace003[56]	2/19/2025 8:02 PM	File	25,600 KB