

## Lesson 1.2

### General Topic: Deleted File Recovery (DFR)

#### High-Level Goals

This lesson helps the student detect the **true signature of a file**.

File extensions can be easily changed, which some attackers use to trick systems into misidentifying file types. In this lab, you will learn how to determine if a file has a false extension by examining its file signature in Autopsy.

To do so, you can see their file signatures in the **Hex** tab at the bottom in Autopsy.

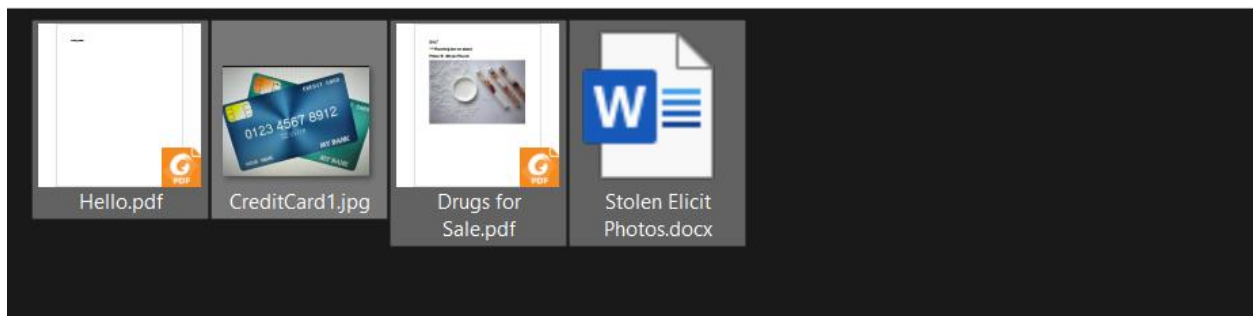
**Items needed:** Windows 10/11, Autopsy, and a USB thumb drive.

**Lab Setup:** Have the Autopsy software pre-installed on the Windows machine.

---

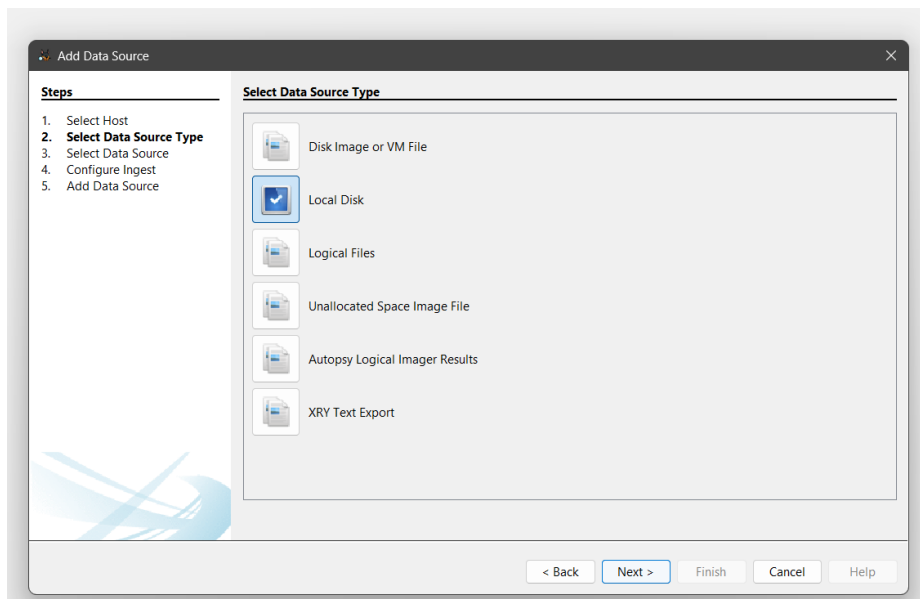
#### Task A: Identifying File Signatures

**Task A1:** In your group, one student will populate the thumb drive with 3-4 files of different file types (.pdf, .docx, and .jpg). These can be files from previous labs.

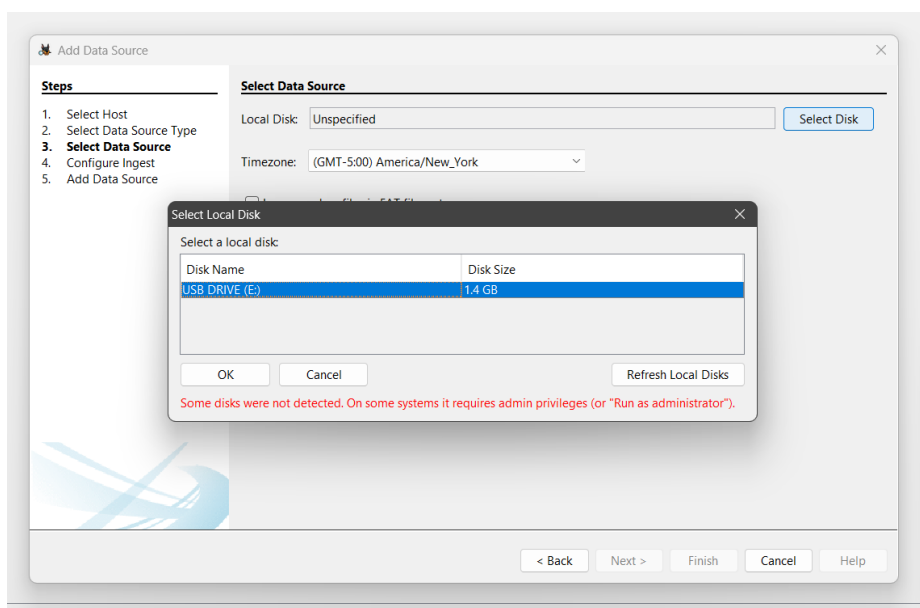


**Task A2:** After the files have been inserted, run Autopsy on the USB drive. (**Don't delete any files.**)

- Since we are using a storage disk, click on "Local Disk".



- Select and verify the drive you are examining.



**Task A3:** Once the analysis is complete, click on the Data Source to look inside the Disk E.

(0)

ie Inform

Name	Type	Size (Bytes)	Sector Size (Bytes)	Timezone	Device ID
E:	Image	1073741824	512	America/New_York	98105684-40fd-4706-8301-b8f34a5a26aa

Save Table as

- Recognize your files and look at the **Hex** tab for each file.

Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	MD5 Hash
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	Allocated	unknown	
\$FAT1				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1044992	Allocated	Allocated	unknown	
\$FAT2				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1044992	Allocated	Allocated	unknown	
\$MBR				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	512	Allocated	Allocated	unknown	
\$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	Allocated	unknown	
System Volume Information				2024-06-14 08:58:54 EDT	0000-00-00 00:00:00	2024-06-14 00:00:00 EDT	2024-06-14 08:58:52 EDT	4096	Allocated	Allocated	unknown	
_WRD0000.tmp				2024-06-16 19:24:10 EDT	0000-00-00 00:00:00	2024-06-16 00:00:00 EDT	2024-06-16 19:14:26 EDT	13173	Unallocated	Unallocated	unknown	
_WRL0001.tmp				2024-06-16 19:14:28 EDT	0000-00-00 00:00:00	2024-06-16 00:00:00 EDT	2024-06-16 19:14:26 EDT	0	Unallocated	Unallocated	unknown	
Hello.docx				2024-06-16 19:14:28 EDT	0000-00-00 00:00:00	2024-06-16 00:00:00 EDT	2024-06-16 19:14:26 EDT	0	Unallocated	Unallocated	unknown	
Hello.docx				2024-06-16 19:24:10 EDT	0000-00-00 00:00:00	2024-06-16 00:00:00 EDT	2024-06-16 19:14:26 EDT	13173	Allocated	Allocated	unknown	
HW2 (Volume Label Entry)				2024-06-14 08:58:54 EDT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	
New Microsoft Word Document.docx				2024-06-16 19:14:28 EDT	0000-00-00 00:00:00	2024-06-16 00:00:00 EDT	2024-06-16 19:14:26 EDT	0	Unallocated	Unallocated	unknown	

HexTextApplicationFile MetadataOS AccountData ArtifactsAnalysis ResultsContextAnnotationsOther Occurrences

Page: 1 of 1PageGo to Page: 1Jump to OffsetLaunch in HxD

0x00000000: 50 4B 03 04 14 00 06 00 08 00 00 00 21 00 DF A4 PK.....  
0x00000010: D2 6C 5A 01 00 00 20 05 00 00 13 00 08 02 5B 43 .12.....[C  
0x00000020: EF 6E 74 65 6E 74 5F 54 79 70 65 73 5D 2E 78 6D content\_Type).xm  
0x00000030: EC 20 A2 04 02 28 A0 00 02 00 00 00 00 00 00 00 1....(.....

- The starting signature of the file should be the starting bytes on page 1, and the ending signature should be the last bytes of the last page. Below is an **example** of a .jpg file whose starting file signature is FFD8 (Page 1) and the ending signature is FFD9 (Page 434). **Page numbers might differ.**

[parent folder]

CreditCard.jpg

creditCardList2.txt

MyListandScript.docx

Stolen Elicit Photos.pdf

HexTextApplicationFile MetadataOS AccountData ArtifactsAnalysis ResultsContextAnnotations

Page: 1 of 434PageGo to Page: 1Jump to Offset

0x00000000: FF D8 FF E0 00 14 4A 46 49 46 00 01 01 01 01 2C .....JFIF.....  
0x00000010: 01 2C 00 00 41 4D 50 46 FF E1 0A 9E 45 78 69 66 ...AMPF...Exif  
0x00000020: 00 00 4D 4D 00 2A 00 00 00 08 00 0C 01 06 00 03 ..MM.\*.....  
0x00000030: 00 00 00 01 88 4C 00 00 01 0F 00 02 00 00 00 06 .....L.....  
0x00000040: 00 00 00 9E 01 10 00 02 00 00 00 12 00 00 00 A4 .....  
0x00000050: 01 12 00 03 00 00 00 01 00 01 00 00 01 1A 00 05 .....

parent folder	0000-00-00 000000	0000-00-00 000000	0000-00-00 000000	0000-00-00 000000	4096	Unallocated	Allocated	unknown	/img_E1_piller1/		
CreditCard1.jpg	2024-06-10 13:41:50 EDT	0000-00-00 000000	2024-06-11 00:00:00 EDT	2024-06-13 08:44:40 EDT	7194723	Unallocated	Unallocated	unknown	/img_E1_piller1/CreditCard1.jpg		
CreditCard1a2.txt	2024-06-10 13:41:50 EDT	0000-00-00 000000	2024-06-11 00:00:00 EDT	2024-06-13 08:44:40 EDT	226	Unallocated	Unallocated	unknown	/img_E1_piller1/CreditCard1a2.txt		
MalwareScript.docx	2024-06-10 13:41:50 EDT	0000-00-00 000000	2024-06-11 00:00:00 EDT	2024-06-13 08:44:40 EDT	23493	Unallocated	Unallocated	unknown	/img_E1_piller1/MalwareScript.docx		
Stolen Elicit Photos.pdf	2024-06-10 13:41:50 EDT	0000-00-00 000000	2024-06-11 00:00:00 EDT	2024-06-13 08:44:40 EDT	267228	Unallocated	Unallocated	unknown	/img_E1_piller1/Stolen Elicit Photos.pdf		
cardist1.txt	2024-06-10 13:41:50 EDT	0000-00-00 000000	2024-06-11 00:00:00 EDT	2024-06-13 08:44:40 EDT	226	Unallocated	Unallocated	unknown	/img_E1/cardist1.txt		
CreditCard1.jpg	2024-06-10 13:41:50 EDT	0000-00-00 000000	2024-06-11 00:00:00 EDT	2024-06-13 08:44:40 EDT	3754911	Unallocated	Unallocated	unknown	/img_E1/CreditCard1.jpg		
CreditCard2.jpg	2024-06-10 13:41:50 EDT	0000-00-00 000000	2024-06-11 00:00:00 EDT	2024-06-13 08:44:50 EDT	9488195	Unallocated	Unallocated	unknown	/img_E1/CreditCard2.jpg		
Drugs for Sale.pdf	2024-06-10 13:41:50 EDT	0000-00-00 000000	2024-06-11 00:00:00 EDT	2024-06-13 08:44:52 EDT	236762	Unallocated	Unallocated	unknown	/img_E1/Drugs for Sale.pdf		
FaWebsiteurl	2024-06-10 13:41:50 EDT	0000-00-00 000000	2024-06-11 00:00:00 EDT	2024-06-13 08:44:52 EDT	73	Unallocated	Unallocated	unknown	/img_E1/FaWebsiteurl		
Journal.txt	2024-06-10 13:41:50 EDT	0000-00-00 000000	2024-06-11 00:00:00 EDT	2024-06-13 08:44:52 EDT	78	Unallocated	Unallocated	unknown	/img_E1/Journal.txt		
Stolen Elicit Photos.docx	2024-06-10 13:41:50 EDT	0000-00-00 000000	2024-06-11 00:00:00 EDT	2024-06-13 08:44:52 EDT	2362836	Unallocated	Unallocated	unknown	/img_E1/Stolen Elicit Photos.docx		
SuperBadSoundtrack.mp4	2024-06-10 13:41:50 EDT	0000-00-00 000000	2024-06-11 00:00:00 EDT	2024-06-13 08:44:53 EDT	632733	Unallocated	Unallocated	unknown	/img_E1/SuperBadSoundtrack.mp4		
10000000.fat	0000-00-00 000000	0000-00-00 000000	0000-00-00 000000	0000-00-00 000000	4096	Unallocated	Unallocated	unknown	/img_E1/SCarvedf1eay1/0000000.fat		
10000000.jpg	10 0000-00-00 000000	0000-00-00 000000	0000-00-00 000000	0000-00-00 000000	6750076	Unallocated	Unallocated	unknown	/img_E1/SCarvedf1eay1/0000000.jpg	87621ec74a6...7721323215735c	
10013208.txt	0000-00-00 000000	0000-00-00 000000	0000-00-00 000000	0000-00-00 000000	438	Unallocated	Unallocated	unknown	/img_E1/SCarvedf1eay1/00013208.txt		
10013888.txt	0000-00-00 000000	0000-00-00 000000	0000-00-00 000000	0000-00-00 000000	226	Unallocated	Unallocated	unknown	/img_E1/SCarvedf1eay1/00013888.txt		
10013888.docx	10 0000-00-00 000000	0000-00-00 000000	0000-00-00 000000	0000-00-00 000000	23493	Unallocated	Unallocated	unknown	/img_E1/SCarvedf1eay1/00013888.docx	a1a80a0b401...7ba10b0c218805c	
10013944.pdf	10 0000-00-00 000000	0000-00-00 000000	0000-00-00 000000	0000-00-00 000000	267228	Unallocated	Unallocated	unknown	/img_E1/SCarvedf1eay1/00013944.pdf	8666d71c30f...c1ba0208ba0d734c	
10025712.jpg	0000-00-00 000000	0000-00-00 000000	0000-00-00 000000	0000-00-00 000000	812125	Unallocated	Unallocated	unknown	/img_E1/SCarvedf1eay1/00025712.jpg		
10014464.jpg	10 0000-00-00 000000	0000-00-00 000000	0000-00-00 000000	0000-00-00 000000	5526330	Unallocated	Unallocated	unknown	/img_E1/SCarvedf1eay1/00014464.jpg	273fe18966a...b44ab0712a1528c	
10042296.pdf	0000-00-00 000000	0000-00-00 000000	0000-00-00 000000	0000-00-00 000000	236762	Unallocated	Unallocated	unknown	/img_E1/SCarvedf1eay1/00042296.pdf		

**Task A4:** Note the file signatures you found on the table below. (For the ending signature, try to find a similar pattern as the start signature)

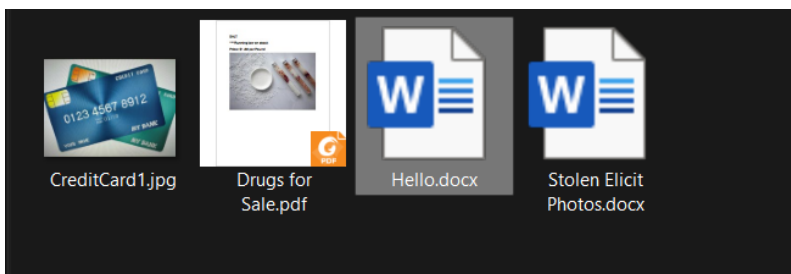
File type	Starting Signature	Ending Signature
.jpg	FF D8	FF D9
.pdf		
.docx		

## Task B

**Task B1:** Like Task A1, one student will populate the thumb drive with 3-4 files of these different file types (.pdf, .docx, and .jpg). These can be random files from previous labs.

**Task B2:** The same student will then change the extensions of some of these files and keep track of the changes. The other students in the group will try to find out which those files are and what the original extension was.

- After pasting the files onto the drive, right-click on a few files and select "Rename" to change their extensions (Here, Hello.pdf is renamed as Hello.docx. Ignore any warnings.)



- Examine the file signatures using the Hex tab in Autopsy and compare them with the signatures you noted in Task A.

✖ myListanascript.docx			2024-06-10 13:41:50 EDT	0000-00-00 00:00:00	2024-06-13 00:00:00 EDT	2024-06-13 08:44:48 EDT	22493	Unallocate
✖ Stolen Elicit Photos.pdf			2024-06-10 13:41:50 EDT	0000-00-00 00:00:00	2024-06-13 00:00:00 EDT	2024-06-13 08:44:48 EDT	261728	Unallocate
✖ cardlist1.txt			2024-06-10 13:41:50 EDT	0000-00-00 00:00:00	2024-06-13 00:00:00 EDT	2024-06-13 08:44:48 EDT	226	Unallocate
✖ CreditCard1.jpg			2024-06-10 13:41:50 EDT	0000-00-00 00:00:00	2024-06-13 00:00:00 EDT	2024-06-13 08:44:48 EDT	5754911	Unallocate
✖ CreditCard2.jpg			2024-06-10 13:41:50 EDT	0000-00-00 00:00:00	2024-06-13 00:00:00 EDT	2024-06-13 08:44:50 EDT	8488195	Unallocate
✖ Drugs for Sale.pdf			2024-06-10 13:41:50 EDT	0000-00-00 00:00:00	2024-06-13 00:00:00 EDT	2024-06-13 08:44:52 EDT	236702	Unallocate
✖ FavWebsite.url			2024-06-10 13:41:50 EDT	0000-00-00 00:00:00	2024-06-13 00:00:00 EDT	2024-06-13 08:44:52 EDT	73	Unallocate
✖ _ource.txt			2024-06-10 13:41:50 EDT	0000-00-00 00:00:00	2024-06-13 00:00:00 EDT	2024-06-13 08:44:52 EDT	78	Unallocate
✖ Stolen Elicit Photos.docx			2024-06-10 13:41:50 EDT	0000-00-00 00:00:00	2024-06-13 00:00:00 EDT	2024-06-13 08:44:52 EDT	2082616	Unallocate
✖ SuperBadSoundtrack.mp4			2024-06-10 13:41:50 EDT	0000-00-00 00:00:00	2024-06-13 00:00:00 EDT	2024-06-13 08:44:53 EDT	632733	Unallocate
✖ f0000000.fat			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	4096	Unallocate
✖ f0000008.jpg		10	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	6758076	Unallocate
✖ f0013208.txt			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	438	Unallocate
✖ f0013888.txt			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	226	Unallocate
✖ f0013896.docx		10	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	22493	Unallocate
✖ f0013944.pdf		10	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	261728	Unallocate
✖ f0025712.jpg			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	8112125	Unallocate
✖ f0014464.jpg		10	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	5528330	Unallocate
✖ f0042296.pdf			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	236702	Unallocate

Hex	Text	Application	File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences
Page: 1 of 16	Page	Go to Page: 1	Jump to Offset	Launch in HxD					
0x00000000: 25 50 44 B6	2D 31 2E 37	0D 0A 25 B5	B5 B5 B5 0D	%PDF-1.7...%.....					
0x00000010: 0A 31 20 30	20 6F 62 6A	0D 0A 3C 3C	2F 54 79 70	..U obj...<</Typ					

- Discuss your findings with your group.