#Lab 4 DIGITAL EVIDENCE FORENSICS (using FTK)

Zobayer Md Ahsanul Mahbub (2125129)

CASE 01a:

Data Acquisition & Recovering Deleted File

Screenshots:

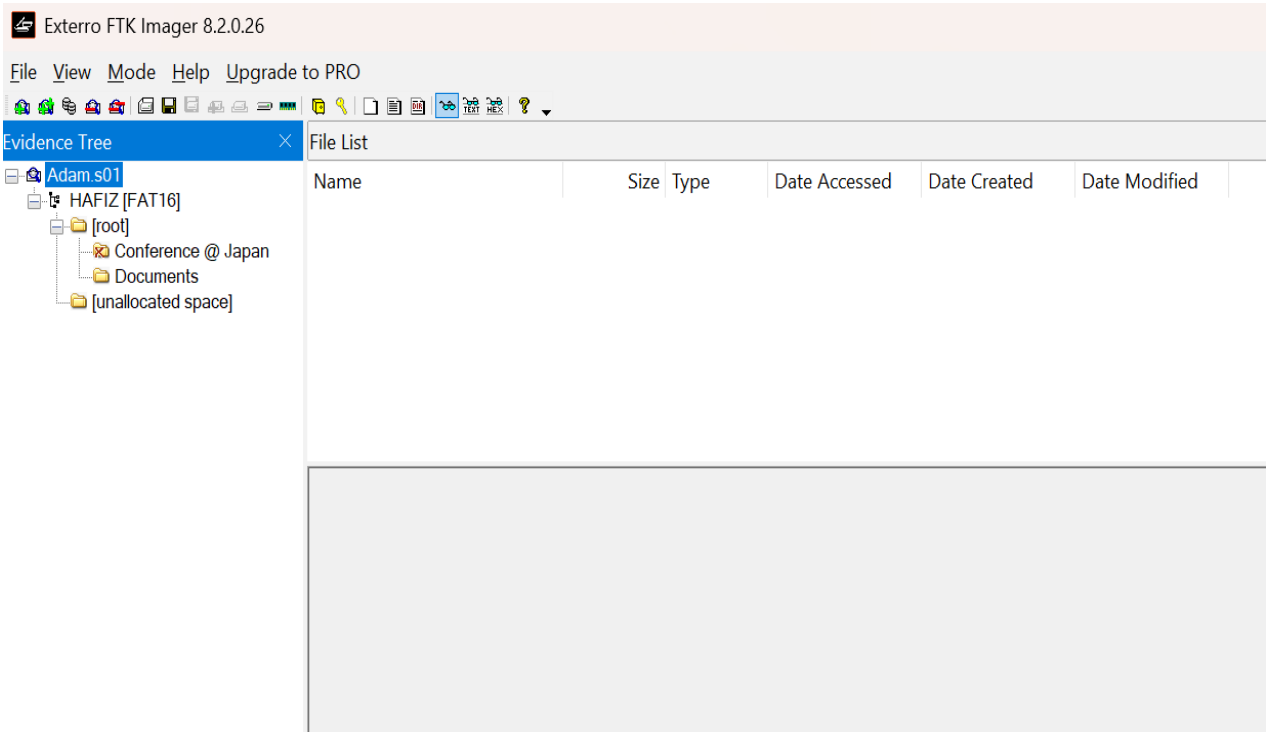


Figure 1: Load the Adam.s01 into FTK Imager

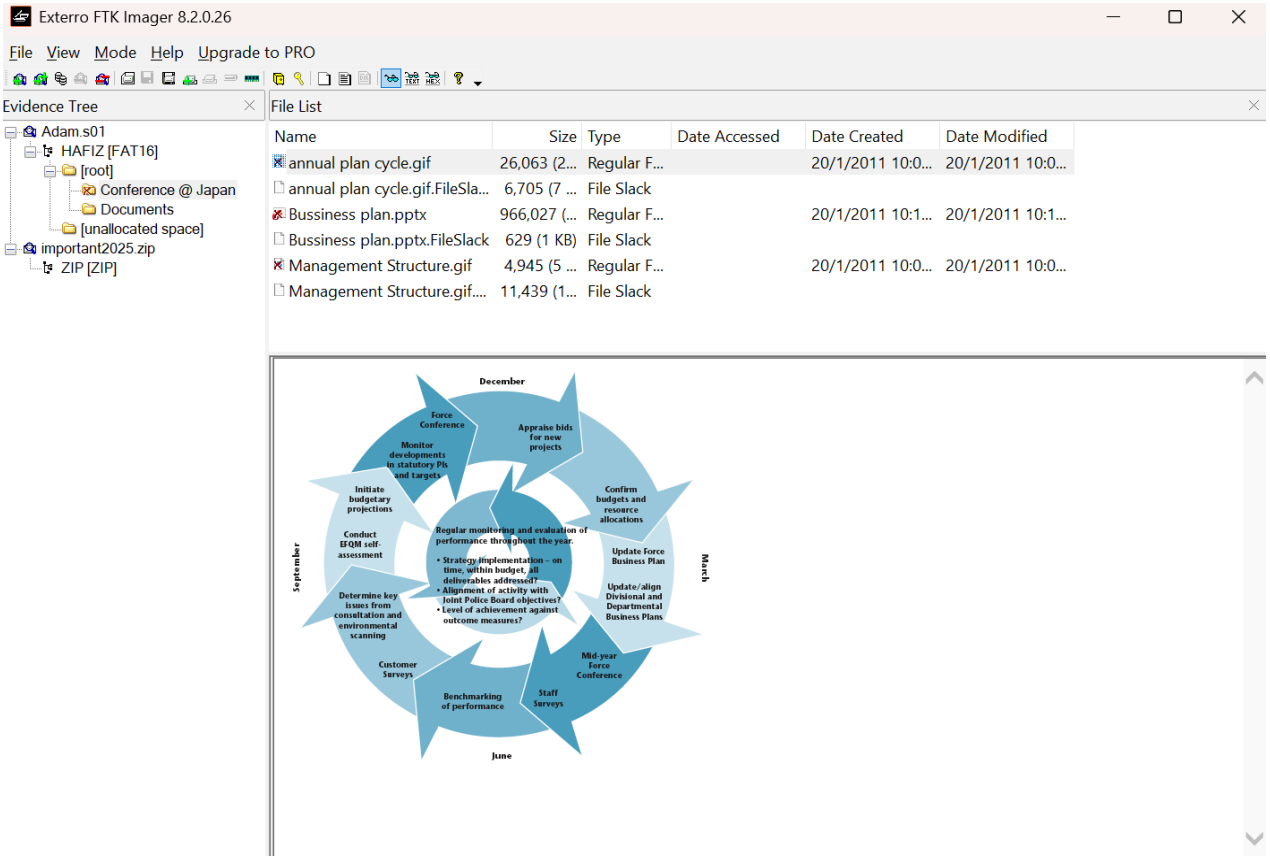
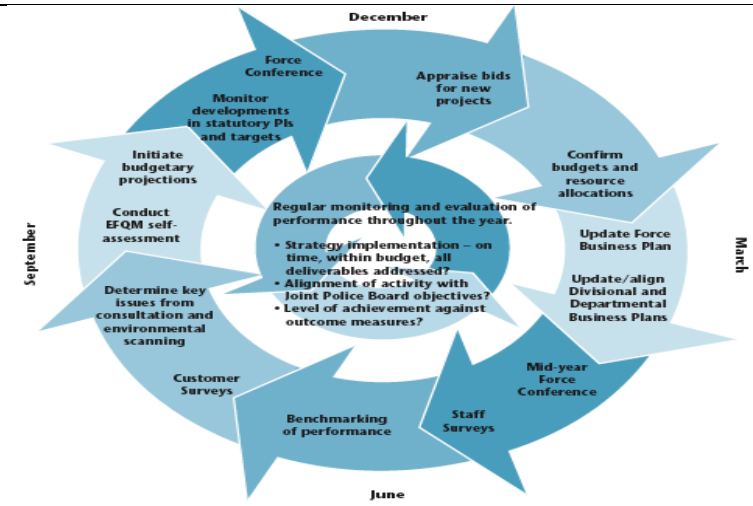
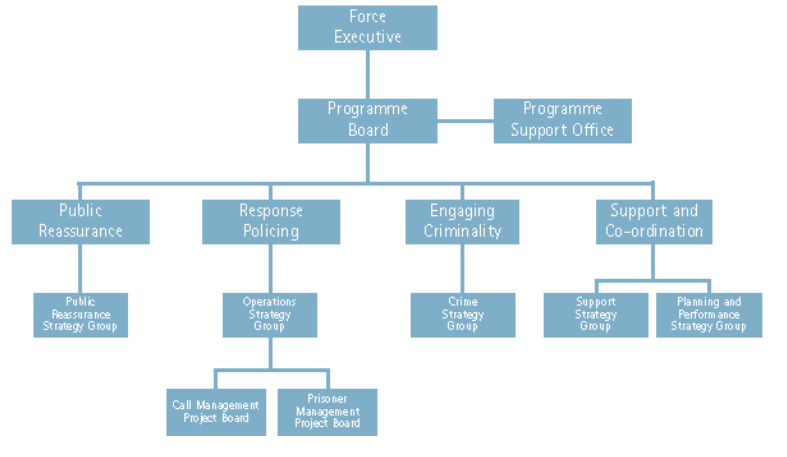


Figure 2: Navigated to the deleted folder Conference @ Japan

Steps to recover the data:

1. Install FTK Imager
2. Upload the Adam.s01 file into the Evidence item
3. Find the deleted file “Conference @ Japan”
4. Export files

Recovered files:

File Name	Screenshots
annual plan cycle.gif	
Business plan.pptx	
Management Structure.gif	

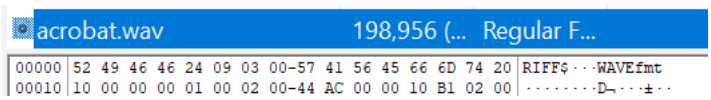
CASE 02a: Files with wrong extensions

I used FTK Imager to find the header of each file. Later, based on the Hex value of the header I fix the file name with the correct extension. The table below shows the work:

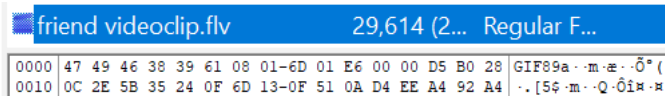
No.	The given File Name (With Extensions) in the hard disk	File Name with the Correct Extension	Correct File Header (in Hex) *eg. FF D8 (jpeg)*
1	acrobat.wav	acrobat.wav	52 49 46 46
2	friend videoclip.flv	friend videoclip.gif	47 49 46 38
3	happy.psd	happy.wav	52 49 46 46
4	header.docx	header.mp4	00 00 00 20 66 74 79 70 69 73 6F 6D
5	Notes.mp3	Notes.zip	50 4B 03 04
6	Notes.txt	Notes.txt	48 69 6E 74
7	readme.exe	readme.zip	50 4B 03 04
8	Sales-Q1-2023.pdf	Sales-Q1-2023.docx	50 4B 03 04
9	viva forever.apk	viva forever.bmp	42 4D 76 FA
10	wave-cell.pdf	wave-cell.jpg	FF D8 FF E0

Screenshots:

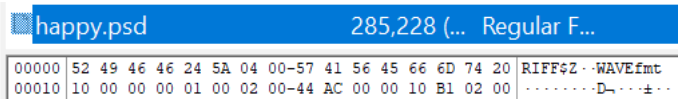
1.



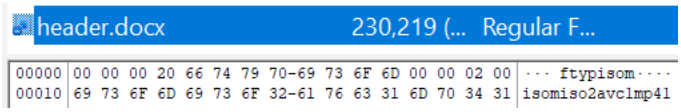
2.



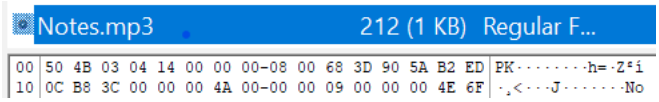
3.


happy.psd 285,228 (... Regular F...
00000 52 49 46 46 24 5A 04 00-57 41 56 45 66 6D 74 20 RIFF$Z··WAVEfmt
00010 10 00 00 00 01 00 02 00-44 AC 00 00 10 B1 02 00 ····D¬···±··

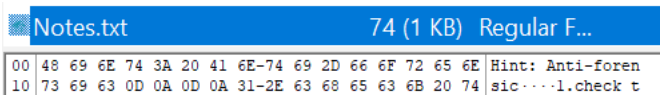
4.


header.docx 230,219 (... Regular F...
00000 00 00 00 20 66 74 79 70-69 73 6F 6D 00 00 02 00 ··· ftypisom····
00010 69 73 6F 6D 69 73 6F 32-61 76 63 31 6D 70 34 31 isomiso2avc1mp41

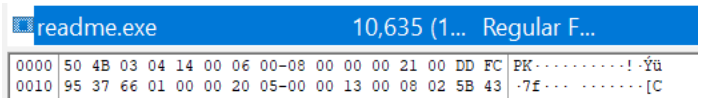
5.


Notes.mp3 212 (1 KB) Regular F...
00 50 4B 03 04 14 00 00 00-08 00 68 3D 90 5A B2 ED PK·····h=·Z²í
10 0C B8 3C 00 00 00 4A 00-00 00 09 00 00 00 4E 6F ·¸<···J·····No

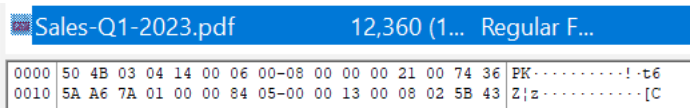
6.


Notes.txt 74 (1 KB) Regular F...
00 48 69 6E 74 3A 20 41 6E-74 69 2D 66 6F 72 65 6E Hint: Anti-foren
10 73 69 63 0D 0A 0D 0A 31-2E 63 68 65 63 6B 20 74 sic····1.check t

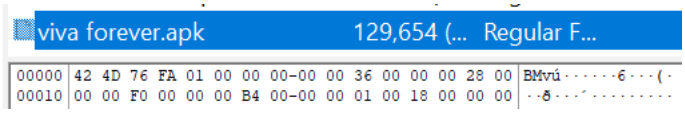
7.


readme.exe 10,635 (1... Regular F...
0000 50 4B 03 04 14 00 06 00-08 00 00 00 21 00 DD FC PK·····!·Ýü
0010 95 37 66 01 00 00 20 05-00 00 13 00 08 02 5B 43 ·7f··· ·····[C

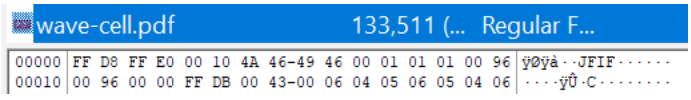
8.

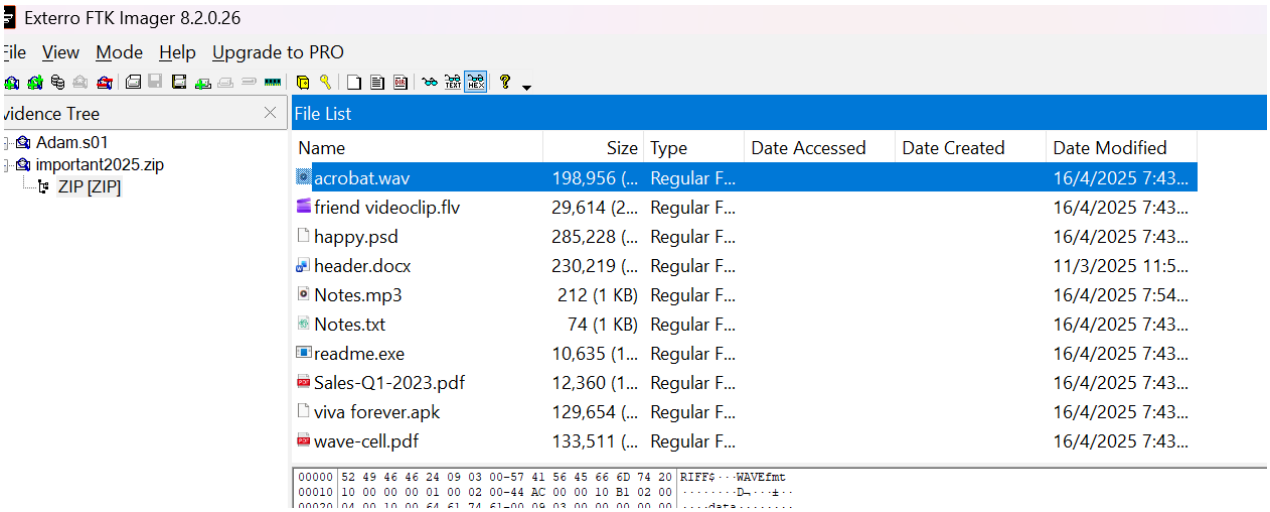

Sales-Q1-2023.pdf 12,360 (1... Regular F...
0000 50 4B 03 04 14 00 06 00-08 00 00 00 21 00 74 36 PK·····!·t6
0010 5A A6 7A 01 00 00 84 05-00 00 13 00 08 02 5B 43 Z¦z·····[C

9.


viva forever.apk 129,654 (... Regular F...
00000 42 4D 76 FA 01 00 00 00-00 00 36 00 00 00 28 00 BMvú·····6···(·
00010 00 00 F0 00 00 00 B4 00-00 00 01 00 18 00 00 00 ··ð···´·····

10.


wave-cell.pdf 133,511 (... Regular F...
00000 FF D8 FF E0 00 10 4A 46-49 46 00 01 01 01 00 96 ÿØÿà··JFIF·····
00010 00 96 00 00 FF DB 00 43-00 06 04 05 06 05 04 06 ····ÿÛ·C·····


Exterro FTK Imager 8.2.0.26
File View Mode Help Upgrade to PRO
Evidence Tree
Adam.s01
important2025.zip
ZIP [ZIP]
File List
Name Size Type Date Accessed Date Created Date Modified
acrobat.wav 198,956 (... Regular F... 16/4/2025 7:43...
friend videoclip.flv 29,614 (2... Regular F... 16/4/2025 7:43...
happy.psd 285,228 (... Regular F... 16/4/2025 7:43...
header.docx 230,219 (... Regular F... 11/3/2025 11:5...
Notes.mp3 212 (1 KB) Regular F... 16/4/2025 7:54...
Notes.txt 74 (1 KB) Regular F... 16/4/2025 7:43...
readme.exe 10,635 (1... Regular F... 16/4/2025 7:43...
Sales-Q1-2023.pdf 12,360 (1... Regular F... 16/4/2025 7:43...
viva forever.apk 129,654 (... Regular F... 16/4/2025 7:43...
wave-cell.pdf 133,511 (... Regular F... 16/4/2025 7:43...
00000 52 49 46 46 24 09 03 00-57 41 56 45 66 6D 74 20 RIFF$...WAVEfmt
00010 10 00 00 00 01 00 02 00-44 AC 00 00 10 B1 02 00 ....D¬...±..