

ITT 593 – LAB ACTIVITIES

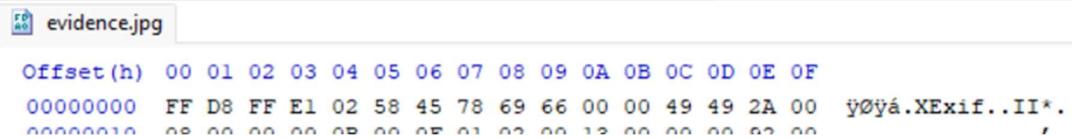
LAB : 1

NAME	:	MUHAMMAD HAFIZUDDIN BIN ROSLI
MATRIX NO	:	2024902995
DATE	:	2/5/2025
TIME	:	2:30 pm
EVIDENCE FILE NAME	:	Evidence.jpg

TASK 1

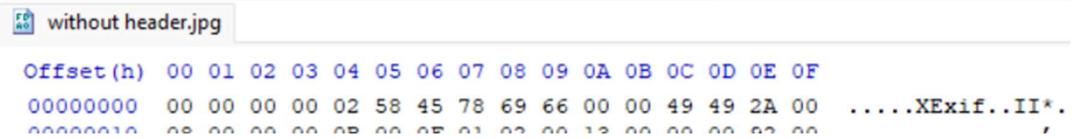
DATE	:	2/5/2025
TIME	:	2:30 pm
EVIDENCE FILE NAME	:	Evidence.jpg

Step 1: Opened the "evidence.jpg" file using HxD hex editor. The file header was displayed as FF D8 FF E1.



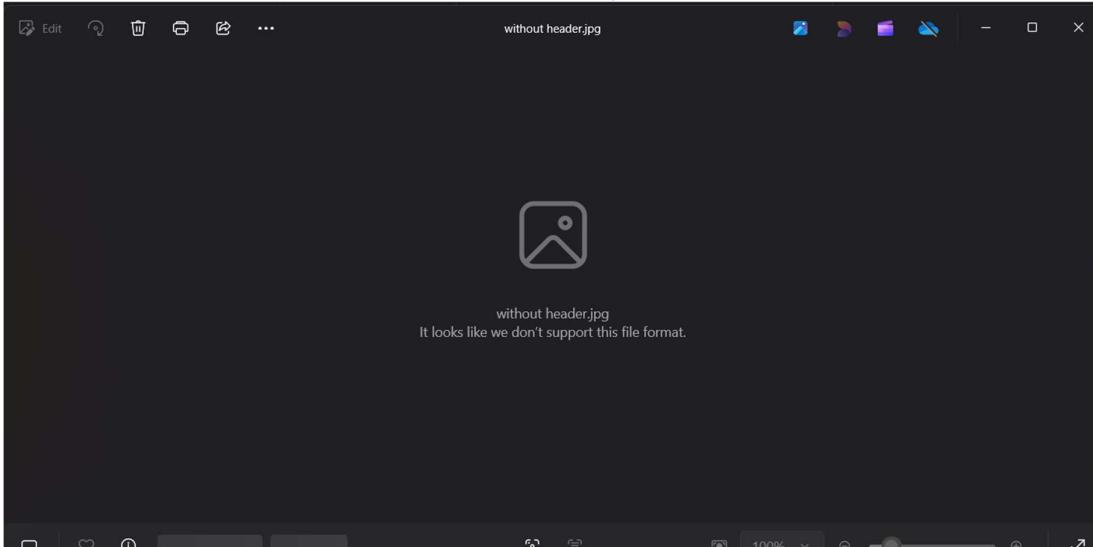
```
evidence.jpg  
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  
00000000 FF D8 FF E1 02 58 45 78 69 66 00 00 49 49 2A 00 ýØýá.XExif..II*.  
00000010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ,
```

Step 2: Replaced the original header with 00 00 00 00 and saved the file as without header.jpg.



```
without header.jpg  
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  
00000000 00 00 00 00 00 02 58 45 78 69 66 00 00 49 49 2A 00 .....XExif..II*.  
00000010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ,
```

Result: The file became unreadable and could not be opened.



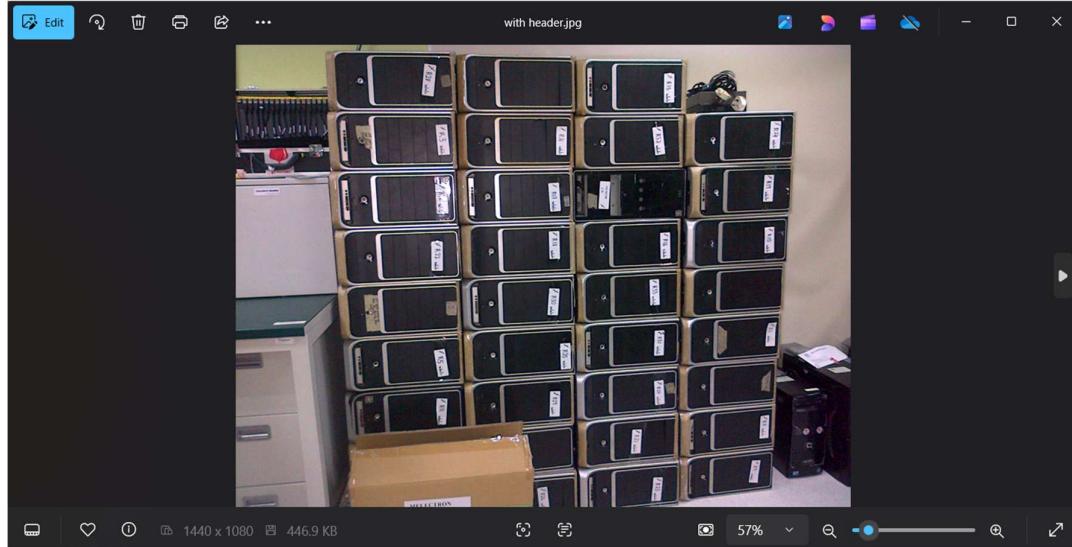
Step 3: Open “without header.jpg” file in the hex editor. Change the header back to FF D8 FF E1 and saved as with header.jpg.



The screenshot shows a hex editor interface with two tabs: "without header.jpg" and "with header.jpg". The "without header.jpg" tab is active, displaying the raw binary data. The first few bytes are shown in blue: 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F. Following these are the bytes FF D8 FF E1, then 02 58 45 78 69 66 00 00 49 49 2A 00, followed by a series of non-printable characters (yøýá, XExif..II*, etc.). The "with header.jpg" tab is visible but not active.

Offset(h)	00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00000000	FF D8 FF E1 02 58 45 78 69 66 00 00 49 49 2A 00 yøýá, XExif..II*
00000010	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Result: The image successfully opened in an image viewer.



This task shows how important the file header is for properly recognizing and opening a file. The file becomes unreadable if the header is removed or changed incorrectly. The file can be reopened by restoring a valid JPG header. This demonstrates how important the file header is for digital forensics file identification and recovery. In this case, the correct JPG header is FF D8 FF E1.

TASK 2

DATE	:	2/5/2025
TIME	:	2:47 pm
EVIDENCE FILE NAME	:	The Dreaming Girl In Me.mp3

The file type is MP3. Its corresponding hex signature is 49 44 33. This indicates the presence of an ID3 metadata tag.

without header.jpg	with header.jpg	The Dreaming Girl In Me.mp3	pic_1.png	July 2023.pdf
--------------------	-----------------	-----------------------------	-----------	---------------

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00000000 49 44 33 03 00 00 00 05 28 7C 54 49 54 32 00 00  ID3.....(|TIT2..
00000010 00 19 00 00 00 54 68 65 20 44 72 65 61 6D 69 6E ....The Dreamin
```

DATE	:	2/5/2025
TIME	:	2:50 pm
EVIDENCE FILE NAME	:	pic_1.png

The file type is PNG. Its corresponding hex signature is 89 50 4E 47 0D 0A 1A 0A. This 8-byte value is used to identify PNG images. This shows the file is indeed a valid PNG format.

without header.jpg	with header.jpg	The Dreaming Girl In Me.mp3	pic_1.png	July 2023.pdf
--------------------	-----------------	-----------------------------	-----------	---------------

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00000000 89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52 %PNG.....IHDR
00000010 00 00 00 F1 00 00 00 F1 00 00 00 00 00 00 00 00
```

DATE	:	2/5/2025
TIME	:	2:53 pm
EVIDENCE FILE NAME	:	July 2023.pdf

The file type is PDF. Its corresponding hex signature is 25 50 44 46. This pattern confirms the file is in Portable Document Format.

without header.jpg	with header.jpg	July 2023.pdf
--------------------	-----------------	---------------

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00000000 25 50 44 46 2D 31 2E 36 0D 25 E2 E3 CF D3 0D 0A %PDF-1.6.%äïÓ..
00000010 31 22 22 22 22 22 22 22 22 22 22 22 22 22 22 22
```

DATE	:	2/5/2025
TIME	:	2:55 pm
EVIDENCE FILE NAME	:	RIDE 4 GAMEPLAY.mp4

The file type is MP4. Its corresponding hex signature is 00 00 00 18 66 74 79 70 6D 70 34 32. This identifies the file as an mp4 video.

without header.jpg	with header.jpg	RIDE 4 GAMEPLAY.mp4
--------------------	-----------------	---------------------

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00000000 00 00 00 18 66 74 79 70 6D 70 34 32 00 00 00 00 ....ftypmp42...
00000010 2B 20 24 21 24 72 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B
```

DATE	:	2/5/2025
TIME	:	2:57 pm
EVIDENCE FILE NAME	:	spongebob.gif

The file type is GIF. Its corresponding hex signature is 47 49 46 38 39 61 for GIF89a or 47 49 46 38 37 61 for GIF87a. These signatures are used for both standard GIF formats.

without header.jpg	with header.jpg	spongebob.gif
--------------------	-----------------	---------------

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00000000 47 49 46 38 39 61 F4 01 27 01 F7 00 00 16 15 11 GIF89a. ....
00000010 14 15 16 20 11 07 2C 1D 0B 0B 17 2B 1D 22 2B 1C 25 14 21 15
```

DATE	:	2/5/2025
TIME	:	2:59 pm
EVIDENCE FILE NAME	:	white shirt.psd

The file type is PSD. Its corresponding hex signature is 38 42 50 53. This signature belongs to Adobe Photoshop files.

without header.jpg	with header.jpg	white shirt.psd
--------------------	-----------------	-----------------

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00000000 38 42 50 53 00 01 00 00 00 00 00 00 00 00 03 00 00 8BPS.....
```

DATE	:	2/5/2025
TIME	:	3:02 pm
EVIDENCE FILE NAME	:	Nature.bmp

The file type is BMP. Its corresponding hex signature is 42 4D. This value is used to identify bitmap image files.

.....

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00000000 42 4D 8A 7B 0C 00 00 00 00 00 8A 00 00 00 7C 00 BM{.....S...}.
```

Each file analyzed had a unique hexadecimal signature at the beginning, known as a file header. These headers are essential for verifying the true file type, especially when extensions are misleading or incorrect. Hex signatures serve as a reliable method for file validation in digital forensic investigations.

TASK 3

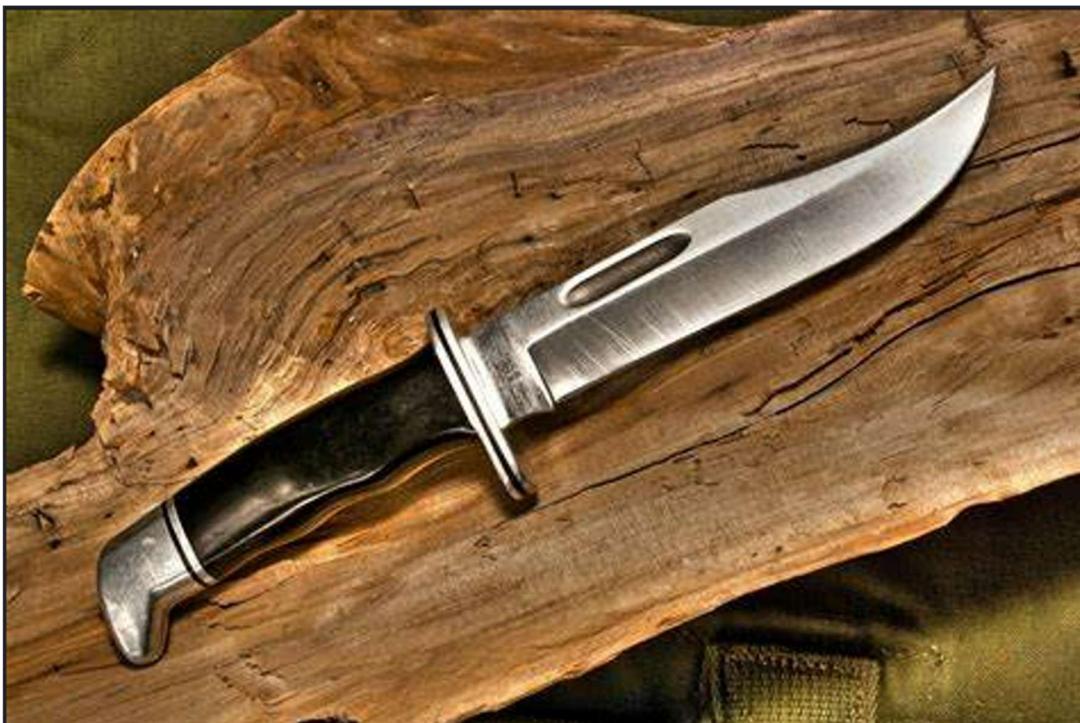
DATE	:	2/5/2025
TIME	:	3:07 pm
EVIDENCE FILE NAME	:	C1.jpg

Before change:

After change:

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  
00000000 FF D8 00 11 22 33 44 DF 30 41 22 01 01 01 00 00 00.."3D80A"....
```

Result:



Initially, the file could not be opened due to corruption. The header was then edited and replaced with FF D8, which is the correct hex signature for JPEG files. After saving it with a .jpg extension, the file opened successfully in an image viewer.

DATE	:	2/5/2025
TIME	:	3:10 pm
EVIDENCE FILE NAME	:	C2.gif

Before change:

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00000000 33 34 35 36 37 38 D0 02 94 01 F7 FF 00 00 00 00 345678D.".÷ÿ....
```

After change:

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00000000 47 49 46 38 39 61 D0 02 94 01 F7 FF 00 00 00 00 GIF89aD.".÷ÿ....
```

Result:



The file was not working at first. After replacing the header with 47 49 46 38 39 61 and saving it as a .gif file, it opened correctly. This confirmed the file was a valid GIF format.

DATE	:	2/5/2025
TIME	:	3:13 pm
EVIDENCE FILE NAME	:	C3.pdf

Before change:

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00000000 11 12 AA 33 44 31 2E 35 0D 0A 25 B5 B5 B5 B5 OD ..*3D1.5..%µµµµ.
```

After change:

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00000000 25 50 44 46 44 31 2E 35 0D 0A 25 B5 B5 B5 B5 OD %PDFD1.5..%µµµµ.
```

Result:

NO. SIRI:



PERMIT PERGERAKAN PERINTAH KAWALAN PERGERAKAN BERSYARAT (PKPB)

Kepada : Ketua Polis Balai

Kawasan Pentadbiran Daerah :

1. Butir-Butir Pemohon

1.1 Nama :

1.2 Kad Pengenalan : 1.3 Warganegara :

1.4 No. Pasport (Bukan Warganegara) :

1.5 Alamat :

1.6 No. Telefon : 1.7 Emel :

1.8 Jenis Kenderaan / No. Pendaftaran:

1.9 Jumlah Orang : orang (Lampirkan Butir-Butir Individu)

1.10 Tarikh / Masa Meninggalkan Rumah :

1.11 Tarikh / Masa Dijangka Balik Ke Rumah :

1.12 Alamat Penuh Destinasi :

2. Sebab-sebab permohonan pergerakan:-

.....
.....
.....
.....

Tandatangan Pemohon :

Tarikh :

Kegunaan Ketua Polis Balai

Keputusan Permohonan : Diluluskan / Tidak Diluluskan

Ulasan :

Tandatangan :

Nama (Huruf Besar) :

Pangkat & Jawatan :

Tarikh :



Cop Rasmii
Salinan Asal sahaja
sahlaku

The file did not open at first. After replacing the header with 25 50 44 46, the recognized hex signature for PDF files, the file was saved again. It then opened successfully in a PDF reader.

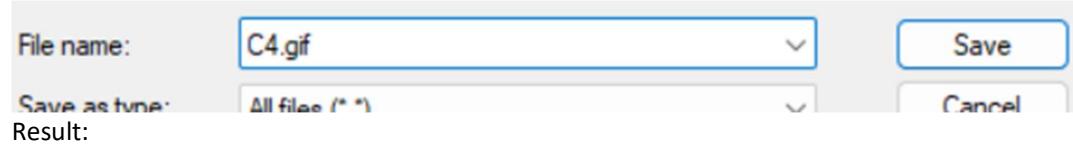
DATE	:	2/5/2025
TIME	:	3:18 pm
EVIDENCE FILE NAME	:	C4.txt

Before change:

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  
00000000 47 49 46 38 39 61 55 03 E0 01 70 00 00 21 FF 0B  GIF89aU.à.p...!ÿ.
```

After change:

Change file name .txt to .gif because the file header format is gif header



Result:



The file had a .txt extension, but no changes were made to the header. The hex signature already present was for a GIF file, which is 47 49 46 38 39 61. After renaming the file to .gif, it opened correctly as an image.

DATE	:	2/5/2025
TIME	:	3:20 pm
EVIDENCE FILE NAME	:	C5.pdf

Before change:

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00000000 38 42 50 53 00 01 00 00 00 00 00 00 00 03 00 00 8BPS.....
```

After change:

Change file name .pdf to .psd because the file header format is psd header

Result:



Although labeled as a PDF, the file header was actually 38 42 50 53, which identifies it as a Photoshop (PSD) file. The extension was changed from .pdf to .psd. The file was then able to open properly in Adobe Photoshop.

DATE	:	2/5/2025
TIME	:	3:25 pm
EVIDENCE FILE NAME	:	C6.mp3

Before change:

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00000000 50 4B 03 04 14 00 06 00 08 00 00 00 21 00 DF CC PK.....!$!
```

After change:

Change file name .mp3 to .zip because the file header format is zip header.

Result:

Name	Type	Compressed size	Password p...	Size	Ratio	Date modified
_rels	File folder					
docProps	File folder					
ppt	File folder					
[Content_Types].xml	Microsoft Edge HTML Document	1 KB	No	4 KB	87%	30/12/1899 8:00 AM

This file was originally named as an MP3, but its header showed 50 4B 03 04, which is the standard hex signature for ZIP archives. After changing the file extension to .zip, the file was opened successfully as a compressed folder.

Through this task, it was found that each unknown or corrupted file could be recovered by analyzing and correcting the file header or changing the file extension. Most files were misidentified due to incorrect headers or names, but were successfully restored to their actual format. This highlights the importance of file header analysis in identifying and recovering files during digital forensic processes.

SUMMARY OF FINDINGS

Throughout Lab 1, the importance of file headers in digital forensics was clearly demonstrated. The test on Task 1 showed how the JPEG file header serves as the authentic identifier of the file format because removing it rendered the image unreadable despite its file extension. The analysis of different files in Task 2 showed that file verification relies on distinctive hex signatures such as 49 44 33 for MP3 and 89 50 4E 47 0D 0A 1A 0A for PNG which exist at the beginning of each file. The recovery of misidentified files succeeded through header identification which enabled the correct labeling of these corrupted files during Task 3. Each file recovered functionality after the hex signature received modifications or the file extension received renaming. This lab demonstrated that digital forensics professionals must master file header identification and hex editor use to achieve successful file validation and repair and recovery operations.

PREPARED BY:

t.t



Muhammad Hafizuddin bin Rosli