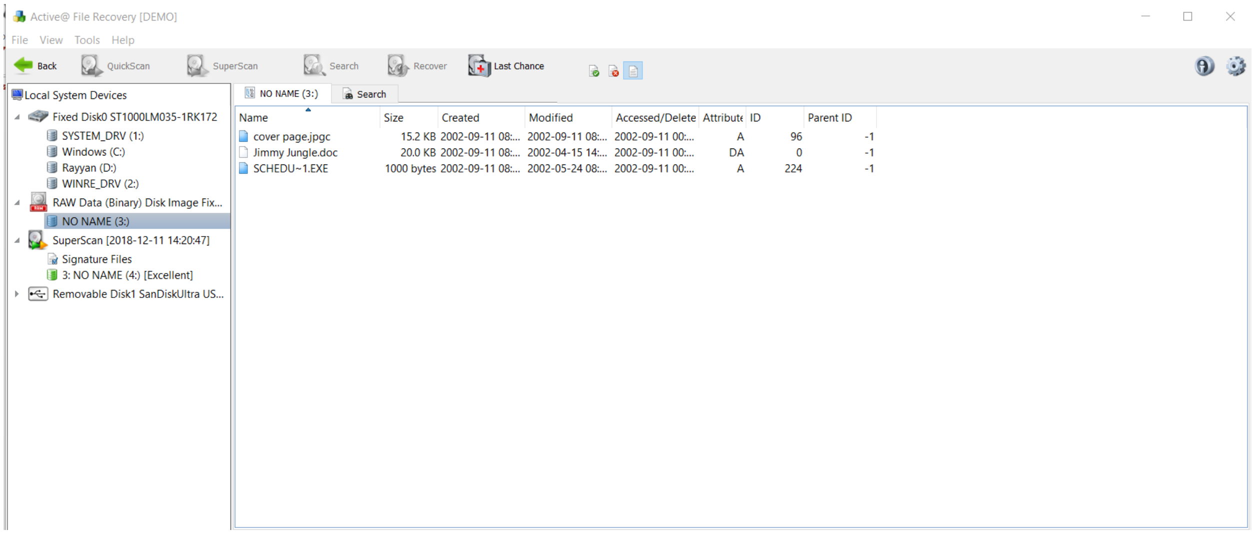
Rayyan
09021181520012

1. Analisa Forensik Image File

Alat yg digunakan : NTFS file recovery

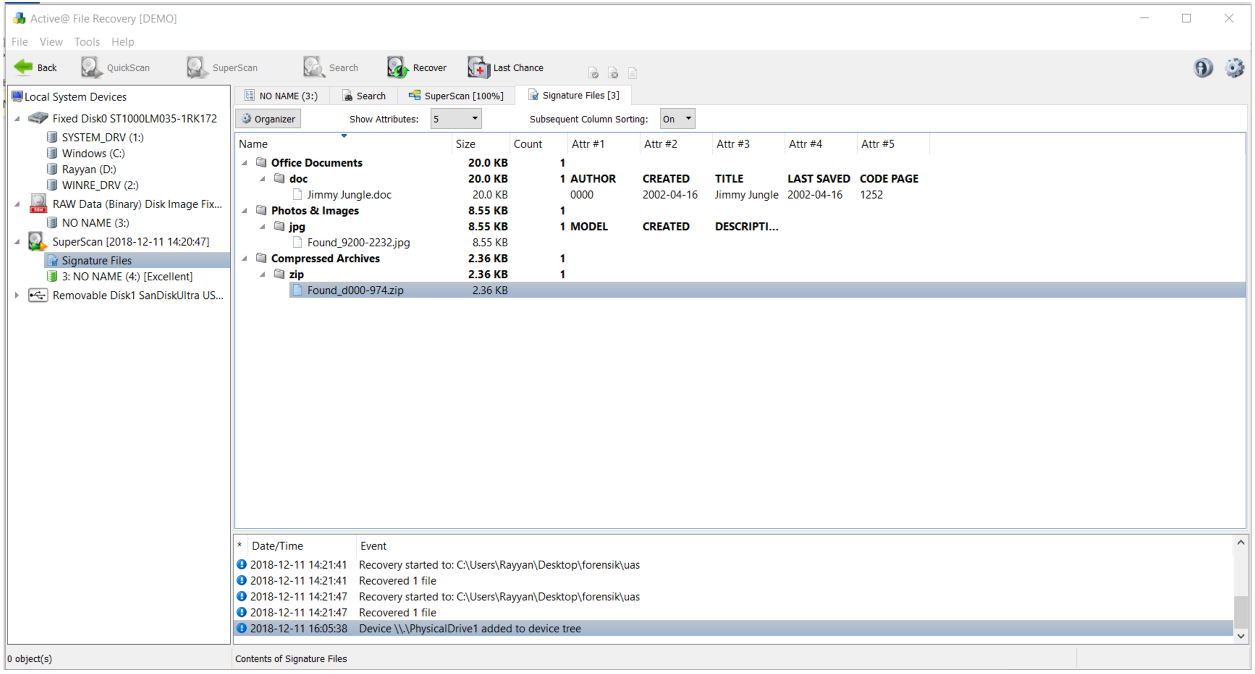
OS : Windows 10

- Mount disk image yang terdapat pada winrar


Active@ File Recovery [DEMO]
File View Tools Help
Back QuickScan SuperScan Search Recover Last Chance
Local System Devices
Fixed Disk0 ST1000LM035-1RK172
SYSTEM_DRV (1:)
Windows (C:)
Rayyan (D:)
WINRE_DRV (2:)
RAW Data (Binary) Disk Image Fix...
NO NAME (3:)
SuperScan [2018-12-11 14:20:47]
Signature Files
3: NO NAME (4:) [Excellent]
Removable Disk1 SanDiskUltra US...
NO NAME (3:)
Search

Name	Size	Created	Modified	Accessed/Delete	Attribute	ID	Parent ID
cover page.jpgc	15.2 KB	2002-09-11 08:...	2002-09-11 08:...	2002-09-11 00:...	A	96	-1
Jimmy Jungle.doc	20.0 KB	2002-09-11 08:...	2002-04-15 14:...	2002-09-11 00:...	DA	0	-1
SCHEDU~1.EXE	1000 bytes	2002-09-11 08:...	2002-05-24 08:...	2002-09-11 00:...	A	224	-1

- Lakukan super scan untuk mengembalikan signature 3 file tersebut


Active@ File Recovery [DEMO]
File View Tools Help
Back QuickScan SuperScan Search Recover Last Chance
Local System Devices
Fixed Disk0 ST1000LM035-1RK172
SYSTEM_DRV (1:)
Windows (C:)
Rayyan (D:)
WINRE_DRV (2:)
RAW Data (Binary) Disk Image Fix...
NO NAME (3:)
SuperScan [2018-12-11 14:20:47]
Signature Files
3: NO NAME (4:) [Excellent]
Removable Disk1 SanDiskUltra US...
NO NAME (3:)
Search
SuperScan [100%]
Signature Files [3]
Organizer
0 object(s)
Contents of Signature Files

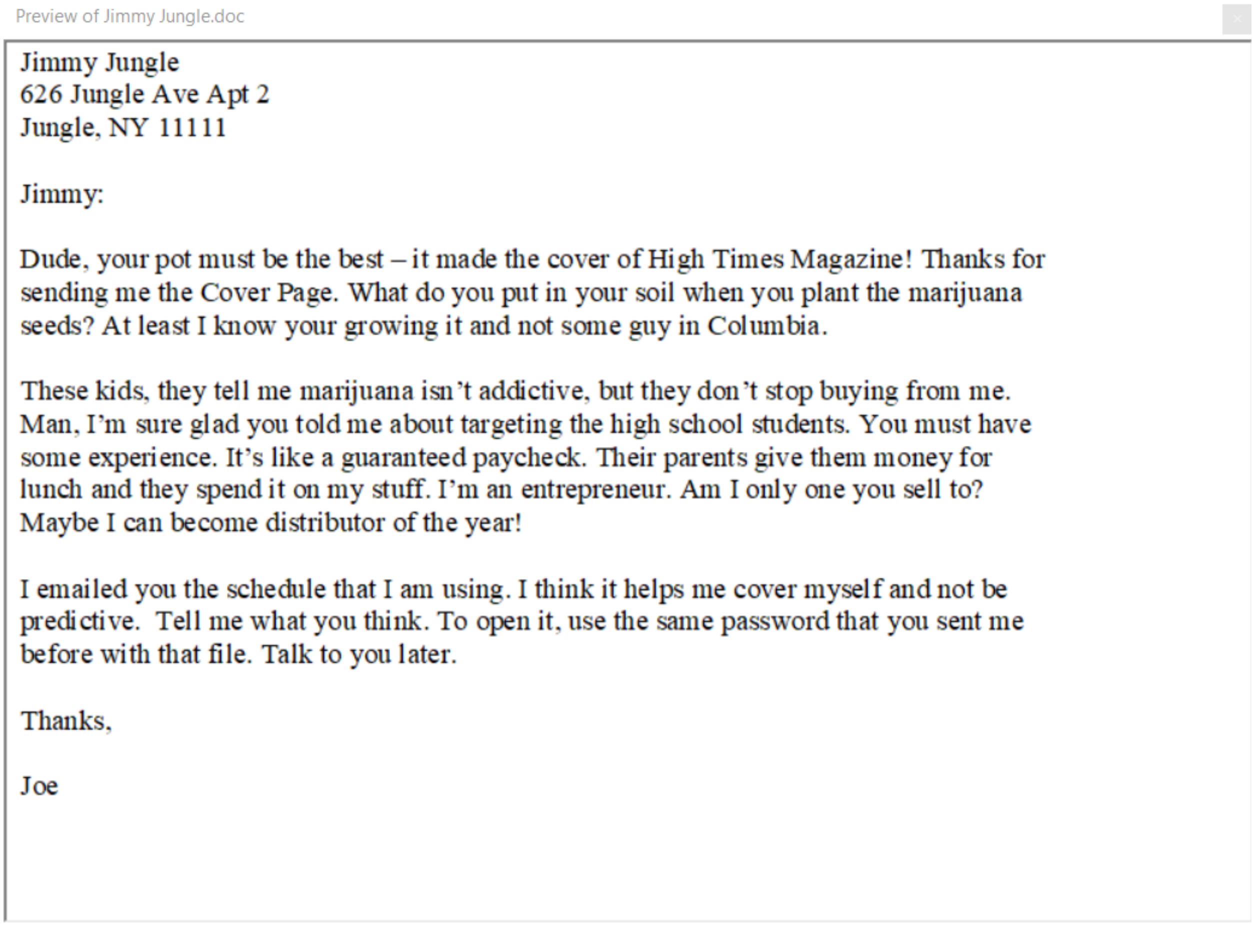
Show Attributes: 5 Subsequent Column Sorting: On

Name	Size	Count	Attr #1	Attr #2	Attr #3	Attr #4	Attr #5
Office Documents	**20.0 KB**	**1**					
doc	**20.0 KB**	**1**	**AUTHOR**	**CREATED**	**TITLE**	**LAST SAVED**	**CODE PAGE**
Jimmy Jungle.doc	20.0 KB		0000	2002-04-16	Jimmy Jungle	2002-04-16	1252
Photos & Images	**8.55 KB**	**1**					
jpg	**8.55 KB**	**1**	**MODEL**	**CREATED**	**DESCRIPTI...**		
Found_9200-2232.jpg	8.55 KB						
Compressed Archives	**2.36 KB**	**1**					
zip	**2.36 KB**	**1**					
Found_d000-974.zip	2.36 KB						

```
*  Date/Time            Event
   2018-12-11 14:21:41  Recovery started to: C:\Users\Rayyan\Desktop\forensik\uas
   2018-12-11 14:21:41  Recovered 1 file
   2018-12-11 14:21:47  Recovery started to: C:\Users\Rayyan\Desktop\forensik\uas
   2018-12-11 14:21:47  Recovered 1 file
   2018-12-11 16:05:38  Device \\.\PhysicalDrive1 added to device tree
```

seperti yang terlihat ternyata file .exe yang terdapat pada image file tersebut adalah .zip dan lalu file .jpgc merupakan file .jpg

- Dan file yang dihapus ternyata sebuah surat dari seorang supplier yang bernama joe yang dikirimkan untuk seseorang yang bernama jimmy jungle.



Jimmy Jungle
626 Jungle Ave Apt 2
Jungle, NY 11111

Jimmy:

Dude, your pot must be the best – it made the cover of High Times Magazine! Thanks for sending me the Cover Page. What do you put in your soil when you plant the marijuana seeds? At least I know your growing it and not some guy in Columbia.

These kids, they tell me marijuana isn't addictive, but they don't stop buying from me. Man, I'm sure glad you told me about targeting the high school students. You must have some experience. It's like a guaranteed paycheck. Their parents give them money for lunch and they spend it on my stuff. I'm an entrepreneur. Am I only one you sell to? Maybe I can become distributor of the year!

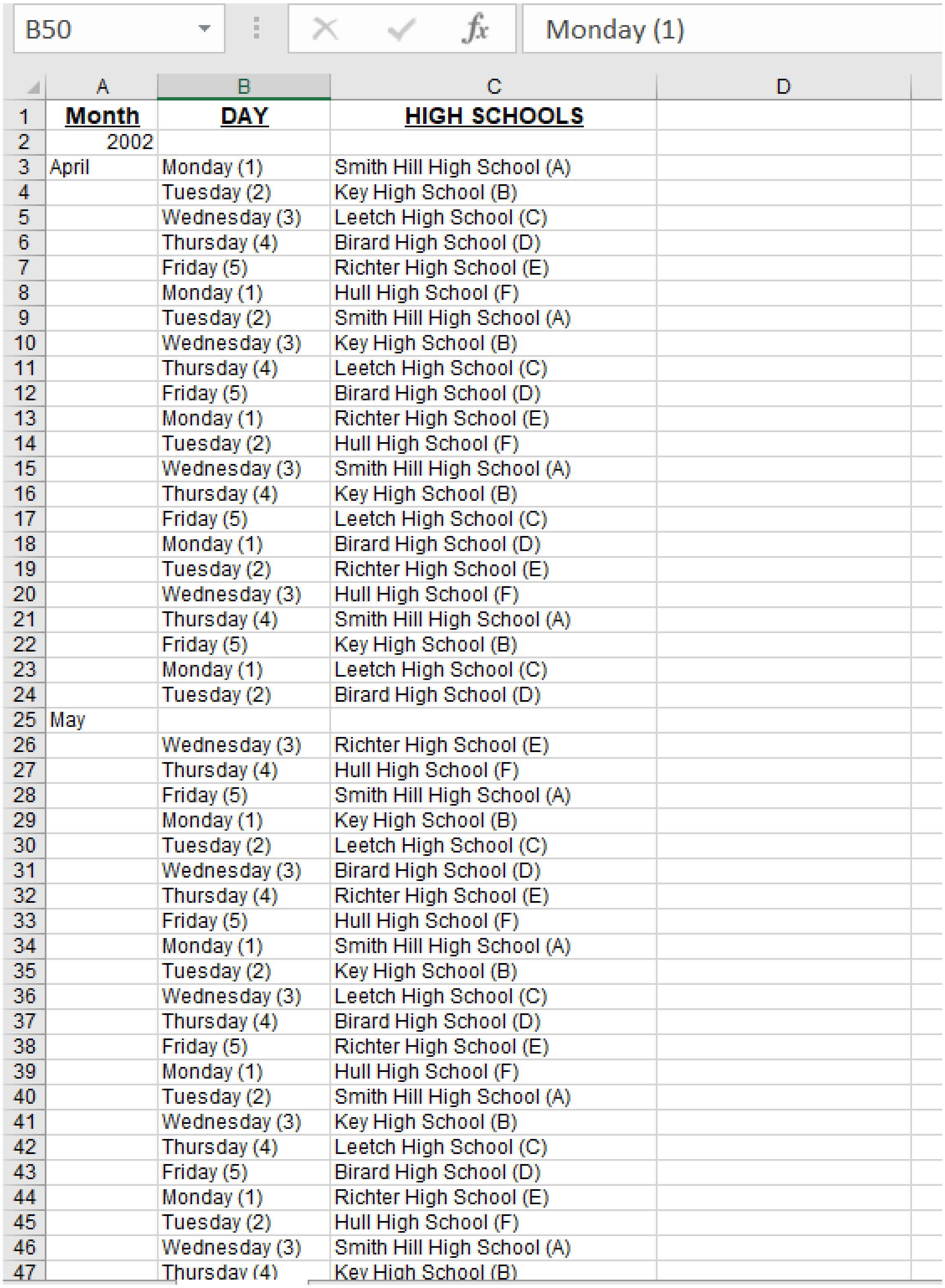
I emailed you the schedule that I am using. I think it helps me cover myself and not be predictive. Tell me what you think. To open it, use the same password that you sent me before with that file. Talk to you later.

Thanks,

Joe

- Saat menginspek header dalam file cover page.jpg terdapat password "`pw=goodtimes`" yang digunakan untuk membuka zip yang ternyata berisikan jadwal transaksinya.

Rayyan
09021181520012



Monday (1)

	A	B	C	D
1	**Month**	**DAY**	**HIGH SCHOOLS**	
2	2002			
3	April	Monday (1)	Smith Hill High School (A)	
4		Tuesday (2)	Key High School (B)	
5		Wednesday (3)	Leetch High School (C)	
6		Thursday (4)	Birard High School (D)	
7		Friday (5)	Richter High School (E)	
8		Monday (1)	Hull High School (F)	
9		Tuesday (2)	Smith Hill High School (A)	
10		Wednesday (3)	Key High School (B)	
11		Thursday (4)	Leetch High School (C)	
12		Friday (5)	Birard High School (D)	
13		Monday (1)	Richter High School (E)	
14		Tuesday (2)	Hull High School (F)	
15		Wednesday (3)	Smith Hill High School (A)	
16		Thursday (4)	Key High School (B)	
17		Friday (5)	Leetch High School (C)	
18		Monday (1)	Birard High School (D)	
19		Tuesday (2)	Richter High School (E)	
20		Wednesday (3)	Hull High School (F)	
21		Thursday (4)	Smith Hill High School (A)	
22		Friday (5)	Key High School (B)	
23		Monday (1)	Leetch High School (C)	
24		Tuesday (2)	Birard High School (D)	
25	May			
26		Wednesday (3)	Richter High School (E)	
27		Thursday (4)	Hull High School (F)	
28		Friday (5)	Smith Hill High School (A)	
29		Monday (1)	Key High School (B)	
30		Tuesday (2)	Leetch High School (C)	
31		Wednesday (3)	Birard High School (D)	
32		Thursday (4)	Richter High School (E)	
33		Friday (5)	Hull High School (F)	
34		Monday (1)	Smith Hill High School (A)	
35		Tuesday (2)	Key High School (B)	
36		Wednesday (3)	Leetch High School (C)	
37		Thursday (4)	Birard High School (D)	
38		Friday (5)	Richter High School (E)	
39		Monday (1)	Hull High School (F)	
40		Tuesday (2)	Smith Hill High School (A)	
41		Wednesday (3)	Key High School (B)	
42		Thursday (4)	Leetch High School (C)	
43		Friday (5)	Birard High School (D)	
44		Monday (1)	Richter High School (E)	
45		Tuesday (2)	Hull High School (F)	
46		Wednesday (3)	Smith Hill High School (A)	
47		Thursday (4)	Key High School (B)	

○

Rayyan
09021181520012

soal:

1. Who is Joe Jacob's supplier of marijuana and what is the address listed for the supplier?
   - ➢ Jimmy jungle, 626 Jungle Ave Apt 2 Jungle, NY 11111

2. What crucial data is available within the coverpage.jpg file and why is this data crucial?
   - ➢ "pw=goodtimes" yang merupakan password untuk membuka file .zip yang berisikan jadwal transaksi joe.

3. What (if any) other high schools besides Smith Hill does Joe Jacobs frequent?
   - ➢ Leetch High School, Birard High School, Richter High School, Key High School, dan Hull High School

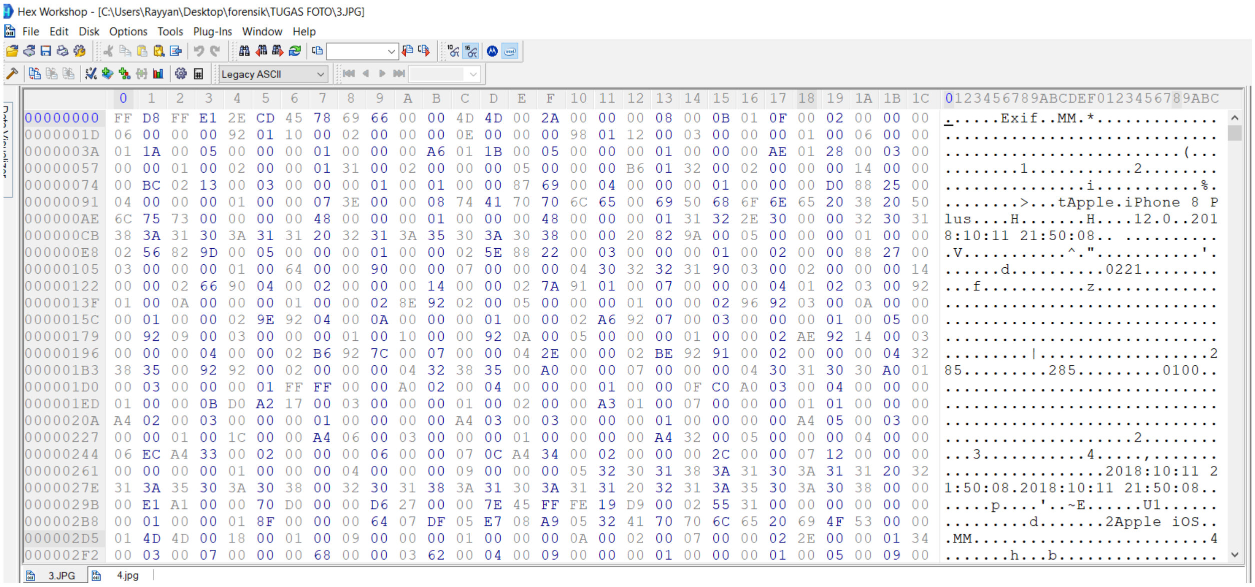
4. For each file, what processes were taken by the suspect to mask them from others?
   - ➢ Menghapus file Jimmyjungle.doc, mengubah format file Cover page.jpg menjadi cover page.jpgc dan menyisipkan passwordnya didalam hexnya

Rayyan
09021181520012

2. Analisa Forensik Gambar / Foto

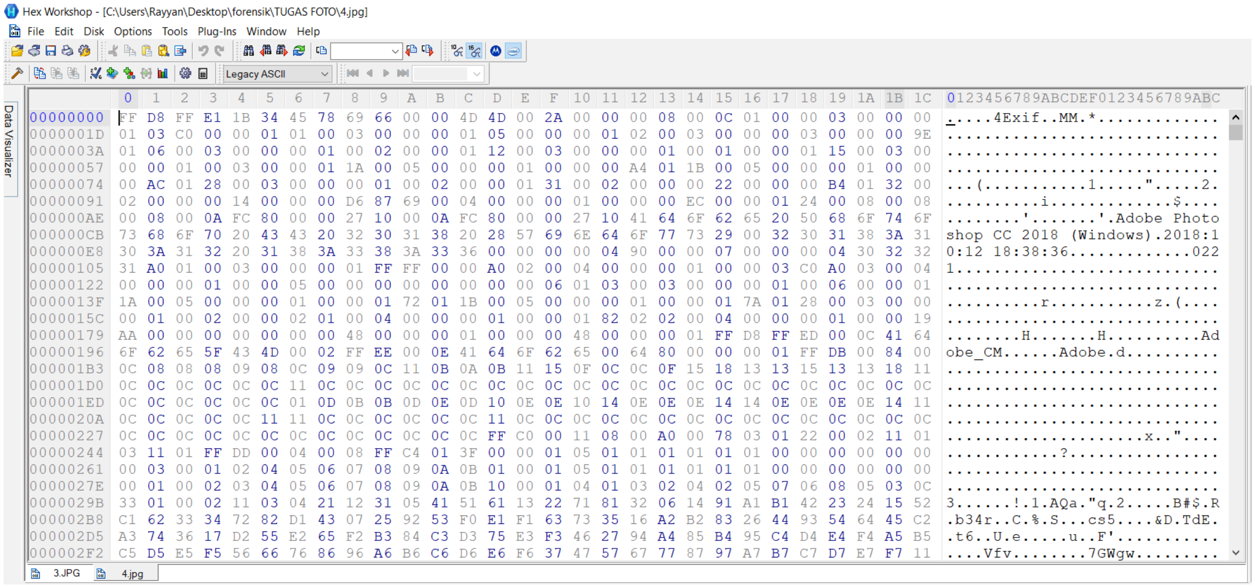
Alat yang digunakan : Hex Workshop

Operating system : Windows 10


Hex Workshop - [C:\Users\Rayyan\Desktop\forensik\TUGAS FOTO\3.JPG]
File Edit Disk Options Tools Plug-Ins Window Help
Legacy ASCII
Data Visualizer
3.JPG
4.jpg

```
          0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F  10 11 12 13 14 15 16 17 18 19 1A 1B 1C 0123456789ABCDEF0123456789ABC
00000000  FF D8 FF E1 2E CD 45 78 69 66 00 00 4D 4D 00 2A 00 00 00 08 00 0B 01 0F 00 02 00 00 00 ......Exif..MM.*.............
0000001D  06 00 00 00 92 01 10 00 02 00 00 00 0E 00 00 00 98 01 12 00 03 00 00 00 01 00 06 00 00 .............................
0000003A  01 1A 00 05 00 00 00 01 00 00 00 A6 01 1B 00 05 00 00 00 01 00 00 00 AE 01 28 00 03 00 .........................(...
00000057  00 00 01 00 02 00 00 01 31 00 02 00 00 00 05 00 00 00 B6 01 32 00 02 00 00 00 14 00 00 ........1..........2.........
00000074  00 BC 02 13 00 03 00 00 00 01 00 01 00 00 87 69 00 04 00 00 00 01 00 00 00 D0 88 25 00 ...............i...........%.
00000091  04 00 00 00 01 00 00 07 3E 00 00 08 74 41 70 70 6C 65 00 69 50 68 6F 6E 65 20 38 20 50 ........>...tApple.iPhone 8 P
000000AE  6C 75 73 00 00 00 00 48 00 00 00 01 00 00 00 48 00 00 00 01 31 32 2E 30 00 00 32 30 31 lus....H.......H....12.0..201
000000CB  38 3A 31 30 3A 31 31 20 32 31 3A 35 30 3A 30 38 00 00 20 82 9A 00 05 00 00 00 01 00 00 8:10:11 21:50:08.. ..........
000000E8  02 56 82 9D 00 05 00 00 00 01 00 00 02 5E 88 22 00 03 00 00 00 01 00 02 00 00 88 27 00 .V...........^."...........'.
00000105  03 00 00 00 01 00 64 00 00 90 00 00 07 00 00 00 04 30 32 32 31 90 03 00 02 00 00 00 14 ......d..........0221........
00000122  00 00 02 66 90 04 00 02 00 00 00 14 00 00 02 7A 91 01 00 07 00 00 00 04 01 02 03 00 92 ...f...........z.............
0000013F  01 00 0A 00 00 00 01 00 00 02 8E 92 02 00 05 00 00 00 01 00 00 02 96 92 03 00 0A 00 00 .............................
0000015C  00 01 00 00 02 9E 92 04 00 0A 00 00 00 01 00 00 02 A6 92 07 00 03 00 00 00 01 00 05 00 .............................
00000179  00 92 09 00 03 00 00 00 01 00 10 00 00 92 0A 00 05 00 00 00 01 00 00 02 AE 92 14 00 03 .............................
00000196  00 00 00 04 00 00 02 B6 92 7C 00 07 00 00 04 2E 00 00 02 BE 92 91 00 02 00 00 00 04 32 .........|..................2
000001B3  38 35 00 92 92 00 02 00 00 00 04 32 38 35 00 A0 00 00 07 00 00 00 04 30 31 30 30 A0 01 85.........285.........0100..
000001D0  00 03 00 00 00 01 FF FF 00 00 A0 02 00 04 00 00 00 01 00 00 0F C0 A0 03 00 04 00 00 00 .............................
000001ED  01 00 00 0B D0 A2 17 00 03 00 00 00 01 00 02 00 00 A3 01 00 07 00 00 00 01 01 00 00 00 .............................
0000020A  A4 02 00 03 00 00 00 01 00 00 00 00 A4 03 00 03 00 00 00 01 00 00 00 00 A4 05 00 03 00 .............................
00000227  00 00 01 00 1C 00 00 A4 06 00 03 00 00 00 01 00 00 00 00 A4 32 00 05 00 00 00 04 00 00 ....................2........
00000244  06 EC A4 33 00 02 00 00 00 06 00 00 07 0C A4 34 00 02 00 00 00 2C 00 00 07 12 00 00 00 ...3...........4.....,.......
00000261  00 00 00 00 01 00 00 00 04 00 00 00 09 00 00 00 05 32 30 31 38 3A 31 30 3A 31 31 20 32 .................2018:10:11 2
0000027E  31 3A 35 30 3A 30 38 00 32 30 31 38 3A 31 30 3A 31 31 20 32 31 3A 35 30 3A 30 38 00 00 1:50:08.2018:10:11 21:50:08..
0000029B  00 E1 A1 00 00 70 D0 00 00 D6 27 00 00 7E 45 FF FE 19 D9 00 02 55 31 00 00 00 00 00 00 .....p....'..~E......U1......
000002B8  00 01 00 00 01 8F 00 00 00 64 07 DF 05 E7 08 A9 05 32 41 70 70 6C 65 20 69 4F 53 00 00 .........d.......2Apple iOS..
000002D5  01 4D 4D 00 18 00 01 00 09 00 00 00 01 00 00 00 0A 00 02 00 07 00 00 02 2E 00 00 01 34 .MM.........................4
000002F2  00 03 00 07 00 00 00 68 00 00 03 62 00 04 00 09 00 00 00 01 00 00 00 01 00 05 00 09 00 .......h...b.................
```

Gambar 3.JPG merupakan gambar yang diambil menggunkan iphone 8 plus yang bermetadata exif


Hex Workshop - [C:\Users\Rayyan\Desktop\forensik\TUGAS FOTO\4.jpg]
File Edit Disk Options Tools Plug-Ins Window Help
Legacy ASCII
Data Visualizer
3.JPG
4.jpg

```
          0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F  10 11 12 13 14 15 16 17 18 19 1A 1B 1C 0123456789ABCDEF0123456789ABC
00000000  FF D8 FF E1 1B 34 45 78 69 66 00 00 4D 4D 00 2A 00 00 00 08 00 0C 01 00 00 03 00 00 00 .....4Exif..MM.*.............
0000001D  01 03 C0 00 00 01 01 00 03 00 00 00 01 05 00 00 00 01 02 00 03 00 00 00 03 00 00 00 9E .............................
0000003A  01 06 00 03 00 00 00 01 00 02 00 00 01 12 00 03 00 00 00 01 00 01 00 00 01 15 00 03 00 .............................
00000057  00 00 01 00 03 00 00 01 1A 00 05 00 00 00 01 00 00 00 A4 01 1B 00 05 00 00 00 01 00 00 .............................
00000074  00 AC 01 28 00 03 00 00 00 01 00 02 00 00 01 31 00 02 00 00 00 22 00 00 00 B4 01 32 00 ...(...........1.....".....2.
00000091  02 00 00 00 14 00 00 00 D6 87 69 00 04 00 00 00 01 00 00 00 EC 00 00 01 24 00 08 00 08 ..........i.............$....
000000AE  00 08 00 0A FC 80 00 00 27 10 00 0A FC 80 00 00 27 10 41 64 6F 62 65 20 50 68 6F 74 6F ........'.......'.Adobe Photo
000000CB  73 68 6F 70 20 43 43 20 32 30 31 38 20 28 57 69 6E 64 6F 77 73 29 00 32 30 31 38 3A 31 shop CC 2018 (Windows).2018:1
000000E8  30 3A 31 32 20 31 38 3A 33 38 3A 33 36 00 00 00 00 04 90 00 00 07 00 00 00 04 30 32 32 0:12 18:38:36.............022
00000105  31 A0 01 00 03 00 00 00 01 FF FF 00 00 A0 02 00 04 00 00 00 01 00 00 03 C0 A0 03 00 04 1............................
00000122  00 00 00 01 00 00 05 00 00 00 00 00 00 00 06 01 03 00 03 00 00 00 01 00 06 00 00 01 .............................
0000013F  1A 00 05 00 00 00 01 00 00 01 72 01 1B 00 05 00 00 00 01 00 00 01 7A 01 28 00 03 00 00 ..........r..........z.(.....
0000015C  00 01 00 02 00 00 02 01 00 04 00 00 00 01 00 00 01 82 02 02 00 04 00 00 00 01 00 00 19 .............................
00000179  AA 00 00 00 00 00 00 00 48 00 00 00 01 00 00 00 48 00 00 00 01 FF D8 FF ED 00 0C 41 64 ........H.......H..........Ad
00000196  6F 62 65 5F 43 4D 00 02 FF EE 00 0E 41 64 6F 62 65 00 64 80 00 00 00 01 FF DB 00 84 00 obe_CM......Adobe.d..........
000001B3  0C 08 08 08 09 08 0C 09 09 0C 11 0B 0A 0B 11 15 0F 0C 0C 0F 15 18 13 13 15 13 13 18 11 .............................
000001D0  0C 0C 0C 0C 0C 0C 11 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C .............................
000001ED  0C 0C 0C 0C 0C 0C 01 0D 0B 0B 0D 0E 0D 10 0E 0E 10 14 0E 0E 0E 14 14 0E 0E 0E 0E 14 11 .............................
0000020A  0C 0C 0C 0C 0C 11 11 0C 0C 0C 0C 0C 0C 11 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C .............................
00000227  0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C FF C0 00 11 08 00 A0 00 78 03 01 22 00 02 11 01 .....................x.."....
00000244  03 11 01 FF DD 00 04 00 08 FF C4 01 3F 00 00 01 05 01 01 01 01 01 01 00 00 00 00 00 00 ............?................
00000261  00 03 00 01 02 04 05 06 07 08 09 0A 0B 01 00 01 05 01 01 01 01 01 01 00 00 00 00 00 00 .............................
0000027E  00 01 00 02 03 04 05 06 07 08 09 0A 0B 10 00 01 04 01 03 02 04 02 05 07 06 08 05 03 0C .............................
0000029B  33 01 00 02 11 03 04 21 12 31 05 41 51 61 13 22 71 81 32 06 14 91 A1 B1 42 23 24 15 52 3......!.1.AQa."q.2.....B#$.R
000002B8  C1 62 33 34 72 82 D1 43 07 25 92 53 F0 E1 F1 63 73 35 16 A2 B2 83 26 44 93 54 64 45 C2 .b34r..C.%.S...cs5....&D.TdE.
000002D5  A3 74 36 17 D2 55 E2 65 F2 B3 84 C3 D3 75 E3 F3 46 27 94 A4 85 B4 95 C4 D4 E4 F4 A5 B5 .t6..U.e.....u..F'...........
000002F2  C5 D5 E5 F5 56 66 76 86 96 A6 B6 C6 D6 E6 F6 37 47 57 67 77 87 97 A7 B7 C7 D7 E7 F7 11 ....Vfv........7GWgw.........
```

Sementara 4.jpg merupakan gambar telah diedit menggunakan adobe photoshop cc 2018 dan pada gambar 4.jpg juga device yang digunakan telah dihapus/hilang sehingga tidak terdeteksi gambar ini diambil menggunakan device apa. Dan file ini sebelum diedit ternyata dikirimkan terlebih dahulu kepada pengedit menggunakan whatsapp.