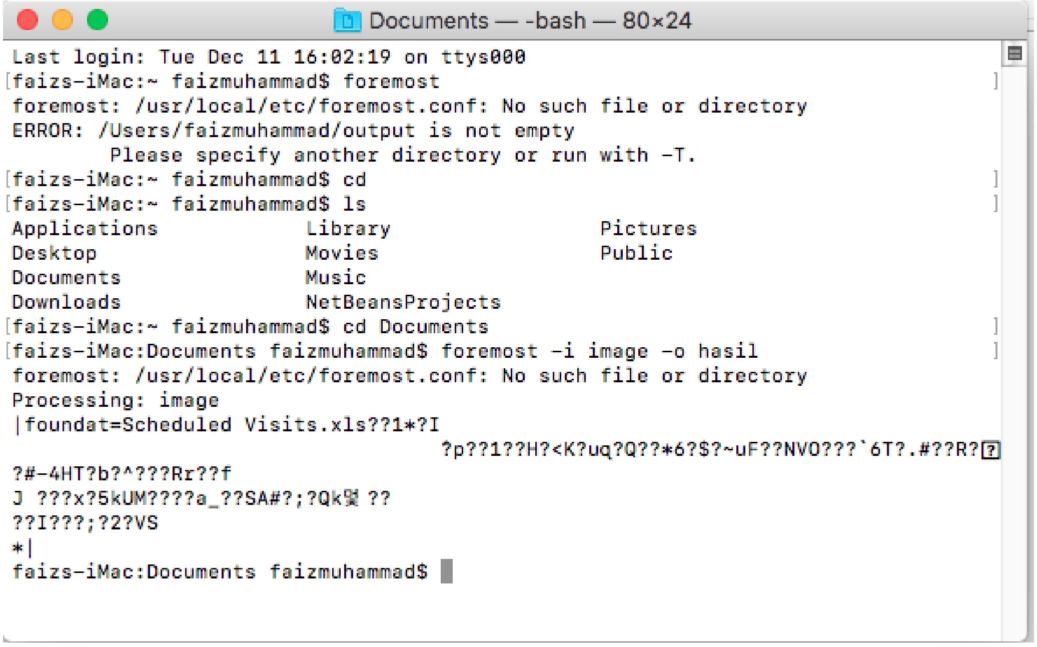
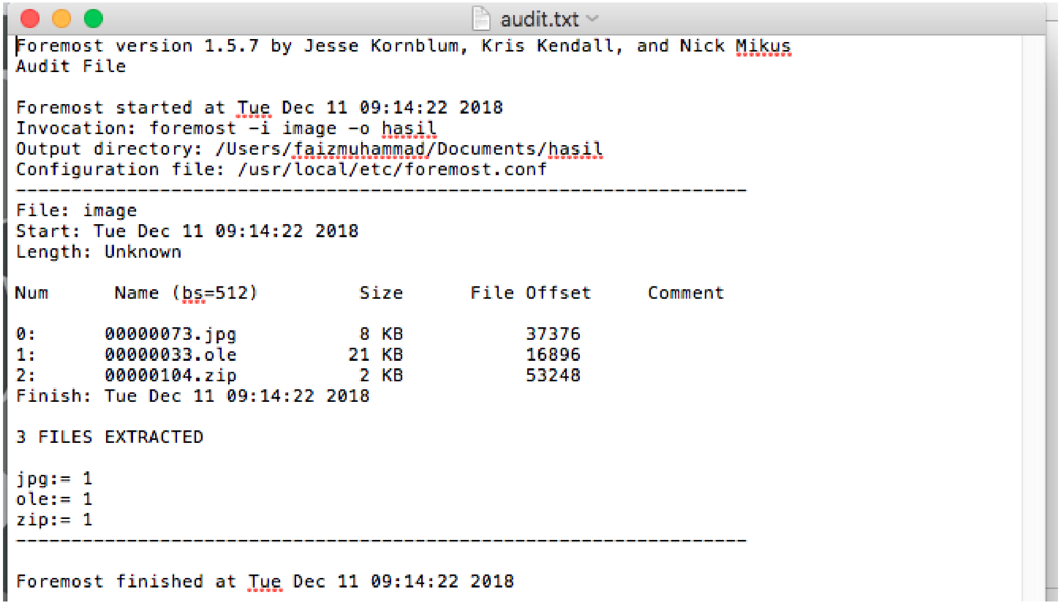
1. Kasus joe Jacob
   Alat yg digunakan : foremost, iHex, Autopsy
   OS : MacOs High Sierra

   - Gunakan foremost untuk melihat data2 dalam file image, output disimpan dalam folder “hasil”



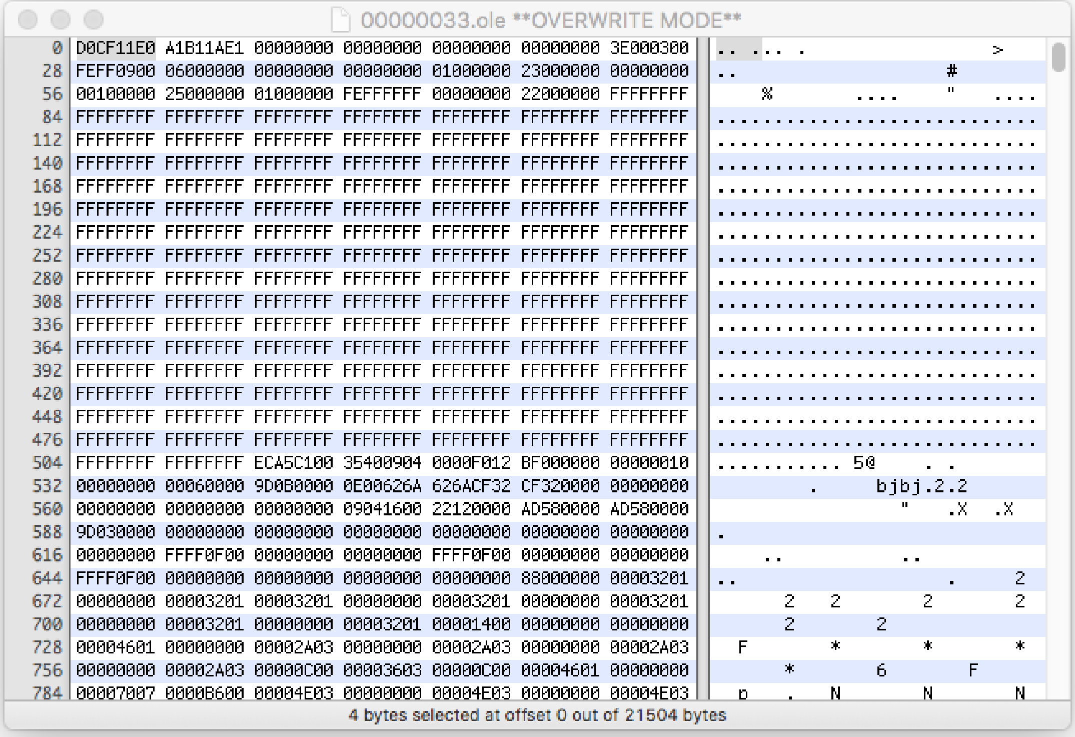
```
Last login: Tue Dec 11 16:02:19 on ttys000
[faizs-iMac:~ faizmuhammad$ foremost                                            ]
foremost: /usr/local/etc/foremost.conf: No such file or directory
ERROR: /Users/faizmuhammad/output is not empty
        Please specify another directory or run with -T.
[faizs-iMac:~ faizmuhammad$ cd                                                  ]
[faizs-iMac:~ faizmuhammad$ ls                                                  ]
Applications            Library                 Pictures
Desktop                 Movies                  Public
Documents               Music
Downloads               NetBeansProjects
[faizs-iMac:~ faizmuhammad$ cd Documents                                        ]
[faizs-iMac:Documents faizmuhammad$ foremost -i image -o hasil                  ]
foremost: /usr/local/etc/foremost.conf: No such file or directory
Processing: image
|foundat=Scheduled Visits.xls??1*?I
                                   ?p??1??H?<K?uq?Q??*6?$?~uF??NVO???`6T?.#??R??
?#-4HT?b?^???Rr??f
J ???x?5kUM????a_??SA#?;?Qk ??
??I???;?2?VS
*|
faizs-iMac:Documents faizmuhammad$ 
```

   - Terdapat 3 file dalam image



```
Foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus
Audit File

Foremost started at Tue Dec 11 09:14:22 2018
Invocation: foremost -i image -o hasil
Output directory: /Users/faizmuhammad/Documents/hasil
Configuration file: /usr/local/etc/foremost.conf
------------------------------------------------------------------
File: image
Start: Tue Dec 11 09:14:22 2018
Length: Unknown

Num      Name (bs=512)         Size      File Offset     Comment

0:      00000073.jpg          8 KB          37376
1:      00000033.ole         21 KB          16896
2:      00000104.zip          2 KB          53248
Finish: Tue Dec 11 09:14:22 2018

3 FILES EXTRACTED

jpg:= 1
ole:= 1
zip:= 1
------------------------------------------------------------------

Foremost finished at Tue Dec 11 09:14:22 2018
```

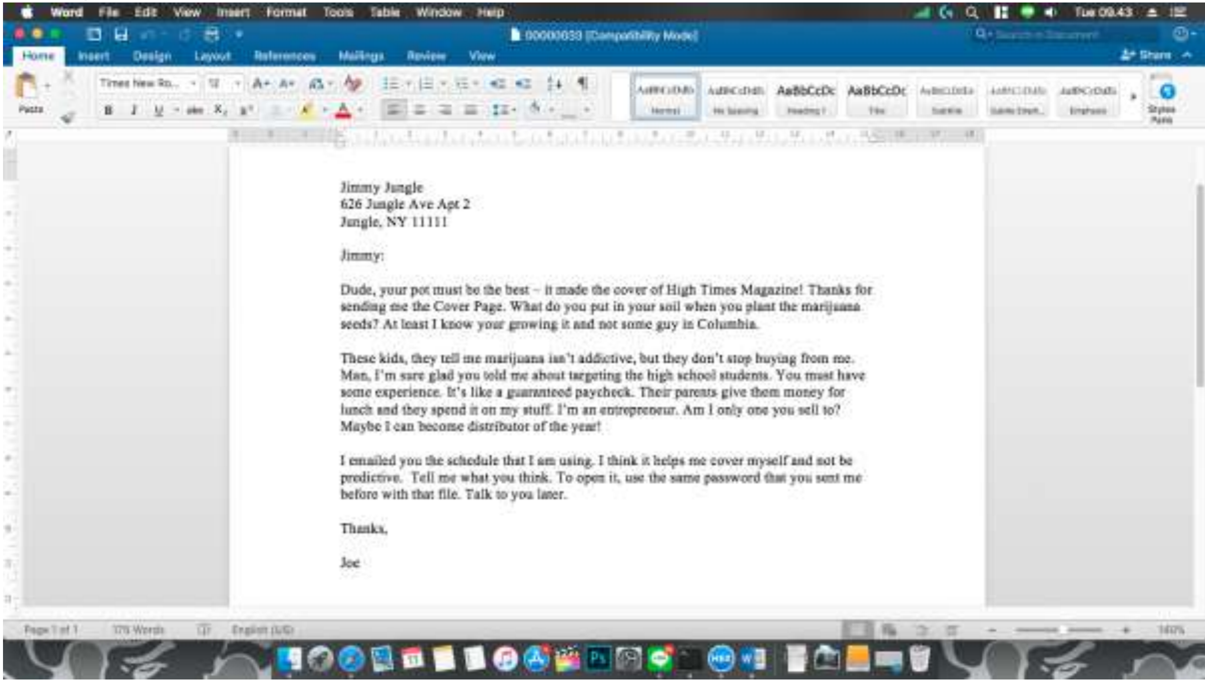
   - Karena file .ole tidak tidak dapat dibuka, maka dilihat dlu File signaturenya menggunakan iHex.



```
  0 D0CF11E0 A1B11AE1 00000000 00000000 00000000 00000000 3E000300 .. ... .                >
 28 FEFF0900 06000000 00000000 00000000 01000000 23000000 00000000 ..                     #
 56 00100000 25000000 01000000 FEFFFFFF 00000000 22000000 FFFFFFFF     %       ....   "   ....
 84 FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF ............................
112 FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF ............................
140 FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF ............................
168 FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF ............................
196 FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF ............................
224 FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF ............................
252 FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF ............................
280 FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF ............................
308 FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF ............................
336 FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF ............................
364 FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF ............................
392 FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF ............................
420 FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF ............................
448 FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF ............................
476 FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF ............................
504 FFFFFFFF FFFFFFFF ECA5C100 35400904 0000F012 BF000000 00000010 ........... 5@    . .
532 00000000 00060000 9D0B0000 0E00626A 626ACF32 CF320000 00000000            .    bjbj.2.2
560 00000000 00000000 00000000 09041600 22120000 AD580000 AD580000                  "   .X   .X
588 9D030000 00000000 00000000 00000000 00000000 00000000 00000000 .
616 00000000 FFFF0F00 00000000 00000000 FFFF0F00 00000000 00000000     ..          ..
644 FFFF0F00 00000000 00000000 00000000 00000000 88000000 00003201 ..                    .   2
672 00000000 00003201 00003201 00000000 00003201 00000000 00003201       2   2       2       2
700 00000000 00003201 00000000 00003201 00001400 00000000 00000000       2       2
728 00004601 00000000 00002A03 00000000 00002A03 00000000 00002A03   F       *       *       *
756 00000000 00002A03 00000C00 00003603 00000C00 00004601 00000000       *       6       F
784 00007007 0000B600 00004E03 00000000 00004E03 00000000 00004E03   p   .   N       N       N
```

4 bytes selected at offset 0 out of 21504 bytes

- File tersebut memiliki header untuk file office, maka dicoba untuk dibuka menngunakan word



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!

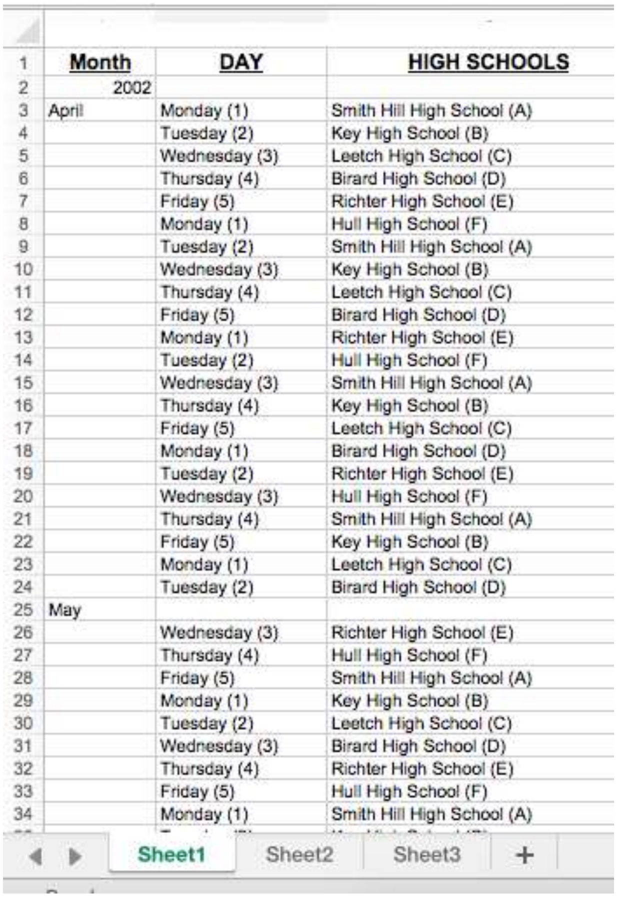
I emailed you the schedule that I am using. I think it helps me cover myself and not be predictive. Tell me what you think. To open it, use the same password that you sent me before with that file. Talk to you later.

Thanks,

Joe

- Terdapat pesan dari supplier joe, termasuk nama dan alamatnya.
- Selanjutnya pada cover page.jpg ketika dibuka dengan ihex terdapat "pw=goodtimes" yg kemungkinan adalah password yg disebutkan pada surat diatas.

- Selanjutnya file scheduled visit, ketika dicek signaturenya dengan ihex ternyata merupakan file zip.
- Ketika mencoba membuka file zip tsb, terdapat password, kemudian dicoba menggunakan password “goodtimes”
- Setelah dibuka, didalam file zip tsb diketahui sekolah2 lain tempat joe berjualan marijuana



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)

soal:

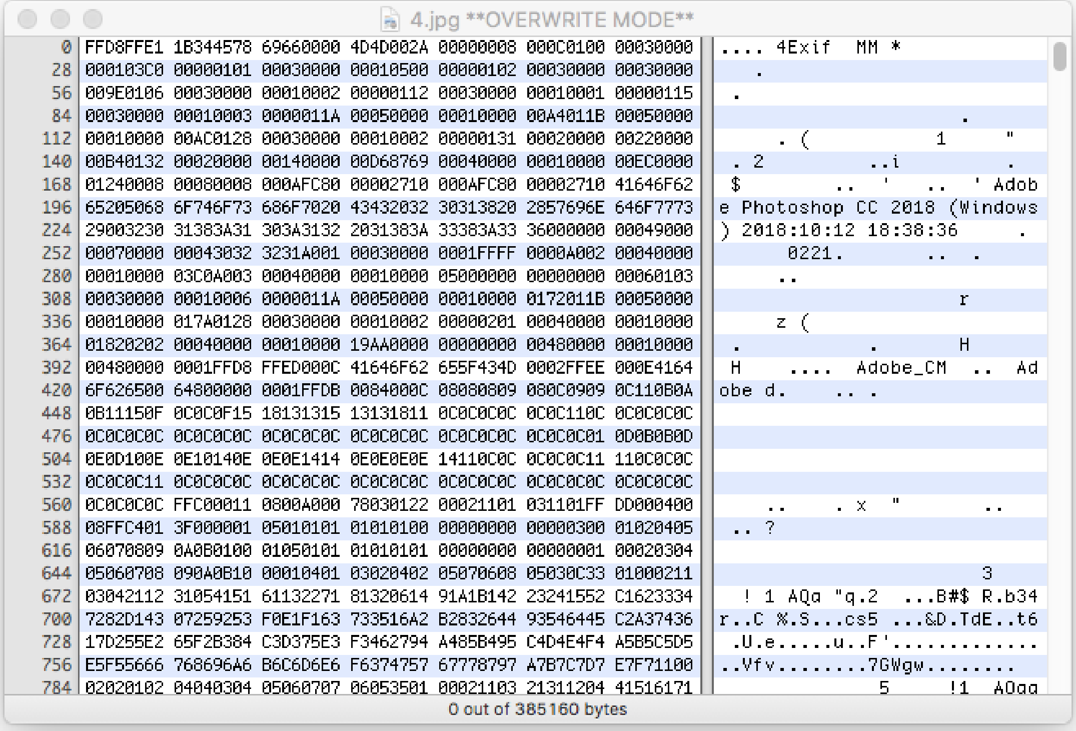
1. Who is Joe Jacob's supplier of marijuana and what is the address listed for the supplier?
   Jimmy jungle,
   626 Jungle Ave Apt 2 Jungle, NY 11111
2. What crucial data is available within the coverpage.jpg file and why is this data crucial?
   Password : goodtimes, karena pass itu merupakan password untuk file zip yg berisi jadwal tempat berjualan 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?
   Jimmyjungle.doc -> dihapus
   Cover page.jpgc - > sebenarnya merupakan file jpg

Scheduled visits.exe -> sebenarnya merupakan file zip yg dipassword yang didalamnya terdapat file xls.

5. What processes did you (the investigator) use to successfully examine the entire contents of each file?
   Dijelaskan diatas

2. Soal analisis foto
   Alat yang digunakan : iHex
   Operating system : MacOS High Sierra

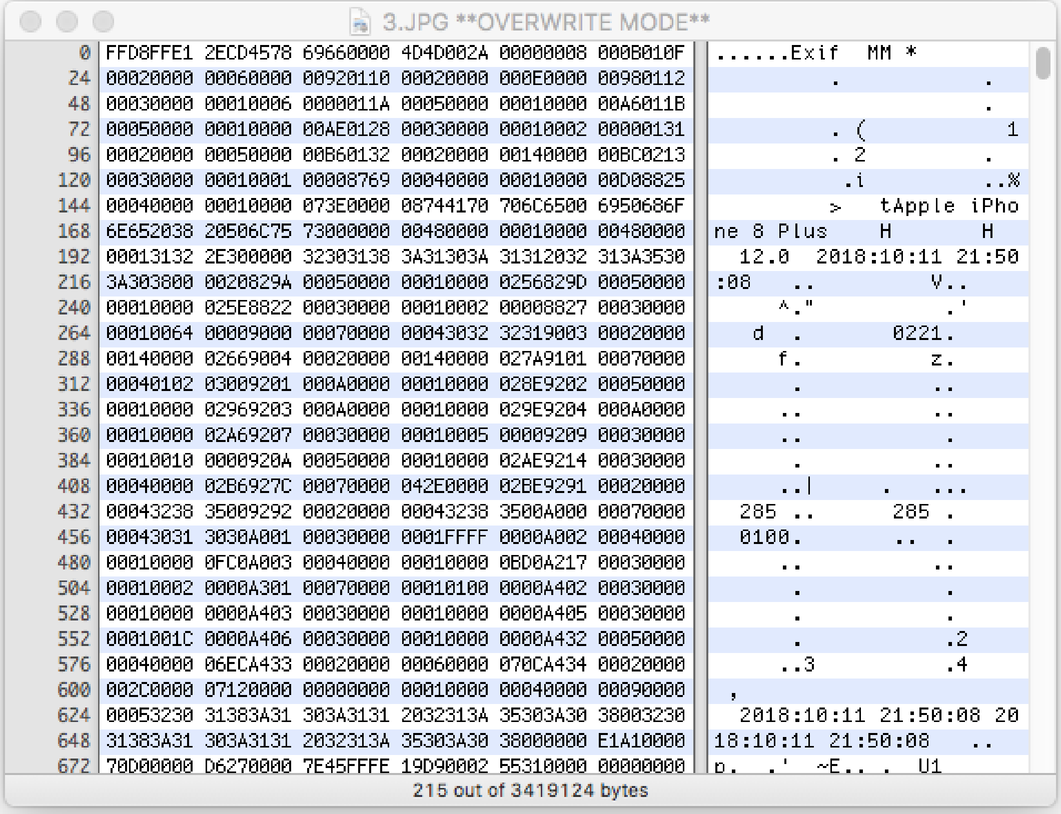
   Kedua file dibuka menggunakan iHex, terlihat bahwa file foto 4.jpg merupakan hasil editan dengan photoshop CC 2018 dengan operating system windows



```
  0 FFD8FFE1 1B344578 69660000 4D4D002A 00000008 000C0100 00030000  .... 4Exif  MM *
 28 000103C0 00000101 00030000 00010500 00000102 00030000 00030000     .
 56 009E0106 00030000 00010002 00000112 00030000 00010001 00000115   .
 84 00030000 00010003 0000011A 00050000 00010000 00A4011B 00050000                      .
112 00010000 00AC0128 00030000 00010002 00000131 00020000 00220000       . (          1     "
140 00B40132 00020000 00140000 00D68769 00040000 00010000 00EC0000   . 2        ..i          .
168 01240008 00080008 000AFC80 00002710 000AFC80 00002710 41646F62   $         ..  '   ..  ' Adob
196 65205068 6F746F73 686F7020 43432032 30313820 2857696E 646F7773  e Photoshop CC 2018 (Windows
224 29003230 31383A31 303A3132 2031383A 33383A33 36000000 00049000  ) 2018:10:12 18:38:36      .
252 00070000 00043032 3231A001 00030000 0001FFFF 0000A002 00040000        0221.         ..  .
280 00010000 03C0A003 00040000 00010000 05000000 00000000 00060103       ..
308 00030000 00010006 0000011A 00050000 00010000 0172011B 00050000                      r
336 00010000 017A0128 00030000 00010002 00000201 00040000 00010000       z (
364 01820202 00040000 00010000 19AA0000 00000000 00480000 00010000   .           .       H
392 00480000 0001FFD8 FFED000C 41646F62 655F434D 0002FFEE 000E4164   H     ....  Adobe_CM  ..  Ad
420 6F626500 64800000 0001FFDB 0084000C 08080809 080C0909 0C110B0A  obe d.     .. .
448 0B11150F 0C0C0F15 18131315 13131811 0C0C0C0C 0C0C110C 0C0C0C0C
476 0C0C0C0C 0C0C0C0C 0C0C0C0C 0C0C0C0C 0C0C0C0C 0C0C0C01 0D0B0B0D
504 0E0D100E 0E10140E 0E0E1414 0E0E0E0E 14110C0C 0C0C0C11 110C0C0C
532 0C0C0C11 0C0C0C0C 0C0C0C0C 0C0C0C0C 0C0C0C0C 0C0C0C0C 0C0C0C0C
560 0C0C0C0C FFC00011 0800A000 78030122 00021101 031101FF DD000400      ..     . x  "        ..
588 08FFC401 3F000001 05010101 01010100 00000000 00000300 01020405   .. ?
616 06070809 0A0B0100 01050101 01010101 00000000 00000001 00020304
644 05060708 090A0B10 00010401 03020402 05070608 05030C33 01000211                         3
672 03042112 31054151 61132271 81320614 91A1B142 23241552 C1623334    ! 1 AQa "q.2  ...B#$ R.b34
700 7282D143 07259253 F0E1F163 733516A2 B2832644 93546445 C2A37436  r..C %.S...cs5 ...&D.TdE..t6
728 17D255E2 65F2B384 C3D375E3 F3462794 A485B495 C4D4E4F4 A5B5C5D5   .U.e.....u..F'............
756 E5F55666 768696A6 B6C6D6E6 F6374757 67778797 A7B7C7D7 E7F71100  ..Vfv........7GWgw........
784 02020102 04040304 05060707 06053501 00021103 21311204 41516171                 5      !1  AQqq
```

0 out of 385160 bytes

Sedangkan foto 3.jpg merupakan foto asli yang diambil menggunakan iPhone 8 plus



3.JPG **OVERWRITE MODE**

```
  0 FFD8FFE1 2ECD4578 69660000 4D4D002A 00000008 000B010F  ......Exif  MM *
 24 00020000 00060000 00920110 00020000 000E0000 00980112           .           .
 48 00030000 00010006 0000011A 00050000 00010000 00A6011B                       .
 72 00050000 00010000 00AE0128 00030000 00010002 00000131           . (           1
 96 00020000 00050000 00B60132 00020000 00140000 00BC0213           . 2         .
120 00030000 00010001 00008769 00040000 00010000 00D08825            .i         ..%
144 00040000 00010000 073E0000 08744170 706C6500 6950686F           >   tApple iPho
168 6E652038 20506C75 73000000 00480000 00010000 00480000  ne 8 Plus    H       H
192 00013132 2E300000 32303138 3A31303A 31312032 313A3530    12.0  2018:10:11 21:50
216 3A303800 0020829A 00050000 00010000 0256829D 00050000  :08   ..         V..
240 00010000 025E8822 00030000 00010002 00008827 00030000       ^."          .'
264 00010064 00009000 00070000 00043032 32319003 00020000     d  .       0221.
288 00140000 02669004 00020000 00140000 027A9101 00070000       f.           z.
312 00040102 03009201 000A0000 00010000 028E9202 00050000        .          ..
336 00010000 02969203 000A0000 00010000 029E9204 000A0000       ..          ..
360 00010000 02A69207 00030000 00010005 00009209 00030000       ..           .
384 00010010 0000920A 00050000 00010000 02AE9214 00030000        .          ..
408 00040000 02B6927C 00070000 042E0000 02BE9291 00020000       ..|     .   ...
432 00043238 35009292 00020000 00043238 3500A000 00070000    285 ..      285 .
456 00043031 3030A001 00030000 0001FFFF 0000A002 00040000    0100.       ..  .
480 00010000 0FC0A003 00040000 00010000 0BD0A217 00030000       ..          ..
504 00010002 0000A301 00070000 00010100 0000A402 00030000        .           .
528 00010000 0000A403 00030000 00010000 0000A405 00030000        .           .
552 0001001C 0000A406 00030000 00010000 0000A432 00050000        .           .2
576 00040000 06ECA433 00020000 00060000 070CA434 00020000       ..3           .4
600 002C0000 07120000 00000000 00010000 00040000 00090000   ,
624 00053230 31383A31 303A3131 2032313A 35303A30 38003230    2018:10:11 21:50:08 20
648 31383A31 303A3131 2032313A 35303A30 38000000 E1A10000  18:10:11 21:50:08    ..
672 70D00000 D6270000 7E45FFFE 19D90002 55310000 00000000  p.  .'  ~E.. .  U1
```

215 out of 3419124 bytes