

Nama : M.A.Rasyid Hilmi

Jurusan :Teknik Informatika 2015

Tugas uas forensik

1.kasus joe jacob

Alat yang digunakan :hex workshop hex editor, Autopsy

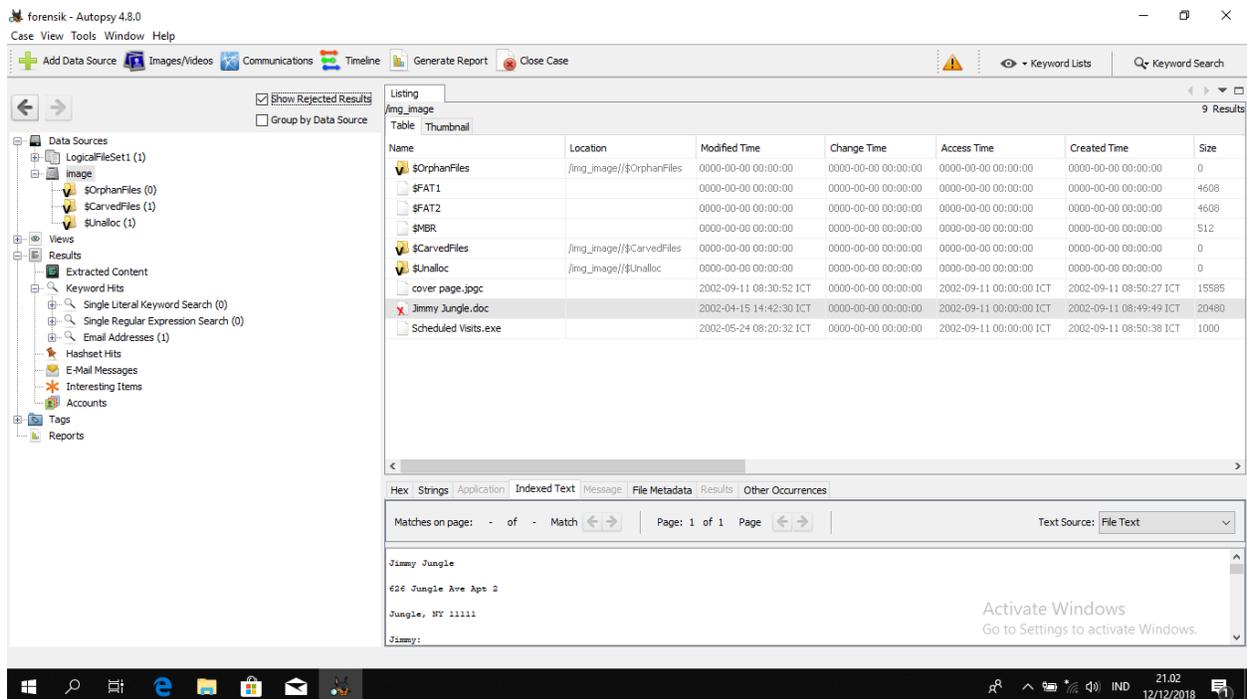
Os: WINDOWS 10 HOME 64 BIT (10.0,BUILD 17134)

SOAL IMAGE FILE

1. Who is Joe Jacob's supplier of marijuana and what is the address listed for the supplier?

Jimmy Jungle

Joe jacob's supplier is jimmy junggle, and the address listed for the supplier at 626 jungle ave apt 2, jungle,NY 11111.



The screenshot shows the Autopsy 4.8.0 interface. The main window displays a table of search results for the keyword 'Jimmy Jungle'. The results are filtered to show only the file 'Jimmy_Jungle.doc'.

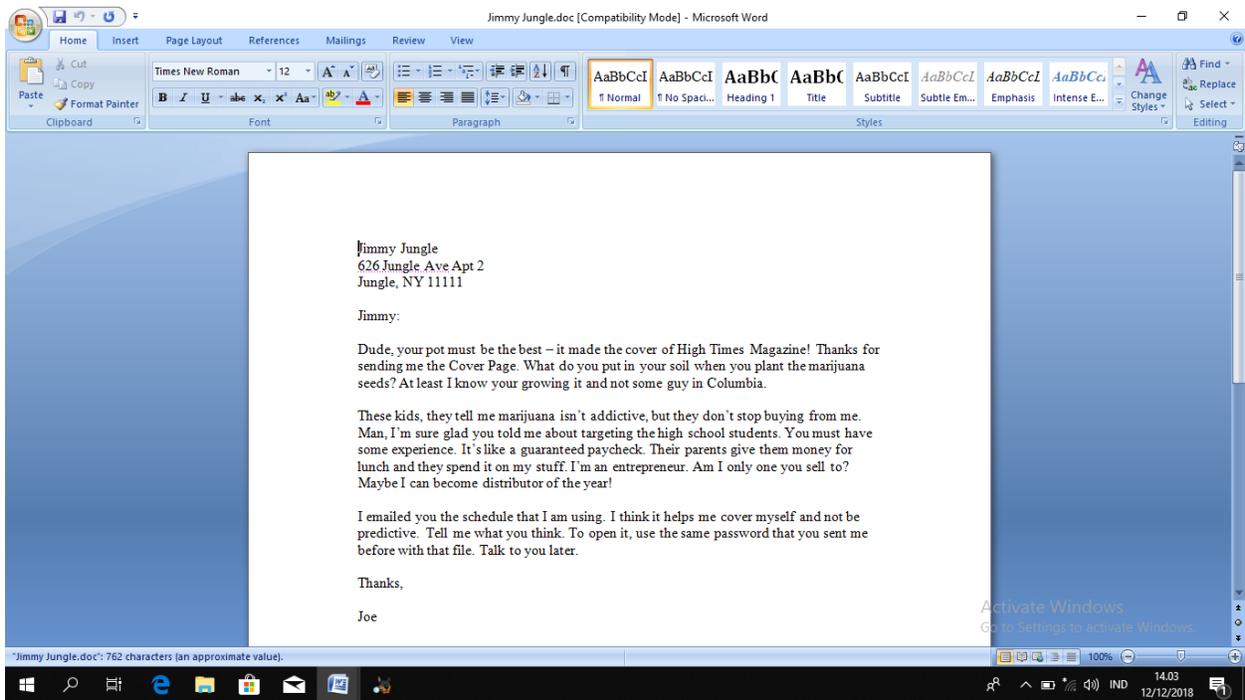
Name	Location	Modified Time	Change Time	Access Time	Created Time	Size
\$OrphanFiles	/img_image/\$OrphanFiles	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0
\$FAT1		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	4608
\$FAT2		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	4608
\$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
\$CarvedFiles	/img_image/\$CarvedFiles	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
\$Unalloc	/img_image/\$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
cover page.jpg		2002-09-11 08:30:52 ICT	0000-00-00 00:00:00	2002-09-11 00:00:00 ICT	2002-09-11 08:50:27 ICT	15585
Jimmy_Jungle.doc		2002-04-15 14:42:30 ICT	0000-00-00 00:00:00	2002-09-11 00:00:00 ICT	2002-09-11 08:49:49 ICT	20480
Scheduled Visits.exe		2002-05-24 08:20:32 ICT	0000-00-00 00:00:00	2002-09-11 00:00:00 ICT	2002-09-11 08:50:38 ICT	1000

The search results for 'Jimmy Jungle' are displayed in the 'Results' tab. The matches are:

```
Jimmy Jungle
626 Jungle Ave Apt 2
Jungle, NY 11111
Jimmy:
```

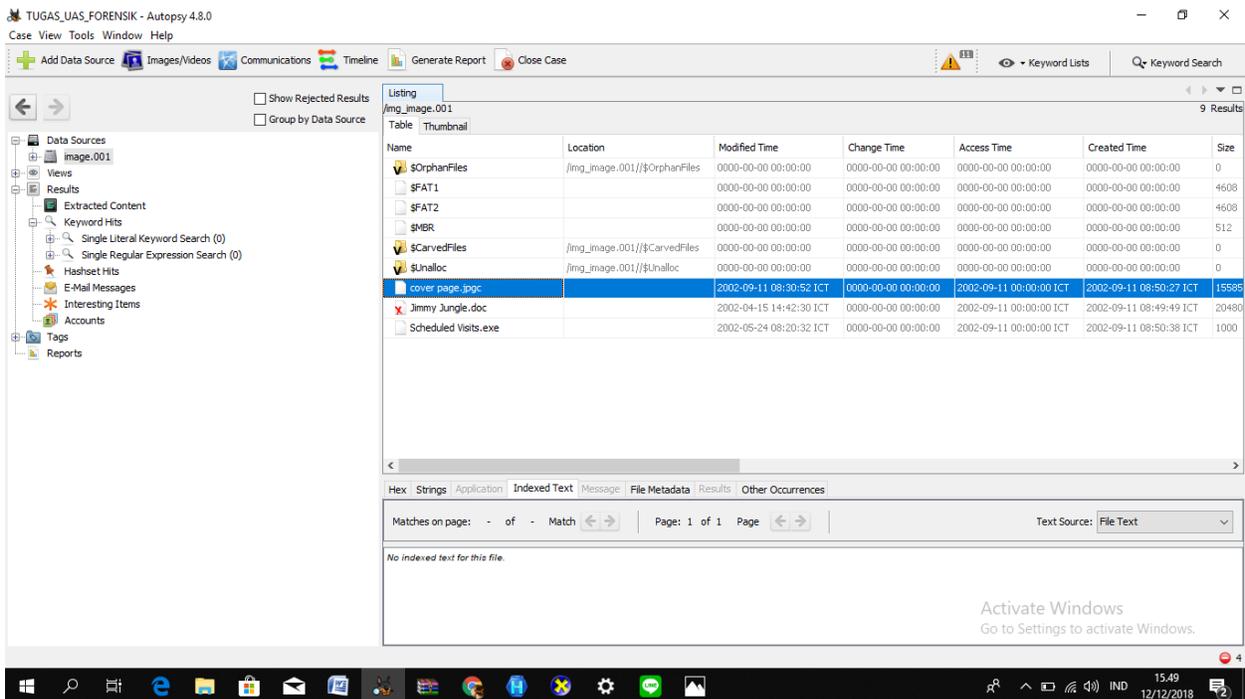
Disini ada file yang dihapus yaitu f0000000.doc

Gambar dibawah ini adalah isinya



2. What crucial data is available within the coverpage.jpg file and why is this data crucial?

Disini terdapat file cover page.jpg c lalu kita rename menjadi cover page.jpg



Pada file ini terdapat string “pw=goodtimes” yang merupakan kata sandi untuk membuka file zip yang berisi tempat jualan joe .

3. What (if any) other high schools besides Smith Hill does Joe Jacobs frequent?

Disini terdapat file scheduled visits.exe yang merupakan file scheduled visits.zip ,dimana untuk membukanya dengan password “goodtimes”

The screenshot shows the Autopsy 4.8.0 interface. The main window displays a file listing table for the image file 'img_image.001'. The table has the following columns: Name, Location, Modified Time, Change Time, Access Time, Created Time, and Size. The file 'Scheduled Visits.exe' is highlighted in blue. Below the table, there are tabs for 'Hex', 'Strings', 'Application', 'Indexed Text', 'Message', 'File Metadata', 'Results', and 'Other Occurrences'. The 'Indexed Text' tab is selected, showing 'No indexed text for this file.' The Windows taskbar at the bottom shows the date and time as 15:49 on 12/12/2018.

Name	Location	Modified Time	Change Time	Access Time	Created Time	Size
\$OrphanFiles	/img_image.001/\$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
\$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	4608
\$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	4608
\$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
\$CarvedFiles	/img_image.001/\$CarvedFiles	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
\$Unalloc	/img_image.001/\$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
cover page.jpgc		2002-09-11 08:30:52 ICT	0000-00-00 00:00:00	2002-09-11 00:00:00 ICT	2002-09-11 08:50:27 ICT	15585
Jimmy Jungle.doc		2002-04-15 14:42:30 ICT	0000-00-00 00:00:00	2002-09-11 00:00:00 ICT	2002-09-11 08:49:49 ICT	20480
Scheduled Visits.exe		2002-05-24 08:20:32 ICT	0000-00-00 00:00:00	2002-09-11 00:00:00 ICT	2002-09-11 08:50:38 ICT	1000

Didalam file tadi terdapat daftar nama sekolah lain tempat joe berjualan marijuana.yaitu :leetch high school,birard high school ,richter high school ,key high school dan hull high school

	Month	DAY	HIGH SCHOOLS
1			
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)

4. For each file, what processes were taken by the suspect to mask them from others?

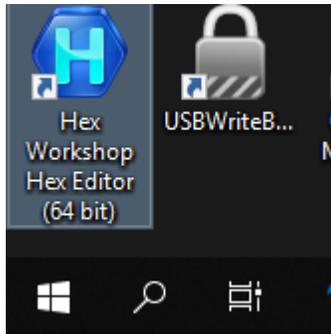
File Jimmyjungle.doc → dihapus

File Cover page.jpg → aslinya Cover page.jpg, didalamnya terdapat password “goodtimes”

File Scheduled visits.exe → aslinya Scheduled.zip, didalamnya terdapat file xls

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

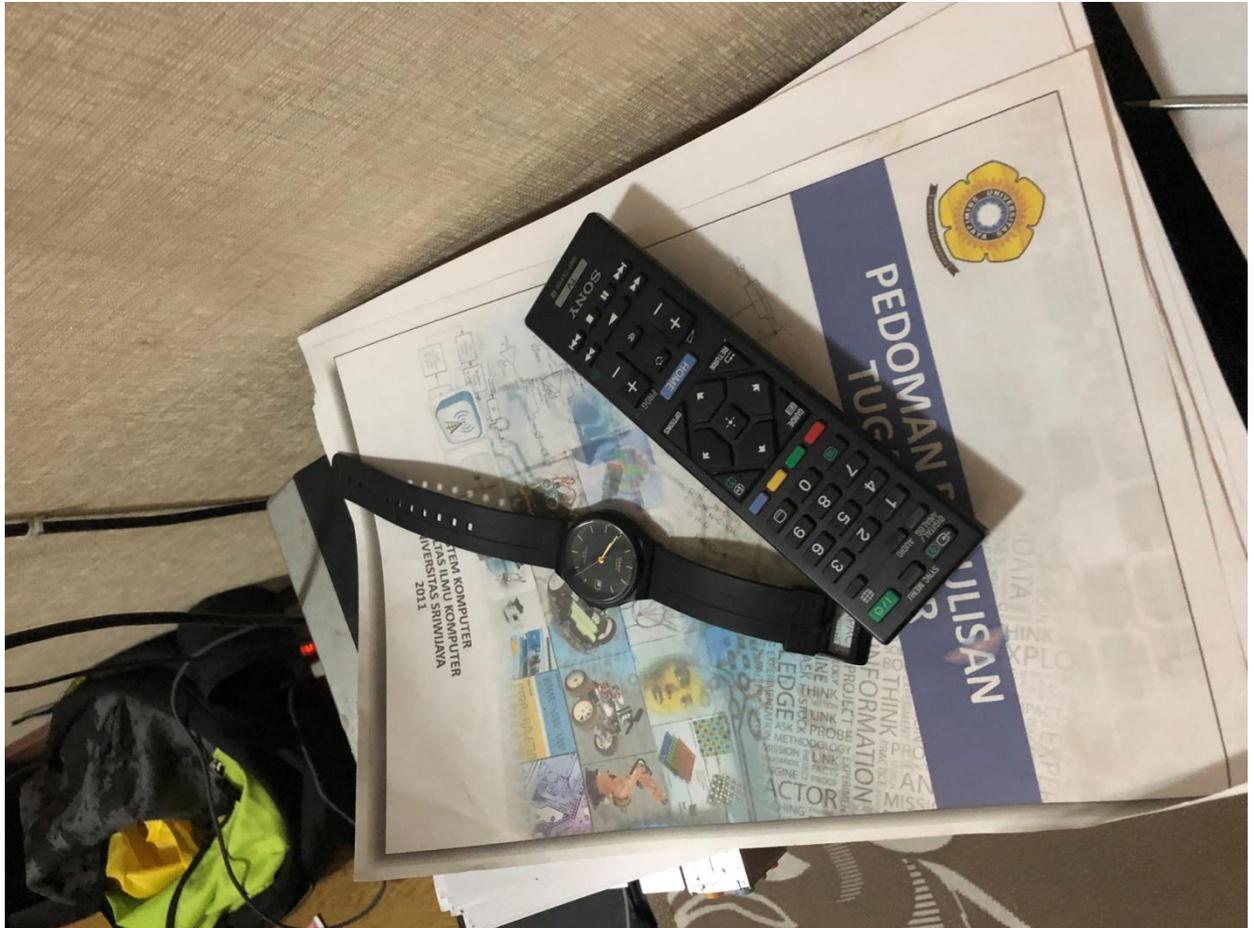
Saya menganalisa bukti dengan menggunakan software Autopsy 4.8.0 yang berjudul Tugas_UAS_FORENSIK . Saya juga menggunakan software Hex Workshop Hex Editor untuk menemukan password yang tersembunyi.



SOAL ANALISIS FOTO

Foto 3.jpg merupakan foto asli yang diambil dengan menggunakan Apple Iphone 8 Plus pada tanggal 11 Oktober 2018 pukul 21:50:08

Dibuka dengan menggunakan software Hex Workshop



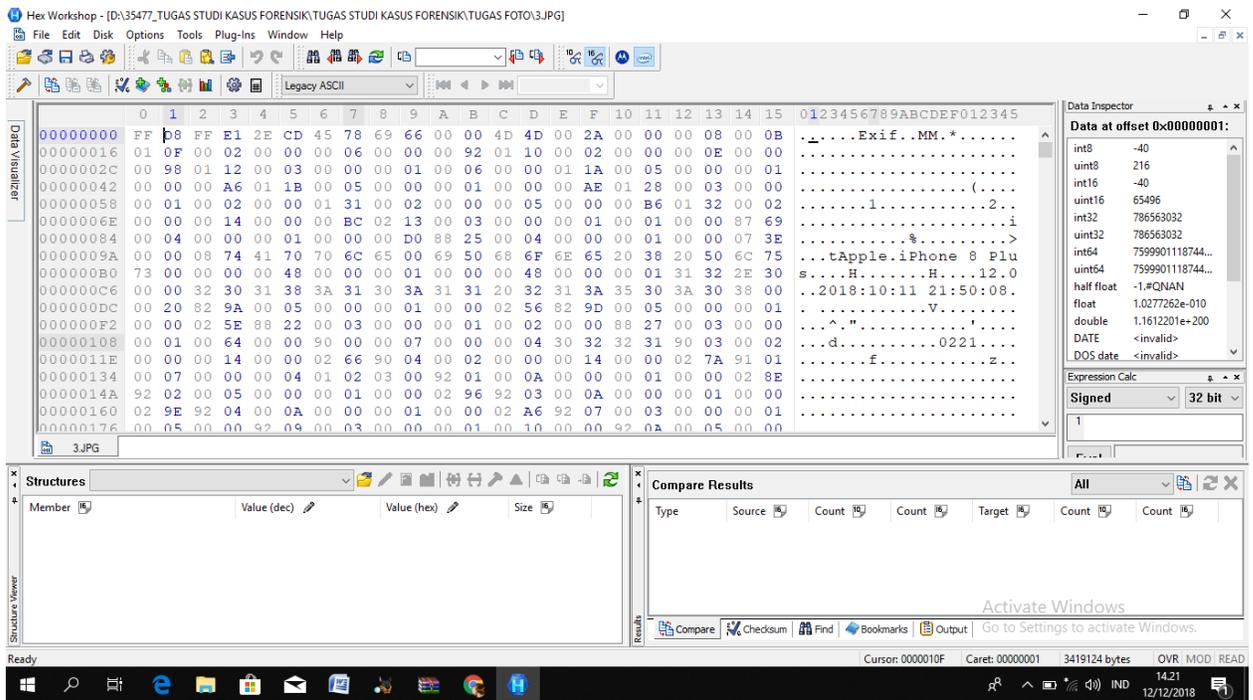
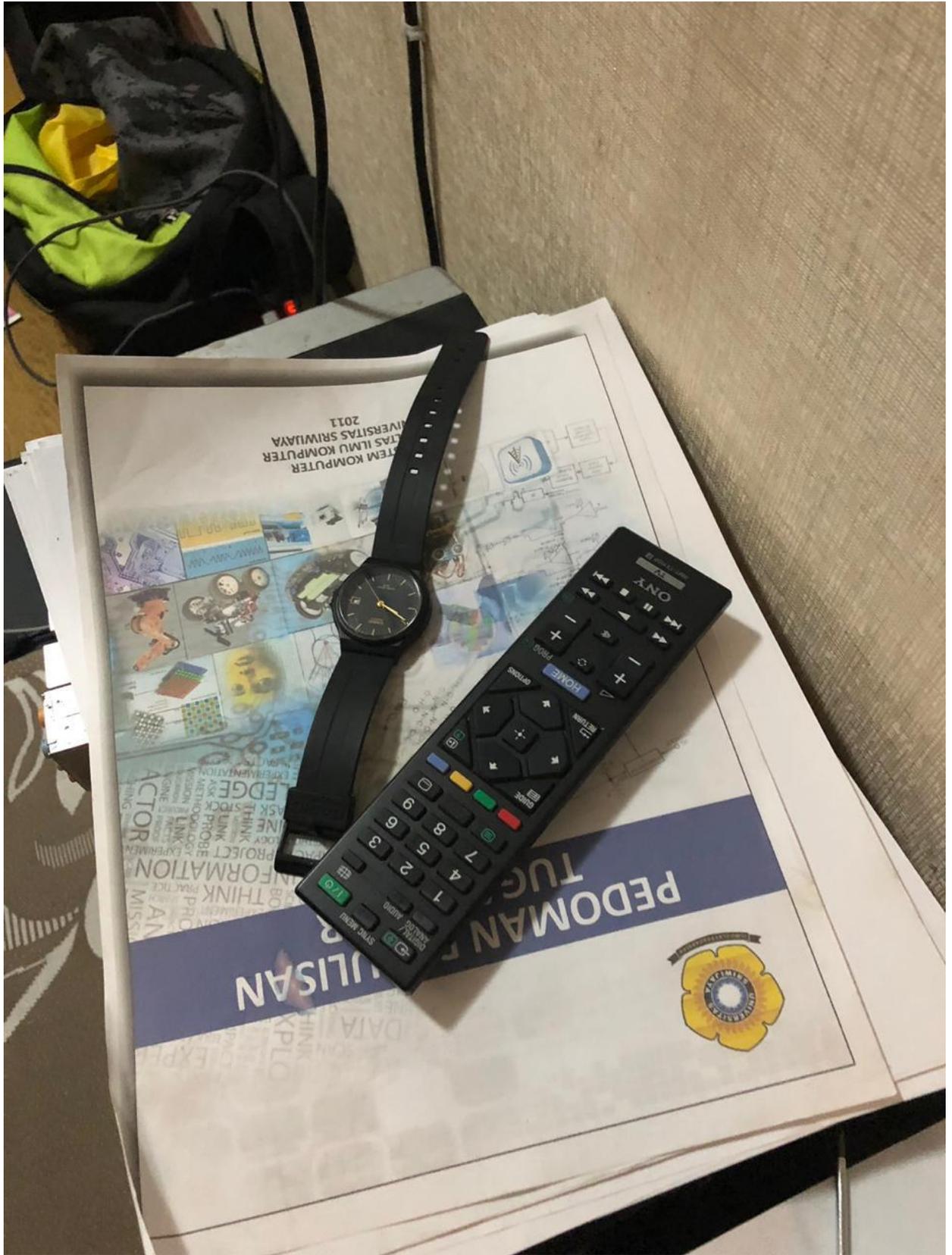


Foto 4.jpg merupakan foto yang telah diedit dengan menggunakan Adobe Photoshop CC 2018 (Windows) pada tanggal 2 Oktober 2018 pukul 18:38:36
Dibuka dengan menggunakan software Hex Workshop



Hex Workshop - [D:\35477_TUGAS STUDI KASUS FORENSIK\TUGAS STUDI KASUS FORENSIK\TUGAS FOTO4.jpg]

File Edit Disk Options Tools Plug-Ins Window Help

Legacy ASCII

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	10	11	12	13	14	15	
00000000	FF	D8	FF	E1	1B	34	45	78	69	66	00	00	4D	4D	00	2A	00	00	00	08	00	0C
00000016	01	00	00	03	00	00	00	01	03	C0	00	00	01	01	00	03	00	00	00	01	05	00
0000002C	00	00	01	02	00	03	00	00	00	03	00	00	00	00	9E	01	06	00	03	00	00	01
00000042	00	02	00	00	01	12	00	03	00	00	00	01	00	01	00	00	01	15	00	03	00	00
00000058	00	01	00	03	00	00	01	1A	00	05	00	00	00	01	00	00	00	A4	01	1B	00	05
0000006E	00	00	00	01	00	00	00	AC	01	28	00	03	00	00	00	01	00	02	00	00	01	31
00000084	00	02	00	00	00	22	00	00	00	B4	01	32	00	02	00	00	00	14	00	00	00	D6
0000009A	87	69	00	04	00	00	00	01	00	00	00	EC	00	00	01	24	00	08	00	08	00	08
000000B0	00	0A	FC	80	00	00	27	10	00	0A	FC	80	00	00	27	10	41	64	6F	62	65	20
000000C6	50	68	6F	74	6F	73	68	6F	70	20	43	43	20	32	30	31	38	20	28	57	69	6E
000000DC	64	6F	77	73	29	00	32	30	31	38	3A	31	30	3A	31	32	20	31	38	3A	33	38
000000F2	3A	33	36	00	00	00	00	04	90	00	00	07	00	00	00	04	30	32	32	31	A0	01
00000108	00	03	00	00	00	01	FF	FF	00	00	A0	02	00	04	00	00	00	01	00	00	03	C0
0000011E	A0	03	00	04	00	00	00	01	00	00	05	00	00	00	00	00	00	00	00	06	01	03
00000134	00	03	00	00	00	01	00	06	00	00	01	1A	00	05	00	00	00	01	00	00	01	72
0000014A	01	1B	00	05	00	00	00	01	00	00	01	7A	01	28	00	03	00	00	00	01	00	02
00000160	00	00	02	01	00	04	00	00	00	01	00	00	01	82	02	02	00	04	00	00	00	01
00000176	00	00	19	AA	00	00	00	00	00	00	00	00	48	00	00	00	01	00	00	00	48	00

0123456789ABCDEF012345

Data Inspector

Data at offset 0x00000000:

- int8 -1
- uint8 255
- int16 -9985
- uint16 55551
- int32 -50326465
- uint32 3791640831
- int64 8666390352304...
- uint64 8666390352304...
- half float -159.875
- float -5.8994449e+020
- double 2.2403439e+271
- DATE <invalid>
- DOS date 31/07/2088

Expression Calc

Signed 32 bit

1

Structures

Member	Value (dec)	Value (hex)	Size
--------	-------------	-------------	------

Compare Results

Type	Source	Count	Count	Target	Count	Count
------	--------	-------	-------	--------	-------	-------

Activate Windows

Ready

Cursor: 000000A4 Caret: 00000000 385160 bytes OVR MOD READ

14.22 12/12/2018