Nama : M.A.Rasyid Hilmi

Jurusan :Teknik Informatika 2015

Tugas uas forensik

1.kasus joe jacob

Alat yang digunakan :hex workshop hex editor, Autopsy

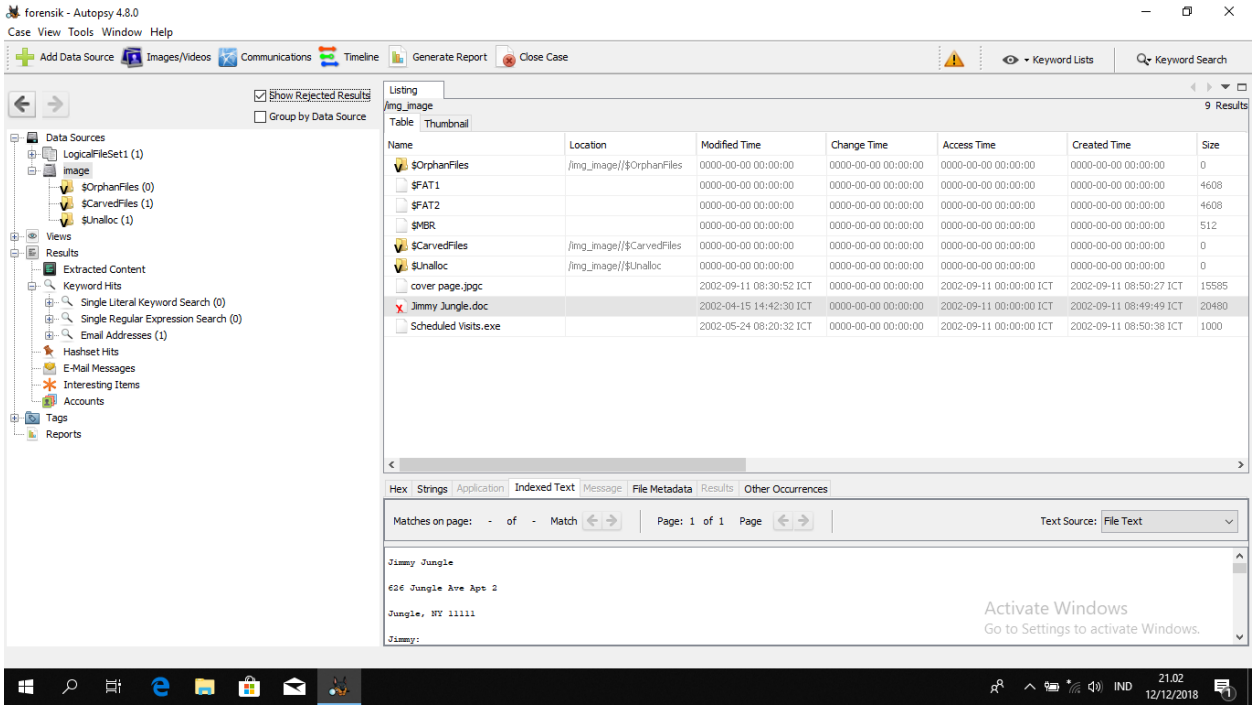
Os: WINDOWS 10 HOME 64 BIT (10.0,BUILD 17134)

SOAL IMAGE FILE

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

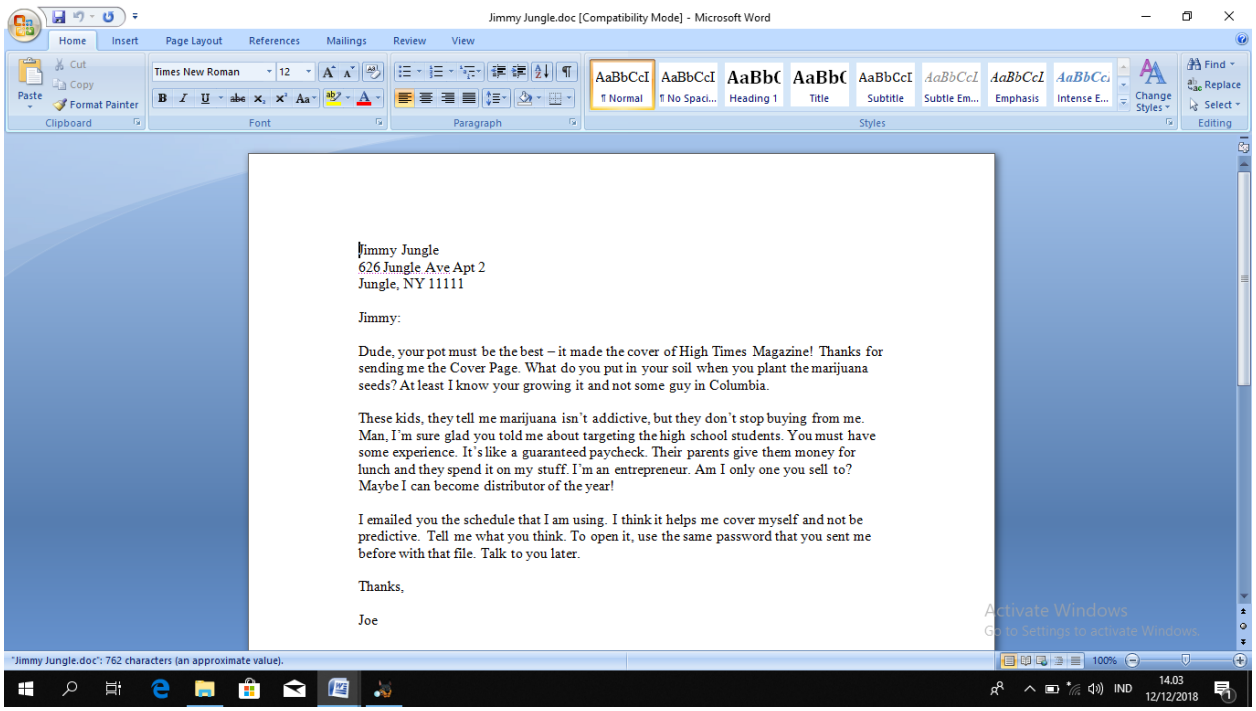
   Jimmy Jungle

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



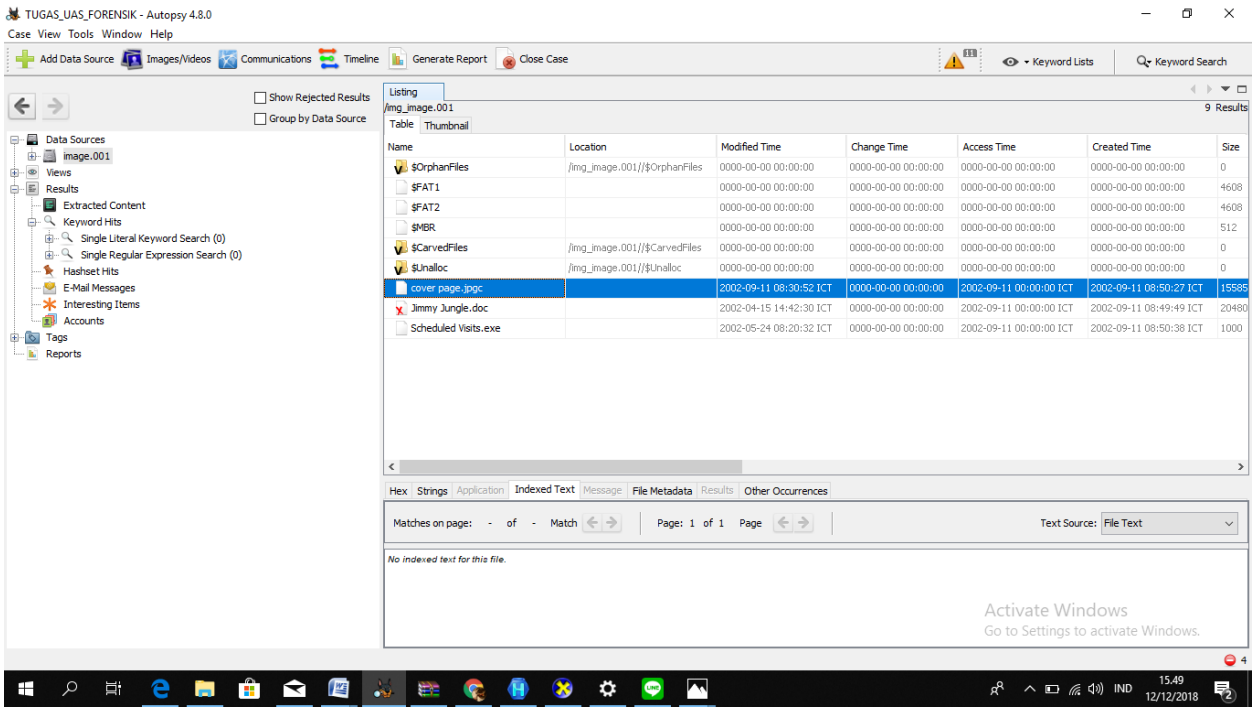
Disini ada file yang dihapus yaitu f0000000.doc

Gambar dibawah ini adalah isinya



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

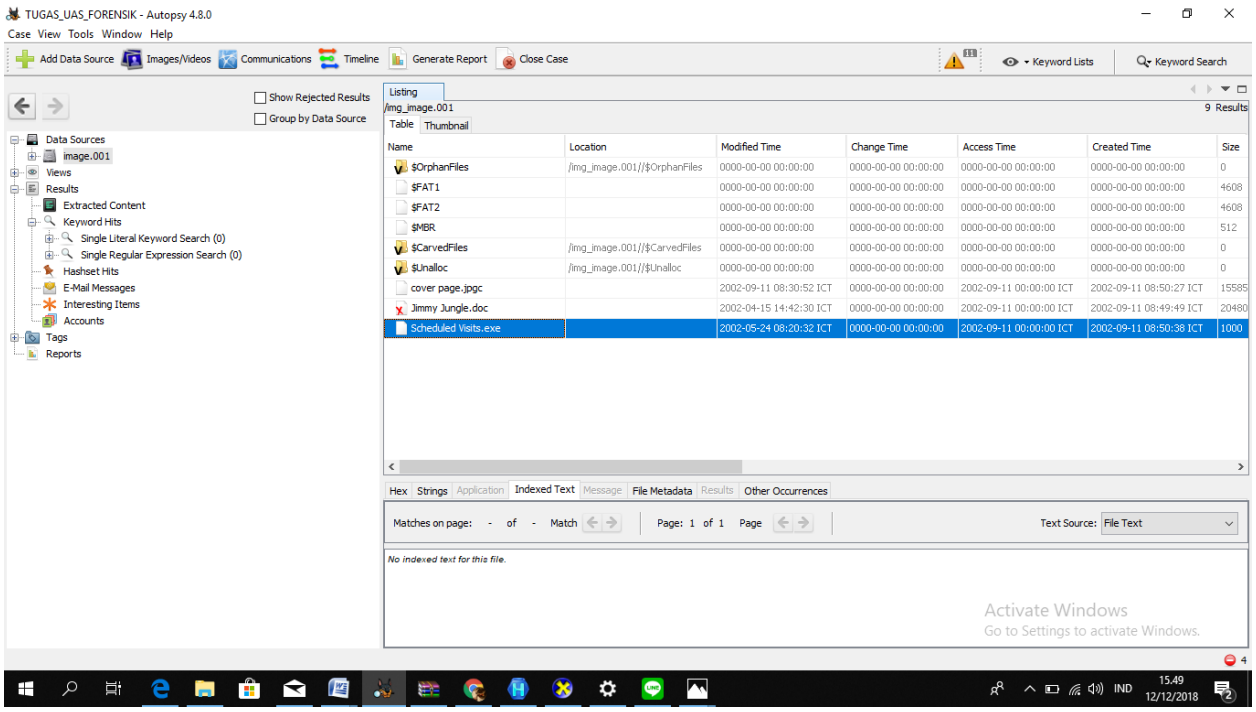
Disini terdapat file cover page.jpg c lalu kita rename menjadi cover page.jpg



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”



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
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)

Sheet1 Sheet2 Sheet3

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

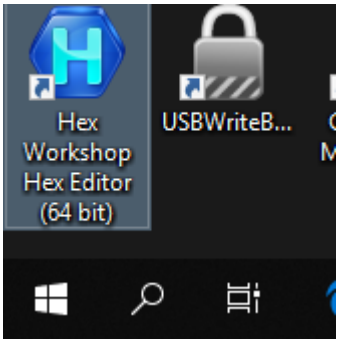
File Jimmyjungle.doc → dihapus

File Cover page.jpgc → 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?

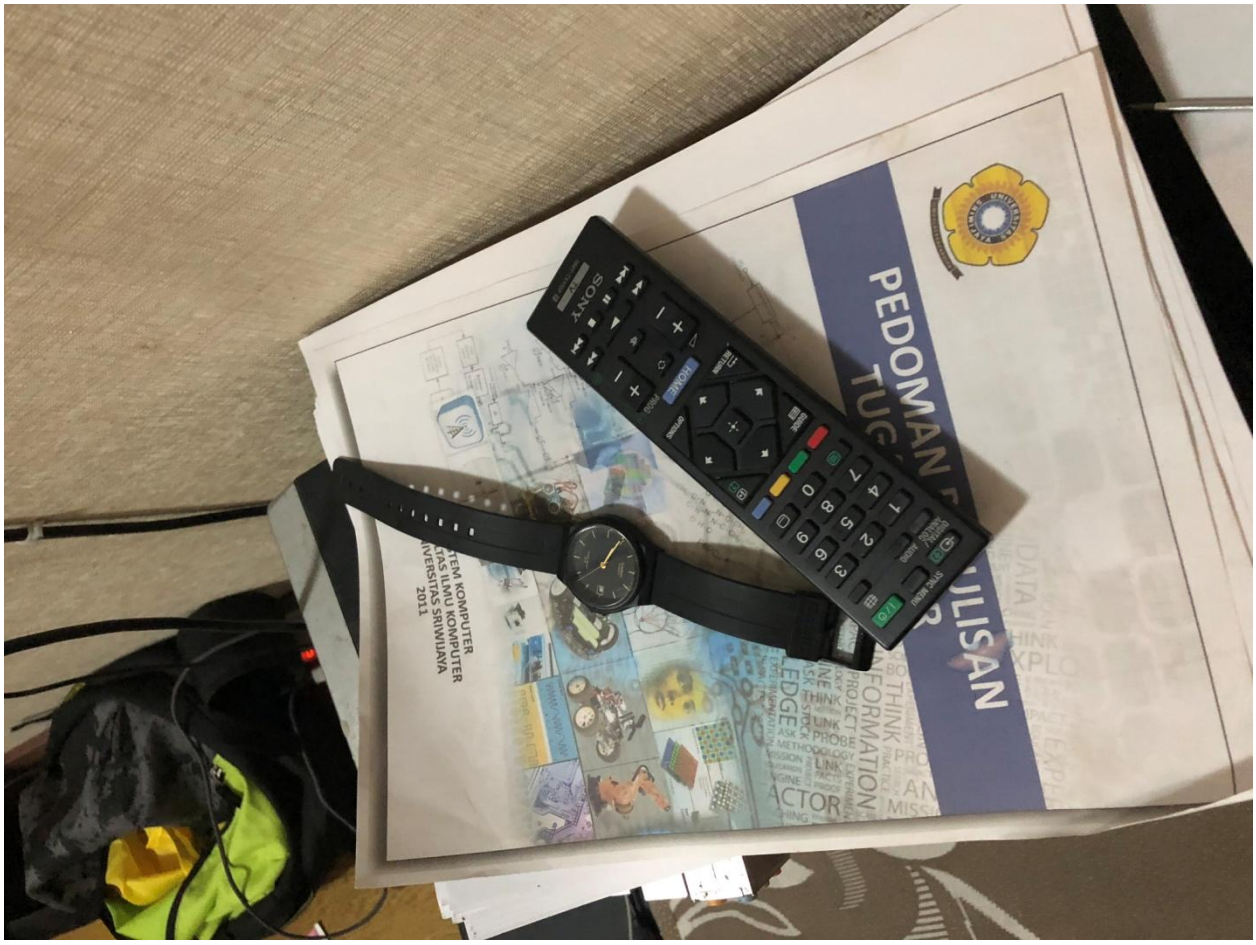
   Saya menganalisa bukti dengan menggunakan software Autopsy 4.8.0 yang berjudul Tugas_UAS_FORENSIK . Saya juga menggunakan software Hex Workshop Hex Editor untuk menemukan password yang tersembunyi.



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



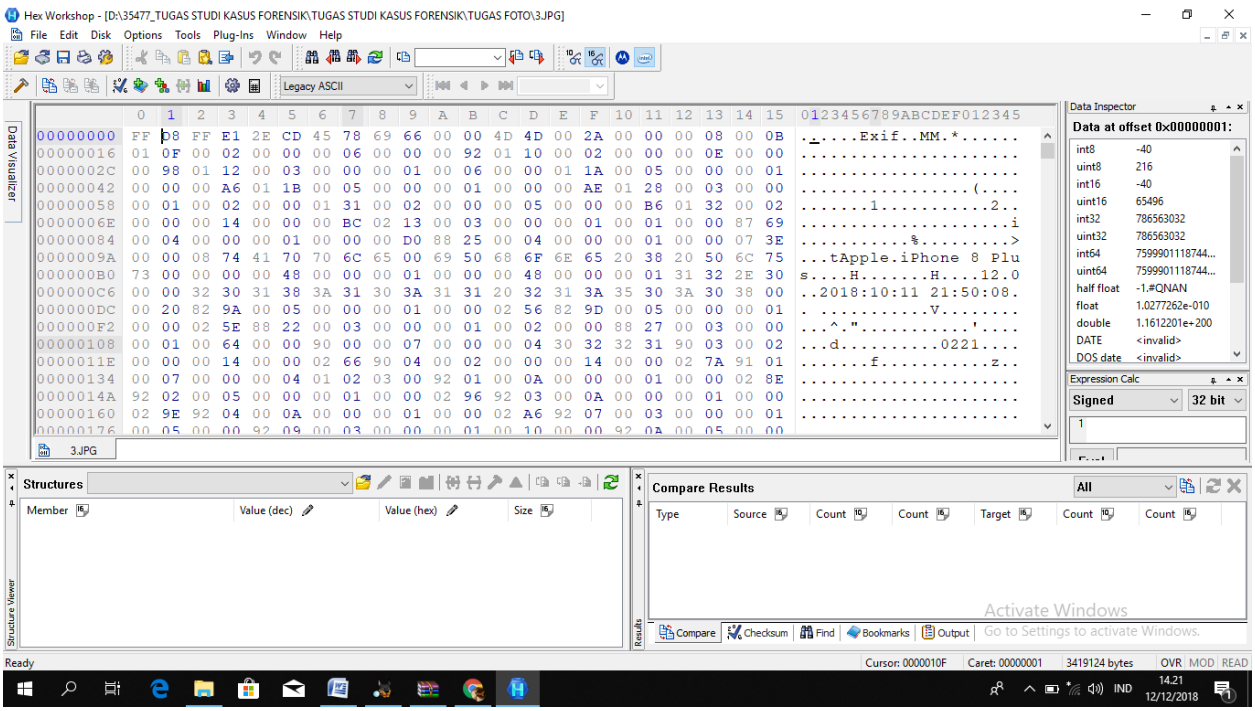
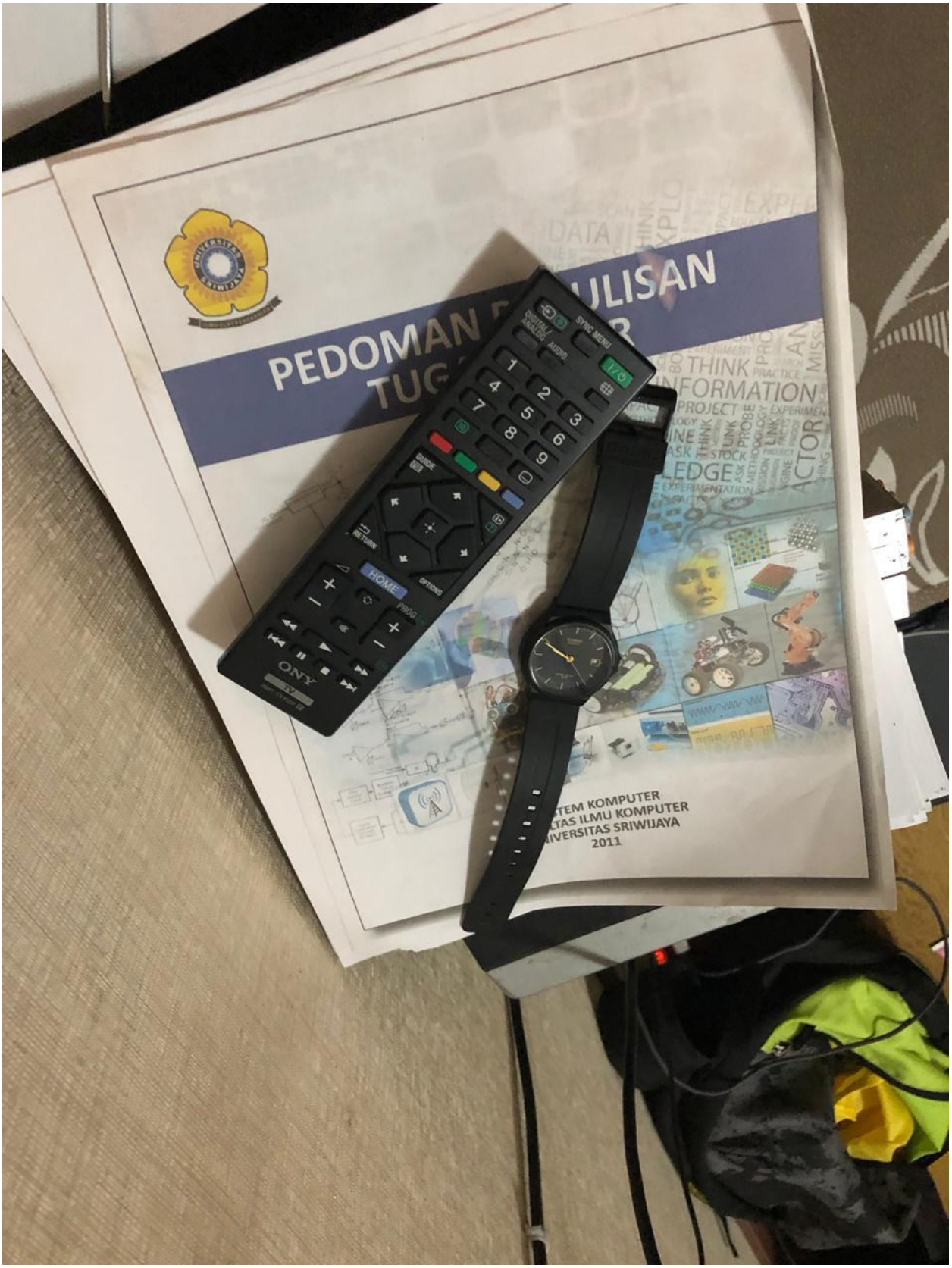
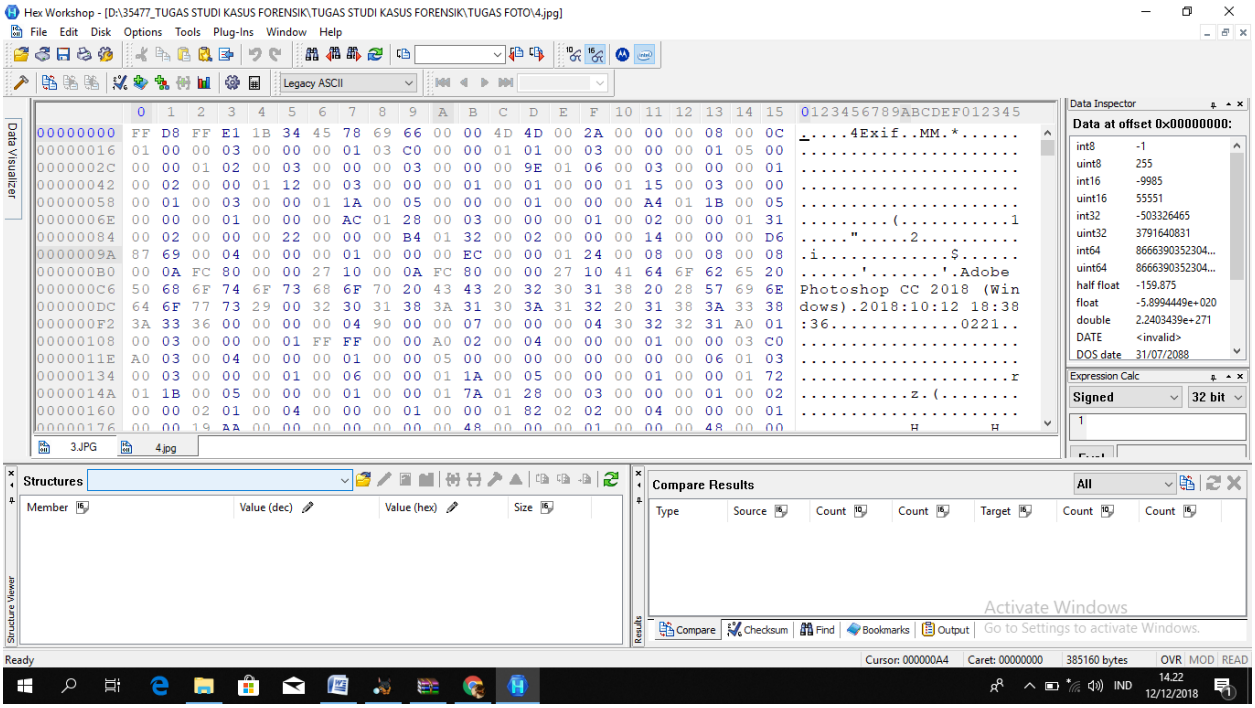


Foto 4.jpg merupakan foto yang telah diedit dengan menggunakan Adobe Photoshop CC 2018 (Windows) pada tanggal 2 Oktober 2018 pukul 18:38:36

Dibuka dengan menggunakan software Hex Workshop


PEDOMAN
ULISAN
TEM KOMPUTER
LTAS ILMU KOMPUTER
IVERSITAS SRIWIJAYA
2011
HOME
ONY


Hex Workshop - [D:\35477_TUGAS STUDI KASUS FORENSIK\TUGAS STUDI KASUS FORENSIK\TUGAS FOTO\4.jpg]
File Edit Disk Options Tools Plug-Ins Window Help
Legacy ASCII
Data Visualizer
Data Inspector
Data at offset 0x00000000:
Expression Calc
Signed
32 bit
3.JPG
4.jpg
Structures
Member
Value (dec)
Value (hex)
Size
Structure Viewer
Compare Results
All
Type
Source
Count
Target
Results
Compare
Checksum
Find
Bookmarks
Output
Activate Windows
Go to Settings to activate Windows.
Ready
Cursor: 000000A4
Caret: 00000000
385160 bytes
OVR MOD READ
IND
14.22
12/12/2018