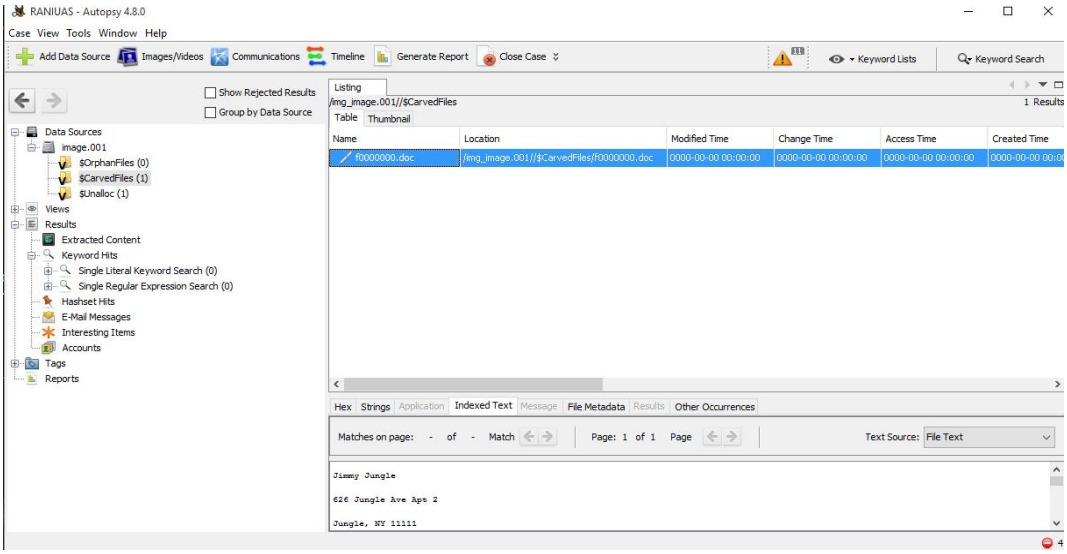
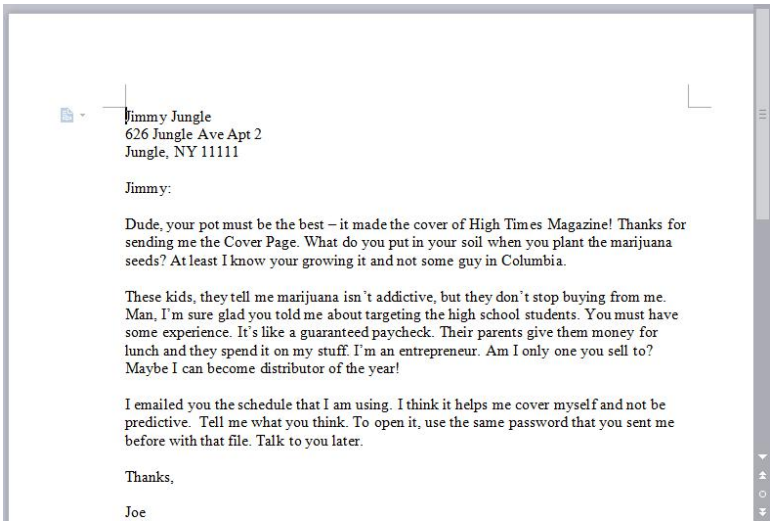
Rani Indah Purwanti
09021181520134
Komputer Forensic

1. Menyelidiki kasus joe jacob

Os : Windows 10
Tools : HEX WORKSHOP, AUTOPSY



Pertama masukan case yakni image kedalam autopsi, maka file diatas bisa diekstrak yang berisikan sebagai beikut



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.

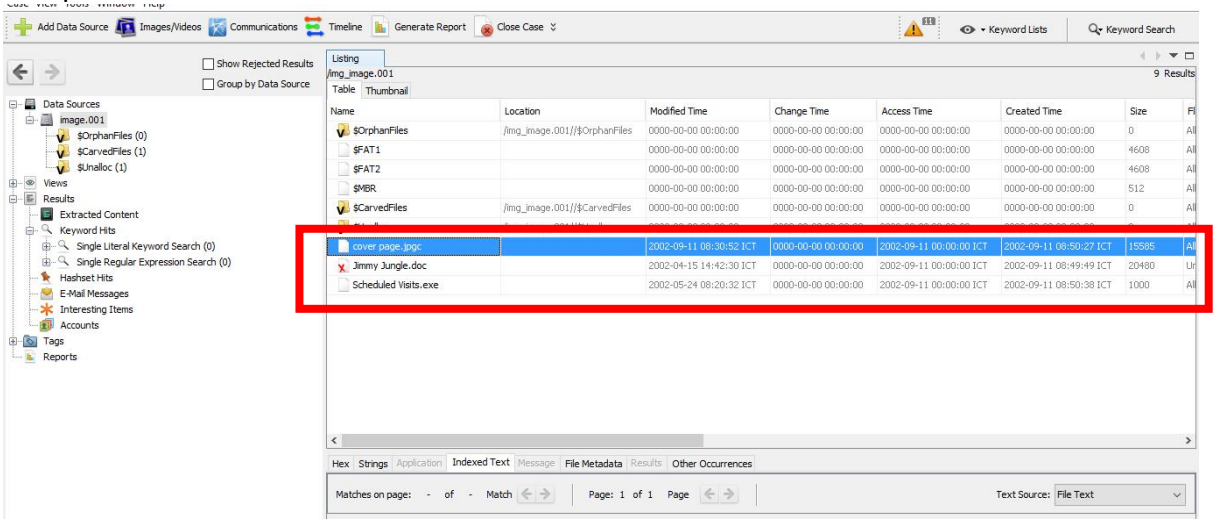
These kids, they tell me marijuana isn't addictive, but they don't stop buying from me. Man, I'm sure glad you told me about targeting the high school students. You must have some experience. It's like a guaranteed paycheck. Their parents give them money for lunch and they spend it on my stuff. I'm an 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,

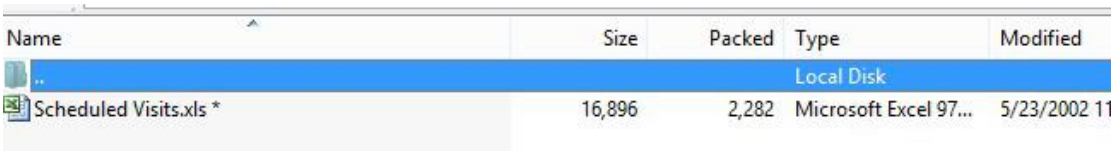
Joe

Rani Indah Purwanti
09021181520134
Komputer Forensic



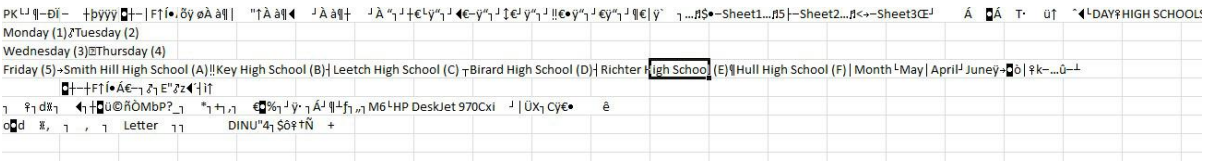
Jika dilihat file image ini sebenernya merupakan file zip yang berisikan 3 hal yang penting yakni yang diberi penekanan garis merah diatas.

Lalu ekstrak scheduled visit.exe lalu ubah tipe filenya ke zip. Lalu diekstrak



Ketika dibuka diaplikasi ke aplikasi winrar terdapat file excel yang hanya bisa di ekstrak menggunakan password yang tersembunyi di file coverpage (goodtimes)

Setelah password dimasukan maka file mampu dibuka dan menampilkan sebagai berikut :



Menjawab pertanyaan :

1. Pemasok narkoba Joe Jacob adalah Jimmy Jugle dengan beralamatkan 26 Jugle Ave Apt 2 Jungle, NY 11

2. Data penting terdapat didalam jimmy jugle yang berisikan alamat pemasok dan coverpage.jpg yang berisika password untuk membuka file scheduled visited

Rani Indah Purwanti
09021181520134
Komputer Forensic

3. Nama sekolah yang sering dijadikan transaksi adalah
    a) Smith hill high school
    b) Key high school
    c) Leetch high school
    d) Birard high school
    e) Richer high school
    f) Hull high school

4. Tersangka melakukan menyembunyikan bukti kejahatannya dengan mengubah semua filenya yang semula bertipe zip ke fie yang tidak bisa dibaca sehingga seolah-olah merupakan file rusak dan tidak mengandung informasi apapun

5. Proses yang digunakan penyidik untuk menyelidiki khasus ini adalah dengan mengetahui tipe file asli file image tersebut lalu menyelidiki lebih dalam apa yang ada didalamnya menggunakan tools autopsy dan hex workshop

2. Menentukan mana foto yang asli berdasarkan metadata

Dari soal yang didapatkan foto yang dicari keaslinya sebagai berikut

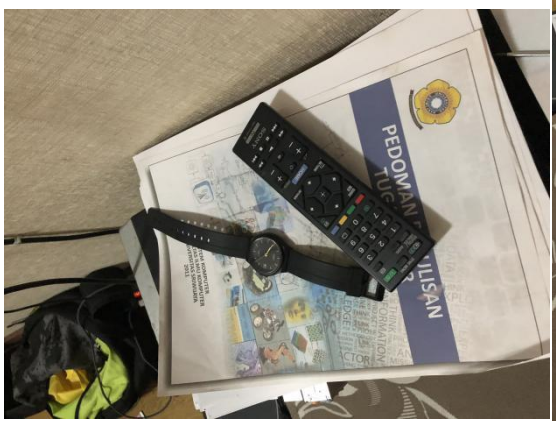


Foto 3

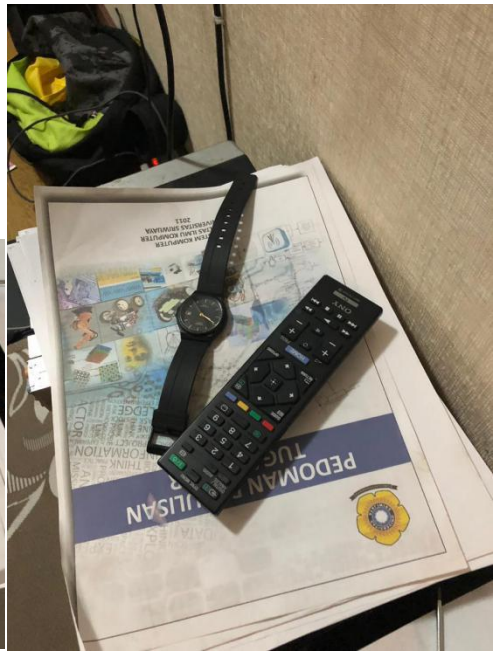


Foto 4

Rani Indah Purwanti
09021181520134
Komputer Forensic
Dengan tools online yakni **fotoforensic.com** didapatlah hasil metadata sebagai berikut :

UNTUK FOTO 3

File	
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg
Exif Byte Order	Big-endian (Motorola, MM)
Image Width	4032
Image Height	3024
Encoding Process	Baseline DCT, Huffman coding
Bits Per Sample	8
Color Components	3
Y Cb Cr Sub Sampling	YCbCr4:2:0 (2 2)
EXIF	
Make	Apple
Camera Model Name	iPhone 8 Plus
Orientation	Rotate 90 CW
X Resolution	72
Y Resolution	72
Resolution Unit	inches
Software	12.0
Modify Date	2018:10:11 21:50:08
Y Cb Cr Positioning	Centered
Exposure Time	1/4
F Number	1.8
Exposure Program	Program AE
ISO	100
Exif Version	0221
Date/Time Original	2018:10:11 21:50:08
Create Date	2018:10:11 21:50:08
Components Configuration	Y, Cb, Cr, -
Shutter Speed Value	1/4
Aperture Value	1.8
Brightness Value	-0.8140645339
Exposure Compensation	0
Metering Mode	Multi-segment
Flash	Off, Did not fire
Focal Length	4.0 mm
Subject Area	2015 1511 2217 1330
Sub Sec Time Original	285
Sub Sec Time Digitized	285
Flashpix Version	0100
Color Space	Uncalibrated
Exif Image Width	4032

Rani Indah Purwanti
09021181520134
Komputer Forensic

Exif Image Height	3024
Sensing Method	One-chip color area
Scene Type	Directly photographed
Exposure Mode	Auto
White Balance	Auto
Focal Length In 35mm Format	28 mm
Scene Capture Type	Standard
Lens Info	3.99000001-6.6mm f/1.8-2.8
Lens Make	Apple
Lens Model	iPhone 8 Plus back dual camera 3.99mm f/1.8
GPS Latitude Ref	South
GPS Longitude Ref	East
GPS Altitude Ref	Above Sea Level
GPS Time Stamp	14:50:06
GPS Speed Ref	km/h
GPS Speed	0.2140531391
GPS Img Direction Ref	True North
GPS Img Direction	122.1445389
GPS Dest Bearing Ref	True North
GPS Dest Bearing	122.1445389
GPS Date Stamp	2018:10:11
GPS Horizontal Positioning Error	32 m
Compression	JPEG (old-style)
Thumbnail Offset	2270
Thumbnail Length	9713
Thumbnail Image	(Binary data 9713 bytes)
MakerNotes	
Run Time Flags	Valid
Run Time Value	132281236382458
Run Time Scale	1000000000
Run Time Epoch	0
Acceleration Vector	0.03067672253 -0.5253151658 -0.8476625079
ICC_Profile	
Profile CMM Type	Apple Computer Inc.
Profile Version	4.0.0
Profile Class	Display Device Profile
Color Space Data	RGB
Profile Connection Space	XYZ
Profile Date Time	2017:07:07 13:22:32
Profile File Signature	acsp
Primary Platform	Apple Computer Inc.
CMM Flags	Not Embedded, Independent
Device Manufacturer	Apple Computer Inc.

Rani Indah Purwanti
09021181520134
Komputer Forensic

Device Model	
Device Attributes	Reflective, Glossy, Positive, Color
Rendering Intent	Perceptual
Connection Space Illuminant	0.9642 1 0.82491
Profile Creator	Apple Computer Inc.
Profile ID	ca1a9582257f104d389913d5d1ea1582
Profile Description	Display P3
Profile Copyright	Copyright Apple Inc., 2017
Media White Point	0.95045 1 1.08905
Red Matrix Column	0.51512 0.2412 -0.00105
Green Matrix Column	0.29198 0.69225 0.04189
Blue Matrix Column	0.1571 0.06657 0.78407
Red Tone Reproduction Curve	(Binary data 32 bytes)
Chromatic Adaptation	1.04788 0.02292 -0.0502 0.02959 0.99048 -0.01706 -0.00923 0.01508 0.75168
Blue Tone Reproduction Curve	(Binary data 32 bytes)
Green Tone Reproduction Curve	(Binary data 32 bytes)

Composite

Aperture	1.8
GPS Altitude	13.4 m Above Sea Level
GPS Date/Time	2018:10:11 14:50:06Z
GPS Latitude	2 deg 57' 44.06" S
GPS Longitude	104 deg 45' 34.91" E
GPS Position	2 deg 57' 44.06" S, 104 deg 45' 34.91" E
Run Time Since Power Up	1 days 12:44:41
Scale Factor To 35 mm Equivalent	7.0
Shutter Speed	1/4
Create Date	2018:10:11 21:50:08.285
Date/Time Original	2018:10:11 21:50:08.285
Circle Of Confusion	0.004 mm
Field Of View	65.5 deg
Focal Length	4.0 mm (35 mm equivalent: 28.0 mm)
Hyperfocal Distance	2.07 m
Image Size	4032x3024
Light Value	3.7
Megapixels	12.2

Approximate GPS Location

This information is interpreted from the GPS metadata. **Locations are approximate**. Although the coordinates appear precise, mobile devices typically have low a

Approximate Coordinates	-2.962239,104.759697
Approximate Location	Unknown
Approximate Range	+/- 32 meters (105 feet)

Rani Indah Purwanti
09021181520134
Komputer Forensic

UNTUK FOTO 4

File	
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg
Exif Byte Order	Big-endian (Motorola, MM)
Current IPTC Digest	cdcffa7da8c7be09057076aeaf05c34e
Image Width	960
Image Height	1280
Encoding Process	Progressive DCT, Huffman coding
Bits Per Sample	8
Color Components	3
Y Cb Cr Sub Sampling	YCbCr4:4:4 (1 1)

EXIF	
Photometric Interpretation	RGB
Orientation	Horizontal (normal)
Samples Per Pixel	3
X Resolution	72
Y Resolution	72
Resolution Unit	inches
Software	Adobe Photoshop CC 2018 (Windows)
Modify Date	2018:10:12 18:38:36
Exif Version	0221
Color Space	Uncalibrated
Exif Image Width	960
Exif Image Height	1280
Compression	JPEG (old-style)
Thumbnail Offset	398
Thumbnail Length	6570
Thumbnail Image	(Binary data 6570 bytes)

Rani Indah Purwanti
09021181520134
Komputer Forensic

IPTC	
Coded Character Set	UTF8
Application Record Version	0
Photoshop	
IPTC Digest	cdcffa7da8c7be09057076aeaf05c34e
Displayed Units X	inches
Displayed Units Y	inches
Print Style	Centered
Print Position	0 0
Print Scale	1
Global Angle	30
Global Altitude	30
URL List	
Slices Group Name	WhatsApp Image 2018-10-11 at 10.33.02 PM
Num Slices	1
Pixel Aspect Ratio	1
Photoshop Thumbnail	(Binary data 6570 bytes)
Has Real Merged Data	Yes
Writer Name	Adobe Photoshop
Reader Name	Adobe Photoshop CC 2018
Photoshop Quality	12
Photoshop Format	Progressive
Progressive Scans	3 Scans
XMP	
XMP Toolkit	Adobe XMP Core 5.6-c142 79.160924, 2017/07/13-01:06:39
Document ID	adobe:docid:photoshop:bd2935de-d513-c84a-b579-3ba3e50526c6
Instance ID	xmp.iid:e4472da2-6686-2646-ac07-0221214db0f8
Original Document ID	917BD0249F6466AA0DA7EB063983BA62
Format	image/jpeg
Color Mode	RGB
ICC Profile Name	
Create Date	2018:10:11 22:34:39+07:00
Metadata Date	2018:10:12 18:38:36+07:00
History Action	saved, saved
History Instance ID	xmp.iid:1cc50e04-54ce-df4c-8eeb-c51e7a2b98fb, xmp.iid:e4472da2-6686-2646-ac07-0221214db0f8
History When	2018:10:12 18:38:36+07:00, 2018:10:12 18:38:36+07:00
History Software Agent	Adobe Photoshop CC 2018 (Windows), Adobe Photoshop CC 2018 (Windows)
History Changed	/, /

APP14	
DCT Encode Version	100
APP14 Flags 0	[14]
APP14 Flags 1	(none)
Color Transform	YCbCr
Composite	
Image Size	960x1280
Megapixels	1.2

Pada metadata yang didapatkan diatas untuk foto 3 memiliki EXIF (Exchange Image File) berupa informasi perangkat apa yang digunakan untuk mengambil foto tersebut. Seperti dilihat diatas foto tersebut diambil melalu smartphone iphone

Sedangkan untuk foto 4 juga memiliki EXIF namun terdapat nama software editor dan jika dilihat pada XMP (Extensible Metadata Platform) menunjukan bahwasannya foto tersebut memiliki history software. **Maka bisa disimpulkan bahwa foto 4 adalah foto yang telah diedit dan foto 3 adalag foto original**