KEAMANAN JARINGAN KOMPUTER



Ulan Purnama Sari

09011181320003

Program Studi Sistem Komputer

Fakultas Ilmu Komputer

Universitas Sriwijaya

2017

Task 6

computer forensics

Komputer forensik atau yang juga dikenal juga dengan istilah digital forensik, adalah salah satu cabang ilmu forensik yang berkaitan dengan bukti legal yang dapat ditemukan pada komputer dan media penyimpanan digital lainnya. Forensik sendiri merupakan sebuah proses ilmiah dalam mengumpulkan, menganalisis, dan menghadirkan berbagai bukti pada sidang pengadilan karena adanya suatu kasus hukum. Secara singkat tujuan dari komputer forensik adalah untuk menjabarkan keadaan terkini dari suatu catatan digital.

Tugas :

Diminta bantuan untuk mendapatkan informasi tentang kasus narkoba

- Tampilkan capture langkah langkahnya
- Jawab pertanyaan untuk memberikan informasi

Tools yang digunakan :

- AutoPsy
- Foremost
- Strings

TAMPILAN CAPTURE LANGKAH – LANGKAH

1. Langkah pertama kali kita melakukan perintah md5sum pada file zip, terlebih dahulu kita download dulu file nya. Gambar dibawah adalah perintah md5sum yang file image.zip nya berada di direktori Videos.



Gambar 1. Perintah md5sum

2. Kemudian kita lakukan perintah file image yang bertujuan untuk melihat tipe file yang digunakan. Dalam hal ini file yang digunakan adalah DOS.



Gambar 2. Perintah file image

 Selanjutnya, kita membuat direktori baru dengan kasus narkoba setelahnya melakukan mount image kedalam direktori itu.



Gambar 3. Perintah mkdir dan mount image

 Setelah kita membuat direktori kita masuk ke dalam direktori tersebut dan masukkan perinta ls, perintah ls tersebut bertujuan untuk kita bisa melihat didalam direktori tersebut telah terdapat isi



Gambar 4. Melihat isi direktori

5. Lalu kita mengekstrak semua file yang terdapat pada direktori kasus.narkoba dengan menggunakan perintah File *.



Gambar 5. Perintah ekstrak file

6. Membuka tools Autopsy



Gambar 6. Membuka tools Autopsy

 Langkah ke-6 kita sudah membuka tools autopsy pada terminal biarkan agar tetap running terminal tersebut, lalu kita buka autopsy pada web dan menuliskan

localhost:9999/autopsy



Gambar 7. Tampilan pada web Autopsy

8. Langkah berikutnya membuat kasus baru, untuk membuat kasus baru nya kita pilih New Case , inputkan sesuai kasus yang kita sedang tangani

| Create A New Case - Mozilla Firefox | |
|--|---|
| 🕼 Create A New Case 🛛 🗙 🕂 | |
| ♦ ① localhost:9999/autopsy?mod=0&view=1 | C Search |
| 🗑 Most Visited 🕶 🕒 Linux Mint 🖺 Community 🐚 Forums | Blog SNews▼ |
| | |
| | CREATE A NEW CASE |
| | |
| | Case Name: The name of this investigation. It can contain only letters, numbers, and symbols. |
| | kasus |
| | |
| | 2. Description: An optional, one line description of this case. |
| | Kasus Haikova |
| | 3. Investigator Names: The optional names (with no spaces) of the investigators for this case. |
| | a. ulan purnama sari b. |
| | c d |
| | e. f. |
| | g, h |
| | i. j. |
| | |
| | New Case Cancel Help |

Gambar 8.1 Membuat kasus baru



Gambar 8.2 Tampilan Kasus berhasil dibuat

Lalu klik ADD HOST, kita akan disuruh menginputkan host name. Disini saya menginputkan host name Joe_Jacob sesuai dengan perintah yang dilakukan.



Gambar 8.3. Add New Host



Gambar 8.4 Tampilan berhasil menambah Host

Lalu langkah selanjutkan memilih Add Image File



Gambar 8.5 Add Image File

Perintah selanjutnya kita diarahkan untuk memberikan lokasi penyimpanan dari gambar tersebut , saya letakkan di direktori */home/dee/Videos/image*

9

| | ADD A NEW IMAG | E |
|--|---|--|
| 1. Location Enter the full path (st If the image is split (e extension. | arting with /) to the ima ither raw or EnCase), t | age file. hen enter '*' for the |
| /home/dee/Videos/imag | e | |
| O Disk | • Partition | |
| 3. Import Method To analyze the image be imported from its o or by moving it. Note then the image could | file, it must be located current location using a that if a system failure become corrupt. | in the evidence locker. It can a symbolic link, by copying it, occurs during the move, |
| Symlink | О Сору | O Move |
| | NEXT | |
| | NEXT | |
| CANCEL | | HELP |

gambar 8.6 Menentukan lokasi penyimpanan



Gambar 8.7 Volume Image Dos

| conf | =1&img_path=%2Fhome%2Fdee%2FVideos%2Fimage&sort= |
|------|--|
| is 1 | Blog SNews▼ |
| | Image File Details |
| | Local Name: images/image |
| | Data Integrity: An MD5 hash can be used to verify the integrity of the image. (With split images, this hash is for the full image file) |
| | Ignore the hash value for this image. |
| | <u>Calculate</u> the hash value for this image. |
| | Add the following MD5 hash value for this image: |
| | |
| | Verify hash after importing? |
| | File System Details |
| | Analysis of the image file shows the following partitions: |
| | Dentifican 1 (Terre fet10) |
| | Paruuon 1 (Type: Tat12) Mount Point: C. File System Type: fst12 |
| | File System Type. Tatz |
| | |

Gambar 8.8 Image file details

| Add a new image to an Autopsy Case - Mozilla Firefox | | | | | | | |
|--|---|---|---|---|--|---|--|
| 🔄 🛈 localhost-9999/autopsy?mod=0&view=15&img_path=%2Fhome%2Fbownloads%2Fimage#_img=1&sort=1&do_md5=1&m C Q Search | ☆ | Ê | ÷ | î | | ≡ | |
| Festing partitions .inking image(s) into evidence locker mage file added with ID img1 /olume image (0 to 0 - fat12 - C:) added with ID vol1 ΟΚ ΑDD IMAGE | | | | | | | |

Gambar 8.9. Testing Partitions

Tampilan setelah kita memilih OK, akan muncul tampilan testing partition

| Open Image In kasus:joe_jacob - Mozilla Firefox | | | | | |
|--|----------------------------|-------------------|-------------------------|----------------|--|
| 🅼 Open Image In kasus:j 🗙 🕂 | | | | | |
| () Iocalhost:9999/autopsy?mod=0&view=16&case=kasu | us&host=joe_jacob&inv=unkn | own | C | Q Search | |
| 🛅 Most Visited 🕶 🗈 Linux Mint 🖲 Community 🗉 Forums 🖼 | Blog News 🕶 | | | | |
| Case: kasus Host: joe_jacob | Select a vol | ume to analyze o | or add a new ir | nage file. | |
| | Case Gallery | HOST GAI | LERY | IOST MANAGER | |
| | mount C:/ | name image-0-0 | fs type fat12 | details | |
| | Analyze | | | CLOSE HOST | |
| | FILE ACTIVITY TIME LINES | | | HASH DATABASES | |

Gambar 8.10. Tampilan Volume Analyze

| kasus:joe_jacob:vol1 · | Mozilla Firefo | x | | | | | | 1 | 008 |
|---------------------------------|-----------------|---------------------------------------|------------------------------|------------------------------|------------------------------|--------------|--------|-----|--------------|
| 🚯 kasus:joe_jacob:vol1 | × + | | | | | | | | |
| (i localhost:9999/aut | opsy?mod=1⊂ | mod=2&case=kasus&hos | st=joe_jacob&inv=unknown&vol | -vol1 C Q Searc | h ☆ | ≜ ∔ ∧ | | ٢ | @ ≡ |
| Most Visited ▼ 🚇 Linux I | Mint 👅 Communit | y 🖫 Forums 🖫 Blog 📗 | News 🕶 | | | | | | |
| | | FILE ANALYSIS KEYWO | RD SEARCH FILE TYPE | IMAGE DETAILS META DATA | DATA UNIT HELP CLOSE | | | | |
| | | 2 | | | ? X | | | | |
| Directory Seek | Current Di | rectory: <u>c:/</u> | | | | | | | |
| Entor the name of | ADD NOTE | GENERATE | MD5 LIST OF FILES | | | | | | |
| a directory that | | | | | | | | | |
| you want to view. | DEL Type | | WRITTEN | ACCESSED | CREATED | SIZE | UID | GID | МЕТА |
| | v / v | <u>SFAT1</u> | 0000-00-00 00:00:00 (UTC) | 0000-00-00 00:00:00 (UTC) | 0000-00-00 00:00:00 (UTC) | 4608 | 0 | 0 | <u>45780</u> |
| | v / v | <u>SFAT2</u> | 0000-00-00 00:00:00 (UTC) | 0000-00-00 00:00:00 (UTC) | 0000-00-00 00:00:00 (UTC) | 4608 | 0 | 0 | <u>45781</u> |
| File Name Search | v / v | SMBR | 0000-00-00 00:00:00 (UTC) | 0000-00-00 00:00:00 (UTC) | 0000-00-00 00:00:00 (UTC) | 512 | 0 | 0 | <u>45779</u> |
| Enter a Perl | d / d | <u>SOrphanFiles/</u> | 0000-00-00 00:00:00 (UTC) | 0000-00-00 00:00:00 (UTC) | 0000-00-00 00:00:00 (UTC) | 0 | 0 | 0 | <u>45782</u> |
| regular expression for the | r/r | <pre>cover page.jpgc</pre> | 2002-09-11 08:30:52 (WIB) | 2002-09-11 00:00:00 (WIB) | 2002-09-11 08:50:27 (WIB) | 15585 | 0 | 0 | <u>8</u> |
| file names you want to find. | ✓ r/r | Jimmy Jungle.doc | 2002-04-15 14:42:30 (WIB) | 2002-09-11 00:00:00 (WIB) | 2002-09-11 08:49:49 (WIB) | 20480 | 0 | 0 | <u>5</u> |
| | r/r | <u>Scheduled</u> <u>Visits.exe</u> | 2002-05-24 08:20:32 (WIB) | 2002-09-11 00:00:00 (WIB) | 2002-09-11 08:50:38 (WIB) | 1000 | 0 | 0 | 11 |
| SEARCH | | | | | | | | | |
| | | | | | | | | | |
| ALL DELETED FILES | | | | | | | | | |
| EXPAND DIRECTORIES | | | | | | | | | |
| 💼 menu 💼 🥹 🖅 🚞 | Videos | 🖾 Terminal | 📧 Terminal | kasus:joe_jacob:vol1 | 50.0°C 👝 💄 📑 🕪 🚅 | U MEM NET | DISK / | 16% | 13:09 🖵 |

Gambar 8.11. Analyze details

Digambar bawah tersebut tampilan setelah kita memilih image detail , terdapat 2 FAT Contens. Kita membuka conten pertama 73-103

| kasus:joe_jacob:vol1 - Mozilla Firefi | x | | | | | | | | | | | e | 00 |
|--|---------------|-----------------------|-----------------|---------------|-----------|-----------|----------|-----|---|----------|---|---|----|
| 🎪 kasus:joe_jacob:vol1 🛛 🗙 🕂 | | | | | | | | | | | | | |
| () localhost:9999/autopsy?mod=1&su | | asus&host=joe_jacob&i | inv=unknown&vol | | C Q Searc | | | ☆ 自 | ÷ | ± | • | ٥ | ≡ |
| 🛅 Most Visited 💌 🛸 Linux Mint 🛸 Communi | ty 🔞 Forums 🐻 | Blog 🔂 News 🔻 | | | | | | | | | | | |
| | FILE ANALYSIS | KEYWORD SEARCH | FILETYPE | IMAGE DETAILS | META DATA | DATA UNIT | HELP CLO | SE. | | | | | |
| File System Layout (in sectors) Total Range: 0 - 2879 * Reserved: 0 - 0 ** Boot Sector: 0 ** Boot Sector: 0 * FAT 0: 1 - 9 * FAT 0: 1 - 9 * Tota Area: 19 - 2879 ** Root Directory: 19 - 32 ** Cluster Area: 33 - 2879 | | | | | | | <u> </u> | _ | | | | | |
| METADATA INFORMATION Range: 2 - 45782 Root Directory: 2 | | | | | | | | | | | | | |
| CONTENT INFORMATION Sector Size: 512 Cluster Size: 512 Total Cluster Range: 2 - 2848 | | | | | | | | | | | | | |
| FAT CONTENTS (in sectors) 73-103 (31) -> EOF 104-108 (5) -> EOF | | | | | | | | | | | | | |

Gambar 8.12. Image Details

| kasus:joe_jacob:vol1 × | + |
|---|---|
| (i) localhost.9999/autopsy?cas | e-kasusőhöst-joe jacobőinv-unknownővol-vol16mod=16oubmod=56block=736k 🛛 🖱 🔍 🤤 search 🔄 🏠 🖄 🖉 🖉 🧔 🚍 |
| Most Visited 💌 🖐 Linux Mint 🖷 C | ommunity 🕏 Forums 🖲 Blog 🔂 News 🕶 |
| | FILE ANALYSIS KEYWORD SEARCH FILE TYPE IMAGE DETAILS META DATA DATA UNIT HELP CLOSE |
| Sector Number: 73 Number of Sectors: 1 | ASCII (display - report) + Hex (display - report) + ASCII Strings (display - report) File Type: JPEG image data, JFIF standard 1.01 Sectors: 73-103 Status: Allocated |
| ALLOCATION LET: | ASCII Contents of Sectors 73-103 in image-0-0 |

Gambar 8.13. Data Unit Image pertama

Dari gambar diatas konten pertama dgn sector 73-103 terdapat JFIF salah satunya adalah format dari image pertama. Format JFIF adalah format dari gambar jpg/jpeg, bisa saya buktikan pada gambar 8.14, informasi tersebut saya dapatkan dari wikepedia.

| kasus:joe_jacob:vol1 | W List of file signatures × + | | | | | 900 |
|-----------------------------|---|--|----------|---------------|---|-----|
| () () () https://en.wikipe | dia.org/wiki/List_of_file_signatures | C Q Sear | ch | ☆ 自 ┨ | k n ⊠ 🗢 6 | ≡ |
| 🛅 Most Visited 💌 🦉 Linux Mi | int 👅 Community 🖫 Forums 🖫 Blog 🔂 New | ¥2.▼ | | | | |
| | bpg | Better Portable Graphics format ⁽⁷⁾ | 0 | BPGû | 42 50 47 FB | |
| | | | | ÿØÿŰ | FF D8 FF DB | |
| | ipg jpeg | JPEG raw or in the JFIF or Exif file format | o | ÿØÿàJ F IF | FF D8 FF E0 nn nn 4A 46 49 46 00 01 | |
| | | | | ÿØÿáE x if | FF D8 FF E1 nn nn 45 78 69 66 00 00 | |
| | ilbm Ibm ibm iff | IFF Interleaved Bitmap Image | 0 any | FORM ILBM | 46 4F 52 4D nn nn nn nn 49 4C 42 4D | |
| | 8svx 8sv svx snd | IFF 8-Bit Sampled Voice | 0 any | FORM 85VX | 46 4F 52 4D nn nn nn 38 53 56 58 | |

Gambar 8.14. Format JFIF

9. Masuk lagi ke terminal



Gambar 9.1 Perintah Membuka Image

Melakukan perintah diatas tidak perlu kita masuk ke root. Setelah melakukan perintah di gambar 9, akan muncul gambar 9.2.



Gambar 9.2. Image Sector 73-103

10. Melakukan sector selanjutnya, yaitu sector yang kedua 104-108. Dimana isi sector 2 terdapat kata PK pada gambar 10.1 dan saya mencari tahu nya lagi dari wikepedia pada gambar 10.2

| 🔒 kasusijoe_jacob:vol1 ж у | x) List of file signatures x + |
|--|---|
| () localhost 9999/autopsy?case | |
| Most Visited * E Linux Mint E Co | mmunity E Forums E Blog |
| | FUE ANALYSIS KEYNOND DEANCH FUE TITE HAGE DETAILS META DATA DATA UNIT HELP CLOSE |
| | |
| Sector Number: 104 Number of Sectors: | Control Control |
| Address Type: Regular (dd) * Lazarus Addr: | ACII Content of Sectors 384-388 in 1869-9-0 Pr |
| ALLOCATION LIST | |

Gambar 10.1 data unit image kedua

| List of file signatures | - Wikipedia - Mozilla Firefox | | 000 | | | | |
|--|--------------------------------------|--|--------------------|--|-------------------------|--|--|
| kasus:joe_jacob:vol1 | × W List of file signatures × + | 📋 Laptop batt | ery critically low | | | | |
| 🐑 🛈 🚔 https://en.wikipedia.org/wiki/List_of_file_signatures 🛛 🖉 🔍 Search | | | | Computer will hibernate very soon unless it is plugged in. | | | |
| 🛅 Most Visited 💌 🚡 Linux M | lint 👅 Community 🖫 Forums 🍯 Blog 题 | News 🔻 | | | | | |
| | | AmiBack on an Amiga. | | | | | |
| | Iz | Izip compressed file | 0 | LZIP | 4C 5A 49 50 | | |
| | exe | DOS MZ executable file format and its descendants (including NE and PE) | 0 | MZ | 4D 5A | | |
| | zip jar odt | | | | 50 48 03 04 | | |
| | ods odp docx | zip file format and formats based on it, such as JAR, ODF, OOXML | 0 | РК | 50 48 05 06 | | |
| | xlsx pptx | | | | (empty archive) | | |
| | vsdx apk | | | | 50 48 07 08 | | |
| | | | | | (spanned archive) | | |
| | rar | RAR archive version 1.50 onwards ^[8] | o | Rarl | 52 61 72 21 1A 07 00 | | |
| 💼 menu 🛅 🍘 📰 🚞 | Videos 🖾 Terminal | 🕅 Terminal 📀 List of file signat 🖾 Terminal | 51.7°C | 1 1 40 00 | 🚝 🐨 🔤 🚉 11% 13:23 🕞 | | |

Gambar 10.2 Wikedpedia

Setelah mencari informasi tentang format Pk didapatkan hasil bahwa format PK sama halnya dengan format ZIP. Seperti yang ditampilkan pada gambar 25.



Gambar 10.3. Perintah Strings Image

Setelah mencari tahu informasi tentang PK maka yang harus dilakukan adalah melakukan strings terhadap file image sector 73-103 untuk mendapatkan password. Terdapat password goodtimes, setelah kita mendapatkan password tersebut kita bisa mengakses file pada file image sector 104.

| 7g% | Jar |
|--------------------------------------|------|
| 9'p+ | |
| R*]I | |
| I+^L | |
| pw=goodtimes | docx |
| <pre>dee@dee-K46CB ~/Videos \$</pre> | ulsx |

Gambatt 10.4 tampilan password



Gambar 10.5 buka password

Digambar 10.6 dibawah ini adalah isi informasi dari rentetan kegiatan untuk mempermudah melacak informasi.

| Scheduled \ | /isits.xls - Libre | eOffice Calc | | | | | | | | | | 000 | |
|-------------------------------|--------------------|--|-------------------|--------------|---------------|-----------|------------|-----|------|----------------|-----------|------------|--|
| <u>File Edit View</u> | Insert Format 3 | bols <u>D</u> ata <u>W</u> indow <u>H</u> elp | | | | | | | | | | × | |
| 10 · m · | C and D | A D D Ab Ab V | 0.8.4. | 0 | a 14 14 1 0 | 5 S P | | 0 | | | | | |
| | | 7 G G 2 | | | - : : : • . • | 1 5 1 7 | | ** | | | | | |
| Arial | - 10 | • a a a = = | = = ··· v · | 2. 20 | 5 B . | • 🖪 • 🤞 | a. • 000 | | | | | | |
| | | | m | | | | - | | | | | | |
| B50 | | = Monday (1) | | | | | | | | | | | |
| | | · · · · | 0 | 6 | E 6 | L H | 1 1 1 | | × 1 | | M I N | LOID | |
| 1 Month | DAY | HIGH SCHOOLS | 0 | | r 0 | | | | n . | | | | |
| 1 monut | | mon seriools | | | | | | | | | | | |
| 2 200 | E Monday (1) | Penith Hill High Pethool (A) | | | | | | | | | | | |
| 3 April | Tuonday (1) | Key High School (R) | | | | | | | | | | | |
| - | Medoesday (2) | Leatch Mah School (C) | | | | | | | | | | | |
| 6 | Thursday (4) | Birard High School (D) | | | | | | | | | | | |
| 7 | Eriday (5) | Dichter Hinh School (E) | | | | | | | | | | | |
| 8 | Monday (1) | Hull High School (E) | | | | | | | | | | | |
| 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) | | | | | | | | | | | |
| * + + H Sheet1 | /Sheet2 / Sheet3 / | t All and the second se | | | | | | | | | | | |
| Sheet 1/3 PageStyle Sheet1 == | | | | | | | Sum=0 | | | | | | |
| | | Videos 🔲 Terminal 🕅 Term | inal Dist of file | [1] Terminal | al well-Secto | N Schadul | ed 5179 | v • | - 1A | cro <u>pan</u> | iar Apr p | 1995 12-28 | |

Gambar 10.6 File scheduled

| kasus:joe jacob:vol1 - Mozilla Firefox | | | | | | | | | |
|---|---|--|--|--|--|--|--|--|--|
| 🔗 kasus;joe_jacob:vol1 🛛 🗙 🐨 List of file signatures 🗙 🕴 + | | | | | | | | | |
| 🗲 🛈 localhost:9999/autopsy?mod=1&submod=3&case=kasus&host=joe_jacob&inv=unknown&vol=vol1 C 🔍 Search | | | | | | | | | |
| 📷 Most Visited ▼ 🖫 Linux Mint 🖫 Community 🖫 Forums 🖫 Blog 🔊 News ▼ | | | | | | | | | |
| | FILE ANALYSIS KEYWORD SEARCH FILE TYPE IMAGE DETAILS META DATA DATA UNIT HELP CLOSE | | | | | | | | |
| Dir Entry Number: | PREVIOUS NEXT REPORT VIEW CONTENTS EXPORT CONTENTS ADD NOTE Search for File Name File Type: empty (Zip archive data, at least v2.0 to extract) MD5 of content: 0022a5xc64deea22a3a580ffbb5a6fa66 - SHA-1 of content: cderf25380d63x50934d9f2zffaab29de1f09240b5 - Details: Directory Entry: 11 Allocated File Attributes: File, Archive Size: 1000 Name: SCHEDU-1.EXE Directory Entry Times: Written: Fri May 24 08:20:32 2002 Accessed: Wed Sep 11 00:00:00 2002 Created: Wed Sep 11 08:50:38 2002 Sectors: 104 105 | | | | | | | | |

Gambar 10.7 meta data



Gambar 10.8 perintah foremost

Perintah diatas adalah fungsinya untuk mengekstrak data yang tertimpa atau tertumpuk.



Gambar 10.9 file doc

Isi dari file doc adalah surat dari Joe untuk Jimmy.

| Videos | | | | | | |
|--|--|--|--|--|--|--|
| File Edit View Go Bookmarks Help | | | | | | |
| 🗧 🖻 🏠 🖸 🎵 📮 //home/dee/Videos | | | | | | |
| | | | | | | |
| vol1-Sector73.jpg - GHex | | | | | | |
| File Edit View Windows Help | | | | | | |
| 00000000 FF D8 FF E0 00 10 4A 46 49 46 00 01 01 01 00 60 JFIF | | | | | | |
| 0000001000 60 00 00 FF DB 00 43 00 08 06 06 07 06 05 08.`C | | | | | | |
| 0000002007 07 07 09 09 08 0A 0C 14 0D 0C 0B 0B 0C 19 12 | | | | | | |
| 0000003013 OF 14 1D 1A 1F 1E 1D 1A 1C 1C 20 24 2E 27 20\$.' | | | | | | |
| 0000004022 2C 23 1C 1C 28 37 29 2C 30 31 34 34 34 1F 27[",#(7),01444.' | | | | | | |
| 0000005039 3D 38 32 3C 2E 33 34 32 FF DB 00 43 01 09 099=82<.342C | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| Signed 8 bit: 74 Signed 32 bit: 1179207242 Hexadecimal: 4A | | | | | | |
| Unsigned 8 bit: 74 Unsigned 32 bit: 1179207242 Octal: 112 | | | | | | |
| Signed 16 bit: 17994 Float 32 bit: 1,288157e+04 Binary: 01001010 | | | | | | |
| Unsigned 16 bit: 17994 Float 64 bit: 7,748599e-304 Stream Length: 8 - + | | | | | | |
| Show little endian decoding Show unsigned and float as hexadecimal | | | | | | |
| Offset: 0x6; 0x5 bytes from 0x6 to 0xA selected | | | | | | |

Gambar 10.10 Konversi Ghex

Gambar 10.10 adalah langkah terakhir melakukan praktikum ini, langkah ini merupakan konveksi huruf ke binner menggunakan tools GHex.

Pertanyaan :

- 1. Siapa pemasok narkoba Joe Jacob dan apa alamatnya?
- 2. Data penting apa yang terdapat di file coverage.jpg dan mengapa data tersebut penting?
- 3. Nama sekolah selain smith hill yang sering menjadi tempat transaksi joe Jacob?
- 4. Untuk setiap file proses apa yang diambil oleh tersangka untuk mengelabuhi orang lain?
- 5. Proses apa yang digunakan penyidik untuk berhasil memeriksa seluruh isi dari setiap file?

Jawab :

- 1. Pemasok adalah Jimmy Jungle
 - alamat tinggalnya di 626 Jungle Ave Apt 2
- file Scheduled Visit.xls tetapi dalam hal ini file tersebut dapat diakses dengan password. Kenapa didalam file tersebut terdapat data tentang nama – nama sekolah yang menjadi tempat transaksi joe jacob
- 3. nama sekolah
 - Key High School
 - Leetch High School
 - Birard High School
 - Richter High School
 - Hull High School
- 4. Mereka mengelabui dengan cara mengganti format zip menjadi raw dari file vol1sector73 dan sector104
- 5. Dalam hal ini proses yang digunakan penyidik adalah dengan mencari informasi informasi penting menggunakan beberapa tools yaitu Autopsy,foremost dan GHex