

**TUGAS FORENSIK
KEAMANAN JARINGAN KOMPUTER**



OLEH :

NAMA : ANGGIT MARDIAN

NIM : 09011281419062

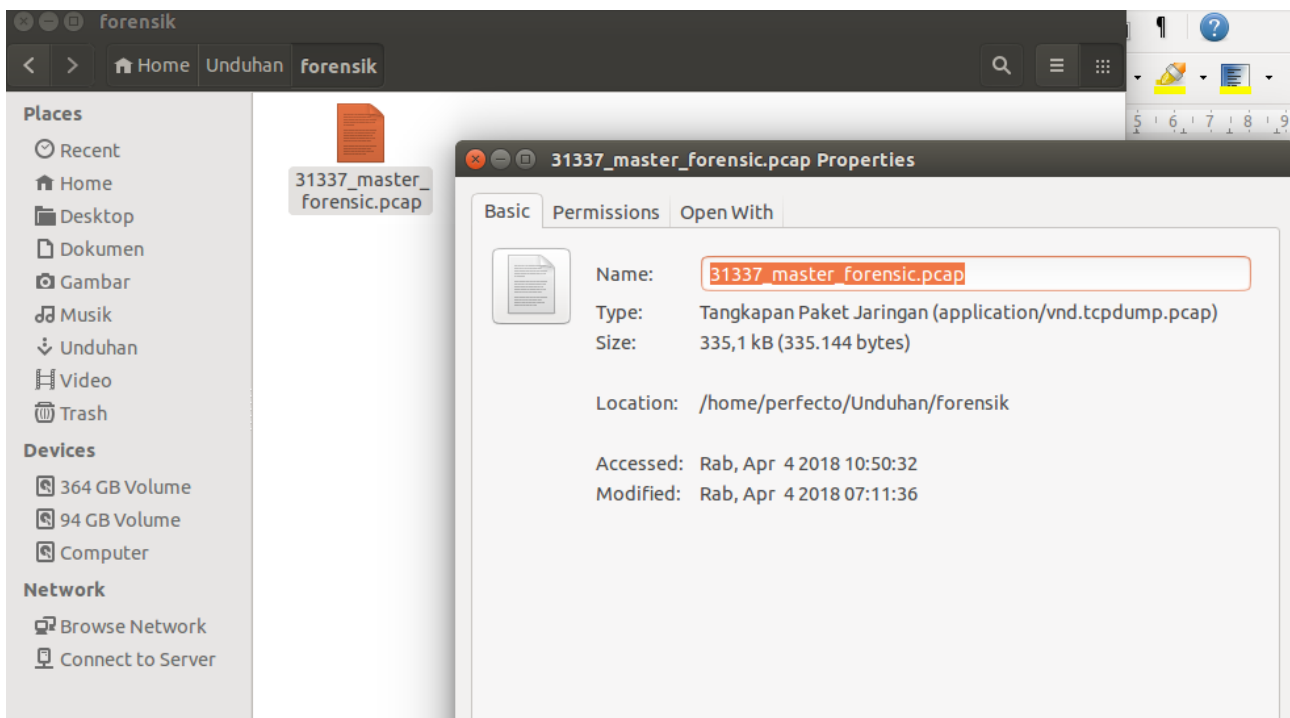
**SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2018**

FORENSIC FILE

Kasus :

Didapat sebuah file pcap hasil penyadapan dua orang kriminal yang melakukan komunikasi untuk mengadakan pertemuan disebuah tempat. Melalui file pcap tersebut akan diketahui dimana lokasi pertemuan yang akan di lakukan oleh dua orang kriminal.

File berukuran 355,1 KB



Langkah – langkah

1. cari tahu string apa saja yang ada di file tersebut dengan mengetikkan perintah “**string -d (nama file) }more**” tanpa tanda petik di terminal linux seperti gambar di bawah.

```

perfecto@perfecto: ~/Unduhan/forensik
perfecto@perfecto:~/Unduhan/forensik$ strings -d 31337_master_forensik.pcap |more
!B<4>Oct 10 12:33:53 gateway kernel: [46735.878849] FIREWALL:BLOCKEDIN=eth2 OUT= M
AC= SRC=10.1.1.10 DST=10.1.1.255 LEN=76 TOS=0x00 PREC=0x00 TTL=64 ID=0 DF PROTO=UD
P SPT=123 DPT=123 LEN=56
!pMO
!pMO
!pMO
{ `Bn
<4>Oct 10 12:34:26 gateway kernel: [46768.856594] FIREWALL:BLOCKEDIN=eth3 OUT= MAC
= SRC=192.168.1.10 DST=192.168.1.255 LEN=76 TOS=0x00 PREC=0x00 TTL=64 ID=0 DF PROT
O=UDP SPT=123 DPT=123 LEN=56
!pMO
  EBEOEOCNEMEBFAFEFPFACACACACACAAA
  FHEPFCELEHFCEPFFFACACACACACACABN
SMB%
\MAILSLOT\BROWSE
<4>Oct 10 12:34:42 gateway kernel: [46784.911050] FIREWALL:BLOCKEDIN=eth3 OUT= MAC
=ff:ff:ff:ff:ff:ff:00:21:70:4d:4f:ae:08:00 SRC=192.168.1.159 DST=192.168.1.255 LEN
=202 TOS=0x00 PREC=0x00 TTL=128 ID=106 PROTO=UDP SPT=138 DPT=138 LEN=182
!pMO
  FHEPFCELEHFCEPFFFACACACACACACABL
<4>Oct 10 12:34:42 gateway kernel: [46784.917306] FIREWALL:BLOCKEDIN=eth3 OUT= MAC
=ff:ff:ff:ff:ff:ff:00:21:70:4d:4f:ae:08:00 SRC=192.168.1.159 DST=192.168.1.255 LEN
=78 TOS=0x00 PREC=0x00 TTL=128 ID=107 PROTO=UDP SPT=137 DPT=137 LEN=58

```

disini kita mencari dengan detail apa saja string yang ada di dalam file tersebut. Dan ditemukan sebuah percakapan melalui email dan terdapat file berekstensi .docx yang telah dienkrupsi. Berikut adalah tampilan email berisi file docx setelah menetikkan perintah “strings -d (nama file) |more” tanpa tanda petik di dalam terminal linux.

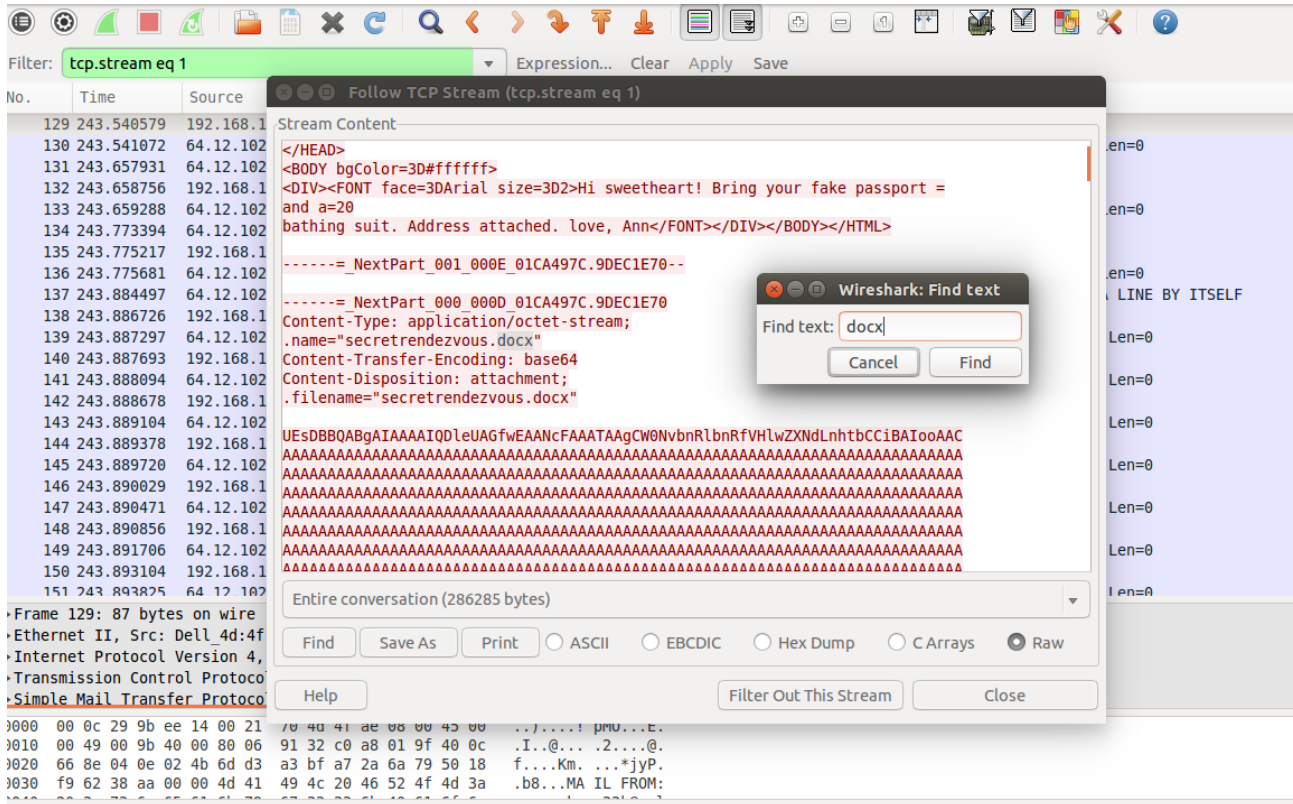
```

perfecto@perfecto: ~/Unduhan/forensik
and a=20
bathing suit. Address attached. love, Ann</FONT></DIV></BODY></HTML>
-----=_NextPart_00D
!pMO
!pMO
1_000E_01CA497C.9DEC1E70--
-----=_NextPart_000_000D_01CA497C.9DEC1E70
Content-Type: application/octet-stream;
      name="secretrendezvous.docx"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
      filename="secretrendezvous.docx"
UESDBBQABgAIAAAAIQDleUAGfwEAANcFAAATAAgCW0NvbnRlbnRfVHlwZXNdLnhtbCCiBAIooAAC
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAC0
VMLuwjAQvVfqP0S+VsTQQ1VVBA5dji1S6QcYexKsepNtr/vOEBEKQSpwCVSPH7LPI/dHy61yubg
--More--

```

2. Karena terdapat percakapan melalui email di dalam file tersebut di mana email menggunakan protokol SMTP, maka file tersebut dapat di buka melalui wireshark untuk mengetahui lebih jelas pesan yang di enkripsi untuk selanjut nya dapat kita terjemah kan menggunakan aplikasi online berbasis **base64**.

File kita open di wireshark dan langsung follow stream pada protokol SMTP. Kemudian find file



berekstensi docx. Copykan teks yang telah dienkripsi.

3. Buka link berikut untuk menerjemahkan teks enkripsi yang telah kita copy dari wireshark

<http://www.motobit.com/util/base64-decoder-encoder.asp>

berikut adalah tampilan dari link tersebut.

Browser tabs: (1) YouTube, Anggit: Mardian - 3 yang, LOGO UNSRI - Penelusur, [Write UP] CTF INDOXPL, Base64 Online - base64 d

Address bar: <https://www.motobit.com/util/base64-decoder-encoder.asp>

The **Form.SizeLimit** is 1000000bytes. Please, do not post more data using this form.

Type (or copy-paste) some text to a textbox below. The text can be a Base64 string to decode or any string to encode to a Base64.

AAAAADcBgAAd29yZC9fcmVscy9kb2N1bWVudC54bWwucmVsc1BLAQITABQABgATAAAAI0A600kIF00AAFGKAAARAAAAA... (Base64 encoded text)

or select a file to convert to a Base64 string.

Browse... No file selected. Convert the source data

What to do with the source data:

- encode the source data to a Base64 string (base64 encoding)
Maximum characters per line: 76
- decode the data from a Base64 string (base64 decoding)

Output data:


- output to a textbox (as a string)
- export to a binary file, filename:

Note: The source file is handled as a binary data. The textbox is handled as a string data, default character set for the textbox is 'iso-8859-1'. You can change the charset using form below.

Change character set

Base64 programming

Base64 component for ASP/VBS
VBS Base64 encoder and Base64 decoder



IC Markets
WWW.ICMARKETS.COM

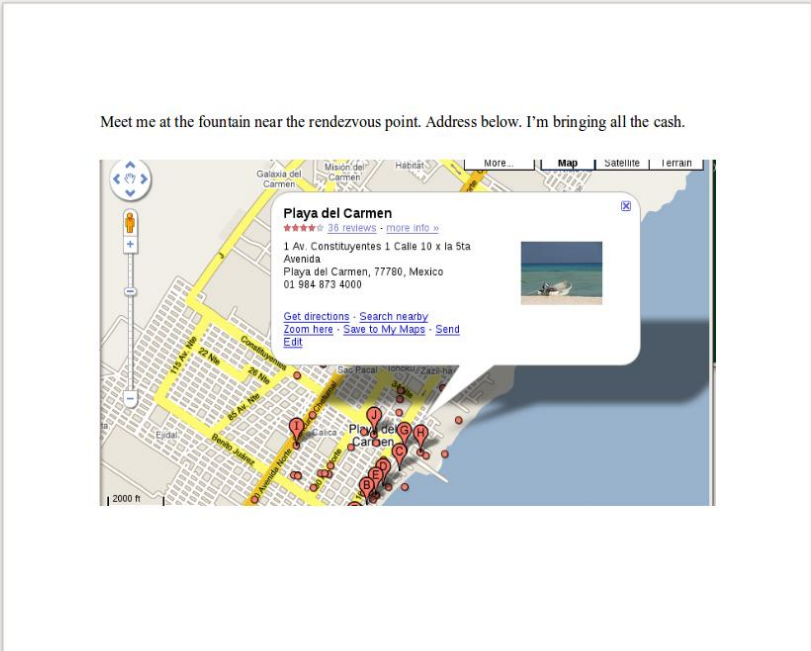
ZERO FEES ON
DEPOSITS
TRUE ECN FOREX BROKER

OPEN AN ACCOUNT NOW

Motobit.com

Pastekan teks yang telah kita copy ke dalam kolom yang telah tersedia. Pilih decode dan export file. Kita beri nama file tersebut dengan forensik.docx. Kemudian pilih convert the source data.

4. Buka file forensik.docx yang telah kita unduh



Meet me at the fountain near the rendezvous point. Address below. I'm bringing all the cash.

Playa del Carmen
 3.6 reviews · [more info](#)
 1 Av. Constituyentes 1 Calle 10 x la 5ta Avenida
 Playa del Carmen, 77780, Mexico
 01 984 873 4000

[Get directions](#) · [Search nearby](#)
[Zoom here](#) · [Save to My Maps](#) · [Send](#) · [Edit](#)

Page 1 / 1 | 16 words, 92 characters | Default Style | 100%

5. kita berhasil menemukan dimana lokasi pertemuan dua orang kriminal.

Daftar Pustaka

Anonim. 2017. [Write UP] CTF INDOXPLOIT – Hard Forensic. Online (<http://www.crypto1412.net/2017/04/write-up-ctf-indexploit-hard-forensic.html>). Diakses pada tanggal 4 april 2018.