TUGAS FORENSIK
KEAMANAN JARINGAN KOMPUTER

OLEH :

NAMA : ANGGIT MARDIAN
NIM : 09011281419062

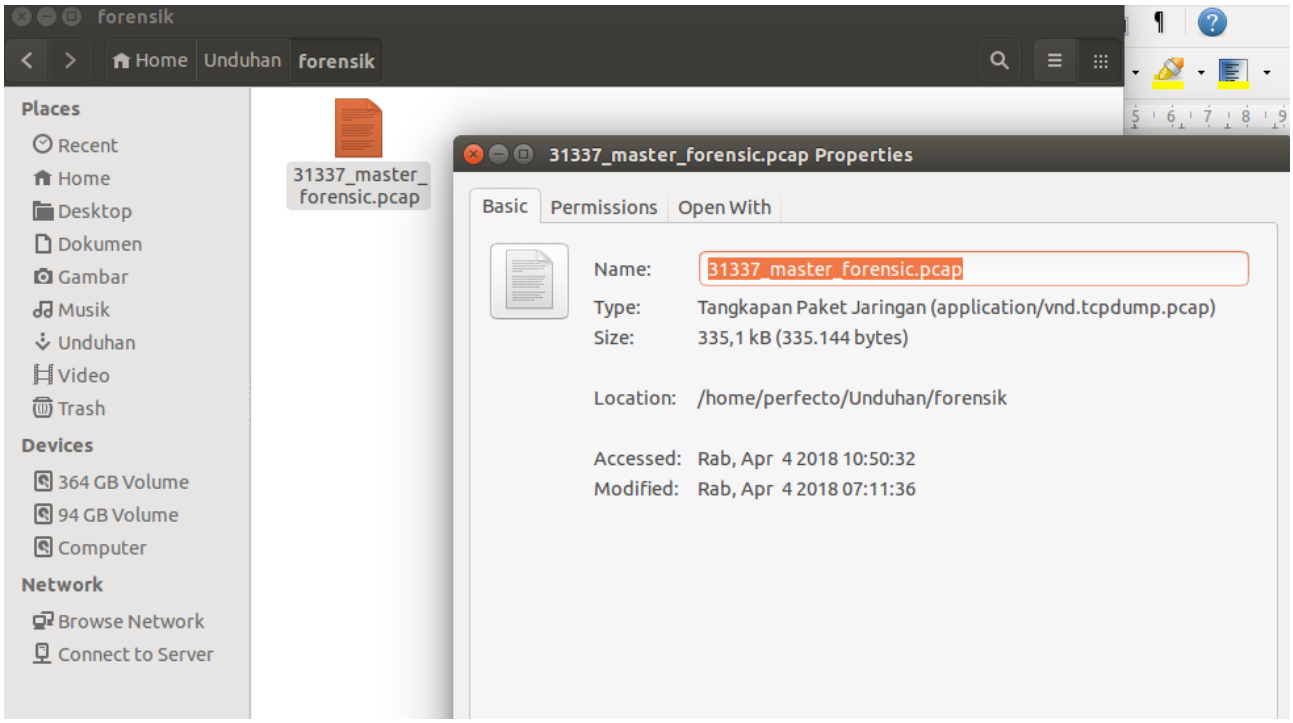
SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2018

FORENSIC FILE

Kasus :

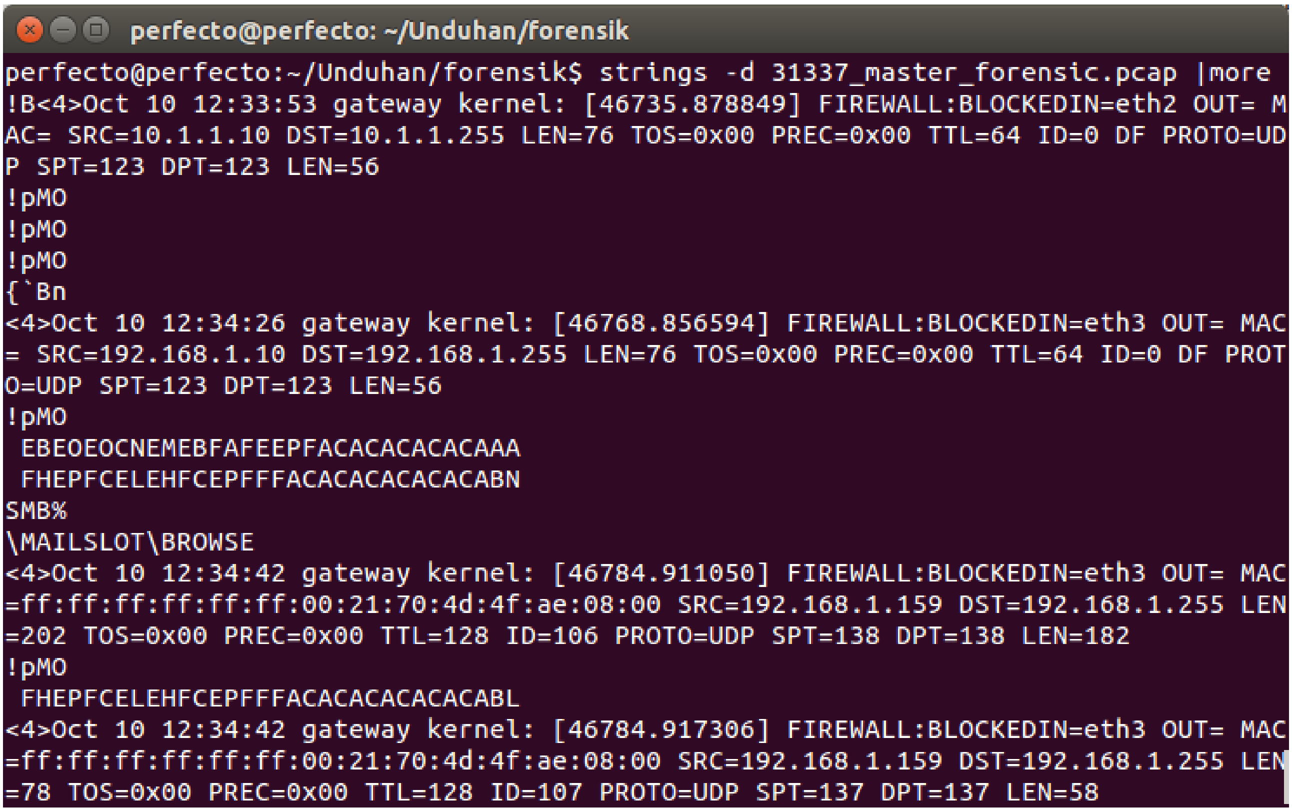
Didapat sebuah file pcap hasil penyadapan dua orang kriminal yang melakukan komunikasi untuk mengadakan pertemuan disebuah tempat. Melalui file pcap tersebut akan diketahui dimana lokasi pertemuan yang akan di lakukan oleh dua orang krimial.

File berukuran 355,1 KB



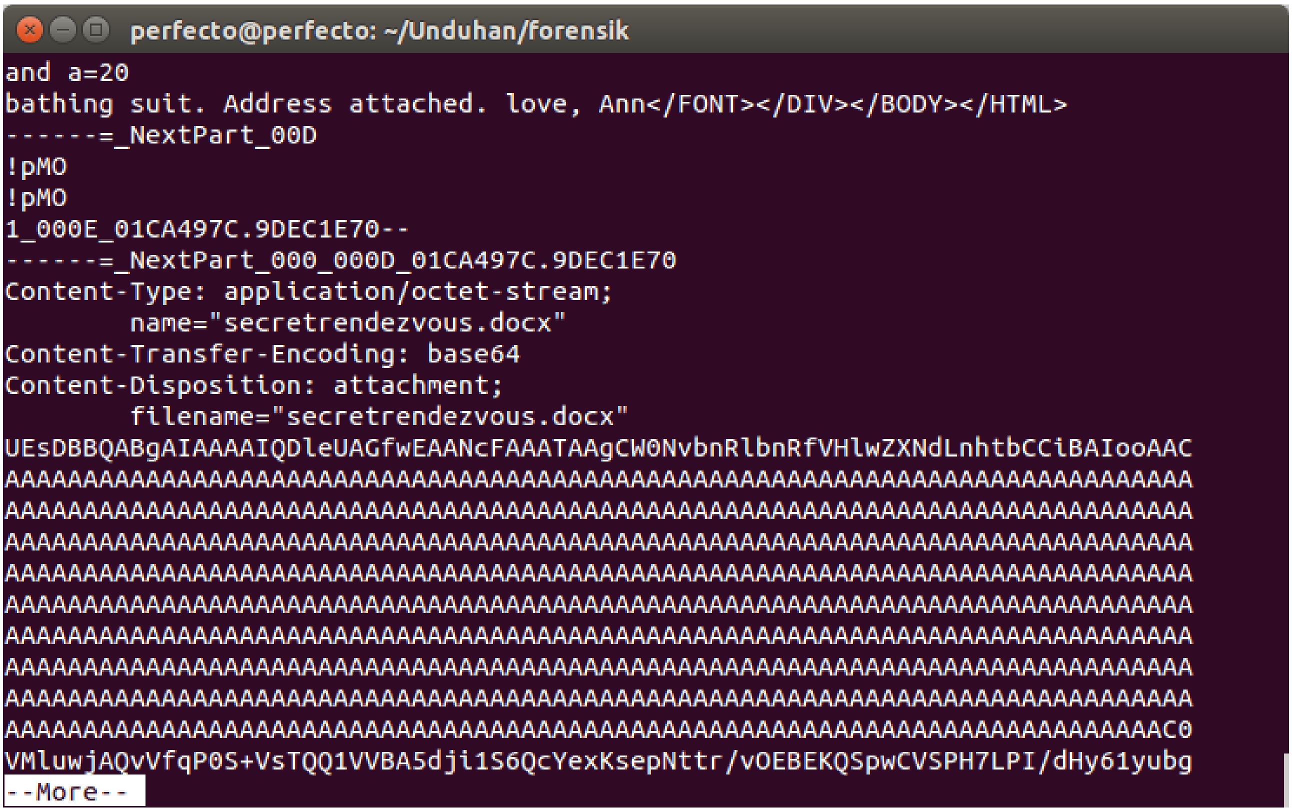
Langkah – langkah

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_forensic.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
 EBEOEOCNEMEBFAFEEPFACACACACACAAA
 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 dienkripsi. Berikut adalah tampilan email berisi file docx setelah mengetikkan perintah **"strings -d (nama file) |more"** tanpa tanda petik di dalam terminal linux.



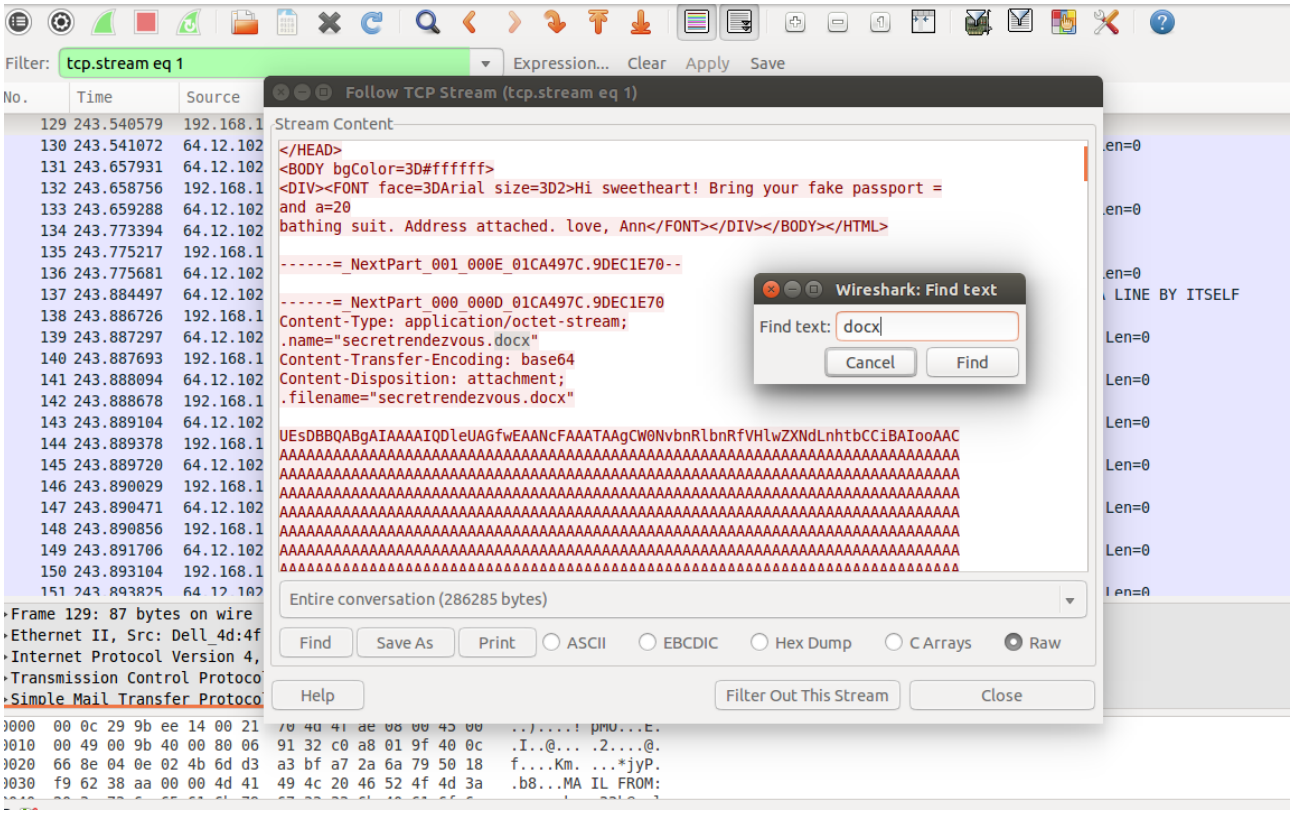
```
perfecto@perfecto: ~/Unduhan/forensik
and a=20
bathing suit. Address attached. love, Ann</FONT></DIV></BODY></HTML>
------=_NextPart_00D
!pMO
!pMO
1_000E_01CA497C.9DEC1E70--
------=_NextPart_000_000D_01CA497C.9DEC1E70
Content-Type: application/octet-stream;
        name="secretrendezvous.docx"
Content-Transfer-Encoding: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


```
UEsDBBQABgAIAAAAIQDleUAGfwEAANcFAAATAAgCW0NvbnRlbnRfVHlwZXNdLnhtbCCiBAIooAAC
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAC0
VMluwjAQvVfqP0S+VsTQQ1VVBA5dji1S6QcYexKSPPH7LPI/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

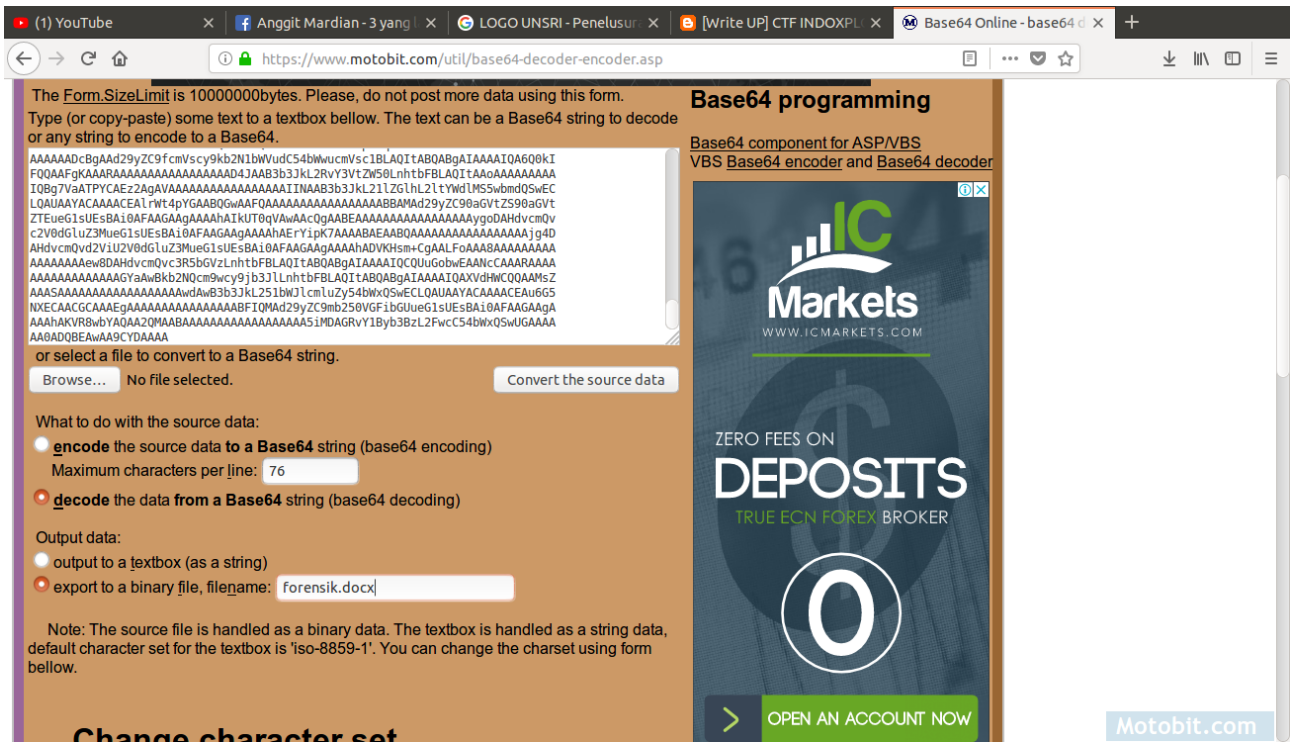


berekstensi docx. Copykan teks yang telah dienkripsi.

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

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

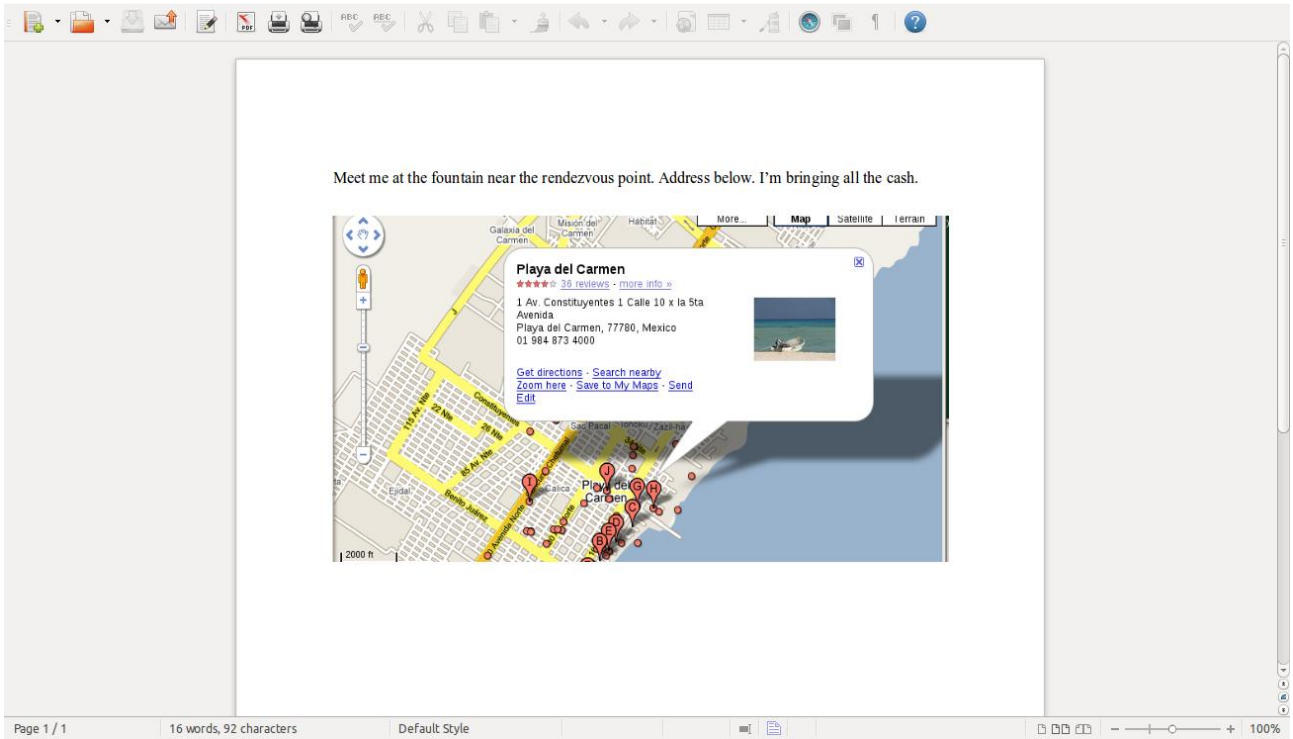
berikut adalah tampilan dari link tersebut.



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



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

Daftar Pusataka

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