Laporan Investigasi

2015

[Laporan investigasi forensika digital terhadap kasus Ann Dercover (Ann Skips Bail)]

[Laboratorium Forensika Digital]

Magister Informatika
Pascasarjana Fakultas Teknologi Industri
Universitas Islam Indonesia
Kampus Terpadu UII Jl. Kaliurang Km. 14,5 – Yogyakarta (55584)

Daftar Isi

Identitas Kasus

Deskripsi Kasus

Ann Dercover adalah tersangka dalam kasus *corporate spy* yang mencuri data penting perusahaan Anarchy-R-Us, Inc. dan menyelundupkannya kepada rekannya di luar perusahaan. Dia telah tertangkap namun dibebaskan dengan jaminan atau disebut penangguhan penahanan.

Dalam masa penangguhan tersebut, Ann Dercover pergi menghilang. Sebelum pergi, Ann sempat melakukan komunikasi melalui jaringan internetnya yang di-*capture* oleh investigator kasus Ann dari Kantor Polda DIY.

Investigator meminta kepada Laboratorium Forensika Digital UII untuk menganalisis file *packet capture* mengenai komunikasi Ann via jaringan internetnya, bertujuan untuk dapat menjawab pertanyaan yang diajukan oleh investigator mengenai informasi keberadaan Ann Dercover.

Memorandum untuk:

Kantor Polda DIY
Investigator Yudha
Jl. Lingkar Utara Condong Catur, Depok, Sleman, Yogyakarta - 55283

Subjek

Laporan Investigasi Forensika Digital
Subjek : Ann Dercover
Nomor Kasus : 007

Ringkasan Kasus

Pemohon	Yudha (Kator Polda DIY)
Alamat Pemohon	Jl. Lingkar Utara Condong Catur, Depok, Sleman, Yogyakarta - 55283
Pihak Penerima	Ninki Hermaduanti (Lab. Forensika Digital UII)
Waktu	Selasa, 4 Agustus 2015, pkl. 15.30 WIB
No. Kasus	007

Deskripsi Permohonan Investigasi

Deskripsi Barang Bukti

Barang bukti yang diajukan pada kasus Ann Dercover ini adalah berupa sebuah file *packet capture* bernama “evidence02.pcap”.

Investigator melakukan monitoring dan *packet capture* terhadap aktivitas komunikasi Ann melalui jaringan internet, sehingga didapatkanlah barang bukti berupa file tersebut.

Informasi yang Diinginkan

Barang bukti berupa file *packet capture* yang telah diajukan tersebut, diminta untuk diperiksa dan dianalisis sehingga didapatkan informasi sebagai berikut:

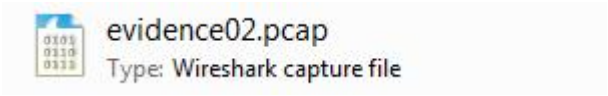
1. Alamat email milik Ann Dercover.
2. Password email milik Ann Dercover.
3. Alamat email milik kekasih Ann Dercover (Mr. X).
4. Barang yang Ann Dercover minta kepada Mr. X untuk dibawa.
5. Nama file *attachment* yang dikirimkan Ann Dercover kepada Mr. X.
6. MD5sum dari file *attachment* tersebut.
7. Kota dan negara di mana Ann Dercover dan Mr. X akan bertemu.
8. MD5sum dari *image* yang ada di dalam file *attachment* tersebut.

Proses Penerimaan Barang Bukti

Penerimaan Barang Bukti

Barang bukti yang akan diuji diterima oleh Laboratorium Forensika Digital UII melalui sebuah *flashdisk*. Di dalam *flashdisk* tersebut terdapat 2 (dua) buah file yaitu:

- File “evidence02.pcap”



- File “evidence02.md5”

Kunci *Hash*

Barang bukti berupa file “evidence02.pcap” yang akan diuji disertai dengan kunci *hash* yang ada pada file “evidence02.md5”, yaitu:

```
evidence02      cfac149a49175ac8e89d5b5b5d69bad3
```

Proses Eksaminasi Barang Bukti

Prosedur

Prosedur yang dilakukan dalam proses eksaminasi barang bukti adalah sebagai berikut:

1. Meng-*copy* file “evidence02.pcap” dan file “evidence02.md5” dari *flashdisk* dan disimpan di harddisk milik Lab.
2. Menyiapkan *environment system* untuk keperluan eksaminasi pada Laboratorium Forensika Digital UII yang berada pada area Pusat Pelatihan ITCentrum FTI UII.
3. Menggunakan sistem operasi Kali Linux beserta *tool* dan *command* di dalamnya untuk melakukan eksaminasi terhadap file “evidence02.pcap”, seperti *tool* Wireshark dan *command* tcpflow.
4. Memeriksa dan menganalisis file “evidence02.pcap” kemudian melakukan *screenshot* hasil temuan sesuai dengan target informasi yang diharapkan.
5. Melaporkan temuan secara internal team Laboratorium Forensika Digital UII maupun eksternal kepada pihak pemohon.

Waktu & Tempat

Proses eksaminasi barang bukti dilakukan pada:

- Waktu : Rabu, 5 Agustus 2015, pkl. 08.00 – 16.00 WIB
- Tempat : Laboratorium Forensika Digital UII (Pusat Pelatihan ITCentrum UII)

Hasil Eksaminasi

Perbandingan Kunci *Hash*

Kunci *hash* yang disertakan di dalam file "evidence02.md5" bersama dengan file "evidence02.pcap" adalah cfac149a49175ac8e89d5b5b5d69bad3.
Kunci tersebut akan dibandingkan dengan hasil MD5sum menggunakan sistem operasi Kali Linux. Berikut adalah hasilnya:

```
root@kali:/home/Ann_Dercover# md5sum evidence02.pcap
cfac149a49175ac8e89d5b5b5d69bad3  evidence02.pcap
```

Terlihat bahwa kunci *hash* dari file "evidence02.pcap" di dalam file "evidence02.md5" dan hasil *generate* dengan *command* md5sum menggunakan sistem operasi Kali Linux adalah sama. Hal ini menunjukkan bahwa tidak ada perubahan di dalam file "evidence02.pcap".

Hasil Eksaminasi Barang Bukti

Hasil eksaminasi barang bukti berupa file "evidence02.pcap" adalah sebagai berikut:

1. Melakukan ekstraksi file "evidence02.pcap" dengan tcpflow, memeriksa satu per satu file hasil ekstraksi tcpflow tersebut, dan mencari alamat email yang terlibat di dalam komunikasi melalui jaringan internet Ann Dercover. Hasilnya adalah sebagai berikut:

Nama File Hasil "tcpflow"	Alamat Email yang Ditemukan
064.012.102.142.00587- 192.168.001.159.01036	N/A
064.012.102.142.00587- 192.168.001.159.01038	N/A
192.168.001.159.01036- 064.012.102.142.00587	sneakyg33k@aol.com sec558@gmail.com
192.168.001.159.01038- 064.012.102.142.00587	sneakyg33k@aol.com misersecretx@aol.com

Memeriksa satu per satu file hasil ekstraksi tcpflow tersebut, dan mencari email apapun yang ada di dalam komunikasi melalui jaringan internet Ann Dercover. Hasilnya adalah sebagai berikut:

Nama File Hasil "tcpflow"	Email yang Ditemukan
064.012.102.142.00587- 192.168.001.159.01036	N/A

064.012.102.142.00587- 192.168.001.159.01038	N/A
192.168.001.159.01036- 064.012.102.142.00587	from: sneakyg33k@aol.com to : sec558@gmail.com Sorry-- I can't do lunch next week after all. Heading out of town. Another time! –Ann
192.168.001.159.01038- 064.012.102.142.00587	from: sneakyg33k@aol.com to: misersecretx@aol.com Hi sweetheart! Bring your fake passport and a bathing suit. Address attached. love, Ann

Jika dilihat dari isi email-nya, Ann Dercover menuliskan namanya di setiap akhir email. Email-email dari Ann Dercover tersebut dikirim oleh sneakyg33k@aol.com.

2. Sesuai dengan pemeriksaan file hasil ekstraksi tcpflow, diketahui bahwa alamat email Ann Dercover adalah sneakyg33k@aol.com dilihat dari file "192.168.001.159.01036-064.012.102.142.00587" dan file "192.168.001.159.01038-064.012.102.142.00587". Kedua file tersebut adalah file yang berisi komunikasi dari IP *source* 192.168.1.159 ke IP *address* 64.12.102.142.

   Melakukan pemeriksaan file "evidence02.pcap" menggunakan *tool* Wireshark dan memfilternya berdasarkan IP, yaitu ip.src==192.168.1.159&&ip.addr==64.12.102.142, kemudian melakukan Follow TCP Stream.

   Autentikasi email menggunakan PLAIN SMTP, yaitu username dan password email berupa *plain-text* yang di-*encode* dengan base64. Pada bagian bawah tulisan "AUTH LOGIN" terdapat karakter-karakter sebagai berikut:
   334 VXNlcm5hbWU6
   c25lYWt5ZzMza0Bhb2wuY29t
   334 UGFzc3dvcmQ6
   NTU4cjAwbHo=

   Melakukan *decode* dengan base64 dan hasilnya adalah sebagai berikut:
   334 Username:
   sneakyg33k@aol.com
   334 Password:
   558r00lz

   Dapat disimpulkan bahwa password email Ann adalah 558r00lz.

3. Merujuk kepada tabel kedua pada *point* nomor 1 mengenai email yang ditemukan dalam komunikasi jaringan internet Ann Dercover, yaitu pada file "192.168.001.159.01038-064.012.102.142.00587", terdapat email dari sneakyg33k@aol.com kepada mistersecretx@aol.com yang berisi:

   Hi sweetheart! Bring your fake passport and a bathing suit. Address attached. love, Ann

   Dari isi email tersebut, dapat diasumsikan bahwa Ann Dercover mengirim email tersebut kepada kekasihnya (Mr. X). Email tersebut dikirim ke alamat mistersecretx@aol.com.

4. Sesuai isi email pada *point* nomor 3, Ann Dercover meminta Mr. X untuk membawa paspor palsu (*fake passport*) dan baju renang (*bathing suit*).

5. Memeriksa secara lengkap file hasil ekstraksi tcpflow, yaitu file "192.168.001.159.01038-064.012.102.142.00587" yang berisi email kiriman Ann Dercover kepada Mr. X. Ditemukan sebuah *attachment* berupa file .DOCX bernama "secretrendezvous.docx".

6. Untuk mendapatkan nilai MD5sum dari file "secretrendezvous.docx", maka perlu dilakukan ekstraksi file tersebut dari file "evidence02.pcap". Caranya adalah dengan membuka file "192.168.001.159.01038-064.012.102.142.00587" dan mengambil semua karakter di bagian bawah tulisan filename="secretrendezvous.docx", yaitu UEsDBBQABg… dst.
   sampai sebelum tulisan:
   ——=_NextPart_000_000D_01CA497C.9DEC1E70–
   .
   QUIT
   yaitu AA0ADQBEAwAA9CYDAAAA.

   Kemudian memasukkannya ke dalam file *temporary*, men-*decode* karakter tersebut dengan base64, dan memasukkan hasil akhirnya ke dalam file "secretrendezvous.docx". Hasilnya adalah sebagai berikut:

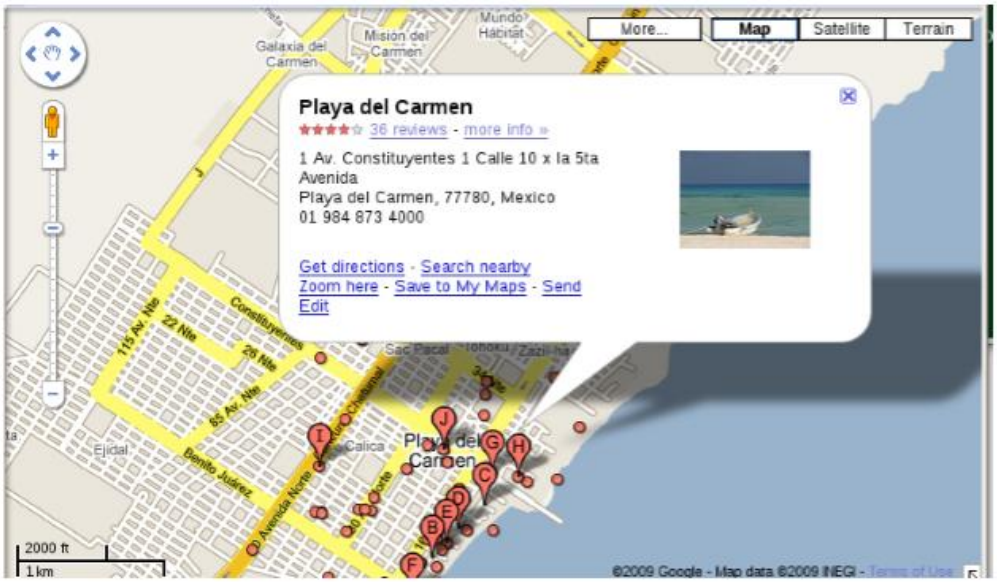
   

   secretrendezvous.docx

   Kemudian melakukan proses *generate* nilai MD5 terhadap file "secretrendezvous.docx" dan menghasilkan nilai 9e423e11db88f01bbff81172839e1923.

7. Memeriksa file “secretrendezvous.docx” untuk mencari informasi mengenai keberadaan Ann Dercover dan Mr. X.

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



Ann Dercover dan Mr. X akan bertemu di kota Playa del Carmen, Mexico.

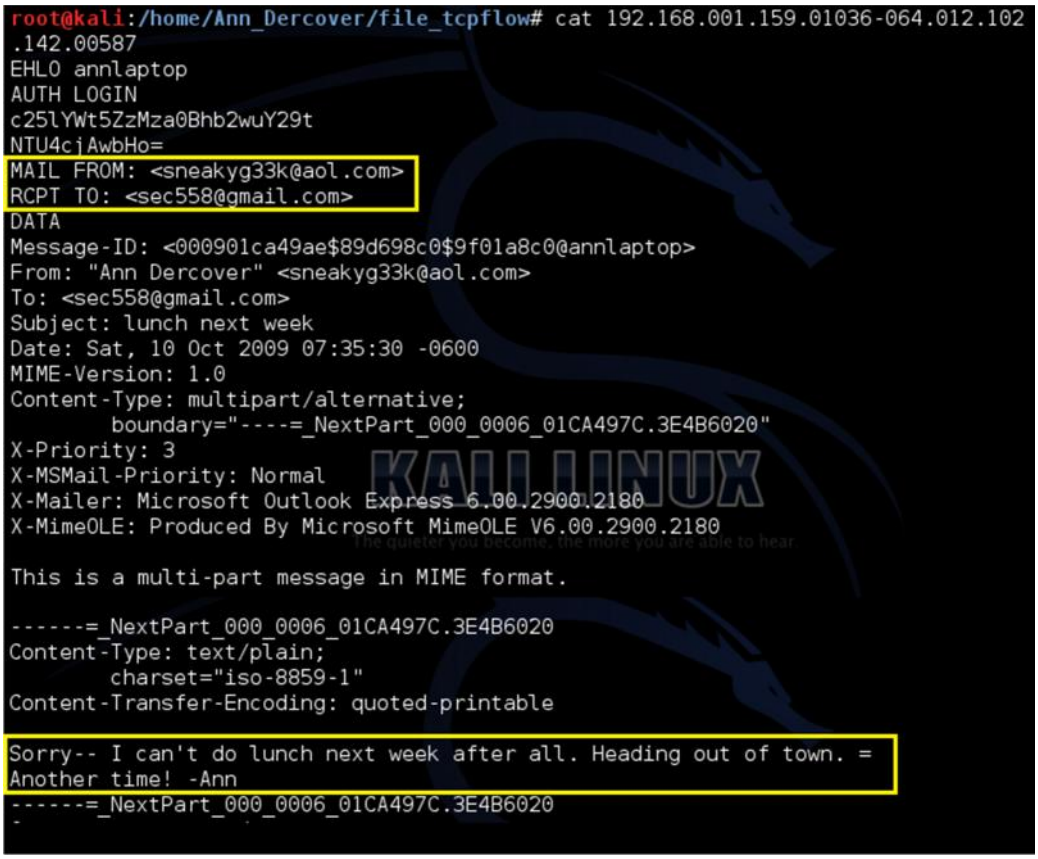
8. Untuk mengetahui nilai MD5sum dari *image* atau gambar yang ada di dalam file “secretrendezvous.docx” tersebut, perlu dilakukan ekstraksi file “secretrendezvous.docx” ke dalam sebuah folder, kemudian mencari gambar yang dimaksud dan men-*generate* MD5sum dari gambar tersebut. Dan didapatkan hasilnya, yaitu aadeace50997b1ba24b09ac2ef1940b7.

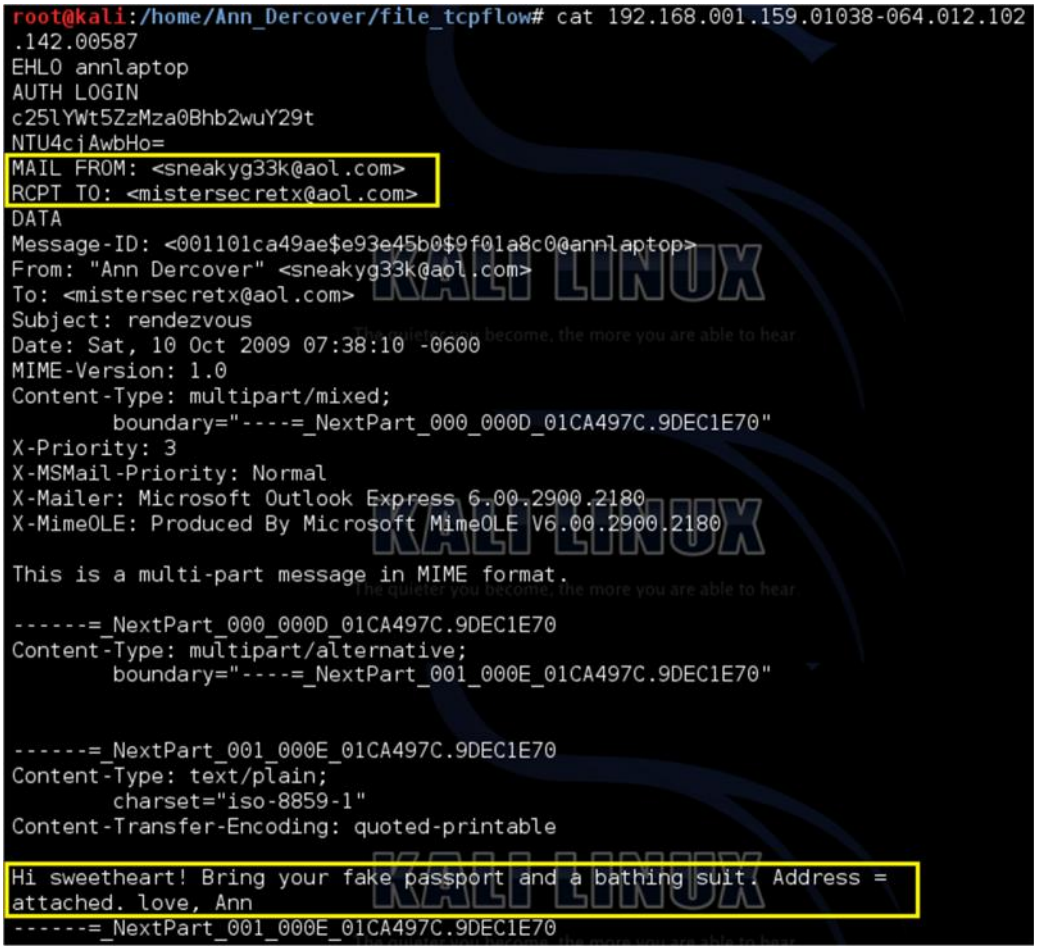
Kesimpulan Akhir

Hasil Analisis

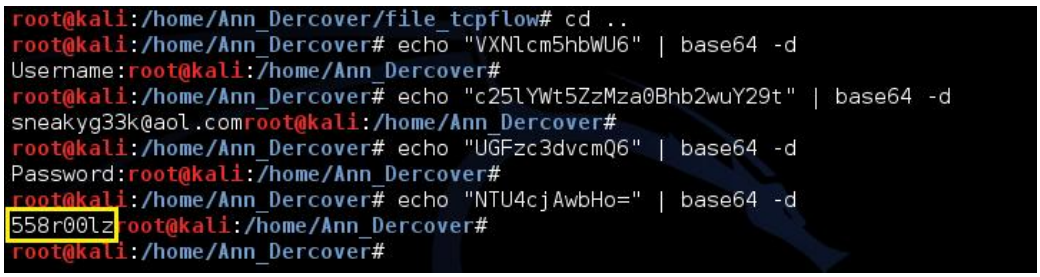
Hasil analisis telah dapat menjawab pertanyaan mengenai informasi yang diinginkan oleh pihak pemohon. Adapun *screenshot* informasi yang ditemukan adalah sebagai berikut:

1. Alamat email milik Ann Dercover adalah sneakyg33k@aol.com.





2. Password email milik Ann Dercover adalah 558r00lz.



3. Alamat email milik kekasih Ann Dercover (Mr. X) adalah mistersecretx@aol.com.

   Screenshot merujuk pada *screenshot* nomor 1.

4. Barang yang Ann Dercover minta kepada Mr. X untuk dibawa adalah paspor palsu dan baju renang.

   Screenshot merujuk pada *screenshot* nomor 1.

5. Nama file *attachment* yang dikirimkan Ann Dercover kepada Mr. X adalah “secretrendezvous.docx”.

```
<STYLE></STYLE>
</HEAD>
<BODY bgColor=3D#ffffff>
<DIV><FONT face=3DArial size=3D2>Hi sweetheart! Bring your fake passport =
and a=20
bathing suit. Address attached. love, Ann</FONT></DIV></BODY></HTML>

------=_NextPart_001_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
```

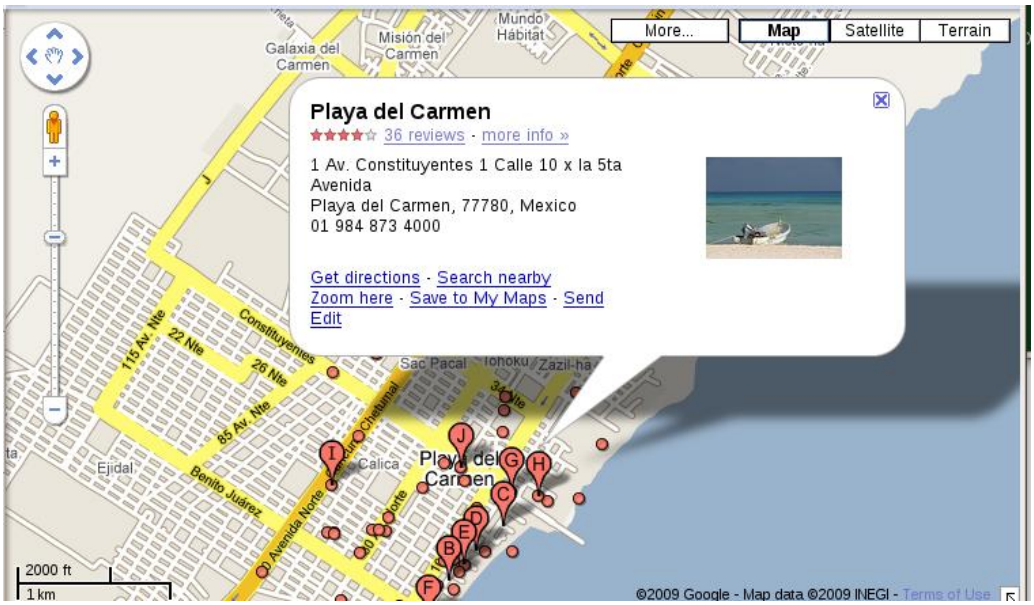
6. Nilai hasil MD5sum dari file “secretrendezvous.docx” adalah 9e423e11db88f01bbff81172839e1923.

```
root@kali:/home/Ann_Dercover# sed -n '61,3700p' secretrendezvous.txt | tr -d "\r
\n" > secretrendezvous.encoded
root@kali:/home/Ann_Dercover# ls
evidence02.pcap   secretrendezvous.encoded
file_tcpflow      secretrendezvous.txt
root@kali:/home/Ann_Dercover#
```

```
root@kali:/home/Ann_Dercover# base64 -d secretrendezvous.encoded > secretrendezv
ous.docx
root@kali:/home/Ann_Dercover# ls
evidence02.pcap          secretrencezvous.encoded
file_tcpflow             secretrendezvous.txt
secretrendezvous.docx
root@kali:/home/Ann_Dercover#
```

```
root@kali:/home/Ann_Dercover# md5sum secretrendezvous.docx
9e423e11db88f01bbff81172839e1923  secretrendezvous.docx
root@kali:/home/Ann_Dercover#
```

7. Ann Dercover dan Mr. X akan bertemu di Playa del Carmen, Mexico.



8. Nilai hasil MD5sum dari *image* yang ada di dalam file “secretrendezvous.docx” adalah aadeace50997b1ba24b09ac2ef1940b7.

```
root@kali:/home/Ann_Dercover# mkdir file_extract
root@kali:/home/Ann_Dercover# unzip secretrendezvous.docx -d file_extract/
Archive:  secretrendezvous.docx
  inflating: file_extract/[Content_Types].xml
  inflating: file_extract/_rels/.rels
  inflating: file_extract/word/_rels/document.xml.rels
  inflating: file_extract/word/document.xml
 extracting: file_extract/word/media/image1.png
  inflating: file_extract/word/theme/theme1.xml
  inflating: file_extract/word/settings.xml
  inflating: file_extract/word/webSettings.xml
  inflating: file_extract/word/styles.xml
  inflating: file_extract/docProps/core.xml
  inflating: file_extract/word/numbering.xml
  inflating: file_extract/word/fontTable.xml
  inflating: file_extract/docProps/app.xml
root@kali:/home/Ann_Dercover# md5sum file_extract/word/media/image1.png
aadeace50997b1ba24b09ac2ef1940b7  file_extract/word/media/image1.png
root@kali:/home/Ann_Dercover#
```

Kesimpulan

Berdasarkan proses pemeriksaan dan analisis terhadap file “evidence02.pcap” menggunakan *tool* Wireshark dan *command* dalam sistem operasi Kali Linux, maka didapatkan beberapa hasil temuan. Temuan-temuan ini telah menjawab pertanyaan mengenai informasi yang diinginkan oleh pihak pemohon.

Informasi Kontak

[Laboratorium Forensika Digital]
Magister Informatika
Pascasarjana Fakultas Teknologi Industri
Universitas Islam Indonesia
Kampus Terpadu UII Jl. Kaliurang Km. 14,5 – Yogyakarta (55584)
Tel +62 274 895287
Fax +62 274 895007
http://fit.uii.ac.id