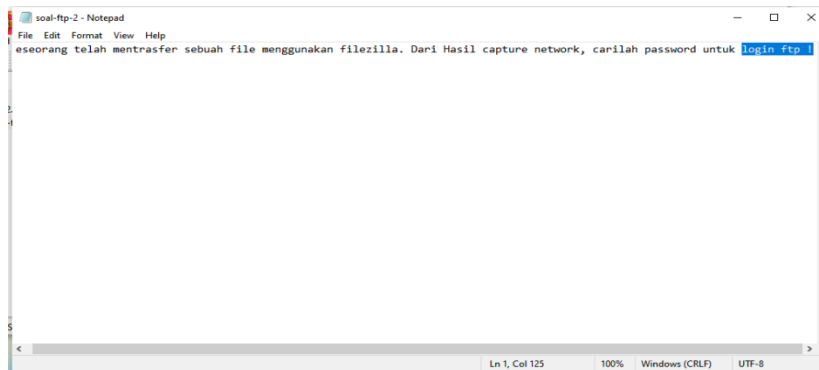


LATIHAN CYBER SECURITY

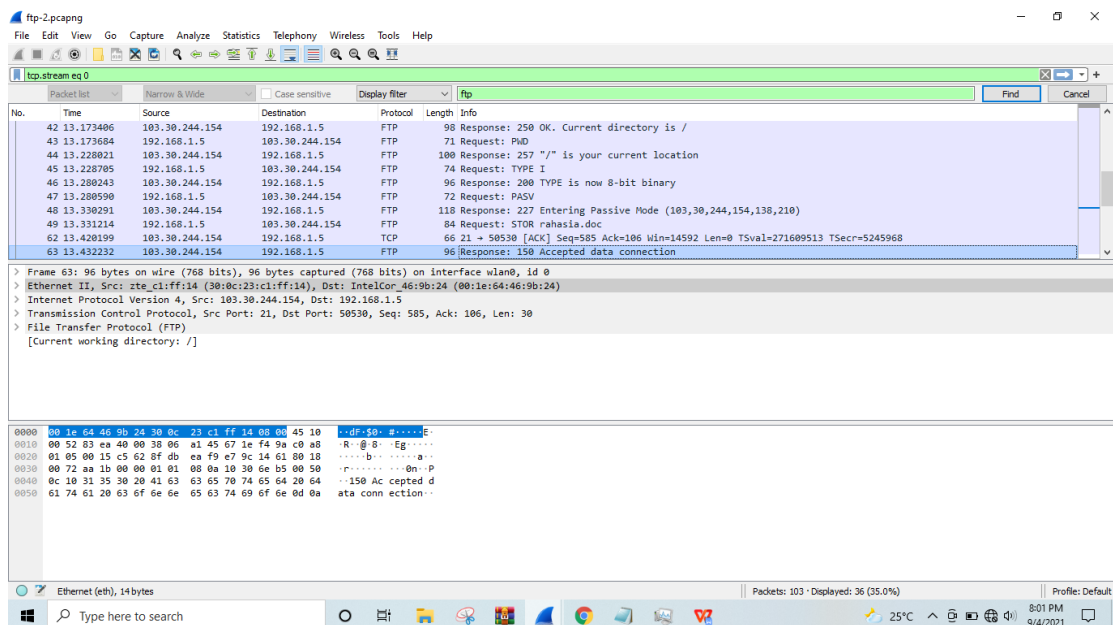
REZKA NORHAFIZAH

NETWORK 1

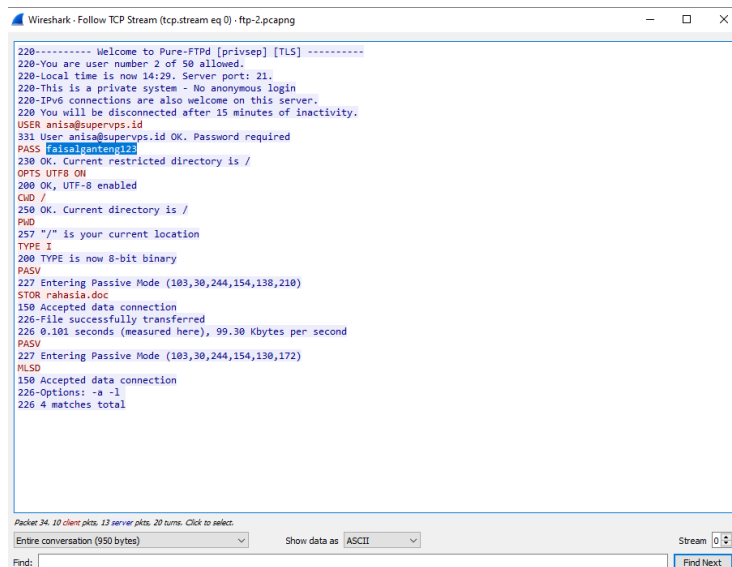
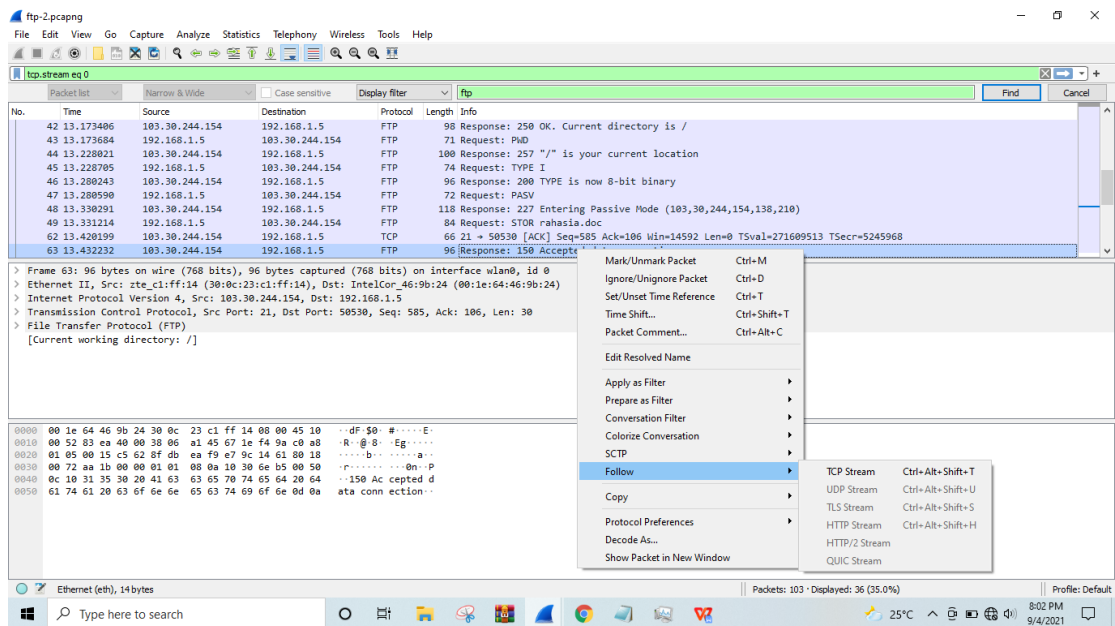
1. Setelah dibuka muncul soal :



2. Kemudian saya buka file ftp-2.pcapng menggunakan aplikasi Wireshark dan saya lakukan display filter ftp seperti berikut :



3. Kemudian saya lakukan follow tcp stream pada packet 63

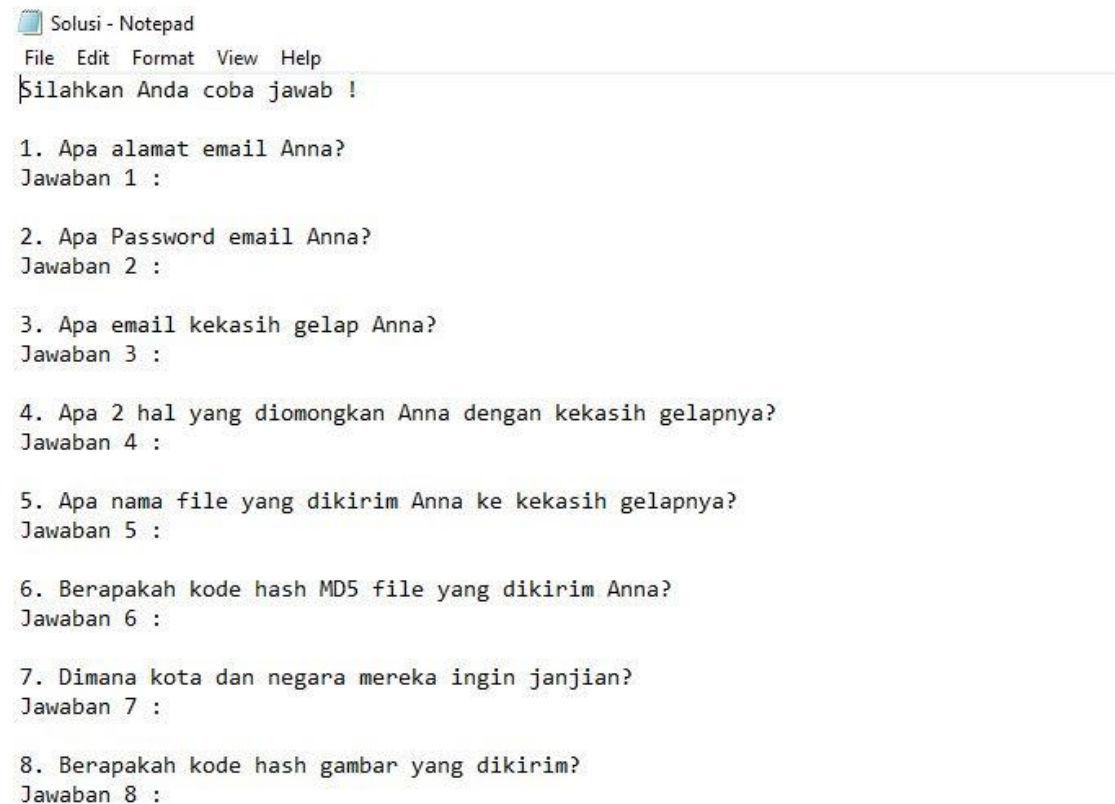


Maka muncul seperti di atas.

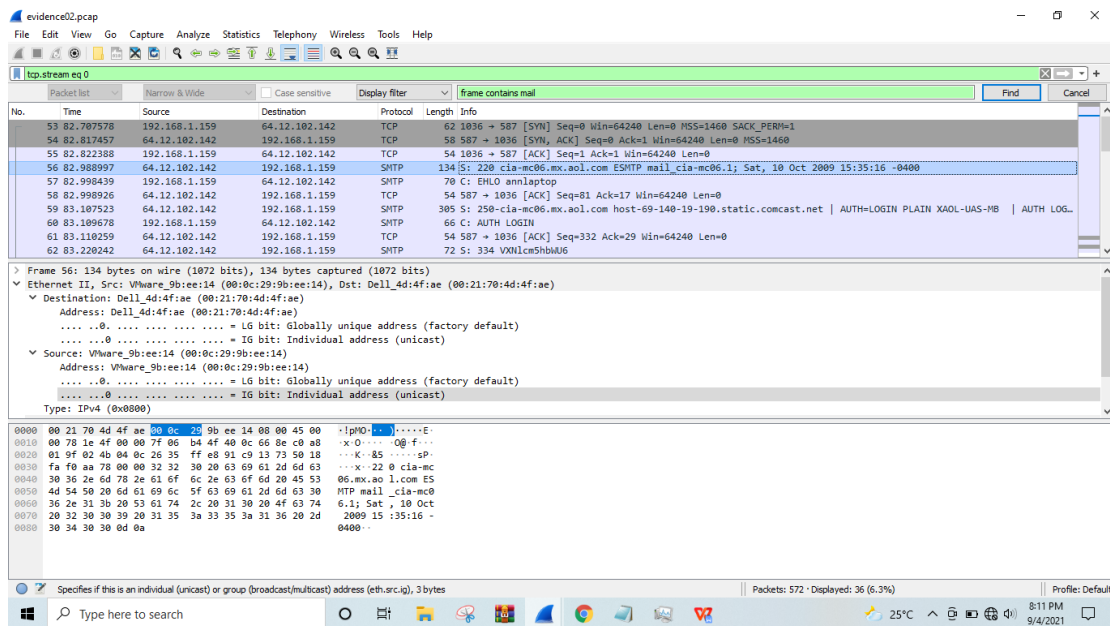
PASSWORD faisalganteng123

NETWORK 2

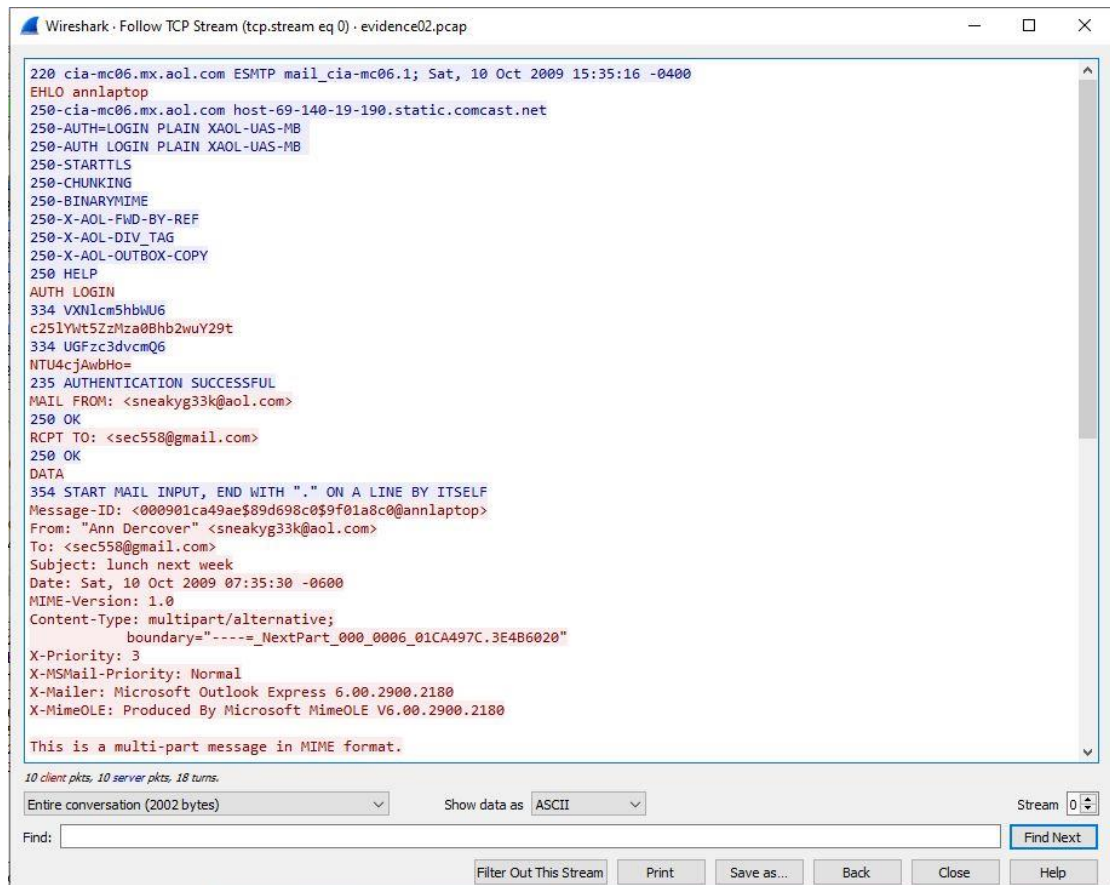
1. Setelah dibuka muncul soal :



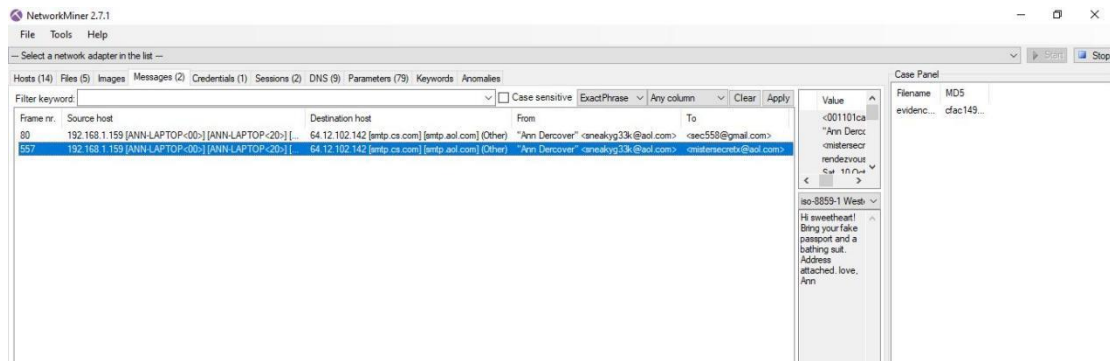
2. Kemudian saya buka file evidence02.pcap menggunakan aplikasi Wireshark dan saya lakukan display filter frame contains mail seperti berikut :



Kemudian saya lakukan follow tcp stream pada packet 56 kemudian muncul seperti berikut :



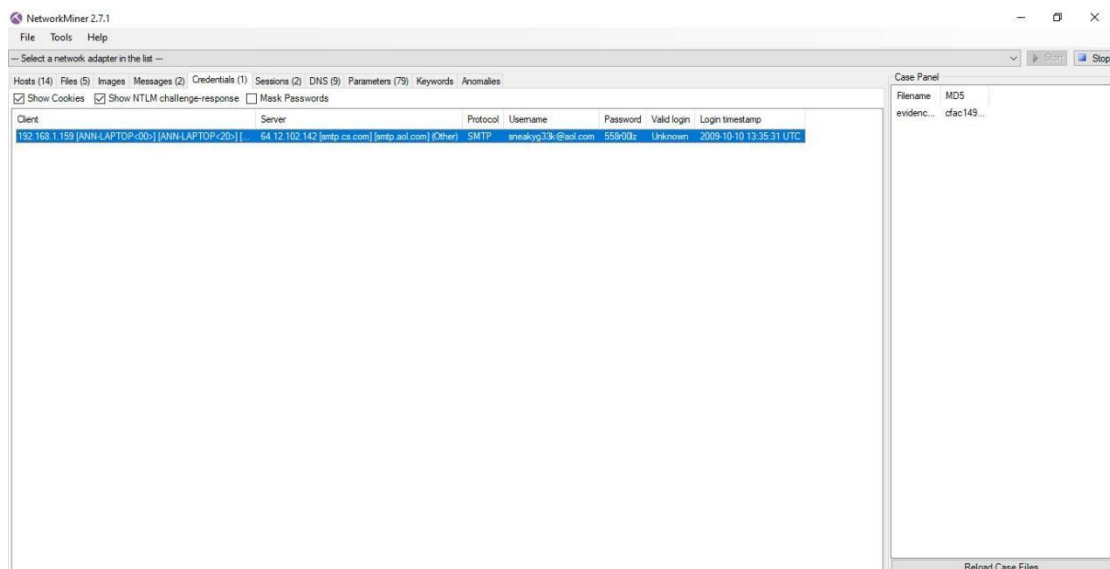
Kemudian saya buka lagi file tersebut menggunakan aplikasi Network Miner dan didapat :



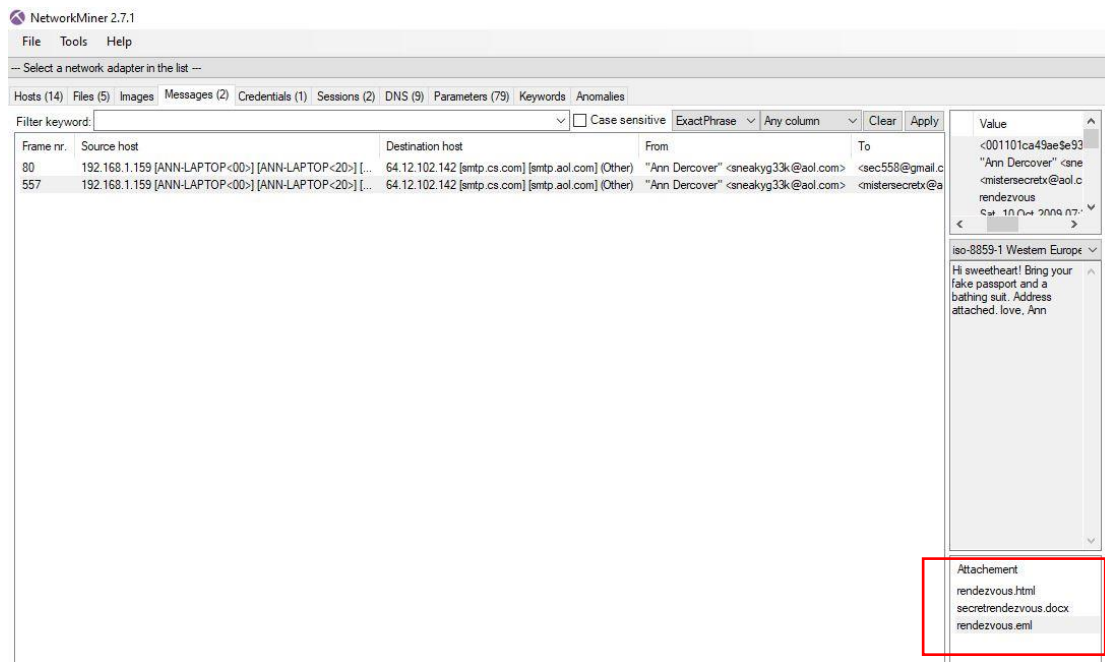
Email Anna : sneakyg33k@aol.com

Email kekasih gelap Anna : mistersecretx@aol.com

2 hal yang diomongkan Anna dengan kekasih gelapnya : bring fake passport and a bathing suit (address attached)



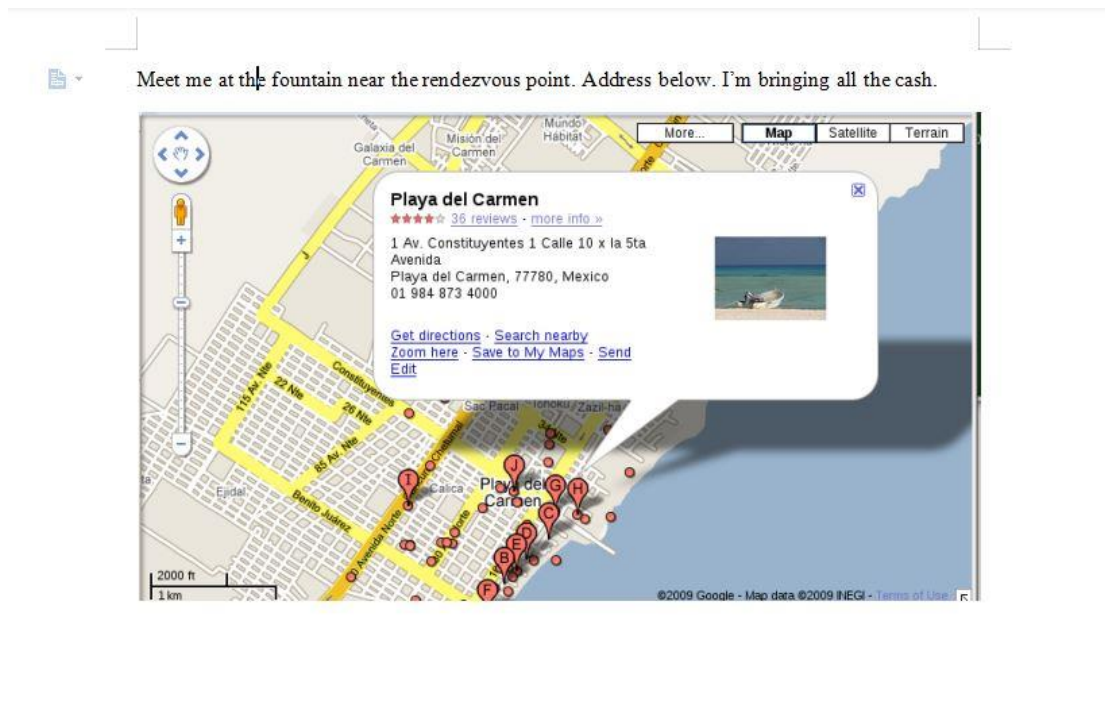
Password email Anna : 558r00lz

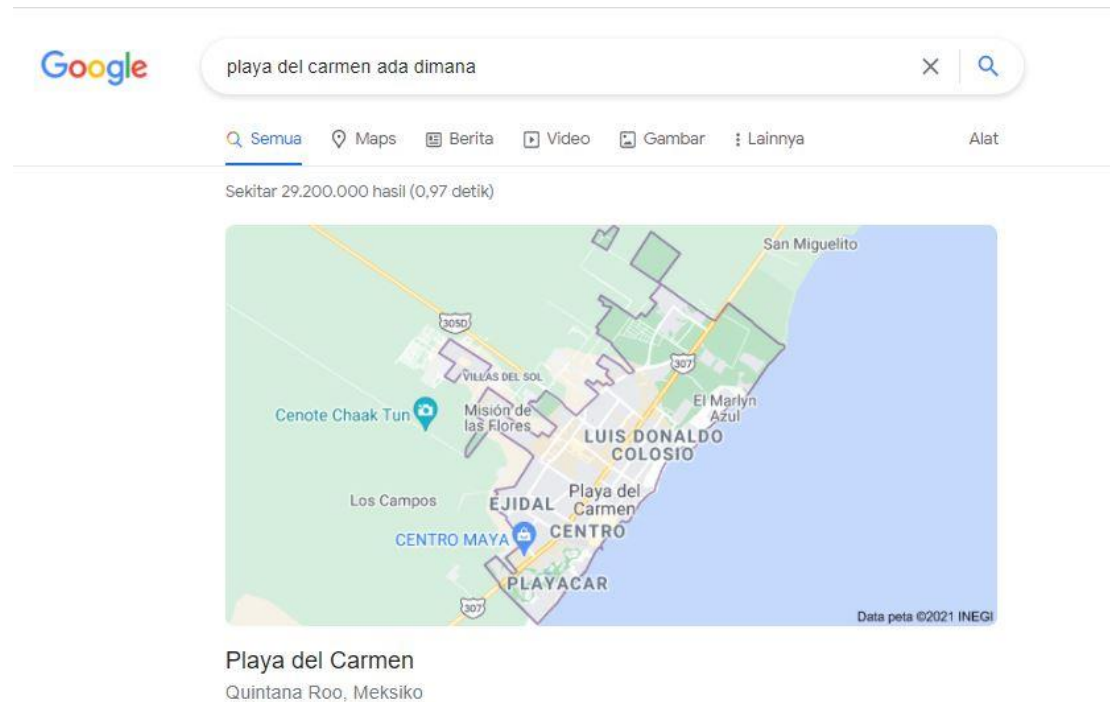


Nama file yang dikirim Anna ke kekasih gelapnya :

- secretrendezvous.docx
- rendezvous.html
- rendezvous.eml

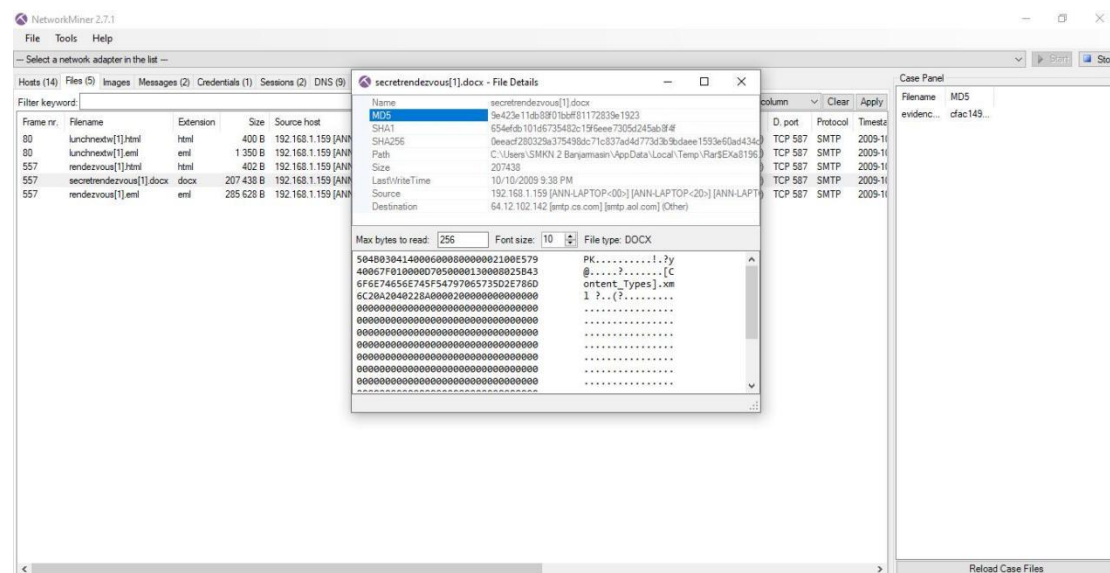
Kemudian saya buka file secretrendezvous.docx dan didapat :





kota dan negara mereka ingin janji : di Playa Del Carmen di Kota Quintana Roo, Meksiko

Lalu saya pergi ke tab files dan klik kanan untuk open details, maka muncul seperti berikut :



Kode hash MD5 file yang dikirim Anna :

- secretrendezvous.docx : 9e423e11db88f01bbff81172839e1923
- rendesvous.html : d07c3b721fed36a725c01e4827c1a563

Kemudian saya cari hash image tersebut di url imageforensic.org dan didapat :

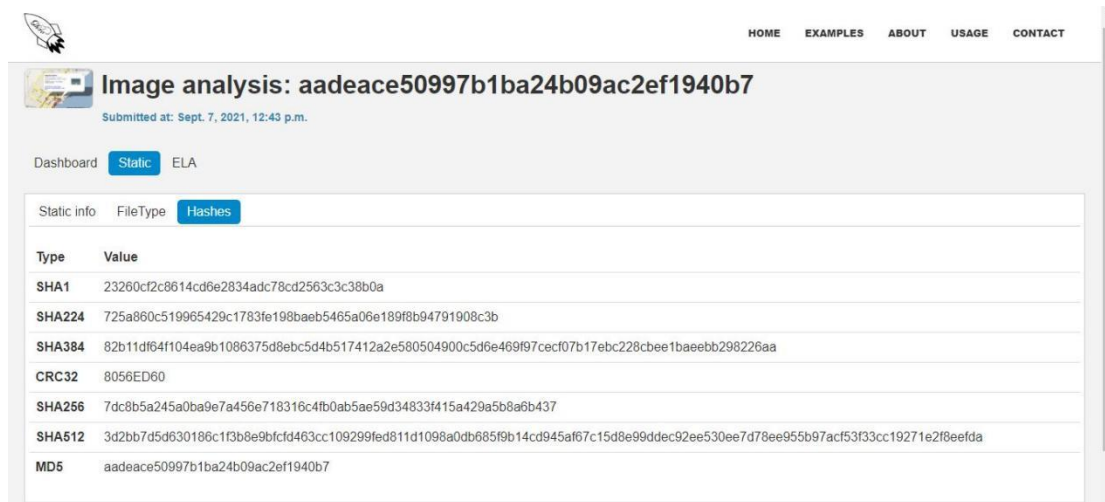


Image analysis: aadeace50997b1ba24b09ac2ef1940b7
Submitted at: Sept. 7, 2021, 12:43 p.m.

Dashboard Static ELA

Static info FileType Hashes

| Type | Value |
|--------|-----------------------------------------------------------------------------------------------------------------------------------|
| SHA1 | 23260cf2c8614cd6e2834adc78cd2563c3c38b0a |
| SHA224 | 725a860c519965429c1783fe198baeb5465a06e189f8b94791908c3b |
| SHA384 | 82b11df64f104ea9b1086375d8ebc5d4b517412a2e580504900c5d6e469f97cecf07b17ebc228cbee1baeebb298226aa |
| CRC32 | 8056ED60 |
| SHA256 | 7dc8b5a245a0ba9e7a456e718316c4fb0ab5ae59d34833f415a429a5b8a6b437 |
| SHA512 | 3d2bb7d5d630186c1f3b8e9bfcfd463cc109299fed811d1098a0db685f9b14cd945af67c15d8e99dddec92ee530ee7d78ee955b97acf53f33cc19271e2f8eefda |
| MD5 | aadeace50997b1ba24b09ac2ef1940b7 |

Kode hash gambar yang dikirim : aadeace50997b1ba24b09ac2ef1940b7

Kesimpulan :

*Jawaban network 2 - Notepad

File Edit Format View Help

Silahkan Anda coba jawab !

1. Apa alamat email Anna?
Jawaban 1 : sneakyg33k@aol.com
2. Apa Password email Anna?
Jawaban 2 : 558r001z
3. Apa email kekasih gelap Anna?
Jawaban 3 : mistersecretx@aol.com
4. Apa 2 hal yang diomongkan Anna dengan kekasih gelapnya?
Jawaban 4 : bring fake passport and a bathing suit (address attached)
5. Apa nama file yang dikirim Anna ke kekasih gelapnya?
Jawaban 5 : secretrendezvous.docx, rendezvous.html, rendezvous.eml
6. Berapakah kode hash MD5 file yang dikirim Anna?
Jawaban 6 :- secretrendezvous.docx : 9e423e11db88f01bbff81172839e1923
- rendezvous.html : d07c3b721fed36a725c01e4827c1a563
- rendezvous.eml : d3e4673749343d1e0fba06552bc0b035
7. Dimana kota dan negara mereka ingin janji?
Jawaban 7 : di Playa Del Carmen di Kota Quintana Roo, Meksiko
8. Berapakah kode hash gambar yang dikirim?
Jawaban 8 : aadeace50997b1ba24b09ac2ef1940b7