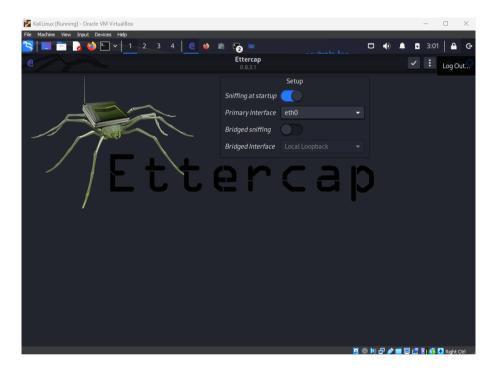
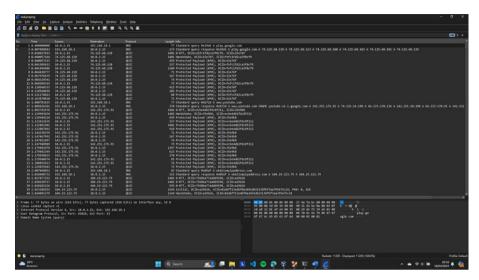
Pada Bagian network forensics saya membantu dalam pembuatan image MITM atau man in the middle dengan menggunakan ettercap yang ada di linux.



Untuk capturing dan analisis nya saya menggunakan wireshark. Berikut beberapa dokumentasinya



Tampilan ketika file image dibuka

```
Wireshark · Packet 11022 · real.pcapng
        Frame 11022: 44 bytes on wire (352 bits), 44 bytes captured (352 bits) on interface any, id 0 Linux cooked capture v1
                                                                                                      10.0.2.2 (08:00:27:4a:fa:bc) - also in use by 52:54:00:12:35:02 (frame 11021)]
              uplicate IP address detected for 10.0.2.2 (08:00:27:4a:fa:bc) - also in use by 52:54:00:12:35:02 (frame 11021)]
[Frame showing earlier use of IP address; 11021]
[Expert Info (Marning/Sequence): Duplicate IP address configured (10.0.2.2)]
[Severity level: Marning]
[Group: Sequence]
[Seconds since earlier frame seen: 0]
uplicate IP address detected for 10.0.2.4 (52:54:00:12:35:04) - also in use by 08:00:27:4a:fa:bc (frame 11021)]
[Irame showing earlier use of IP address; 11021]

* [Expert Info (Marning/Sequence): Duplicate IP address configured (10.0.2.4)]
[Severity level: Marning]
[Group: Sequence]
[Seconds since earlier frame seen: 0]
                00 04 00 01 00 06 08 00 27 4a fa bc 00 00 08 06 00 01 08 00 06 04 00 02 08 00 27 4a fa bc 0a 00 02 02 02 52 54 00 12 35 04 0a 00 02 04
Show packet bytes
```

Duplikasi IP yang terjadi

Filtering ARP poison attack



Menambah label



Memberi nama label