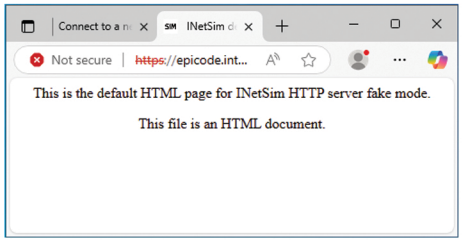
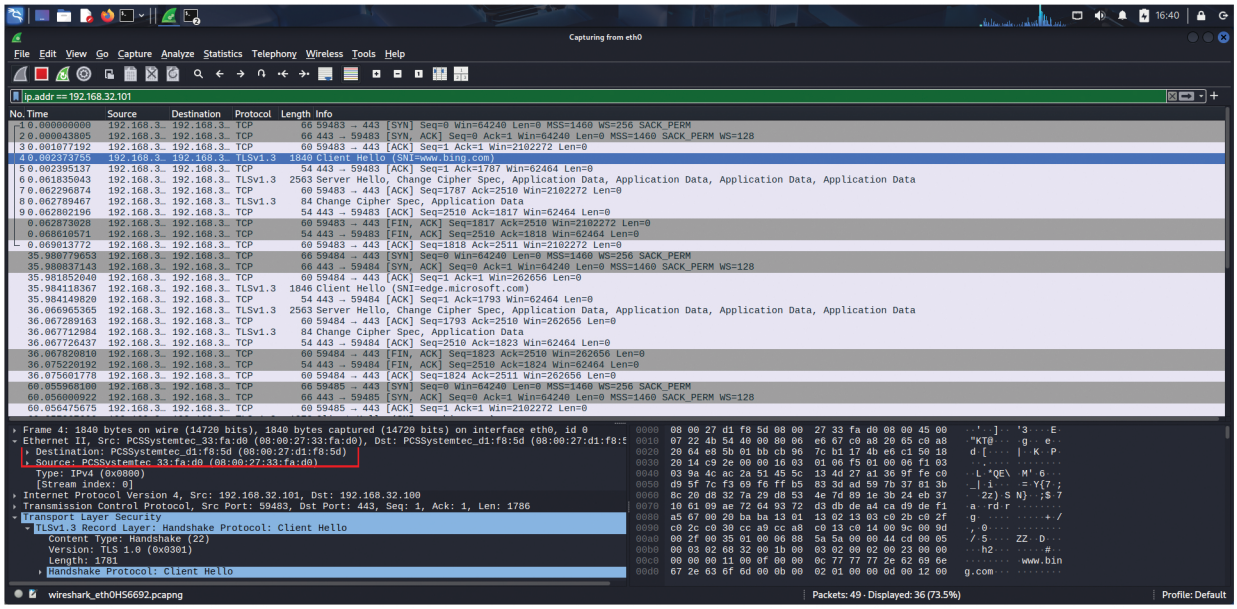
Emy Mangogna - W4D4 - Pratica

Simulatazione di un’architettura client-server in ambiente di laboratorio virtuale, con un client Windows **(192.168.32.101)** e un server Kali **(192.168.32.100)** che esegue iNetSim per emulare servizi di rete (DNS, HTTP, HTTPS).

```
┌──(kali㉿kali)-[~]
└─$ sudo inetsim
INetSim 1.3.2 (2020-05-19) by Matthias Eckert & Thomas Hungenberg
Using log directory:      /var/log/inetsim/
Using data directory:     /var/lib/inetsim/
Using report directory:   /var/log/inetsim/report/
Using configuration file: /etc/inetsim/inetsim.conf
Parsing configuration file.
Warning: Unknown option 'Service' in configuration file '/etc/inetsim/inetsim.conf' line 368
Configuration file parsed successfully.
=== INetSim main process started (PID 53465) ===
Session ID:     53465
Listening on:   0.0.0.0
Real Date/Time: 2025-07-24 15:42:49
Fake Date/Time: 2025-07-24 15:42:49 (Delta: 0 seconds)
 Forking services...
  * dns_53_tcp_udp - started (PID 53477)
  * http_80_tcp - started (PID 53478)
  * https_443_tcp - started (PID 53479)
 done.
Simulation running.
```

Cattura del traffico generato da una richiesta HTTPS del client Windows verso epicode.internal utilizzando Wireshark.





I MAC address di sorgente e destinazione risultano visibili nella sezione Ethernet II, mentre il contenuto della richiesta è cifrato, come evidenziato dalla presenza di pacchetti TLS (Encrypted Application Data)

Cattura del traffico generato da una richiesta HTTP del client Windows verso epicode.internal. I MAC address sono visibili nella sezione Ethernet II e, a differenza del traffico HTTPS, il contenuto della richiesta (metodo GET, intestazioni Host e User-Agent) risulta leggibile in chiaro, mostrando la mancanza di cifratura.