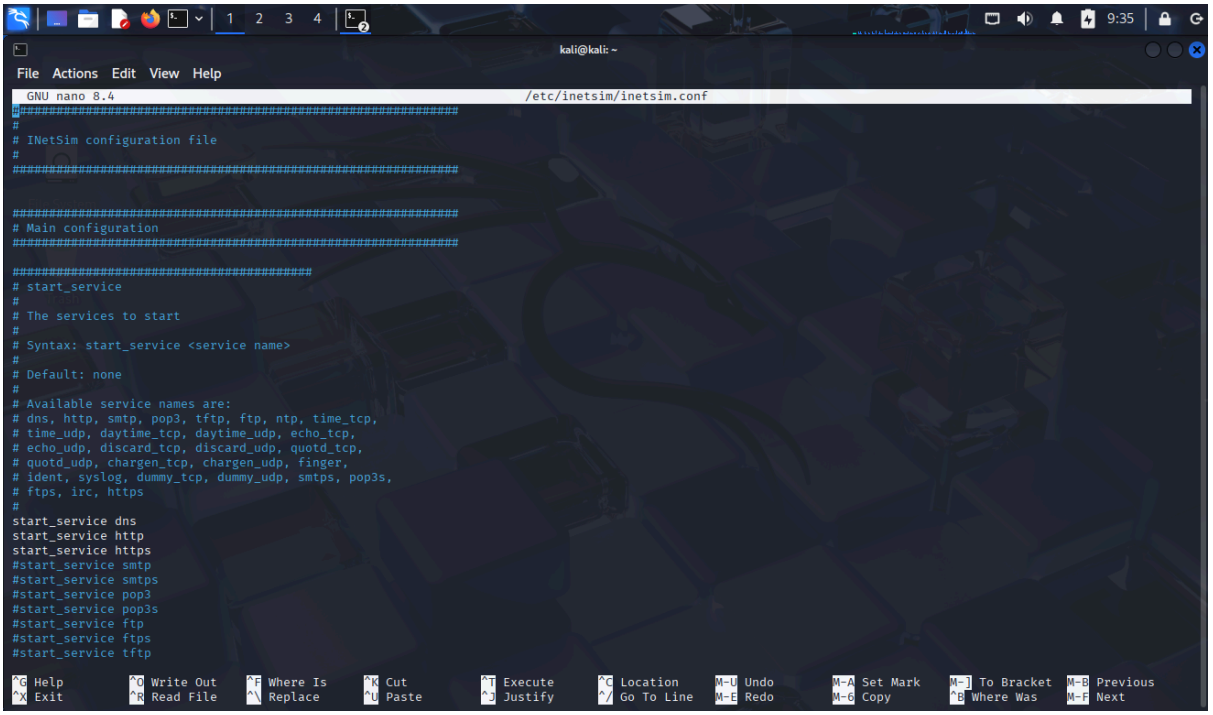
M1 - PROGETTO FINALE

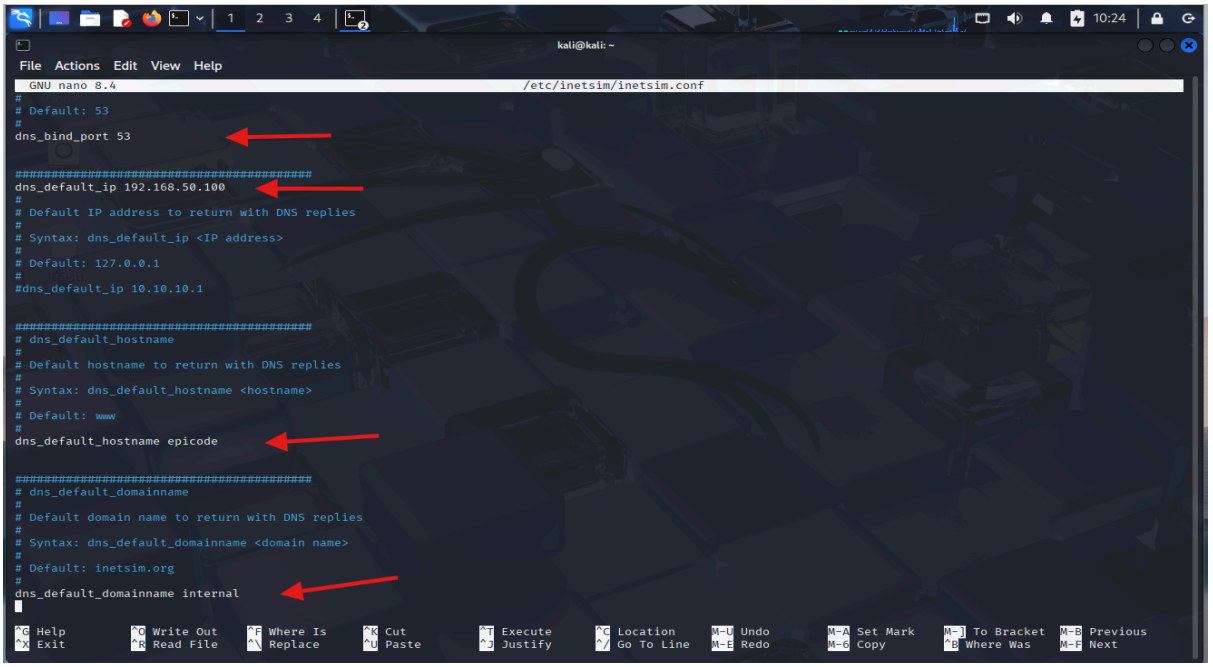
Traccia: Simulare, in ambiente di laboratorio virtuale, un'architettura client server in cui un client con indirizzo 192.168.50.102 (Windows) richiede tramite web browser una risorsa all' hostname epicode.internal che risponde all'indirizzo 192.168.50.100 (Kali).
Si intercetti poi la comunicazione con Wireshark, evidenziando i MAC address di sorgente e destinazione ed il contenuto della richiesta HTTPS.
Ripetere l'esercizio, sostituendo il server HTTPS, con un server HTTP. Si intercetti nuovamente il traffico, evidenziando le eventuali differenze tra il traffico appena catturato in HTTP ed il traffico precedente in HTTPS.
Spiegare, motivandole, le principali differenze se presenti.

Svolgimento: Per simulare un ambiente virtuale client server, è necessario predisporre due macchine virtuali, la prima con il ruolo di server e la seconda con il ruolo di client.
Sulla macchina server, ho utilizzato il tool INetSim per emulare diversi servizi di rete. In particolare, ho attivato i servizi DNS, HTTP e HTTPS modificando il file di configurazione rimuovendo il carattere di commento "**#**" dalle relative voci.

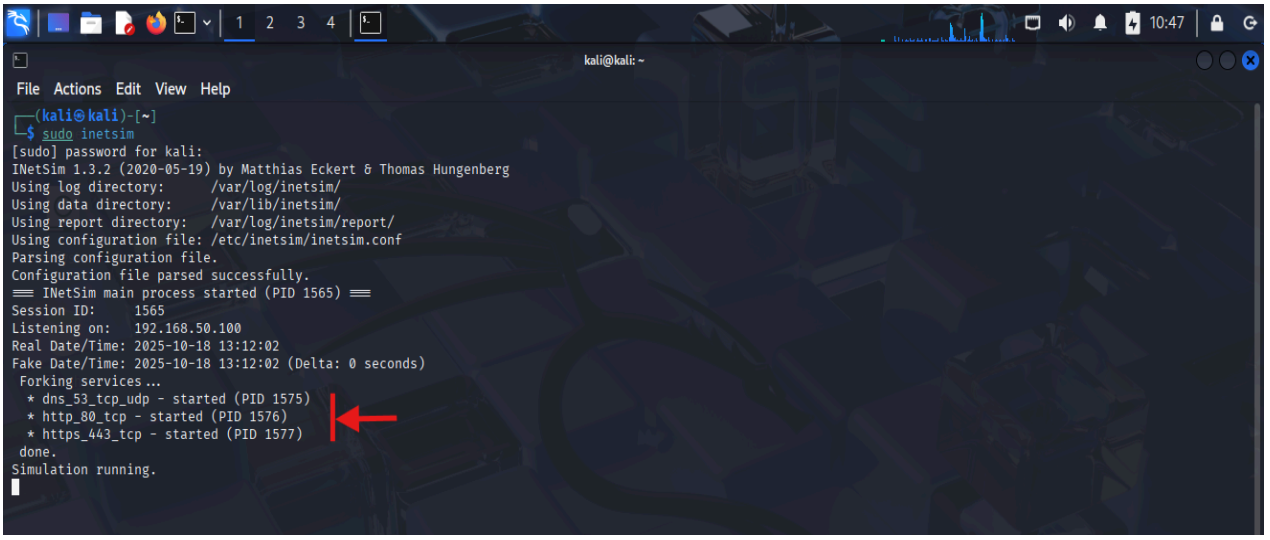


Successivamente, scendendo nel file di configurazione fino alla sezione dei servizi DNS, ho:

- attivato la porta del DNS, ovvero la n. 53
- impostato l'indirizzo IP del DNS 192.168.50.100, ovvero l'indirizzo IP della macchina Kali
- impostato l'hostname "epicode" e il dominio "internal"

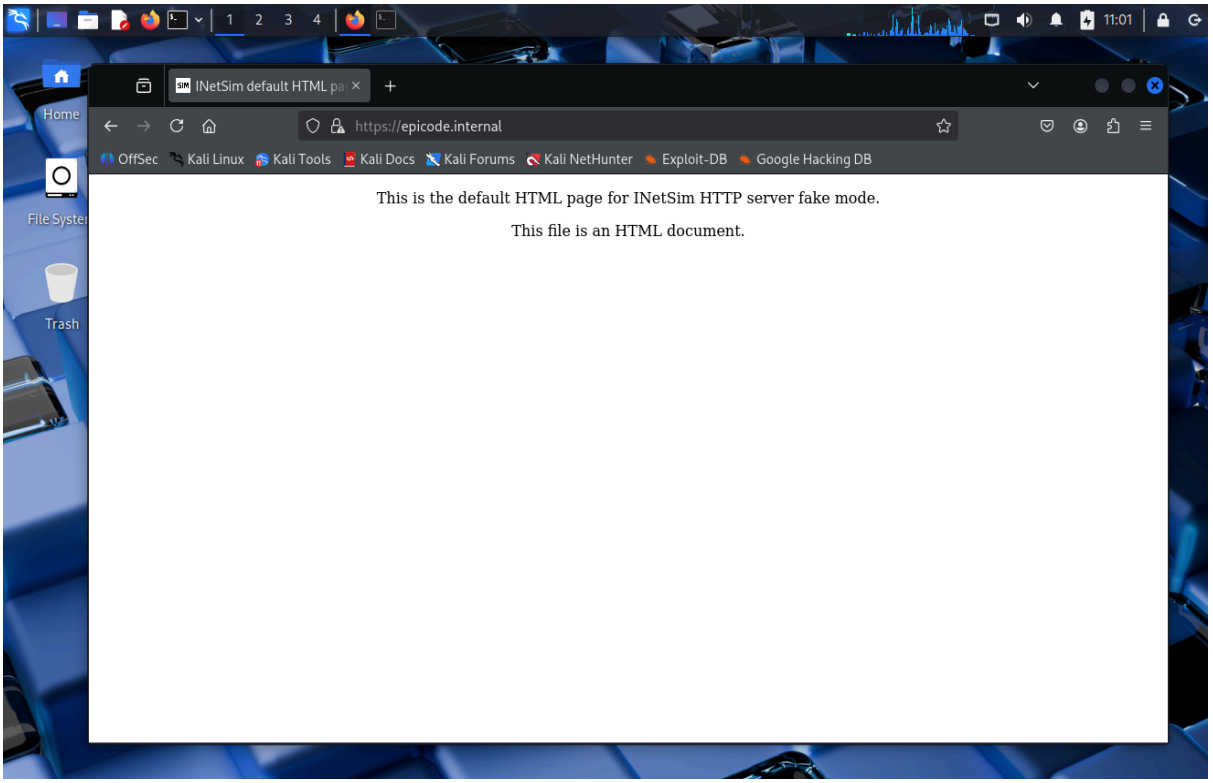


Per verificare il corretto funzionamento del server e dei relativi servizi, ho avviato il tool INetSim dal terminale di kali con il comando "sudo inetsim".

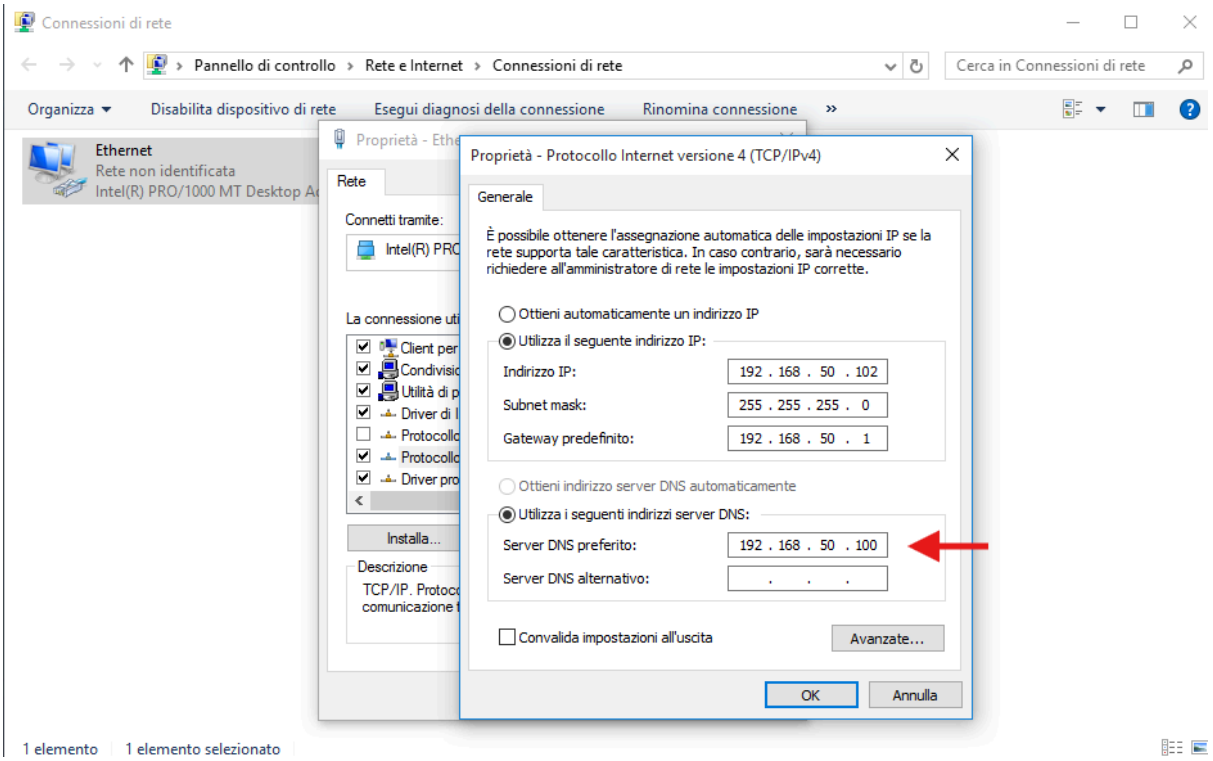


Come si puo' osservare dalla foto, i servizi DNS, HTTP e HTTPS risultano essere attivi.

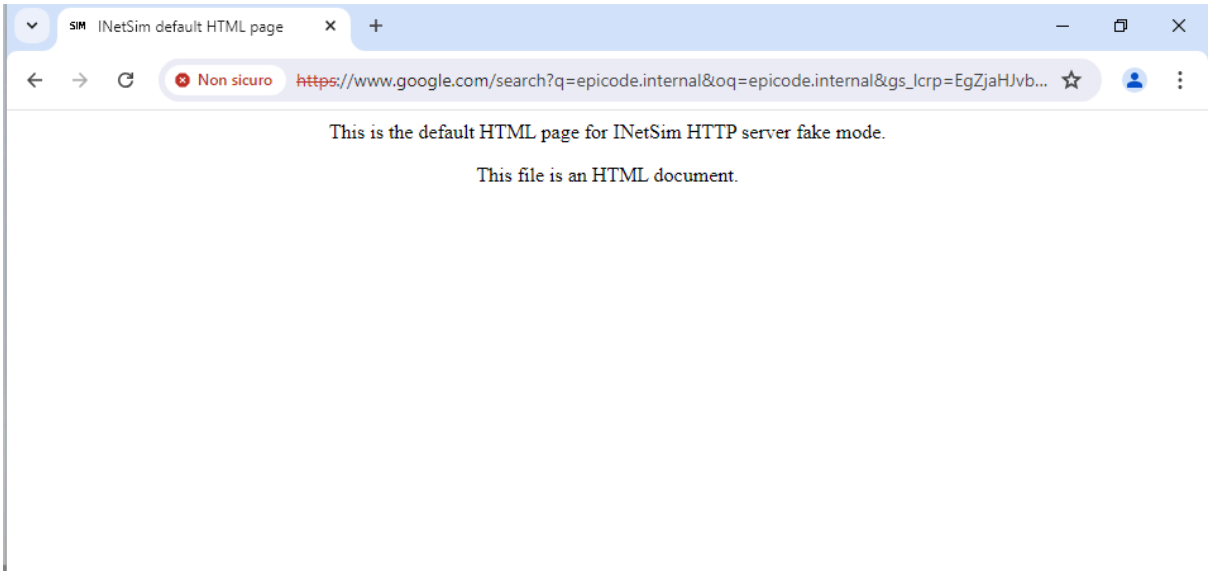
In un primo momento, dopo aver configurato i servizi su INetSim, non era possibile accedere all'indirizzo epicode.internal tramite browser. Dopo diverse ricerche è emerso che il problema era legato alla versione del servizio DNS e per questo motivo ho dovuto effettuare un downgrade alla versione 1.37.
Così facendo, ho successivamente aperto il browser sulla macchina server e inserito nella barra degli indirizzi "https://epicode.internal". Il browser ha correttamente risposto, collegandosi al sito, confermando così che le impostazioni e i relativi parametri di configurazione sono stati applicati correttamente.



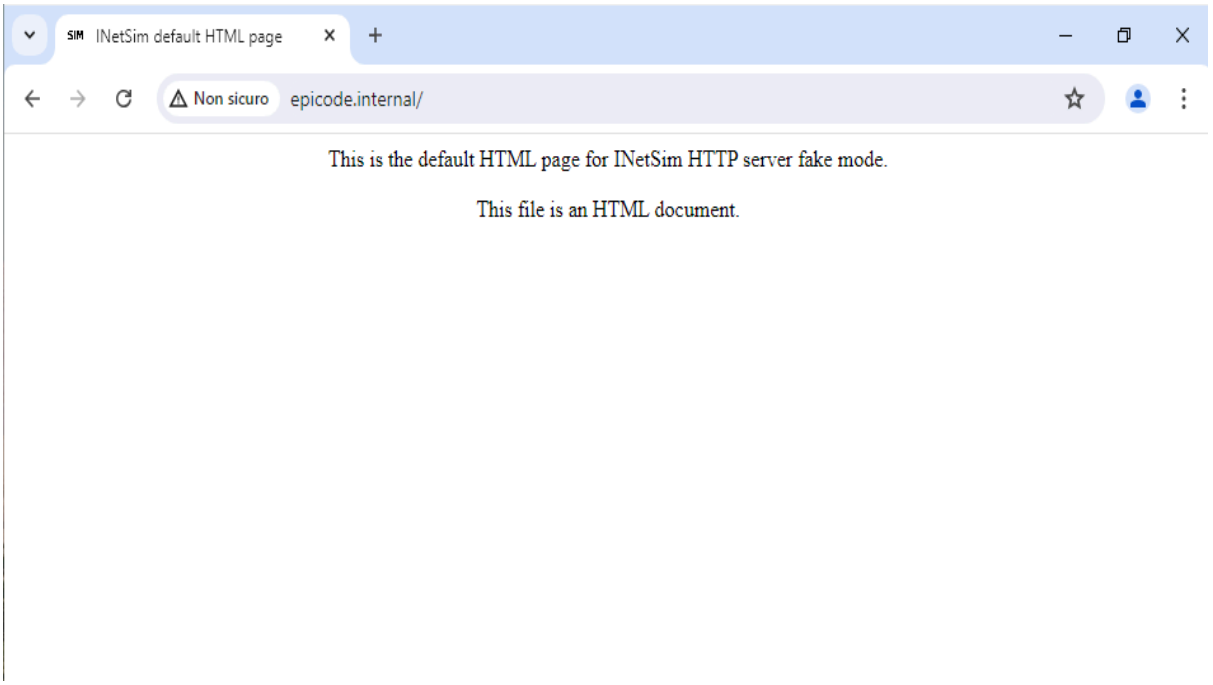
Successivamente, mi sono spostato sulla macchina client (Windows) e per prima cosa, nelle impostazioni della scheda di rete, più precisamente nelle proprietà del “Protocollo Internet versione 4 (TCP/IPv4)”, ho inserito l’indirizzo DNS 192.168.50.100 (server Kali).



Così facendo, inserendo nella barra di ricerca del browser https://epicode.internal e http://epicode.internal , la macchina client invierà la richiesta collegandosi all’ hostname che risponde all’ indirizzo 192.168.50.100.

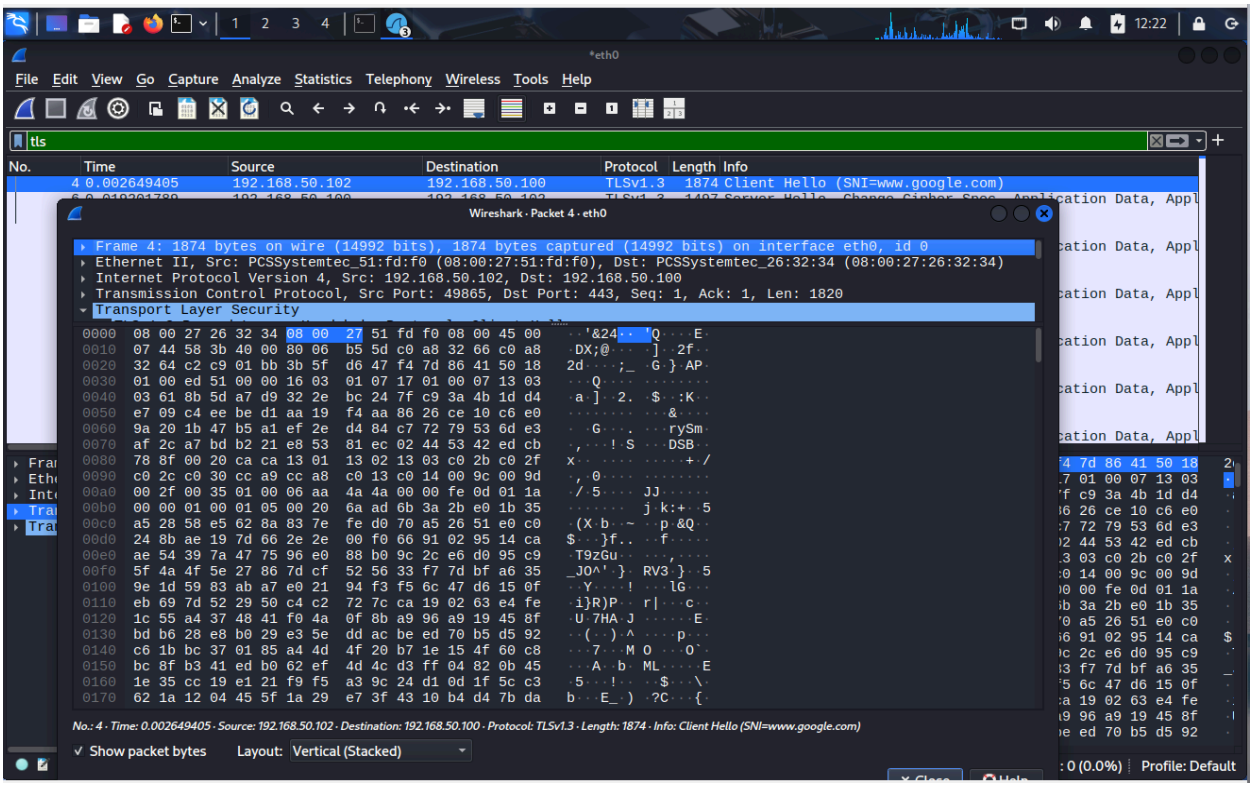


https

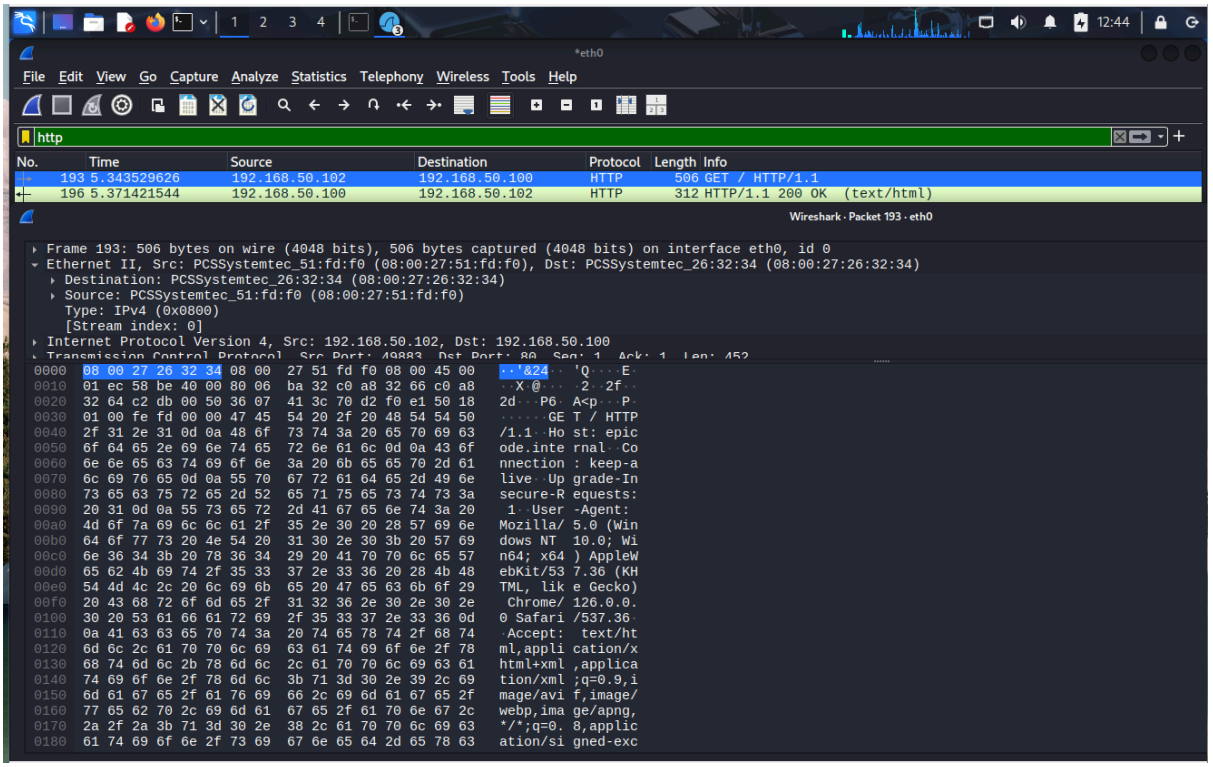


http

Infine, tornando sulla macchina server Kali, attraverso il tool Wireshark, ho intercettato e analizzato il traffico di rete sia in HTTP che in HTTPS andando a filtrare i pacchetti evidenziando solamente quelli che utilizzano i suddetti protocolli.
Nelle foto che seguono possiamo osservare le caratteristiche di un pacchetto HTTPS e di uno HTTP.
Possiamo evidenziare il source MAC address, quello del client Windows (08:00:27:51:FD:F0) e il destination MAC address, quello del server Kali (08:00:27:26:32:34), i quali rimangono invariati in entrambi i casi.
La differenza sostanziale tra questi due tipi di comunicazione sta nel contenuto della richiesta, il quale, possiamo vedere “cifrato” all’interno del pacchetto HTTPS.
Quando parliamo di pacchetti HTTPS, ci riferiamo a dati crittografati che vengono trasmessi in modo sicuro, in modo tale da non poter essere letti da chi non è autorizzato, mentre, in HTTP, header e il payload sono in chiaro.
Un'ulteriore caratteristica che possiamo osservare analizzando il traffico di rete riguarda le porte utilizzate: la porta 80 per il protocollo HTTP e la porta 443 per HTTPS.



https



http

Roma, 20/10/2025
Riccardo Ricci