W4D4

TRACCIA:

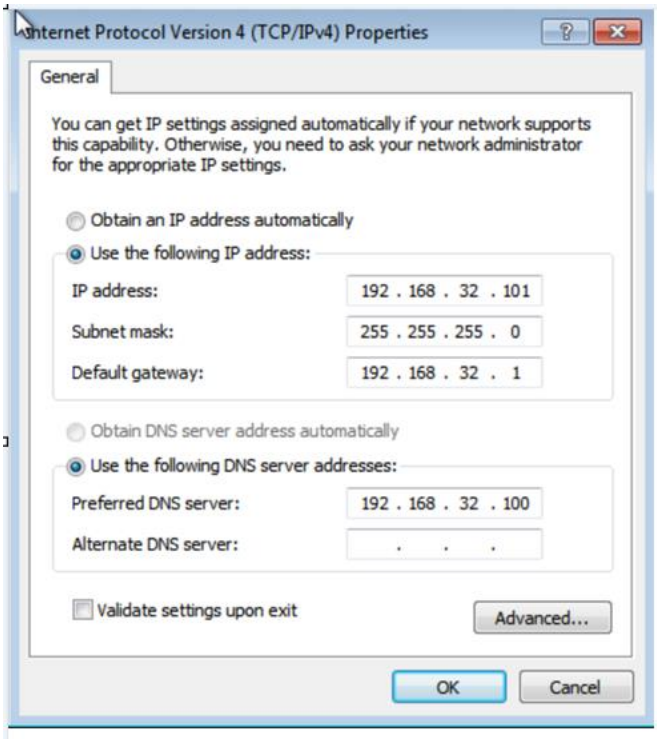
Simulare, in ambiente di laboratorio virtuale, un'architettura client server in cui un client con indirizzo 192.168.32.101 (Windows 7) richiede tramite web browser una risorsa all'hostname epicode.internal che risponde all'indirizzo 192.168.32.100 (Kali).

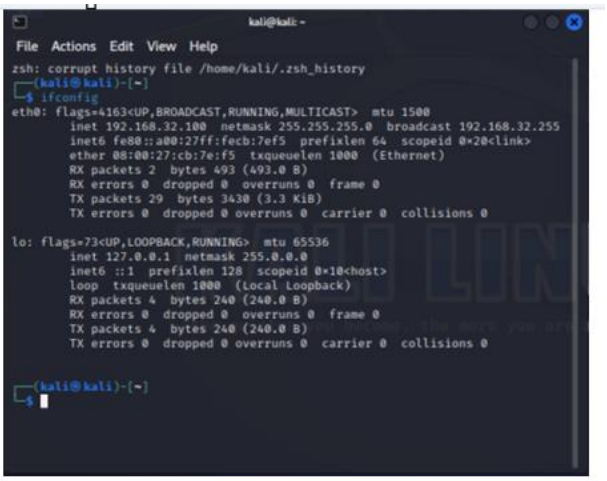
Si intercetti poi la comunicazione con Whireshark, evidenziando i MAC address di sorgente e destinazione ed il contenuto della richiesta HTTPS.

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.

SOLUZIONE:

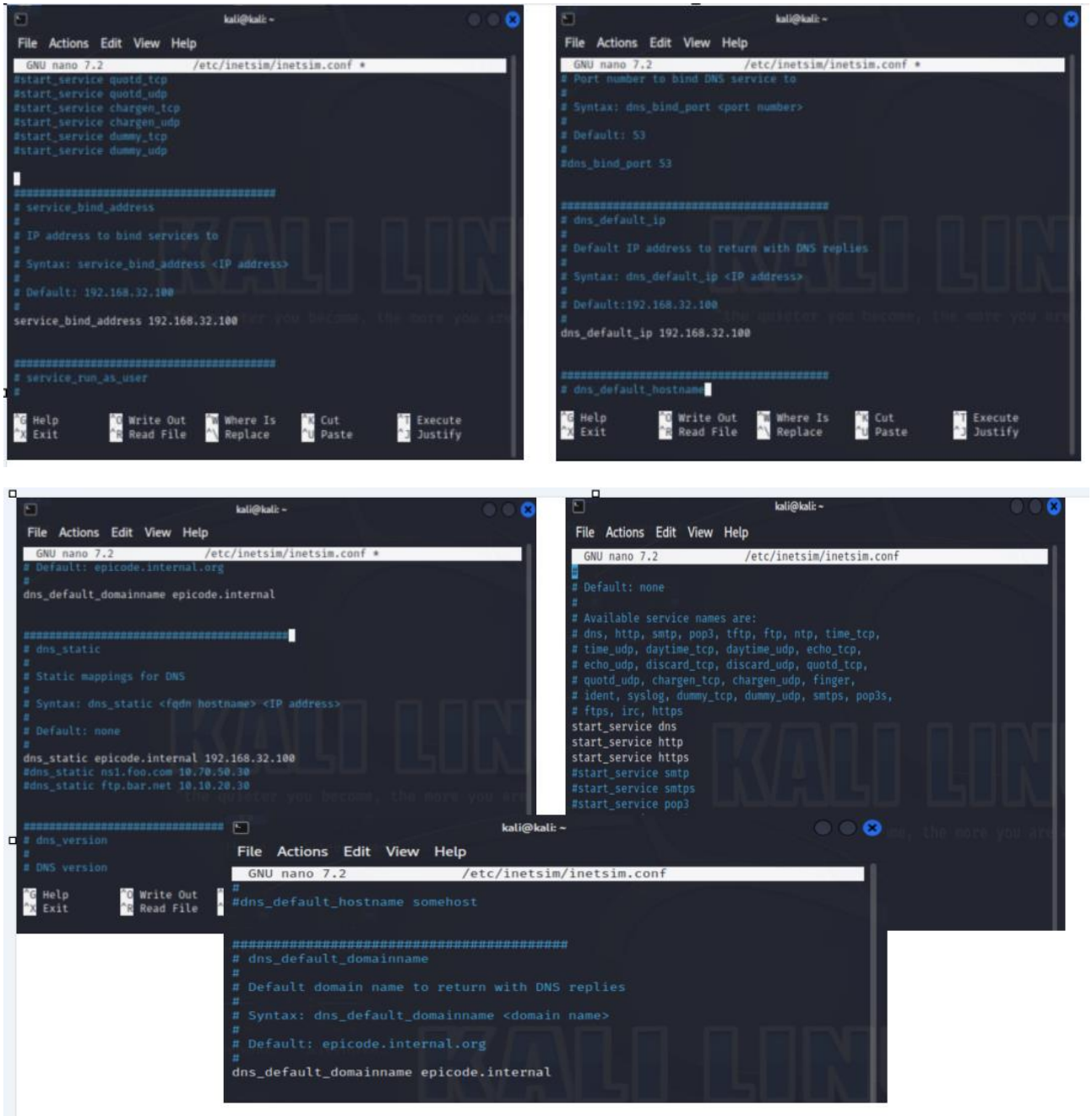
Come primo passaggio andiamo a configurare gli IP statici sulle due macchine come indicato nella traccia.





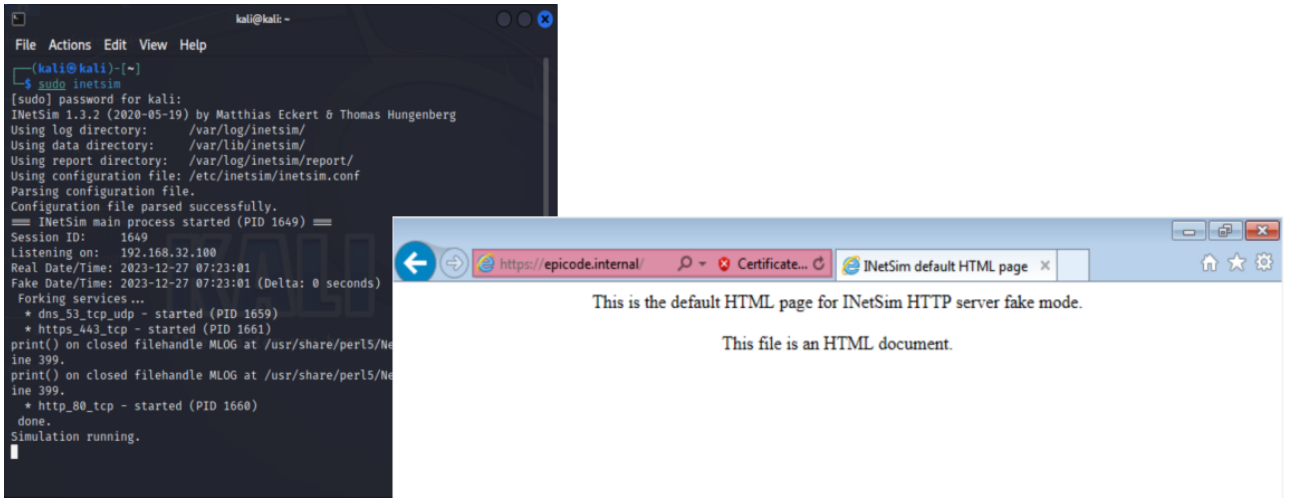
Successivamente passiamo alla configurazione di Inetsim che poi ci permetterà di simulare il traffico fra host e server.

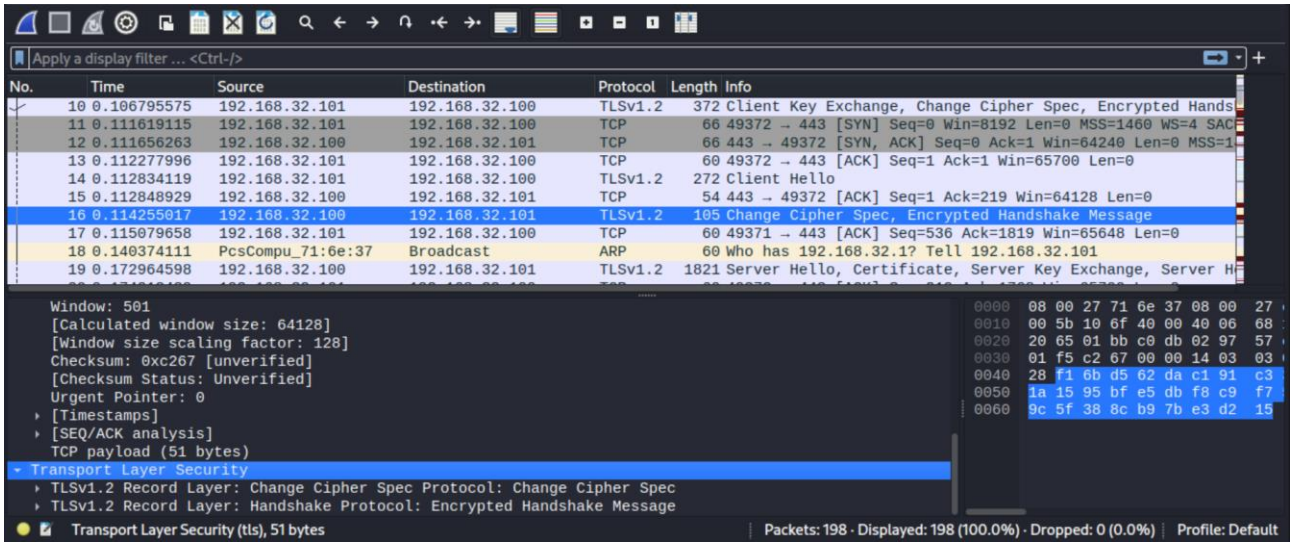
In particolare, andiamo a settare il servizio DNS oltre all'HTTP e all'HTTPS.



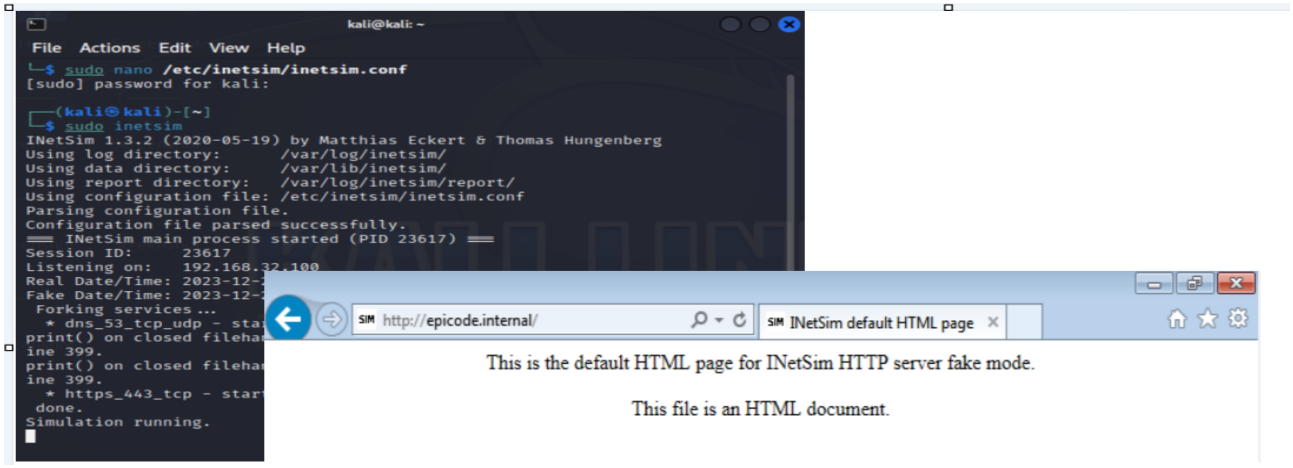
Dopo aver effettuato la configurazione di Inetsim e dei relativi servizi possiamo procedere ad analizzare i pacchetti che vengono scambiati fra host e server utilizzando il tool Whireshark.

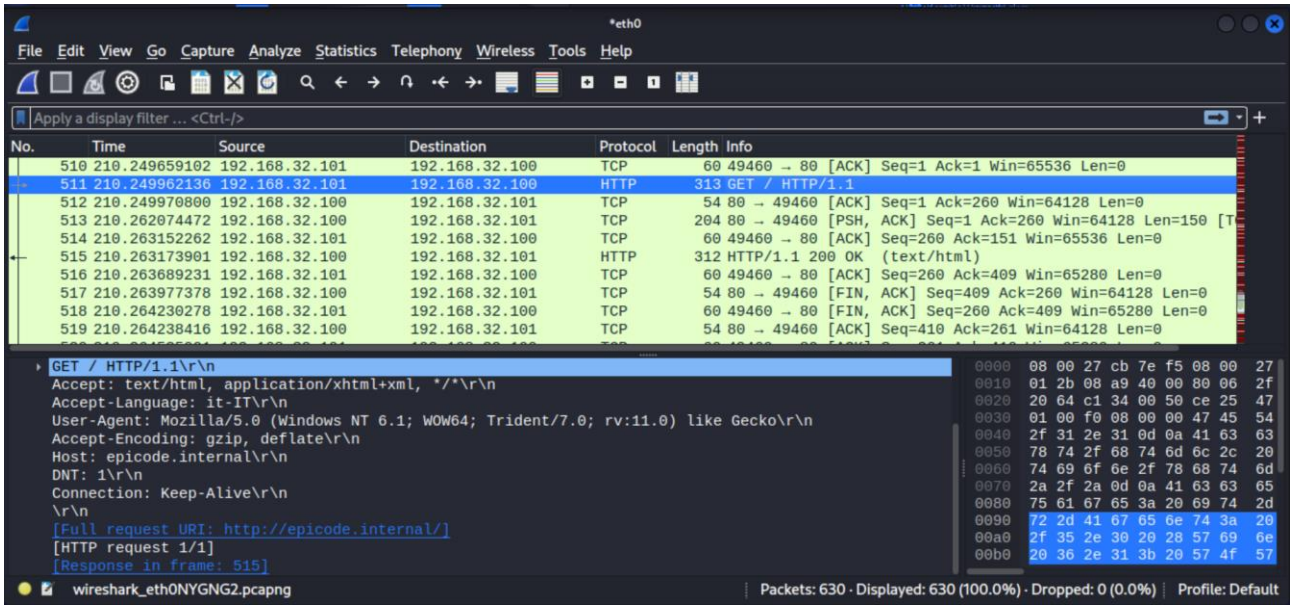
Analisi servizio HTTPS:





ANALISI SERVIZIO HTTP:





CONCLUSIONI:

La differenza sostanziale che si può notare fra l'HTTP e l'HTTPS è che nel primo, non essendo un protocollo sicuro, l'indirizzo richiesto dall'host è visibile mentre nel secondo, essendo un protocollo sicuro, i pacchetti sono crittografati mediante l'utilizzo del protocollo TLSv 1.2.