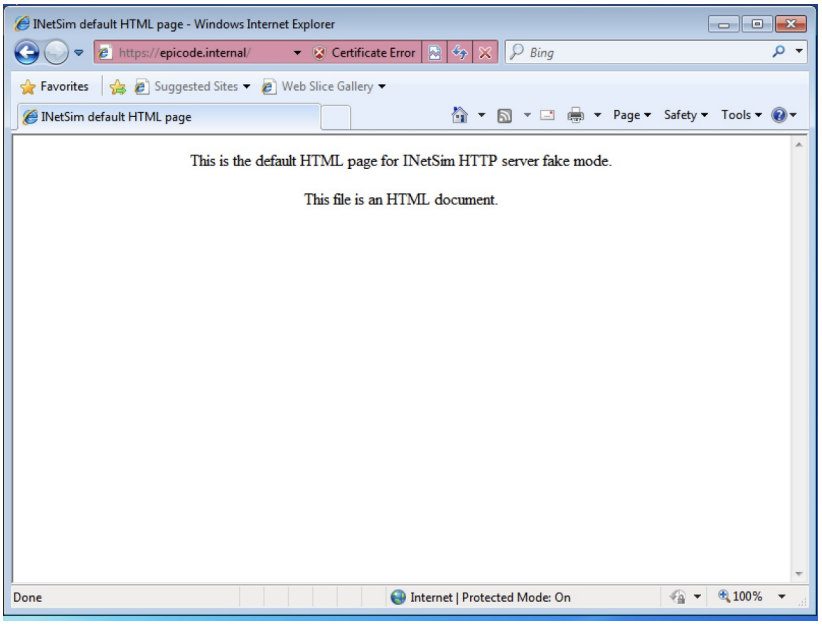
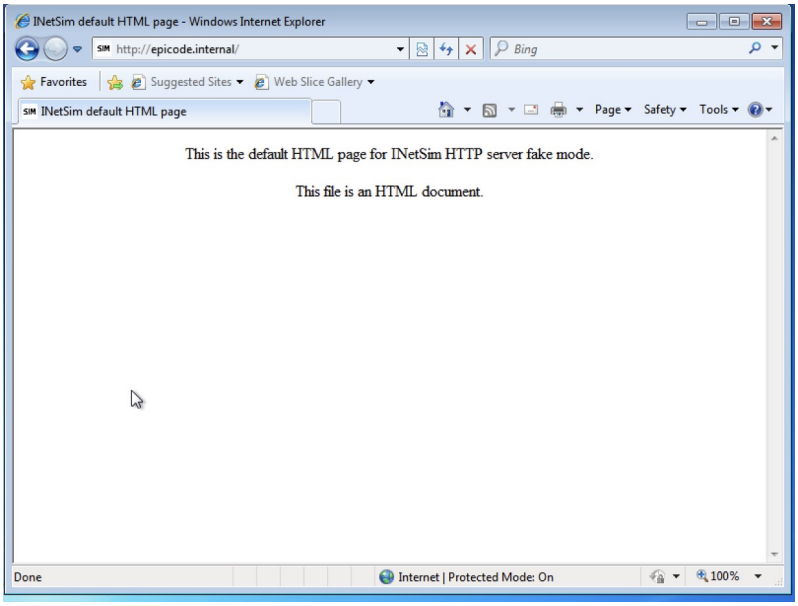
L’esercizio richiede di simulare in ambiente virtuale, un’architettura client server in cui il client 192.168.32.101 (Windows 7) richiede tramite Web Browser una risorsa all’hostname epicode.internal che risponde all’indirizzo di 192.168.32.100 (Kali)

In questo caso, come da screen sottostanti, entrambe le richieste sono avvenute con successo:

-Richiesta HTTPS



-Richiesta HTTP



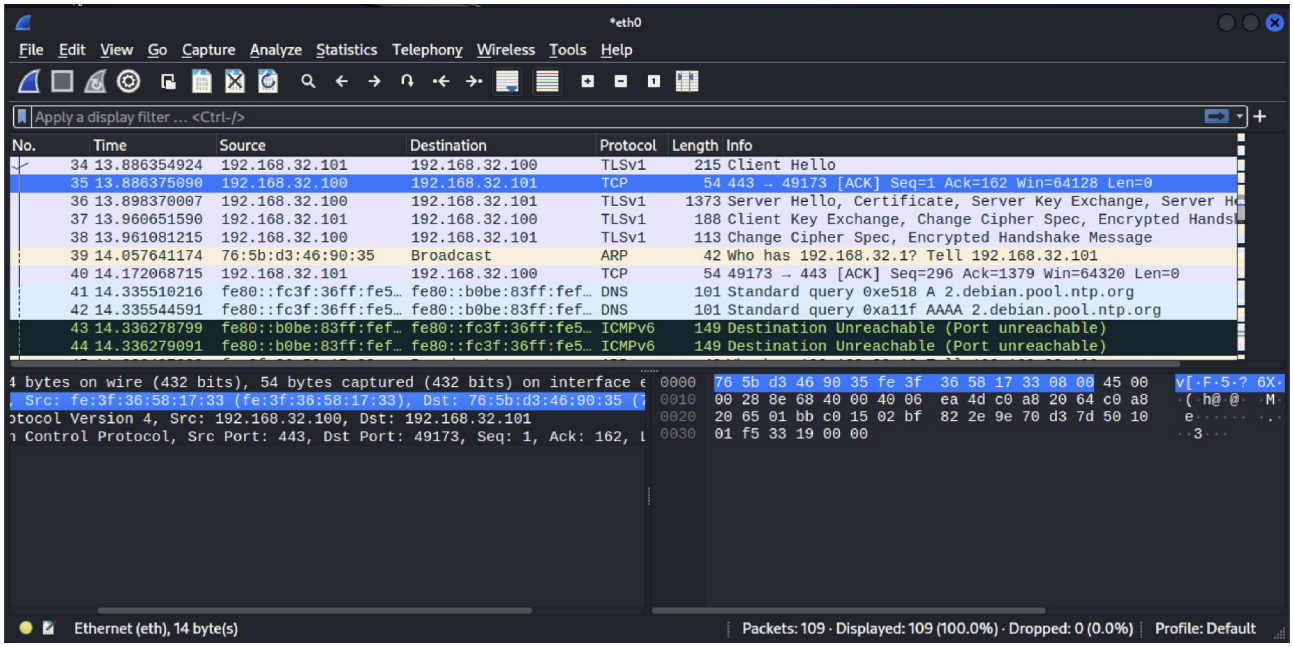
Per fare che cio avvenga ho modificato gli indirizzi IP che la traccia assegnava alle 2 macchine, dopodichè nella macchina W7 ho settato nel campo DNS l’indirizzo IP corrispondente alla macchina Kali per poi procedere su quest’ultima a preparare l’app Inetsim.
Su Inetsim ho attivato le voci service DNS e HTTP la prima volta e poi per ripere l’operazione ho attivato il service HTTPS spegnendo quello HTTP. Scorrendo le voci piu in basso ho impostato service_bind_address su 0.0.0.0 e scendendo ancora nella sezione DNS ho attivato e modificato la

voce in dns_static epicode.internal 192.168.32.100 di modo tale che la macchina Windows 7 e Kali possano risolvere la richiesta di W7 di richiamare la pagina web.

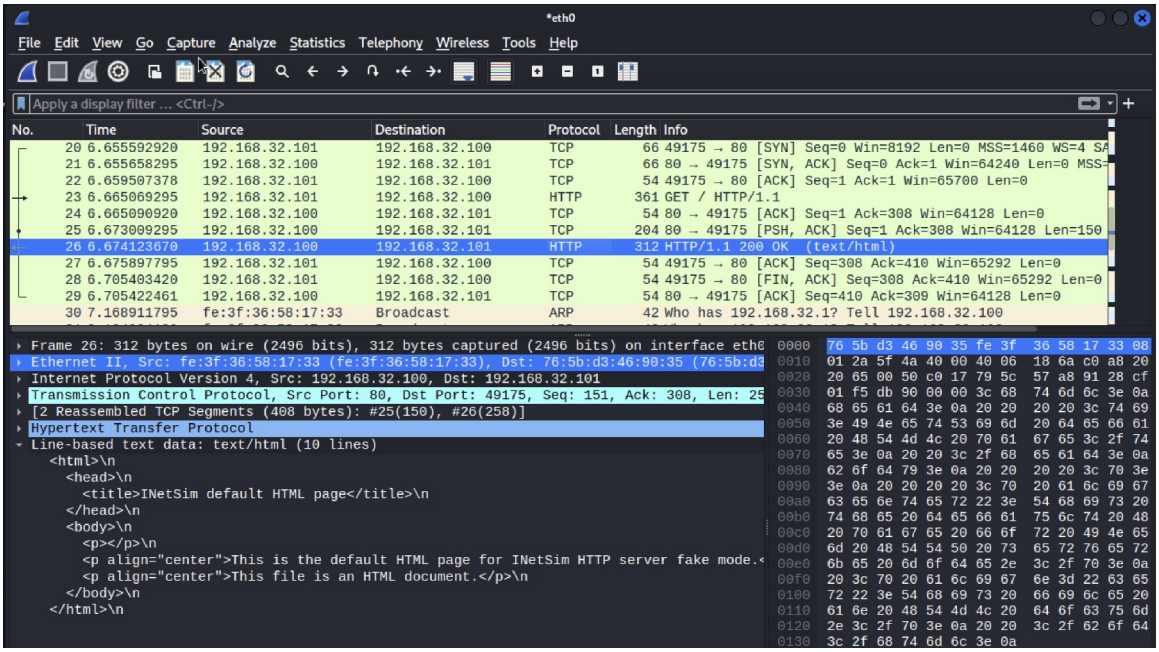
La seconda parte dell'esercizio prevedeva l'intercettazione della comunicazione tra le 2 macchine con wireshark evidenziando gli indirizzi mac di sorgente e destinazione ed il contenuto ddella richiesta HTTPS e successivamente HTTP, evidenziando le differenze se ce ne fossero state.

Dagli screen HTTPS e HTTP qua sotto della cattura del traffico:

HTTPS:



HTTP:



Si evince principalmente il fatto che nella connessione HTTP il contenuto delle informazioni non è cifrato e ben leggibile, al contrario della connessione HTTPS che cifra i contenuti della pagina rendendoli impossibili da interpretare.