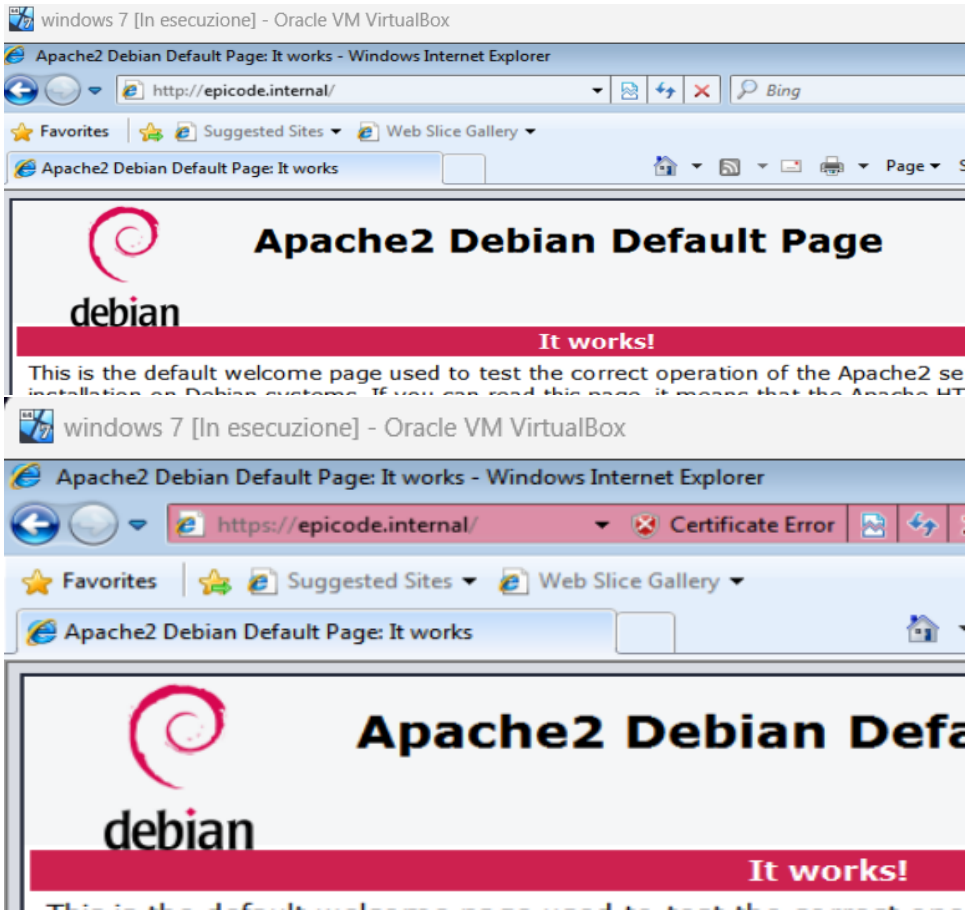
Traccia: Simulare, in ambiente di laboratorio virtuale, un'architettura client server in cui un client con indirizzo 192.168.32.101 (Windows 7) richiede tramite web browser una risorsa all'hostname epicode.internal che risponde all'indirizzo 192.168.32.100 (Kali).

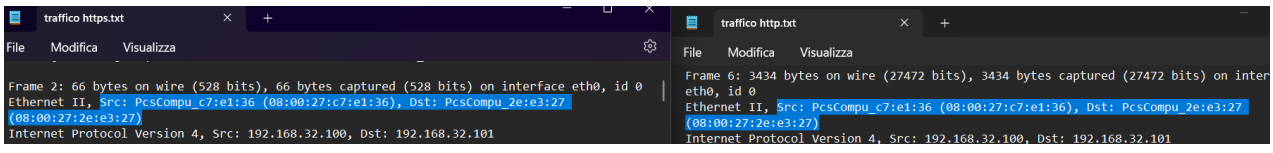
Risoluzione: impostazione di IP statico sia in Windows7 che in Kali. Modifica del file "host" in W7 in modo che riconosca "epicode.internal" come 192.168.32.100.

Simulazione di server tramite Apache2 su Kali.

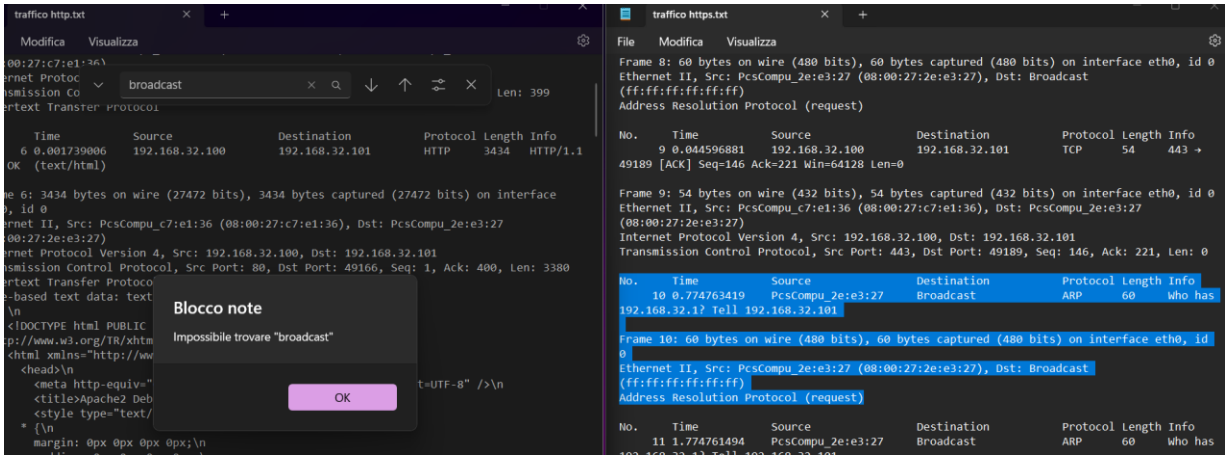
Creazione di certificato di crittografia (finto, motivo per cui da errore) e modifica Apache2 per la gestione di HTTP e HTTPS.



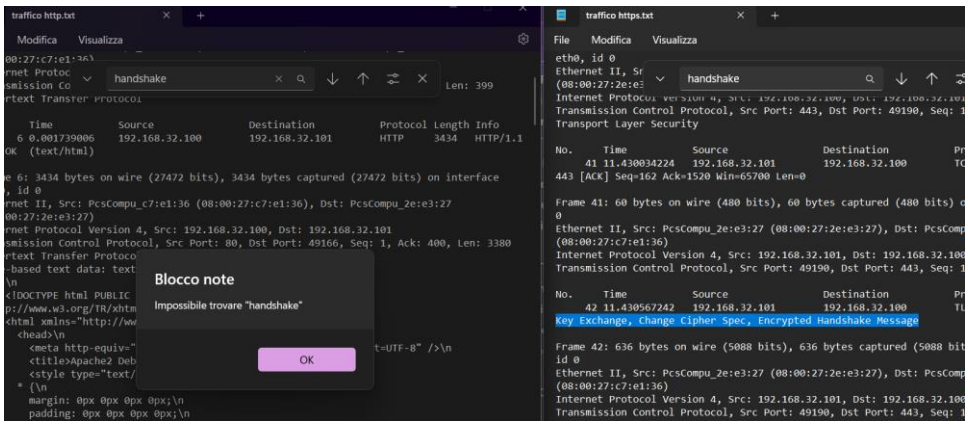
Si intercetti poi la comunicazione con Wireshark, evidenziando i MAC address di sorgente e destinazione ed il contenuto della richiesta HTTPS.



Il contenuto della richiesta HTTPS è crittografato.



Scambio di certificati



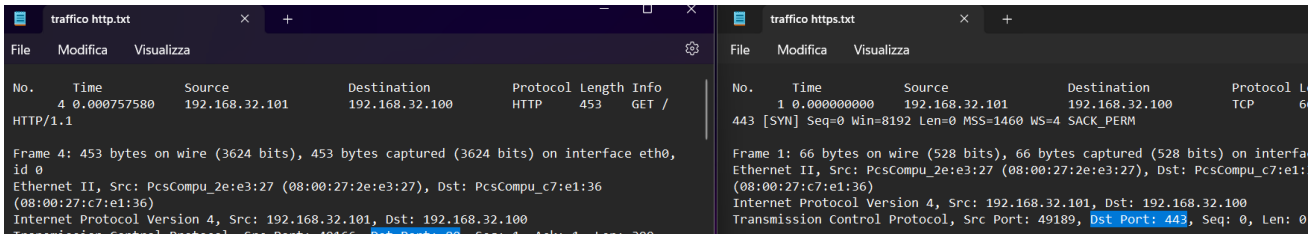
Ripetere l'esercizio, sostituendo il server HTTPS, con un server HTTP. Si intercetti nuovamente il traffico,evidenziando le eventuali differenze tra il traffico appena catturato in HTTP ed il traffico precedente in HTTPS. Spiegare, motivandole, le principali differenze se presenti.

Contenuto HTTP in chiaro rispetto a contenuto crittografato HTTPS

Il traffico HTTP ,il traffico HTTPS utilizza una crittografia SSL/TLS per proteggere i dati durante la trasmissione. Questo significa che il contenuto del traffico HTTPS sarà crittografato e non leggibile.

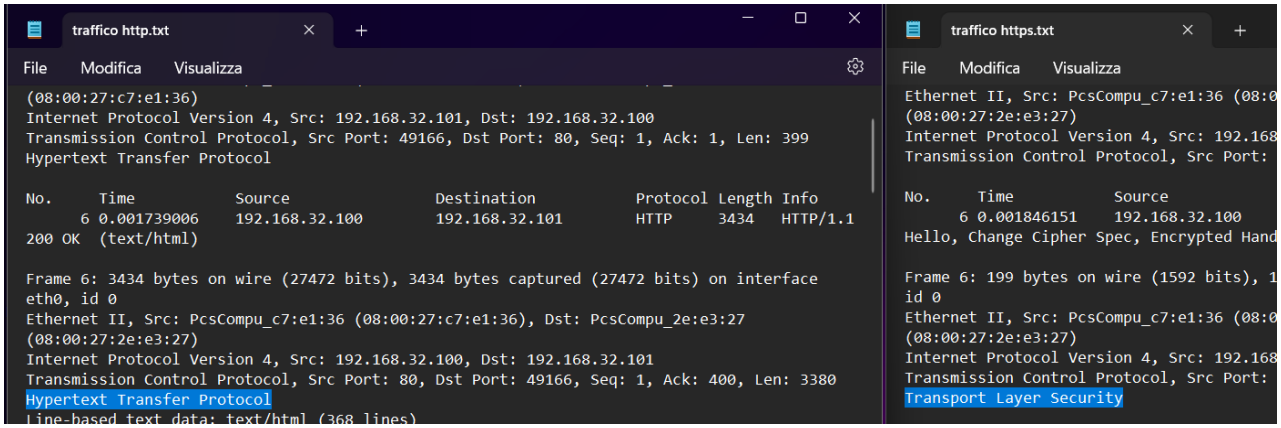
Porte differenti

Il traffico HTTP di solito utilizza la porta 80 come porta di destinazione predefinita, mentre il traffico HTTPS utilizza la porta 443



Livelli di crittografia in HTTPS

i pacchetti HTTP sono composti principalmente da intestazioni e dati del corpo del messaggio, mentre i pacchetti HTTPS avranno un livello aggiuntivo di crittografia.



Metodi di richiesta differenti (es.GET in chiaro)