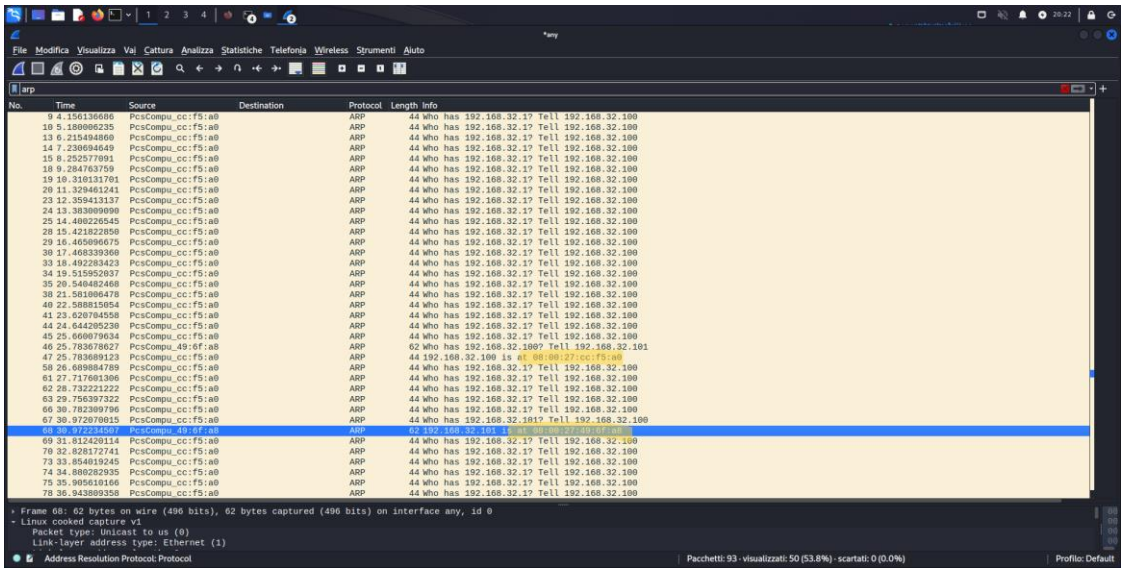
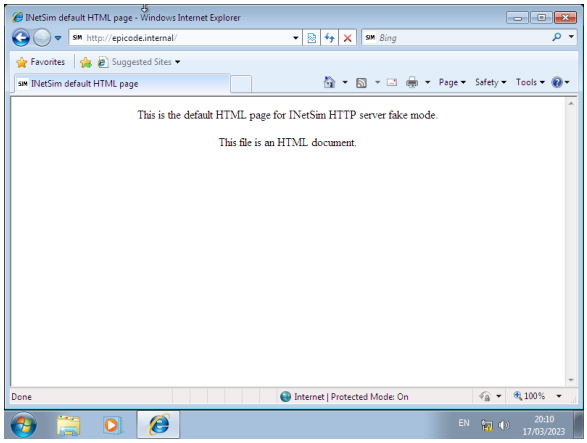
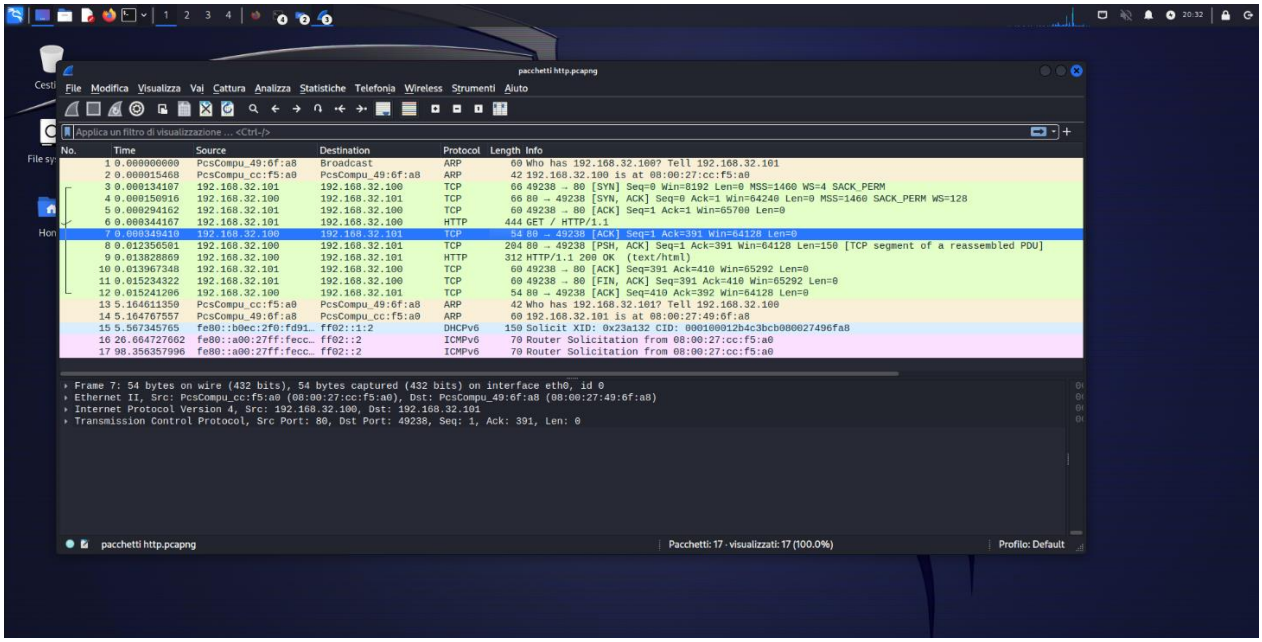
Progetto 17.03 – cattura pacchetti wireshark e differenza fra http e https



Nella schermata superiore è possibile leggerei due mac address delle macchine win7 (riga 68) e kali (riga 47)

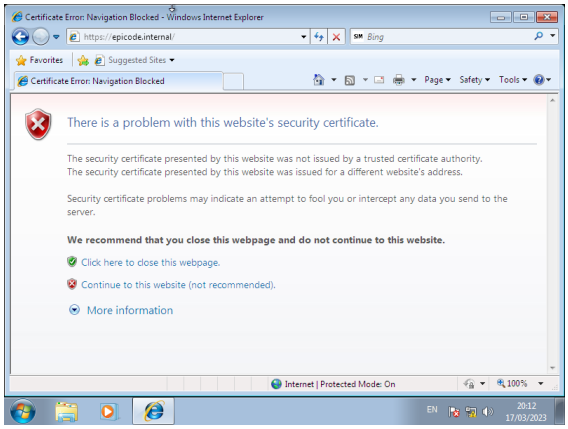


Qui si osserva la risoluzione dell'hostname epicode.internal in http

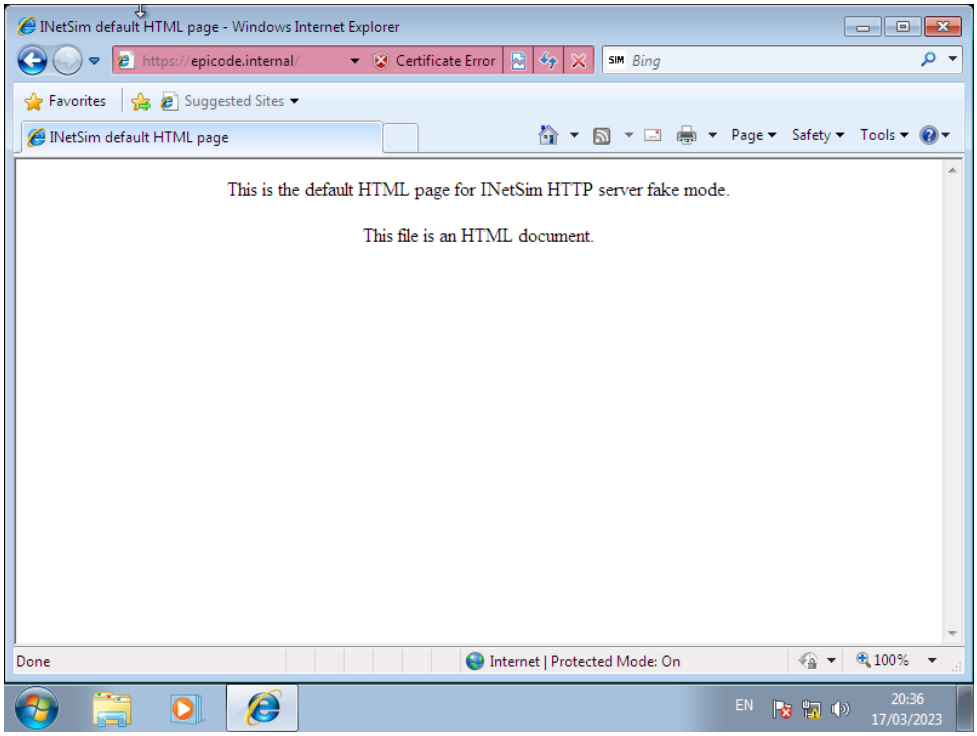


Questi sono i pacchetti catturati da wireshark durante la richiesta in http

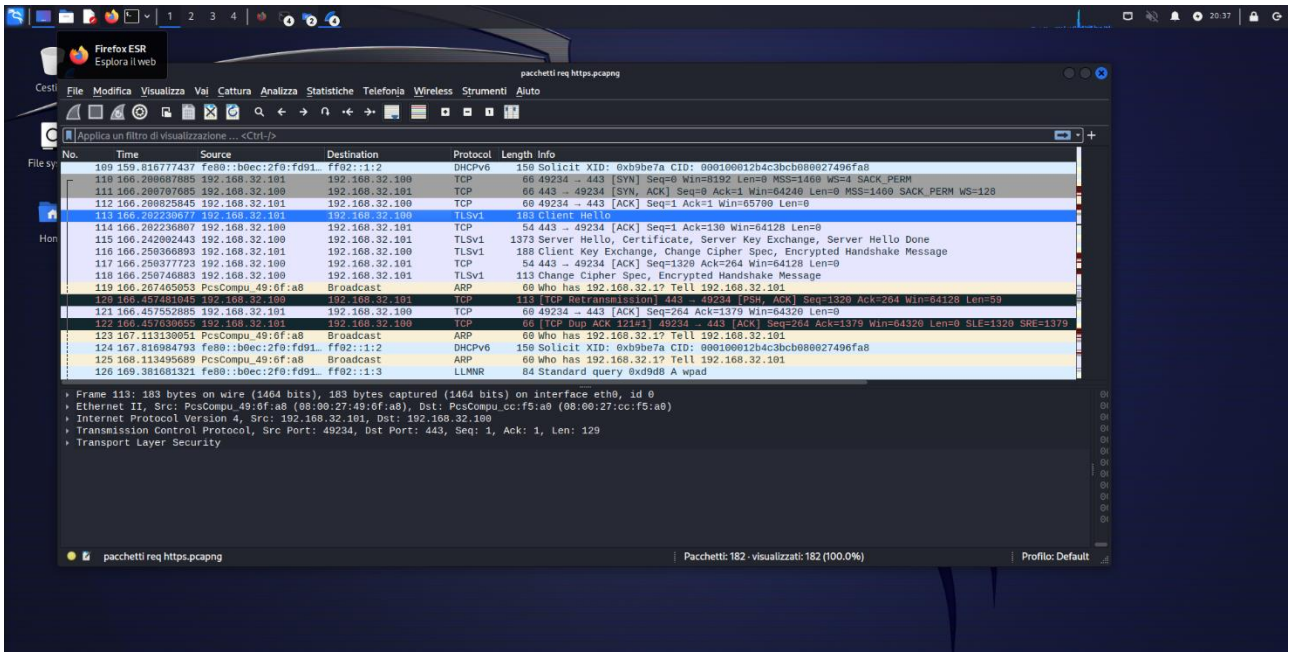
anche qui sono osservabili source (src) e destination address (dst) sulla riga “Ethernet II”



In questo step è osservabile la richiesta del certificato https e dopo aver acconsentito all’autenticazione viene risolto come nella schermata a seguire



Risoluzione https.



Qui sopra sono evidenziati i pacchetti catturati durante la richiesta https.

La differenza fondamentale fra i due sniffing è la presenza del protocollo TLSv1, tramite il quale viene eseguito lo scambio delle chiavi di cifratura fra server e client.

Per completezza nella directory Github sono accessibili anche i file prodotti tramite wireshark.