Relazione – Analisi del traffico HTTP e HTTPS con Wireshark

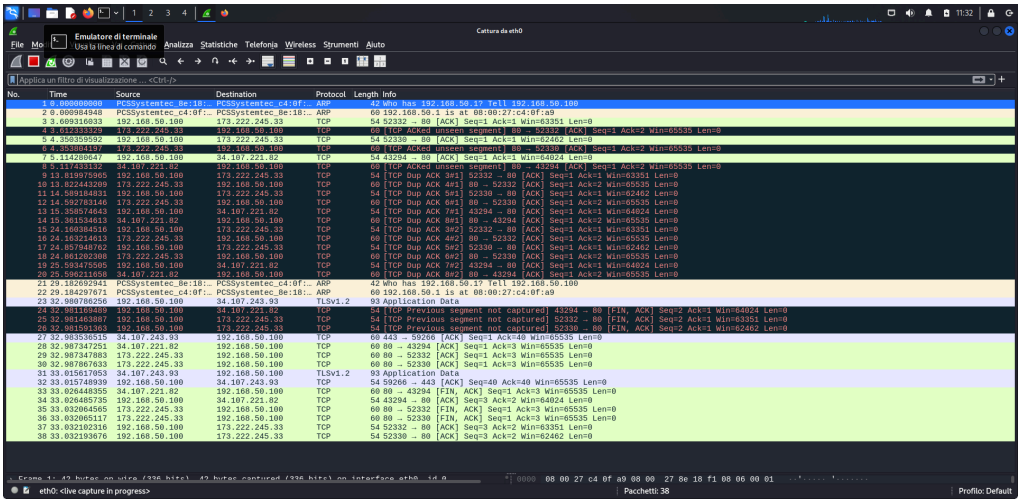
Per questo esercizio ho utilizzato Wireshark, uno strumento molto utile per l'analisi del traffico di rete. L'obiettivo era catturare e visualizzare pacchetti HTTP e HTTPS (TLS).

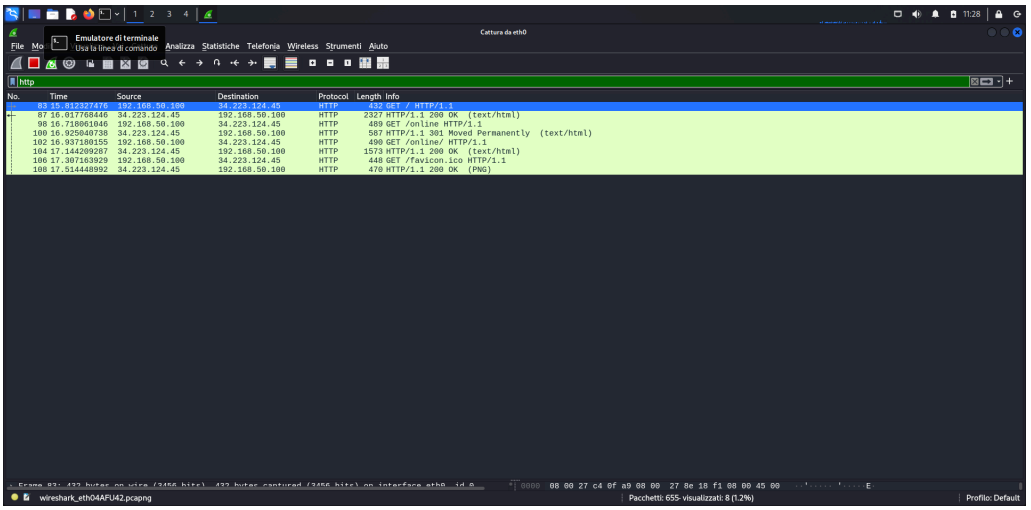
Dopo aver aperto Wireshark, ho selezionato l'interfaccia di rete `eth0` per iniziare a catturare il traffico. Ho fatto delle semplici navigazioni in rete (sia su siti HTTP che HTTPS) per generare traffico da analizzare.

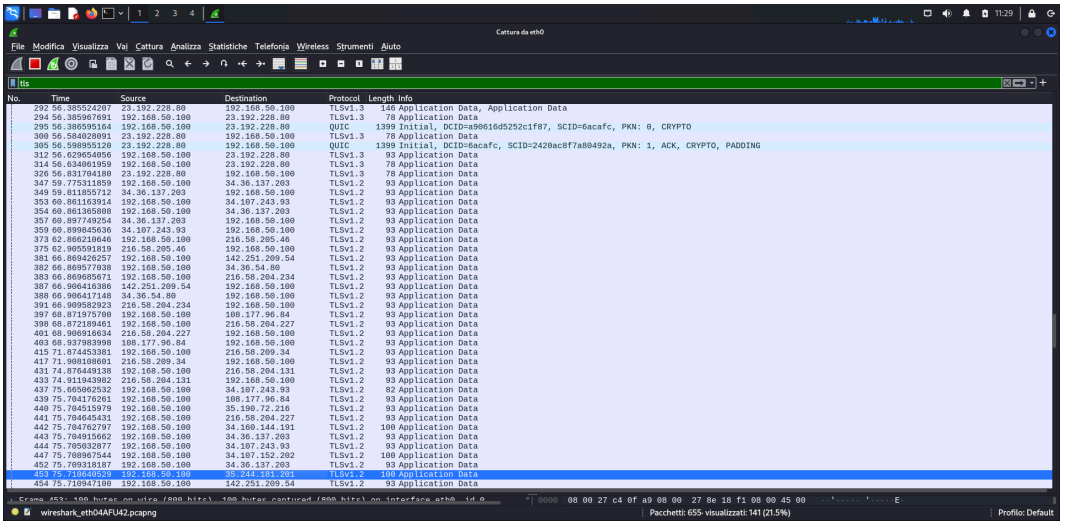
Nel campo dei filtri ho scritto `http`, e Wireshark ha mostrato chiaramente i pacchetti non cifrati. Si poteva leggere direttamente il contenuto, come ad esempio richieste GET e risposte 200 OK. Questo mostra come il traffico HTTP non sia sicuro, perché chiunque potrebbe leggerne i dati se intercettati.

Ho poi cambiato il filtro in `tls` per visualizzare il traffico cifrato HTTPS. In questo caso il contenuto delle richieste non è visibile, perché cifrato. Si riesce a vedere che esiste una comunicazione, ma non cosa viene inviato o ricevuto.

Screenshot







Conclusione

Ho dimostrato la differenza tra HTTP e HTTPS. I pacchetti HTTP sono facilmente leggibili, mentre quelli HTTPS sono protetti grazie alla cifratura TLS. Questo evidenzia l'importanza di utilizzare sempre connessioni sicure per proteggere i dati, soprattutto quando si trasmettono informazioni sensibili.

.