Esame Modulo 1

Kali: 192.168.32.110/24
Windows 7: 192.168.32.101/24

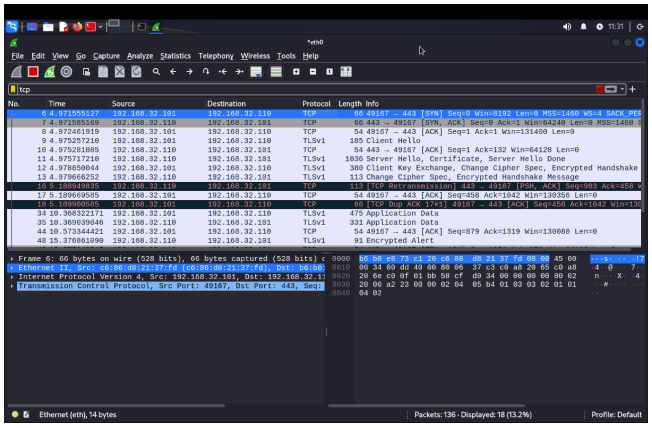
Una volta configurate le macchine ho installato “Apache2” su Kali in modo da poter tirare su un server http, il cui indirizzo è lo stesso della macchina e che risponde al dominio “epicode.internal”.

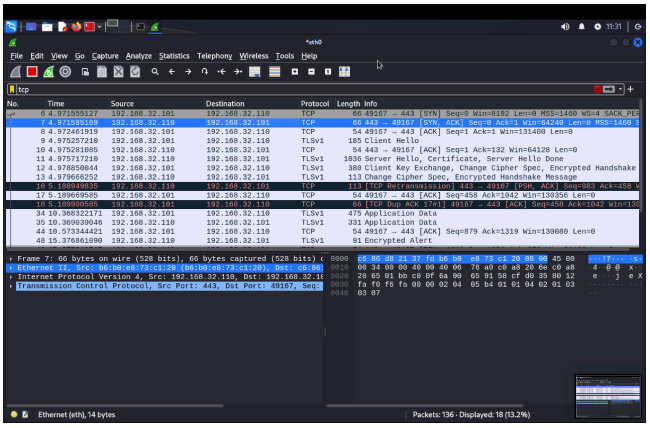
Le principali differenze che troviamo quando analizziamo il traffico di rete tra https e http sono due:

- il protocollo http lavora sulla porta 80 mentre https sulla porta 443

- i pacchetti analizzati mentre operiamo con http non sono crittografati, quindi con un applicativo come Wireshark siamo in grado di vedere le informazioni che si scambiano.

Pacchetti analizzati con http:
(Evidenziati in blu troviamo i MAC di sorgente e destinazione)





I pacchetti https infatti sono crittografati, ciò non permette di analizzare i pacchetti tramite Wireshark e invece del protocollo HTTP viene utilizzato il protocollo TLS (transport layer security) o SSL (Secure Socket Layer).

Pacchetti analizzati con https: