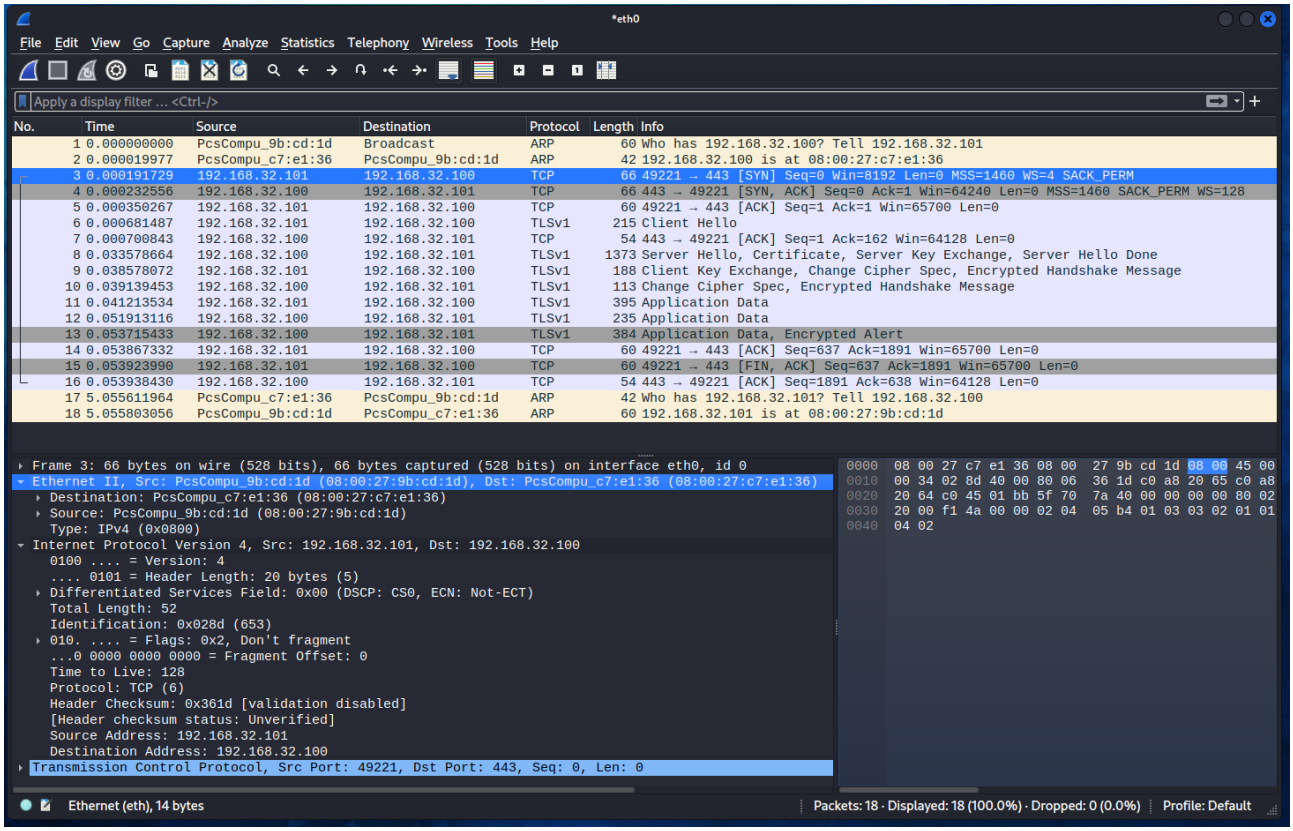
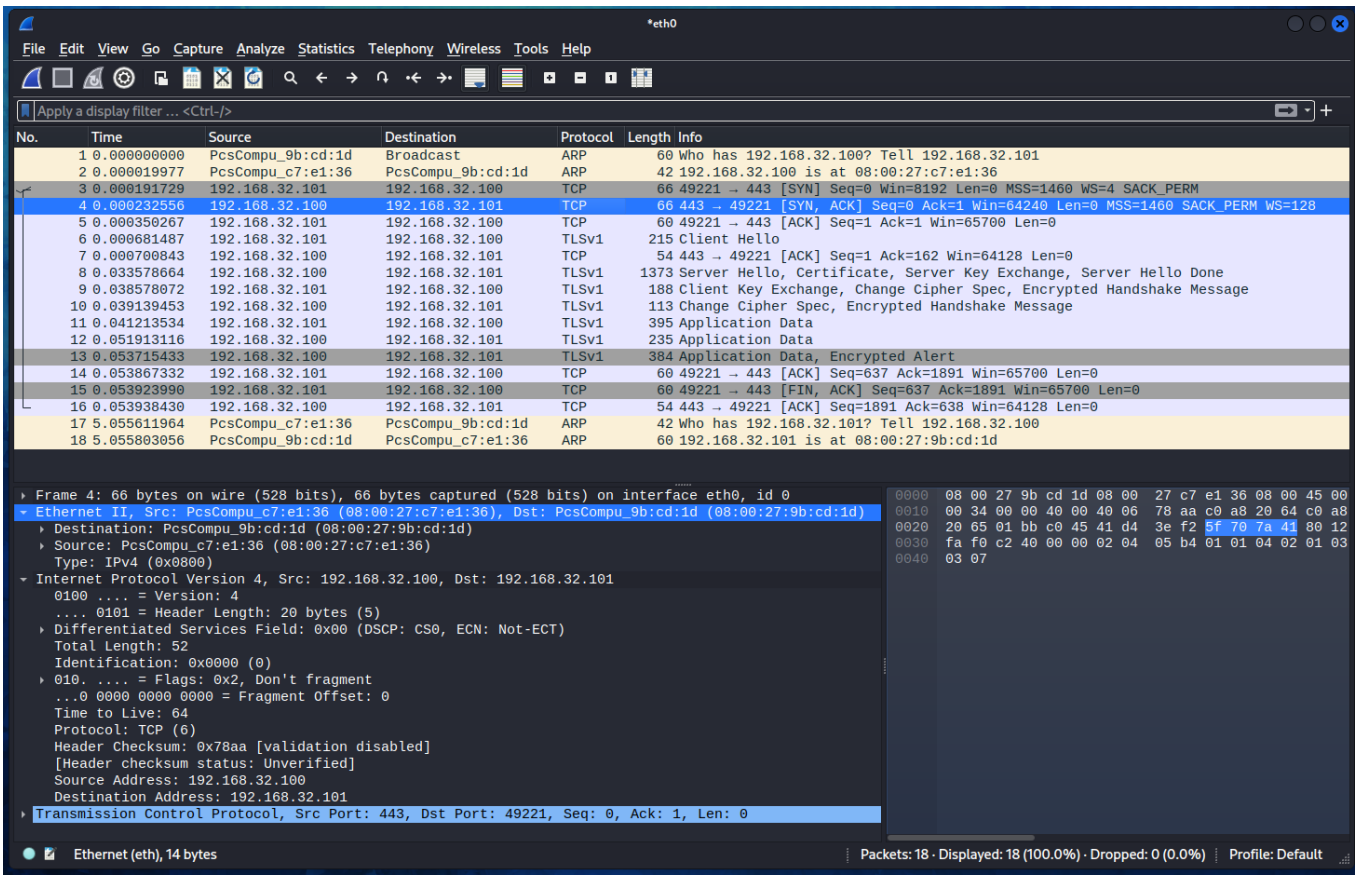
ANALISI PACCHETTI

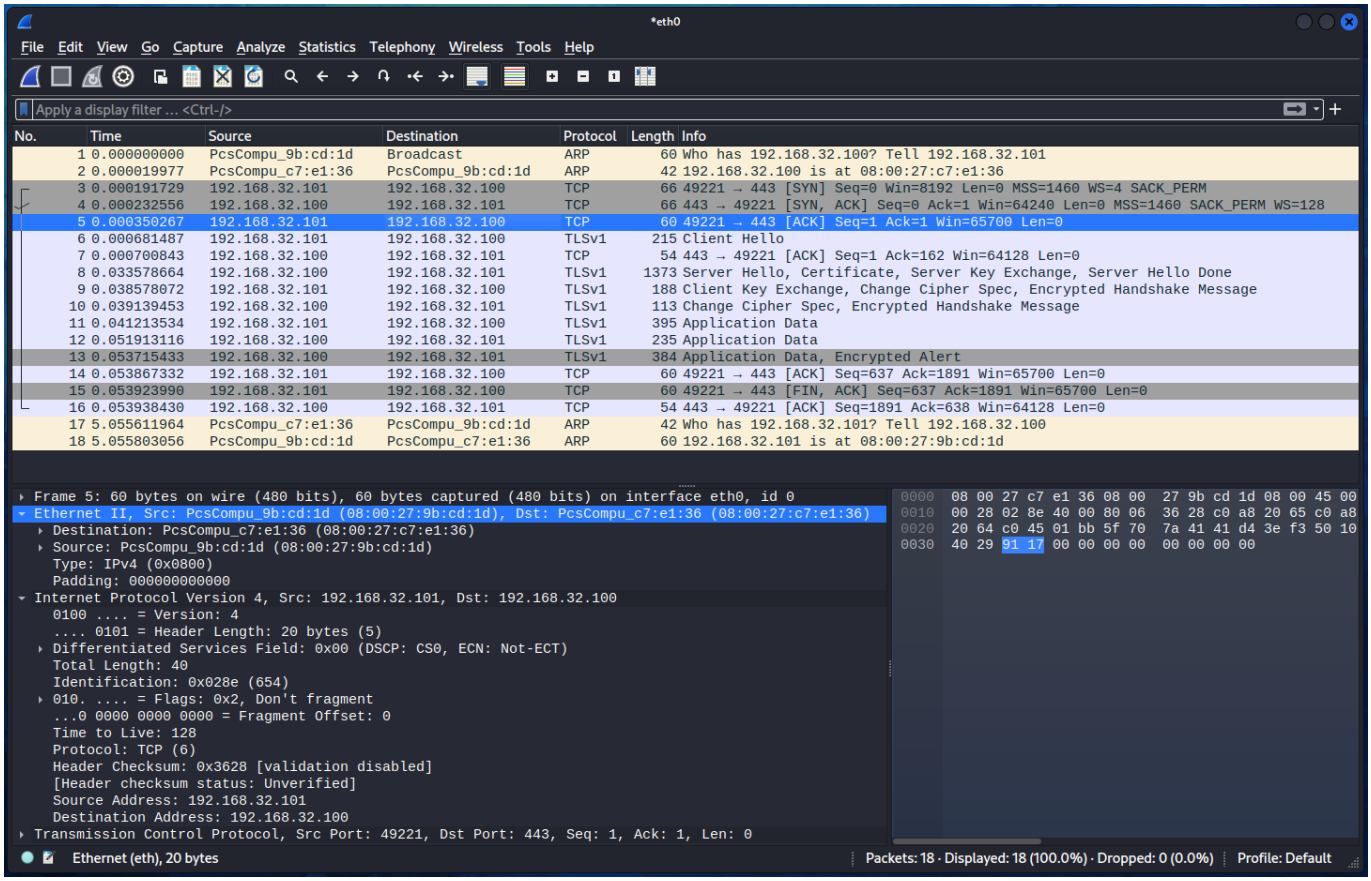
HTTPS



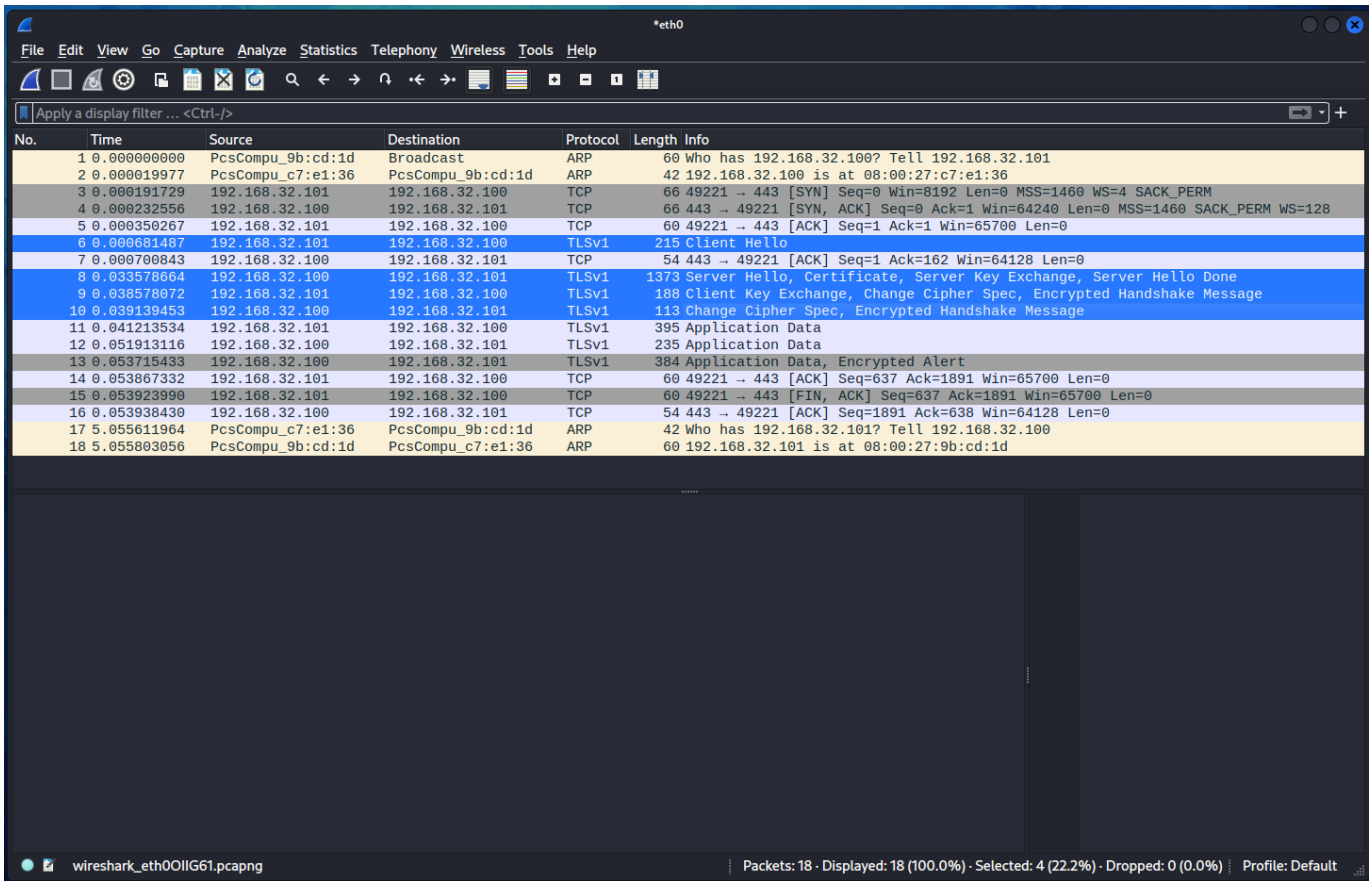
Dall'immagine precedente si può notare che:
- il MAC address sorgente è quello del client (windows 7) ovvero "08:00:27:9b:cd:1d"
- il MAC address destinazione è quello del server (kali linux) ovvero "08:00:27:c7:e1:36"

Nelle schermate successive tali MAC address si alternano tra source address e destination address in quanto sta avvenendo il cosiddetto "three way handshake" al fine di poter stabilire una connessione con protocollo TCP.





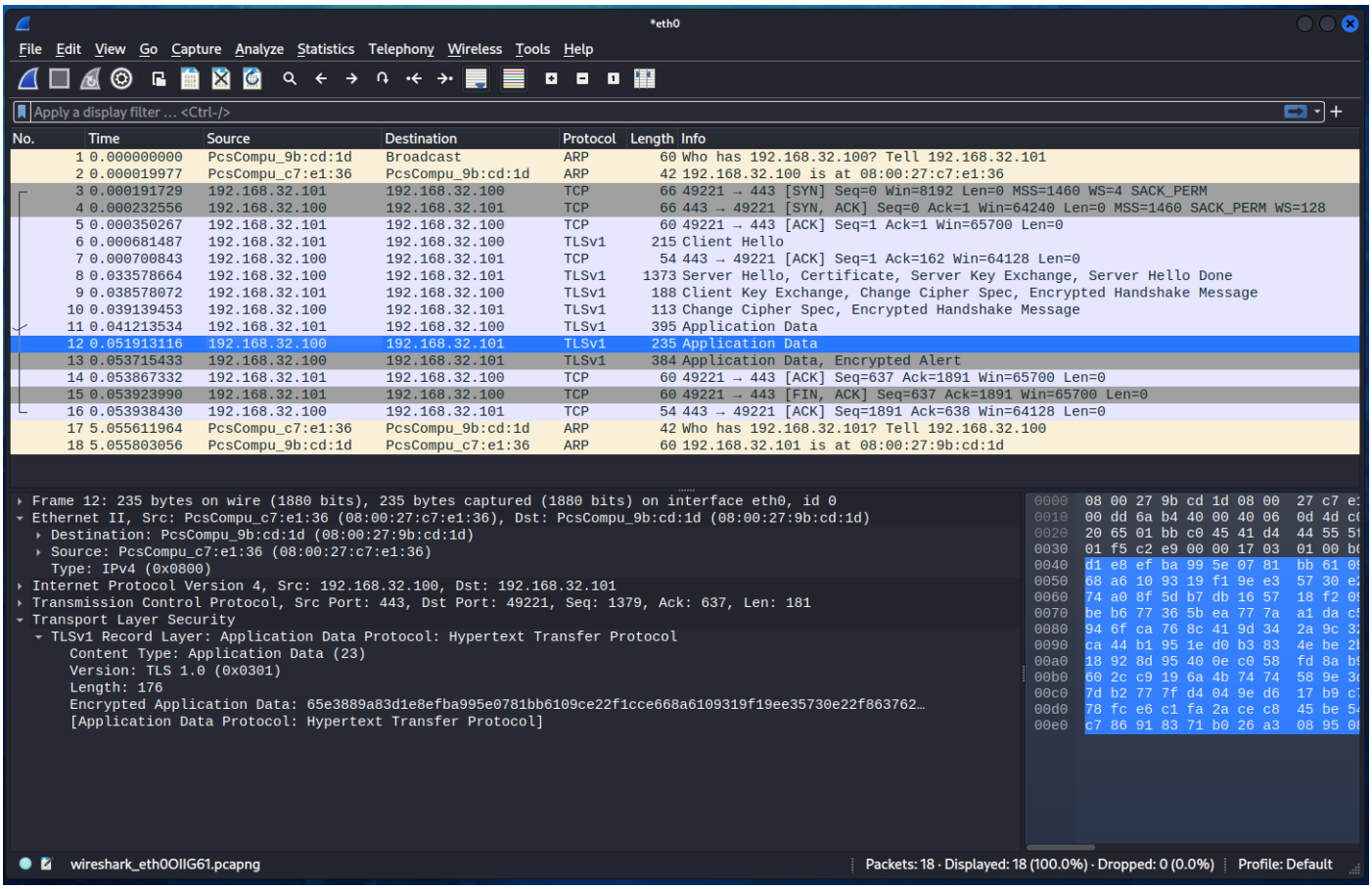
Nelle schermate precedenti possiamo notare che sono stati catturati pacchetti con protocollo TLSv1. Questi pacchetti sono presenti poiché la pagina web richiesta utilizza il protocollo “HTTPS” perciò viene utilizzato il protocollo di crittografia dei dati detto TLS (Transport Layer Security).



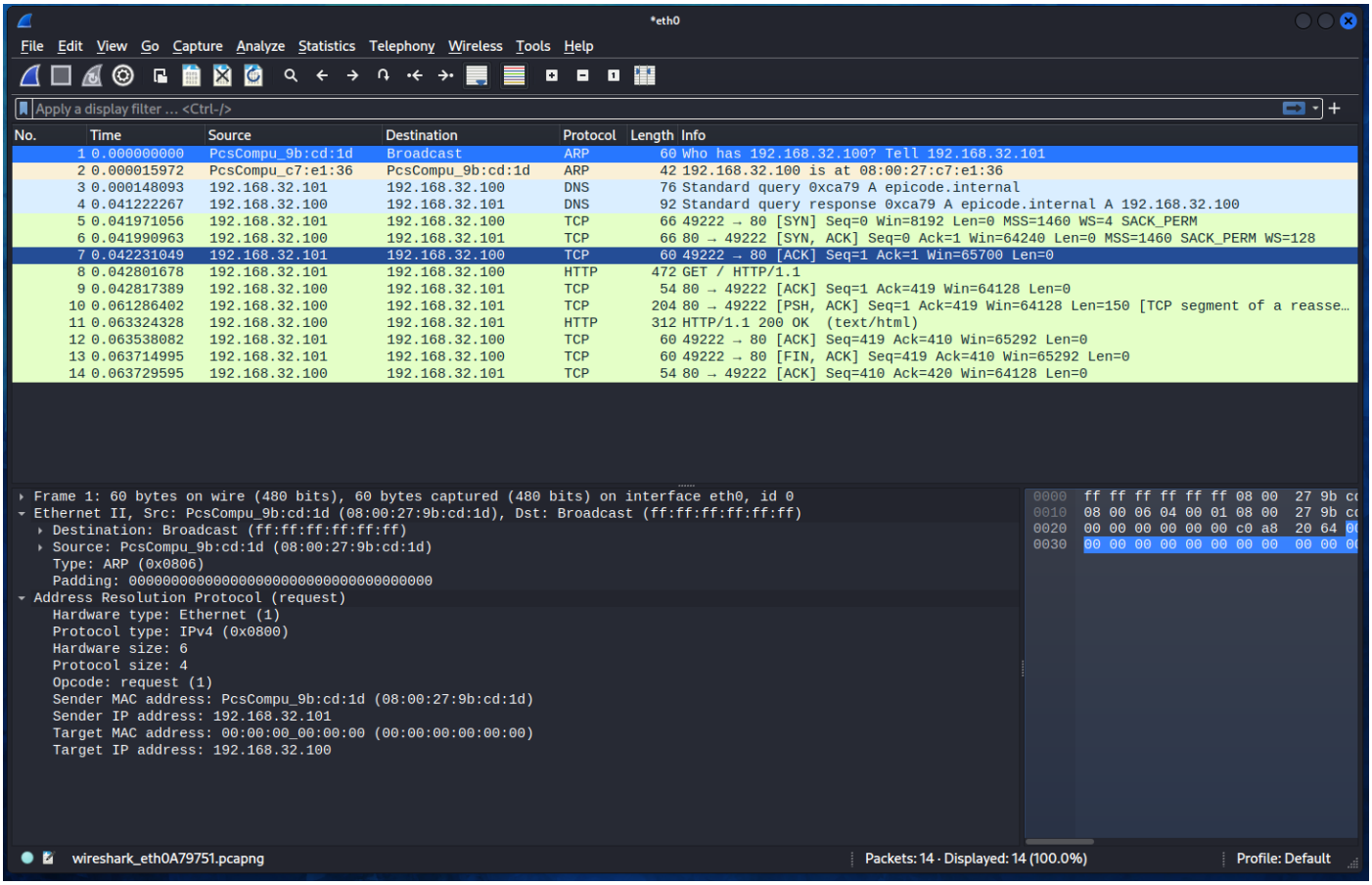
I pacchetti evidenziati in blu nell’immagine precedente rappresentano lo scambio di informazioni tra client e server al fine di poter instaurare la sessione crittografata. Il client ha inviato al server un messaggio “Client Hello” che riporta la

versione di TLS utilizzata e un elenco di suite di cifratura. Il server invia come risposta un messaggio “Server Hello” che riporta la suite di cifratura selezionata, il certificato e l'identificativo della sessione.

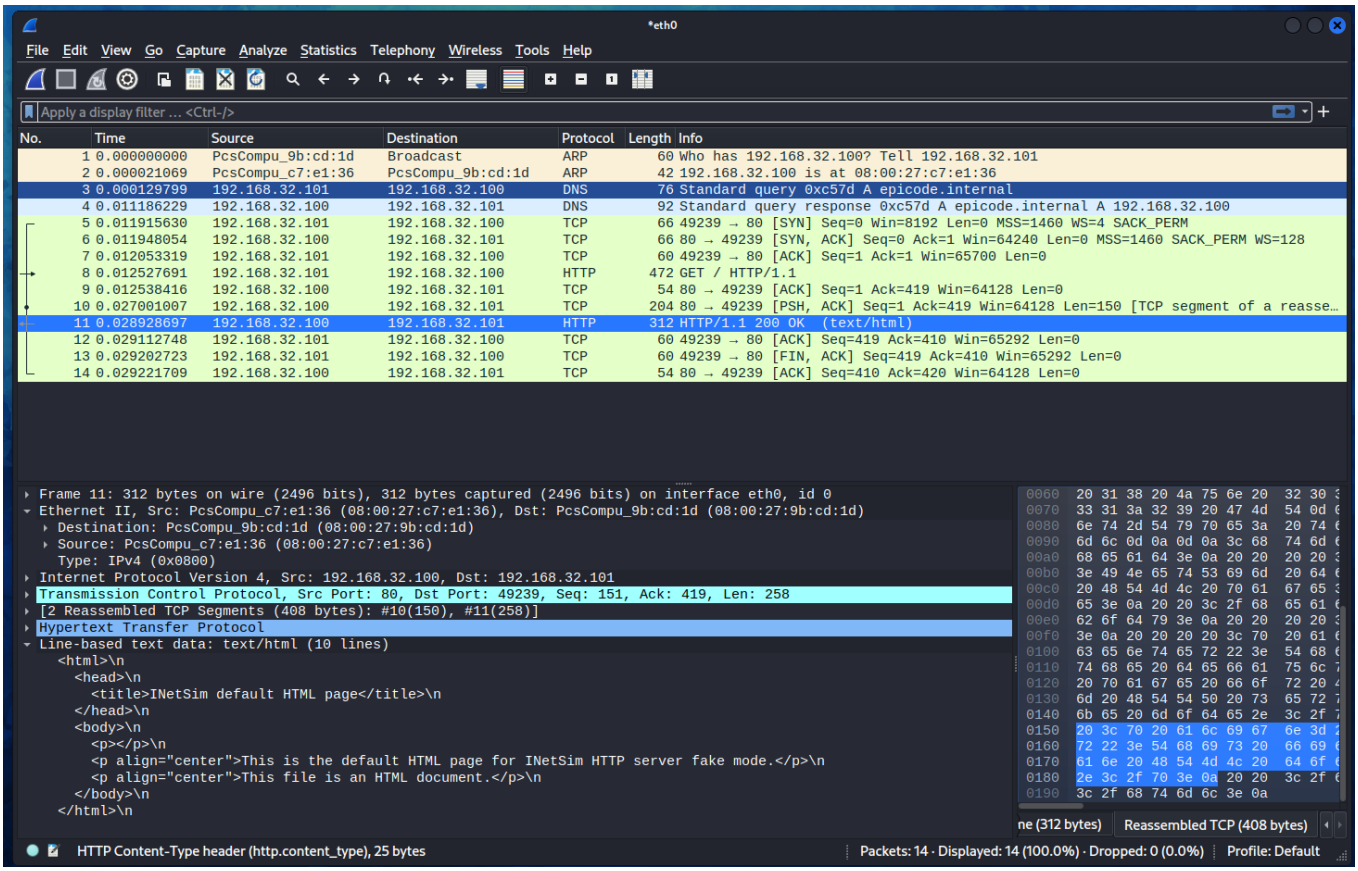
Arriviamo infine ai pacchetti contenenti i dati della pagina web che, come possiamo vedere nella penultima stringa del dettaglio del pacchetto selezionato, risultano crittografati.



HTTP



Nell'immagine precedente possiamo vedere i pacchetti che sono stati scambiati tra il client e il server HTTP.
Rispetto al server HTTPS rimangono invariati i tre pacchetti TCP sia all'inizio della connessione (three way handshake) che alla fine con la differenza che la porta utilizzata è diversa ovvero con HTTP viene utilizzata la porta 80 mentre con HTTPS viene utilizzata la porta 443.



Un’altra sostanziale differenza è nel tipo di pacchetti in quanto non vediamo più dei pacchetti di tipo TLS ma solo pacchetti di tipo HTTP in quanto questi ultimi non sono più crittografati infatti, come mostrato nella schermata precedente si può notare che riusciamo a leggere il codice HTML della pagina visitata dal client.
Nella cattura dei pacchetti possiamo vedere anche i quelli di tipo DNS che dimostrano che è stata fatta richiesta al server DNS per la risoluzione del nome di dominio “epicode.internal”.