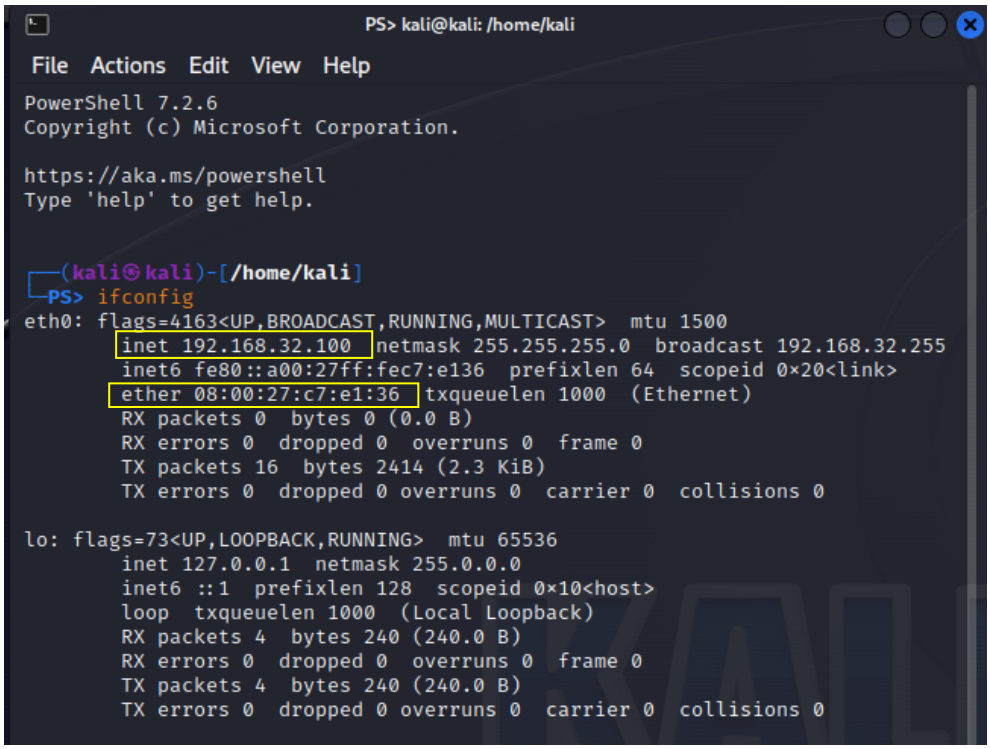
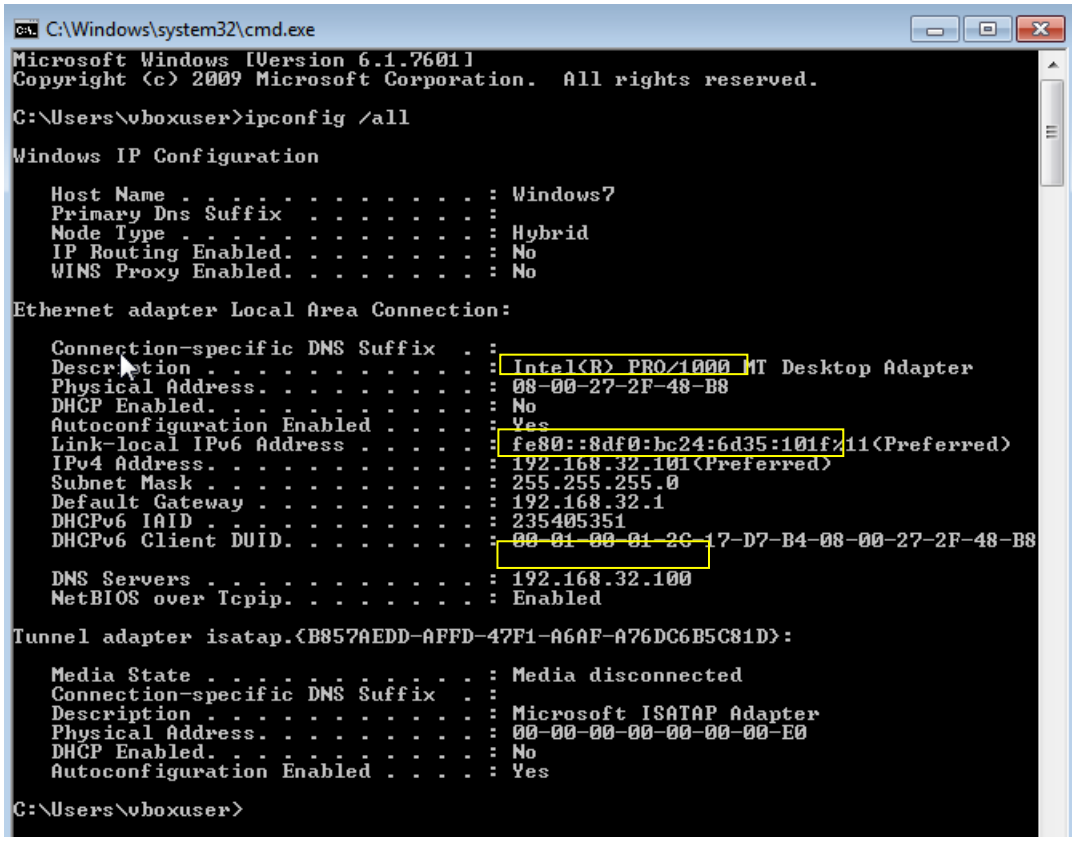
Configurazione IP statico e client/server DSN

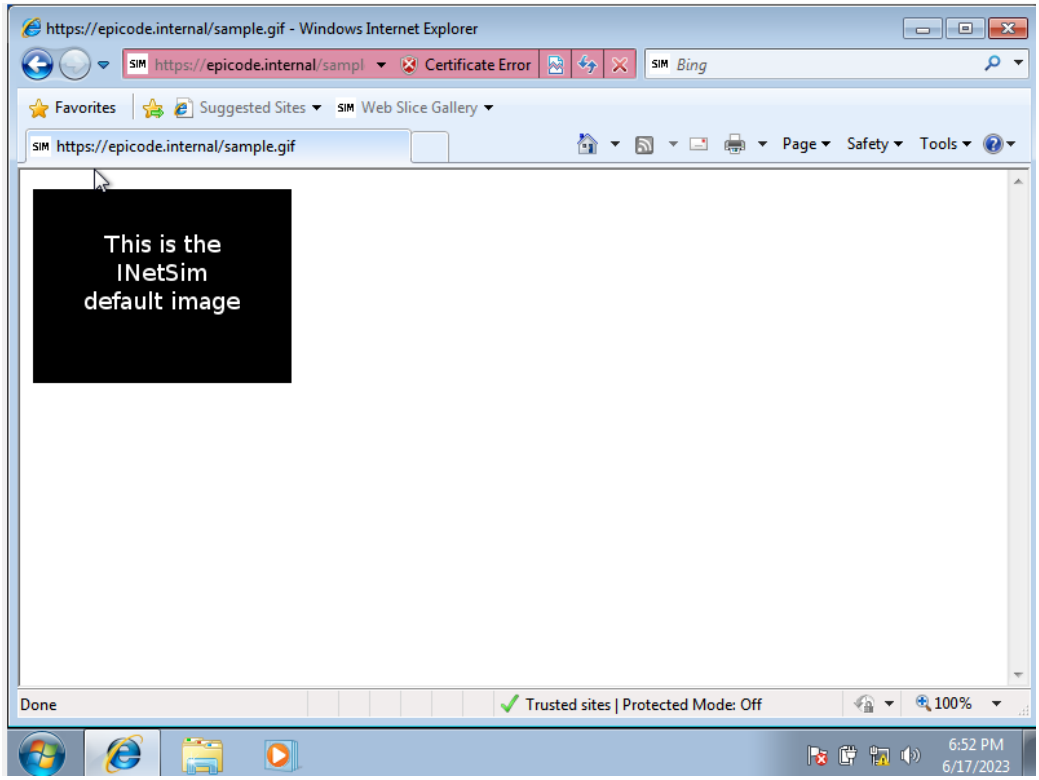
Kali Linux 192.168.32.100



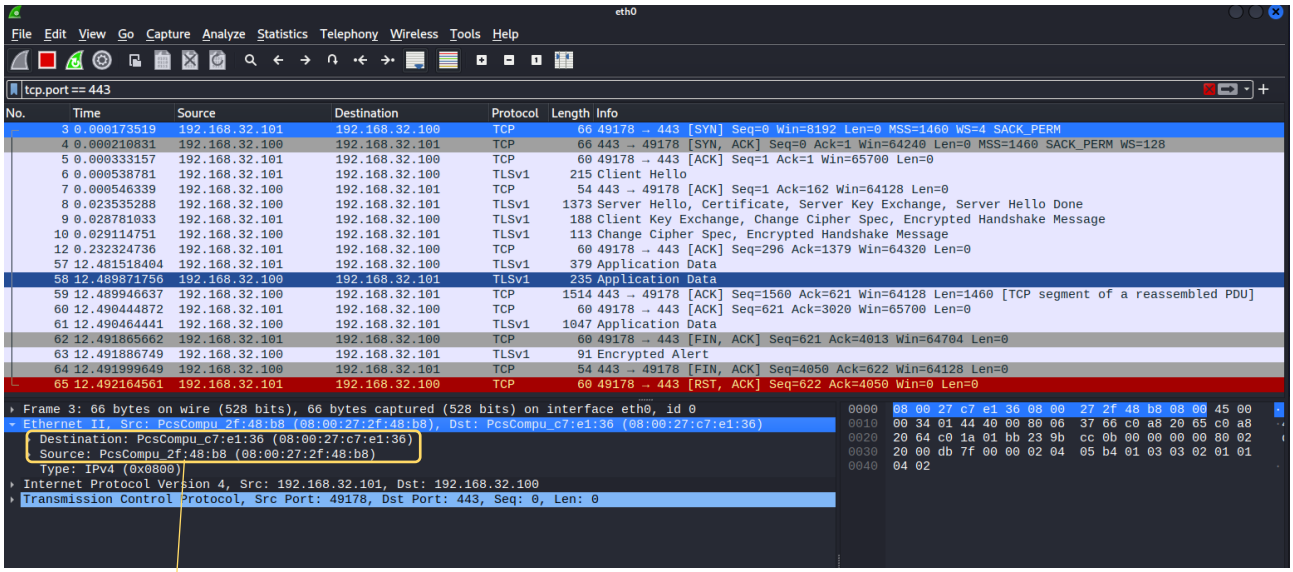
Windows 7 192.168.32.101



Richiesta HTTPS da Windows 7 a epicode.internal/sample.gif



Pacchetti catturati con Wireshark (richiesta HTTPS)

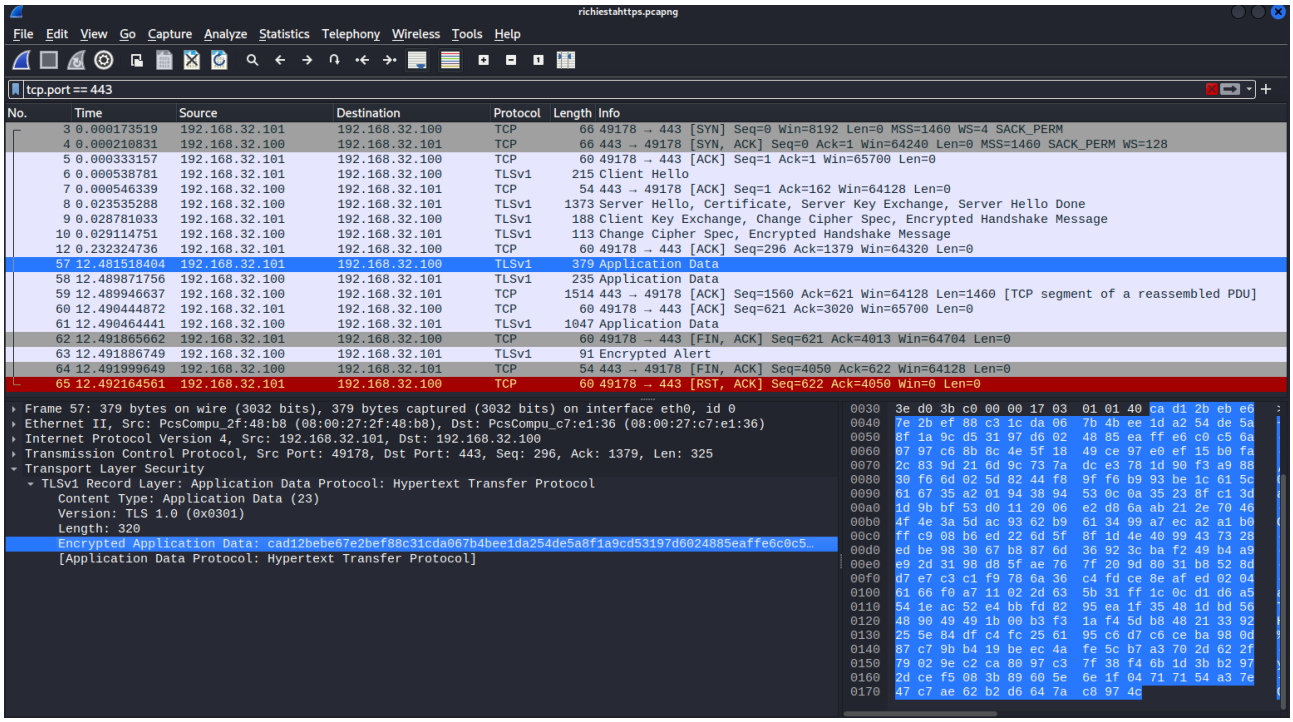


indirizzo MAC sorgente: 08:00:27:2f:48:b8

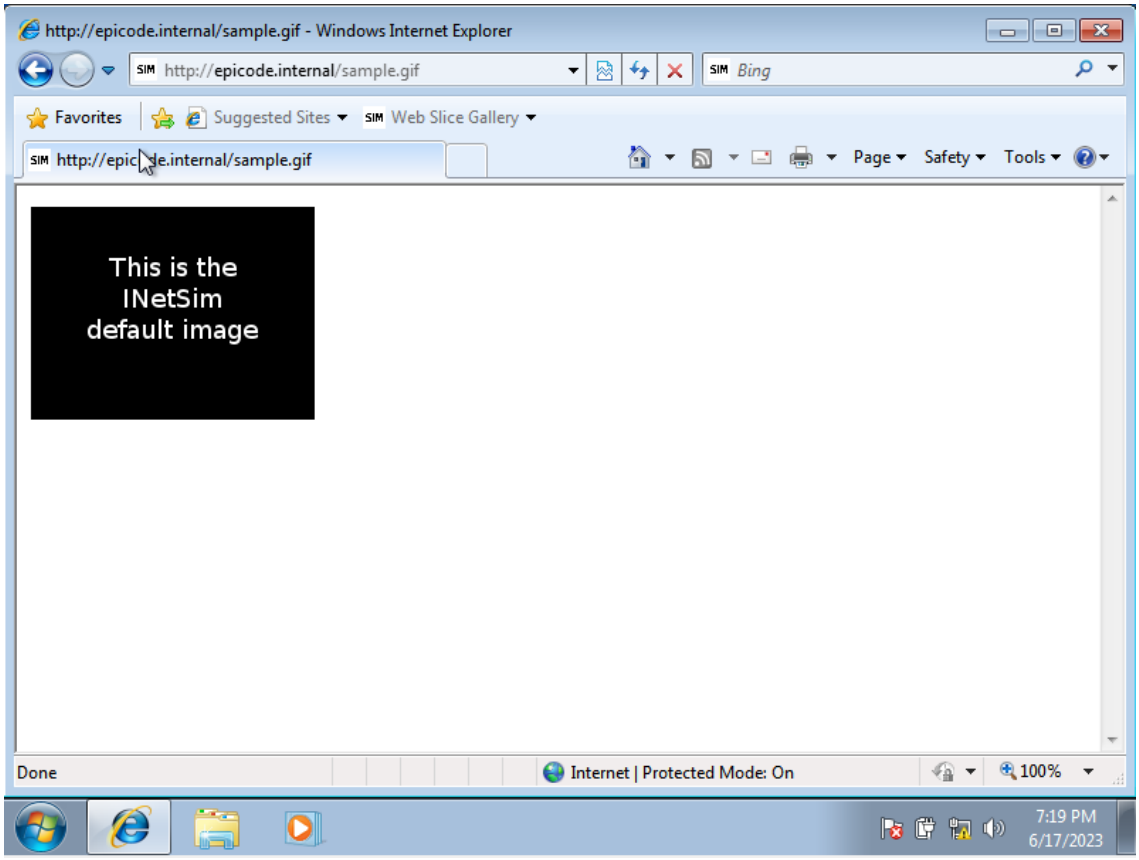
indirizzo MAC destinazione: 08:00:27:c7:e1:36

Contenuto della richiesta HTTPS

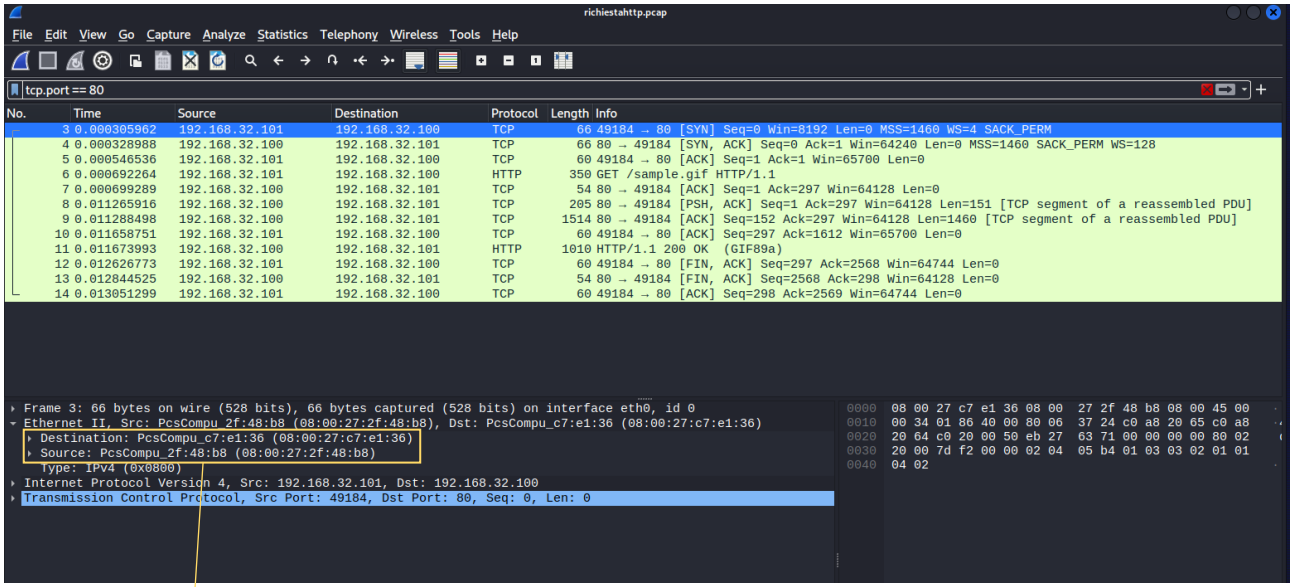
Trattandosi di richiesta HTTPS (o HTTP secure), il contenuto è criptato



Richiesta HTTP da Windows 7 a epicode.internal/sample.gif



Pacchetti catturati con Wireshark (richiesta HTTP)

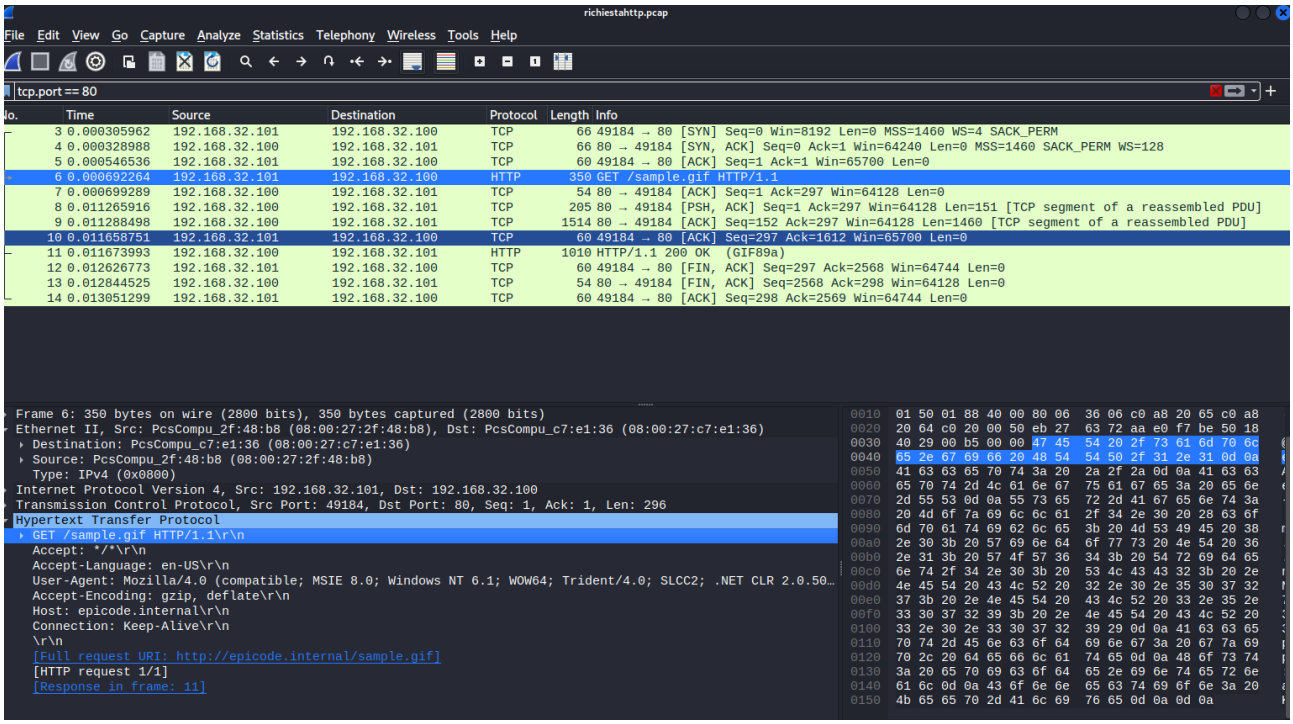


indirizzo MAC sorgente: 08:00:27:2f:48:b8

indirizzo MAC destinazione: 08:00:27:c7:e1:36

Contenuto della richiesta HTTP

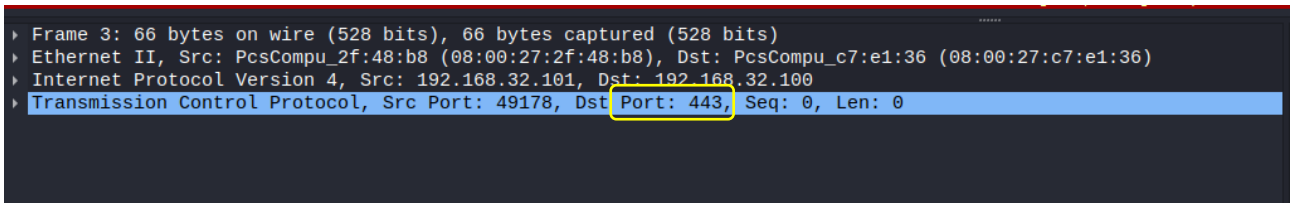
In questo caso il contenuto della richiesta è in chiaro:



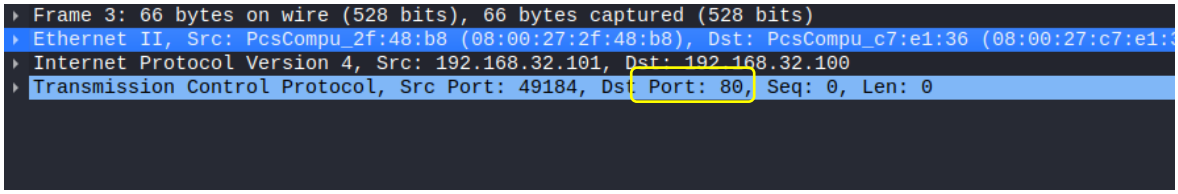
Differenze tra HTTPS e HTTP

Le richieste HTTPS e HTTP utilizzano entrambe il protocollo TCP per il trasporto su porte differenti.

Il protocollo HTTPS utilizza la porta 443



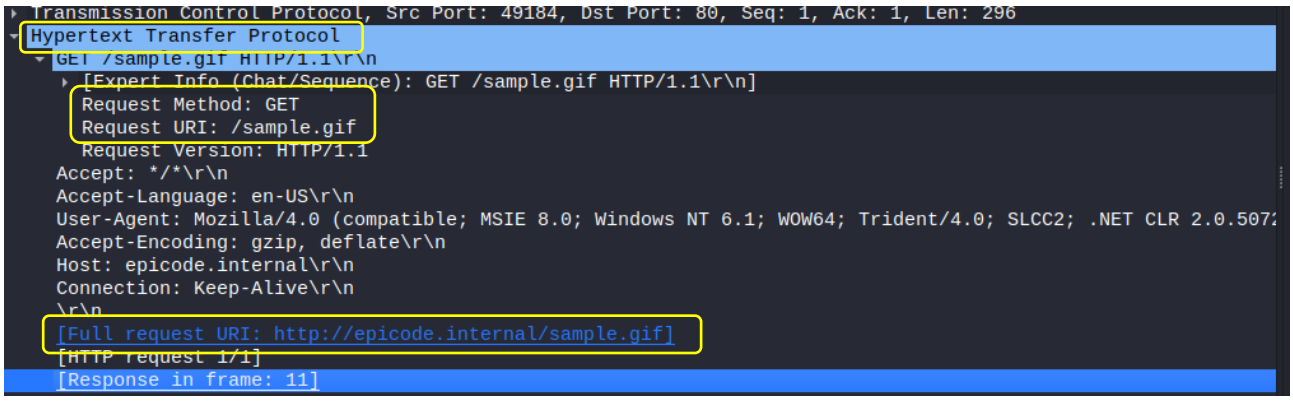
mentre il protocollo HTTP utilizza la porta 80



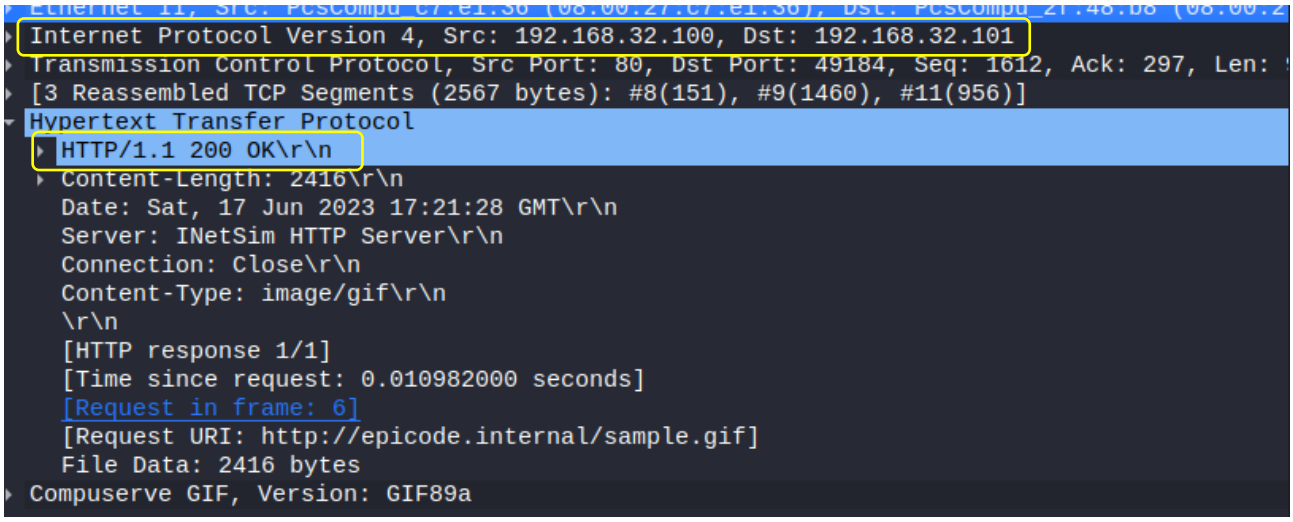
La differenza principale tra i due protocolli però sta nel layer applicazione.

Nel caso di HTTP, il protocollo utilizzato è HTTP e la richiesta è in chiaro.

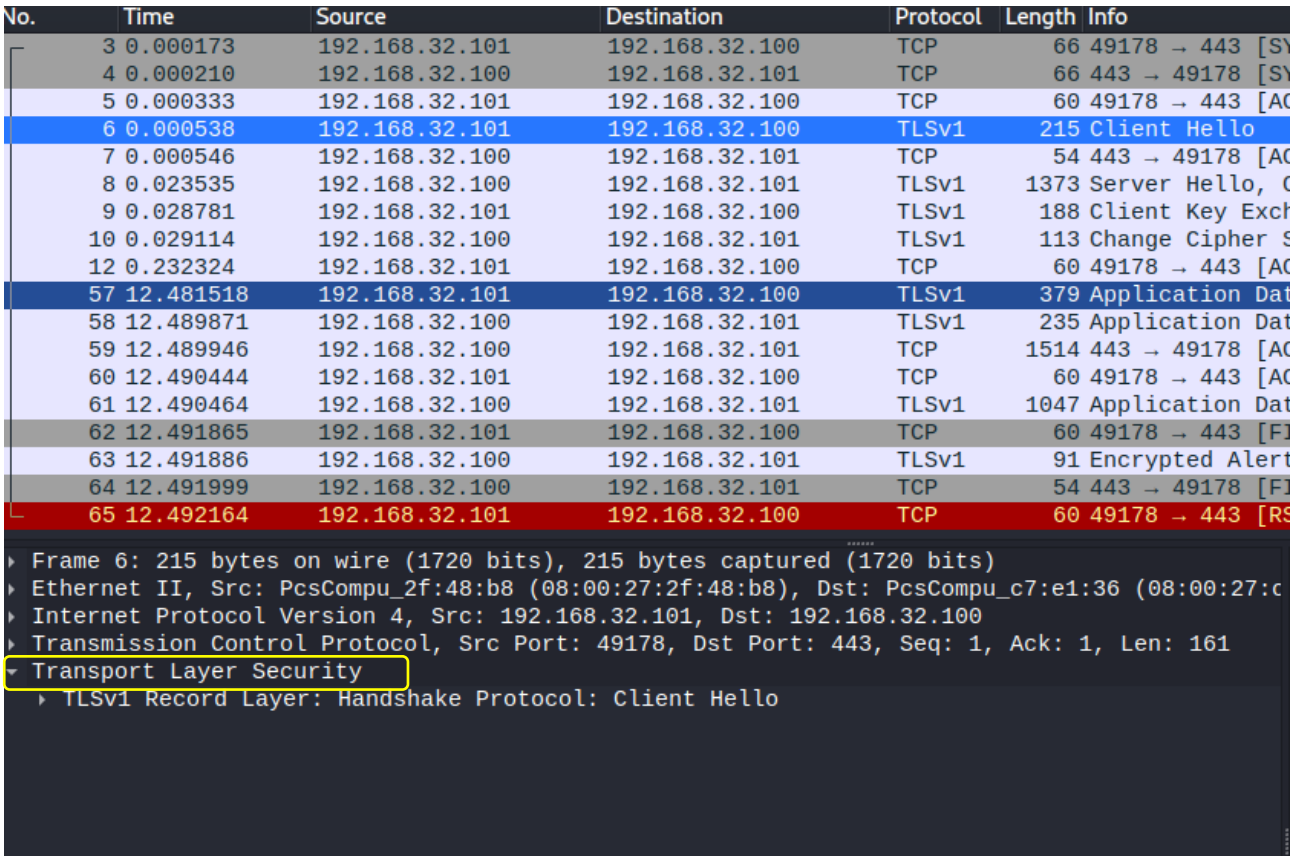
Nel layer applicazione vediamo che viene utilizzato l'Hypertext Transfer Protocol. In questo caso la richiesta utilizza il metodo GET e il file "sample.gif" che è stato richiesto è visibile in chiaro nel pacchetto.

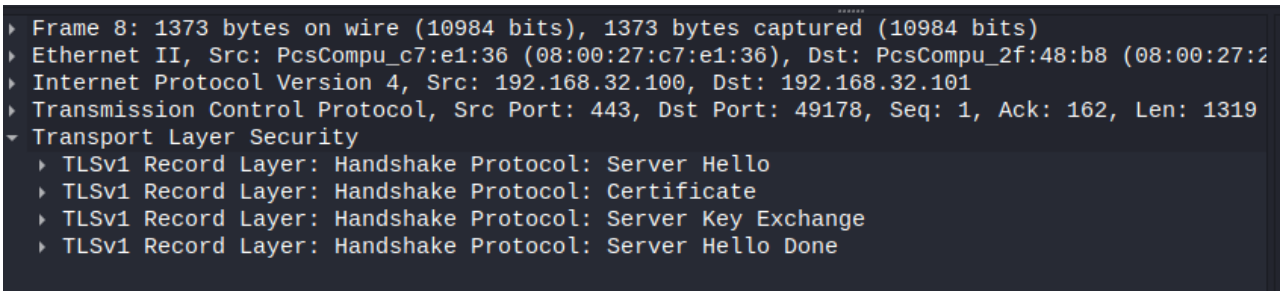


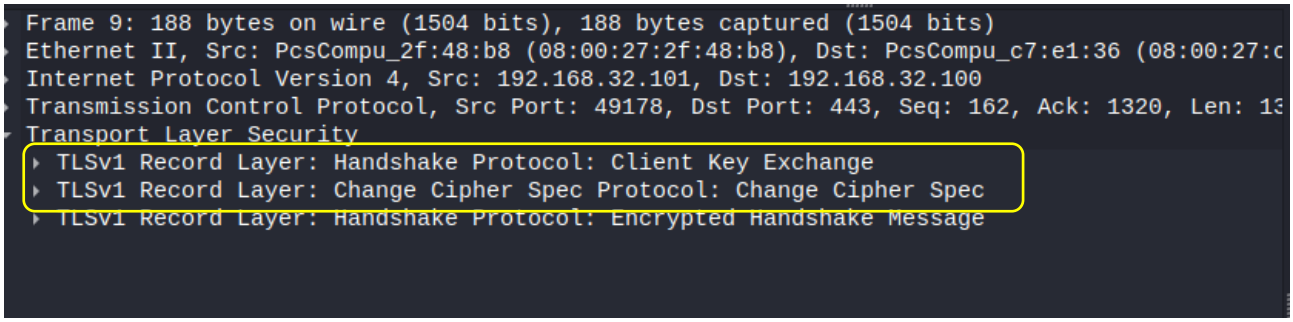
Vediamo nel pacchetto successivo di risposta dal server che l'esito della richiesta è OK (codice stato 200).

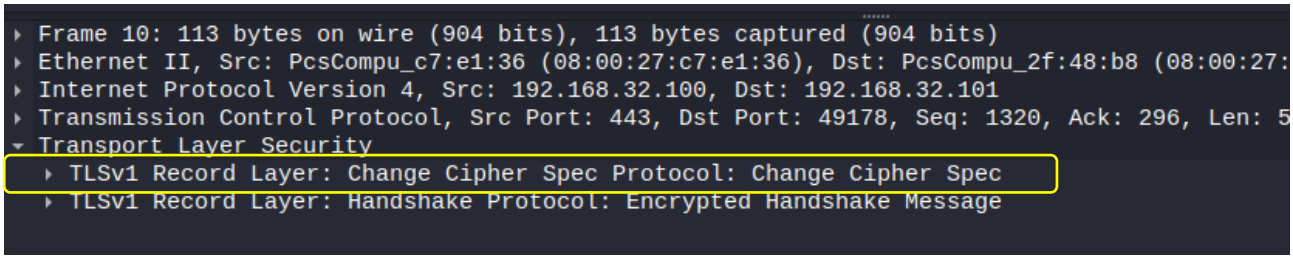


Nel caso di HTTPS, il contenuto è criptato utilizzando un protocollo cifrato (TLSv1 in questo caso). Al protocollo "Hypertext Transfer Protocol" che abbiamo nel caso di HTTP, nella richiesta HTTPS viene sovrapposto il protocollo "Transport Layer Security". I pacchetti vengono scambiati in formato cifrato dopo una comunicazione client/server che comprende lo scambio della chiave di sicurezza:









fino ad arrivare alla richiesta vera e propria, che viene trasmessa in formato criptato e non è quindi direttamente leggibile nel pacchetto.