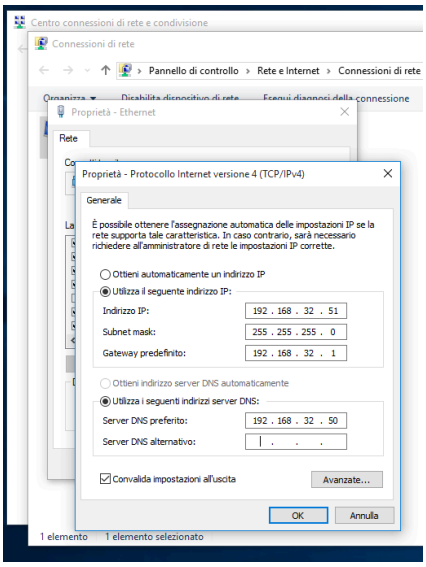
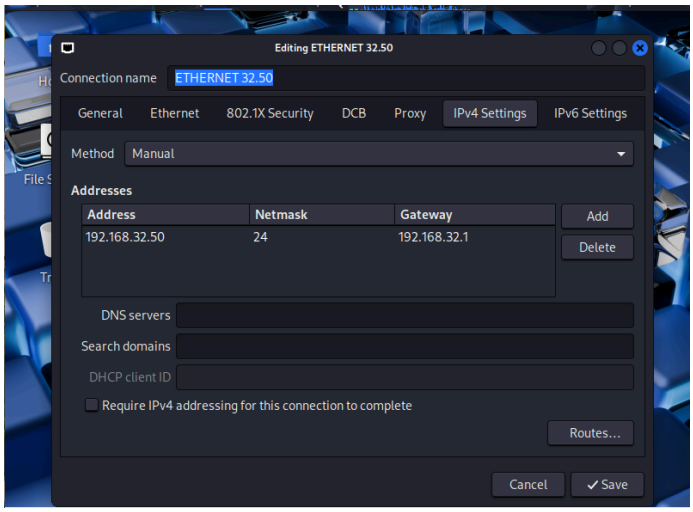
PROGETTO FINE MODULO M1

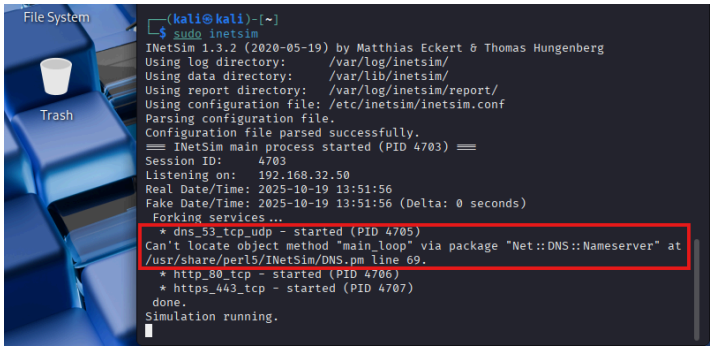
Simulare, in ambiente di laboratorio virtuale, un'architettura client server in cui un client con indirizzo 192.168.32.51 (Windows) richiede tramite web browser una risorsa all'hostname epicode.internal che risponde all'indirizzo 192.168.32.50 (Kali).
Si intercetti poi la comunicazione con Wireshark, evidenziando i MAC address di sorgente e destinazione ed il contenuto della richiesta HTTPS. Ripetere l'esercizio, sostituendo il server HTTPS, con un server HTTP. Si intercetti nuovamente il traffico, evidenziando le eventuali differenze tra il traffico appena catturato in HTTP ed il traffico precedente in HTTPS. Spiegare, motivandole, le principali differenze se presenti.

Sono partito impostando rete interna delle due macchine virtuali su VirtualBox, poi ho impostato indirizzi IP manualmente su KALI 192.168.32.50 e poi su Windows 192.168.32.51 e infine sempre su Windows ho inserito come DNS predefinito quello dato a KALI ovvero 192.168.32.50. Immagini Windows a sinistra e a destra KALI.

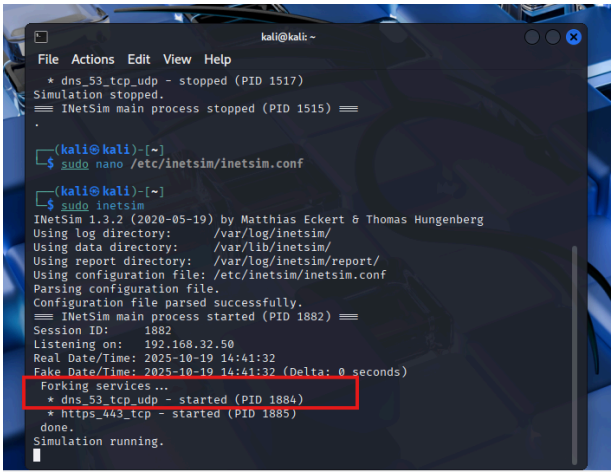




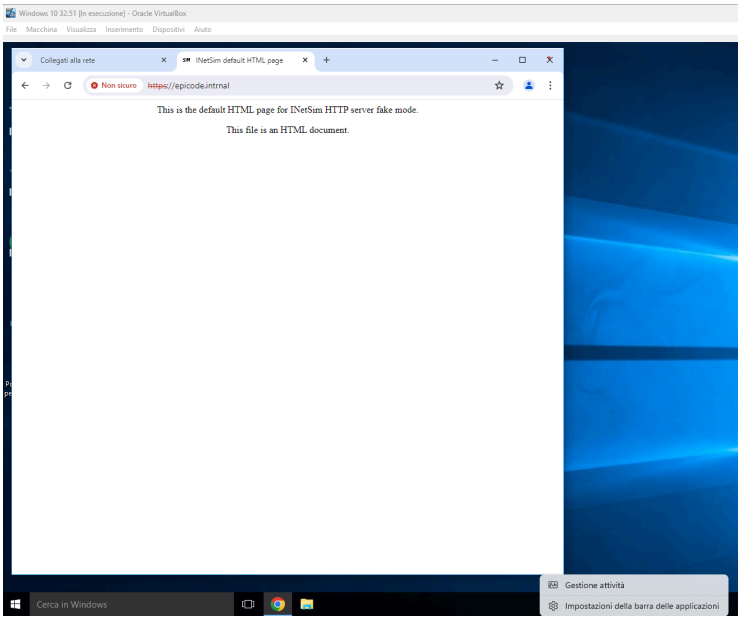
Dopo aver attribuito gli indirizzi IP alle macchine virtuali e aver messo un DNS di riferimento a Windows, su kali ho modificato le impostazioni di Inetsim rendendo attivi i servizi DNS, HTTP e HTTPS per poter simulare dei servizi web. Ho inserito su Inetsim nella riga dns_default.ip e nella riga service_bind_address l'indirizzo 192.168.32.50. Poi ho inserito nella riga dns_default_name epicode, mentre nella riga dns_default_domainname internal. ho cancellato i cancelletti ha inizo riga per poter rendere tutti i servizi necessari attivi. Dopodiché ho salvato le modifiche e sembrava tutto pronto ma una volta provato ad avviare Inetsim il DNS dava un errore:



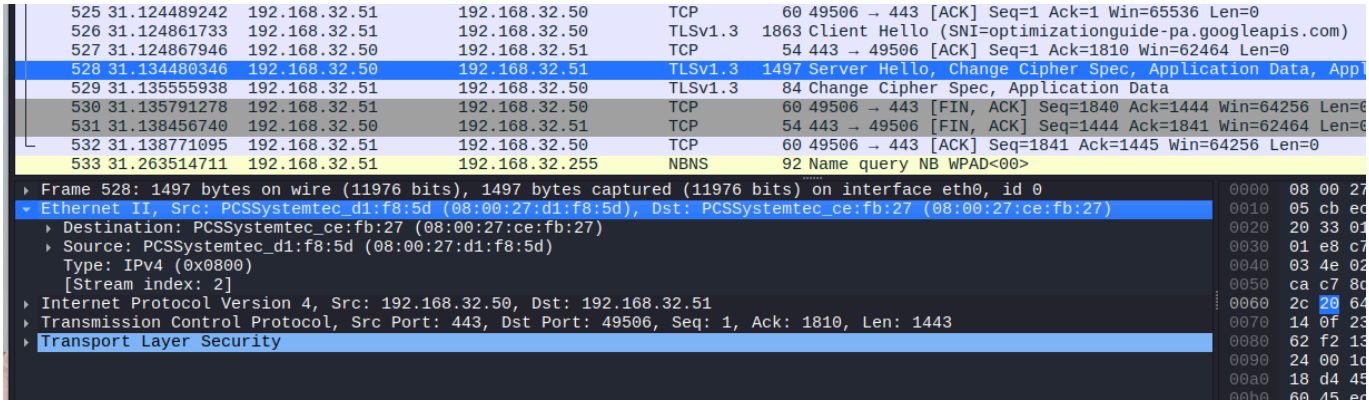
Ho risolto l'errore copiandolo e incollandolo su google, sono giunto ad una pagina di discussioni dove veniva spiegato che per far funzionare quel servizio di Inetsim bisognava installare una versione più vecchia del sevizio DNS, nella conversazione ho trovato il link per il download e tutti i comandi utili alla sua installazione, eccetto il comando che serviva per decomprimere il file scaricato, il quale mi ha fatto sudare per essere trovato. Dunque ho collegato Kali ad internet per poter scaricare il file e una volta eseguiti tutti i comandi per la usa installazione il servizio DNS di Inetsim ha iniziato a funzionare.



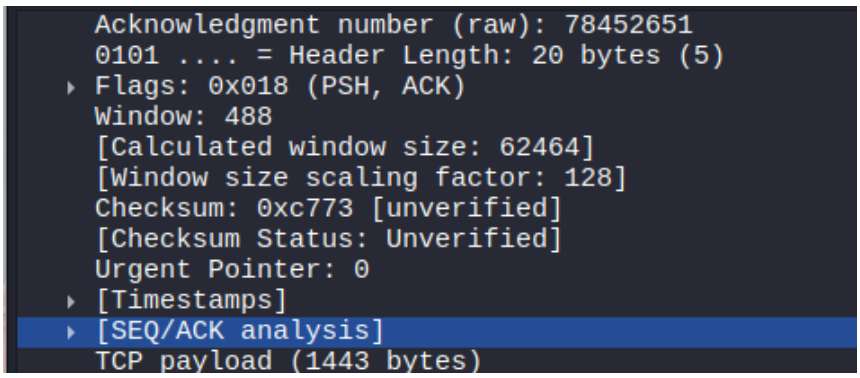
Una volta avviato Inetsim senza errori ho tentato la ricerca da il Browser di Windows, e la ricerca è andata in porto:



Visto che tutto è andato come dovrebbe ho iniziato a osservare i pacchetti con wireshark, iniziando ad osservare una connessione HTTPS:

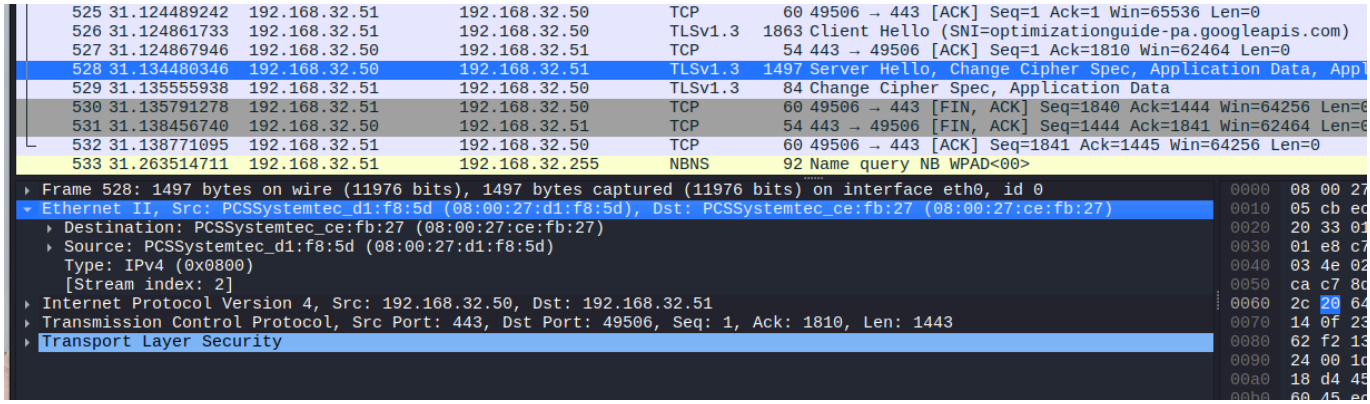


Questo è lo screenshot della risposta del server al client, si possono trovare gli indirizzi MAC ed attribuirli agli indirizzi IP, perché sapendo che è la risposta del server il source IP è 192.268.32.50 e nella riga evidenziata troviamo il source mac address che è 08:00:27:d1:f8:5d e troviamo anche il destination address quindi IP 192.168.32.51 e il suo MAC address 08:00:27:ce:fb:27 che sono gli indirizzi del client.
Da questa foto si possono anche rilevare il numero di bytes che sono passati nel cavo.

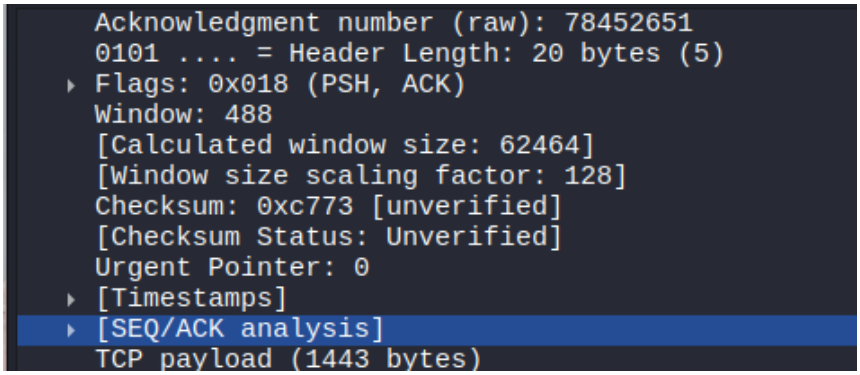


OSSERVAZIONE PACCHETTI HTTPS CON WIRESHARK

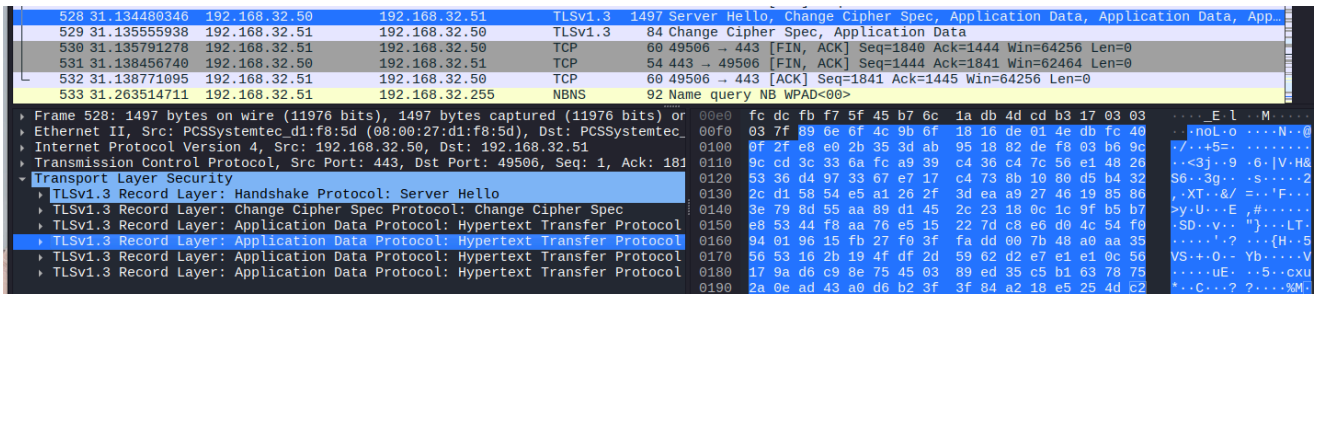
Visto che tutto è andato come dovrebbe ho iniziato a osservare i pacchetti con wireshark, iniziando ad osservare una connessione HTTPS:



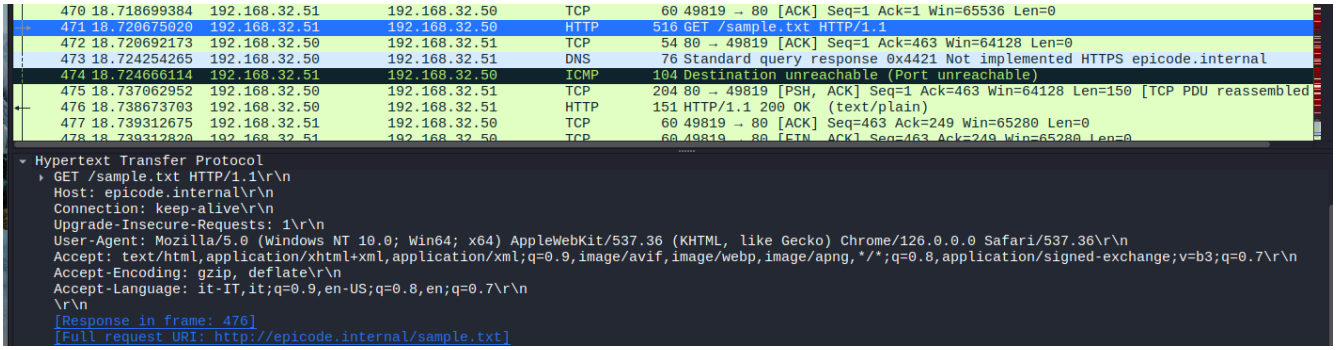
Questo è lo screenshot della risposta del server al client, si possono trovare gli indirizzi MAC ed attribuirli agli indirizzi IP, perché sapendo che è la risposta del server il source IP è 192.268.32.50 e nella riga evidenziata troviamo il source mac address che è 08:00:27:d1:f8:5d e troviamo anche il destination address quindi IP 192.168.32.51 e il suo MAC address 08:00:27:ce:fb:27 che sono gli indirizzi del client.
Da questa foto si possono anche rilevare il numero di bytes che sono passati nel cavo.



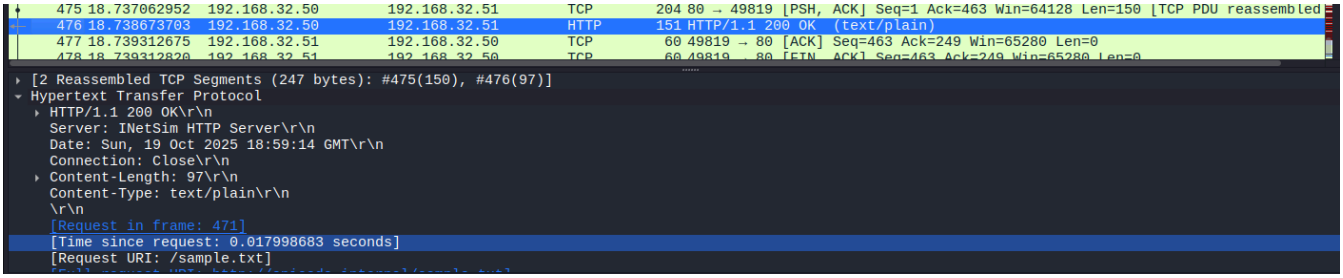
gli unici altri dati che si riescono a carpire su HTTPS sono la lunghezza dell'header e del payload in bytes il resto dei dati è tutto cifrato e impossibile da leggere.



OSSERVAZIONE PACCHETTI CON WIRESHARK SU HTTP



Qui sopra abbiamo una richiesta del client ad un server in HTTP, si possono vedere in chiaro il tipo di richiesta, il formato del file richiesto, tipo di connessione, il nome dell'host, da quale programma sta effettuando la richiesta e in che lingua è stata effettuata la richiesta. e poi in fondo c'é anche l'URI completo



Anche dalla risposta del server possiamo carpire molte informazioni: ad esempio che la risposta è stata positiva, informazioni sul server, la data con giorno e orario e la lunghezza del contenuto in bytes.

CONCLUSIONE

Le principali differenze tra HTTP e HTTPS sono che utilizzano numeri di porta differenti HTTP (80) e HTTPS (403), e soprattutto i dati su HTTP possono essere visti in chiaro se intercettati da qualcuno, mentre su HTTPS i pacchetti vengono cifrati da TLS cosicché se venissero intercettati da qualcuno questi siano incomprensibili garantendo la privacy dei client che intendono usare i servizi di un sito web.