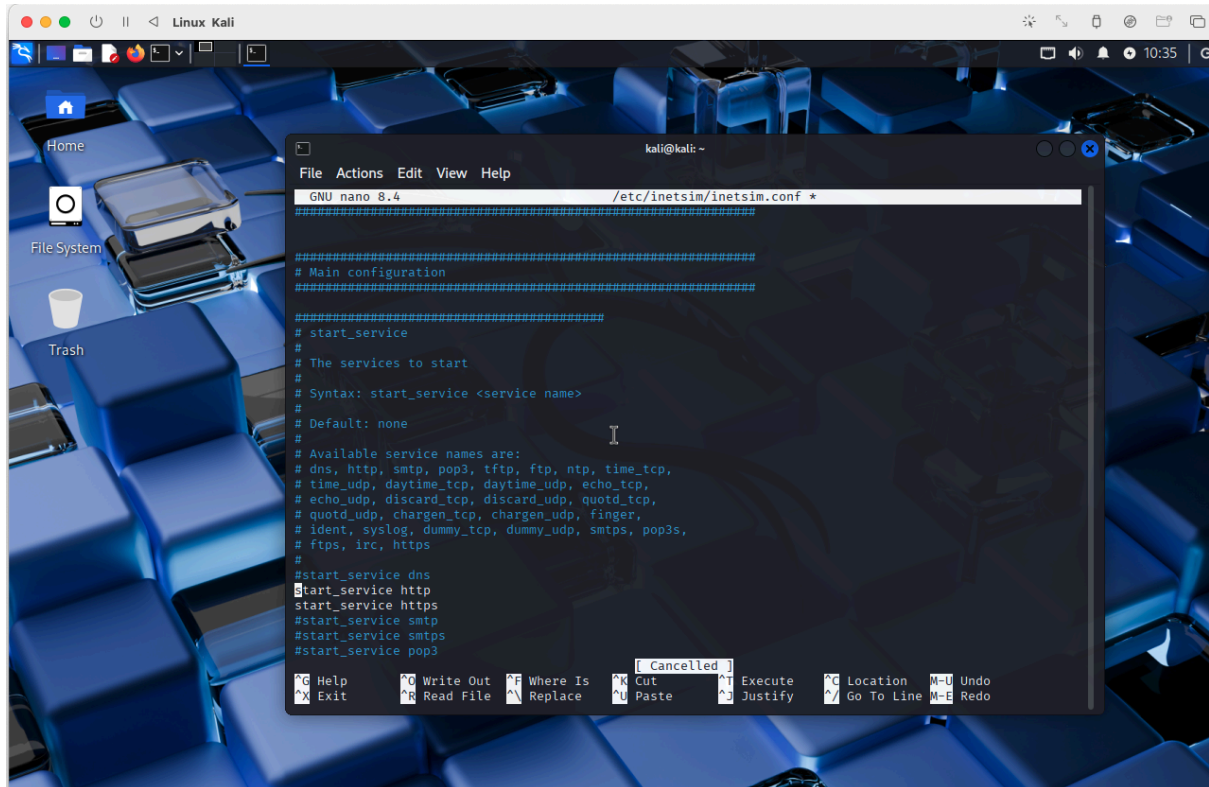


CONSEGNA FINE PRIMO MODULO BRUNI GABRIELE

Obiettivo: Simulare una comunicazione HTTP/HTTPS tra un client Windows e un server Kali Linux, analizzando il traffico con Wireshark e documentando le differenze tra i protocolli.

STEP 1: configurazione di Inetsim. Ho decommentato i servizi necessari e, una volta salvato, ho avviato il servizio.



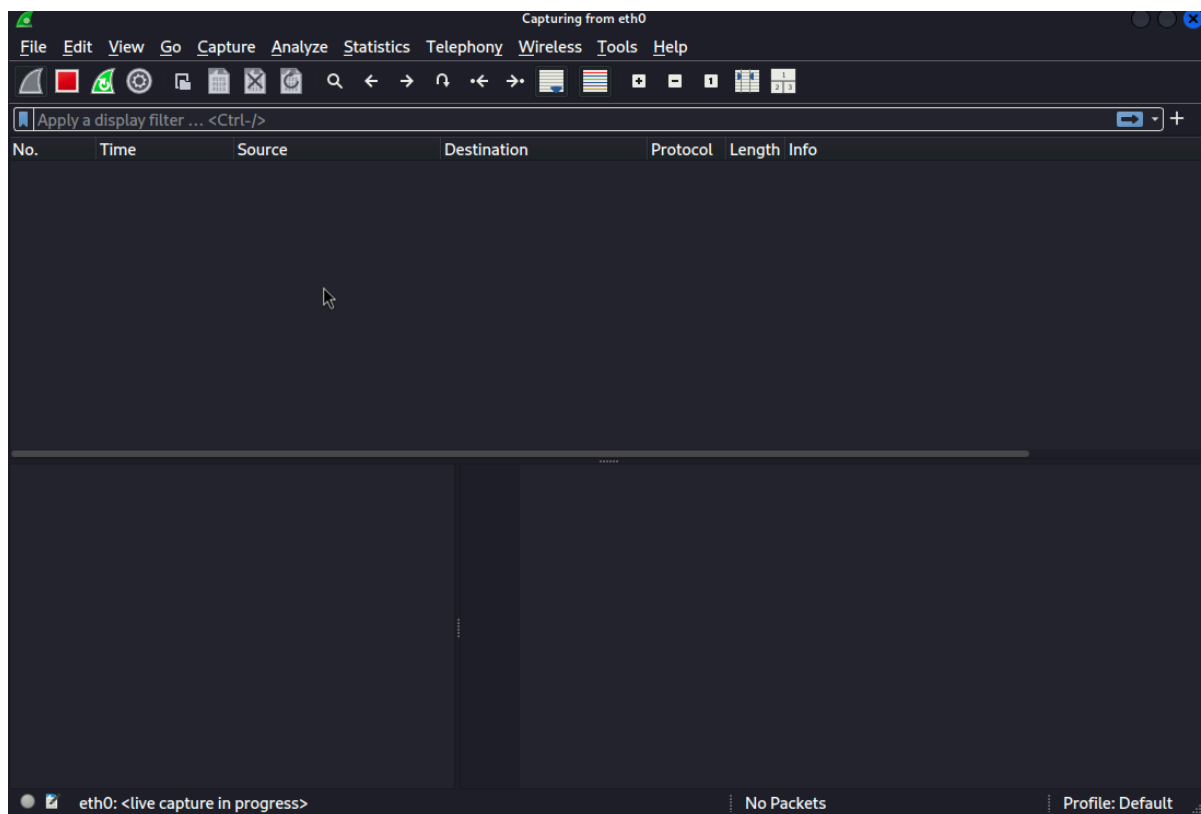
```
File Actions Edit View Help
GNU nano 8.4 /etc/inetsim/inetsim.conf *
#####
# Main configuration
#####
#####
# start_service
#
# The services to start
# Syntax: start_service <service name>
# Default: none
#
# Available service names are:
# dns, http, smtp, pop3, tftp, ftp, ntp, time_tcp,
# time_udp, daytime_tcp, daytime_udp, echo_tcp,
# echo_udp, discard_tcp, discard_udp, quotd_tcp,
# quotd_udp, chargen_tcp, chargen_udp, finger,
# ident, syslog, dummy_tcp, dummy_udp, smtps, pop3s,
# ftps, irc, https
#
#start_service dns
start_service http
start_service https
start_service smtp
start_service smtps
start_service pop3

[Cancelled]
Help Write Out Where Is Cut Execute Location M-U Undo
Exit Read File Replace Paste Justify Go To Line M-E Redo
```

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ sudo nano /etc/inetsim/inetsim.conf  
[sudo] password for kali:  
(kali@kali)-[~]  
$ sudo inetsim  
INetSim 1.3.2 (2020-05-19) by Matthias Eckert & Thomas Hungenberg  
Using log directory: /var/log/inetsim/  
Using data directory: /var/lib/inetsim/  
Using report directory: /var/log/inetsim/report/  
Using configuration file: /etc/inetsim/inetsim.conf  
Parsing configuration file.  
Configuration file parsed successfully.  
== INetSim main process started (PID 8644) ==  
Session ID: 8644  
Listening on: 127.0.0.1  
Real Date/Time: 2025-07-23 10:41:31  
Fake Date/Time: 2025-07-23 10:41:31 (Delta: 0 seconds)  
Forking services ...  
* https_443_tcp - started (PID 8647)  
* http_80_tcp - started (PID 8646)  
done.  
Simulation running.  
█
```

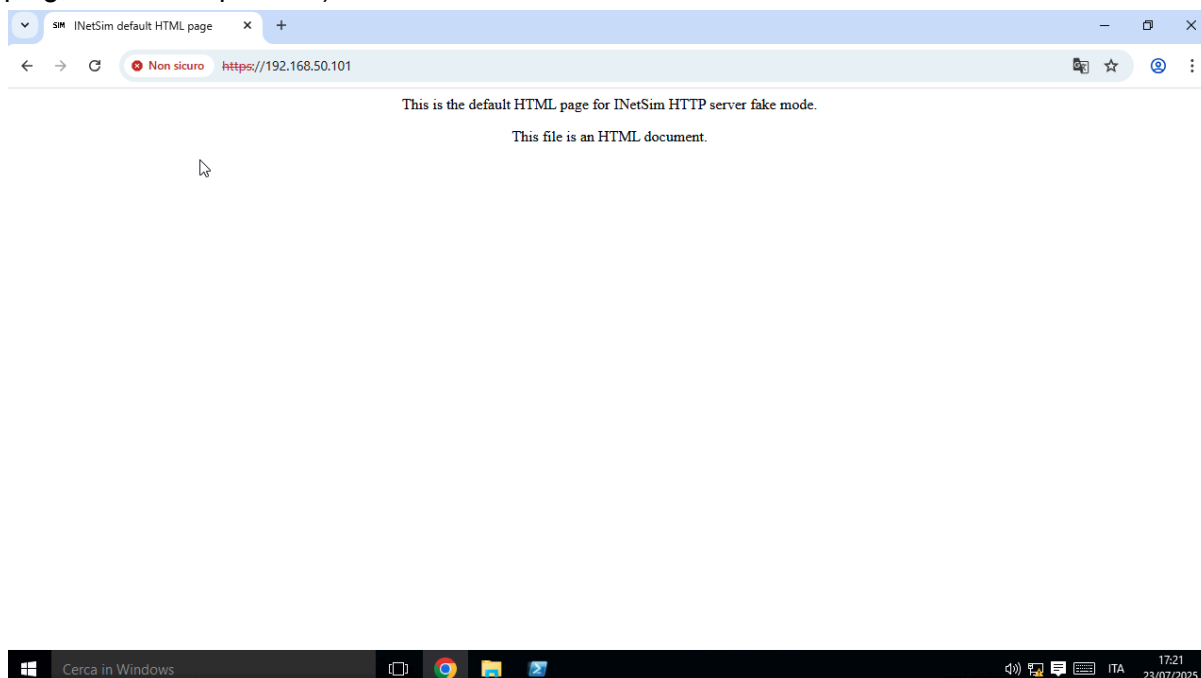
STEP 2:

Una volta avviato il servizio, posso aprire Wireshark.

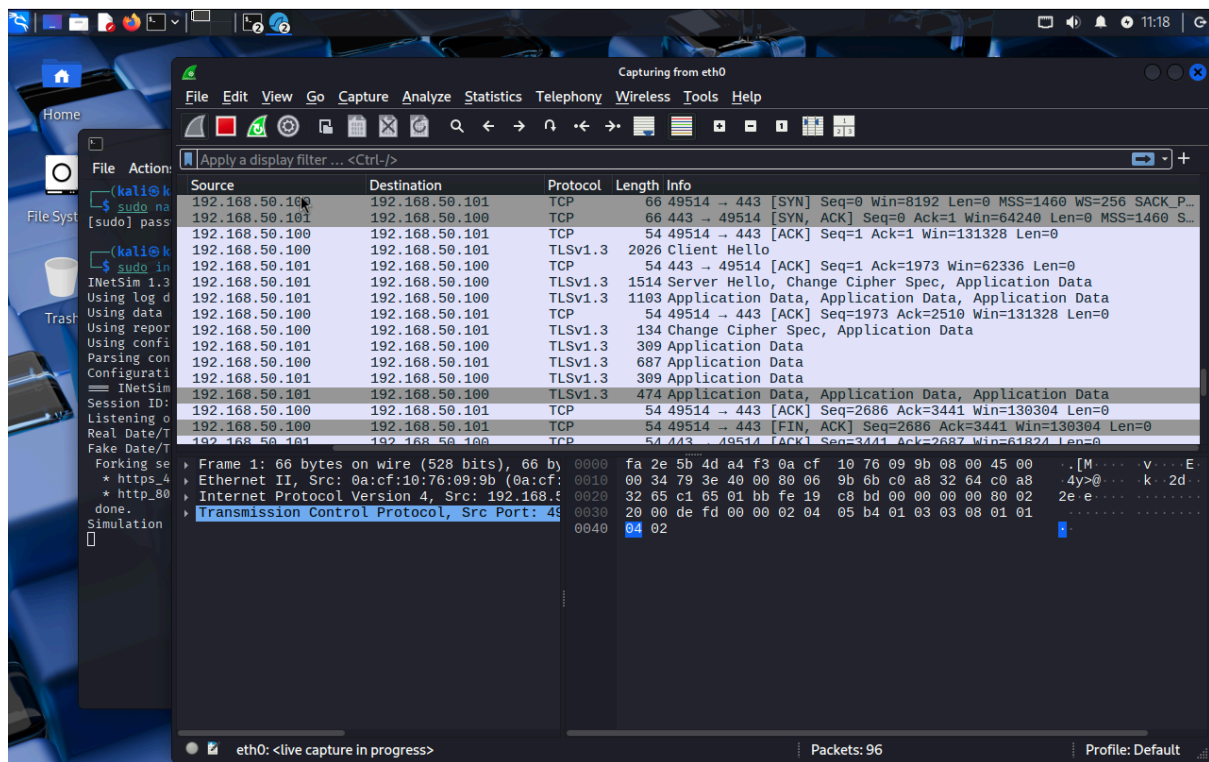


STEP 3:

Mi sposto sulla VM Windows. (È consigliabile simulare la connettività tra le macchine tramite ping, come best practice). RICERCHIAMO HTTPS://192.168.50.101

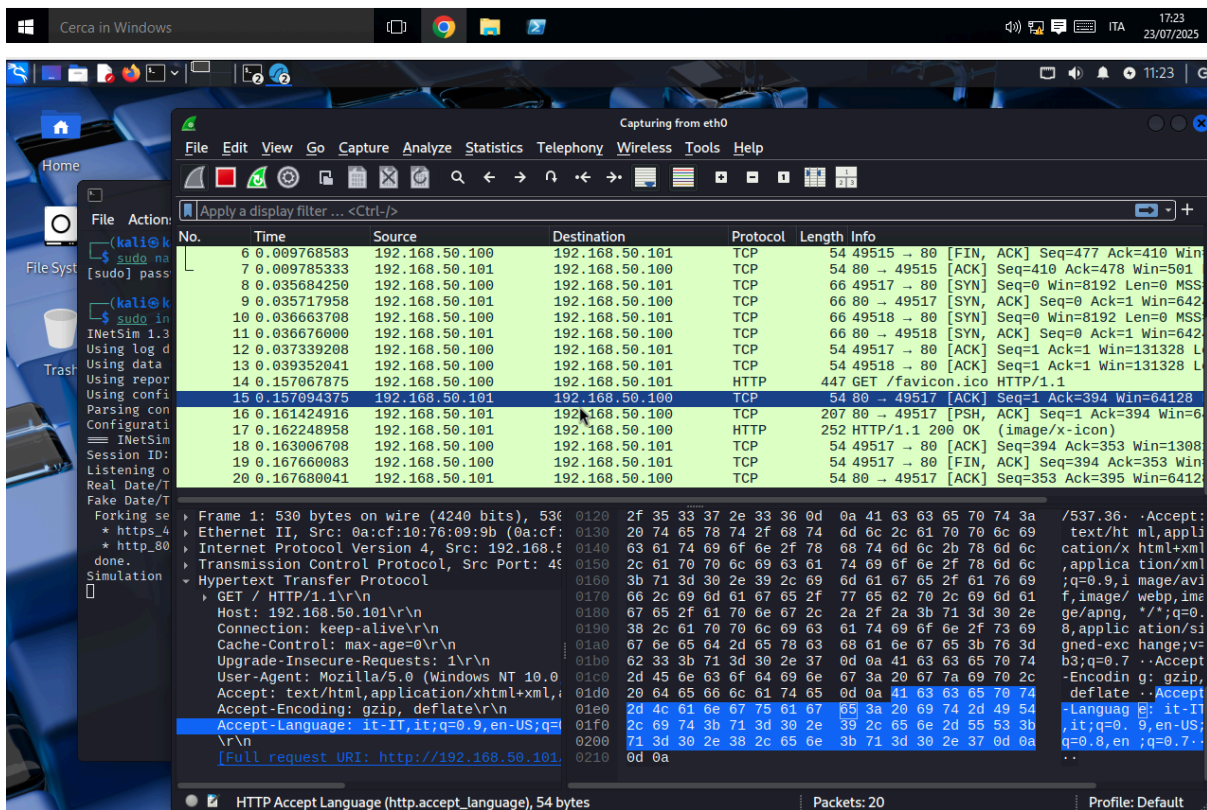
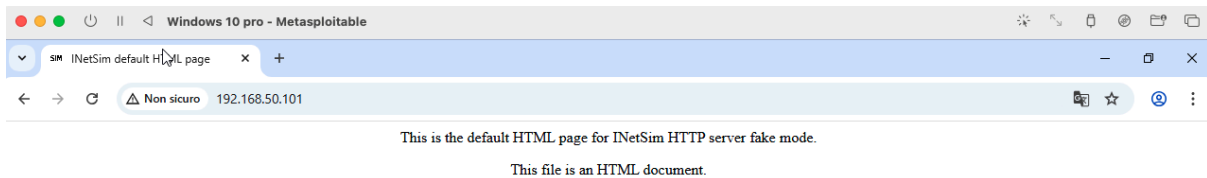


Risultato:



STEP 4:

Eseguiamo la stessa operazione in HTTP (senza necessità di ulteriori passaggi, dato che i servizi sono già stati avviati su INETSIM).



Confronto e Spiegazione delle Differenze Principali HTTP/HTTPS

Come evidenziato dalle acquisizioni Wireshark, la differenza più critica tra il traffico HTTP e quello HTTPS risiede nella crittografia dei dati.

- Nel caso della connessione HTTP: Il traffico è trasmesso in chiaro. Ciò significa che qualsiasi dato scambiato tra il client (Windows) e il server (Kali Linux), incluse le intestazioni della richiesta e l'eventuale contenuto della pagina web, è immediatamente leggibile da chiunque sia in grado di intercettare i pacchetti di rete. Questo compromette la confidenzialità e l'integrità delle informazioni, rendendo la connessione vulnerabile ad attacchi di intercettazione e manomissione.
- Nel caso della connessione HTTPS (che vedremo nella prossima analisi): Il traffico sarà incapsulato e criptato utilizzando il protocollo SSL/TLS. I dettagli della richiesta HTTP e della risposta non saranno visibili in chiaro, ma appariranno come dati criptati, rendendoli illeggibili senza la chiave di decrittografia. Questo garantisce la confidenzialità (i dati sono segreti), l'integrità (i dati non sono stati manomessi) e l'autenticazione del server (attraverso il certificato SSL/TLS).