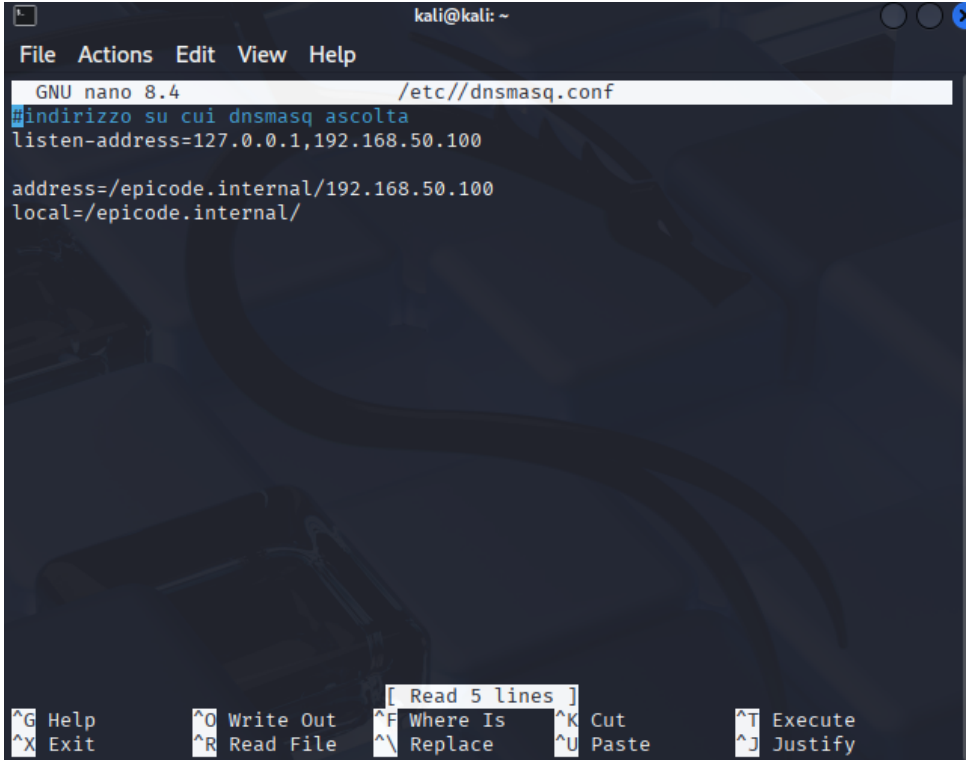


Architettura client-server

Per iniziare ho aperto le mie VM con Kali linux e Windows 10, su cui avevo già settato gli indirizzi IP, la mia Kali 192.168.50.100, la mia Windows 192.168.50.102.

Dopodiché ho settato il mio DNS utilizzando dnsmasq e andando ad aprire l'editor di testo Nano con privilegi di amministratore

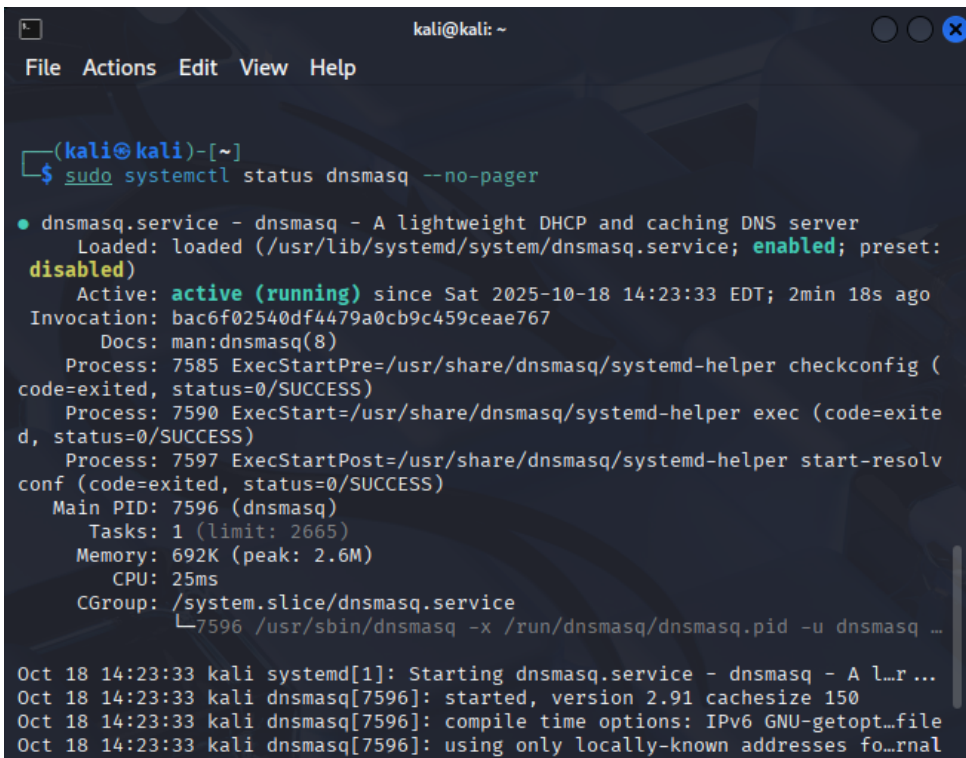


```
kali@kali: ~
File Actions Edit View Help
GNU nano 8.4 /etc/dnsmasq.conf
#indirizzo su cui dnsmasq ascolta
listen-address=127.0.0.1,192.168.50.100

address=/epicode.internal/192.168.50.100
local=/epicode.internal/

[ Read 5 lines ]
^G Help      ^O Write Out
^X Exit      ^R Read File
^F Where Is  ^K Cut
^_ Replace   ^U Paste
^T Execute   ^J Justify
```

Appena configurato l'ho abilitato



```
kali@kali: ~
File Actions Edit View Help

(kali@kali)-[~]
$ sudo systemctl status dnsmasq --no-pager

● dnsmasq.service - dnsmasq - A lightweight DHCP and caching DNS server
   Loaded: loaded (/usr/lib/systemd/system/dnsmasq.service; enabled; preset: disabled)
   Active: active (running) since Sat 2025-10-18 14:23:33 EDT; 2min 18s ago
 Invocation: bac6f02540df4479a0cb9c459ceae767
    Docs: man:dnsmasq(8)
   Process: 7585 ExecStartPre=/usr/share/dnsmasq/systemd-helper checkconfig (code=exited, status=0/SUCCESS)
   Process: 7590 ExecStart=/usr/share/dnsmasq/systemd-helper exec (code=exited, status=0/SUCCESS)
   Process: 7597 ExecStartPost=/usr/share/dnsmasq/systemd-helper start-resolvconf (code=exited, status=0/SUCCESS)
    Main PID: 7596 (dnsmasq)
      Tasks: 1 (limit: 2665)
     Memory: 692K (peak: 2.6M)
        CPU: 25ms
    CGroup: /system.slice/dnsmasq.service
            └─7596 /usr/sbin/dnsmasq -x /run/dnsmasq/dnsmasq.pid -u dnsmasq ...

Oct 18 14:23:33 kali systemd[1]: Starting dnsmasq.service - dnsmasq - A l...
Oct 18 14:23:33 kali dnsmasq[7596]: started, version 2.91 cachesize 150
Oct 18 14:23:33 kali dnsmasq[7596]: compile time options: IPv6 GNU-getopt...file
Oct 18 14:23:33 kali dnsmasq[7596]: using only locally-known addresses fo...rnal
```

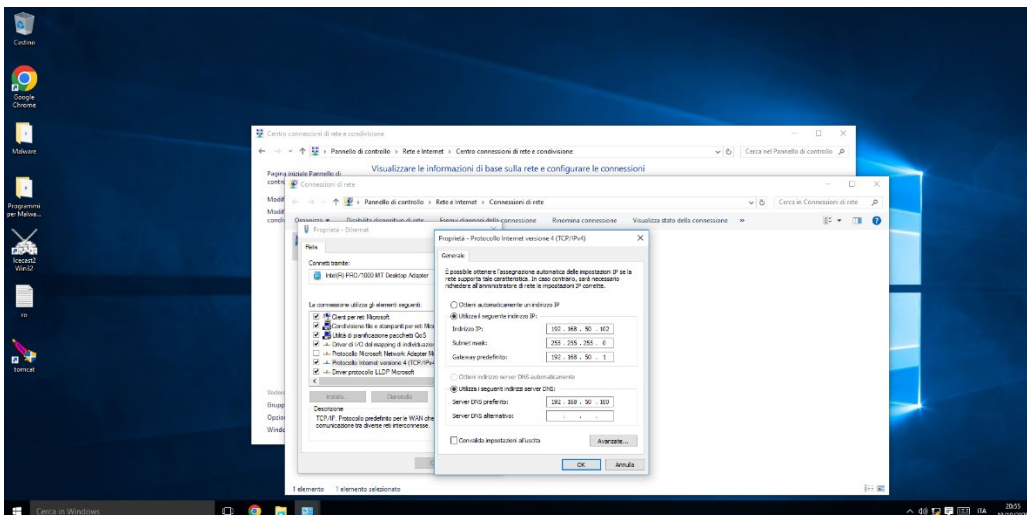
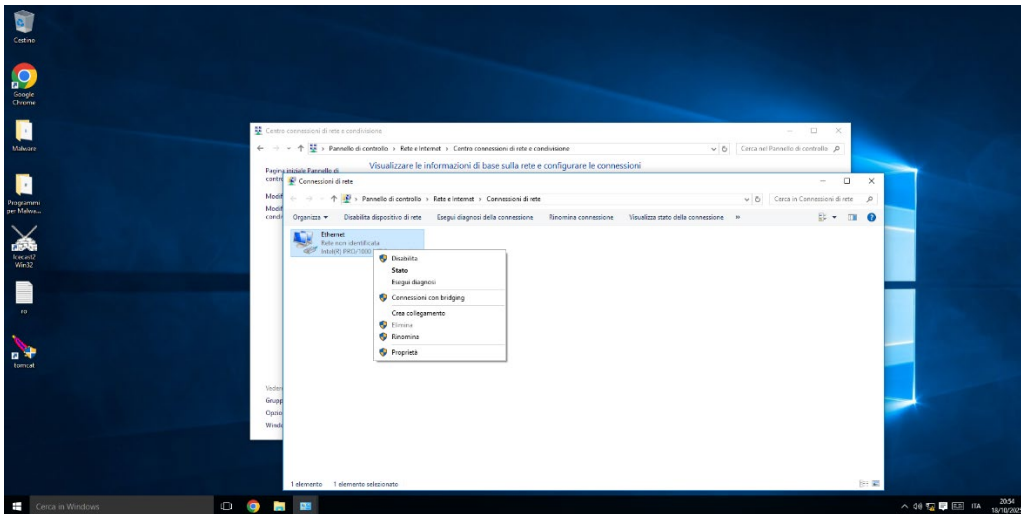
Quindi adesso avendo il DNS attivo e funzionante ci resta solo da abilitare il servizio HTTPS ed HTTP, e per farlo utilizzerò Inetsim (tool preinstallato su Kali), ma prima di abilitarlo cambio l'indirizzo in cui verrà hostato il servizio.

```
kali@kali: ~  
File Actions Edit View Help  
GNU nano 8.4 /etc/inetsim/inetsim.conf *  
#start_service discard_tcp  
#start_service discard_udp  
#start_service quotd_tcp  
#start_service quotd_udp  
#start_service chargen_tcp  
#start_service chargen_udp  
#start_service dummy_tcp  
#start_service dummy_udp  
  
#####  
# service_bind_address  
#  
# IP address to bind services to  
#  
# Syntax: service_bind_address <IP address>  
#  
Default: 192.168.50.100  
#  
#service_bind_address 0.0.0.0  
  
#####  
# service_run_as_user  
  
^G Help      ^O Write Out  ^F Where Is   ^K Cut        ^T Execute  
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify
```

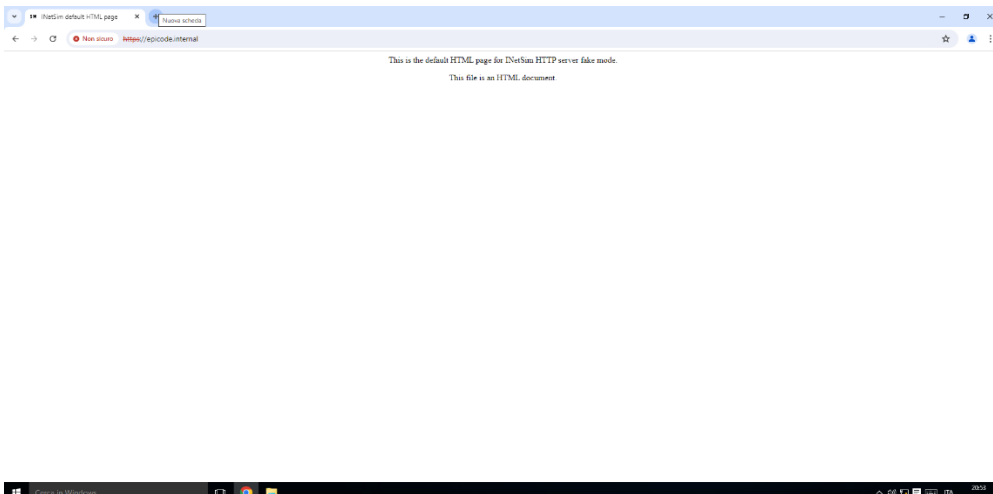
A questo punto basta che avviamo inetsim con dnsmasq.

```
kali@kali: ~  
File Actions Edit View Help  
└─$ sudo nano /etc/inetsim/dns.conf  
└─(kali@kali)-[~]  
└─$ sudo nano /etc/inetsim/inetsim.conf  
└─(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 7098) ==  
Session ID: 7098  
Listening on: 0.0.0.0  
Real Date/Time: 2025-10-18 08:49:07  
Fake Date/Time: 2025-10-18 08:49:07 (Delta: 0 seconds)  
Forking services ...  
* dns_53_tcp_udp - started (PID 7100)  
Can't locate object method "main_loop" via package "Net::DNS::Nameserver" at /usr/share/perl5/INetSim/DNS.pm line 69.  
* http_80_tcp - started (PID 7101)  
* https_443_tcp - started (PID 7102)  
done.  
Simulation running.  
└─
```

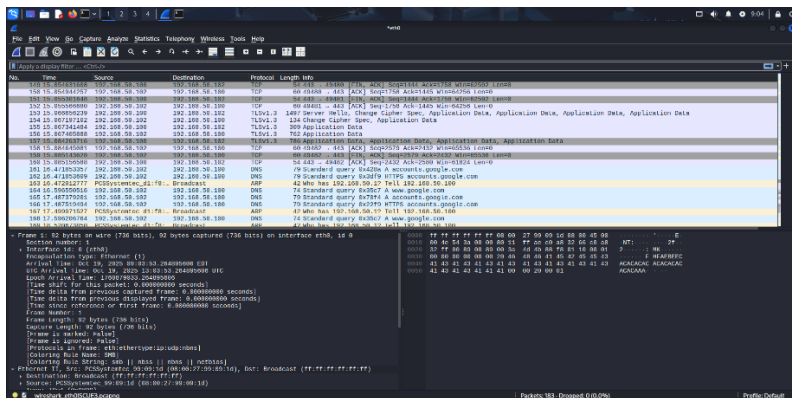
Fatto ciò, ci spostiamo su windows e andiamo a configurare il DNS aprendo il pannello di controllo, e modificando le impostazioni della scheda



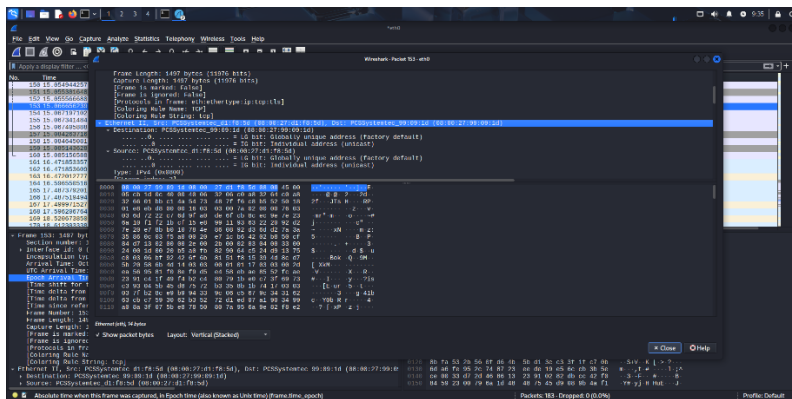
Adesso che tutto è attivo andiamo sul nostro browser e cerchiamo prima <https://epicode.internal> e poi <http://epicode.internal>



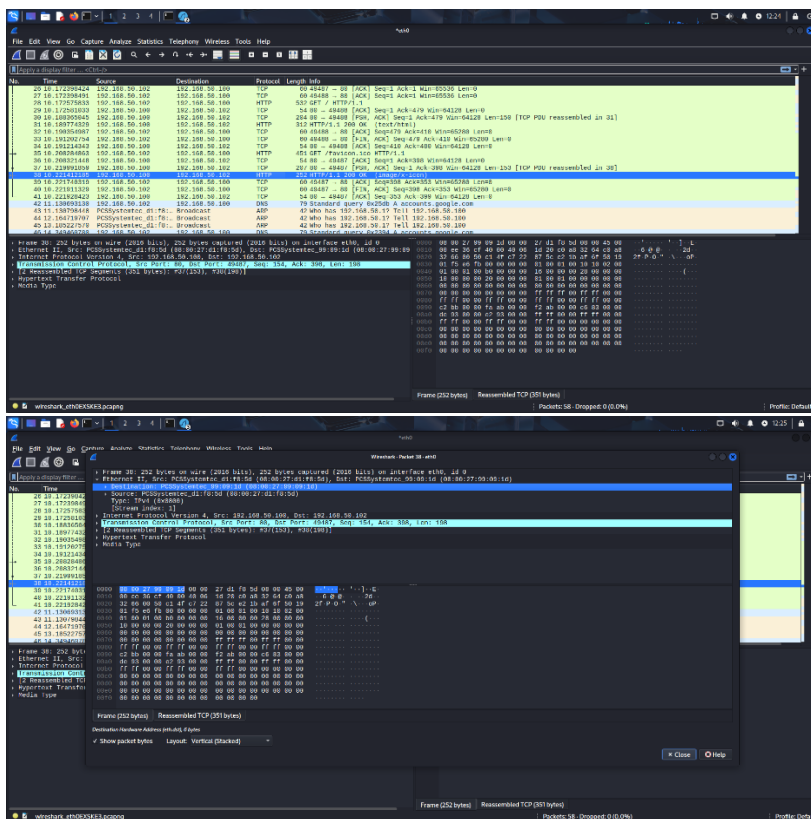
Ora dobbiamo rispostarci su Kali e fare uno sniffing con wireshark



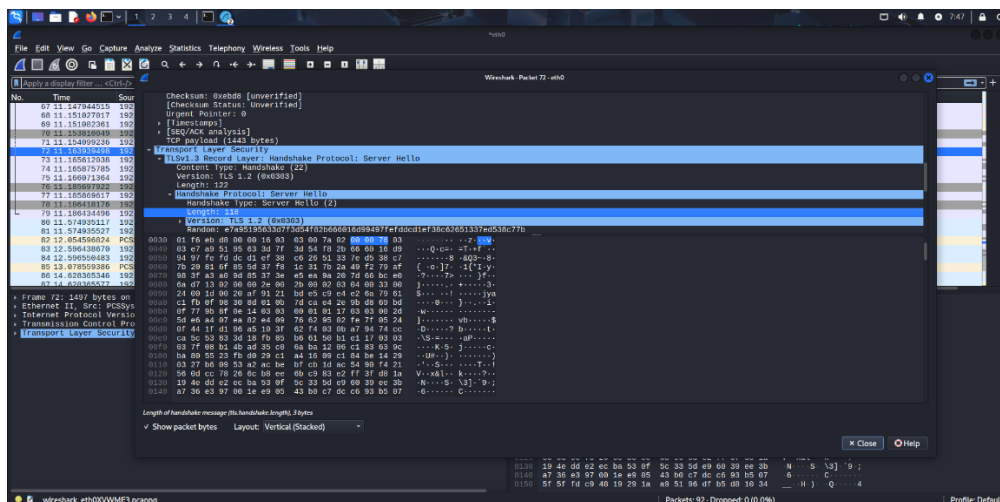
Iniziamo prima con i pacchetti https che vedremo in wireshark col protocollo TLS perché è un protocollo che protegge le comunicazioni su internet tramite crittografia. Adesso vediamo i MAC address



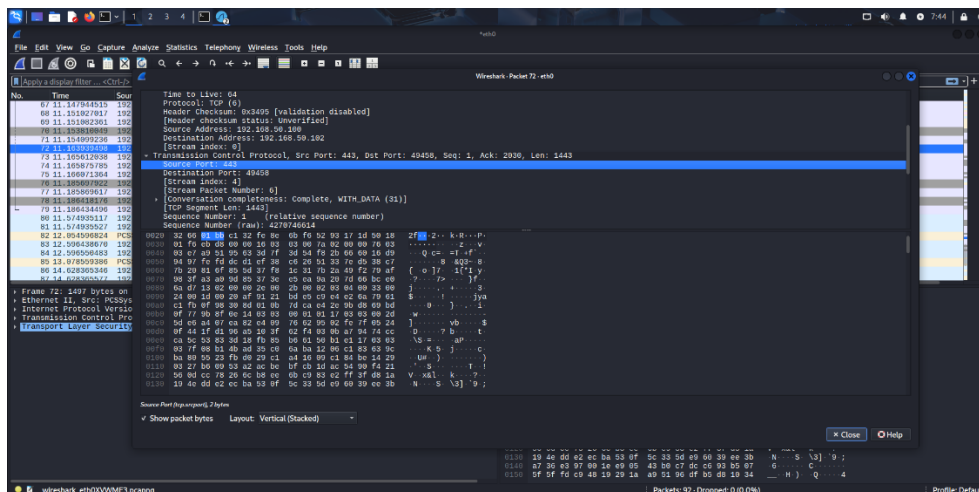
Adesso vediamo però con protocollo http



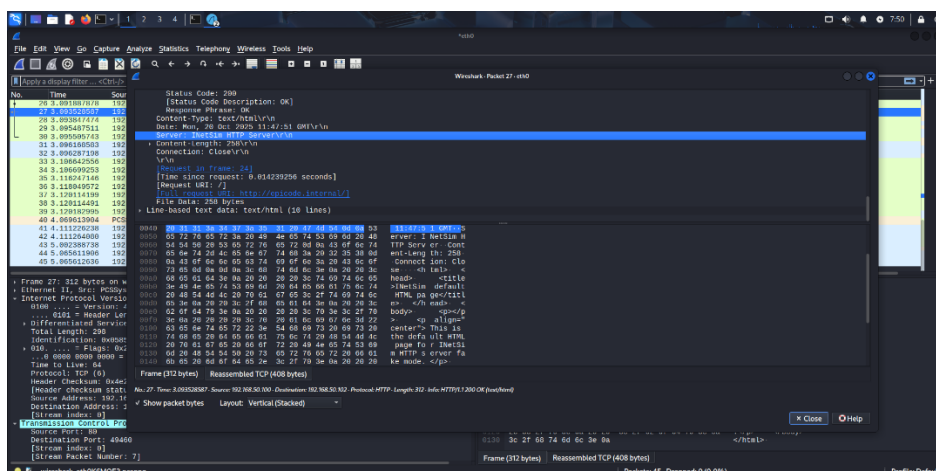
Ci sono alcune differenze tra i pacchetti in https e http, nei pacchetti in https non si legge quasi nulla se non poche informazioni come handshake protocol

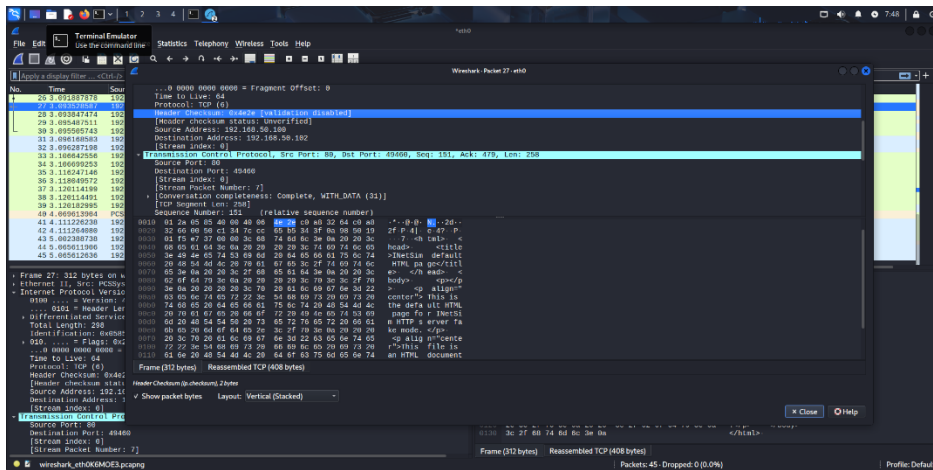


E anche la porta su cui sta ascoltando che in questo caso sarà la 443



Nell'http possiamo vedere anche il sito che il client ha visitato nonché la porta su cui è in ascolto





Conclusione

Abbiamo configurato un servizio DNS e attivato un servizio HTTPS e http poi abbiamo sniffato con wireshark i pacchetti tra client e server ed analizzati, visto i MAC Address e alcune differenze presenti tra i pacchetti in http e HTTPS.