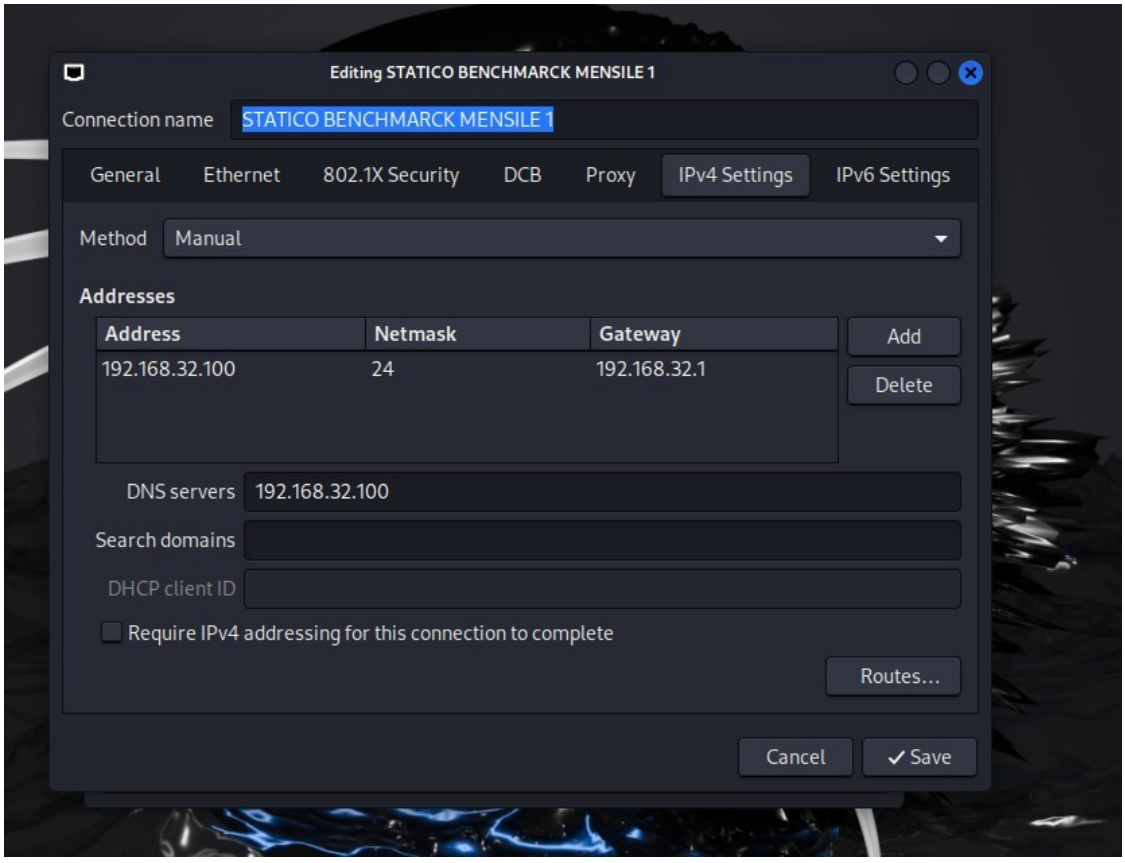
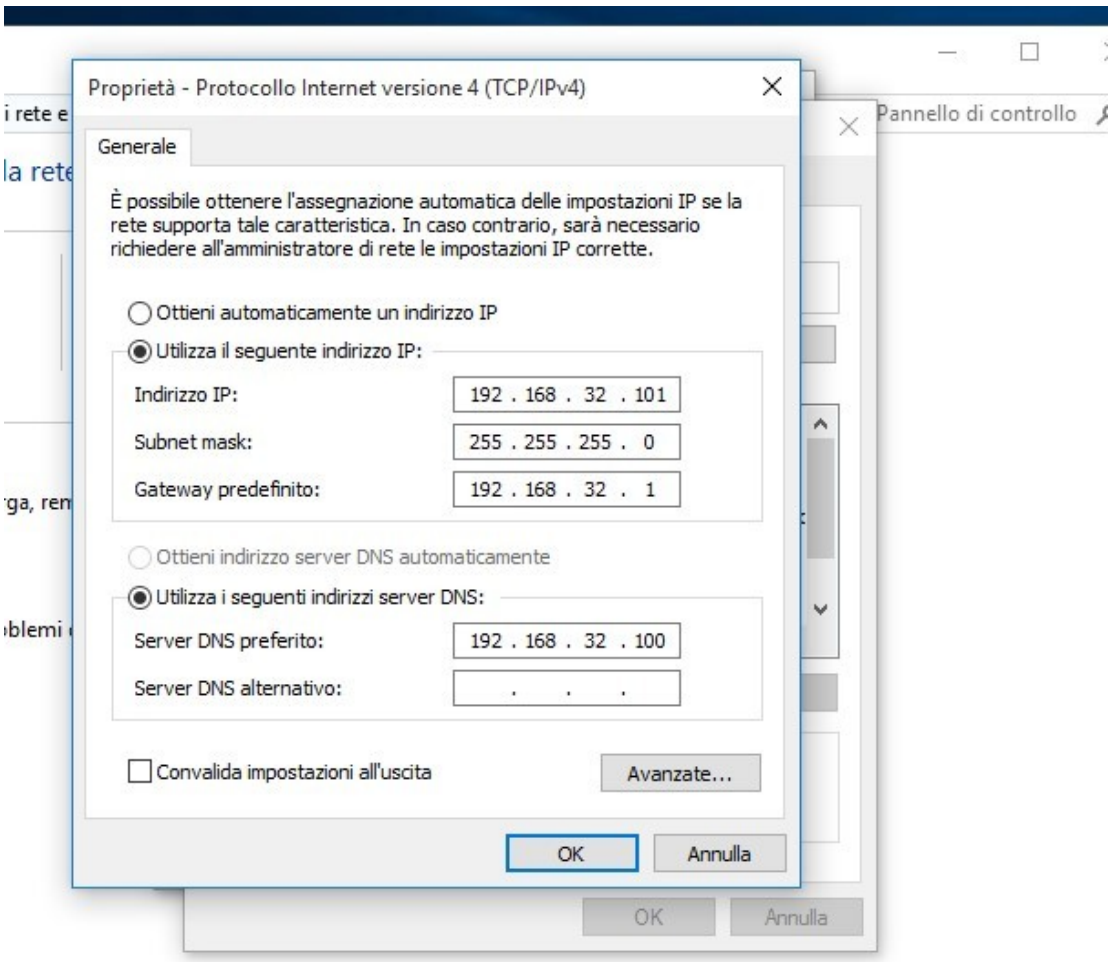
ESERCITAZIONE DI FINE MODULO M1W4

STUDENTE: Gatti Francesco

1. Ho impostato nuovo indirizzo IP statico su Kali Linux che utilizzeremo come server HTTP- HTTPS - DNS



2. Successivamente ho configurato la macchina Windows che utilizzeremo come client specificando:
   - l’indirizzo IP sorgente
   - subnetmask
   - gateway
   - DNS preferito



3. Ho eseguito il controllo per gli aggiornamenti del software in modo tale da avere le ultime versioni a disposizione con il seguente comando:

4.Successivamente ho configurato il DNS tramite comando INETSIM

sudo nano /etc/inetsim/inetsim.conf

```
##########################################
# service_bind_address
#
# IP address to bind services to
#
# Syntax: service_bind_address <IP address>
#
# Default: 127.0.0.1
#
service_bind_address 192.168.32.100
```

```
##########################################################
# Service DNS
##########################################################

########################################
# dns_bind_port
#
# Port number to bind DNS service to
#
# Syntax: dns_bind_port <port number>
#
# Default: 53
#
dns_bind_port 53


########################################
# dns_default_ip
#
# Default IP address to return with DNS replies
#
# Syntax: dns_default_ip <IP address>
#
# Default: 127.0.0.1
#
dns_default_ip 192.168.32.100
```

```
##########################################
# dns_default_domainname
#
# Default domain name to return with DNS replies
#
# Syntax: dns_default_domainname <domain name>
#
# Default: inetsim.org
#
dns_default_domainname epicode.internal
```

5. Ho installato e configurato Apache 2 per la gestione del HTTP/HTTPS

```
┌──(kali㉿kali)-[~]
└─$ sudo apt install apache2
[sudo] password for kali:
apache2 is already the newest version (2.4.62-3).
apache2 set to manually installed.
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 1857
```

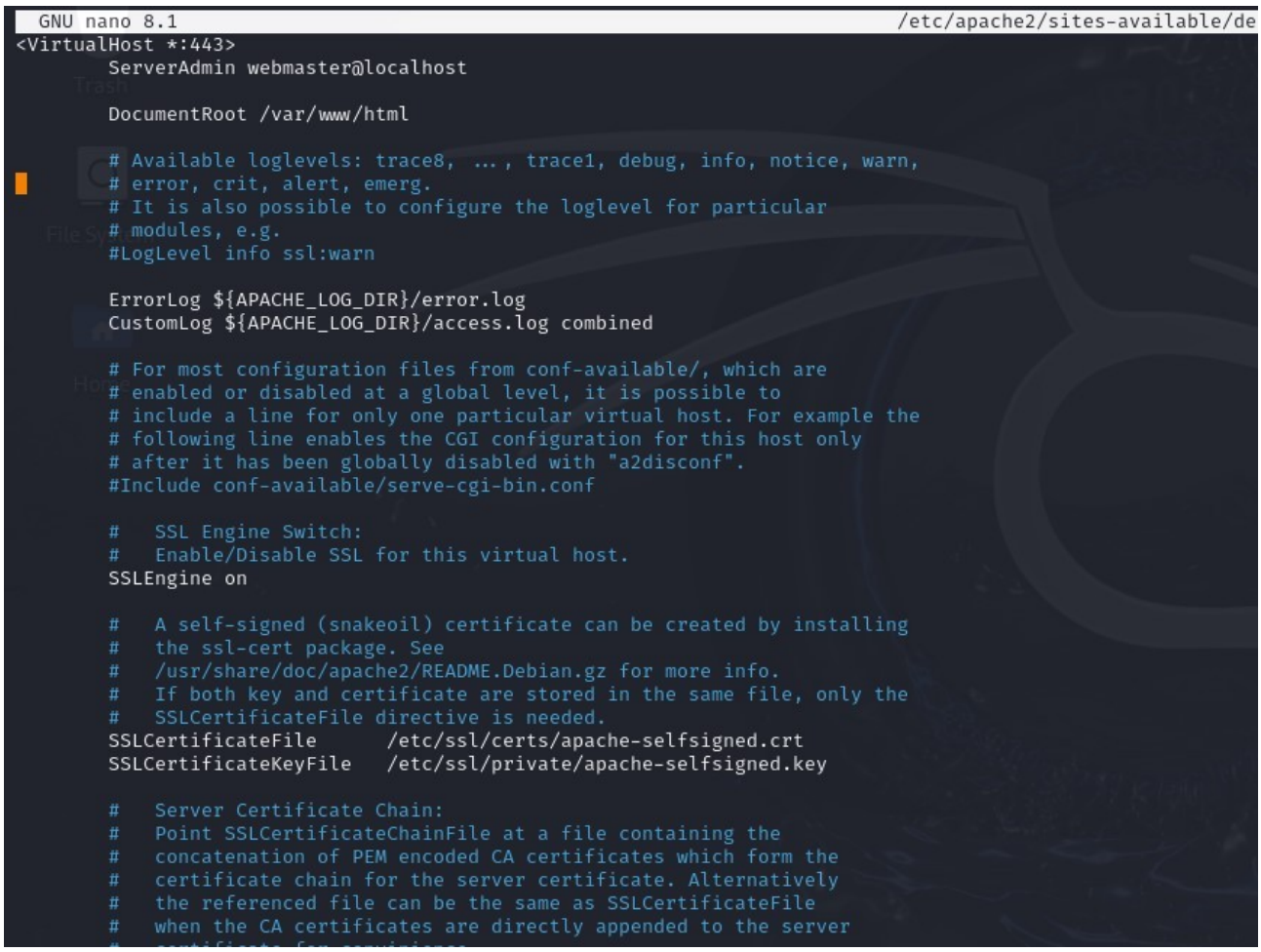
6. Abilito modulo SSL

```
┌──(kali㉿kali)-[~]
└─$ sudo a2enmod ssl
[sudo] password for kali:
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Module socache_shmcb already enabled
Module ssl already enabled

┌──(kali㉿kali)-[~]
└─$
```

7. Creo certificato privato HTTPS

```
┌──(kali㉿kali)-[~]
└─$ sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 \
-keyout /etc/ssl/private/apache-selfsigned.key \
-out /etc/ssl/certs/apache-selfsigned.crt

...+...+.+..........+.........+.+..+.+..+.........+...+.......+......+.....+....+........+.+.....+.+.....+.........+...+...+...+..+.........+..+...+.......+.....+......+.+..
..+...+.........+...+......+......+.....+......+...+....+..+.+..+......++++++++++++++++++++++++++++++++++++++++++++*....+.........+.+......+........+......+......+...+....+..+.++++++++++++++++++++
++++++++++++++++*...+..+.+..........+.+..+.................+..+...+.+...+..+.+...+.........+.....+......+.................+....+.........+..+...+....+...+.....+...+.....+.....+..+....
.........+..+...++++++
.............++++++++++++++++++++++++++++++++++++++++++*.......+...+...+..............+....+...+...+..+....++++++++++++++++++++++++++++++++++++*..+...+..............+...+.........+..+...+.
..+....+.....+.....+......+..................+..............+..+...+.+..................+.........+...+..+......+.......+..+.....+...+....+..+.....+.....+.....+.....+..+.....
+.+.....+..............+......+.........+.+........+.+.....................+.+..............+..............+.....+......+....+............+.....+....+........+...+...+.+.....+.++++++
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
```

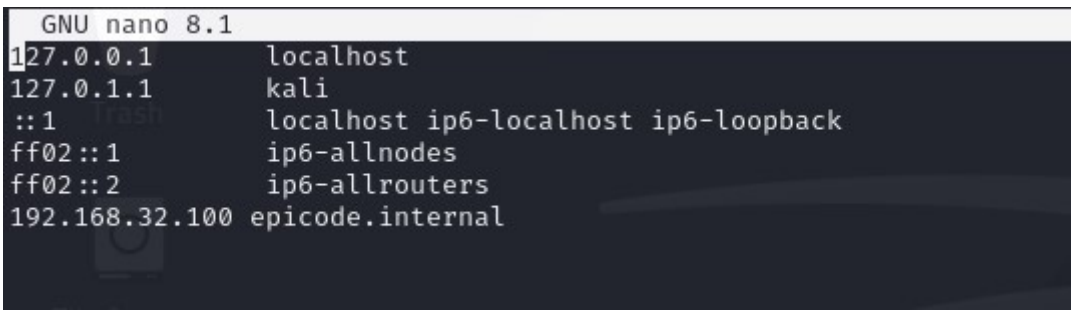
8. Configuro Apache con il seguente comando ed aggiungo il path dei file relativi al certificato e la chiave, precedentemente specificati nel comando



9. Abilito SSL tramite questa stringa di comando

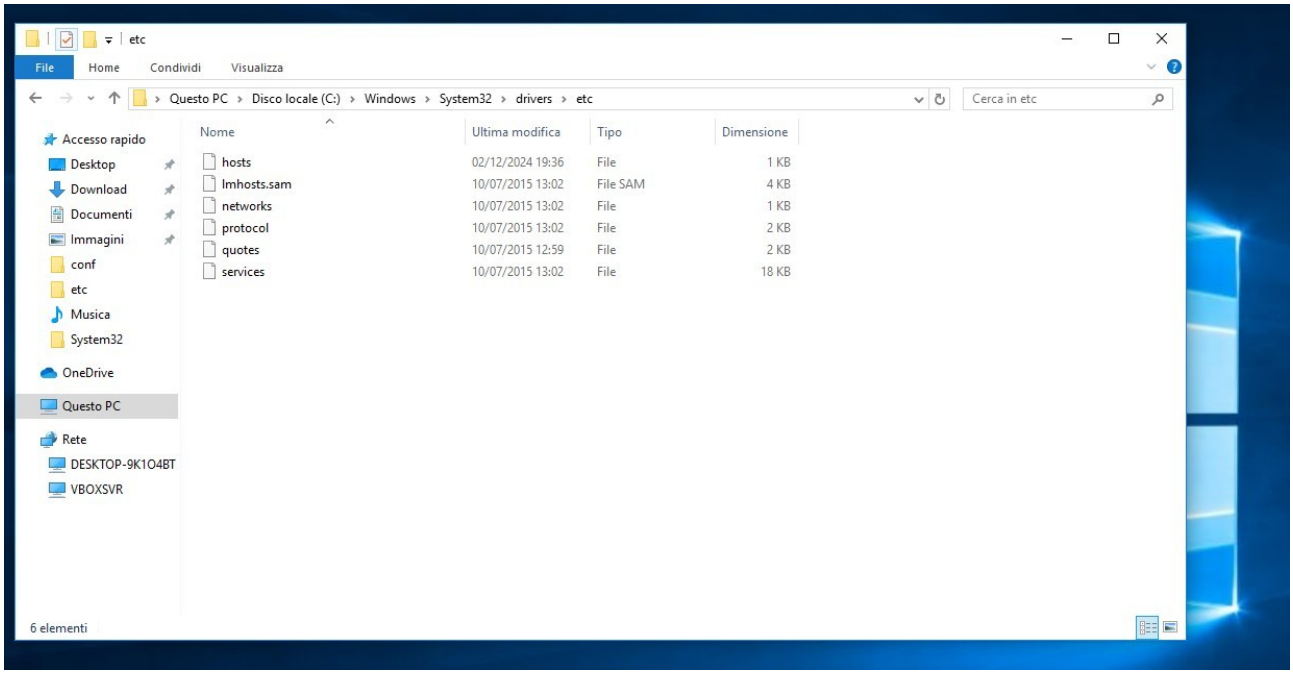
sudo a2nsite default-ssl
e riavvio Apache2 per salvare le modifiche, con il comando
sudo systemctl reload apache2

10. Come ultimo passaggio per la configurazione HTTPS inserisco IP e dominio del Server nel file hosts

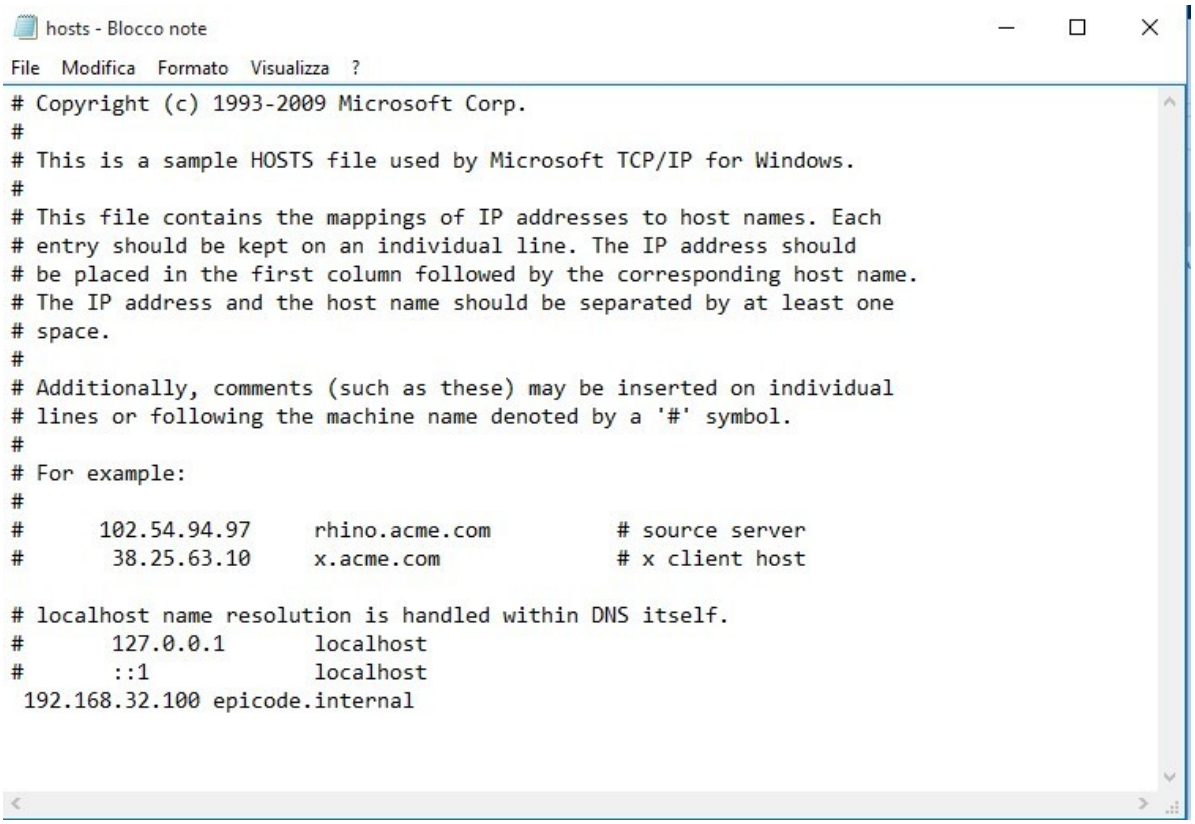


Successivamente è stato necessario eseguire delle configurazioni anche sulla parte client

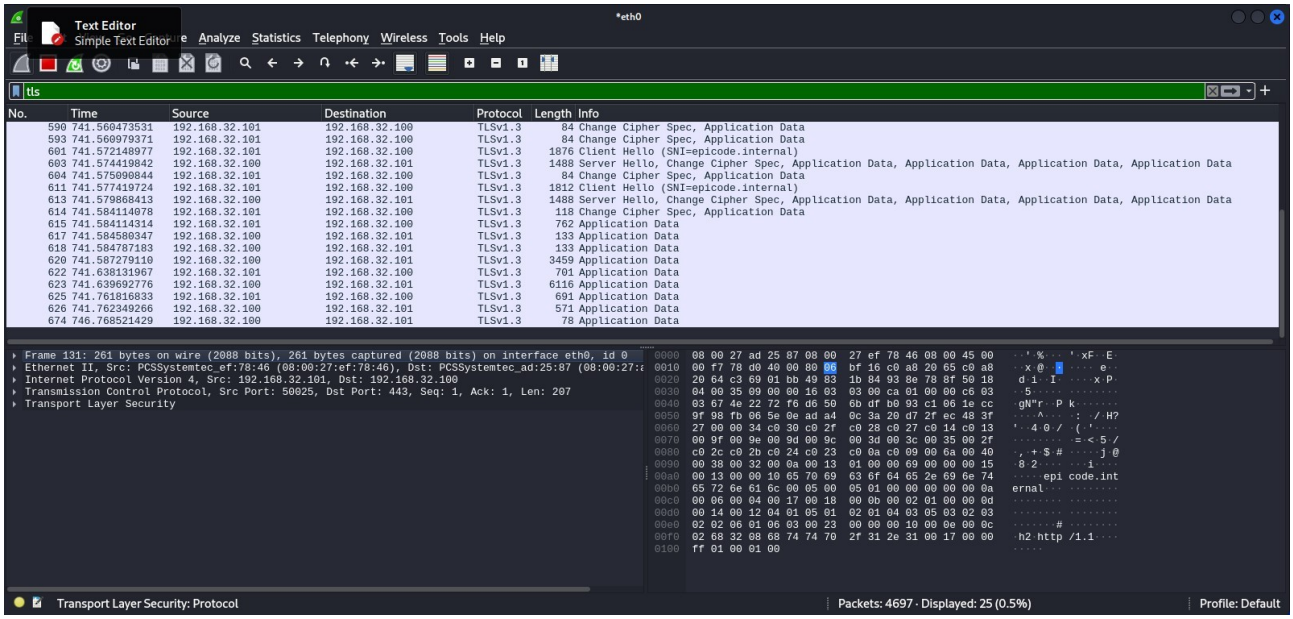
11.

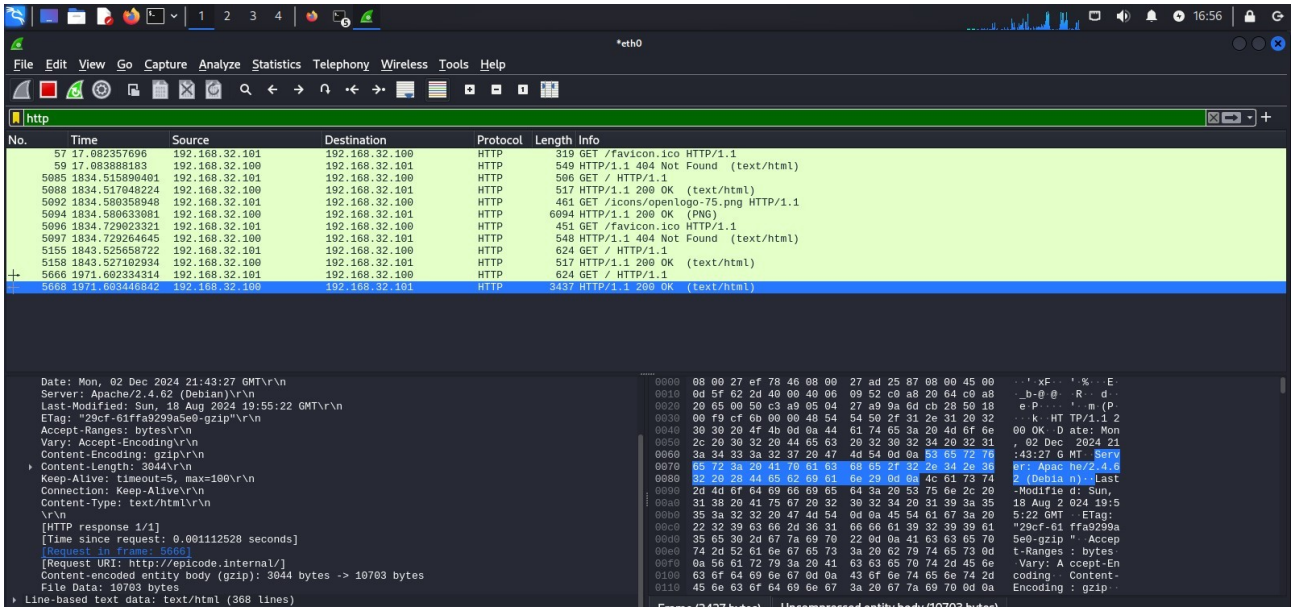


12. Ho aperto il file hosts con diritti di amministratore e ho inserito l'indirizzo **192.168.32.100** specificando come hostname **epicode.internal**



13. Ho intercettato tramite apposito software Wireshark il traffico dati abilitando i filtri TLS e HTTP





Tramite queste due immagini relative al traffico dati su Wireshark possiamo notare come i dati intercettati come HTTPS sono crittografati, mentre quelli intercettati in HTTP sono in chiaro.