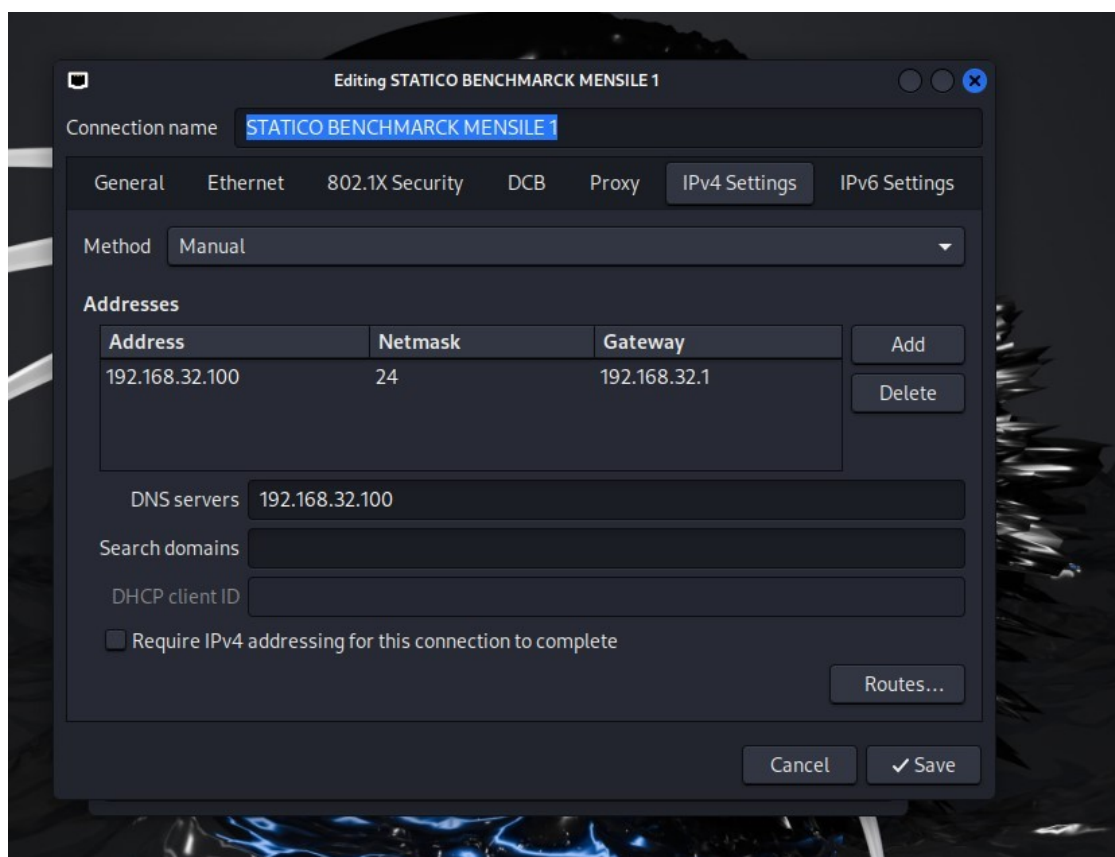


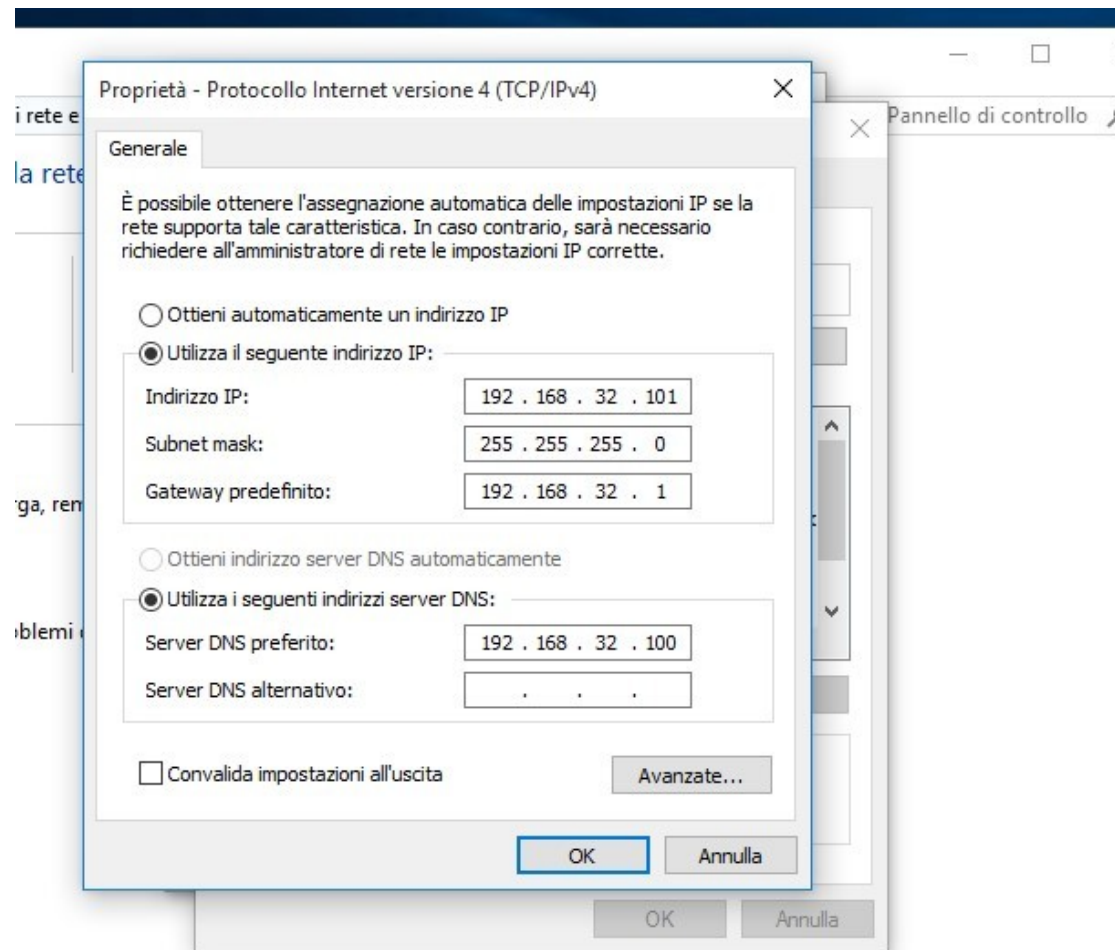
# ESERCITAZIONE DI FINE MODULO M1W4

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:

```
(kali@kali)-[~]  
$ sudo apt update
```

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

[illegible]

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

```
GNU nano 8.1 /etc/apache2/sites-available/de
<VirtualHost *:443>
    ServerAdmin webmaster@localhost

    DocumentRoot /var/www/html

    # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
    # error, crit, alert, emerg.
    # It is also possible to configure the loglevel for particular
    # modules, e.g.
    #LogLevel info ssl:warn

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

    # For most configuration files from conf-available/, which are
    # enabled or disabled at a global level, it is possible to
    # include a line for only one particular virtual host. For example the
    # following line enables the CGI configuration for this host only
    # after it has been globally disabled with "a2disconf".
    #Include conf-available/serve-cgi-bin.conf

    # SSL Engine Switch:
    # Enable/Disable SSL for this virtual host.
    SSLEngine on

    # A self-signed (snakeoil) certificate can be created by installing
    # the ssl-cert package. See
    # /usr/share/doc/apache2/README.Debian.gz for more info.
    # If both key and certificate are stored in the same file, only the
    # SSLCertificateFile directive is needed.
    SSLCertificateFile /etc/ssl/certs/apache-selfsigned.crt
    SSLCertificateKeyFile /etc/ssl/private/apache-selfsigned.key

    # Server Certificate Chain:
    # Point SSLCertificateChainFile at a file containing the
    # concatenation of PEM encoded CA certificates which form the
    # certificate chain for the server certificate. Alternatively
    # the referenced file can be the same as SSLCertificateFile
    # when the CA certificates are directly appended to the server
    # certificate. For configurations that want to embed certificates into
```

9. Abilito SSL tramite questa stringa di comando

**sudo a2ensite default-ssl**

e riavvio Apache2 per salvare le modifiche, con il comando

**sudo systemctl reload apache2**

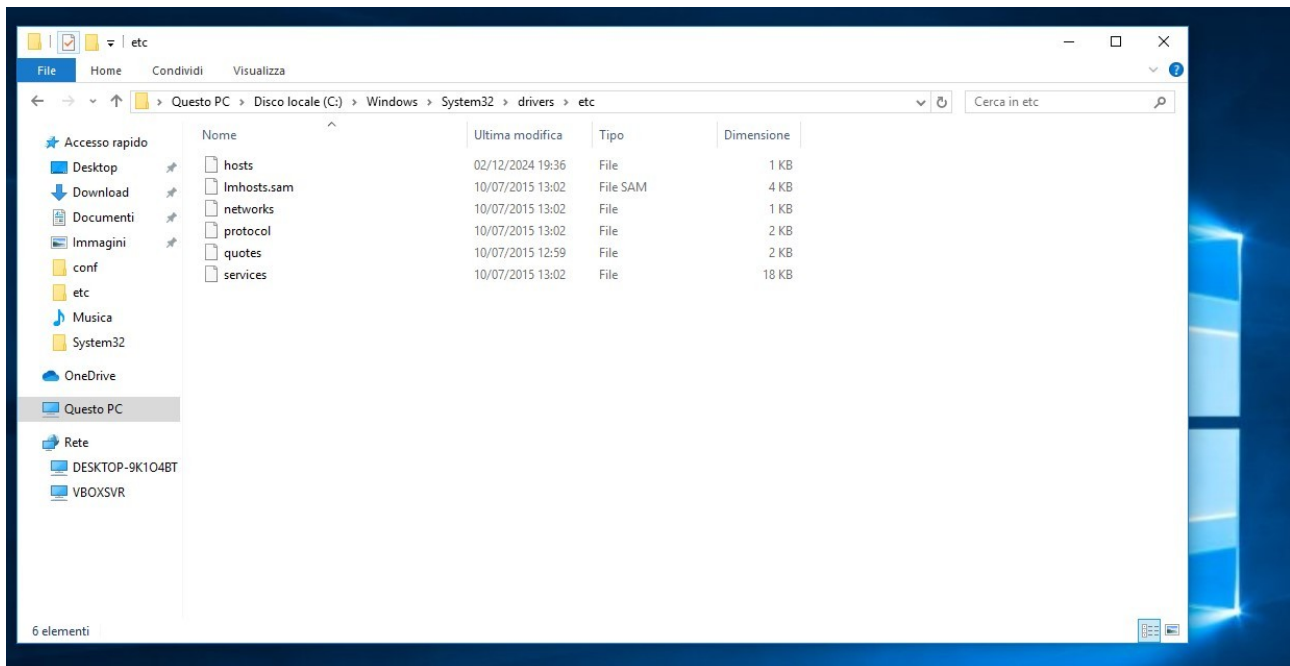
10. Come ultimo passaggio per la configurazione HTTPS inserisco IP e dominio del Server nel file hosts

```
GNU nano 8.1
127.0.0.1 localhost
127.0.1.1 kali
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
192.168.32.100 epicode.internal
```



**Successivamente è stato necessario eseguire delle configurazioni anche sulla parte client**

11.

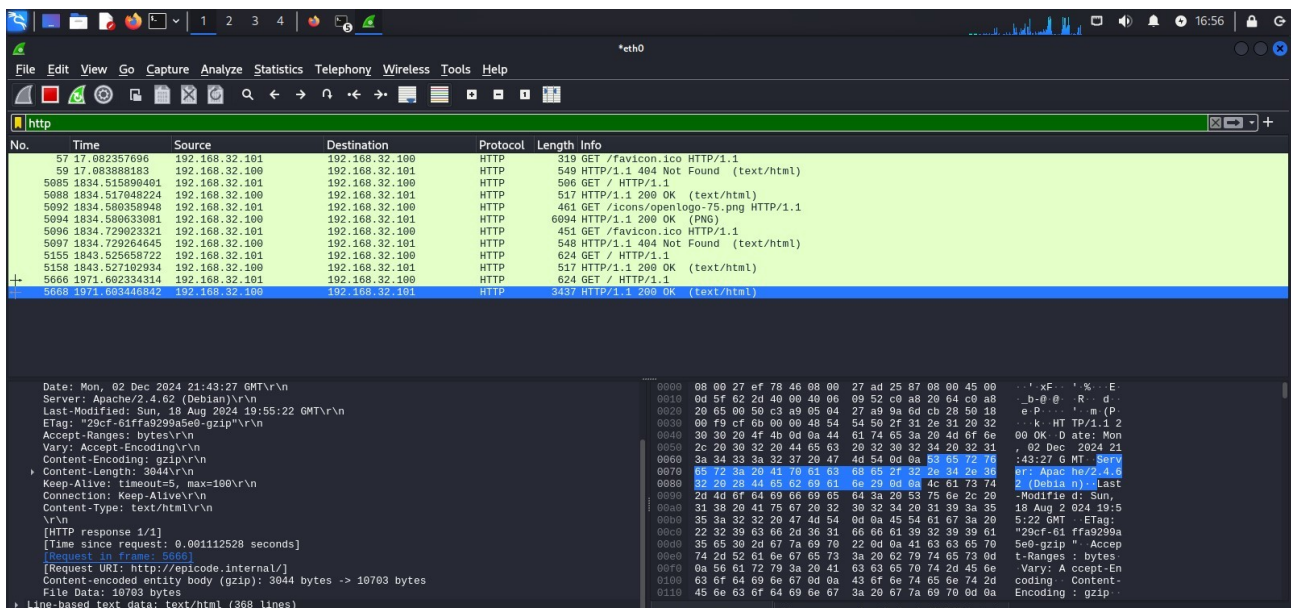
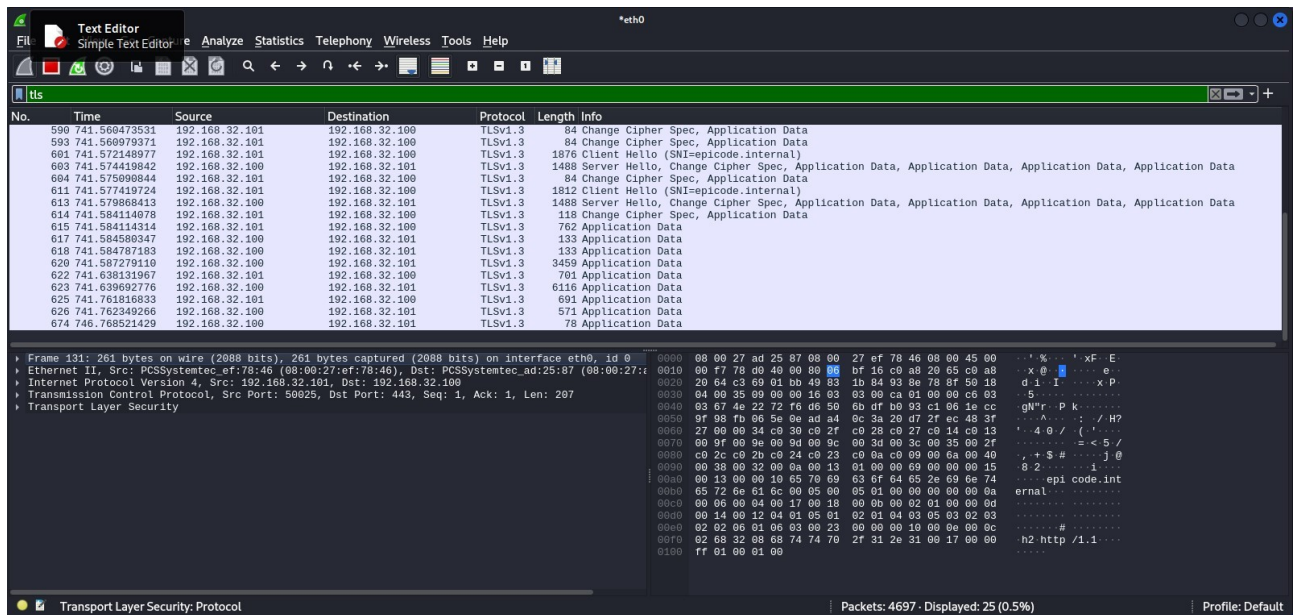


12. Ho aperto il file hosts con diritti di amministratore e ho inserito l'indirizzo **192.168.32.100** specificando come hostname **epicode.internal**

The screenshot shows a Notepad window titled 'hosts - Blocco note'. The menu bar includes 'File', 'Modifica', 'Formato', 'Visualizza', and '?'. The text content is as follows:

```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com           # source server
#       38.25.63.10      x.acme.com               # x client host
#
# localhost name resolution is handled within DNS itself.
#       127.0.0.1        localhost
#       ::1              localhost
192.168.32.100 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.