

TRACCIA:

Nell'esercizio di oggi metteremo insieme le competenze acquisite finora. Lo studente verrà valutato sulla base della risoluzione al problema seguente.

Requisiti e servizi:

-Kali Linux IP 192.168.32.100

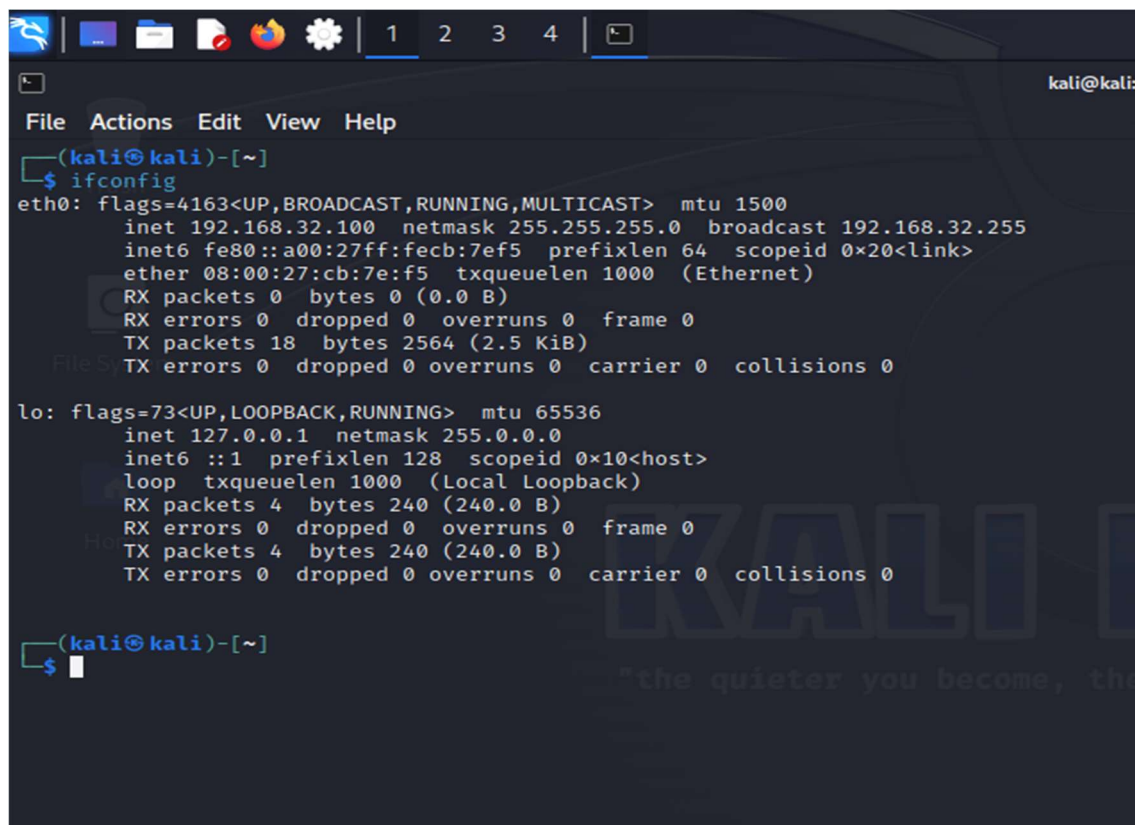
-Windows 7 IP 192.168.32.101

-HTTPS server: attivo-Servizio DNS per risoluzione nomi di dominio: attivo

Simulare, in ambiente di laboratorio virtuale, un'architettura client server in cui un client con indirizzo 192.168.32.101 (Windows 7) richiede tramite web browser una risorsa all'hostname epicode.internal che risponde all'indirizzo 192.168.32.100 (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.

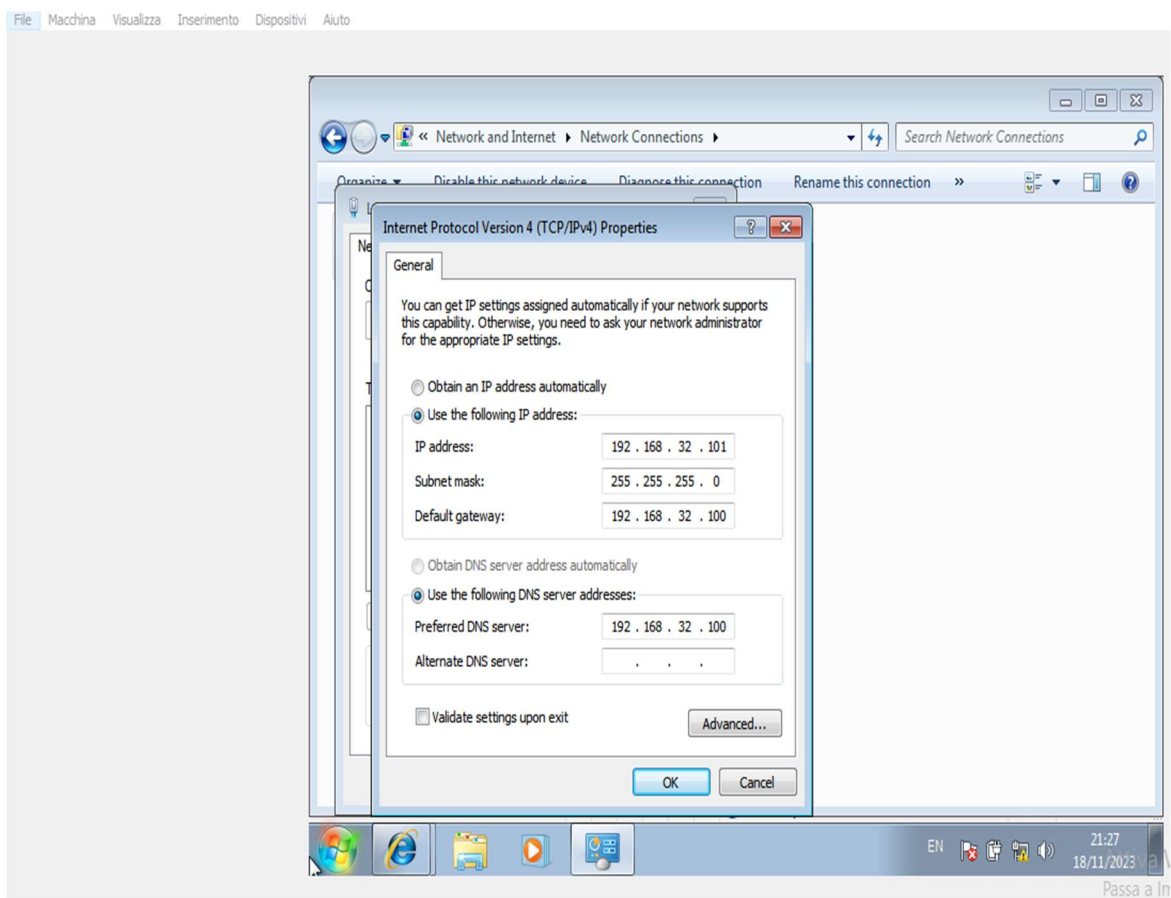
1. Usando il lab. Virtuale Virtual box, apro le due macchine: Kali linux e Windows 7.
2. Configuro gli indirizzi ip sulle due macchine virtuali come da consegna:



```
(kali@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.32.100 netmask 255.255.255.0 broadcast 192.168.32.255
    inet6 fe80::a00:27ff:feeb:7ef5 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:cb:7e:f5 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 18 bytes 2564 (2.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

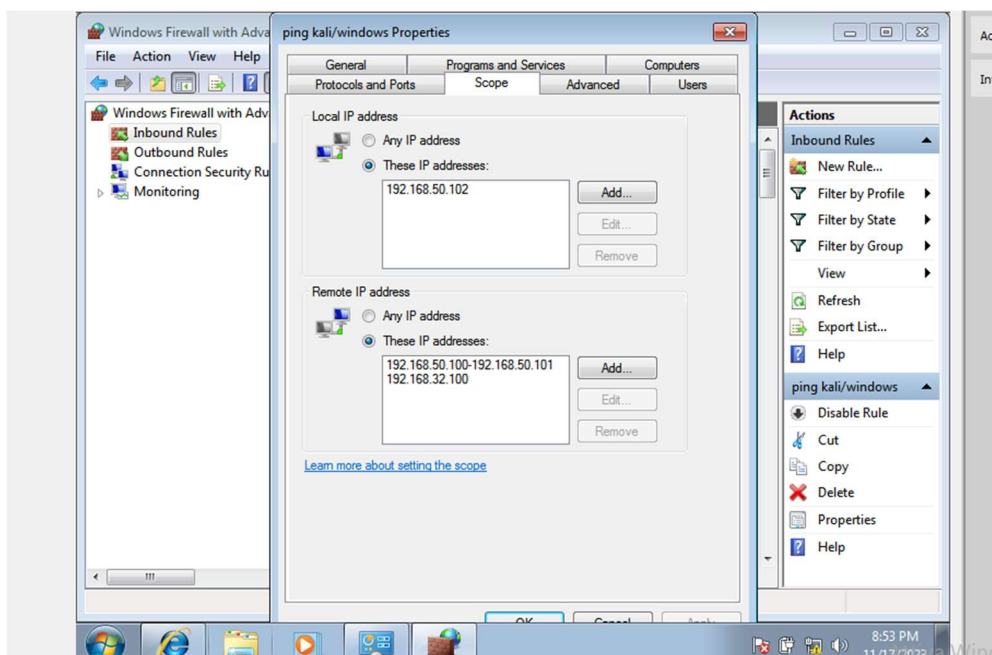
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4 bytes 240 (240.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 240 (240.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali@kali)-[~]
$
```



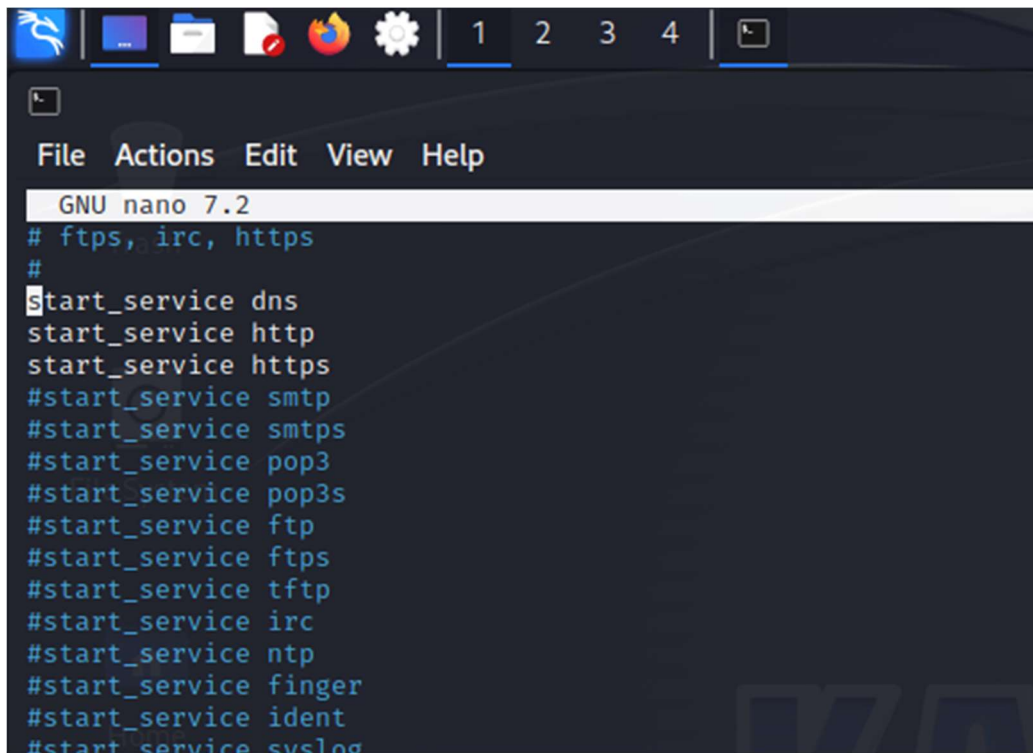
Nota: nello screen è presente anche la configurazione del Dns che ho effettuato dopo la configurazione del Dns su inetsim della macchina kali.

3. Modifico la policy del Firewall di windows 7 per permettere il traffico di rete tra le due macchine.



4. Utilizzo il software Inetsim su Kali simulando una rete virtuale e servizi come il DNS, HTTP, HTTPS per risolvere la traccia.

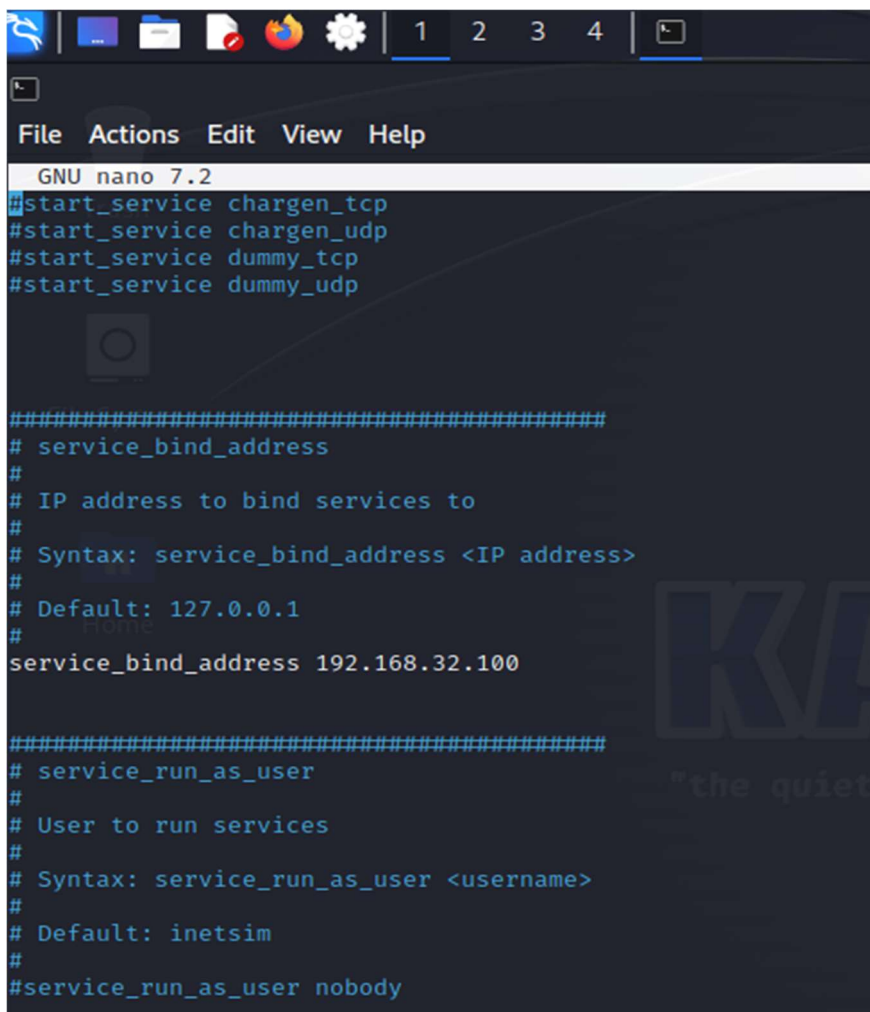
Procedo configurando Inetsim in questo modo:



The screenshot shows a terminal window with a dark background and light blue text. The window title is "GNU nano 7.2". The menu bar at the top includes "File", "Actions", "Edit", "View", and "Help". The terminal content shows the following lines of text:

```
# ftps, irc, https
#
start_service dns
start_service http
start_service https
#start_service smtp
#start_service smtps
#start_service pop3
#start_service pop3s
#start_service ftp
#start_service ftps
#start_service tftp
#start_service irc
#start_service ntp
#start_service finger
#start_service ident
#start_service syslog
```

Attivo i servizi di cui abbiamo bisogno: DNS, HTTP, HTTPS.



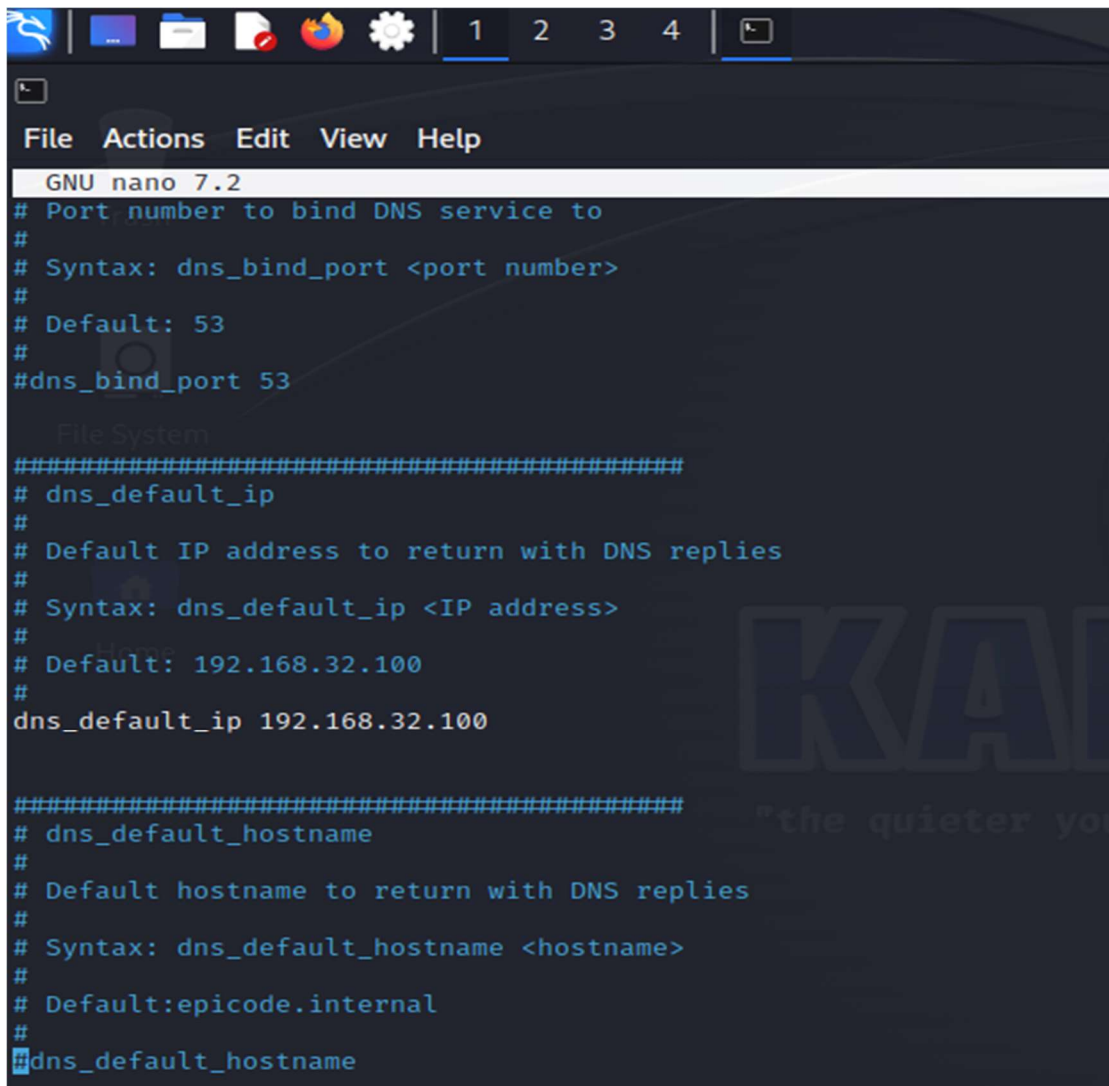
The screenshot shows a Kali Linux desktop environment. At the top, there is a taskbar with icons for a web browser, file manager, terminal, and other applications. Below the taskbar, a terminal window is open, displaying the GNU nano 7.2 text editor. The editor is editing a file, likely a service configuration file, and the content is as follows:

```
GNU nano 7.2
#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: 127.0.0.1
#
service_bind_address 192.168.32.100

#####
# service_run_as_user
#
# User to run services
#
# Syntax: service_run_as_user <username>
#
# Default: inetsim
#
#service_run_as_user nobody
```

Procedo ad inserire il bind_address che corrisponde all'indirizzo ip della macchina kali che gestisce la simulazione inetsim in ascolto.



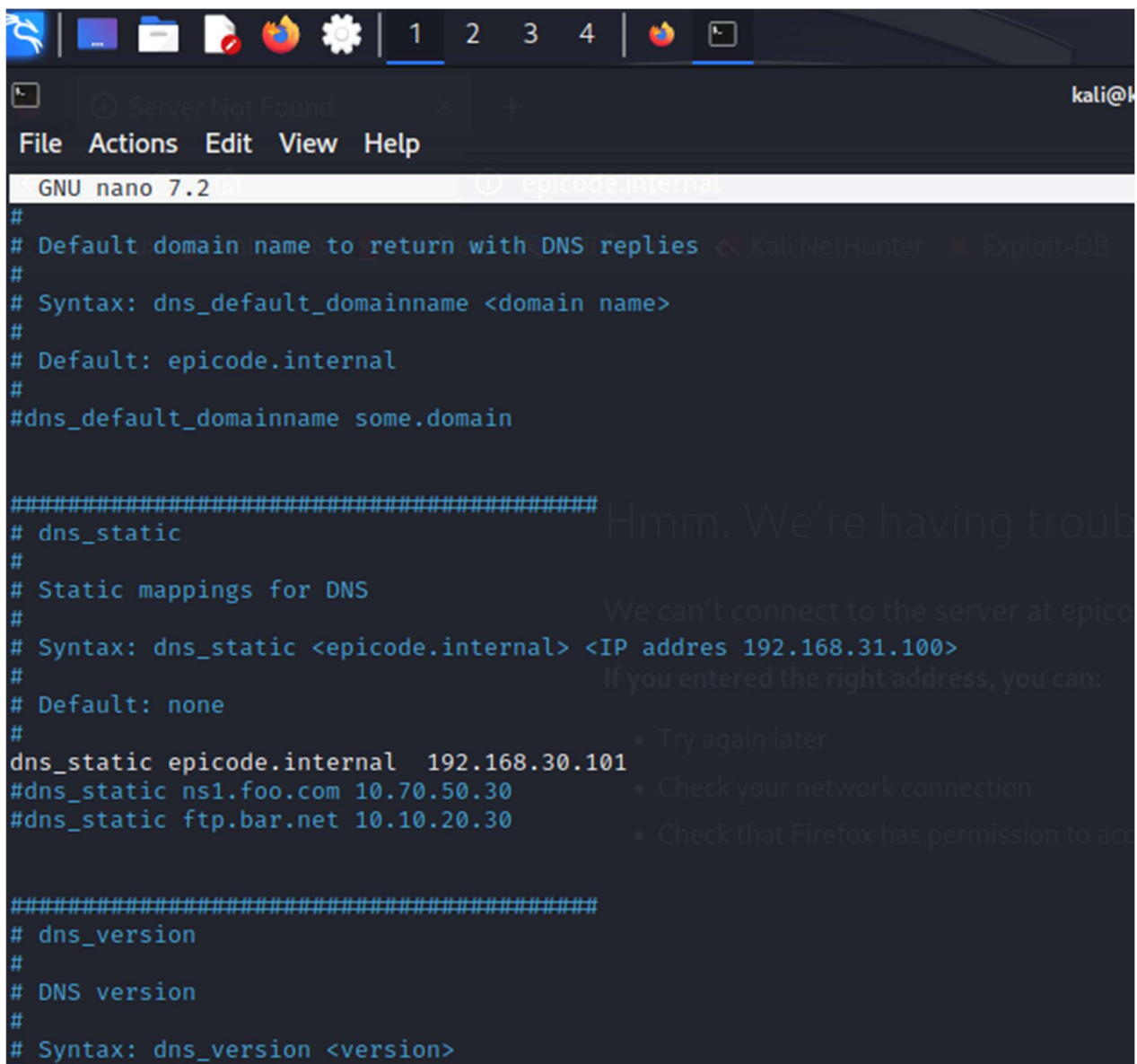
The image shows a terminal window with a dark background and light blue text. At the top, there is a taskbar with icons for a terminal, a file manager, a web browser, and a settings application. Below the taskbar, the terminal window has a menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'. The main content area shows the GNU nano 7.2 editor. The text in the editor is as follows:

```
GNU nano 7.2
# Port number to bind DNS service to
#
# Syntax: dns_bind_port <port number>
#
# Default: 53
#
#dns_bind_port 53

File System
#####
# dns_default_ip
#
# Default IP address to return with DNS replies
#
# Syntax: dns_default_ip <IP address>
#
# Default: 192.168.32.100
#
dns_default_ip 192.168.32.100

#####
# dns_default_hostname
#
# Default hostname to return with DNS replies
#
# Syntax: dns_default_hostname <hostname>
#
# Default:epicode.internal
#
#dns_default_hostname
```

Procedo a configurare il DNS con l'ip di default che in questo caso facciamo corrispondere all'indirizzo ip del server inetsim.



```
GNU nano 7.2 epicode.internal
#
# Default domain name to return with DNS replies
#
# Syntax: dns_default_domainname <domain name>
#
# Default: epicode.internal
#
#dns_default_domainname some.domain

#####
# dns_static
#
# Static mappings for DNS
#
# Syntax: dns_static <epicode.internal> <IP address 192.168.31.100>
#
# Default: none
#
dns_static epicode.internal 192.168.30.101
#dns_static ns1.foo.com 10.70.50.30
#dns_static ftp.bar.net 10.10.20.30

#####
# dns_version
#
# DNS version
#
# Syntax: dns_version <version>
```

Procedo ad associare il dominio con il nome epicode.internal all'indirizzo ip di Windows per permetterne la risoluzione.

Salvo la configurazione.

5. Attivo la simulazione inetsim:

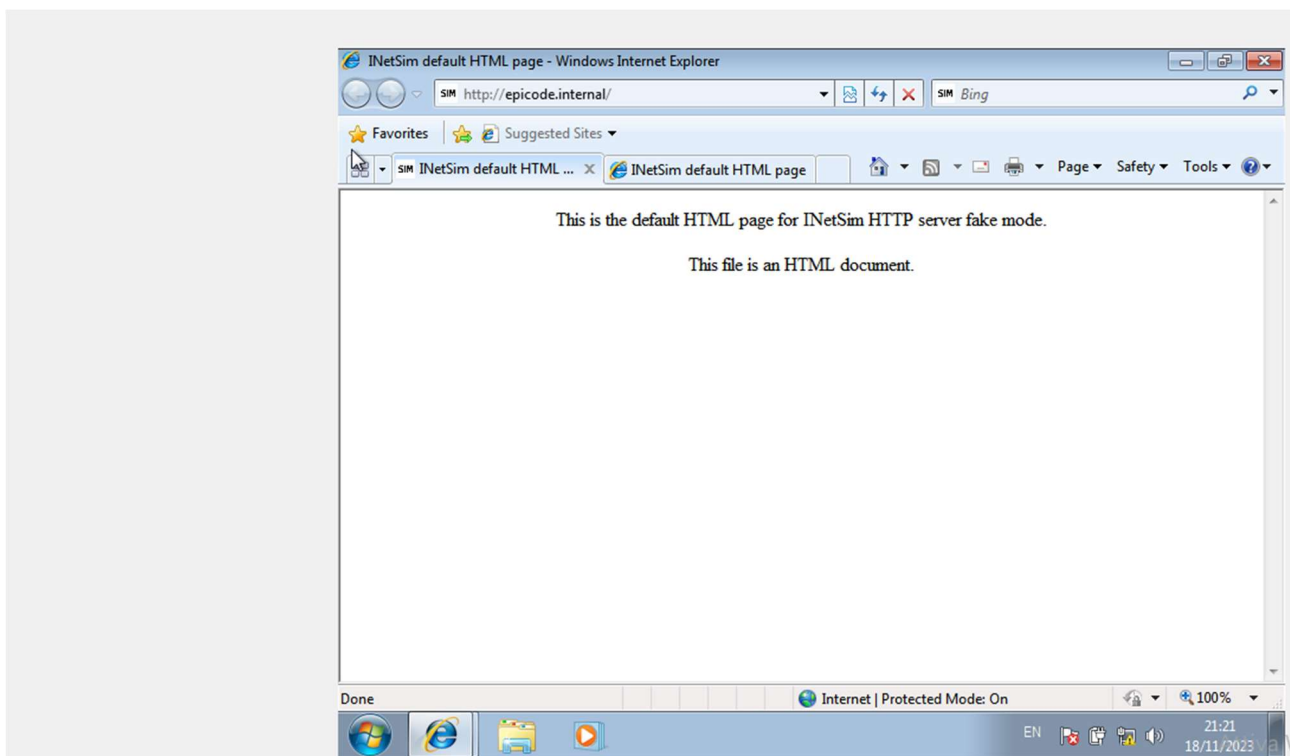

```

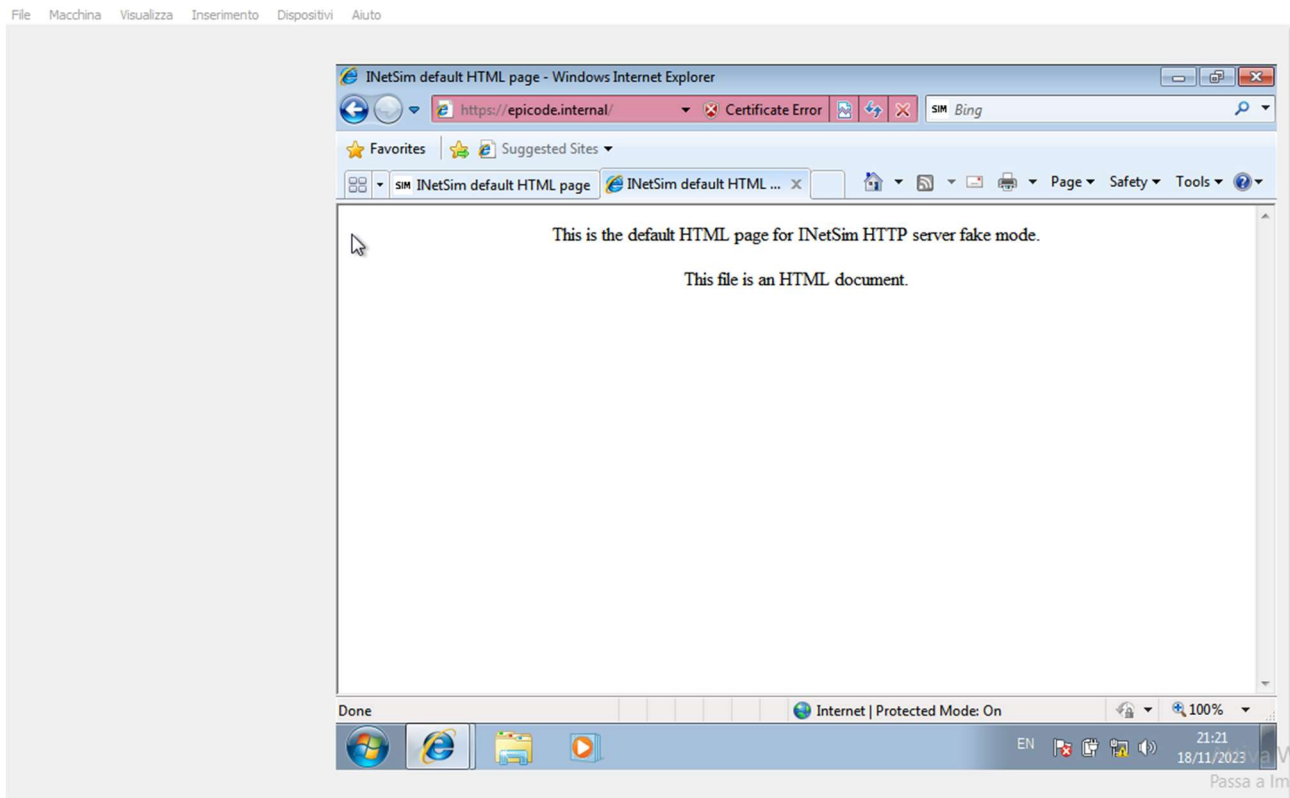
(kali@kali)-[/etc/inetsim]
$ sudo nano inetsim.conf

(kali@kali)-[/etc/inetsim]
$ 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 6888) ==
Session ID: 6888
Listening on: 192.168.32.100
Real Date/Time: 2023-11-18 21:13:03
Fake Date/Time: 2023-11-18 21:13:03 (Delta: 0 seconds)
Forking services...
* dns_53_tcp_udp - started (PID 6898)
print() on closed filehandle MLOG at /usr/share/perl5/Net/DNS/Nameserver.pm line 399.
print() on closed filehandle MLOG at /usr/share/perl5/Net/DNS/Nameserver.pm line 399.
* https_443_tcp - started (PID 6900)
* http_80_tcp - started (PID 6899)
done.
Simulation running.

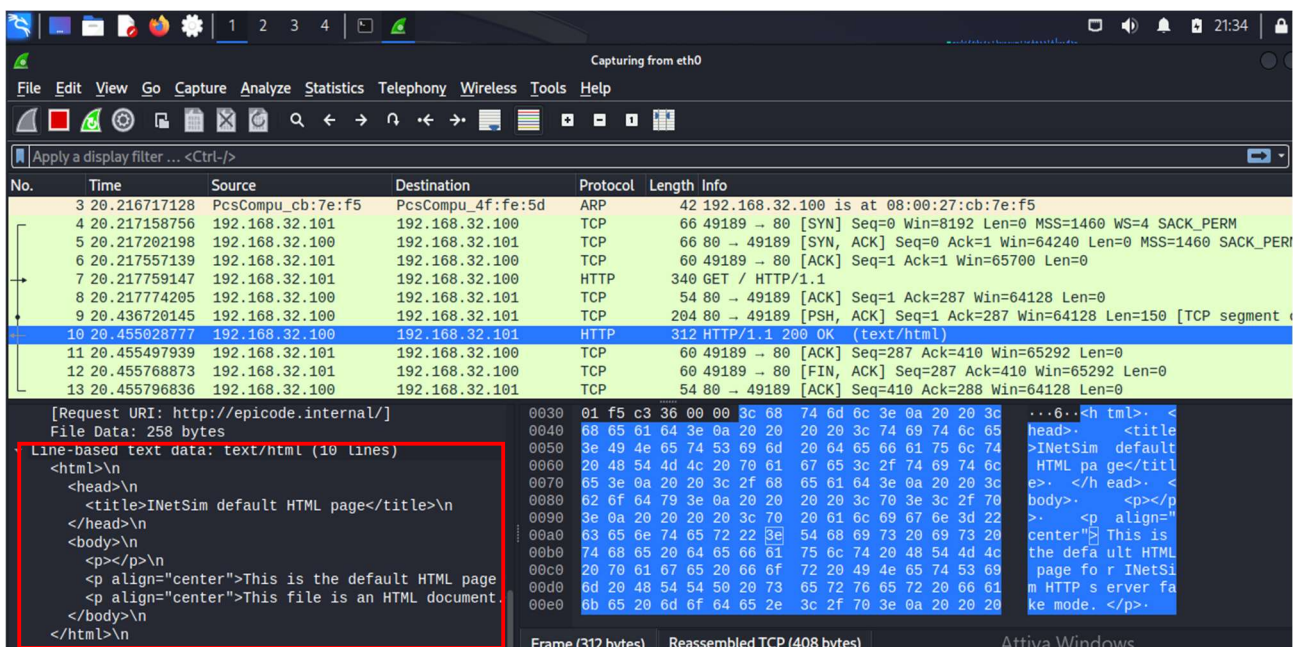
```

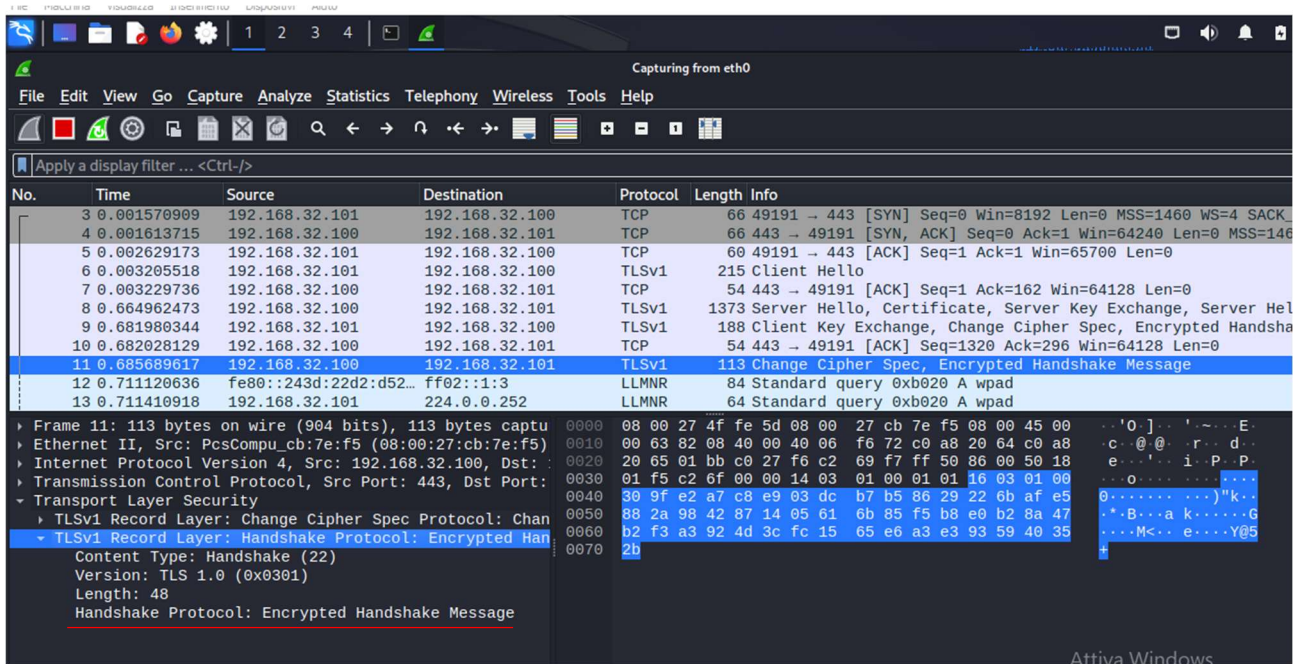
6. Apro il browser di windows e verifico se dominio epicode.internal viene risolto sia in HTTP che HTTPS:



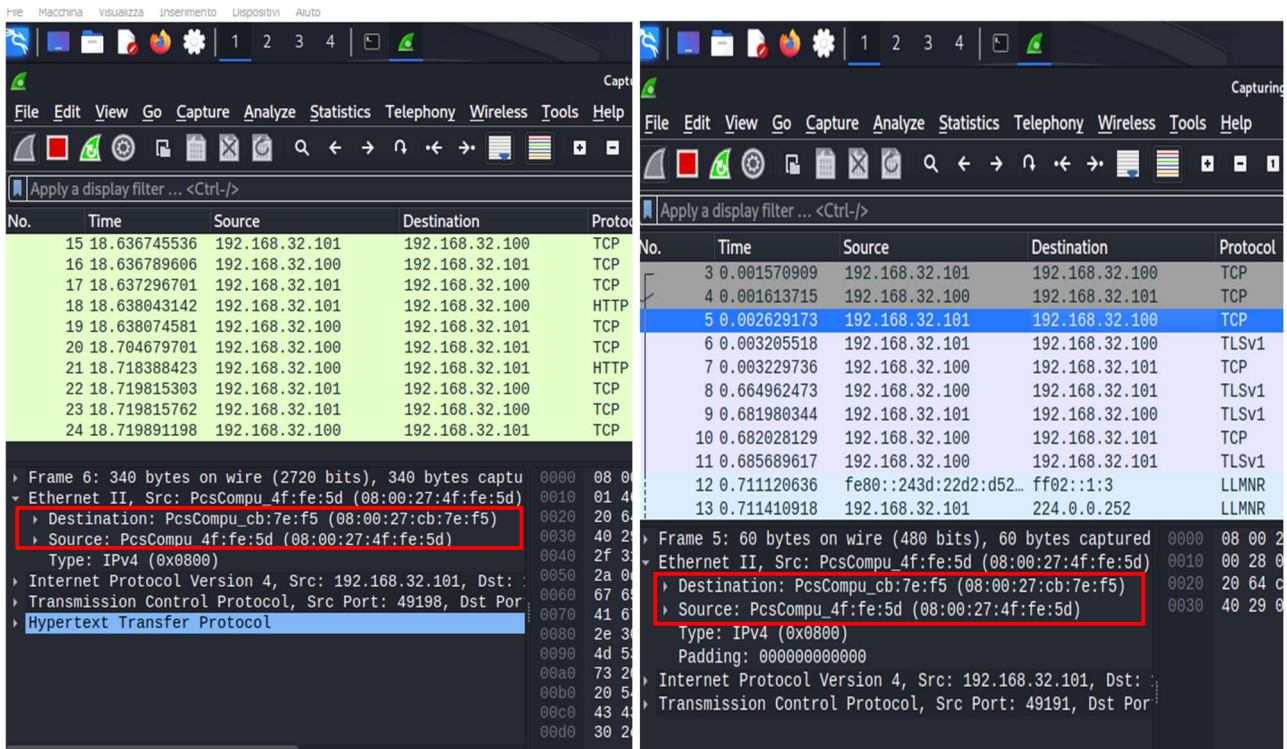


7. Utilizzo Wireshark dalla macchina kali per intercettare la comunicazione sia in HTTP che HTTPS:





- Confronto i mac address delle due macchine con le loro configurazioni per vedere se c'è corrispondenza:



Http

Https

```
C:\Windows\system32\CMD.exe
Windows IP Configuration

Host Name . . . . . : Windows7-1
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
Physical Address. . . . . : 08-00-27-4F-FE-5D
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::243d:22d2:d522:6478%11(Preferred)
IPv4 Address. . . . . : 192.168.32.101(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.32.100
DHCPv6 IAD . . . . . : 235405351
DHCPv6 Client DUID. . . . . : 00-01-00-01-2C-CE-42-0A-08-00-27-4F-FE-5D

DNS Servers . . . . . : 192.168.32.100
NetBIOS over Tcpip. . . . . : Enabled

Tunnel adapter isatap.{EDCC1871-CF16-4F4F-AD59-9E3F9F163C59}:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Microsoft ISATAP Adapter
Physical Address. . . . . : 00-00-00-00-00-00-E0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes

C:\Users\wboxuser>
```

```
kali@kali:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.32.100 netmask 255.255.255.0 broadcast 192.168.32.255
    inet6 fe80::a00:27ff:feeb:7ef5 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:cb:7e:f5 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 18 bytes 2564 (2.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4 bytes 240 (240.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 240 (240.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

kali@kali:~$
```

9. Evidenzio le eventuali differenze tra il traffico in HTTP ed il traffico precedente in HTTPS:

Come si può evincere dagli screen presenti al punto 7 nella richiesta HTTPS lo scambio d'informazioni è criptato pertanto non è possibile visualizzarlo (protocollo TLS); al contrario nella richiesta HTTP tutto risulta essere in chiaro (es: chiamata GET, Testo ecc.)

