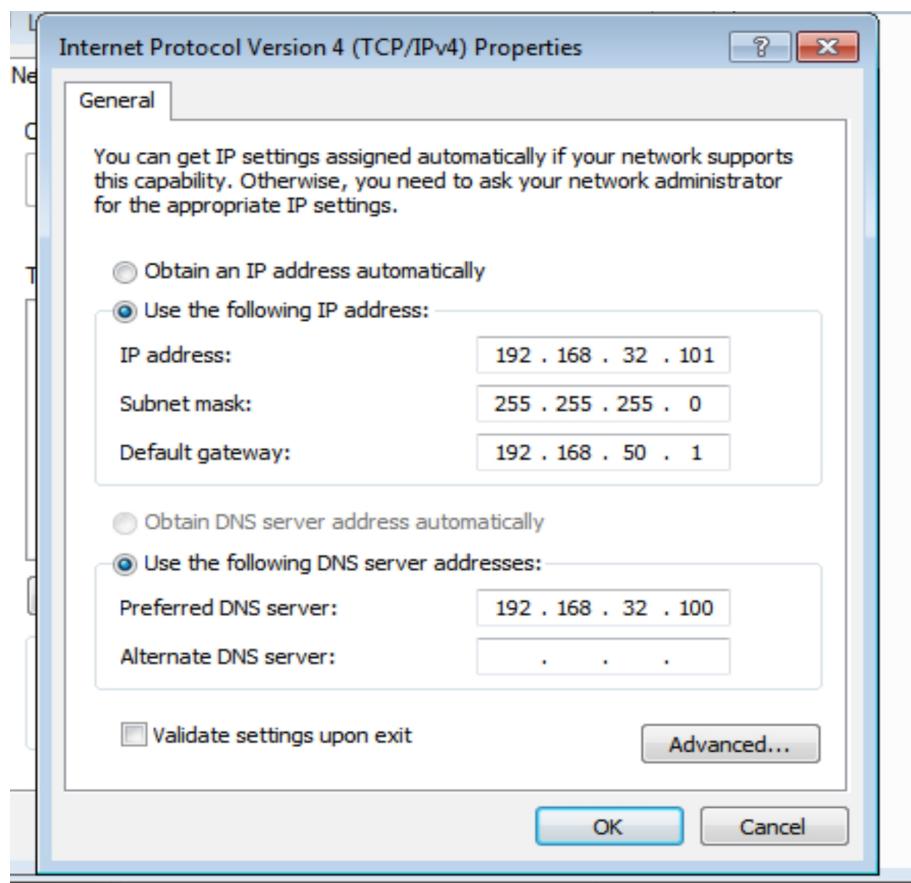


Esercitazione W4-D4

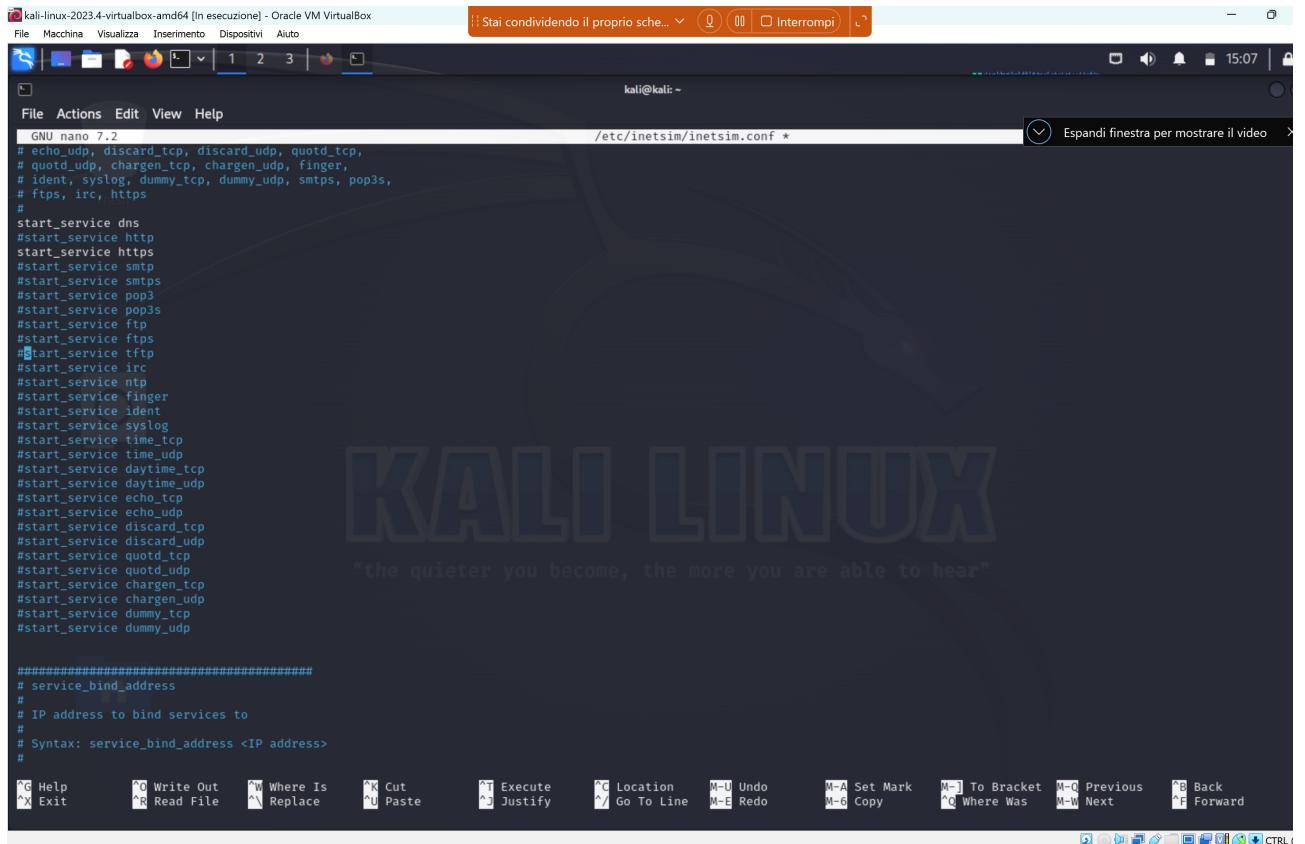
Per prima cosa è stato necessario settare le macchine virtuali con i nuovi indirizzi IP e gateway:
Kali 192.168.32.100 (IP)
Windows 192.168.32.101 (IP)
Windows 192.168.32.100 (DNS)



```
(kali㉿kali)-[~] $ ifconfig | tail -41 340 bytes on wlo <inet 192.168.32.100 netmask 255.255.255.0 broadcast 192.168.32.255  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
      inet 192.168.32.100 netmask 255.255.255.0 broadcast 192.168.32.255  
      ether 08:00:27:21:b1:d0 txqueuelen 1000 (Ethernet)  
        RX packets 198 bytes 17706 (17.2 KiB)  
        RX errors 0 dropped 0 overruns 0 frame 0  
        TX packets 105 bytes 18828 (18.3 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  
      ether ::1 txqueuelen 1000 (Local Loopback)  
        RX packets 332 bytes 27880 (27.2 KiB)  
        RX errors 0 dropped 0 overruns 0 frame 0  
        TX packets 332 bytes 27880 (27.2 KiB)  
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Per seconda cosa è stato necessario settare DNS e HTTPS su kali:

-percorso sudo nano /etc/inetsim/inetsim.conf

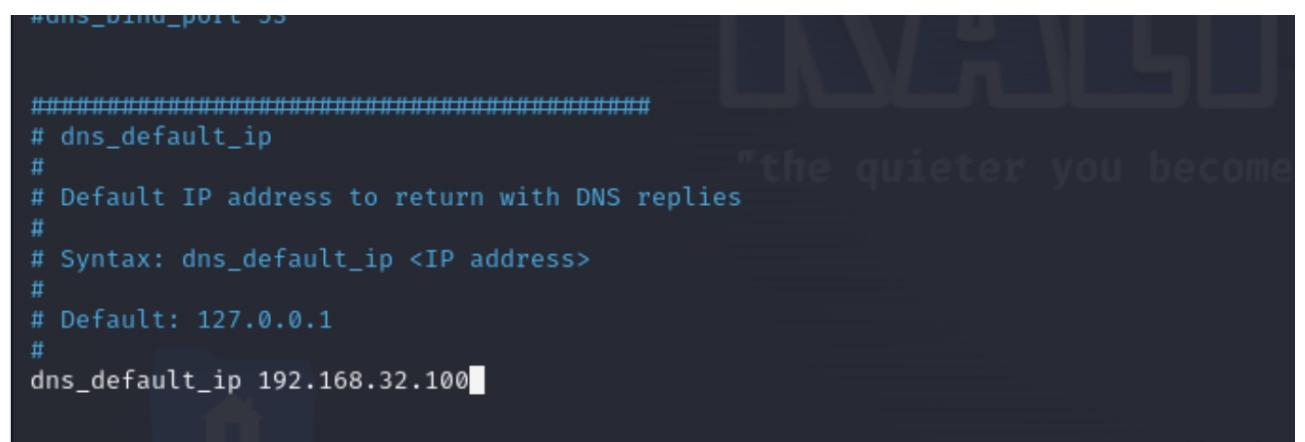


```
GNU nano 7.2
# echo_udp, discard_tcp, discard_udp, quod_tcp,
# quod_udp, chargen_tcp, chargen_udp, finger,
# ident, syslog, dummy_tcp, dummy_udp, smtps, pop3s,
# ftps, irc, https
#
#start_service dns
#start_service http
start_service https
#start_service smtp
#start_service smtps
#start_service pop3
#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
#start_service time_tcp
#start_service time_udp
#start_service daytime_tcp
#start_service daytime_udp
#start_service echo_tcp
#start_service echo_udp
#start_service discard_tcp
#start_service discard_udp
#start_service quod_tcp
#start_service quod_udp
#start_service chargen_tcp
#start_service chargen_udp
#start_service dummy_tcp
#start_service dummy_udp

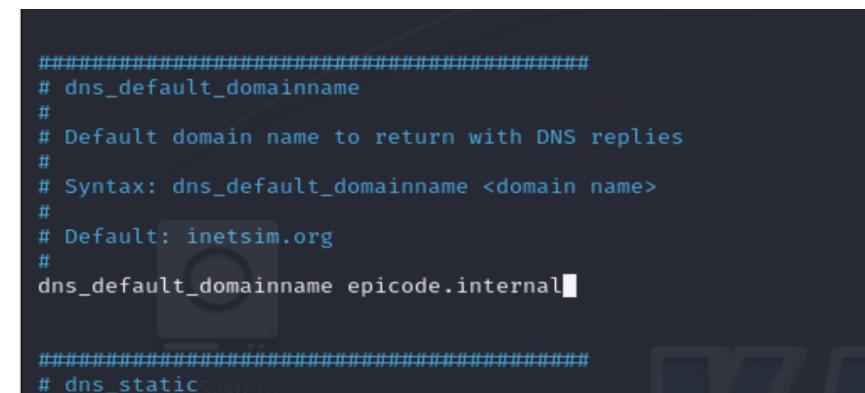
#####
# service_bind_address
#
# IP address to bind services to
#
# Syntax: service_bind_address <IP address>
#
```

GN Help ^O Write Out ^W Where Is ^X Cut ^T Execute ^C Location M-U Undo M-A Set Mark M-[To Bracket M-Q Previous ^B Back
^X Exit ^R Read File ^W Replace ^U Paste ^J Justify ^G Go To Line M-E Redo M-6 Copy M-Q Where Was M-W Next ^F Forward

settare il dns di default e dominio



```
#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

#####
# dns_static
```

Attivate le fake mode per i serviti http (in previsione della seconda parte), https e dns

```
File System
#####
# http_fakemode
#
# Turn HTTP fake mode on or off
#
# Syntax: http_fakemode [yes|no]
#
# Default: yes
#
http_fakemode yes

#####
# http_fakefile
```

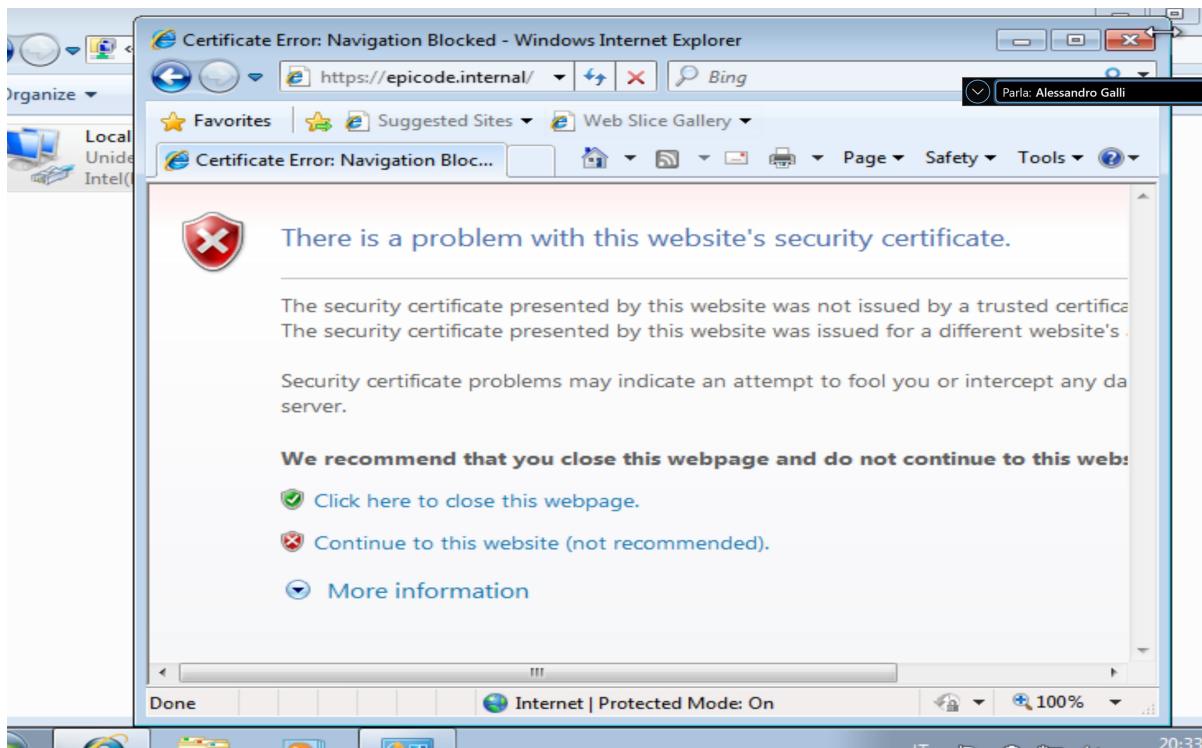
```
File System
#####
# https_fakemode
#
# Turn HTTPS fake mode on or off
#
# Syntax: https_fakemode [yes|no]
#
# Default: yes
#
https_fakemode yes

#####
# https_fakefile
```

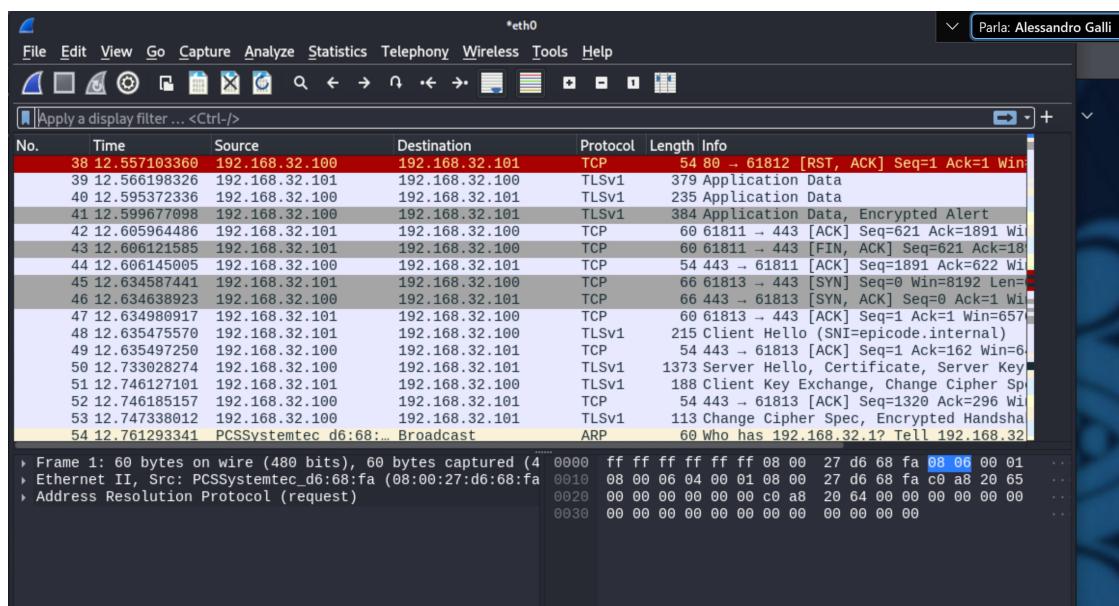
Sono state salvate tutte le impostazioni e avviato il processo inetsim

```
(kali㉿kali)-[~]
$ sudo nano /etc/network/interfaces
(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 21808) ==
Session ID:      21808
Listening on:    192.168.32.100
Real Date/Time:  2024-03-20 15:14:41
Fake Date/Time:  2024-03-20 15:14:41 (Delta: 0 seconds)
Forking services ...
 * dns_53_tcp_udp - started (PID 21810)
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 21811)
done.
Simulation running.
```

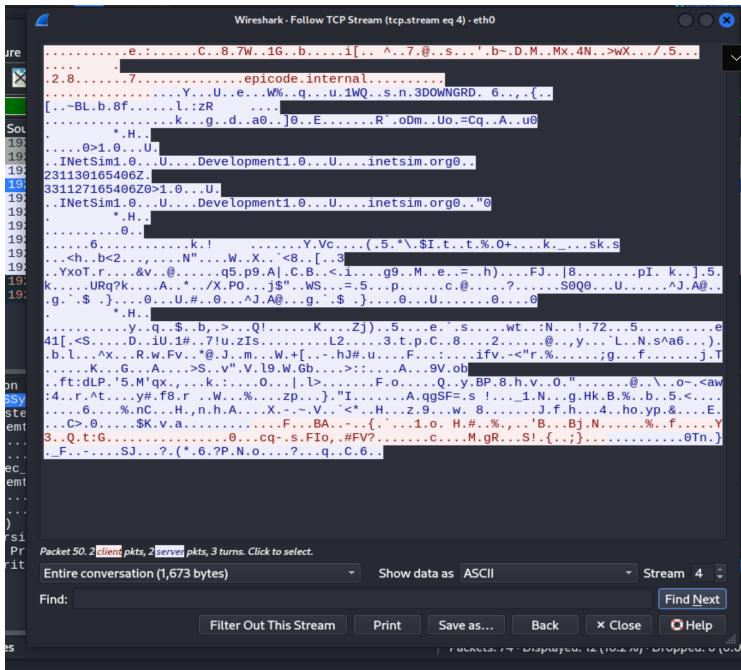
Tramite windows ho cercato l'indirizzo https://epicode.internal



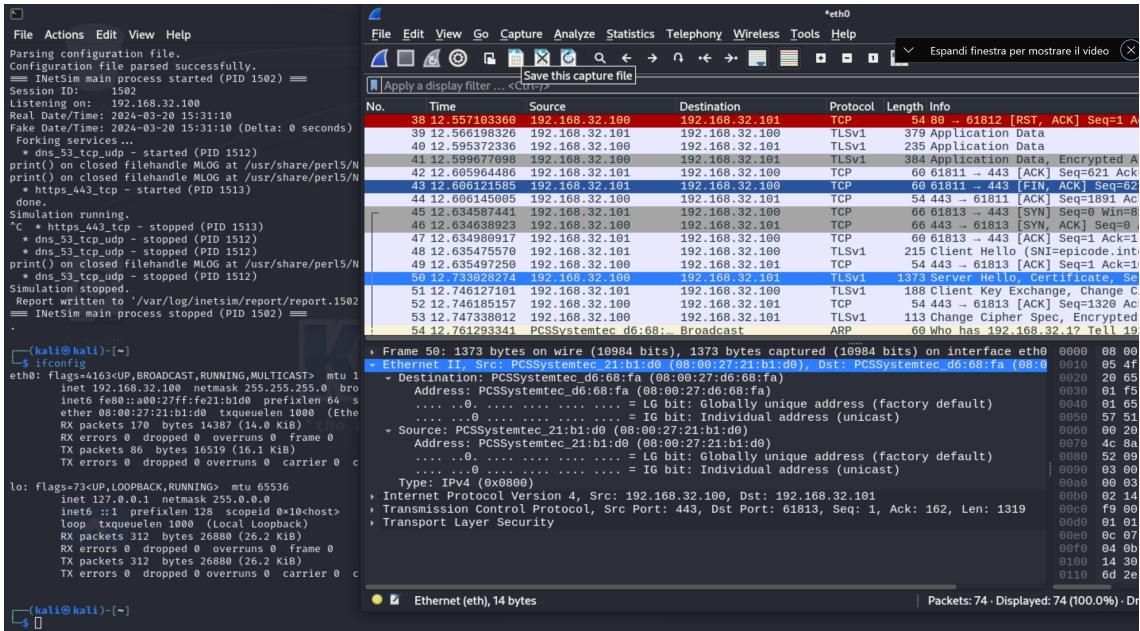
Tramite wireshark è stata analizzata la connessione tra le macchine



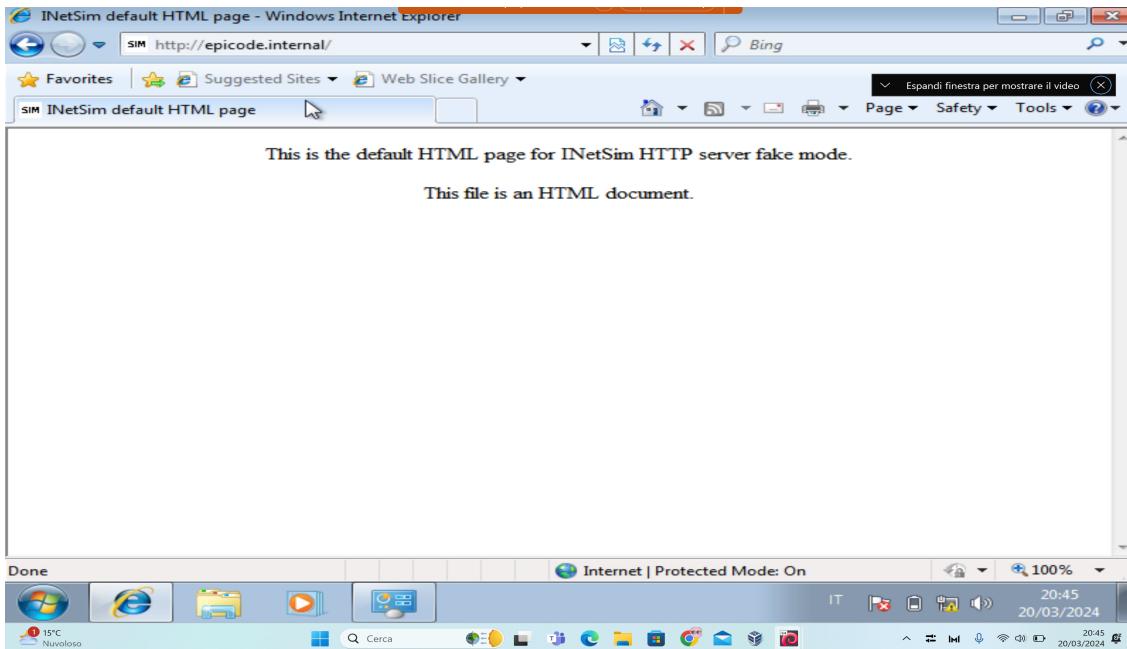
Con protocollo https la comunicazione tra le macchine è avvenuta in modo cifrato:



Di seguito indirizzi IP e mac address



Ho ripetuto la procedura con indirizzo http:



Questa volta la comunicazione non era cifrata:

