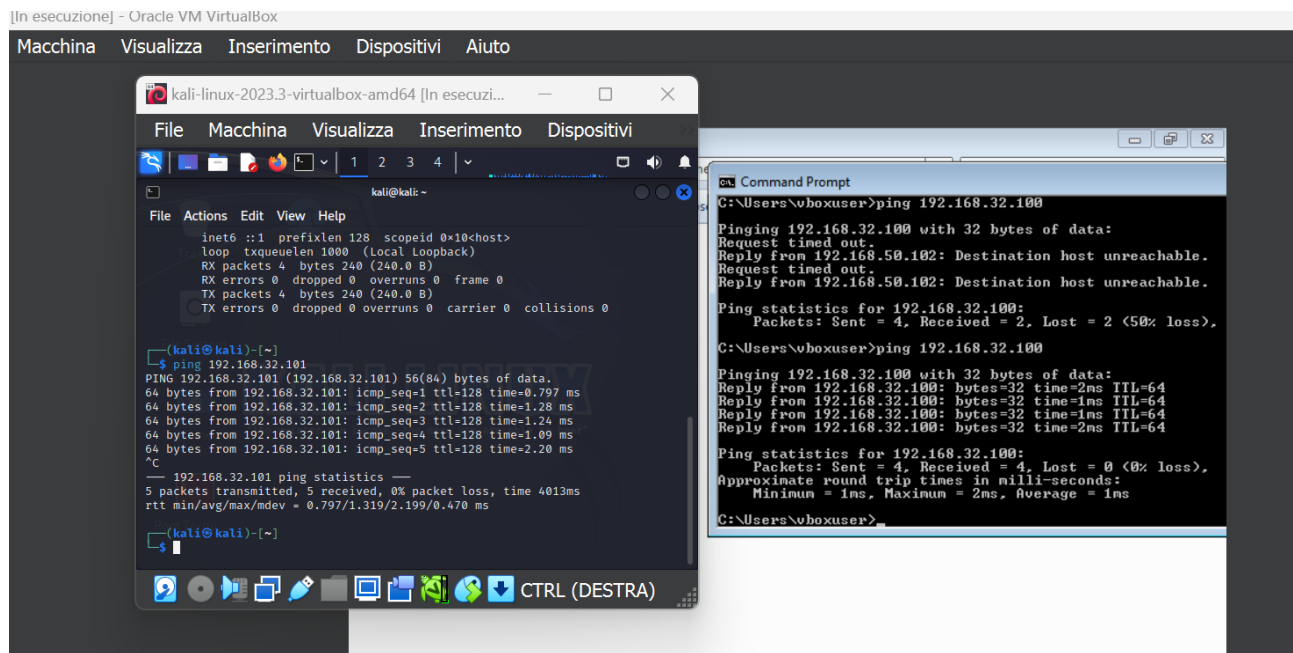


## Report Prova pratica Modulo 1

Per lo svolgimento del compito assegnato sono state avviate le macchine virtuali Kali Linux e Windows 7, sono stati impostati i nuovi IP 192.168.32.100 per Kali e IP 192.168.32.101 per il Sistema Operativo Windows 7. Sulla macchina Kali è stata aperta, tramite terminale e comando `sudo nano inetsim.conf`, la finestra dei file di configurazione di INetSim, sono stati commentati (#) tutti i servizi presenti meno i servizi dns, http e https necessari per la configurazione del server DNS, impostandone IP e hostname.



```
[In esecuzione] - Oracle VM VirtualBox
Macchina Visualizza Inserimento Dispositivi Aiuto

kali-linux-2023.3-virtualbox-amd64 [In esecuzione]
File Macchina Visualizza Inserimento Dispositivi

kali@kali:~$ ping 192.168.32.101
PING 192.168.32.101 (192.168.32.101) 56(84) bytes of data:
64 bytes from 192.168.32.101: icmp_seq=1 ttl=128 time=0.797 ms
64 bytes from 192.168.32.101: icmp_seq=2 ttl=128 time=1.28 ms
64 bytes from 192.168.32.101: icmp_seq=3 ttl=128 time=1.24 ms
64 bytes from 192.168.32.101: icmp_seq=4 ttl=128 time=1.09 ms
64 bytes from 192.168.32.101: icmp_seq=5 ttl=128 time=2.20 ms
^C
--- 192.168.32.101 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4013ms
rtt min/avg/max/mdev = 0.797/1.319/2.199/0.470 ms

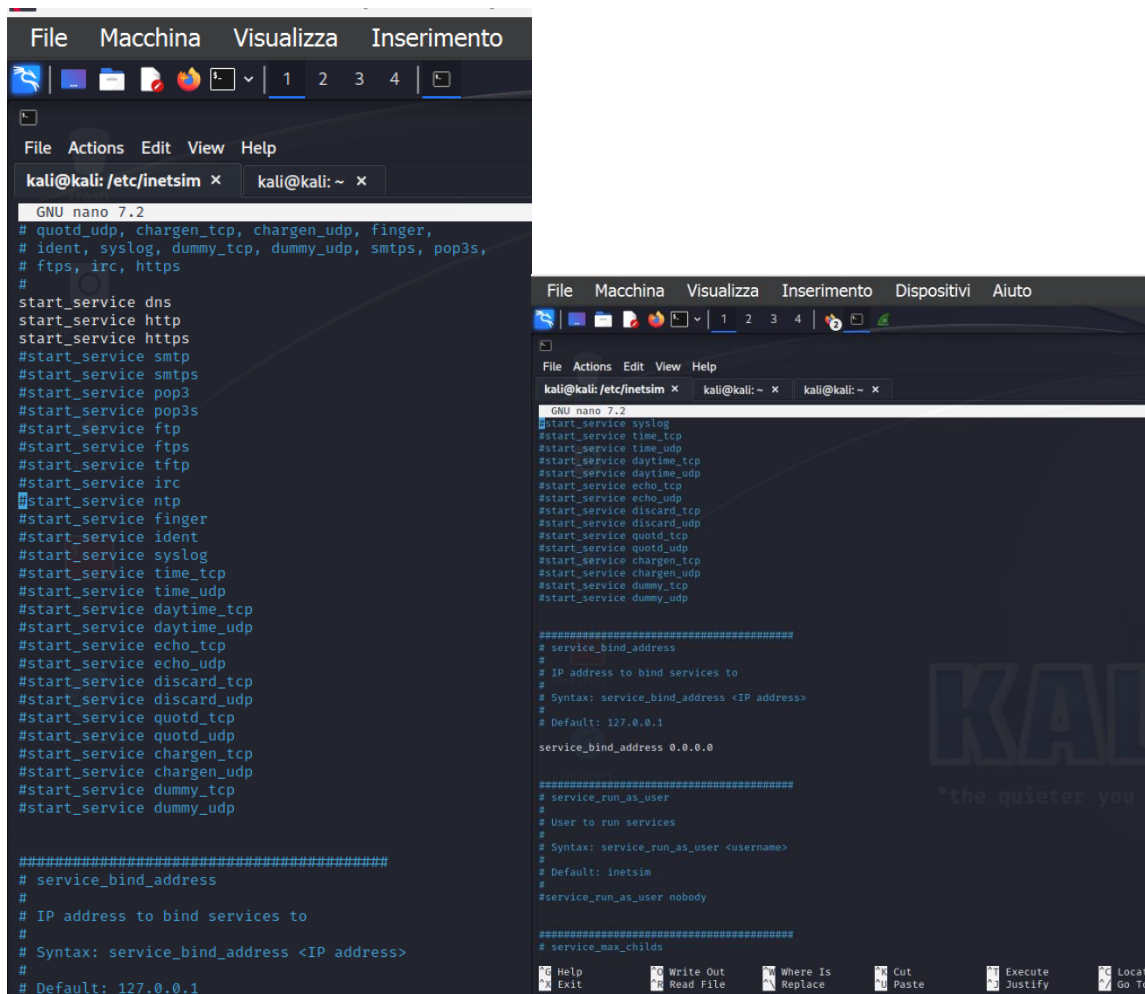
C:\Users\ vboxuser> ping 192.168.32.100
Pinging 192.168.32.100 with 32 bytes of data:
Request timed out.
Reply from 192.168.50.102: Destination host unreachable.
Request timed out.
Reply from 192.168.50.102: Destination host unreachable.

Ping statistics for 192.168.32.100:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),

C:\Users\ vboxuser> ping 192.168.32.100
Pinging 192.168.32.100 with 32 bytes of data:
Reply from 192.168.32.100: bytes=32 time=2ms TTL=64
Reply from 192.168.32.100: bytes=32 time=1ms TTL=64
Reply from 192.168.32.100: bytes=32 time=1ms TTL=64
Reply from 192.168.32.100: bytes=32 time=2ms TTL=64

Ping statistics for 192.168.32.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\Users\ vboxuser>
```



```
File Macchina Visualizza Inserimento
GNU nano 7.2
# quotd_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 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: 127.0.0.1
service_bind_address 0.0.0.0

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

#####
# service_max_childs
#
```

```
File Macchina Visualizza Inserimento Dispositivi Aiuto
GNU nano 7.2
#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 quotd_tcp
#start_service quotd_udp
#start_service chargen_tcp
#start_service chargen_udp
#start_service dummy_tcp
#start_service dummy_udp

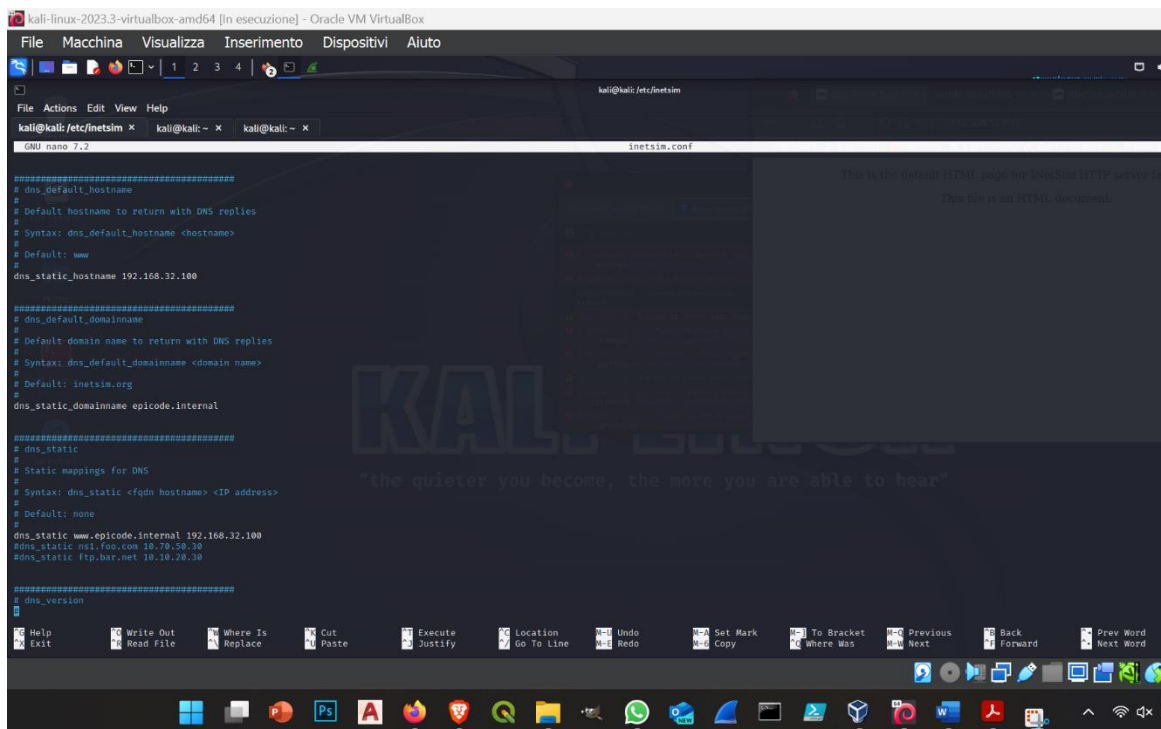
#####
# service_bind_address
#
# IP address to bind services to
#
# Syntax: service_bind_address <IP address>
#
# Default: 127.0.0.1
service_bind_address 0.0.0.0

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

#####
# service_max_childs
#
```

Successivamente è stato attivato il service\_bind\_address attribuendo l'IP 0.0.0.0 in modo che qualunque macchina esterna possa contattare il server DNS.

Nella sezione dedicata ai servizi DNS sono state modificate le voci dns\_default\_hostname in dns\_static\_hostname aggiungendo l'indirizzo IP 192.168.32.100 della macchina Kali; dns\_default\_domainname in dns\_static\_domainname aggiungendo il dominio "epicode.internal", infine nella sezione successiva è stato attivato il servizio dns\_static www.epicode.internal per permettere inviare la richiesta al DNS server kali dal Client Windows 7.



```
kali@kali: /etc/inetsim
GNU nano 7.2 inetsim.conf

#####
# dns_default_hostname
#
# Default hostname to return with DNS replies
#
# Syntax: dns_default_hostname <hostname>
#
# Default: www
#
dns_default_hostname 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
#
# Static mappings for DNS
#
# Syntax: dns_static <fqdn hostname> <IP address>
#
# Default: none
#
dns_static www.epicode.internal 192.168.32.100
#dns_static ns1.foo.com 10.70.50.30
#dns_static ftp.bar.net 10.10.20.30

#####
# dns_version
#
```

Terminata la configurazione è stato avviato il comando con i permessi da amministratore `sudo inetsim` per avviare il simulatore di rete INetSim. Durante l'avvio della simulazione sono stati evidenziati due avvertimenti relativi ad un problema di configurazione INetSim

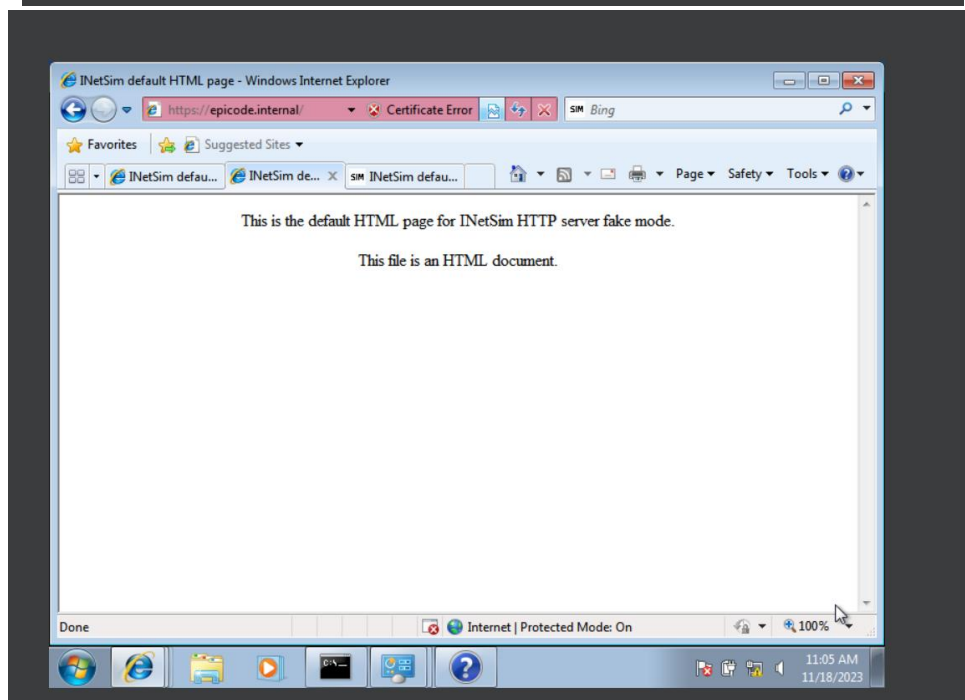
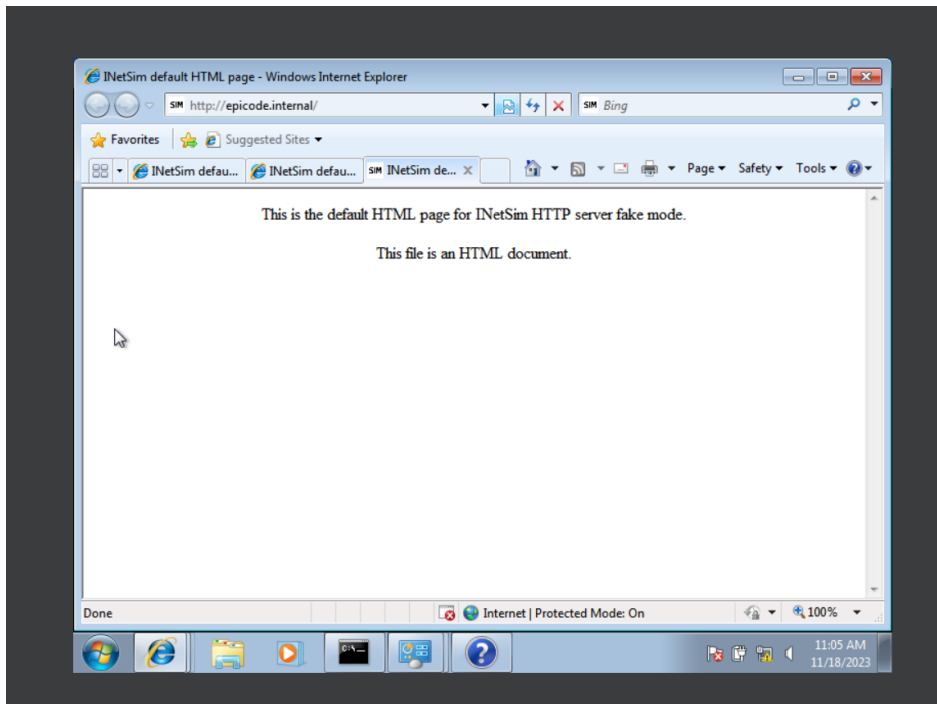
- Warning: Unknown option 'dns\_static\_hostname' in configuration file '/etc/inetsim/inetsim.conf' line 219
- Warning: Unknown option 'dns\_static\_domainname' in configuration file '/etc/inetsim/inetsim.conf' line 231

```
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
kali@kali: /etc/inetsim x  kali@kali: ~ x  kali@kali: ~ x
Using data directory: /var/lib/inetsim/
Using report directory: /var/log/inetsim/report/
Using configuration file: /etc/inetsim/inetsim.conf
Parsing configuration file.
Error: '192.168.32.100' is not a valid hostname in configuration file '/etc/inetsim/inetsim.conf' line 219.

(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.
Warning: Unknown option 'dns_static_hostname' in configuration file '/etc/inetsim/inetsim.conf' line 219
Warning: Unknown option 'dns_static_domainname' in configuration file '/etc/inetsim/inetsim.conf' line 231
Configuration file parsed successfully.
== INetSim main process started (PID 331276) ==
Session ID: 331276
Listening on: 0.0.0.0
Real Date/Time: 2023-11-20 05:35:12
Fake Date/Time: 2023-11-20 05:35:12 (Delta: 0 seconds)
Forking services ...
* dns_53_tcp_udp - started (PID 331278)
print() on closed filehandle MLOG at /usr/share/perl5/Net/DNS/Nameserver.pm line 399.
* https_443_tcp - started (PID 331280)
print() on closed filehandle MLOG at /usr/share/perl5/Net/DNS/Nameserver.pm line 399.
* http_80_tcp - started (PID 331279)
done.
Simulation running.
```

I precedenti Warning relativi alle linee di dialogo evidenziate non sono stati rimossi dopo le correzioni, permane dunque il problema di configurazione, ma questo non impedisce l'avvio della simulazione di rete.

Dopo aver avviato la simulazione sono state avviate due richieste dal Client Browser di Windows 7 al server epicode.internal, una mediante protocollo http e una in https. Le richieste hanno entrambe raggiunto il server DNS kali. La richiesta in https evidenzia un errore di certificato ed è stato necessario accettare i rischi di navigazione della pagina.



Successivamente è stato avviato il Software Wireshark per poter intercettare la comunicazione e il traffico di pacchetti dal Client Windows 7 verso il Server DNS, sia della richiesta in http e https. HTTP è un protocollo a livello di applicazione nel modello ISO/OSI che definisce diversi tipi di richieste e risposte HTTP GET, questa richiesta avviene tramite una porta di rete diversa da 443 che veicola il traffico di dati per tramite https.

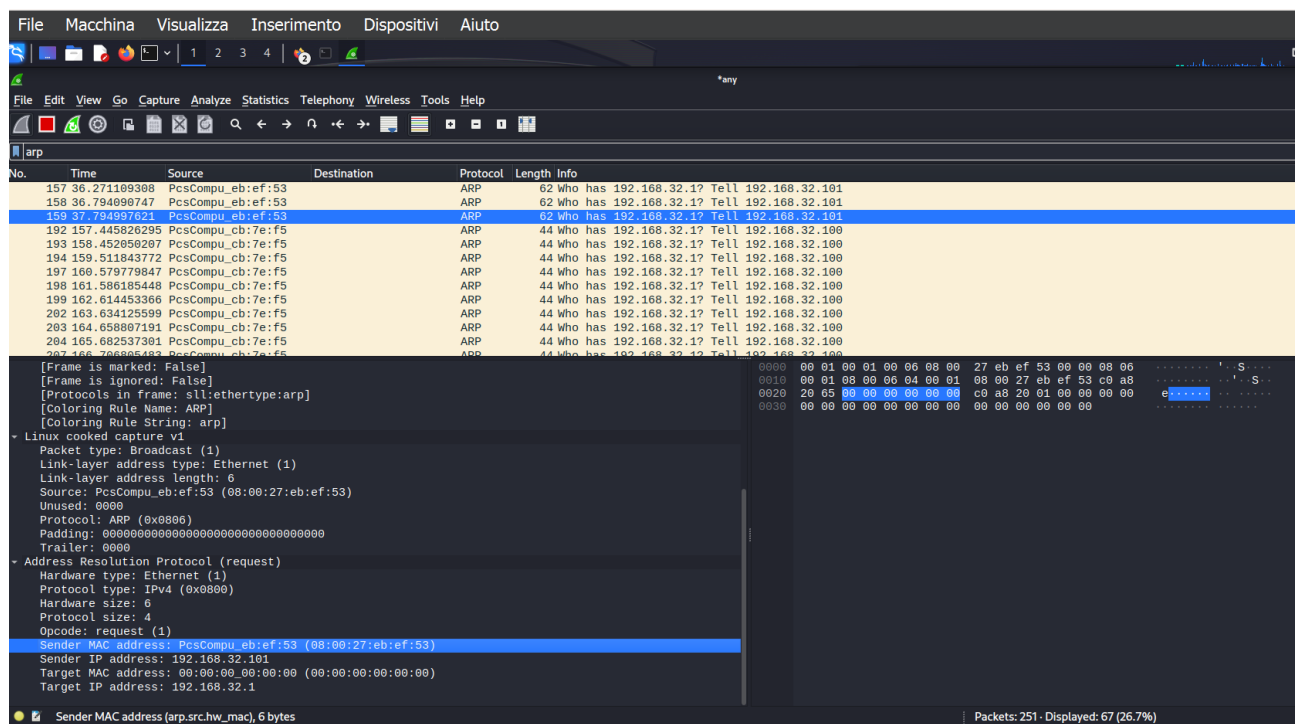
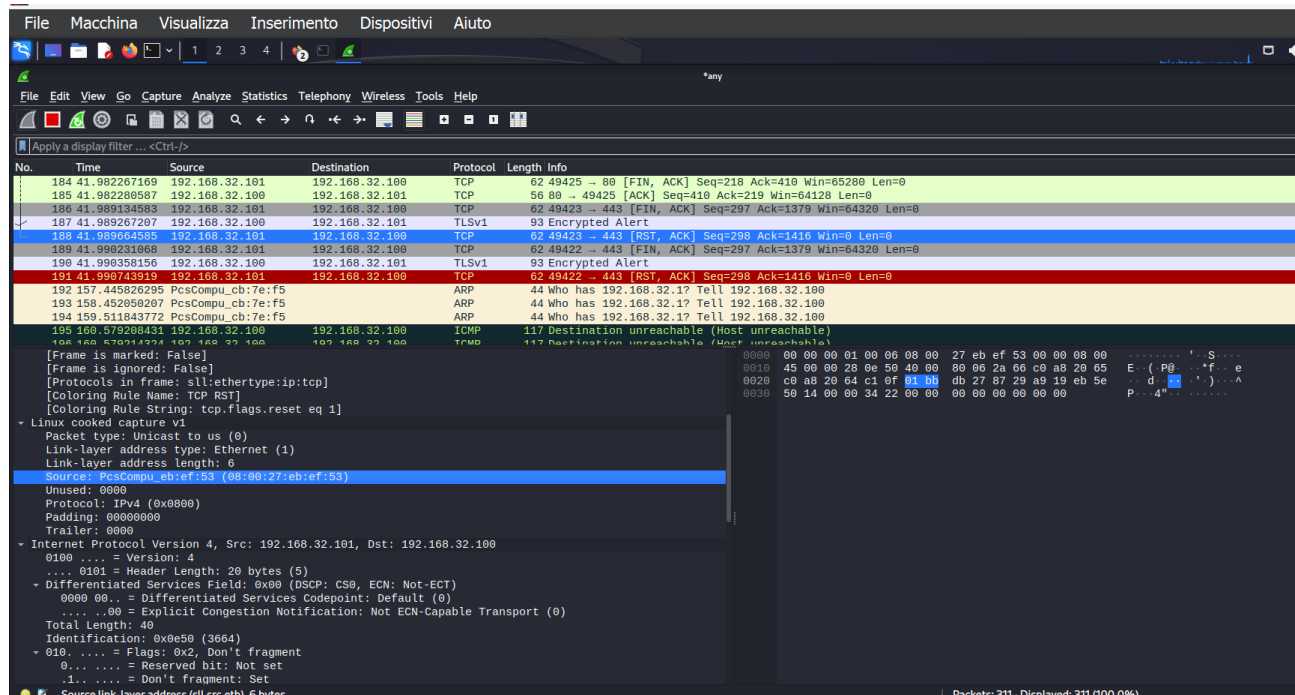
Per la richiesta in https i siti Web HTTPS devono ottenere un certificato SSL/TLS da un'autorità di certificazione indipendente che lo condividono con il browser prima di scambiare dati. Il certificato SSL contiene anche informazioni crittografiche, quindi il server e i browser Web possono scambiarsi dati crittografati o criptati e avviene tramite la porta 443.

Sempre tramite il software Wireshark sono stati evidenziati i MAC address di destinazione dei pacchetti utilizzando il filtro per visualizzare il protocollo ARP per poter evidenziare gli indirizzi MAC sorgente e destinazione. I MAC address sono codici univoci a livello fisico attribuiti dal produttore delle schede di rete e

non modificabili e si possono trovare in ogni device di rete: pc, router, switch, server ecc. La richiesta in https, essendo una trasmissione sicura e criptata dei dati, risulta essere differente dalla richiesta http per evitare lo sniffing e il man in the middle, inviando pacchetti dati e MAC address criptato.

(Di seguito vengono allegati gli screenshot della registrazione del traffico dei pacchetti in http/https e dei MAC address).

https:





Wireshark interface showing ARP traffic. The packet list displays several ARP requests and replies. The selected packet (No. 191) is an ARP request from 192.168.32.101 to 192.168.32.100. The packet details pane shows the Ethernet II, ARP, and Internet Protocol (IPv4) layers. The packet bytes pane displays the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
157	36.271109398	PcsCompu_eb:ef:53	192.168.32.101	ARP	62	Who has 192.168.32.1? Tell 192.168.32.101
158	36.794099747	PcsCompu_eb:ef:53	192.168.32.101	ARP	62	Who has 192.168.32.1? Tell 192.168.32.101
159	37.794997621	PcsCompu_eb:ef:53	192.168.32.101	ARP	62	Who has 192.168.32.1? Tell 192.168.32.101
192	157.445826295	PcsCompu_cb:7e:f5	192.168.32.100	ARP	44	Who has 192.168.32.1? Tell 192.168.32.100
193	158.452850207	PcsCompu_cb:7e:f5	192.168.32.100	ARP	44	Who has 192.168.32.1? Tell 192.168.32.100
191	159.311043772	PcsCompu_cb:7e:f5	192.168.32.100	ARP	44	Who has 192.168.32.1? Tell 192.168.32.100
197	180.579779847	PcsCompu_cb:7e:f5	192.168.32.100	ARP	44	Who has 192.168.32.1? Tell 192.168.32.100
198	161.586185448	PcsCompu_cb:7e:f5	192.168.32.100	ARP	44	Who has 192.168.32.1? Tell 192.168.32.100
199	162.614453366	PcsCompu_cb:7e:f5	192.168.32.100	ARP	44	Who has 192.168.32.1? Tell 192.168.32.100
202	163.634125599	PcsCompu_cb:7e:f5	192.168.32.100	ARP	44	Who has 192.168.32.1? Tell 192.168.32.100
203	164.658807191	PcsCompu_cb:7e:f5	192.168.32.100	ARP	44	Who has 192.168.32.1? Tell 192.168.32.100
204	165.682537301	PcsCompu_cb:7e:f5	192.168.32.100	ARP	44	Who has 192.168.32.1? Tell 192.168.32.100
207	166.788084932	PcsCompu_cb:7e:f5	192.168.32.100	ARP	44	Who has 192.168.32.1? Tell 192.168.32.100

Packet details for No. 191:

- Frame is marked: False
- Frame is ignored: False
- Protocols in frame: II:ethertype:arp
- Coloring Rule Name: ARP
- Coloring Rule String: arp
- Linux cooked capture v1
  - Packet type: Broadcast (1)
  - Link-layer address type: Ethernet (1)
  - Link-layer address length: 6
  - Source: PcsCompu\_eb:ef:53 (08:00:27:eb:ef:53)
  - Unused: 0000
  - Protocol: ARP (0x0806)
  - Padding: 00000000000000000000000000000000
  - Trailer: 0000
- Address Resolution Protocol (request)
  - Hardware type: Ethernet (1)
  - Protocol type: IPv4 (0x0800)
  - Hardware size: 6
  - Protocol size: 4
  - Opcode: request (1)
  - Sender MAC address: PcsCompu\_eb:ef:53 (08:00:27:eb:ef:53)
  - Sender IP address: 192.168.32.101
  - Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)
  - Target IP address: 192.168.32.1

Target MAC address (arp.dst.hw\_mac), 6 bytes

Packets: 211 - Displayed: 43 (20.4%)

http:

Wireshark interface showing HTTP traffic. The packet list displays several HTTP GET requests and responses. The selected packet (No. 25) is an HTTP GET request from 192.168.32.101 to 192.168.32.100. The packet details pane shows the Ethernet II, Internet Protocol (IPv4), and Transmission Control Protocol (TCP) layers. The packet bytes pane displays the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
16	3.247528471	192.168.32.101	192.168.32.100	HTTP	273	GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab HTTP/1.1
21	3.249369234	192.168.32.101	192.168.32.100	HTTP	273	GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab HTTP/1.1
23	3.268603884	192.168.32.100	192.168.32.101	HTTP	314	HTTP/1.1 200 OK (text/html)
25	3.269401572	192.168.32.101	192.168.32.100	HTTP	314	HTTP/1.1 200 OK (text/html)

Packet details for No. 25:

- Frame 25: 314 bytes on wire (2512 bits), 314 bytes captured (2512 bits) on interface any, id 0
- Linux cooked capture v1
  - Packet type: Sent by us (4)
  - Link-layer address type: Ethernet (1)
  - Link-layer address length: 6
  - Source: PcsCompu\_cb:7e:f5 (08:00:27:cb:7e:f5)
  - Unused: 0000
  - Protocol: IPv4 (0x0800)
- Internet Protocol Version 4, Src: 192.168.32.100, Dst: 192.168.32.101
  - 0100 .... = Version: 4
  - .... 0101 = Header Length: 20 bytes (5)
  - Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  - Total Length: 298
  - Identification: 0xe54e (58702)
  - 010. .... = Flags: 0x2, Don't fragment
  - ...0 0000 0000 0000 = Fragment Offset: 0
  - Time to Live: 64
  - Protocol: TCP (6)
  - Header Checksum: 0x9265 [validation disabled]
  - [Header checksum status: Unverified]
  - Source Address: 192.168.32.100
  - Destination Address: 192.168.32.101
- Transmission Control Protocol, Src Port: 80, Dst Port: 49434, Seq: 151, Ack: 218, Len: 258
  - Source Port: 80
  - Destination Port: 49434
  - [Stream index: 1]
  - [Conversation completeness: Complete, WITH\_DATA (31)]
  - [TCP Segment Len: 258]
  - Sequence Number: 151 (relative sequence number)
  - Sequence Number (raw): 2277622220
  - [Next Sequence Number: 410 (relative sequence number)]
  - Acknowledgment Number: 218 (relative ack number)
  - Acknowledgment number (raw): 1136410040

Frame (314 bytes) Reassembled TCP (408 bytes)

File Macchina Visualizza Inserimento Dispositivi Aiuto

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

\*any

arp

No.	Time	Source	Destination	Protocol	Length	Info
6	1.023660507	PcsCompu_cb:7e:f5		ARP	44	who has 192.168.32.1? Tell 192.168.32.100
9	2.048337170	PcsCompu_cb:7e:f5		ARP	44	who has 192.168.32.1? Tell 192.168.32.100
12	3.071443912	PcsCompu_cb:7e:f5		ARP	44	who has 192.168.32.1? Tell 192.168.32.100

Frame 12: 44 bytes on wire (352 bits), 44 bytes captured (352 bits) on interface any, id 0

Linux cooked capture v1

Packet type: Sent by us (4)

Link-layer address type: Ethernet (1)

Link-layer address length: 6

Source: PcsCompu\_cb:7e:f5 (08:00:27:cb:7e:f5)

Unused: 0000

Protocol: ARP (0x0806)

Address Resolution Protocol (request)

Hardware type: Ethernet (1)

Protocol type: IPv4 (0x0800)

Hardware size: 6

Protocol size: 4

Opcode: request (1)

Sender MAC address: PcsCompu\_cb:7e:f5 (08:00:27:cb:7e:f5)

Sender IP address: 192.168.32.100

Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)

Target IP address: 192.168.32.1

0000 00 04 00 01 00 06 08 00 27 cb 7e f5 00 00 08 06 .....  
0010 00 01 08 00 06 04 00 01 08 00 27 cb 7e f5 c0 a8 .....  
0020 20 64 08 00 00 00 00 00 c0 a8 20 01 d.....

Target MAC address (arp.dst.hw\_mac), 6 bytes

Packets: 40 - Displayed: 4 (10.0%)

kali-linux-2023.3-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

\*any

arp

No.	Time	Source	Destination	Protocol	Length	Info
6	1.023660507	PcsCompu_cb:7e:f5		ARP	44	who has 192.168.32.1? Tell 192.168.32.100
9	2.048337170	PcsCompu_cb:7e:f5		ARP	44	who has 192.168.32.1? Tell 192.168.32.100
12	3.071443912	PcsCompu_cb:7e:f5		ARP	44	who has 192.168.32.1? Tell 192.168.32.100

Frame 12: 44 bytes on wire (352 bits), 44 bytes captured (352 bits) on interface any, id 0

Linux cooked capture v1

Packet type: Sent by us (4)

Link-layer address type: Ethernet (1)

Link-layer address length: 6

Source: PcsCompu\_cb:7e:f5 (08:00:27:cb:7e:f5)

Unused: 0000

Protocol: ARP (0x0806)

Address Resolution Protocol (request)

Hardware type: Ethernet (1)

Protocol type: IPv4 (0x0800)

Hardware size: 6

Protocol size: 4

Opcode: request (1)

Sender MAC address: PcsCompu\_cb:7e:f5 (08:00:27:cb:7e:f5)

Sender IP address: 192.168.32.100

Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)

Target IP address: 192.168.32.1

0000 00 04 00 01 00 06 08 00 27 cb 7e f5 00 00 08 06 .....  
0010 00 01 08 00 06 04 00 01 08 00 27 cb 7e f5 c0 a8 .....  
0020 20 64 08 00 00 00 00 00 c0 a8 20 01 d.....