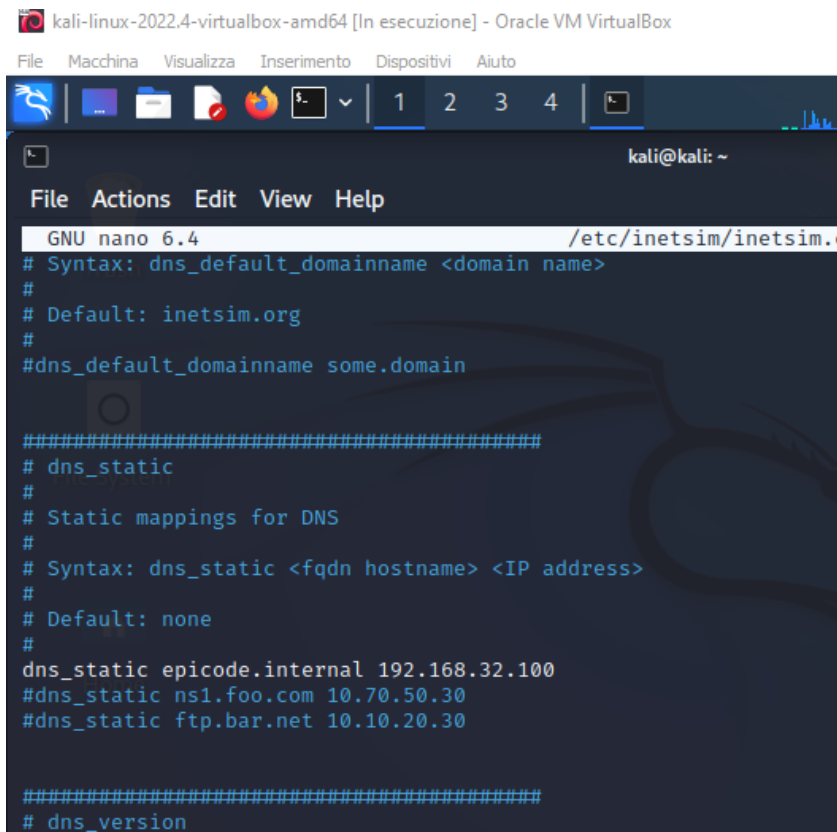


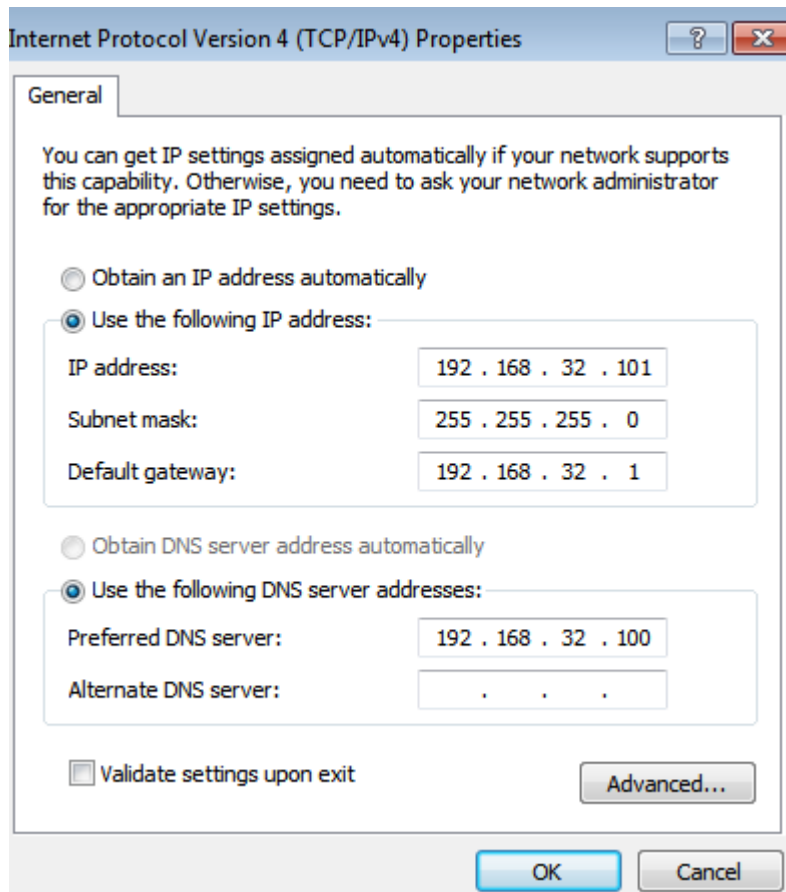
1)



```
kali-linux-2022.4-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
GNU nano 6.4 /etc/inetsim/inetsim.conf
# Syntax: dns_default_domainname <domain name>
#
# Default: inetsim.org
#
#dns_default_domainname some.domain

#####
# dns_static
#
# Static mappings for DNS
#
# Syntax: dns_static <fqdn hostname> <IP address>
#
# Default: none
#
dns_static 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
```



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

☐ Obtain an IP address automatically

☒ Use the following IP address:

IP address: 192 . 168 . 32 . 101

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 32 . 1

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

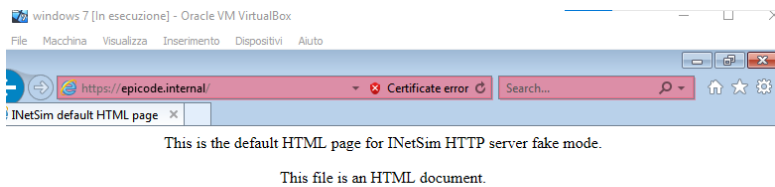
Preferred DNS server: 192 . 168 . 32 . 100

Alternate DNS server:

☐ Validate settings upon exit

Advanced...

OK Cancel



2)

| | | | | | |
|----|-------------|-------------------|----------------|---------|------------------------|
| 12 | 7.259234001 | PcsCompu_38:36:2a | ARP | 62 | Who has 192.168.32.100 |
| 13 | 7.758921983 | PcsCompu_38:36:2a | ARP | 62 | Who has 192.168.32.100 |
| 14 | 7.758940298 | PcsCompu_6b:fa:26 | ARP | 44 | 192.168.32.100 |
| 15 | 8.259480885 | PcsCompu_38:36:2a | ARP | 62 | Who has 192.168.32.100 |
| 16 | 9.530664548 | 192.168.32.101 | 192.168.32.100 | TCP | 64 49167 → 443 |
| 17 | 9.530787463 | 192.168.32.100 | 192.168.32.101 | TCP | 64 443 → 49167 |
| 18 | 9.531611551 | 192.168.32.101 | 192.168.32.100 | TCP | 62 49167 → 443 |
| 19 | 9.532268602 | 192.168.32.101 | 192.168.32.100 | TLSv1.2 | 273 Client Hello |
| 20 | 9.532302793 | 192.168.32.100 | 192.168.32.101 | TCP | 56 443 → 49167 |
| 21 | 9.565987084 | 192.168.32.101 | 192.168.32.100 | TCP | 64 49168 → 443 |

| | | |
|--|------|-------------|
| Frame 16: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface | 0000 | 00 00 00 00 |
| Linux cooked capture v1 | 0010 | 45 00 00 00 |
| Packet type: Unicast to us (0) | 0020 | c0 a8 20 00 |
| Link-layer address type: Ethernet (1) | 0030 | 70 02 20 00 |
| Link-layer address length: 6 | | |
| Source: PcsCompu_38:36:2a (08:00:27:38:36:2a) | | |
| Unused: 0000 | | |
| Protocol: IPv4 (0x0800) | | |
| Internet Protocol Version 4, Src: 192.168.32.101, Dst: 192.168.32.100 | | |
| Transmission Control Protocol Src Port: 49167 Dst Port: 443 Seq: 0 | | |

MAC ADDRESS SOURCE (WINDOWS) 08:00:27:38:36:2 a

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-------------|-------------------|----------------|----------|--------|---------------|
| 10 | 6.284131704 | 192.168.32.101 | 192.168.32.100 | DNS | 74 | Standard quer |
| 11 | 6.303442715 | 192.168.32.100 | 192.168.32.101 | DNS | 90 | Standard quer |
| 12 | 7.259234661 | PcsCompu_38:36:2a | | ARP | 62 | Who has 192.1 |
| 13 | 7.758921983 | PcsCompu_38:36:2a | | ARP | 62 | Who has 192.1 |
| 14 | 7.758940298 | PcsCompu_6b:fa:26 | | ARP | 44 | 192.168.32.10 |
| 15 | 8.259480885 | PcsCompu_38:36:2a | | ARP | 62 | Who has 192.1 |
| 16 | 9.530664548 | 192.168.32.101 | 192.168.32.100 | TCP | 64 | 49167 → 443 [|
| 17 | 9.530787463 | 192.168.32.100 | 192.168.32.101 | TCP | 64 | 443 → 49167 [|
| 18 | 9.531611551 | 192.168.32.101 | 192.168.32.100 | TCP | 62 | 49167 → 443 [|
| 19 | 9.532268602 | 192.168.32.101 | 192.168.32.100 | TLSv1.2 | 273 | Client Hello |
| 20 | 9.532302793 | 192.168.32.100 | 192.168.32.101 | TCP | 56 | 443 → 49167 [|
| 21 | 9.565987084 | 192.168.32.101 | 192.168.32.100 | TCP | 64 | 49168 → 443 [|

▶ Frame 17: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface
 - Linux cooked capture v1
 Packet type: Sent by us (4)
 Link-layer address type: Ethernet (1)
 Link-layer address length: 6
 Source: PcsCompu_6b:fa:26 (08:00:27:6b:fa:26)
 Unused: 0000
 Protocol: IPv4 (0x0800)
 ▶ Internet Protocol Version 4, Src: 192.168.32.100, Dst: 192.168.32.101
 ▶ Transmission Control Protocol, Src Port: 443, Dst Port: 49167, Seq: 0, A

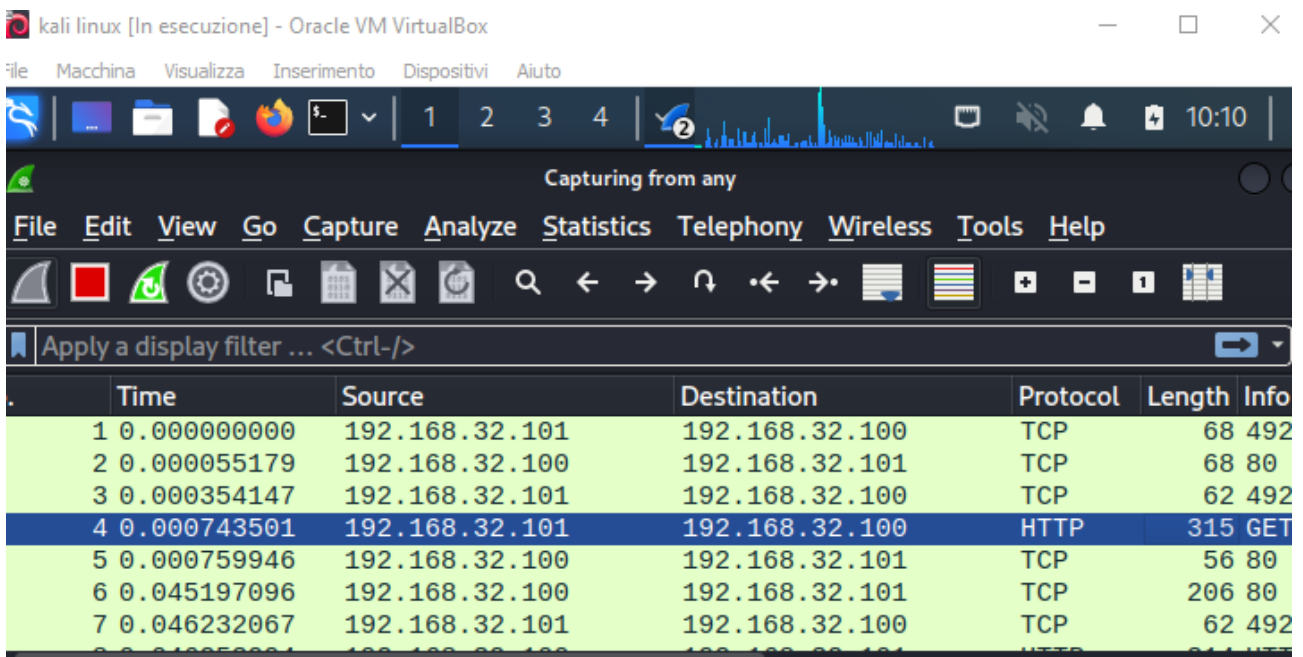
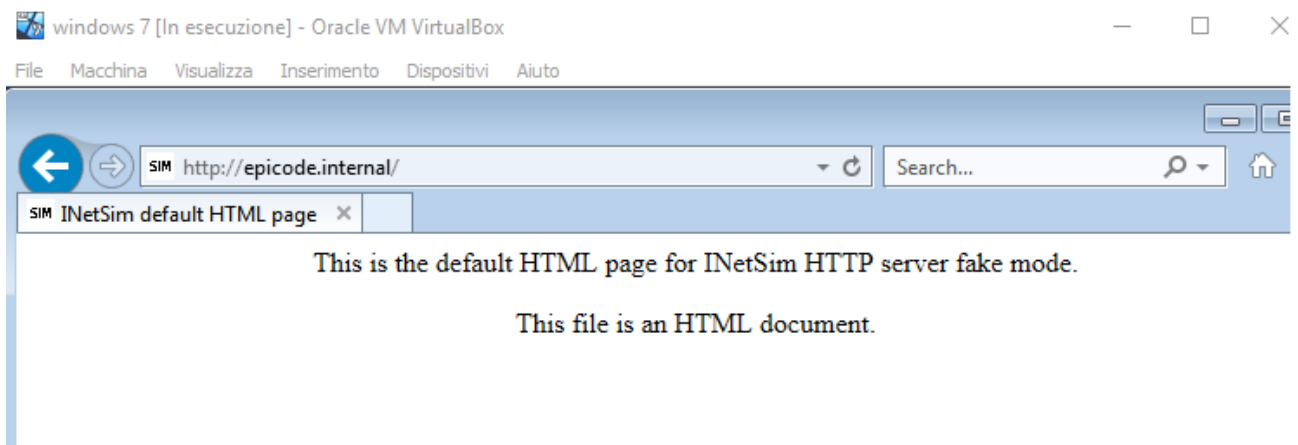
MAC ADDRESS SOURCE (linux) : 08:00:27:6b : fa :26

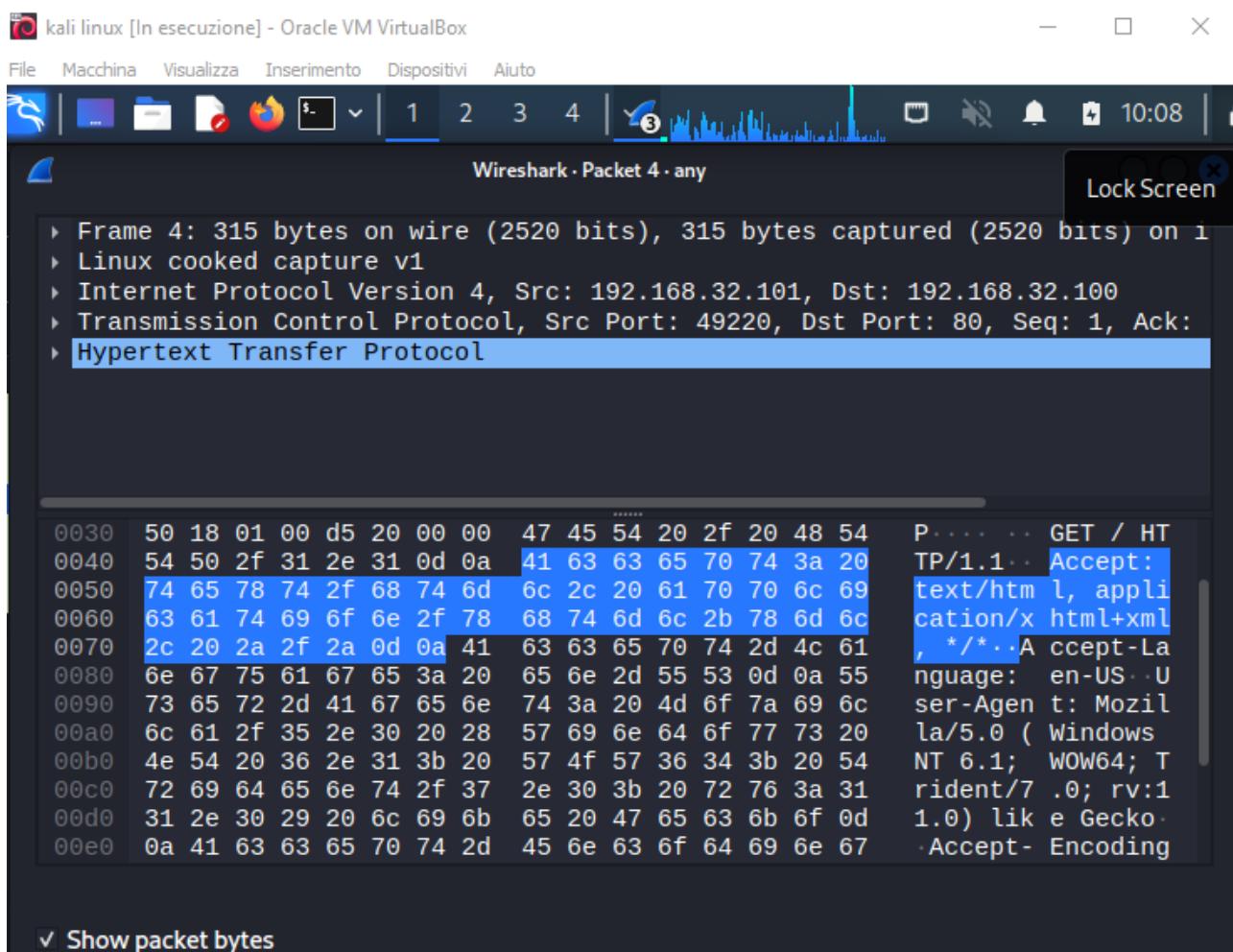
| Wireshark - Packet 16 - any | | | | | | | | | |
|--|-------------------------|-------------------------|----------------|--|--|--|--|--|--|
| Frame 16: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface Section number: 1 Interface id: 0 (any) Interface name: any Encapsulation type: Linux cooked-mode capture v1 (25) Arrival Time: Jan 27, 2023 09:46:20.515661709 EST [Time shift for this packet: 0.000000000 seconds] Epoch Time: 1674830780.515661709 seconds [Time delta from previous captured frame: 1.271183663 seconds] | | | | | | | | | |
| 0000 | 00 00 00 01 00 06 08 00 | 27 38 36 2a 00 00 08 00 | '86*.... | | | | | | |
| 0010 | 45 00 00 30 01 14 40 00 | 80 06 37 9a c0 a8 20 65 | E..0..@..7...e | | | | | | |
| 0020 | c0 a8 20 64 c0 0f 01 bb | eb 8f 54 a7 00 00 00 00 | ..d...T..... | | | | | | |
| 0030 | 70 02 20 00 9f 03 00 00 | 02 04 05 b4 01 01 04 02 | p..... | | | | | | |

Contenuto https cifrato

3)

```
kali@kali: ~  
File Actions Edit View Help  
GNU nano 6.4 /etc/inetsim/inetsim.conf *  
  
#####  
# start_service  
#  
# The services to start  
#  
# Syntax: start_service <service name>  
#  
# Default: none  
#  
# Available service names are:  
# dns, http, smtp, pop3, tftp, ftp, ntp, time_tcp,  
# time_udp, daytime_tcp, daytime_udp, echo_tcp,  
# echo_udp, discard_tcp, discard_udp, quotd_tcp,  
# 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
```





La Differenza sostanziale è l'utilizzo di un canale di comunicazione cifrato (TLS) nel HTTPS e ne consegue che il messaggio non potrà essere letto, ma sarà un insieme di lettere, numeri, simboli senza significato; mentre nell'http non troviamo tls, ed inoltre il messaggio del pacchetto risulterà chiaramente leggibile.