PROGETTO 17/06/2023 Christian Brenci

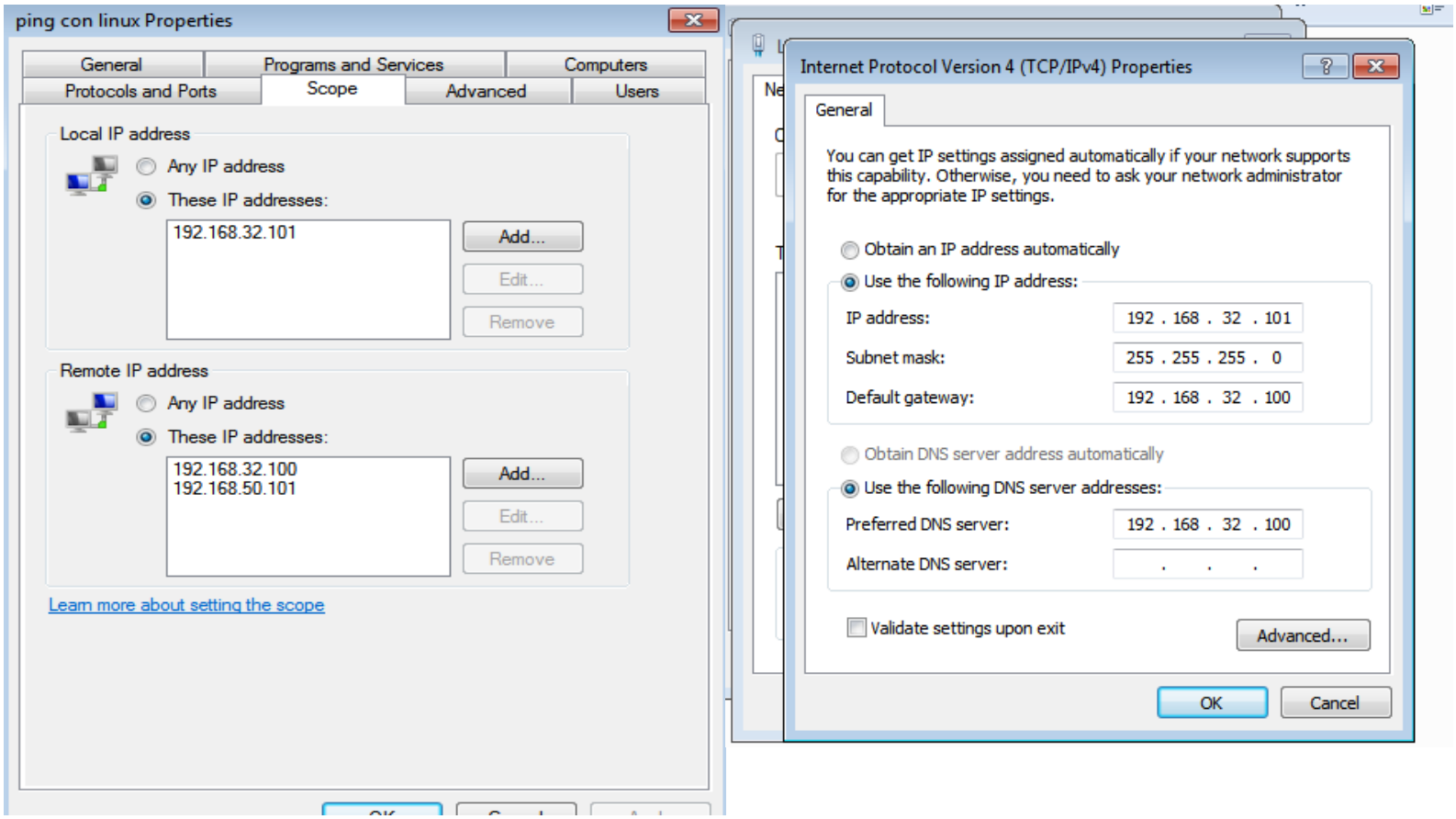
Come da prima richiesta sono andato a cambiare gli indirizzi IP sulle macchine Linux e Kali come nelle immagini.

```
┌──(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:fec7:e136  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:c7:e1:36  txqueuelen 1000  (Ethernet)
        RX packets 3472  bytes 339603 (331.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1477  bytes 296254 (289.3 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
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 76  bytes 4360 (4.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 76  bytes 4360 (4.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
C:\Windows\system32\cmd.exe
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\christian>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::b504:bc94:9c37:423a%11
   IPv4 Address. . . . . . . . . . . : 192.168.32.101
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.32.100

Tunnel adapter isatap.{C92B4E13-41E2-482F-A458-A603C6CCDAB7}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\christian>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=1ms 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 = 0ms, Maximum = 2ms, Average = 1ms
```

Successivamente ho aggiornato le Policy del firewall della macchina WIN(client). in modo tale che le macchine, nonostante la presenza di quest'ultimo, potessero comunicare tra di loro, ed infine ho assegnato come default gateway e indirizzo del server DNS l'IP quello della macchina di Kali (server).

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.32.101 -c 4
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=1.64 ms
64 bytes from 192.168.32.101: icmp_seq=2 ttl=128 time=0.996 ms
64 bytes from 192.168.32.101: icmp_seq=3 ttl=128 time=0.659 ms
64 bytes from 192.168.32.101: icmp_seq=4 ttl=128 time=1.08 ms

--- 192.168.32.101 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3035ms
```



Una volta fatto ciò, mi sono spostato sulla macchina server, e tramite il pannello di controllo ho configurato le impostazioni dell'utility "ifconfig" impostando il "Bind address", il "dns default ip" ed infine il "dns static" con l'indirizzo della macchina server Kali(192.168.32.100), salvo per quest'ultimo a cui ho anche assegnato anche un hostname chiamato "epicode.internal"

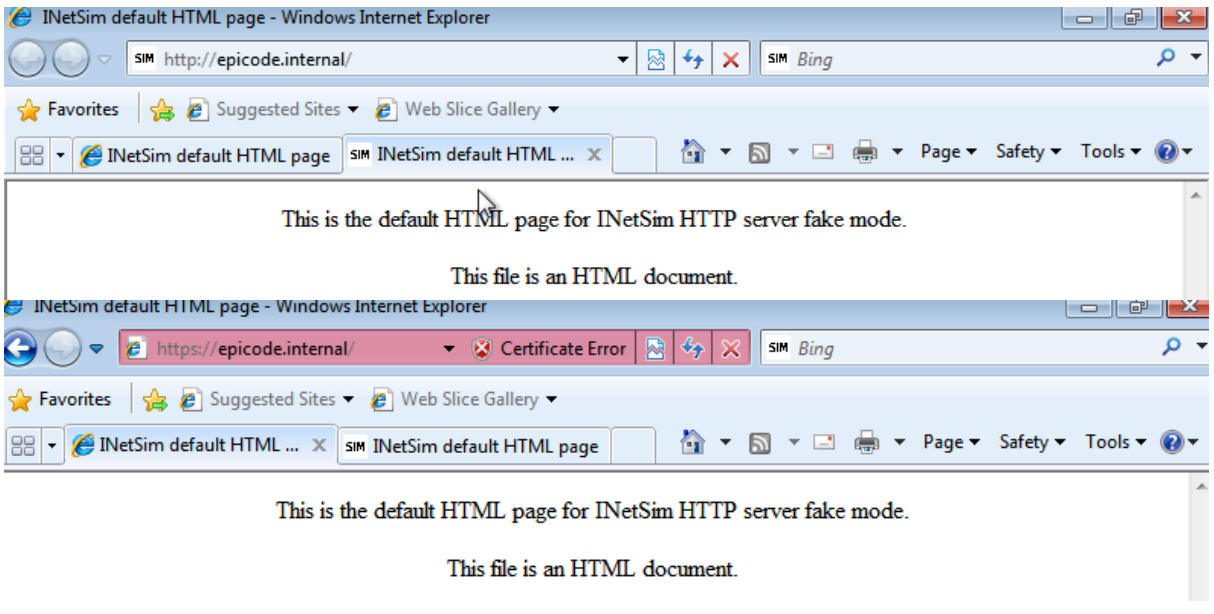
```
##################################################
# service_bind_address
#
# IP address to bind services to
#
# Syntax: service_bind_address <IP address>
#
# Default: 127.0.0.1
#
service_bind_address 192.168.32.100
```

```
##################################################
# 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
```

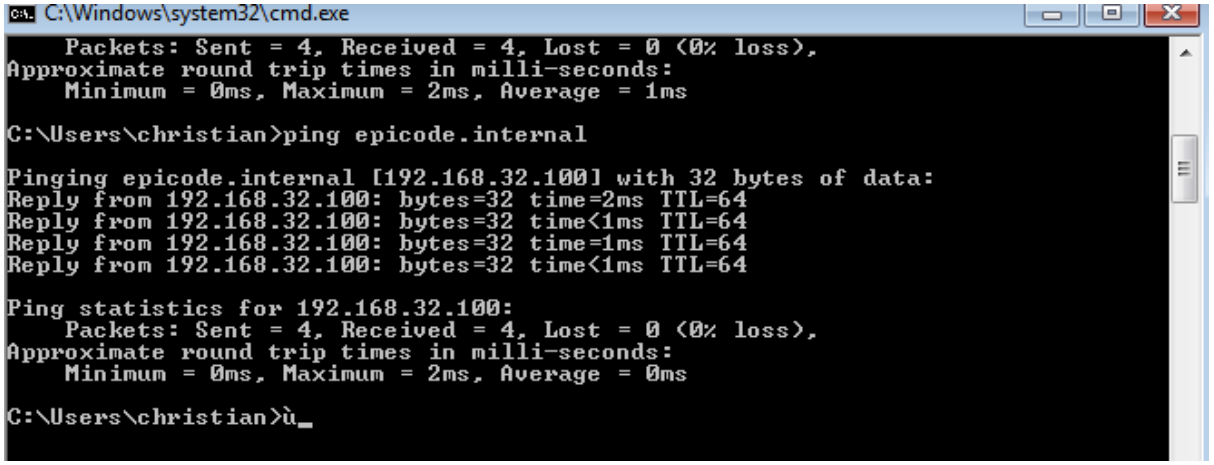
A questo punto ho eseguito il comando “sudo inetsim” ed ho avviato la simulazione.

```
┌──(kali㉿kali)-[~]
└─$ sudo inetsim
[sudo] password for kali:
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 148677) ===
Session ID:     148677
Listening on:   192.168.32.100
Real Date/Time: 2023-06-17 10:28:17
Fake Date/Time: 2023-06-17 10:28:17 (Delta: 0 seconds)
 Forking services...
  * https_443_tcp - started (PID 148689)
  * pop3s_995_tcp - started (PID 148693)
  * http_80_tcp - started (PID 148688)
  * dns_53_tcp_udp - started (PID 148687)
  * time_37_tcp - started (PID 148702)
  * ftps_990_tcp - started (PID 148695)
  * irc_6667_tcp - started (PID 148697)
  * daytime_13_tcp - started (PID 148704)
  * ntp_123_udp - started (PID 148698)
  * daytime_13_udp - started (PID 148705)
  * echo_7_tcp - started (PID 148706)
  * smtp_25_tcp - started (PID 148690)
  * echo_7_udp - started (PID 148707)
  * finger_79_tcp - started (PID 148699)
  * syslog_514_udp - started (PID 148701)
  * ident_113_tcp - started (PID 148700)
  * pop3_110_tcp - started (PID 148692)
  * quotd_17_udp - started (PID 148711)
  * time_37_udp - started (PID 148703)
  * chargen_19_tcp - started (PID 148712)
  * quotd_17_tcp - started (PID 148710)
  * tftp_69_udp - started (PID 148696)
  * dummy_1_udp - started (PID 148715)
  * chargen_19_udp - started (PID 148713)
  * ftp_21_tcp - started (PID 148694)
  * discard_9_tcp - started (PID 148708)
  * dummy_1_tcp - started (PID 148714)
  * smtps_465_tcp - started (PID 148691)
  * discard_9_udp - started (PID 148709)
 done.
Simulation running.
```

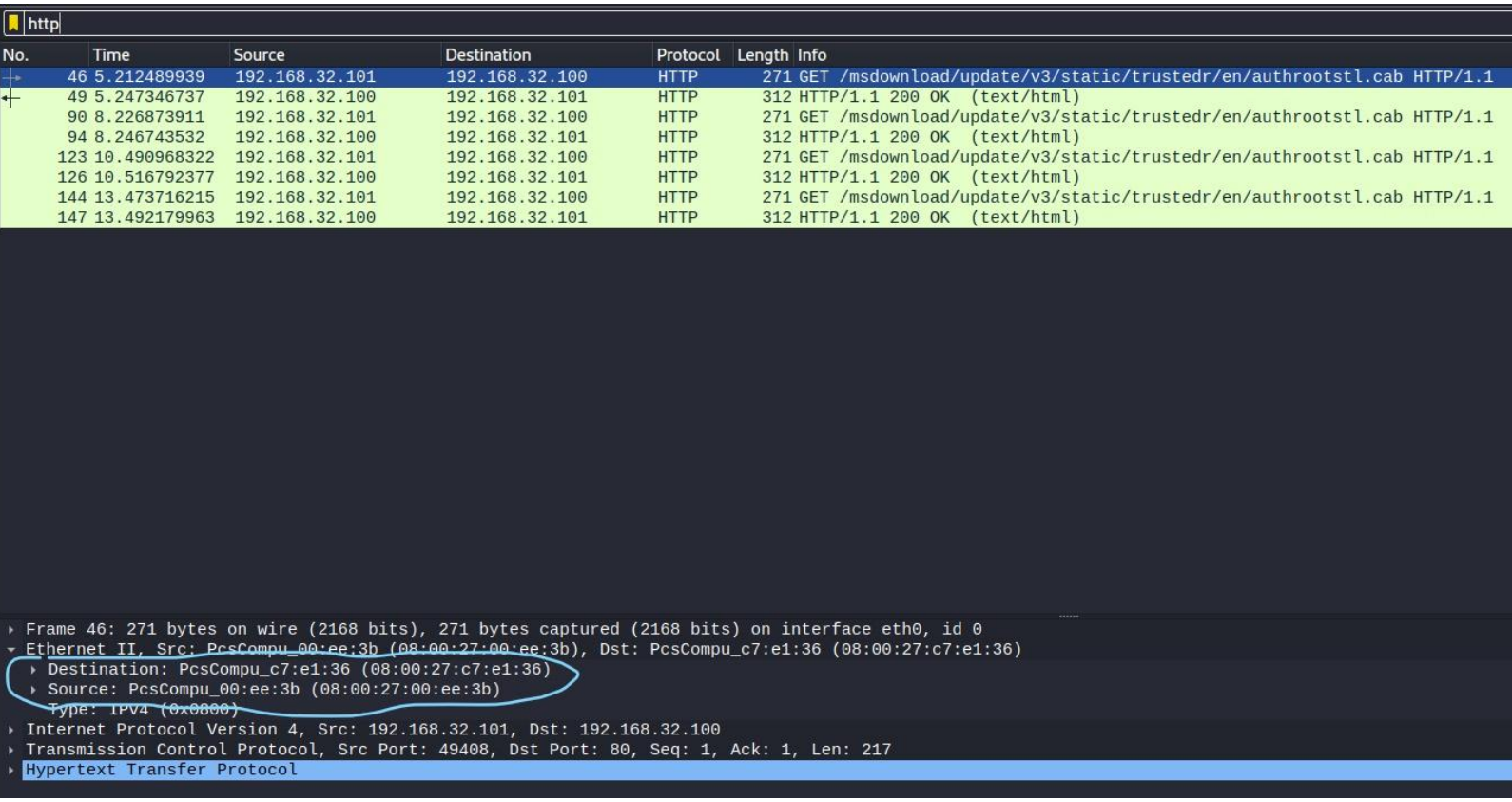
nel mentre ho aperto il programma “Wireshark” pronto per catturare il traffico di pacchetti che stava per arrivare. Usando la macchina client, ho aperto il web browser ed ho fatto una ricerca del sito “epicode.internal” tramite protocollo HTTP, e successivamente usando il protocollo HTTPS, così facendo wireshark ha avuto modo di intercettare il traffico di pacchetti,



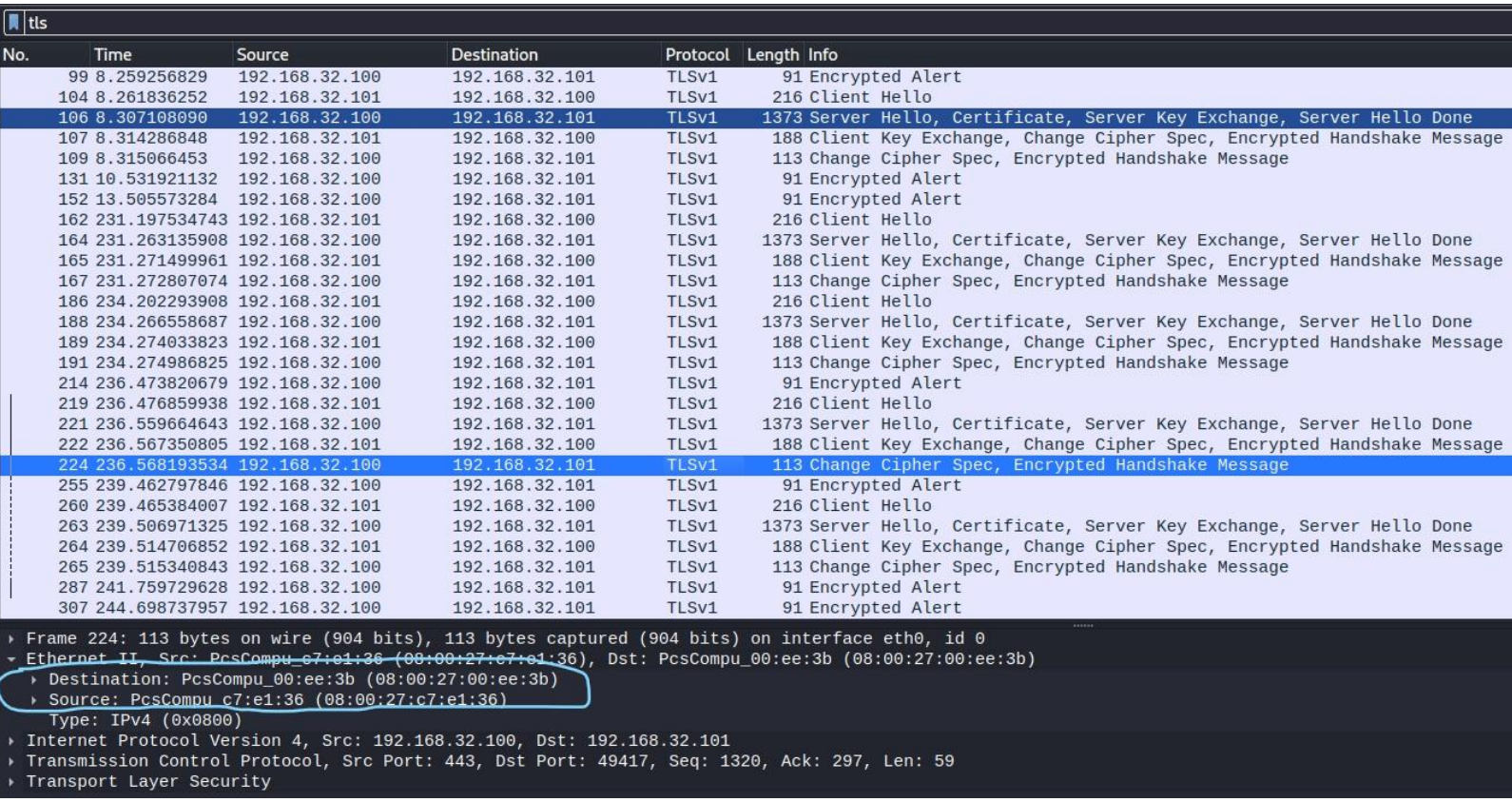
e come ultimo passo ho pingato l'hostname "epicode.internal" sul CMD di WIN.



Spostandosi sulla macchina server, vediamo su wireshark i pacchetti catturati scegliendo quelli con i protocolli "HTTP" e "TLSv1" (HTTPS). Ovviamente la principale differenza sta nel contenuto "info", essendo una protocollo non cifrato http, possiamo vedere tutta la sua history di desinenza "GET /msdownload/update/v3Vstatic/trustedr/en/authrootstl.cab HTTP/1.1" mentre essendo https un protocollo cifrato quest'ultima voce non verrà visualizzata ma verranno visualizzati gli allert di cifratura.



Infine nella voce Ethernet cliccando sul menù a tendina possiamo vedere come cambiano i MAC address d'origine e di destinazione.


tls
No. Time Source Destination Protocol Length Info
99 8.259256829 192.168.32.100 192.168.32.101 TLSv1 91 Encrypted Alert
104 8.261836252 192.168.32.101 192.168.32.100 TLSv1 216 Client Hello
106 8.307108090 192.168.32.100 192.168.32.101 TLSv1 1373 Server Hello, Certificate, Server Key Exchange, Server Hello Done
107 8.314286848 192.168.32.101 192.168.32.100 TLSv1 188 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
109 8.315066453 192.168.32.100 192.168.32.101 TLSv1 113 Change Cipher Spec, Encrypted Handshake Message
131 10.531921132 192.168.32.100 192.168.32.101 TLSv1 91 Encrypted Alert
152 13.505573284 192.168.32.100 192.168.32.101 TLSv1 91 Encrypted Alert
162 231.197534743 192.168.32.101 192.168.32.100 TLSv1 216 Client Hello
164 231.263135908 192.168.32.100 192.168.32.101 TLSv1 1373 Server Hello, Certificate, Server Key Exchange, Server Hello Done
165 231.271499961 192.168.32.101 192.168.32.100 TLSv1 188 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
167 231.272807074 192.168.32.100 192.168.32.101 TLSv1 113 Change Cipher Spec, Encrypted Handshake Message
186 234.202293908 192.168.32.101 192.168.32.100 TLSv1 216 Client Hello
188 234.266558687 192.168.32.100 192.168.32.101 TLSv1 1373 Server Hello, Certificate, Server Key Exchange, Server Hello Done
189 234.274033823 192.168.32.101 192.168.32.100 TLSv1 188 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
191 234.274986825 192.168.32.100 192.168.32.101 TLSv1 113 Change Cipher Spec, Encrypted Handshake Message
214 236.473820679 192.168.32.100 192.168.32.101 TLSv1 91 Encrypted Alert
219 236.476859938 192.168.32.101 192.168.32.100 TLSv1 216 Client Hello
221 236.559664643 192.168.32.100 192.168.32.101 TLSv1 1373 Server Hello, Certificate, Server Key Exchange, Server Hello Done
222 236.567350805 192.168.32.101 192.168.32.100 TLSv1 188 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
224 236.568193534 192.168.32.100 192.168.32.101 TLSv1 113 Change Cipher Spec, Encrypted Handshake Message
255 239.462797846 192.168.32.100 192.168.32.101 TLSv1 91 Encrypted Alert
260 239.465384007 192.168.32.101 192.168.32.100 TLSv1 216 Client Hello
263 239.506971325 192.168.32.100 192.168.32.101 TLSv1 1373 Server Hello, Certificate, Server Key Exchange, Server Hello Done
264 239.514706852 192.168.32.101 192.168.32.100 TLSv1 188 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
265 239.515340843 192.168.32.100 192.168.32.101 TLSv1 113 Change Cipher Spec, Encrypted Handshake Message
287 241.759729628 192.168.32.100 192.168.32.101 TLSv1 91 Encrypted Alert
307 244.698737957 192.168.32.100 192.168.32.101 TLSv1 91 Encrypted Alert
Frame 224: 113 bytes on wire (904 bits), 113 bytes captured (904 bits) on interface eth0, id 0
Ethernet II, Src: PcsCompu_c7:e1:36 (08:00:27:c7:e1:36), Dst: PcsCompu_00:ee:3b (08:00:27:00:ee:3b)
Destination: PcsCompu_00:ee:3b (08:00:27:00:ee:3b)
Source: PcsCompu_c7:e1:36 (08:00:27:c7:e1:36)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.32.100, Dst: 192.168.32.101
Transmission Control Protocol, Src Port: 443, Dst Port: 49417, Seq: 1320, Ack: 297, Len: 59
Transport Layer Security