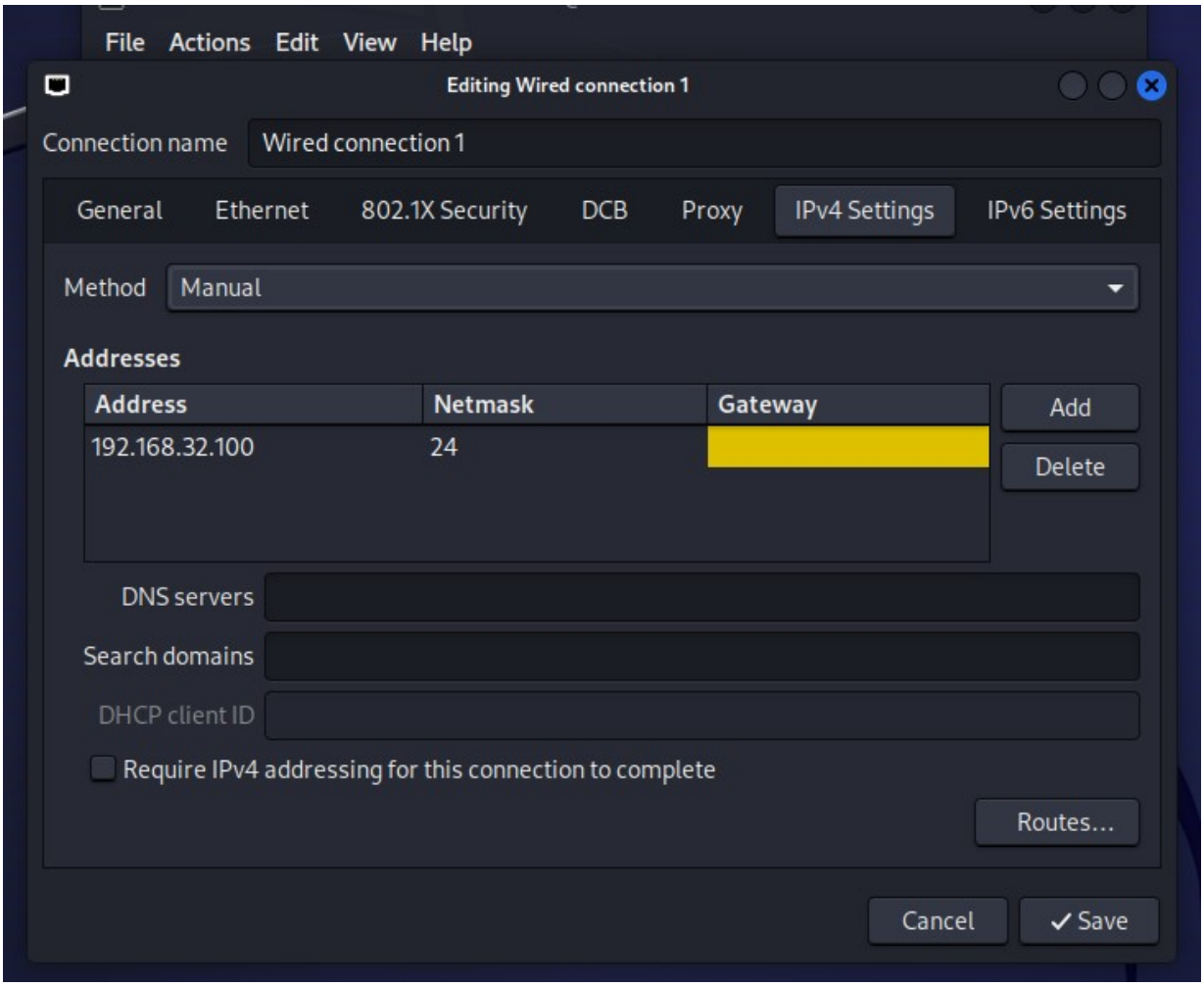
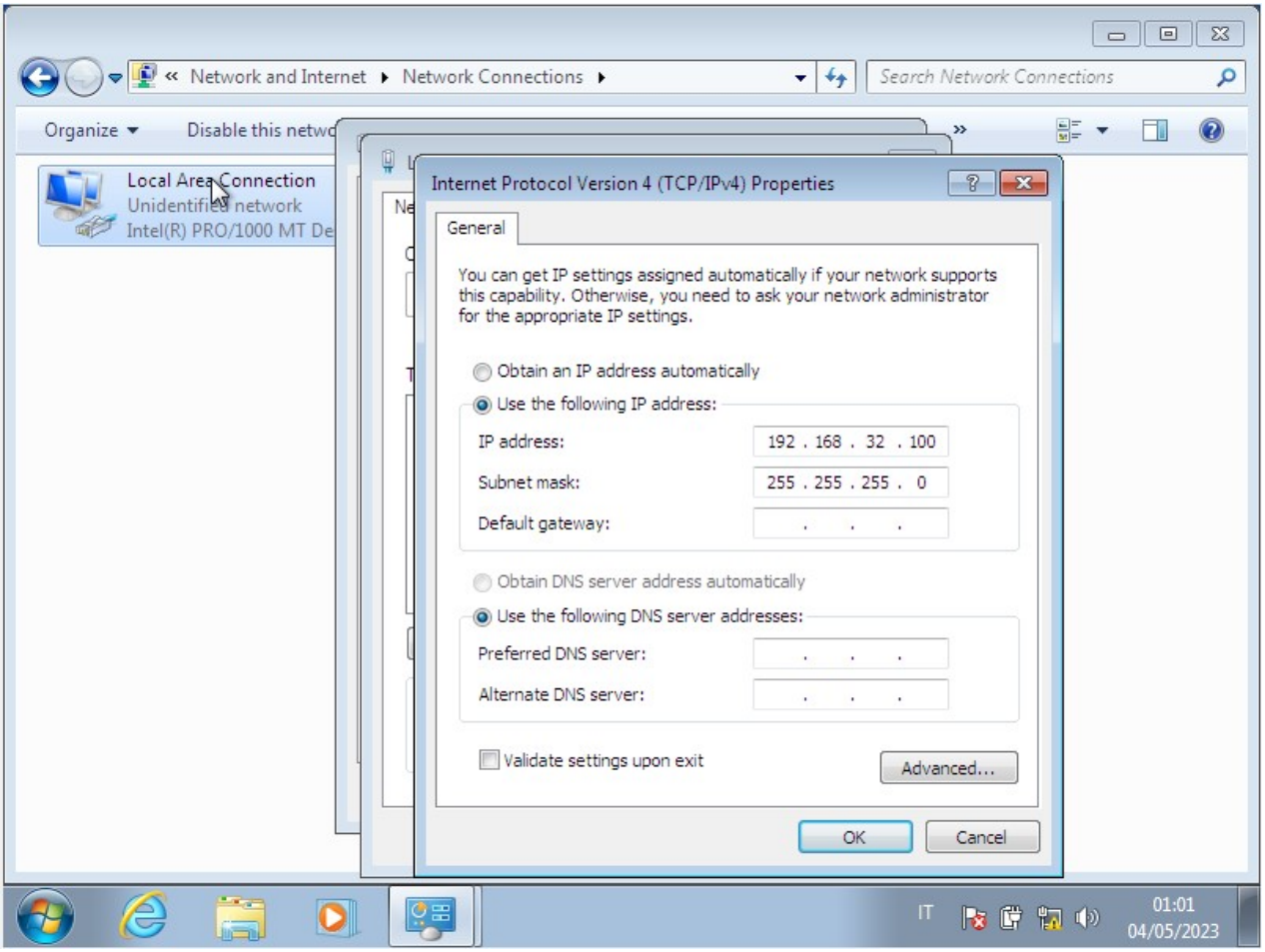
ESERCIZIO

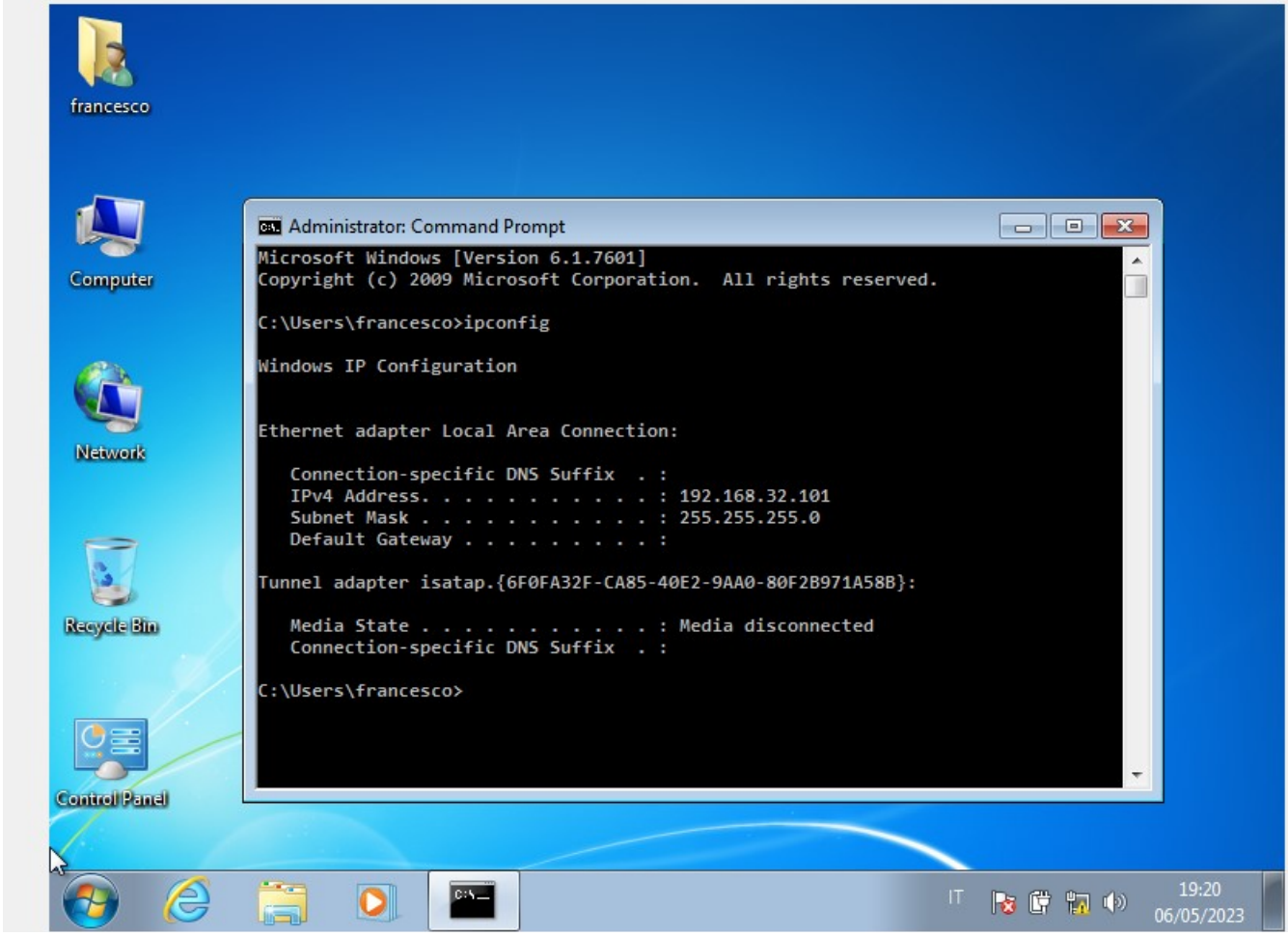
Per la creazione della rete complessa ho dovuto eseguire questi passaggi:

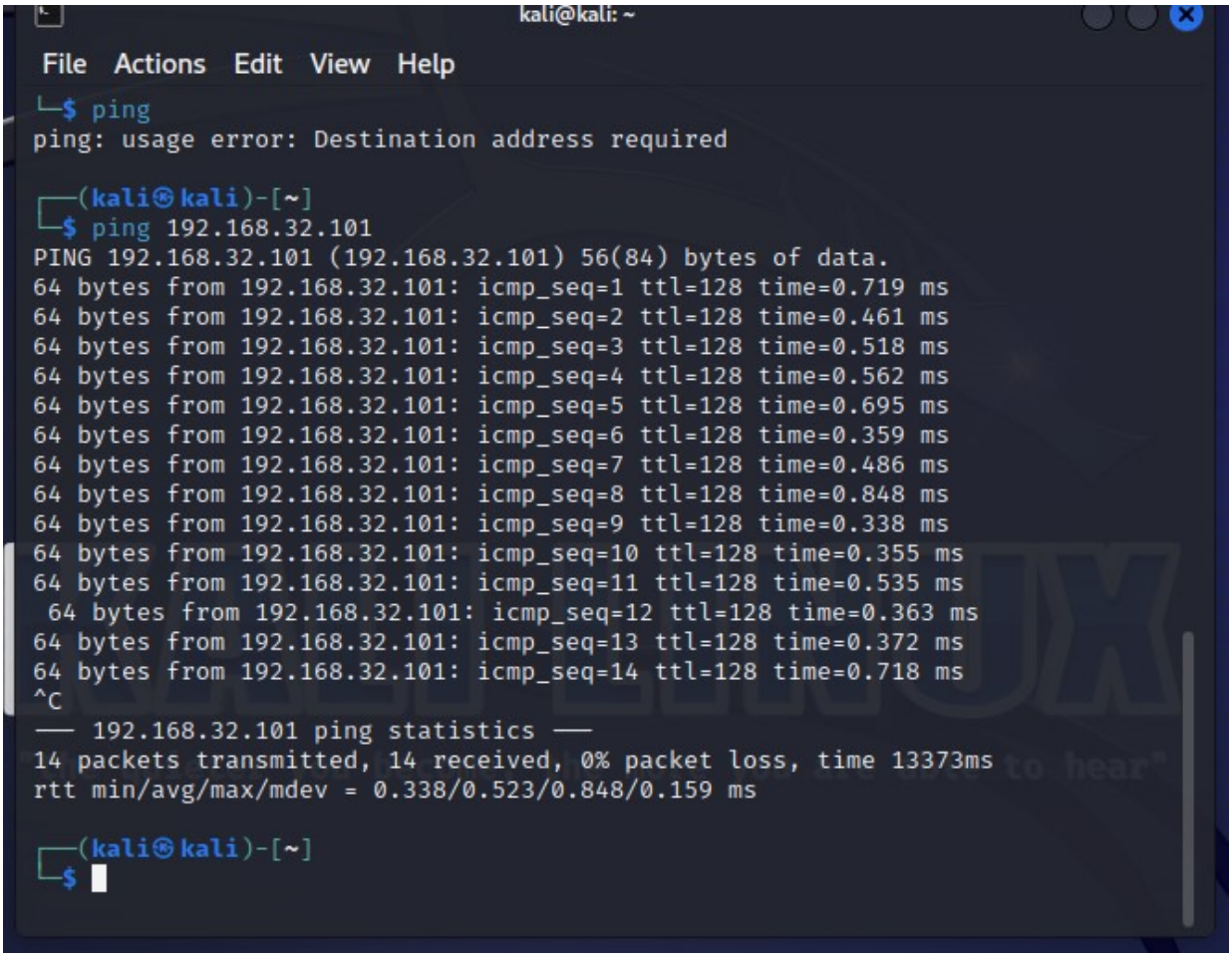
1) In questo primo passaggio ho impostato gli indirizzi IP per Kali Linux (192.168.32.100) e Windows7(192.168.32.101).

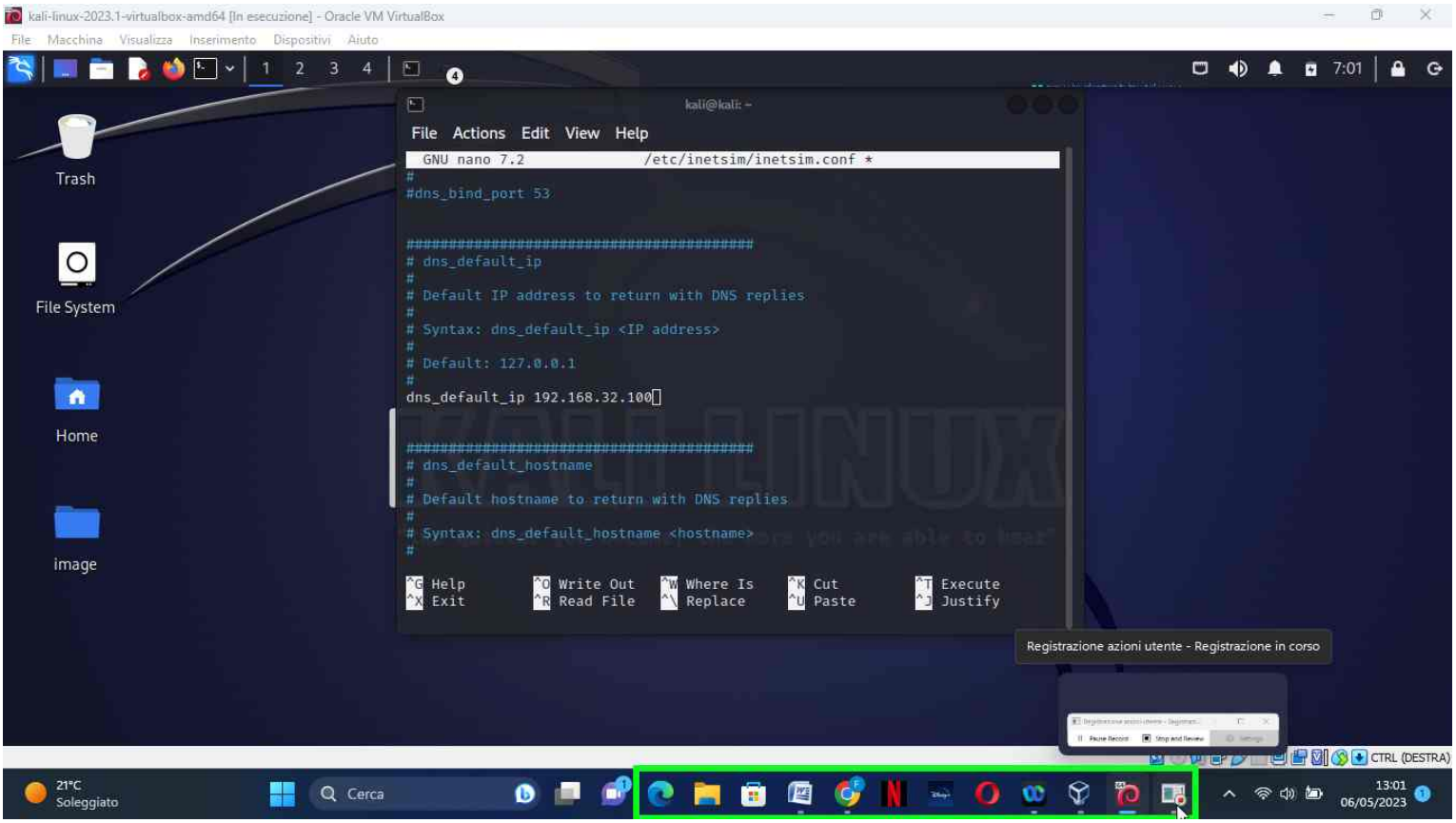

File Actions Edit View Help
Editing Wired connection 1
Connection name
Wired connection 1
General
Ethernet
802.1X Security
DCB
Proxy
IPv4 Settings
IPv6 Settings
Method
Manual
Addresses
Address
Netmask
Gateway
192.168.32.100
24
Add
Delete
DNS servers
Search domains
DHCP client ID
Require IPv4 addressing for this connection to complete
Routes...
Cancel
Save



2)Una volta impostati gli indirizzi IP, tramite il terminale di windows7 e con quello di kali linux ho visto, con la combinazione ping +IP, se i due sistemi operativi comunicavano tra di loro.


francesco
Computer
Network
Recycle Bin
Control Panel
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\francesco>ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . :
IPv4 Address. . . . . : 192.168.32.101
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
Tunnel adapter isatap.{6F0FA32F-CA85-40E2-9AA0-80F2B971A58B}:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
C:\Users\francesco>
IT
19:20
06/05/2023


kali@kali: ~
File Actions Edit View Help
└─$ ping
ping: usage error: Destination address required
┌──(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=0.719 ms
64 bytes from 192.168.32.101: icmp_seq=2 ttl=128 time=0.461 ms
64 bytes from 192.168.32.101: icmp_seq=3 ttl=128 time=0.518 ms
64 bytes from 192.168.32.101: icmp_seq=4 ttl=128 time=0.562 ms
64 bytes from 192.168.32.101: icmp_seq=5 ttl=128 time=0.695 ms
64 bytes from 192.168.32.101: icmp_seq=6 ttl=128 time=0.359 ms
64 bytes from 192.168.32.101: icmp_seq=7 ttl=128 time=0.486 ms
64 bytes from 192.168.32.101: icmp_seq=8 ttl=128 time=0.848 ms
64 bytes from 192.168.32.101: icmp_seq=9 ttl=128 time=0.338 ms
64 bytes from 192.168.32.101: icmp_seq=10 ttl=128 time=0.355 ms
64 bytes from 192.168.32.101: icmp_seq=11 ttl=128 time=0.535 ms
64 bytes from 192.168.32.101: icmp_seq=12 ttl=128 time=0.363 ms
64 bytes from 192.168.32.101: icmp_seq=13 ttl=128 time=0.372 ms
64 bytes from 192.168.32.101: icmp_seq=14 ttl=128 time=0.718 ms
^C
— 192.168.32.101 ping statistics —
14 packets transmitted, 14 received, 0% packet loss, time 13373ms
rtt min/avg/max/mdev = 0.338/0.523/0.848/0.159 ms
┌──(kali㉿kali)-[~]
└─$

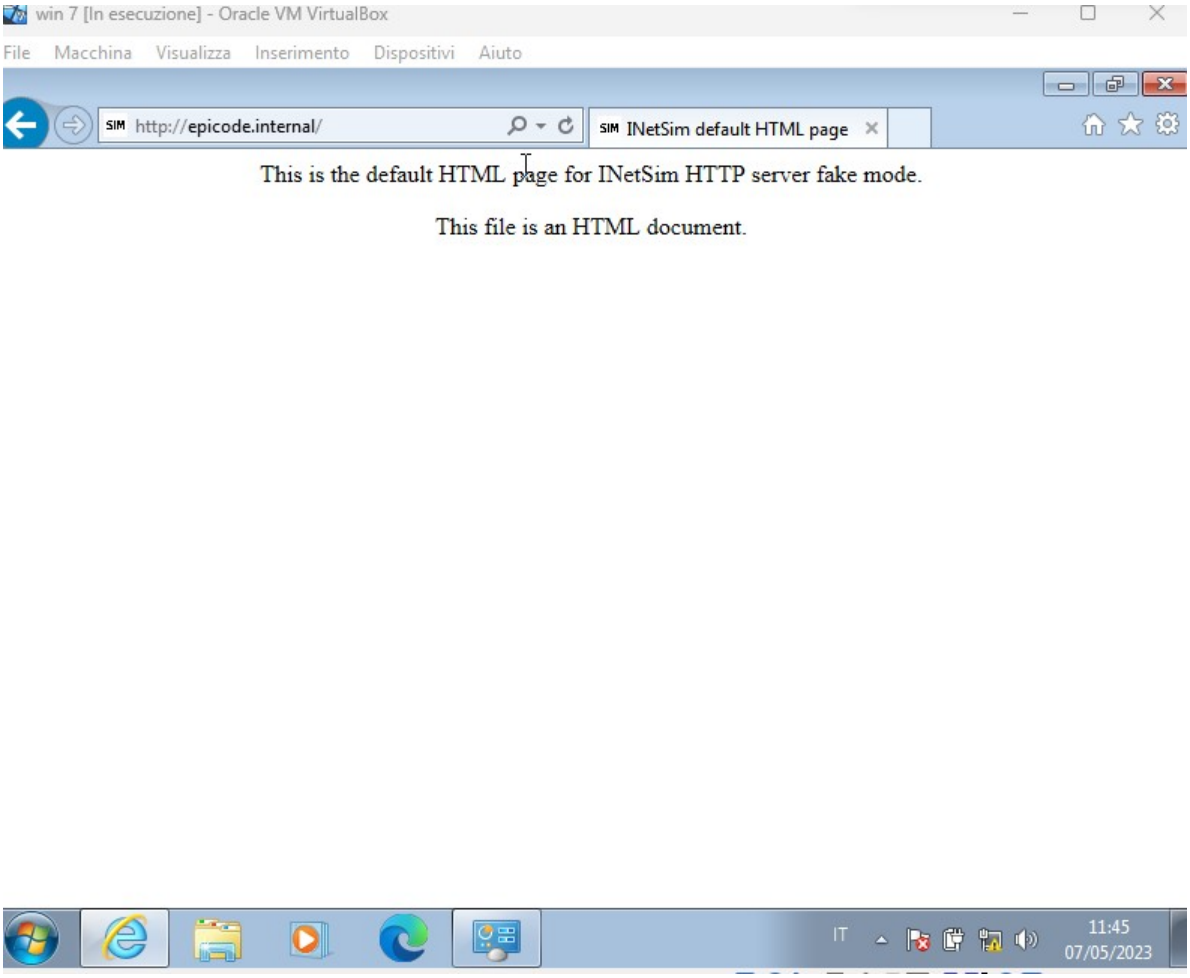


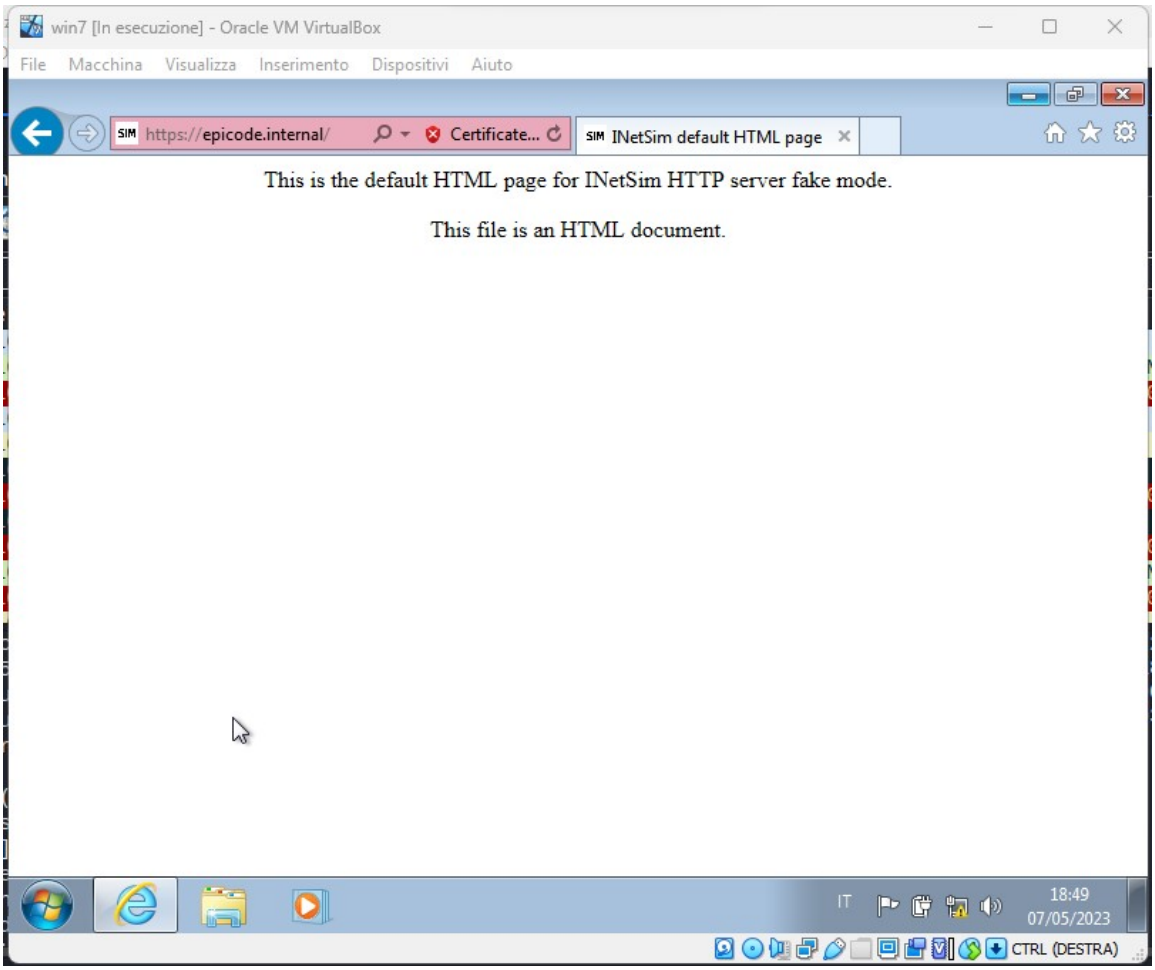
3)In questa terza fase ho attivato i server DNS e http tramite il software InetSim su kali linux, ma prima di attivare i server ho dovuto fare la configurazione del software.

Per configurare il software, ho aperto una finestra di terminale ho inserito la combinazione (cp /etc/inetsim/inetsim.conf /etc/inetsim/inetsim.conf.orig nano /etc/inetsim/inetsim.conf) si è aperta la finestra delle impostazioni poi ho inserito IP: 192.168.32.100.

Finito di configurare il software, sempre dalla finestra delle informazioni, ho attivato i server http e DNS, assegnando gli IP192.168.32.100 e il dominio Epicode.Internal.

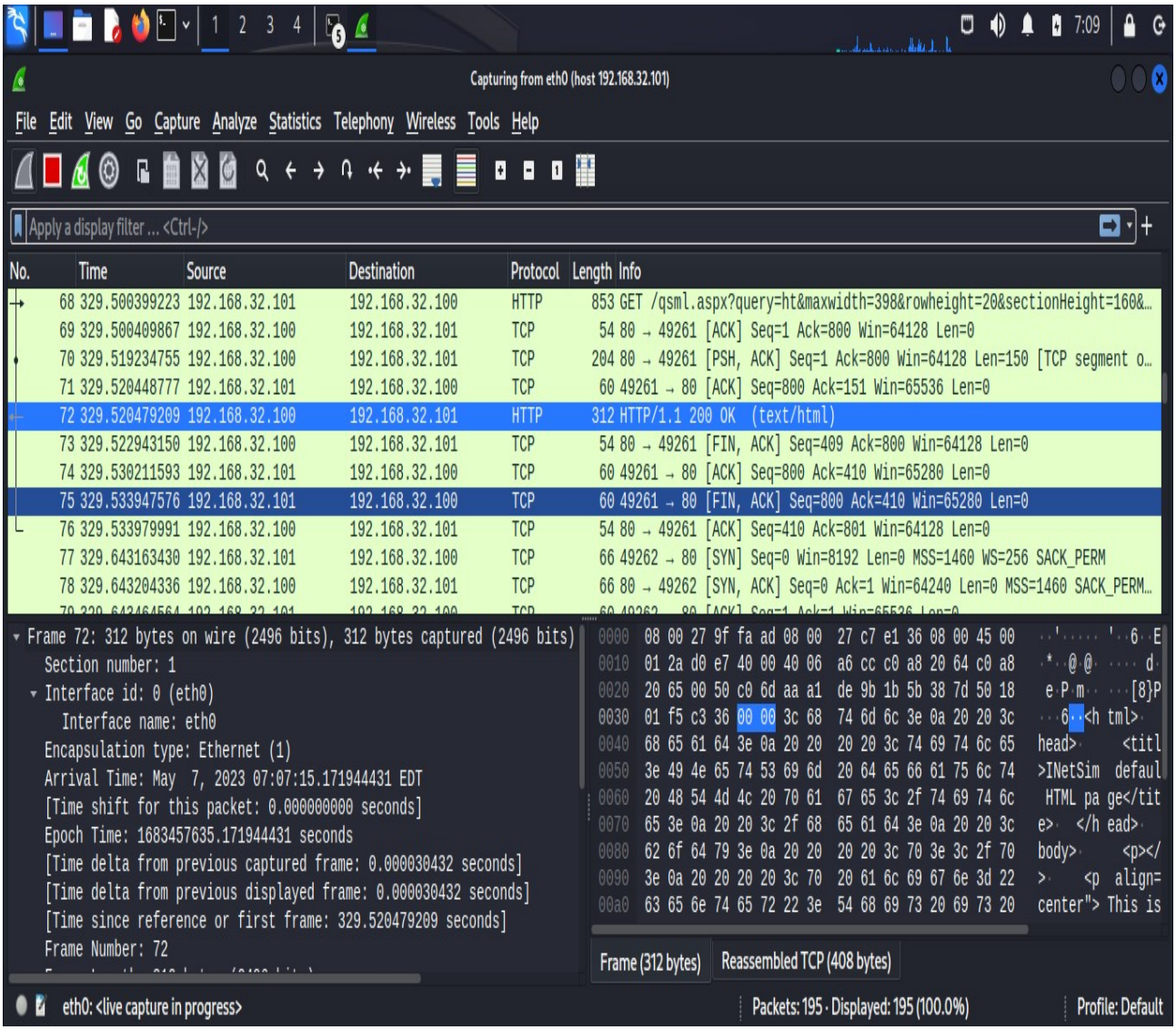
4)Una volta impostati su kali linux i server DNS, http e https, da windows ho aperto una pagina web, cliccando sulla barra di ricerca e scrivendo “Epicode.Internal” mi ha perto la pagina web. Come si può vedere nella prima foto ho fatto la prova con il protocollo http, invece nella seconda foto ho fatto la prova con il protocollo https.

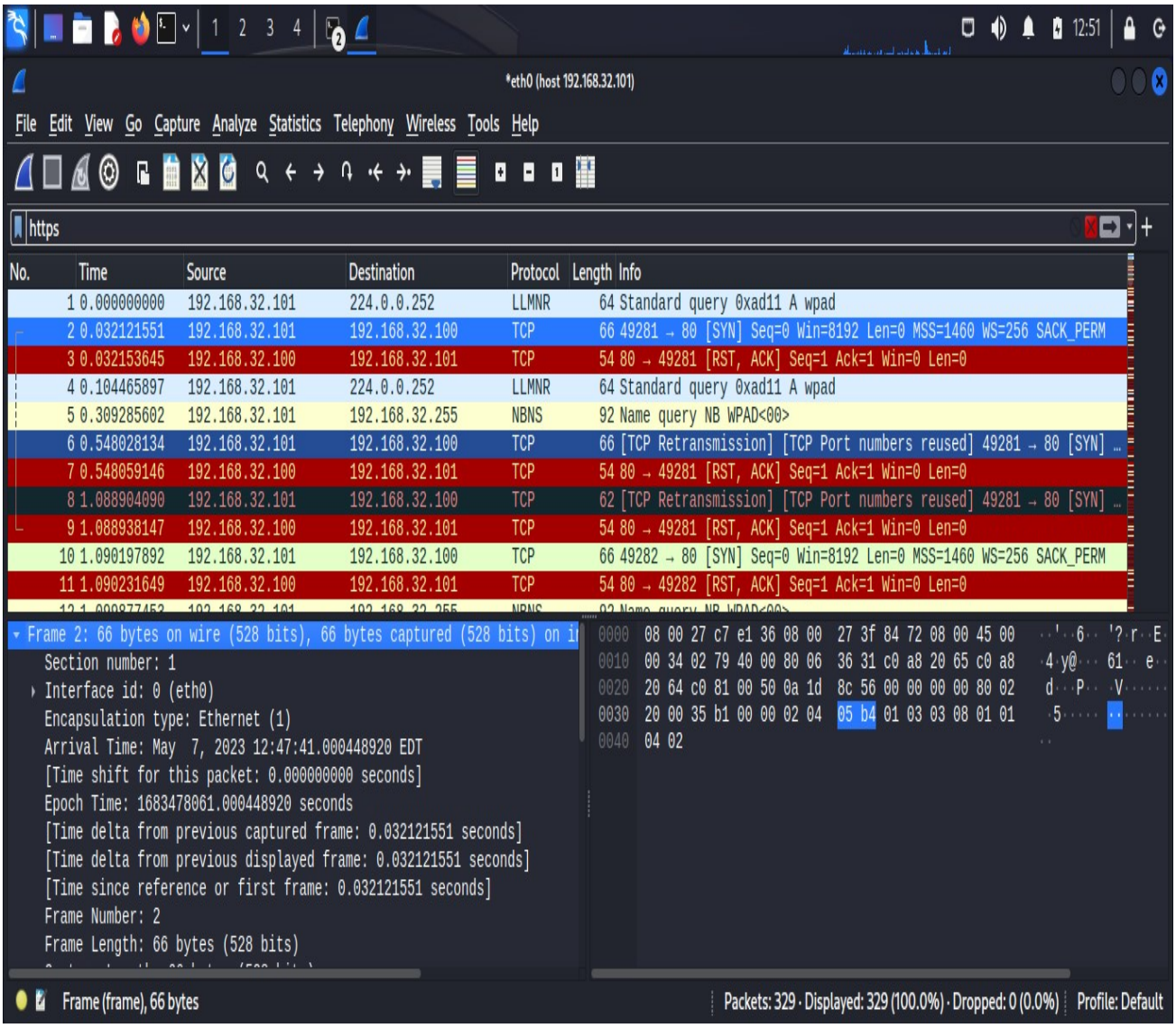

win 7 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
http://epicode.internal/
INetSim default HTML page
This is the default HTML page for INetSim HTTP server fake mode.
This file is an HTML document.
IT
11:45
07/05/2023



5) Nell'ultima fase dell'esercizio, con il software whireshark che si trova su kali linux; wireshark e un network sniffer, permette di analizzare qualsiasi pacchetto che passa attraverso la scheda di rete del pc.

Io l'ho usato per analizzare i pacchetti che passavano da windows7 a kali linux, nella prima foto sono i pacchetti con il protocollo http, nella seconda foto i pacchetti con il protocollo https, come si può notare sono diverse tra loro le foto sono diverse, questo perché entrambi i protocolli, sono protocolli web e servono per la comunicazione tra server web e client, ma la differenza e che l'http serve solamente ad effettuare uno scambio comunicativo, invece l'https serve a proteggere la comunicazione rendendola criptata.


Capturing from eth0 (host 192.168.32.101)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
68 329.500399223 192.168.32.101 192.168.32.100 HTTP 853 GET /qsml.aspx?query=ht&maxwidth=398&rowheight=20&sectionHeight=160&...
69 329.500409867 192.168.32.100 192.168.32.101 TCP 54 80 → 49261 [ACK] Seq=1 Ack=800 Win=64128 Len=0
70 329.519234755 192.168.32.100 192.168.32.101 TCP 204 80 → 49261 [PSH, ACK] Seq=1 Ack=800 Win=64128 Len=150 [TCP segment o...
71 329.520448777 192.168.32.101 192.168.32.100 TCP 60 49261 → 80 [ACK] Seq=800 Ack=151 Win=65536 Len=0
72 329.520479209 192.168.32.100 192.168.32.101 HTTP 312 HTTP/1.1 200 OK (text/html)
73 329.522943150 192.168.32.100 192.168.32.101 TCP 54 80 → 49261 [FIN, ACK] Seq=409 Ack=800 Win=64128 Len=0
74 329.530211593 192.168.32.101 192.168.32.100 TCP 60 49261 → 80 [ACK] Seq=800 Ack=410 Win=65280 Len=0
75 329.533947576 192.168.32.101 192.168.32.100 TCP 60 49261 → 80 [FIN, ACK] Seq=800 Ack=410 Win=65280 Len=0
76 329.533979991 192.168.32.100 192.168.32.101 TCP 54 80 → 49261 [ACK] Seq=410 Ack=801 Win=64128 Len=0
77 329.643163430 192.168.32.101 192.168.32.100 TCP 66 49262 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
78 329.643204336 192.168.32.100 192.168.32.101 TCP 66 80 → 49262 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM...
Frame 72: 312 bytes on wire (2496 bits), 312 bytes captured (2496 bits)
Section number: 1
Interface id: 0 (eth0)
Interface name: eth0
Encapsulation type: Ethernet (1)
Arrival Time: May 7, 2023 07:07:15.171944431 EDT
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1683457635.171944431 seconds
[Time delta from previous captured frame: 0.000030432 seconds]
[Time delta from previous displayed frame: 0.000030432 seconds]
[Time since reference or first frame: 329.520479209 seconds]
Frame Number: 72
0000 08 00 27 9f fa ad 08 00 27 c7 e1 36 08 00 45 00
0010 01 2a d0 e7 40 00 40 06 a6 cc c0 a8 20 64 c0 a8
0020 20 65 00 50 c0 6d aa a1 de 9b 1b 5b 38 7d 50 18
0030 01 f5 c3 36 00 00 3c 68 74 6d 6c 3e 0a 20 20 3c
0040 68 65 61 64 3e 0a 20 20 20 20 3c 74 69 74 6c 65
0050 3e 49 4e 65 74 53 69 6d 20 64 65 66 61 75 6c 74
0060 20 48 54 4d 4c 20 70 61 67 65 3c 2f 74 69 74 6c
0070 65 3e 0a 20 20 3c 2f 68 65 61 64 3e 0a 20 20 3c
0080 62 6f 64 79 3e 0a 20 20 20 20 3c 70 3e 3c 2f 70
0090 3e 0a 20 20 20 20 3c 70 20 61 6c 69 67 6e 3d 22
00a0 63 65 6e 74 65 72 22 3e 54 68 69 73 20 69 73 20
Frame (312 bytes)
Reassembled TCP (408 bytes)
eth0: <live capture in progress>
Packets: 195 · Displayed: 195 (100.0%)
Profile: Default


*eth0 (host 192.168.32.101)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
https
No. Time Source Destination Protocol Length Info
1 0.000000000 192.168.32.101 224.0.0.252 LLMNR 64 Standard query 0xad11 A wpad
2 0.032121551 192.168.32.101 192.168.32.100 TCP 66 49281 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
3 0.032153645 192.168.32.100 192.168.32.101 TCP 54 80 → 49281 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4 0.104465897 192.168.32.101 224.0.0.252 LLMNR 64 Standard query 0xad11 A wpad
5 0.309285602 192.168.32.101 192.168.32.255 NBNS 92 Name query NB WPAD<00>
6 0.548028134 192.168.32.101 192.168.32.100 TCP 66 [TCP Retransmission] [TCP Port numbers reused] 49281 → 80 [SYN]
7 0.548059146 192.168.32.100 192.168.32.101 TCP 54 80 → 49281 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
8 1.088904090 192.168.32.101 192.168.32.100 TCP 62 [TCP Retransmission] [TCP Port numbers reused] 49281 → 80 [SYN]
9 1.088938147 192.168.32.100 192.168.32.101 TCP 54 80 → 49281 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
10 1.090197892 192.168.32.101 192.168.32.100 TCP 66 49282 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
11 1.090231649 192.168.32.100 192.168.32.101 TCP 54 80 → 49282 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
Frame 2: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on i
Section number: 1
Interface id: 0 (eth0)
Encapsulation type: Ethernet (1)
Arrival Time: May 7, 2023 12:47:41.000448920 EDT
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1683478061.000448920 seconds
[Time delta from previous captured frame: 0.032121551 seconds]
[Time delta from previous displayed frame: 0.032121551 seconds]
[Time since reference or first frame: 0.032121551 seconds]
Frame Number: 2
Frame Length: 66 bytes (528 bits)
0000 08 00 27 c7 e1 36 08 00 27 3f 84 72 08 00 45 00
0010 00 34 02 79 40 00 80 06 36 31 c0 a8 20 65 c0 a8
0020 20 64 c0 81 00 50 0a 1d 8c 56 00 00 00 00 80 02
0030 20 00 35 b1 00 00 02 04 05 b4 01 03 03 08 01 01
0040 04 02
Frame (frame), 66 bytes
Packets: 329 · Displayed: 329 (100.0%) · Dropped: 0 (0.0%)
Profile: Default