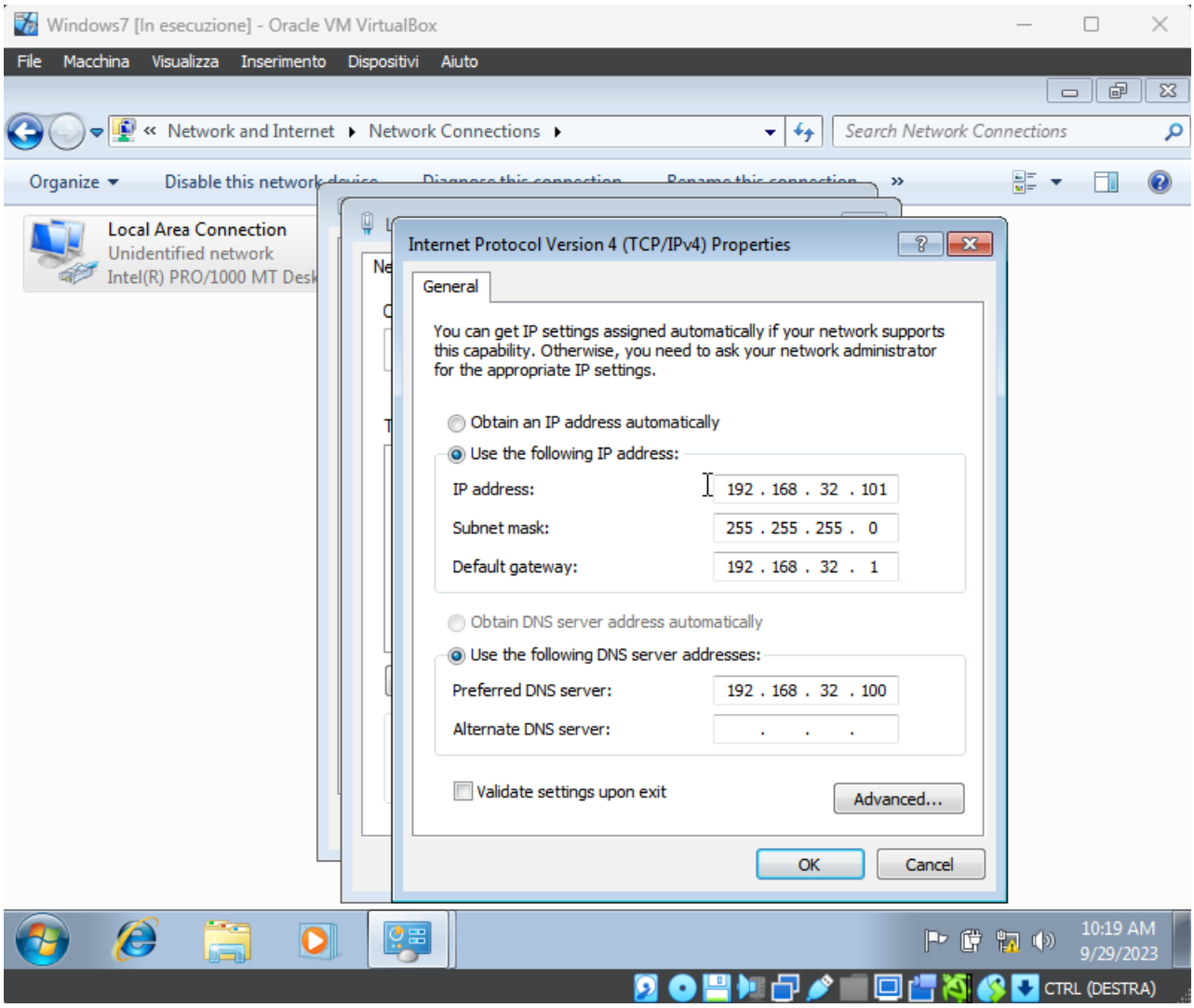
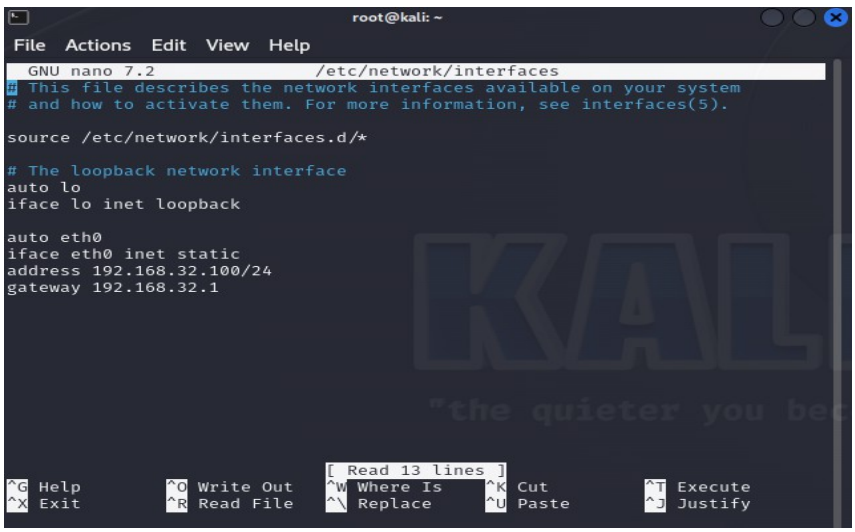
Progetto 29/09 - Luca Danelli

Imposto l'ip sulla macchina windows 7 configurando come server DNS l'ip che andrò ad assegnare alla macchina kali:



Imposto l'ip sulla macchina Kali con il comando **sudo nano /etc/network/interfaces**, andando quindi a modificare il file di configurazione di rete con l'editor nano, successivamente riavvio la macchina con il comando **sudo reboot** per applicare la configurazione:



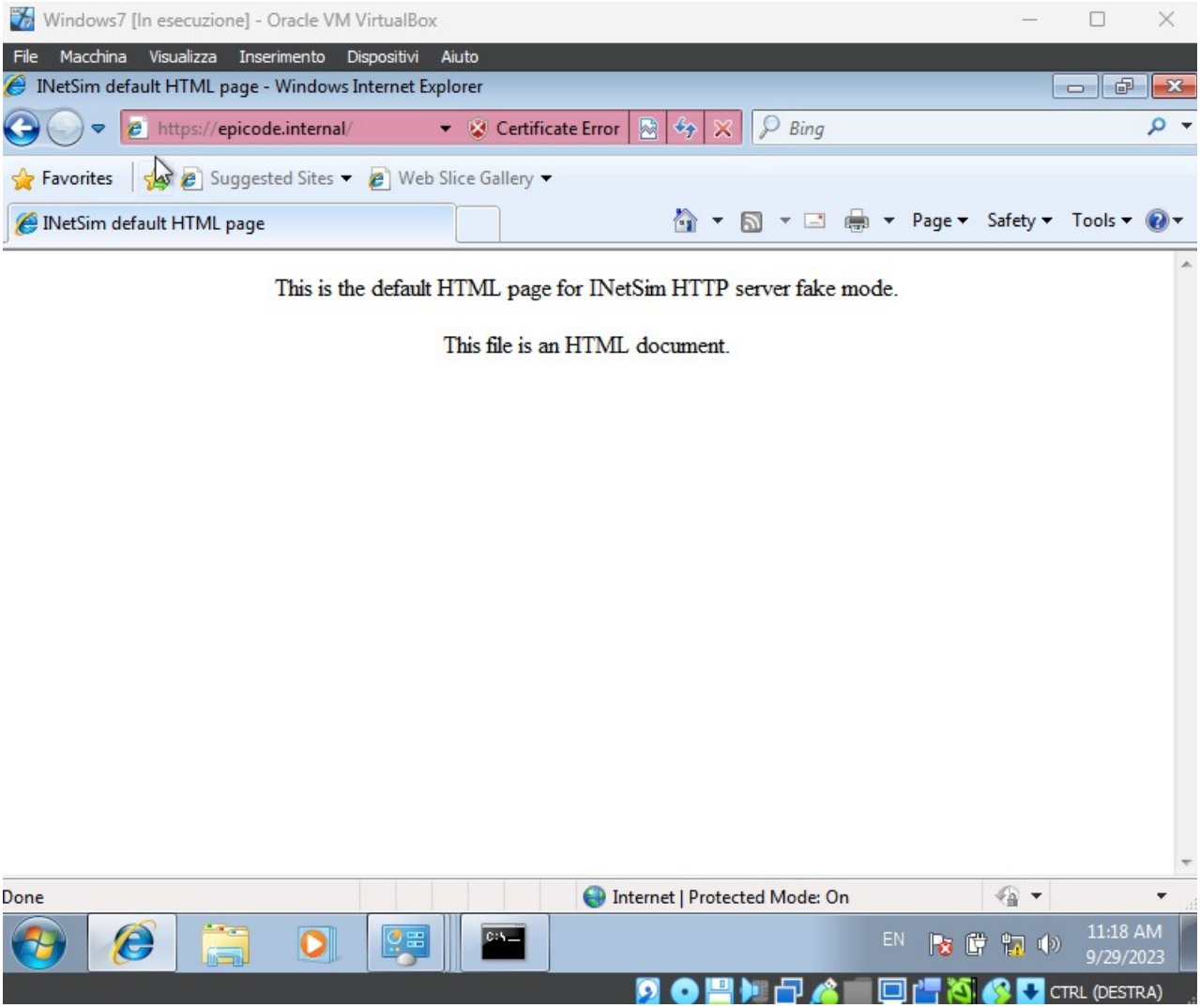
```
root@kali: ~
File  Actions  Edit  View  Help
┌──(root㉿kali)-[~]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.32.100  netmask 255.255.255.0  broadcast 192.168.32.255
        inet6 fe80::a00:27ff:fecb:7ef5  prefixlen 64  scopeid 0×20<link>
        inet6 2001:b07:aac:7465:a00:27ff:fecb:7ef5  prefixlen 64  scopeid 0×0
<global>
        ether 08:00:27:cb:7e:f5  txqueuelen 1000  (Ethernet)
        RX packets 67  bytes 14341 (14.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 22  bytes 8379 (8.1 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 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Con il comando **sudo nano /etc/inetsim/inetsim.conf** vado ad editare il file di configurazione di inetsim, andando ad attivare i servizi DNS e HTTPS come in figura e creando il record per associare epicode.internal all'indirizzo 192.168.32.100

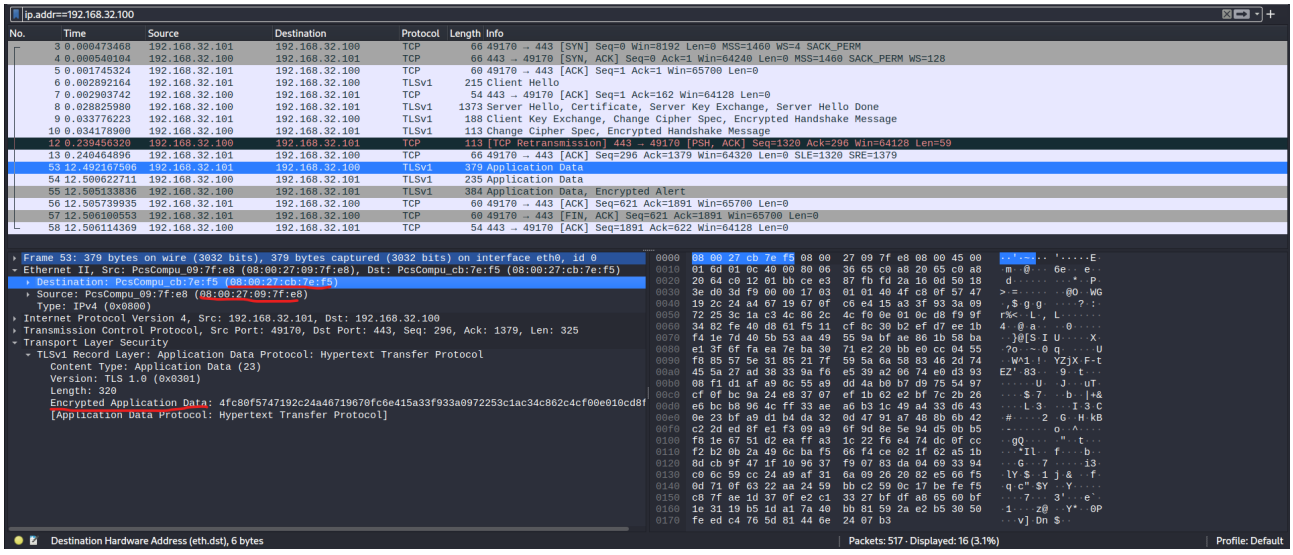
```
root@kali: ~
File  Actions  Edit  View  Help
  GNU nano 7.2                /etc/inetsim/inetsim.conf *
# ftps, irc, https
#
start_service dns
#start_service http
start_service https
#start_service smtp
#start_service smtps
#start_service pop3
#start_service pop3s
#start_service ftp
#start_service 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
^G Help        ^O Write Out   ^W Where Is    ^K Cut         ^T Execute
^X Exit        ^R Read File   ^\ Replace     ^U Paste       ^J Justify
```

```
##########################################
# dns_static
#
# Static mappings for DNS
#
# Syntax: dns_static <fqdn hostname> <IP address>
#
# Default: none
#
#dns_static www.foo.com 10.10.10.10
#dns_static ns1.foo.com 10.70.50.30
#dns_static ftp.bar.net 10.10.20.30
dns_static epicode.internal 192.168.32.100
```

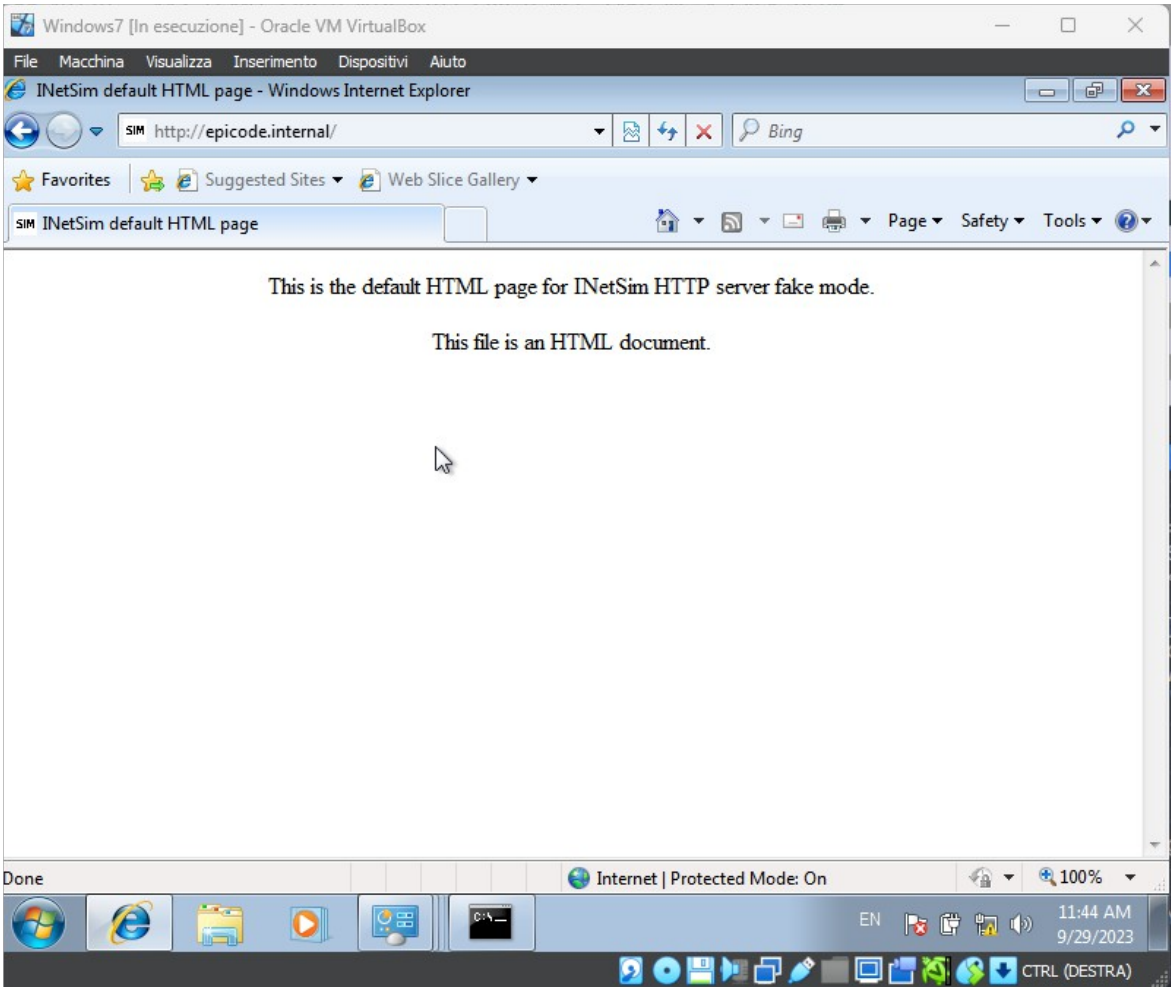
Successivamente da W7 punto da browser all'indirizzo epicode.internal. Accettando il rischio per la mancanza di certificato viene esposta questa pagina:



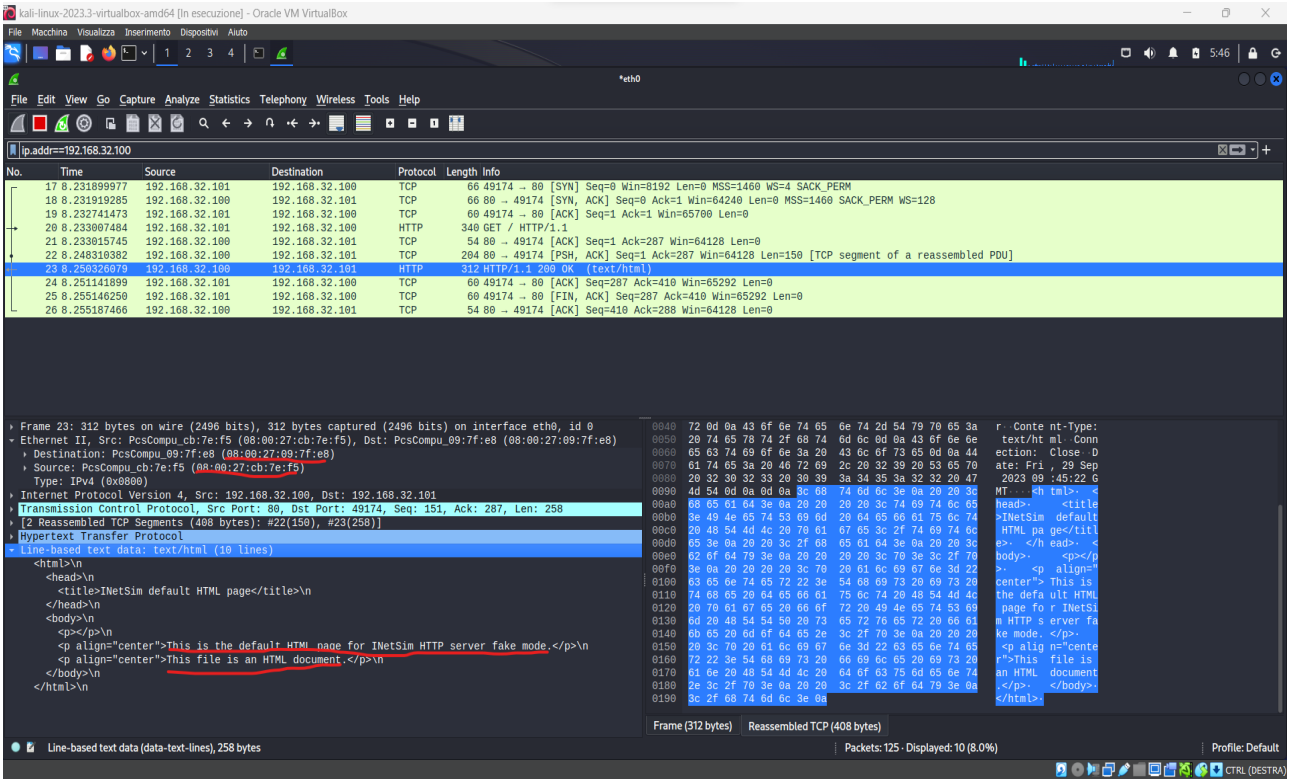
Di seguito la cattura con wireshark filtrata per ip 192.168.32.100, nell'immagine ho evidenziato in rosso i mac-address sorgente e destinazione di un pacchetto Application Data e la parte dove informa che il contenuto del payload è criptato:



Ripeto poi il procedimento visto sopra per attivare il servizio HTTP da inetsim andando a togliere il commento questa volta sul service_http su macchina Kali ed effettuo una richiesta HTTP da W7 verso Kali:



Traccio anche questa comunicazione con Wireshark da Kali. Noto che questa volta il testo html scambiato risulta visibile, evidenziato in rosso nell'immagine assieme ai mac-address. Questo perché il protocollo HTTP non si avvale di cifratura come l'HTTPS:


kali-linux-2023.3-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr==192.168.32.100
No. Time Source Destination Protocol Length Info
17 8.231899977 192.168.32.101 192.168.32.100 TCP 66 49174 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM
18 8.231919285 192.168.32.100 192.168.32.101 TCP 66 80 → 49174 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
19 8.232741473 192.168.32.101 192.168.32.100 TCP 60 49174 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
20 8.233007484 192.168.32.101 192.168.32.100 HTTP 340 GET / HTTP/1.1
21 8.233015745 192.168.32.100 192.168.32.101 TCP 54 80 → 49174 [ACK] Seq=1 Ack=287 Win=64128 Len=0
22 8.248310382 192.168.32.100 192.168.32.101 TCP 204 80 → 49174 [PSH, ACK] Seq=1 Ack=287 Win=64128 Len=150 [TCP segment of a reassembled PDU]
23 8.250326079 192.168.32.100 192.168.32.101 HTTP 312 HTTP/1.1 200 OK (text/html)
24 8.251141899 192.168.32.101 192.168.32.100 TCP 60 49174 → 80 [ACK] Seq=287 Ack=410 Win=65292 Len=0
25 8.255146250 192.168.32.101 192.168.32.100 TCP 60 49174 → 80 [FIN, ACK] Seq=287 Ack=410 Win=65292 Len=0
26 8.255187466 192.168.32.100 192.168.32.101 TCP 54 80 → 49174 [ACK] Seq=410 Ack=288 Win=64128 Len=0
Frame 23: 312 bytes on wire (2496 bits), 312 bytes captured (2496 bits) on interface eth0, id 0
Ethernet II, Src: PcsCompu_cb:7e:f5 (08:00:27:cb:7e:f5), Dst: PcsCompu_09:7f:e8 (08:00:27:09:7f:e8)
Destination: PcsCompu_09:7f:e8 (08:00:27:09:7f:e8)
Source: PcsCompu_cb:7e:f5 (08:00:27:cb:7e:f5)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.32.100, Dst: 192.168.32.101
Transmission Control Protocol, Src Port: 80, Dst Port: 49174, Seq: 151, Ack: 287, Len: 258
[2 Reassembled TCP Segments (408 bytes): #22(150), #23(258)]
Hypertext Transfer Protocol
Line-based text data: text/html (10 lines)
<html>\n
<head>\n
<title>INetSim default HTML page</title>\n
</head>\n
<body>\n
\n
This is the default HTML page for INetSim HTTP server fake mode. \n
This file is an HTML document. \n
</body>\n
</html>\n
0040 72 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a r··Conte nt-Type:
0050 20 74 65 78 74 2f 68 74 6d 6c 0d 0a 43 6f 6e 6e text/ht ml··Conn
0060 65 63 74 69 6f 6e 3a 20 43 6c 6f 73 65 0d 0a 44 ection: Close··D
0070 61 74 65 3a 20 46 72 69 2c 20 32 39 20 53 65 70 ate: Fri , 29 Sep
0080 20 32 30 32 33 20 30 39 3a 34 35 3a 32 32 20 47 2023 09 :45:22 G
0090 4d 54 0d 0a 0d 0a 3c 68 74 6d 6c 3e 0a 20 20 3c MT····<h tml>·· <
00a0 68 65 61 64 3e 0a 20 20 20 20 3c 74 69 74 6c 65 head>·· <title
00b0 3e 49 4e 65 74 53 69 6d 20 64 65 66 61 75 6c 74 >INetSim default
00c0 20 48 54 4d 4c 20 70 61 67 65 3c 2f 74 69 74 6c HTML pa ge</titl
00d0 65 3e 0a 20 20 3c 2f 68 65 61 64 3e 0a 20 20 3c e>·· </h ead>·· <
00e0 62 6f 64 79 3e 0a 20 20 20 20 3c 70 3e 3c 2f 70 body>·· </p
00f0 3e 0a 20 20 20 20 3c 70 20 61 6c 69 67 6e 3d 22 >·· <p align="
0100 63 65 6e 74 65 72 22 3e 54 68 69 73 20 69 73 20 center"> This is
0110 74 68 65 20 64 65 66 61 75 6c 74 20 48 54 4d 4c the defa ult HTML
0120 20 70 61 67 65 20 66 6f 72 20 49 4e 65 74 53 69 page fo r INetSi
0130 6d 20 48 54 54 50 20 73 65 72 76 65 72 20 66 61 m HTTP s erver fa
0140 6b 65 20 6d 6f 64 65 2e 3c 2f 70 3e 0a 20 20 20 ke mode. ··
0150 20 3c 70 20 61 6c 69 67 6e 3d 22 63 65 6e 74 65 <p alig n="cente
0160 72 22 3e 54 68 69 73 20 66 69 6c 65 20 69 73 20 r">This file is
0170 61 6e 20 48 54 4d 4c 20 64 6f 63 75 6d 65 6e 74 an HTML document
0180 2e 3c 2f 70 3e 0a 20 20 3c 2f 62 6f 64 79 3e 0a . ·· </body>·
0190 3c 2f 68 74 6d 6c 3e 0a </html>·
Frame (312 bytes)
Reassembled TCP (408 bytes)
Line-based text data (data-text-lines), 258 bytes
Packets: 125 · Displayed: 10 (8.0%)
Profile: Default
CTRL (DESTRA)