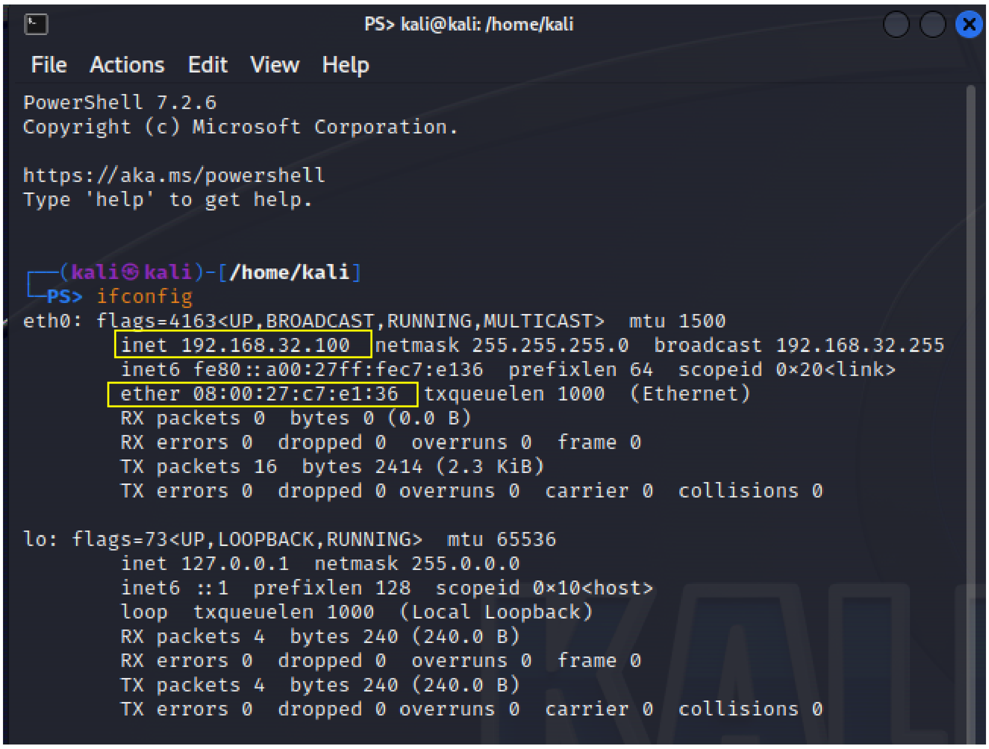
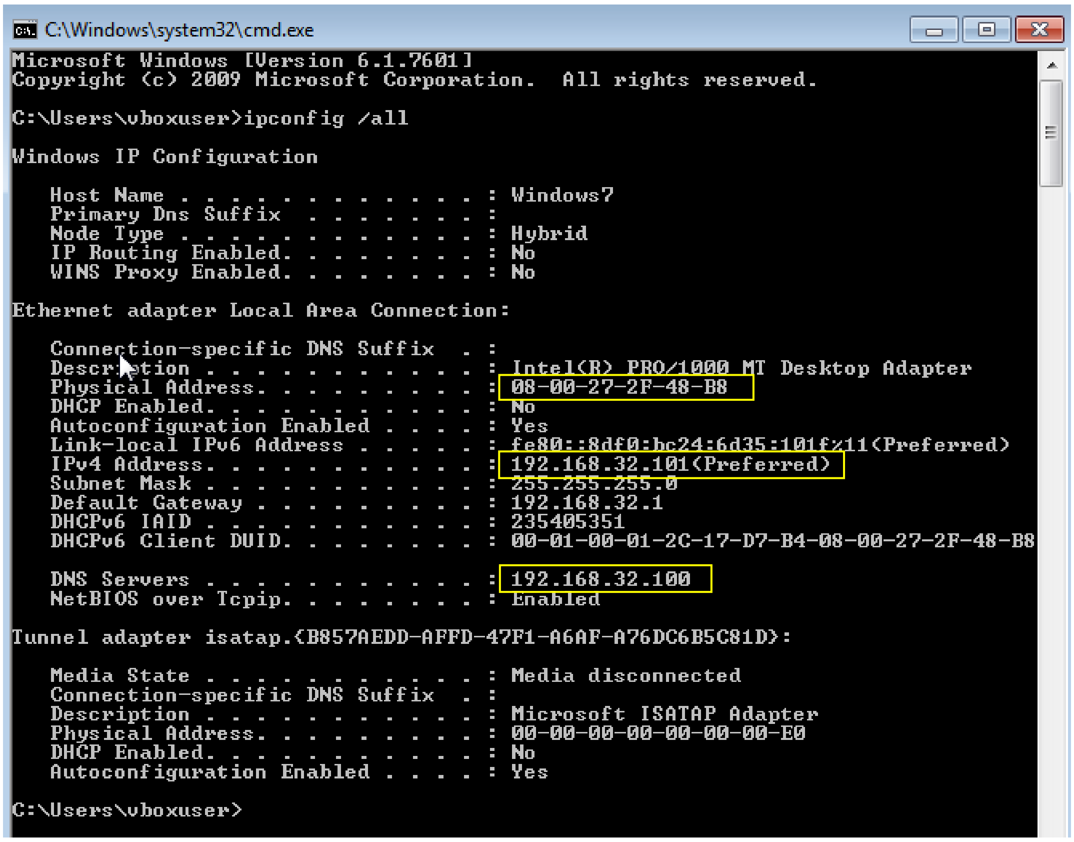
Configurazione IP statico e client/server DSN – evidenza indirizzi IP e MAC

Kali Linux 192.168.32.100



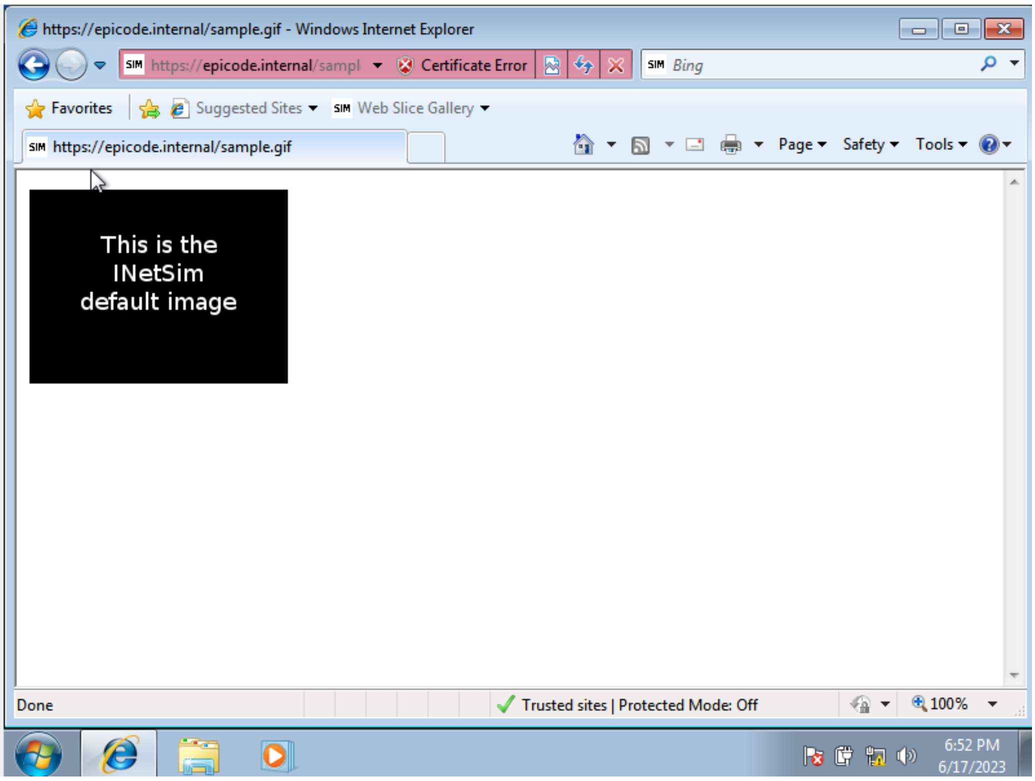
```
PowerShell 7.2.6
Copyright (c) Microsoft Corporation.

https://aka.ms/powershell
Type 'help' to get help.


┌──(kali㉿kali)-[/home/kali]
└─PS> 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 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 16  bytes 2414 (2.3 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 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
```

Windows 7 192.168.32.101



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\vboxuser>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : Windows7
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
   Physical Address. . . . . . . . . : 08-00-27-2F-48-B8
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::8df0:bc24:6d35:101f%11(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.32.101(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.32.1
   DHCPv6 IAID . . . . . . . . . . . : 235405351
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2C-17-D7-B4-08-00-27-2F-48-B8

   DNS Servers . . . . . . . . . . . : 192.168.32.100
   NetBIOS over Tcpip. . . . . . . . : Enabled

Tunnel adapter isatap.{B857AEDD-AFFD-47F1-A6AF-A76DC6B5C81D}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft ISATAP Adapter
   Physical Address. . . . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes

C:\Users\vboxuser>
```

Richiesta HTTPS da Windows 7 a epicode.internal/sample.gif



https://epicode.internal/sample.gif - Windows Internet Explorer

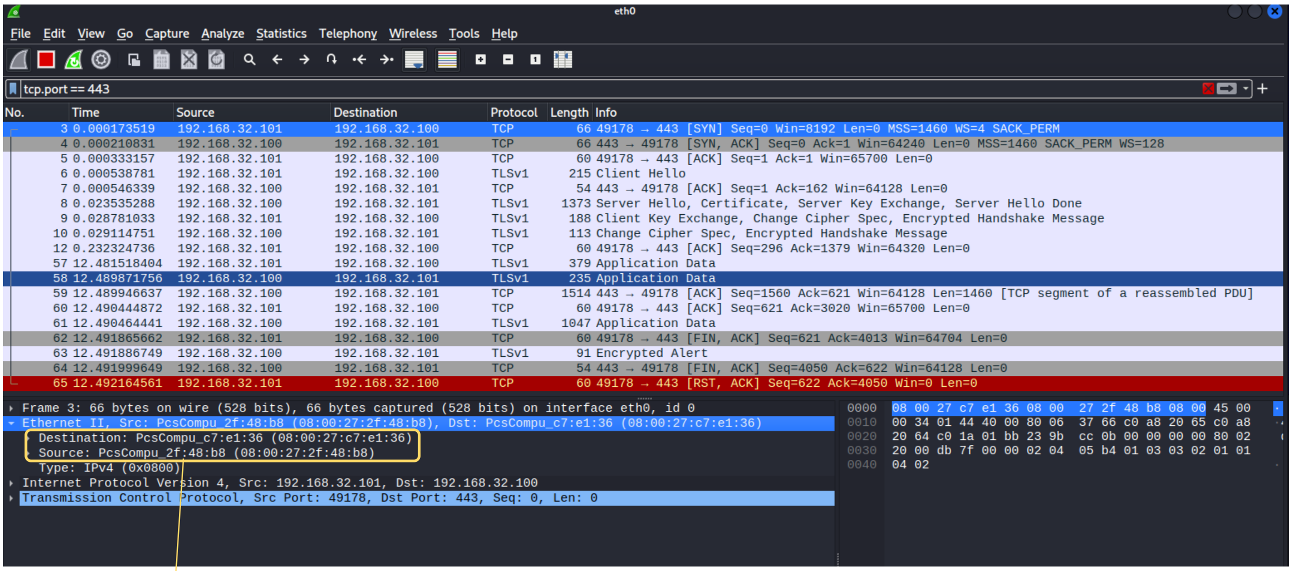
https://epicode.internal/sampl — Certificate Error

This is the INetSim default image

Done — Trusted sites | Protected Mode: Off — 100%

6:52 PM 6/17/2023

Pacchetti catturati con Wireshark (richiesta HTTPS)



tcp.port == 443

```
No.  Time          Source          Destination     Protocol Length Info
   3 0.000173519   192.168.32.101  192.168.32.100  TCP        66 49178 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM
   4 0.000210831   192.168.32.100  192.168.32.101  TCP        66 443 → 49178 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
   5 0.000333157   192.168.32.101  192.168.32.100  TCP        60 49178 → 443 [ACK] Seq=1 Ack=1 Win=65700 Len=0
   6 0.000538781   192.168.32.101  192.168.32.100  TLSv1     215 Client Hello
   7 0.000546339   192.168.32.100  192.168.32.101  TCP        54 443 → 49178 [ACK] Seq=1 Ack=162 Win=64128 Len=0
   8 0.023535288   192.168.32.100  192.168.32.101  TLSv1    1373 Server Hello, Certificate, Server Key Exchange, Server Hello Done
   9 0.028781033   192.168.32.101  192.168.32.100  TLSv1     188 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
  10 0.029114751   192.168.32.100  192.168.32.101  TLSv1     113 Change Cipher Spec, Encrypted Handshake Message
  12 0.232324736   192.168.32.101  192.168.32.100  TCP        60 49178 → 443 [ACK] Seq=296 Ack=1379 Win=64320 Len=0
  57 12.481518404  192.168.32.101  192.168.32.100  TLSv1     379 Application Data
  58 12.489871756  192.168.32.100  192.168.32.101  TLSv1     235 Application Data
  59 12.489946637  192.168.32.100  192.168.32.101  TCP      1514 443 → 49178 [ACK] Seq=1560 Ack=621 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
  60 12.490444872  192.168.32.101  192.168.32.100  TCP        60 49178 → 443 [ACK] Seq=621 Ack=3020 Win=65700 Len=0
  61 12.490464441  192.168.32.100  192.168.32.101  TLSv1    1047 Application Data
  62 12.491865662  192.168.32.101  192.168.32.100  TCP        60 49178 → 443 [FIN, ACK] Seq=621 Ack=4013 Win=64704 Len=0
  63 12.491886749  192.168.32.100  192.168.32.101  TLSv1      91 Encrypted Alert
  64 12.491999649  192.168.32.100  192.168.32.101  TCP        54 443 → 49178 [FIN, ACK] Seq=4050 Ack=622 Win=64128 Len=0
  65 12.492164561  192.168.32.101  192.168.32.100  TCP        60 49178 → 443 [RST, ACK] Seq=622 Ack=4050 Win=0 Len=0
```

```
› Frame 3: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface eth0, id 0
⌄ Ethernet II, Src: PcsCompu_2f:48:b8 (08:00:27:2f:48:b8), Dst: PcsCompu_c7:e1:36 (08:00:27:c7:e1:36)
  › Destination: PcsCompu_c7:e1:36 (08:00:27:c7:e1:36)
  › Source: PcsCompu_2f:48:b8 (08:00:27:2f:48:b8)
    Type: IPv4 (0x0800)
› Internet Protocol Version 4, Src: 192.168.32.101, Dst: 192.168.32.100
› Transmission Control Protocol, Src Port: 49178, Dst Port: 443, Seq: 0, Len: 0
```

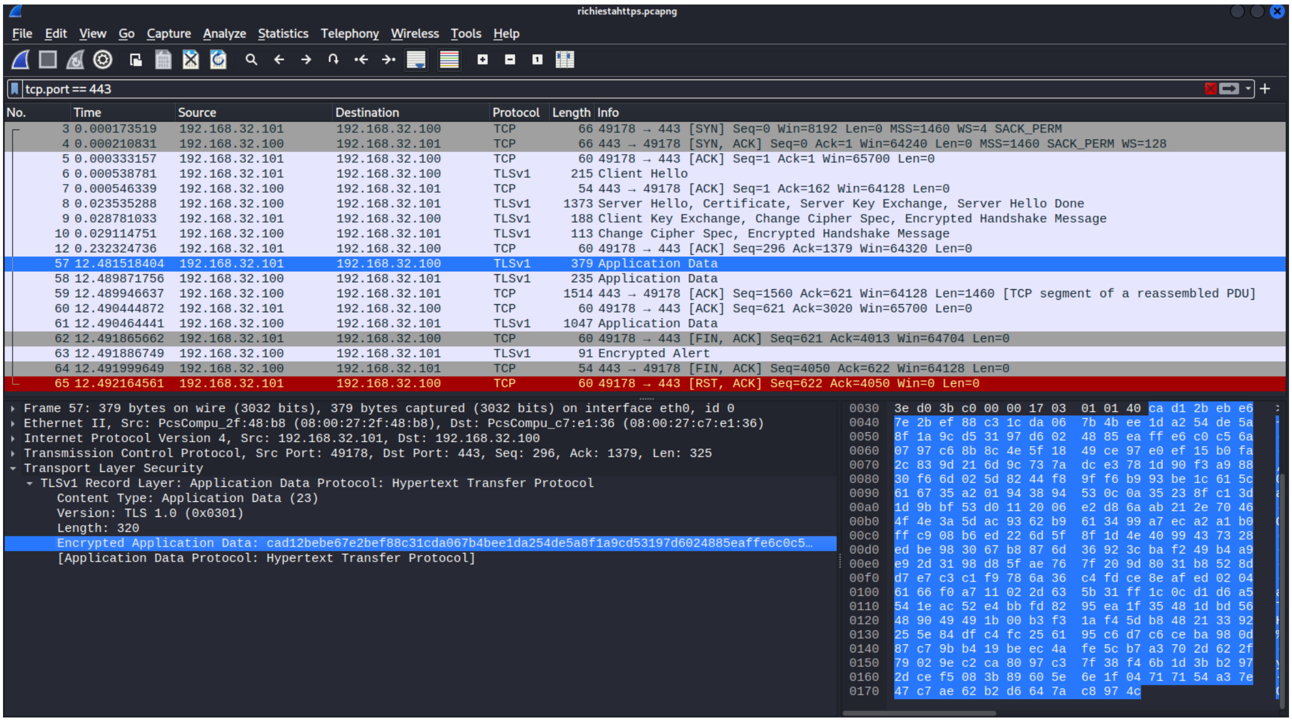
```
0000  08 00 27 c7 e1 36 08 00  27 2f 48 b8 08 00 45 00
0010  00 34 01 44 40 00 80 06  37 66 c0 a8 20 65 c0 a8
0020  20 64 c0 1a 01 bb 23 9b  cc 0b 00 00 00 00 80 02
0030  20 00 db 7f 00 00 02 04  05 b4 01 03 03 02 01 01
0040  04 02
```

indirizzo MAC sorgente: 08:00:27:2f:48:b8

indirizzo MAC destinazione: 08:00:27:c7:e1:36

Contenuto della richiesta HTTPS

Trattandosi di richiesta HTTPS (o HTTP secure), il contenuto è criptato


richiestahttps.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

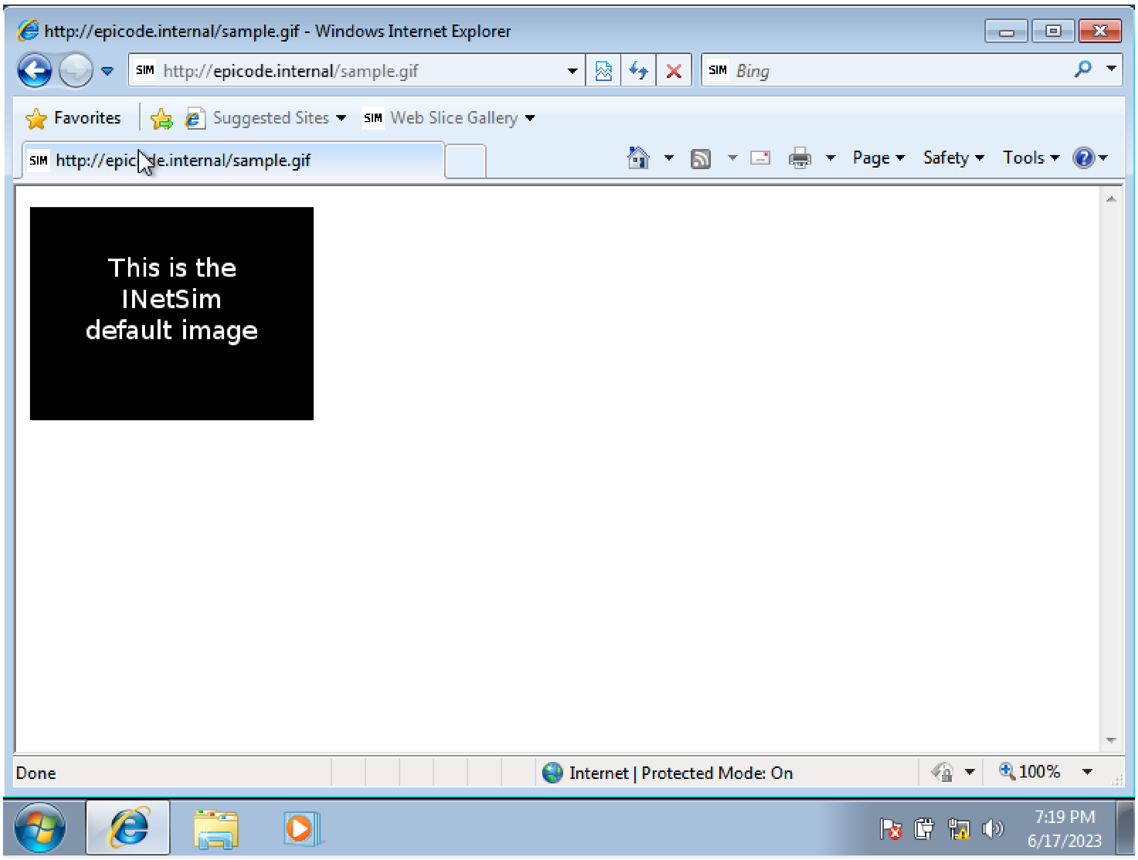
tcp.port == 443

```
No.  Time          Source          Destination     Protocol Length Info
   3 0.000173519   192.168.32.101  192.168.32.100  TCP        66 49178 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM
   4 0.000210831   192.168.32.100  192.168.32.101  TCP        66 443 → 49178 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
   5 0.000333157   192.168.32.101  192.168.32.100  TCP        60 49178 → 443 [ACK] Seq=1 Ack=1 Win=65700 Len=0
   6 0.000538781   192.168.32.101  192.168.32.100  TLSv1     215 Client Hello
   7 0.000546339   192.168.32.100  192.168.32.101  TCP        54 443 → 49178 [ACK] Seq=1 Ack=162 Win=64128 Len=0
   8 0.023535288   192.168.32.100  192.168.32.101  TLSv1    1373 Server Hello, Certificate, Server Key Exchange, Server Hello Done
   9 0.028781033   192.168.32.101  192.168.32.100  TLSv1     188 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
  10 0.029114751   192.168.32.100  192.168.32.101  TLSv1     113 Change Cipher Spec, Encrypted Handshake Message
  12 0.232324736   192.168.32.101  192.168.32.100  TCP        60 49178 → 443 [ACK] Seq=296 Ack=1379 Win=64320 Len=0
  57 12.481518404  192.168.32.101  192.168.32.100  TLSv1     379 Application Data
  58 12.489871756  192.168.32.100  192.168.32.101  TLSv1     235 Application Data
  59 12.489946637  192.168.32.100  192.168.32.101  TCP      1514 443 → 49178 [ACK] Seq=1560 Ack=621 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
  60 12.490444872  192.168.32.101  192.168.32.100  TCP        60 49178 → 443 [ACK] Seq=621 Ack=3020 Win=65700 Len=0
  61 12.490464441  192.168.32.100  192.168.32.101  TLSv1    1047 Application Data
  62 12.491865662  192.168.32.101  192.168.32.100  TCP        60 49178 → 443 [FIN, ACK] Seq=621 Ack=4013 Win=64704 Len=0
  63 12.491886749  192.168.32.100  192.168.32.101  TLSv1      91 Encrypted Alert
  64 12.491999649  192.168.32.100  192.168.32.101  TCP        54 443 → 49178 [FIN, ACK] Seq=4050 Ack=622 Win=64128 Len=0
  65 12.492164561  192.168.32.101  192.168.32.100  TCP        60 49178 → 443 [RST, ACK] Seq=622 Ack=4050 Win=0 Len=0
```

```
› Frame 57: 379 bytes on wire (3032 bits), 379 bytes captured (3032 bits) on interface eth0, id 0
› Ethernet II, Src: PcsCompu_2f:48:b8 (08:00:27:2f:48:b8), Dst: PcsCompu_c7:e1:36 (08:00:27:c7:e1:36)
› Internet Protocol Version 4, Src: 192.168.32.101, Dst: 192.168.32.100
› Transmission Control Protocol, Src Port: 49178, Dst Port: 443, Seq: 296, Ack: 1379, Len: 325
⌄ Transport Layer Security
  ⌄ TLSv1 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
      Content Type: Application Data (23)
      Version: TLS 1.0 (0x0301)
      Length: 320
      Encrypted Application Data: cad12bebe67e2bef88c31cda067b4bee1da254de5a8f1a9cd53197d6024885eaffe6c0c5…
      [Application Data Protocol: Hypertext Transfer Protocol]
```

```
0030  3e d0 3b c0 00 00 17 03  01 01 40 ca d1 2b eb e6
0040  7e 2b ef 88 c3 1c da 06  7b 4b ee 1d a2 54 de 5a
0050  8f 1a 9c d5 31 97 d6 02  48 85 ea ff e6 c0 c5 6a
0060  07 97 c6 8b 8c 4e 5f 18  49 ce 97 e0 ef 15 b0 fa
0070  2c 83 9d 21 6d 9c 73 7a  dc e3 78 1d 90 f3 a9 88
0080  30 f6 6d 02 5d 82 44 f8  9f f6 b9 93 be 1c 61 5c
0090  61 67 35 a2 01 94 38 94  53 0c 0a 35 23 8f c1 3d
00a0  1d 9b bf 53 d0 11 20 06  e2 d8 6a ab 21 2e 70 46
00b0  4f 4e 3a 5d ac 93 62 b9  61 34 99 a7 ec a2 a1 b0
00c0  ff c9 08 b6 ed 22 6d 5f  8f 1d 4e 40 99 43 73 28
00d0  ed be 98 30 67 b8 87 6d  36 92 3c ba f2 49 b4 a9
00e0  e9 2d 31 98 d8 5f ae 76  7f 20 9d 80 31 b8 52 8d
00f0  d7 e7 c3 c1 f9 78 6a 36  c4 fd ce 8e af ed 02 04
0100  61 66 f0 a7 11 02 2d 63  5b 31 ff 1c 0c d1 d6 a5
0110  54 1e ac 52 e4 bb fd 82  95 ea 1f 35 48 1d bd 56
0120  48 90 49 49 1b 00 b3 f3  1a f4 5d b8 48 21 33 92
0130  25 5e 84 df c4 fc 25 61  95 c6 d7 c6 ce ba 98 0d
0140  87 c7 9b b4 19 be ec 4a  fe 5c b7 a3 70 2d 62 2f
0150  79 02 9e c2 ca 80 97 c3  7f 38 f4 6b 1d 3b b2 97
0160  2d ce f5 08 3b 89 60 5e  6e 1f 04 71 71 54 a3 7e
0170  47 c7 ae 62 b2 d6 64 7a  c8 97 4c
```

Richiesta HTTP da Windows 7 a epicode.internal/sample.gif

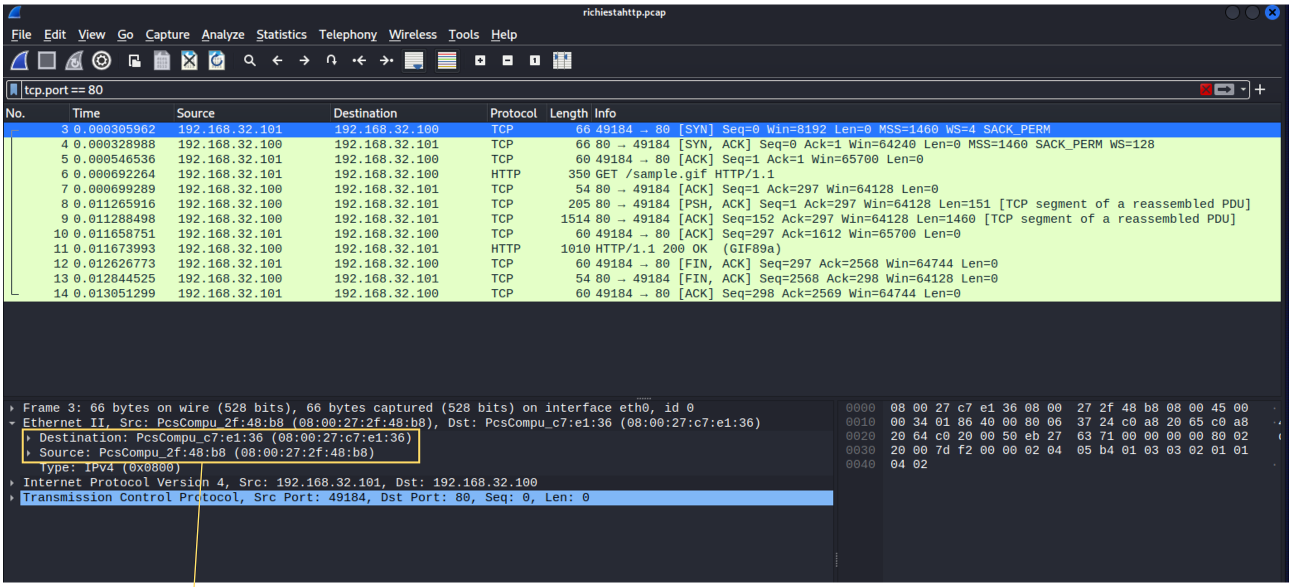


http://epicode.internal/sample.gif - Windows Internet Explorer

http://epicode.internal/sample.gif

Bing

Pacchetti catturati con Wireshark (richiesta HTTP)



```
tcp.port == 80
```

```
No.    Time          Source           Destination      Protocol Length Info
     3 0.000305962   192.168.32.101   192.168.32.100   TCP        66 49184 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM
     4 0.000328988   192.168.32.100   192.168.32.101   TCP        66 80 → 49184 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
     5 0.000546536   192.168.32.101   192.168.32.100   TCP        60 49184 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
     6 0.000692264   192.168.32.101   192.168.32.100   HTTP      350 GET /sample.gif HTTP/1.1
     7 0.000699289   192.168.32.100   192.168.32.101   TCP        54 80 → 49184 [ACK] Seq=1 Ack=297 Win=64128 Len=0
     8 0.011265916   192.168.32.100   192.168.32.101   TCP       205 80 → 49184 [PSH, ACK] Seq=1 Ack=297 Win=64128 Len=151 [TCP segment of a reassembled PDU]
     9 0.011288498   192.168.32.100   192.168.32.101   TCP      1514 80 → 49184 [ACK] Seq=152 Ack=297 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
    10 0.011658751   192.168.32.101   192.168.32.100   TCP        60 49184 → 80 [ACK] Seq=297 Ack=1612 Win=65700 Len=0
    11 0.011673993   192.168.32.100   192.168.32.101   HTTP     1010 HTTP/1.1 200 OK  (GIF89a)
    12 0.012626773   192.168.32.101   192.168.32.100   TCP        60 49184 → 80 [FIN, ACK] Seq=297 Ack=2568 Win=64744 Len=0
    13 0.012844525   192.168.32.100   192.168.32.101   TCP        54 80 → 49184 [FIN, ACK] Seq=2568 Ack=298 Win=64128 Len=0
    14 0.013051299   192.168.32.101   192.168.32.100   TCP        60 49184 → 80 [ACK] Seq=298 Ack=2569 Win=64744 Len=0
```

```
› Frame 3: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface eth0, id 0
⌄ Ethernet II, Src: PcsCompu_2f:48:b8 (08:00:27:2f:48:b8), Dst: PcsCompu_c7:e1:36 (08:00:27:c7:e1:36)
  › Destination: PcsCompu_c7:e1:36 (08:00:27:c7:e1:36)
  › Source: PcsCompu_2f:48:b8 (08:00:27:2f:48:b8)
    Type: IPv4 (0x0800)
› Internet Protocol Version 4, Src: 192.168.32.101, Dst: 192.168.32.100
› Transmission Control Protocol, Src Port: 49184, Dst Port: 80, Seq: 0, Len: 0
```

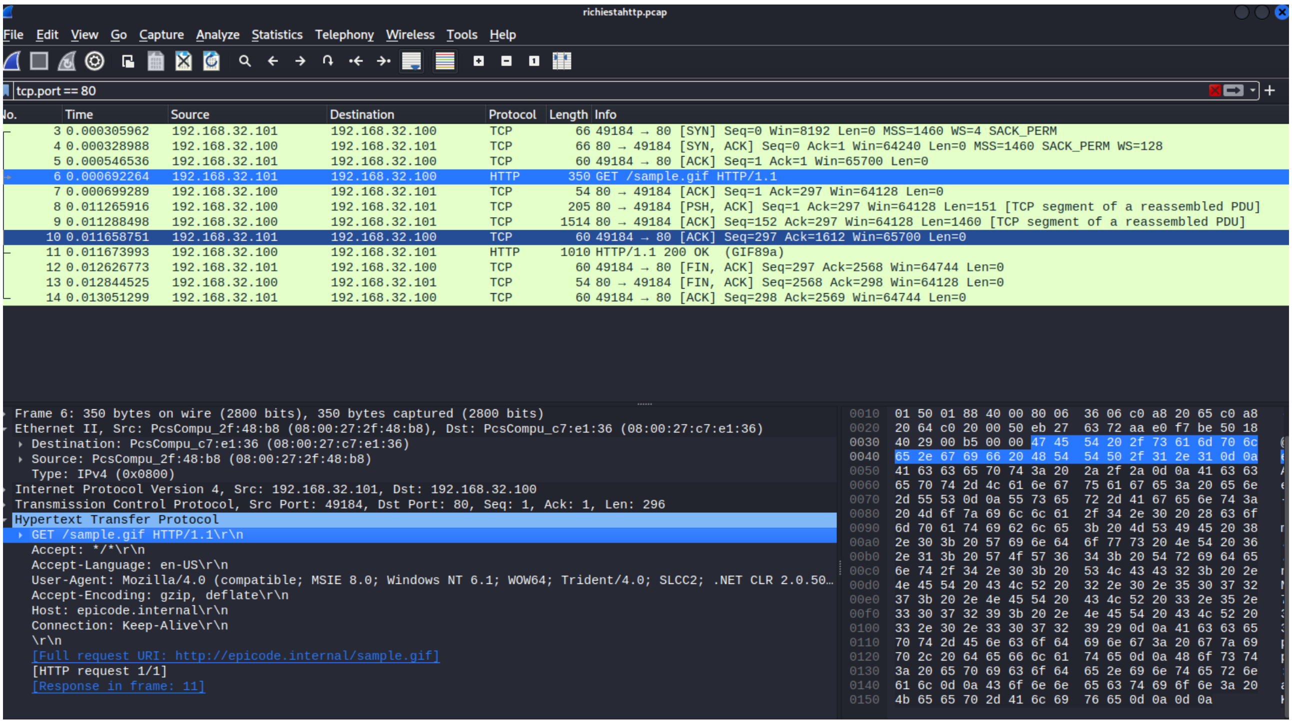
```
0000  08 00 27 c7 e1 36 08 00  27 2f 48 b8 08 00 45 00
0010  00 34 01 86 40 00 80 06  37 24 c0 a8 20 65 c0 a8
0020  20 64 c0 20 00 50 eb 27  63 71 00 00 00 00 80 02
0030  20 00 7d f2 00 00 02 04  05 b4 01 03 03 02 01 01
0040  04 02
```

indirizzo MAC sorgente: 08:00:27:2f:48:b8

indirizzo MAC destinazione: 08:00:27:c7:e1:36

Contenuto della richiesta HTTP

In questo caso il contenuto della richiesta è in chiaro:



```
tcp.port == 80
```

```
No.    Time          Source           Destination      Protocol Length Info
     3 0.000305962   192.168.32.101   192.168.32.100   TCP        66 49184 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM
     4 0.000328988   192.168.32.100   192.168.32.101   TCP        66 80 → 49184 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
     5 0.000546536   192.168.32.101   192.168.32.100   TCP        60 49184 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
     6 0.000692264   192.168.32.101   192.168.32.100   HTTP      350 GET /sample.gif HTTP/1.1
     7 0.000699289   192.168.32.100   192.168.32.101   TCP        54 80 → 49184 [ACK] Seq=1 Ack=297 Win=64128 Len=0
     8 0.011265916   192.168.32.100   192.168.32.101   TCP       205 80 → 49184 [PSH, ACK] Seq=1 Ack=297 Win=64128 Len=151 [TCP segment of a reassembled PDU]
     9 0.011288498   192.168.32.100   192.168.32.101   TCP      1514 80 → 49184 [ACK] Seq=152 Ack=297 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
    10 0.011658751   192.168.32.101   192.168.32.100   TCP        60 49184 → 80 [ACK] Seq=297 Ack=1612 Win=65700 Len=0
    11 0.011673993   192.168.32.100   192.168.32.101   HTTP     1010 HTTP/1.1 200 OK  (GIF89a)
    12 0.012626773   192.168.32.101   192.168.32.100   TCP        60 49184 → 80 [FIN, ACK] Seq=297 Ack=2568 Win=64744 Len=0
    13 0.012844525   192.168.32.100   192.168.32.101   TCP        54 80 → 49184 [FIN, ACK] Seq=2568 Ack=298 Win=64128 Len=0
    14 0.013051299   192.168.32.101   192.168.32.100   TCP        60 49184 → 80 [ACK] Seq=298 Ack=2569 Win=64744 Len=0
```

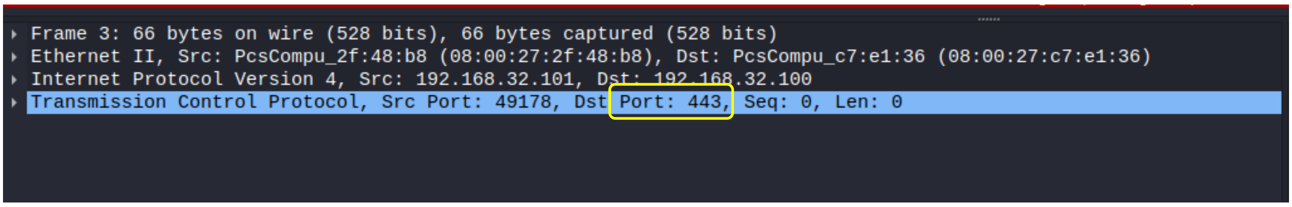
```
Frame 6: 350 bytes on wire (2800 bits), 350 bytes captured (2800 bits)
Ethernet II, Src: PcsCompu_2f:48:b8 (08:00:27:2f:48:b8), Dst: PcsCompu_c7:e1:36 (08:00:27:c7:e1:36)
  › Destination: PcsCompu_c7:e1:36 (08:00:27:c7:e1:36)
  › Source: PcsCompu_2f:48:b8 (08:00:27:2f:48:b8)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.32.101, Dst: 192.168.32.100
Transmission Control Protocol, Src Port: 49184, Dst Port: 80, Seq: 1, Ack: 1, Len: 296
Hypertext Transfer Protocol
  › GET /sample.gif HTTP/1.1\r\n
    Accept: */*\r\n
    Accept-Language: en-US\r\n
    User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50…
    Accept-Encoding: gzip, deflate\r\n
    Host: epicode.internal\r\n
    Connection: Keep-Alive\r\n
    \r\n
    [Full request URI: http://epicode.internal/sample.gif]
    [HTTP request 1/1]
    [Response in frame: 11]
```

```
0010  01 50 01 88 40 00 80 06  36 06 c0 a8 20 65 c0 a8
0020  20 64 c0 20 00 50 eb 27  63 72 aa e0 f7 be 50 18
0030  40 29 00 b5 00 00 47 45  54 20 2f 73 61 6d 70 6c
0040  65 2e 67 69 66 20 48 54  54 50 2f 31 2e 31 0d 0a
0050  41 63 63 65 70 74 3a 20  2a 2f 2a 0d 0a 41 63 63
0060  65 70 74 2d 4c 61 6e 67  75 61 67 65 3a 20 65 6e
0070  2d 55 53 0d 0a 55 73 65  72 2d 41 67 65 6e 74 3a
0080  20 4d 6f 7a 69 6c 6c 61  2f 34 2e 30 20 28 63 6f
0090  6d 70 61 74 69 62 6c 65  3b 20 4d 53 49 45 20 38
00a0  2e 30 3b 20 57 69 6e 64  6f 77 73 20 4e 54 20 36
00b0  2e 31 3b 20 57 4f 57 36  34 3b 20 54 72 69 64 65
00c0  6e 74 2f 34 2e 30 3b 20  53 4c 43 43 32 3b 20 2e
00d0  4e 45 54 20 43 4c 52 20  32 2e 30 2e 35 30 37 32
00e0  37 3b 20 2e 4e 45 54 20  43 4c 52 20 33 2e 35 2e
00f0  33 30 37 32 39 3b 20 2e  4e 45 54 20 43 4c 52 20
0100  33 2e 30 2e 33 30 37 32  39 29 0d 0a 41 63 63 65
0110  70 74 2d 45 6e 63 6f 64  69 6e 67 3a 20 67 7a 69
0120  70 2c 20 64 65 66 6c 61  74 65 0d 0a 48 6f 73 74
0130  3a 20 65 70 69 63 6f 64  65 2e 69 6e 74 65 72 6e
0140  61 6c 0d 0a 43 6f 6e 6e  65 63 74 69 6f 6e 3a 20
0150  4b 65 65 70 2d 41 6c 69  76 65 0d 0a 0d 0a
```

Differenze tra HTTPS e HTTP

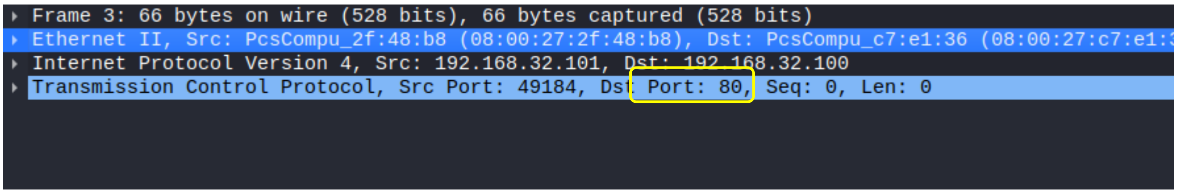
Le richieste HTTPS e HTTP utilizzano entrambe il protocollo TCP per il trasporto su porte differenti.

Il protocollo HTTPS utilizza la porta 443



```
▸ Frame 3: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
▸ Ethernet II, Src: PcsCompu_2f:48:b8 (08:00:27:2f:48:b8), Dst: PcsCompu_c7:e1:36 (08:00:27:c7:e1:36)
▸ Internet Protocol Version 4, Src: 192.168.32.101, Dst: 192.168.32.100
▸ Transmission Control Protocol, Src Port: 49178, Dst Port: 443, Seq: 0, Len: 0
```

mentre il protocollo HTTP utilizza la porta 80

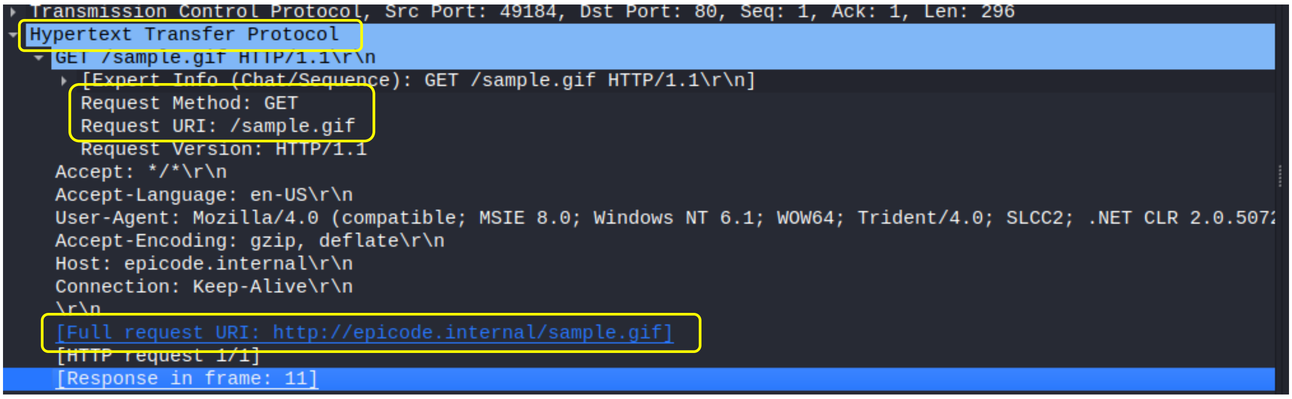


```
▸ Frame 3: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
▸ Ethernet II, Src: PcsCompu_2f:48:b8 (08:00:27:2f:48:b8), Dst: PcsCompu_c7:e1:36 (08:00:27:c7:e1:
▸ Internet Protocol Version 4, Src: 192.168.32.101, Dst: 192.168.32.100
▸ Transmission Control Protocol, Src Port: 49184, Dst Port: 80, Seq: 0, Len: 0
```

<u>La differenza principale tra i due protocolli però sta nel layer applicazione.</u>

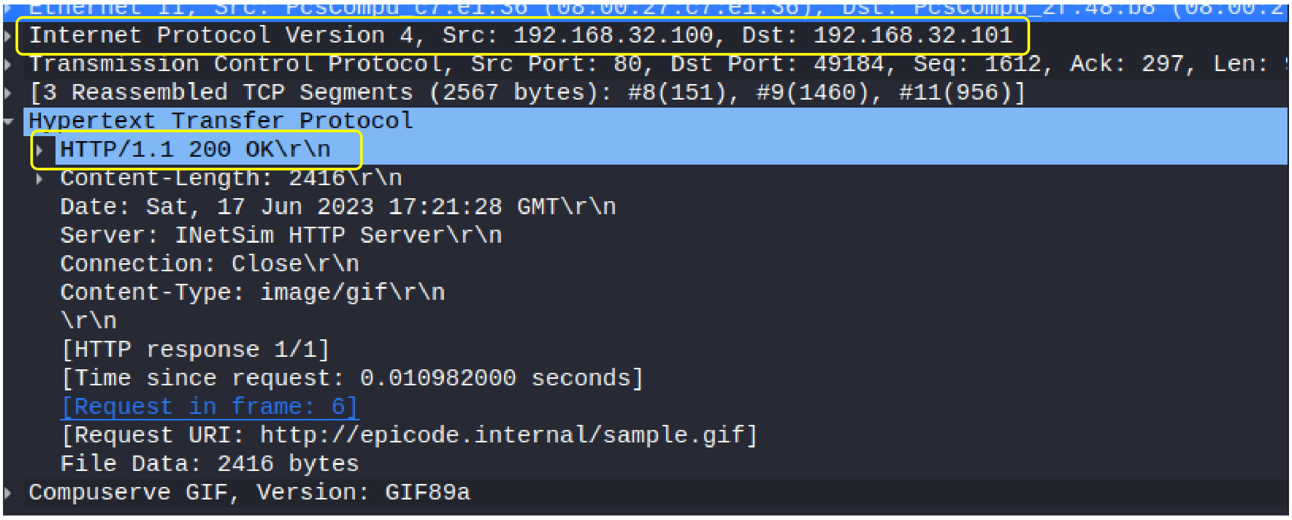
Nel caso di HTTP, il protocollo utilizzato è HTTP e la richiesta è in chiaro.

Nel layer applicazione vediamo che viene utilizzato l’Hypertext Transfer Protocol. In questo caso la richiesta utilizza il metodo GET e il file “sample.gif” che è stato richiesto è visibile in chiaro nel pacchetto.



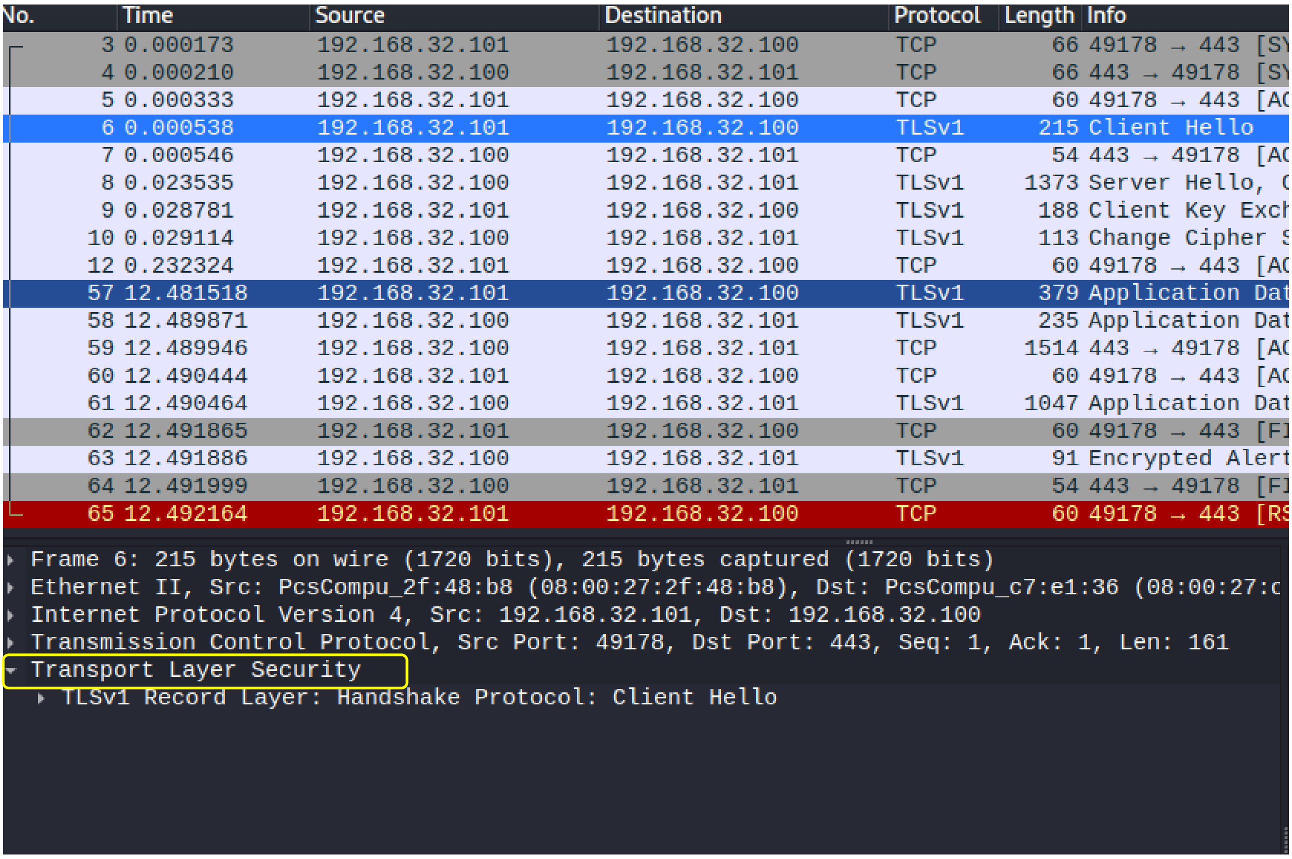
```
▸ Transmission Control Protocol, Src Port: 49184, Dst Port: 80, Seq: 1, Ack: 1, Len: 296
▾ Hypertext Transfer Protocol
  ▾ GET /sample.gif HTTP/1.1\r\n
    ▸ [Expert Info (Chat/Sequence): GET /sample.gif HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /sample.gif
      Request Version: HTTP/1.1
    Accept: */*\r\n
    Accept-Language: en-US\r\n
    User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.507
    Accept-Encoding: gzip, deflate\r\n
    Host: epicode.internal\r\n
    Connection: Keep-Alive\r\n
    \r\n
    [Full request URI: http://epicode.internal/sample.gif]
    [HTTP request 1/1]
    [Response in frame: 11]
```

Vediamo nel pacchetto successivo di risposta dal server che l'esito della richiesta è OK (codice stato 200).



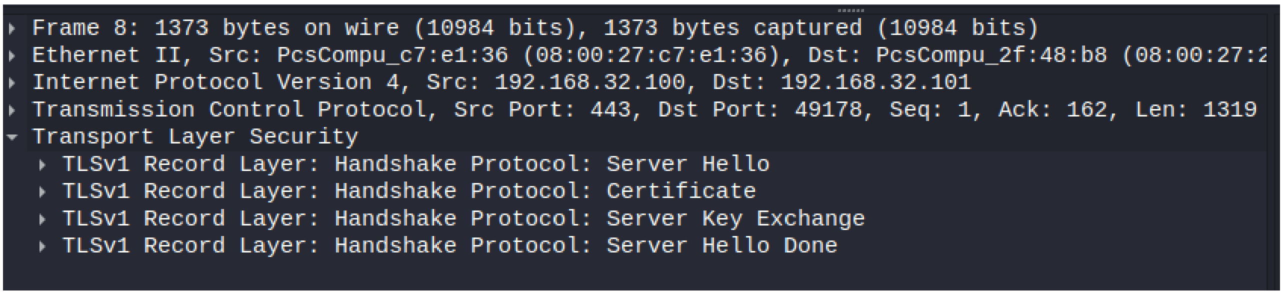
```
▸ Ethernet II, Src: PcsCompu_c7:e1:36 (08:00:27:c7:e1:36), Dst: PcsCompu_2f:48:b8 (08:00:2
▸ Internet Protocol Version 4, Src: 192.168.32.100, Dst: 192.168.32.101
▸ Transmission Control Protocol, Src Port: 80, Dst Port: 49184, Seq: 1612, Ack: 297, Len:
▸ [3 Reassembled TCP Segments (2567 bytes): #8(151), #9(1460), #11(956)]
▾ Hypertext Transfer Protocol
  ▸ HTTP/1.1 200 OK\r\n
  ▸ Content-Length: 2416\r\n
    Date: Sat, 17 Jun 2023 17:21:28 GMT\r\n
    Server: INetSim HTTP Server\r\n
    Connection: Close\r\n
    Content-Type: image/gif\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.010982000 seconds]
    [Request in frame: 6]
    [Request URI: http://epicode.internal/sample.gif]
    File Data: 2416 bytes
▸ Compuserve GIF, Version: GIF89a
```

Nel caso di HTTPS, il contenuto è criptato utilizzando un protocollo cifrato (TLSv1 in questo caso). Al protocollo "Hypertext Transfer Protocol" che abbiamo nel caso di HTTP, nella richiesta HTTPS viene sovrapposto il protocollo "Transport Layer Security". I pacchetti vengono scambiati in formato cifrato dopo una comunicazione client/server che comprende lo scambio della chiave di sicurezza:

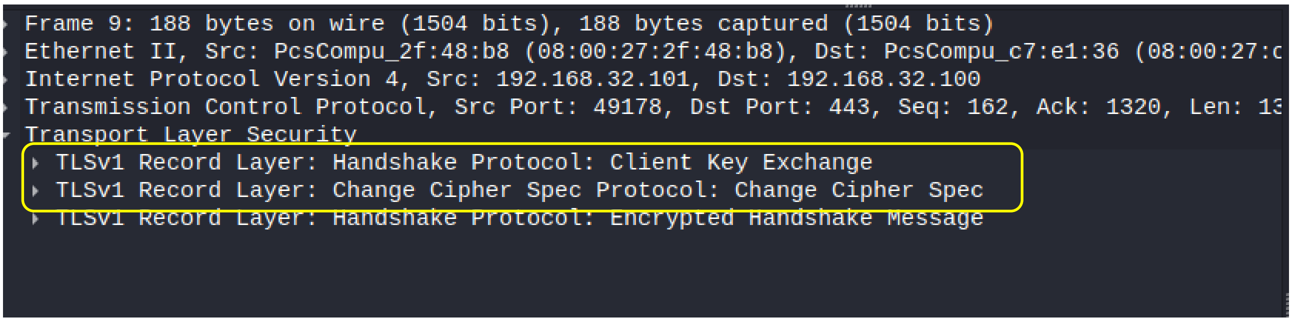


No.	Time	Source	Destination	Protocol	Length	Info
3	0.000173	192.168.32.101	192.168.32.100	TCP	66	49178 → 443 [SY
4	0.000210	192.168.32.100	192.168.32.101	TCP	66	443 → 49178 [SY
5	0.000333	192.168.32.101	192.168.32.100	TCP	60	49178 → 443 [AC
6	0.000538	192.168.32.101	192.168.32.100	TLSv1	215	Client Hello
7	0.000546	192.168.32.100	192.168.32.101	TCP	54	443 → 49178 [AC
8	0.023535	192.168.32.100	192.168.32.101	TLSv1	1373	Server Hello, C
9	0.028781	192.168.32.101	192.168.32.100	TLSv1	188	Client Key Exch
10	0.029114	192.168.32.100	192.168.32.101	TLSv1	113	Change Cipher S
12	0.232324	192.168.32.101	192.168.32.100	TCP	60	49178 → 443 [AC
57	12.481518	192.168.32.101	192.168.32.100	TLSv1	379	Application Dat
58	12.489871	192.168.32.100	192.168.32.101	TLSv1	235	Application Dat
59	12.489946	192.168.32.100	192.168.32.101	TCP	1514	443 → 49178 [AC
60	12.490444	192.168.32.101	192.168.32.100	TCP	60	49178 → 443 [AC
61	12.490464	192.168.32.100	192.168.32.101	TLSv1	1047	Application Dat
62	12.491865	192.168.32.101	192.168.32.100	TCP	60	49178 → 443 [FI
63	12.491886	192.168.32.100	192.168.32.101	TLSv1	91	Encrypted Alert
64	12.491999	192.168.32.100	192.168.32.101	TCP	54	443 → 49178 [FI
65	12.492164	192.168.32.101	192.168.32.100	TCP	60	49178 → 443 [RS

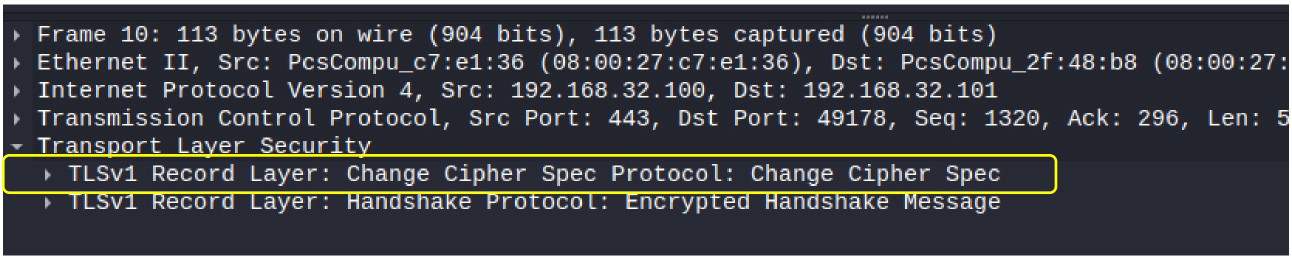
```
▸ Frame 6: 215 bytes on wire (1720 bits), 215 bytes captured (1720 bits)
▸ Ethernet II, Src: PcsCompu_2f:48:b8 (08:00:27:2f:48:b8), Dst: PcsCompu_c7:e1:36 (08:00:27:c
▸ Internet Protocol Version 4, Src: 192.168.32.101, Dst: 192.168.32.100
▸ Transmission Control Protocol, Src Port: 49178, Dst Port: 443, Seq: 1, Ack: 1, Len: 161
▾ Transport Layer Security
  ▸ TLSv1 Record Layer: Handshake Protocol: Client Hello
```



```
▸ Frame 8: 1373 bytes on wire (10984 bits), 1373 bytes captured (10984 bits)
▸ Ethernet II, Src: PcsCompu_c7:e1:36 (08:00:27:c7:e1:36), Dst: PcsCompu_2f:48:b8 (08:00:27:2
▸ Internet Protocol Version 4, Src: 192.168.32.100, Dst: 192.168.32.101
▸ Transmission Control Protocol, Src Port: 443, Dst Port: 49178, Seq: 1, Ack: 162, Len: 1319
▾ Transport Layer Security
  ▸ TLSv1 Record Layer: Handshake Protocol: Server Hello
  ▸ TLSv1 Record Layer: Handshake Protocol: Certificate
  ▸ TLSv1 Record Layer: Handshake Protocol: Server Key Exchange
  ▸ TLSv1 Record Layer: Handshake Protocol: Server Hello Done
```

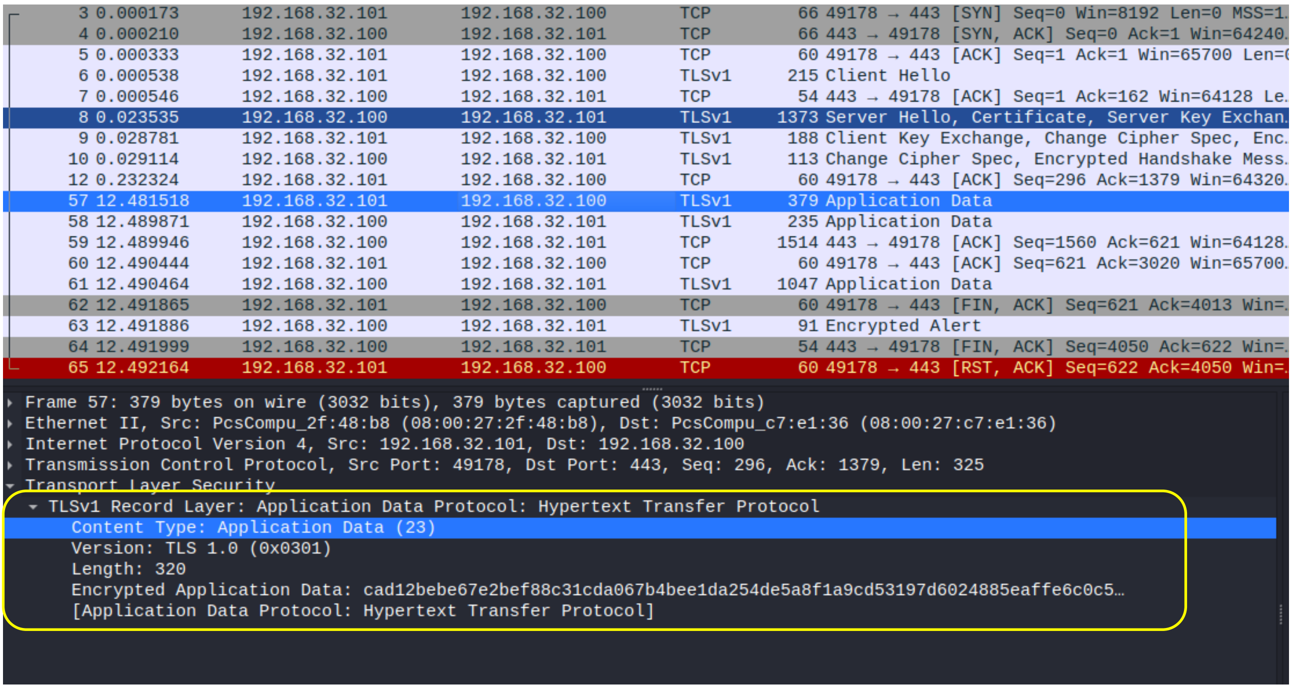


```
▸ Frame 9: 188 bytes on wire (1504 bits), 188 bytes captured (1504 bits)
▸ Ethernet II, Src: PcsCompu_2f:48:b8 (08:00:27:2f:48:b8), Dst: PcsCompu_c7:e1:36 (08:00:27:c
▸ Internet Protocol Version 4, Src: 192.168.32.101, Dst: 192.168.32.100
▸ Transmission Control Protocol, Src Port: 49178, Dst Port: 443, Seq: 162, Ack: 1320, Len: 13
▾ Transport Layer Security
  ▸ TLSv1 Record Layer: Handshake Protocol: Client Key Exchange
  ▸ TLSv1 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
  ▸ TLSv1 Record Layer: Handshake Protocol: Encrypted Handshake Message
```



```
▸ Frame 10: 113 bytes on wire (904 bits), 113 bytes captured (904 bits)
▸ Ethernet II, Src: PcsCompu_c7:e1:36 (08:00:27:c7:e1:36), Dst: PcsCompu_2f:48:b8 (08:00:27:
▸ Internet Protocol Version 4, Src: 192.168.32.100, Dst: 192.168.32.101
▸ Transmission Control Protocol, Src Port: 443, Dst Port: 49178, Seq: 1320, Ack: 296, Len: 5
▾ Transport Layer Security
  ▸ TLSv1 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
  ▸ TLSv1 Record Layer: Handshake Protocol: Encrypted Handshake Message
```

fino ad arrivare alla richiesta vera e propria, che viene trasmessa in formato criptato e non è quindi direttamente leggibile nel pacchetto.



```
 3 0.000173   192.168.32.101  192.168.32.100  TCP      66 49178 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1…
 4 0.000210   192.168.32.100  192.168.32.101  TCP      66 443 → 49178 [SYN, ACK] Seq=0 Ack=1 Win=64240…
 5 0.000333   192.168.32.101  192.168.32.100  TCP      60 49178 → 443 [ACK] Seq=1 Ack=1 Win=65700 Len=(
 6 0.000538   192.168.32.101  192.168.32.100  TLSv1   215 Client Hello
 7 0.000546   192.168.32.100  192.168.32.101  TCP      54 443 → 49178 [ACK] Seq=1 Ack=162 Win=64128 Le…
 8 0.023535   192.168.32.100  192.168.32.101  TLSv1  1373 Server Hello, Certificate, Server Key Exchan…
 9 0.028781   192.168.32.101  192.168.32.100  TLSv1   188 Client Key Exchange, Change Cipher Spec, Enc…
10 0.029114   192.168.32.100  192.168.32.101  TLSv1   113 Change Cipher Spec, Encrypted Handshake Mess…
12 0.232324   192.168.32.101  192.168.32.100  TCP      60 49178 → 443 [ACK] Seq=296 Ack=1379 Win=64320…
57 12.481518  192.168.32.101  192.168.32.100  TLSv1   379 Application Data
58 12.489871  192.168.32.100  192.168.32.101  TLSv1   235 Application Data
59 12.489946  192.168.32.100  192.168.32.101  TCP    1514 443 → 49178 [ACK] Seq=1560 Ack=621 Win=64128…
60 12.490444  192.168.32.101  192.168.32.100  TCP      60 49178 → 443 [ACK] Seq=621 Ack=3020 Win=65700…
61 12.490464  192.168.32.100  192.168.32.101  TLSv1  1047 Application Data
62 12.491865  192.168.32.101  192.168.32.100  TCP      60 49178 → 443 [FIN, ACK] Seq=621 Ack=4013 Win=…
63 12.491886  192.168.32.100  192.168.32.101  TLSv1    91 Encrypted Alert
64 12.491999  192.168.32.100  192.168.32.101  TCP      54 443 → 49178 [FIN, ACK] Seq=4050 Ack=622 Win=…
65 12.492164  192.168.32.101  192.168.32.100  TCP      60 49178 → 443 [RST, ACK] Seq=622 Ack=4050 Win=…
```

```
▸ Frame 57: 379 bytes on wire (3032 bits), 379 bytes captured (3032 bits)
▸ Ethernet II, Src: PcsCompu_2f:48:b8 (08:00:27:2f:48:b8), Dst: PcsCompu_c7:e1:36 (08:00:27:c7:e1:36)
▸ Internet Protocol Version 4, Src: 192.168.32.101, Dst: 192.168.32.100
▸ Transmission Control Protocol, Src Port: 49178, Dst Port: 443, Seq: 296, Ack: 1379, Len: 325
▾ Transport Layer Security
  ▾ TLSv1 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
      Content Type: Application Data (23)
      Version: TLS 1.0 (0x0301)
      Length: 320
      Encrypted Application Data: cad12bebe67e2bef88c31cda067b4bee1da254de5a8f1a9cd53197d6024885eaffe6c0c5…
      [Application Data Protocol: Hypertext Transfer Protocol]
```