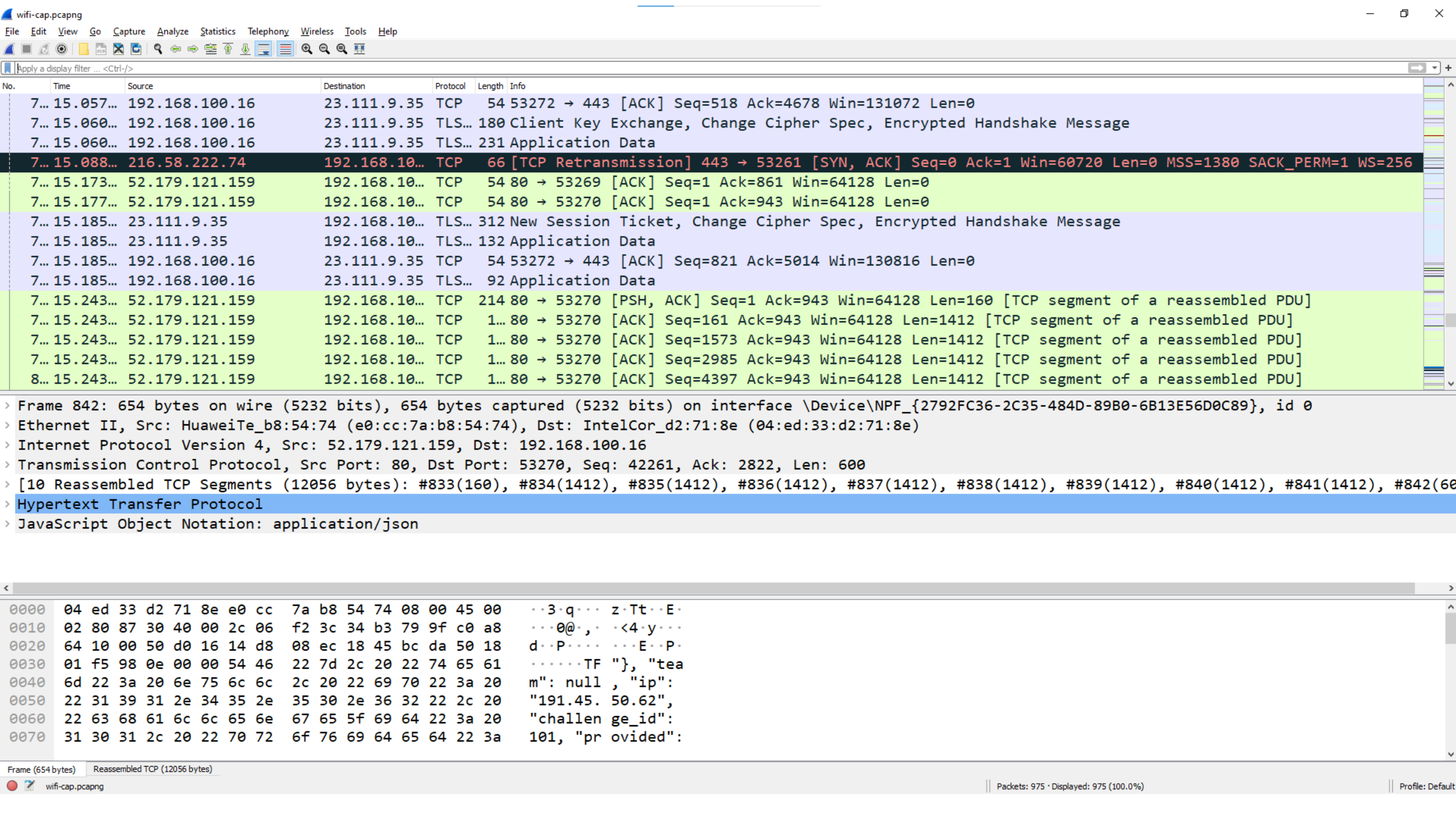
Redes de Computadores

Análise de Redes

Wireshark

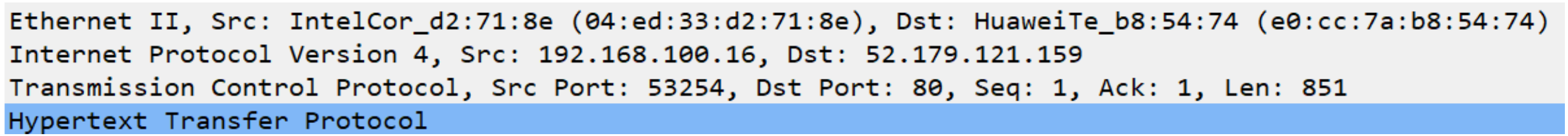

wifi-cap.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
7… 15.057… 192.168.100.16 23.111.9.35 TCP 54 53272 → 443 [ACK] Seq=518 Ack=4678 Win=131072 Len=0
7… 15.060… 192.168.100.16 23.111.9.35 TLS… 180 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
7… 15.060… 192.168.100.16 23.111.9.35 TLS… 231 Application Data
7… 15.088… 216.58.222.74 192.168.10… TCP 66 [TCP Retransmission] 443 → 53261 [SYN, ACK] Seq=0 Ack=1 Win=60720 Len=0 MSS=1380 SACK_PERM=1 WS=256
7… 15.173… 52.179.121.159 192.168.10… TCP 54 80 → 53269 [ACK] Seq=1 Ack=861 Win=64128 Len=0
7… 15.177… 52.179.121.159 192.168.10… TCP 54 80 → 53270 [ACK] Seq=1 Ack=943 Win=64128 Len=0
7… 15.185… 23.111.9.35 192.168.10… TLS… 312 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
7… 15.185… 23.111.9.35 192.168.10… TLS… 132 Application Data
7… 15.185… 192.168.100.16 23.111.9.35 TCP 54 53272 → 443 [ACK] Seq=821 Ack=5014 Win=130816 Len=0
7… 15.185… 192.168.100.16 23.111.9.35 TLS… 92 Application Data
7… 15.243… 52.179.121.159 192.168.10… TCP 214 80 → 53270 [PSH, ACK] Seq=1 Ack=943 Win=64128 Len=160 [TCP segment of a reassembled PDU]
7… 15.243… 52.179.121.159 192.168.10… TCP 1… 80 → 53270 [ACK] Seq=161 Ack=943 Win=64128 Len=1412 [TCP segment of a reassembled PDU]
7… 15.243… 52.179.121.159 192.168.10… TCP 1… 80 → 53270 [ACK] Seq=1573 Ack=943 Win=64128 Len=1412 [TCP segment of a reassembled PDU]
7… 15.243… 52.179.121.159 192.168.10… TCP 1… 80 → 53270 [ACK] Seq=2985 Ack=943 Win=64128 Len=1412 [TCP segment of a reassembled PDU]
8… 15.243… 52.179.121.159 192.168.10… TCP 1… 80 → 53270 [ACK] Seq=4397 Ack=943 Win=64128 Len=1412 [TCP segment of a reassembled PDU]
Frame 842: 654 bytes on wire (5232 bits), 654 bytes captured (5232 bits) on interface \Device\NPF_{2792FC36-2C35-484D-89B0-6B13E56D0C89}, id 0
Ethernet II, Src: HuaweiTe_b8:54:74 (e0:cc:7a:b8:54:74), Dst: IntelCor_d2:71:8e (04:ed:33:d2:71:8e)
Internet Protocol Version 4, Src: 52.179.121.159, Dst: 192.168.100.16
Transmission Control Protocol, Src Port: 80, Dst Port: 53270, Seq: 42261, Ack: 2822, Len: 600
[10 Reassembled TCP Segments (12056 bytes): #833(160), #834(1412), #835(1412), #836(1412), #837(1412), #838(1412), #839(1412), #840(1412), #841(1412), #842(60
Hypertext Transfer Protocol
JavaScript Object Notation: application/json
0000 04 ed 33 d2 71 8e e0 cc 7a b8 54 74 08 00 45 00 ··3·q··· z·Tt··E·
0010 02 80 87 30 40 00 2c 06 f2 3c 34 b3 79 9f c0 a8 ···0@·,· ·<4·y···
0020 64 10 00 50 d0 16 14 d8 08 ec 18 45 bc da 50 18 d··P···· ···E··P·
0030 01 f5 98 0e 00 00 54 46 22 7d 2c 20 22 74 65 61 ·····TF "}, "tea
0040 6d 22 3a 20 6e 75 6c 6c 2c 20 22 69 70 22 3a 20 m": null , "ip":
0050 22 31 39 31 2e 34 35 2e 35 30 2e 36 32 22 2c 20 "191.45. 50.62",
0060 22 63 68 61 6c 6c 65 6e 67 65 5f 69 64 22 3a 20 "challen ge_id":
0070 31 30 31 2c 20 22 70 72 6f 76 69 64 65 64 22 3a 101, "pr ovided":
Frame (654 bytes)
Reassembled TCP (12056 bytes)
wifi-cap.pcapng
Packets: 975 · Displayed: 975 (100.0%)
Profile: Default

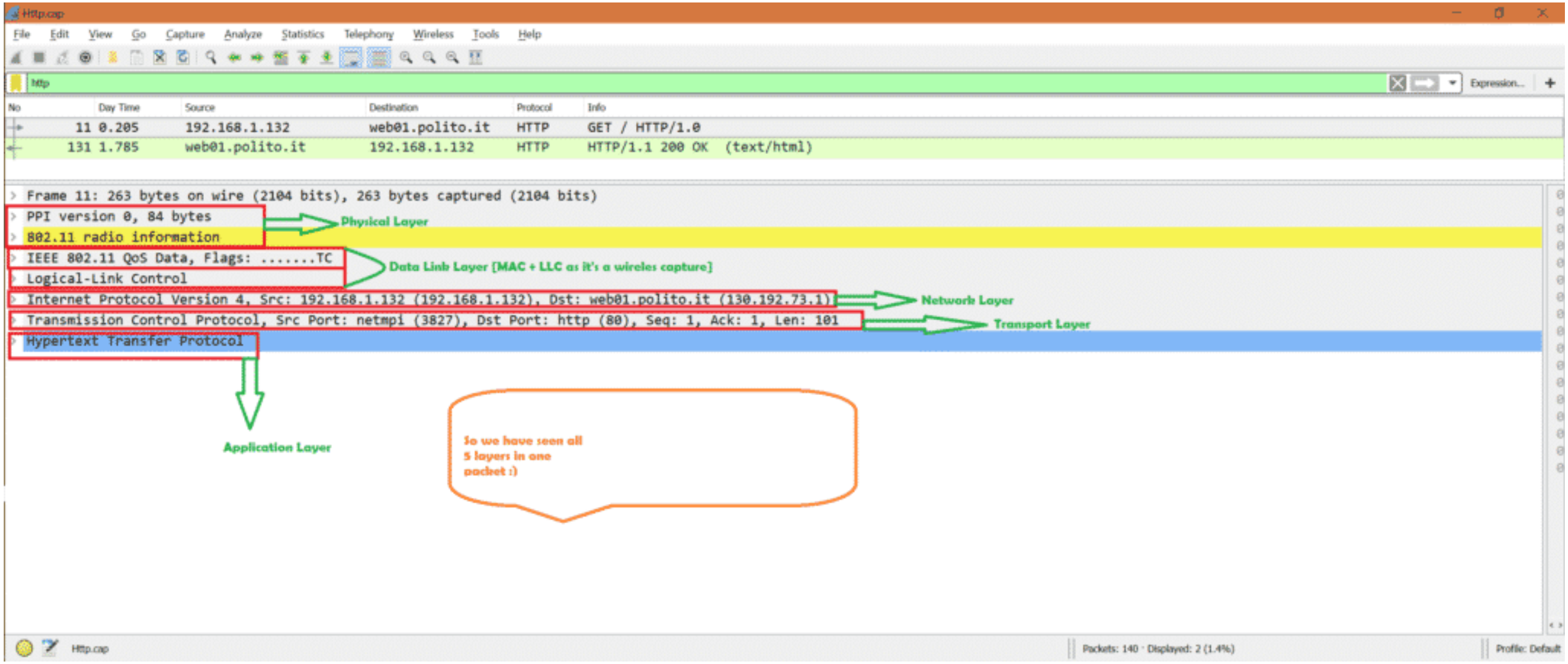
OSI Model	TCP/IP Model
Application Layer	Application Layer
Presentation Layer	
Session Layer	
Transport Layer	Transport Layer
Network Layer	Internet Layer
Data Link Layer	Network access Layer
Physical Layer	

Como o Wireshark espera

Camadas	
Application Layer	[Layer 5]
Transport Layer	[Layer 4]
Network Layer	[Layer 3]
Data Link Layer	[Layer 2]
Physical Layer*	[Layer 1]

Camadas no http (exemplo)




Http.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression...
No Day Time Source Destination Protocol Info
11 0.205 192.168.1.132 web01.polito.it HTTP GET / HTTP/1.0
131 1.785 web01.polito.it 192.168.1.132 HTTP HTTP/1.1 200 OK (text/html)
Frame 11: 263 bytes on wire (2104 bits), 263 bytes captured (2104 bits)
PPI version 0, 84 bytes
802.11 radio information
Physical Layer
IEEE 802.11 QoS Data, Flags: ....TC
Logical-Link Control
Data Link Layer [MAC + LLC as it's a wireles capture]
Internet Protocol Version 4, Src: 192.168.1.132 (192.168.1.132), Dst: web01.polito.it (130.192.73.1)
Network Layer
Transmission Control Protocol, Src Port: netmpi (3827), Dst Port: http (80), Seq: 1, Ack: 1, Len: 101
Transport Layer
Hypertext Transfer Protocol
Application Layer
So we have seen all
5 layers in one
packet :)
Http.cap
Packets: 140 · Displayed: 2 (1.4%)
Profile: Default

Prática!