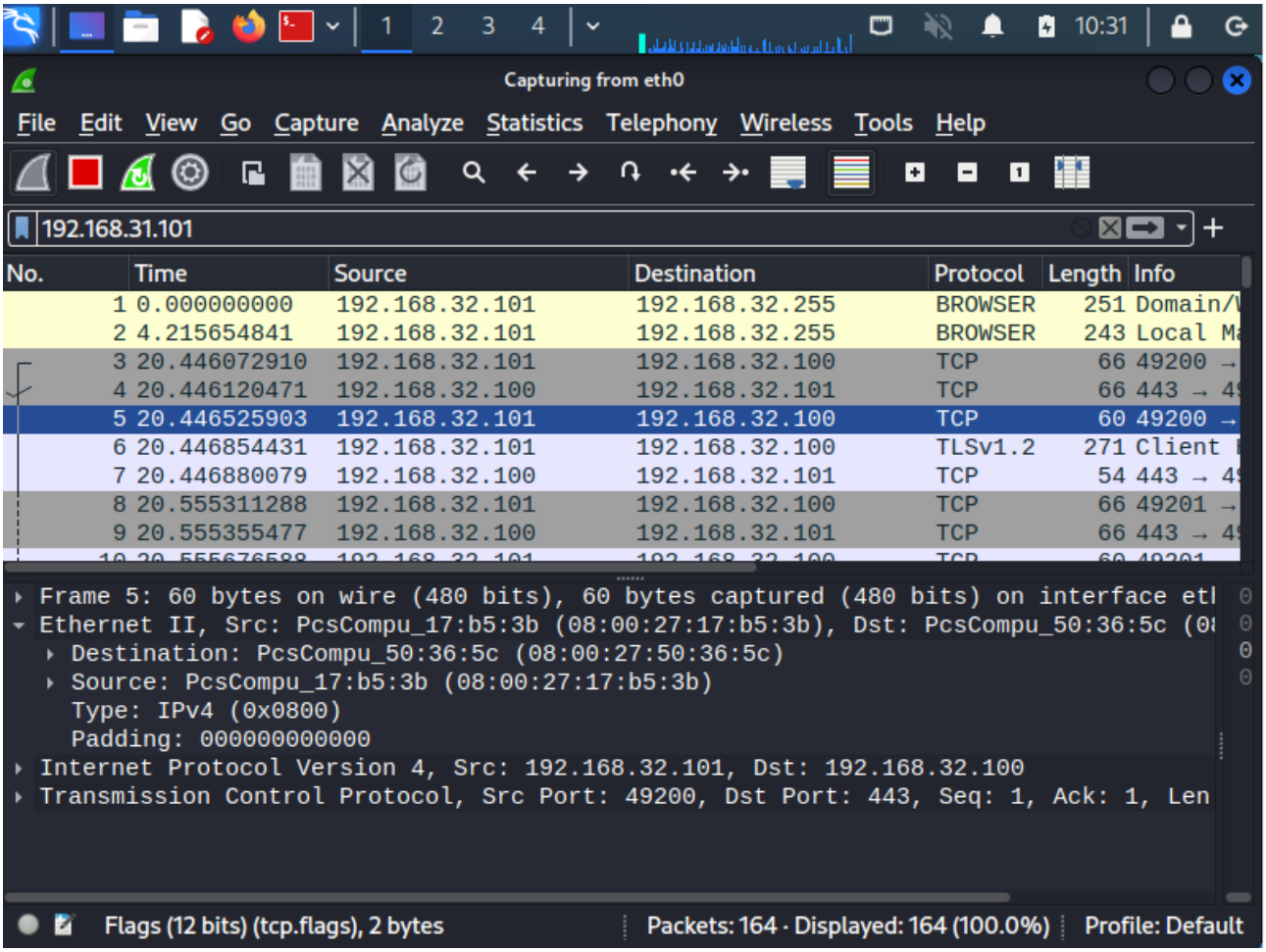
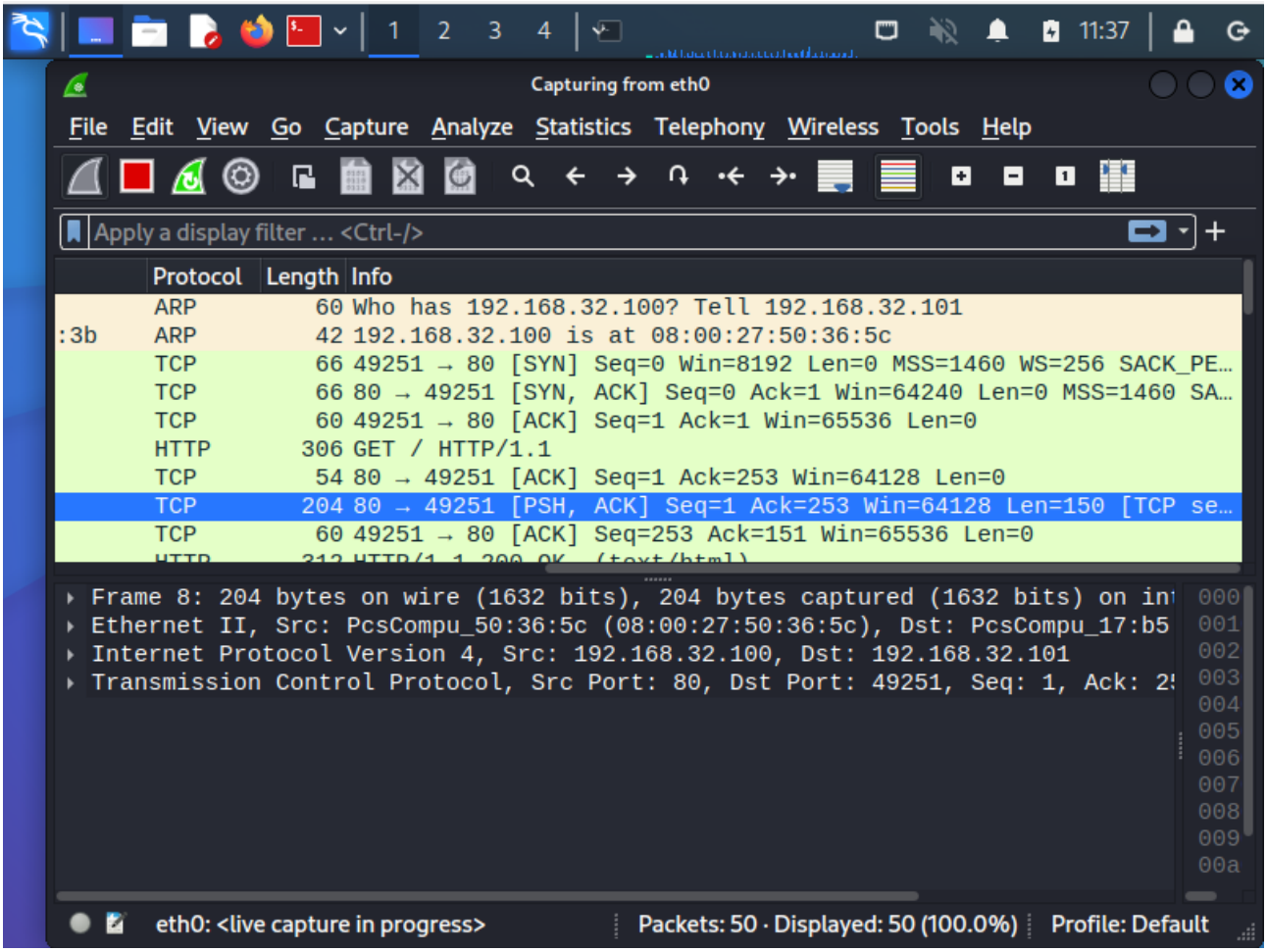
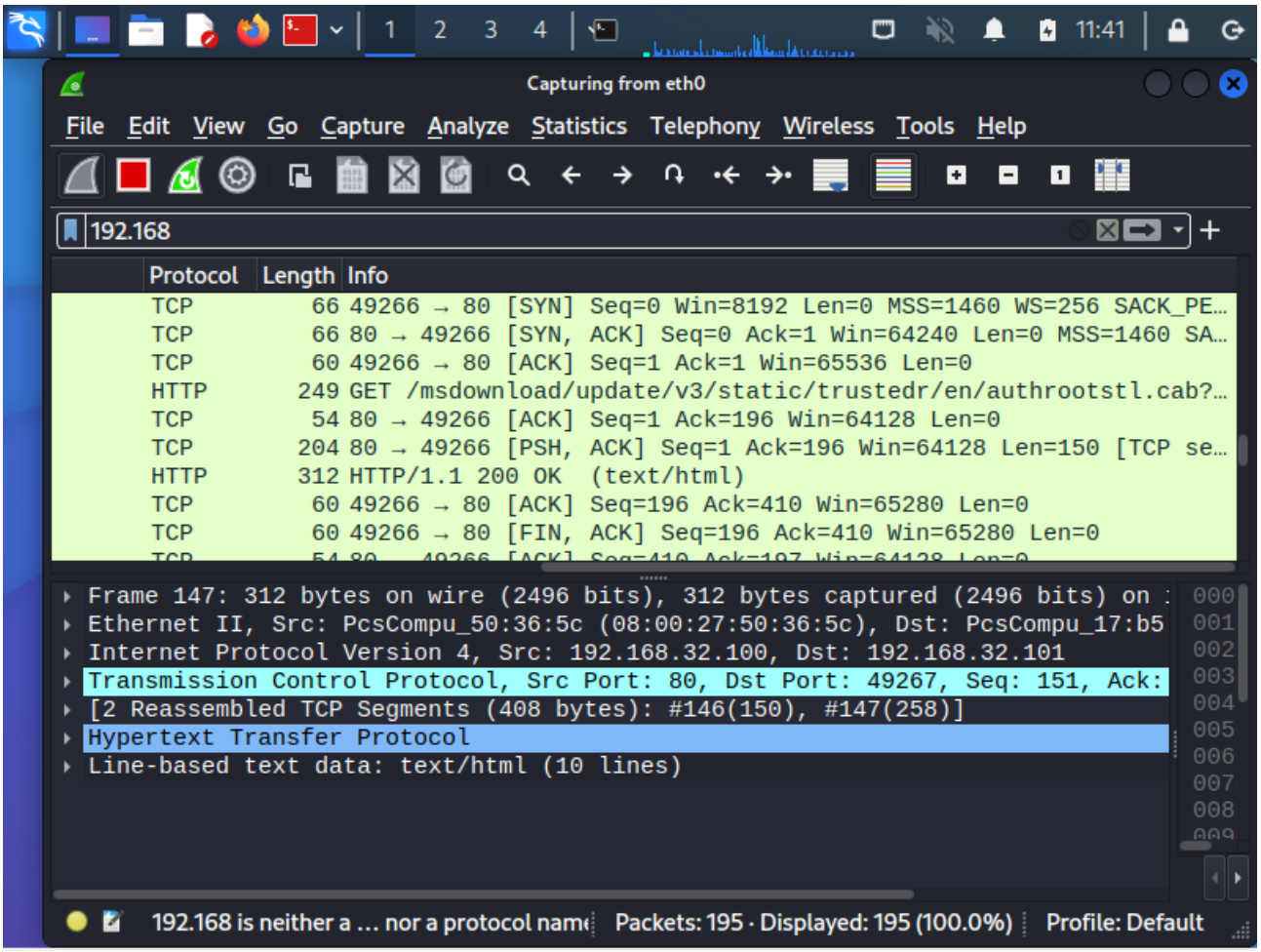
Nell esercizi di oggi e precisamente nello screen sotto dimostro 1 che ho cambiato i due indirizzi ip di della machina con linux e mac e, su whire shark, dpo aver stabilito l connessione fra windows ed un server https (linux in questo caso il quale e stato impostato anche come dns per dar modo a windows 7 dileggere la pagina epicode.internal come indirizzo ip) sul frame 2 (pacchetto a livello data) evidenzio il MAC fra le due macchine :

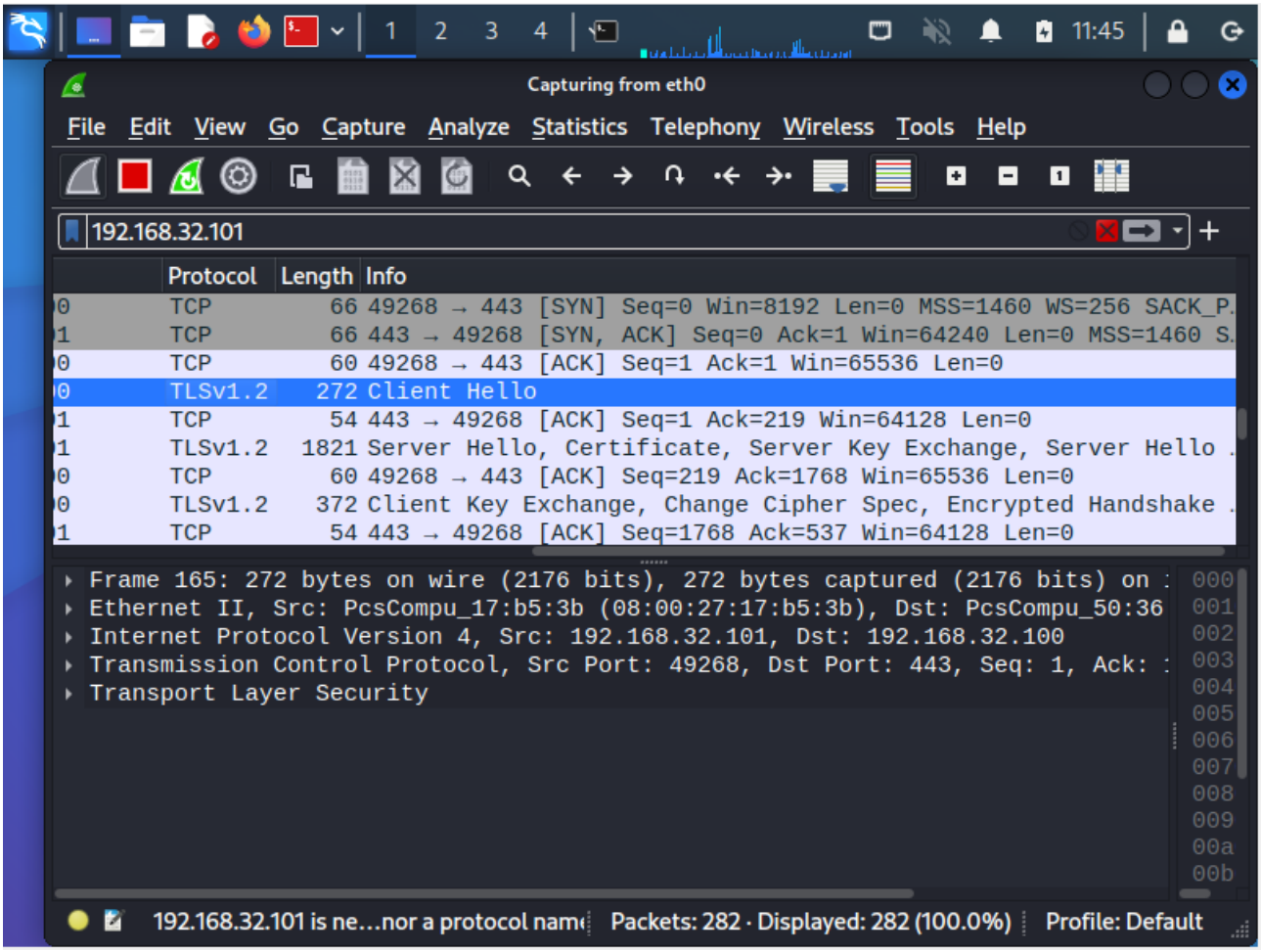


Per l esattezza 08:00:27:17:b5:3b e il mac del source address, ovvero il pc windows, mentre l'altro appartiene al server https (macchina linux per impostazione).

Infine ci viene chiesto di levare l impostazione https dalla macchina linux e farla diventare un server htttp e studiare le differenze:


1 2 3 4
11:37
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Protocol Length Info
ARP 60 Who has 192.168.32.100? Tell 192.168.32.101
:3b ARP 42 192.168.32.100 is at 08:00:27:50:36:5c
TCP 66 49251 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PE…
TCP 66 80 → 49251 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SA…
TCP 60 49251 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
HTTP 306 GET / HTTP/1.1
TCP 54 80 → 49251 [ACK] Seq=1 Ack=253 Win=64128 Len=0
TCP 204 80 → 49251 [PSH, ACK] Seq=1 Ack=253 Win=64128 Len=150 [TCP se…
TCP 60 49251 → 80 [ACK] Seq=253 Ack=151 Win=65536 Len=0
Frame 8: 204 bytes on wire (1632 bits), 204 bytes captured (1632 bits) on int
Ethernet II, Src: PcsCompu_50:36:5c (08:00:27:50:36:5c), Dst: PcsCompu_17:b5
Internet Protocol Version 4, Src: 192.168.32.100, Dst: 192.168.32.101
Transmission Control Protocol, Src Port: 80, Dst Port: 49251, Seq: 1, Ack: 2
000
001
002
003
004
005
006
007
008
009
00a
eth0: <live capture in progress>
Packets: 50 · Displayed: 50 (100.0%)
Profile: Default


1 2 3 4
11:41
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
192.168
Protocol Length Info
TCP 66 49266 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PE…
TCP 66 80 → 49266 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SA…
TCP 60 49266 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
HTTP 249 GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab?…
TCP 54 80 → 49266 [ACK] Seq=1 Ack=196 Win=64128 Len=0
TCP 204 80 → 49266 [PSH, ACK] Seq=1 Ack=196 Win=64128 Len=150 [TCP se…
HTTP 312 HTTP/1.1 200 OK (text/html)
TCP 60 49266 → 80 [ACK] Seq=196 Ack=410 Win=65280 Len=0
TCP 60 49266 → 80 [FIN, ACK] Seq=196 Ack=410 Win=65280 Len=0
Frame 147: 312 bytes on wire (2496 bits), 312 bytes captured (2496 bits) on
Ethernet II, Src: PcsCompu_50:36:5c (08:00:27:50:36:5c), Dst: PcsCompu_17:b5
Internet Protocol Version 4, Src: 192.168.32.100, Dst: 192.168.32.101
Transmission Control Protocol, Src Port: 80, Dst Port: 49267, Seq: 151, Ack:
[2 Reassembled TCP Segments (408 bytes): #146(150), #147(258)]
Hypertext Transfer Protocol
Line-based text data: text/html (10 lines)
192.168 is neither a … nor a protocol name
Packets: 195 · Displayed: 195 (100.0%)
Profile: Default



Con questi due screen dimostriamo qualche differenza i dati fra windows ed i due server:

innanzitutto cambia la porta che,come sappiamo, per https è 443 e per http è 80. Nell'https che come sappiamo e piu sicura, e presente il protocollo tls che cripta il pacchetto, difatti se clicchiamo sul pacchetto dati interconnesso fra windows ed http è leggibile, mentre per https è criptato.