

Figure 1.1. Wireshark initial showing interfaces (sudo mode)

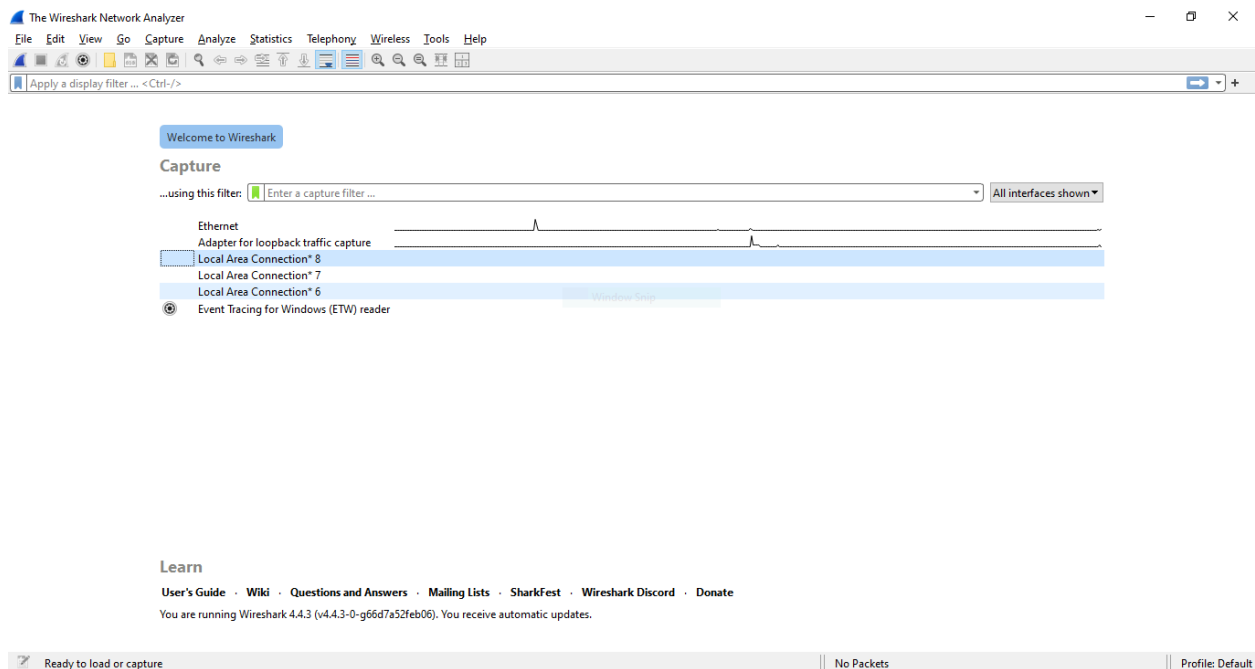


Figure 1.2. An example of a Wireshark capture.

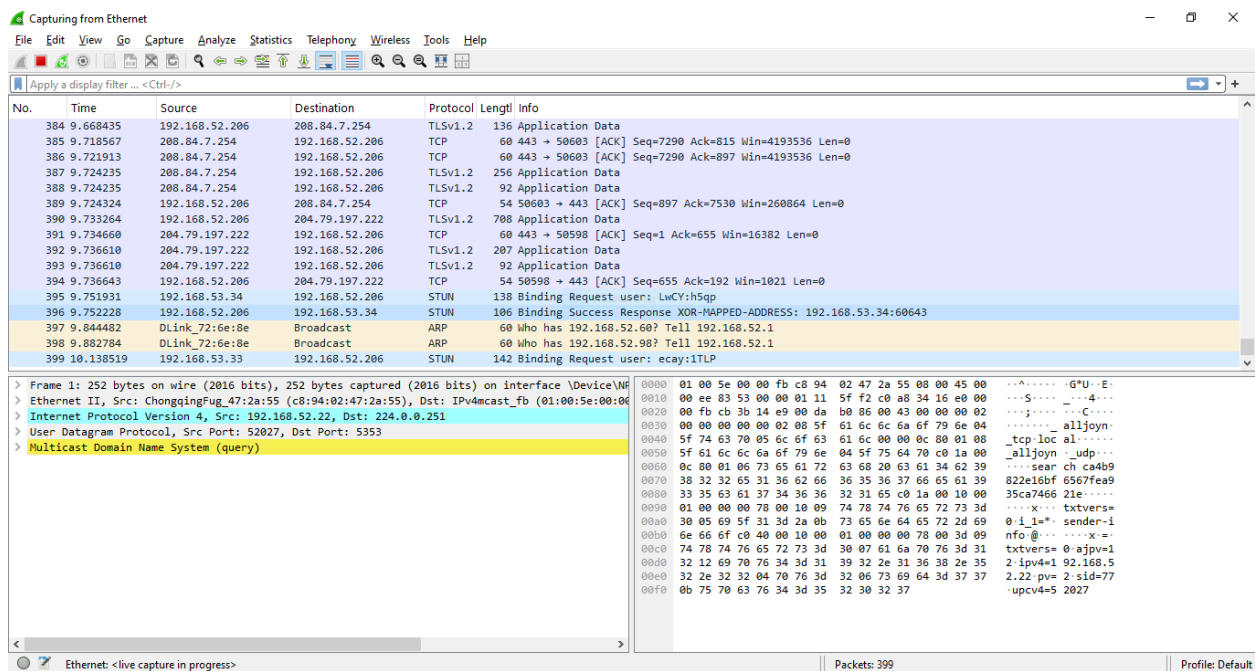


Figure 2. The summary before the protocols in a Wireshark packet. Information about the packet characteristic.

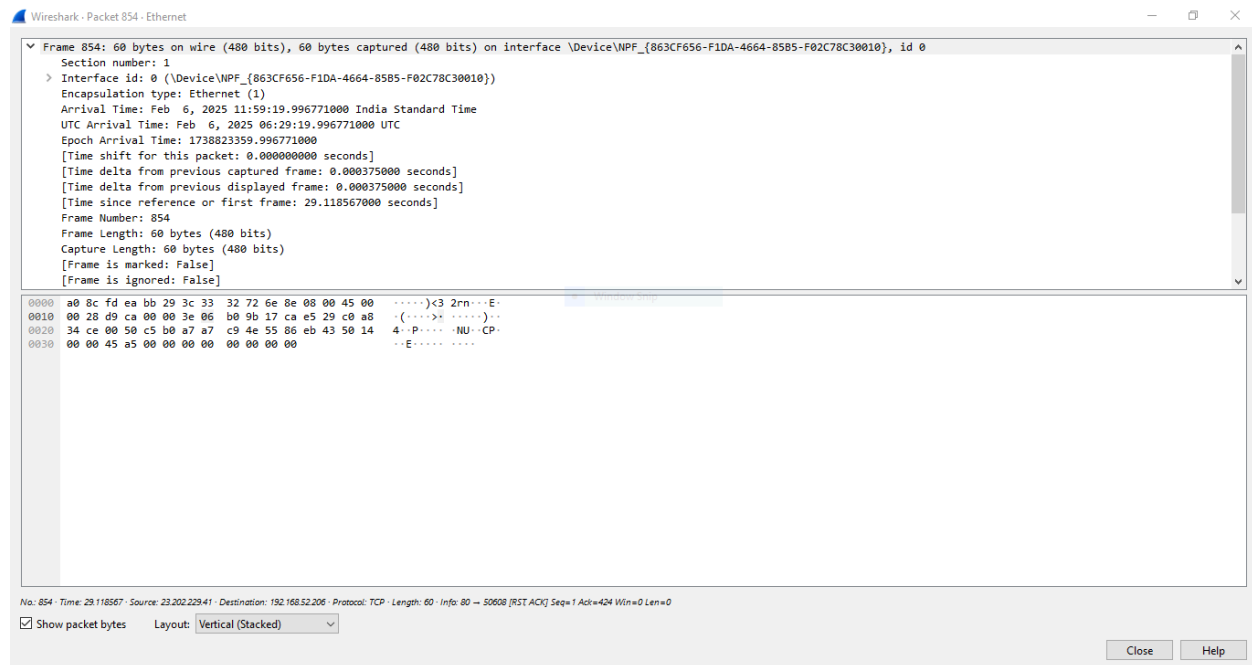


Figure 3. Ethernet II (Layer 2) header along with the Wireshark

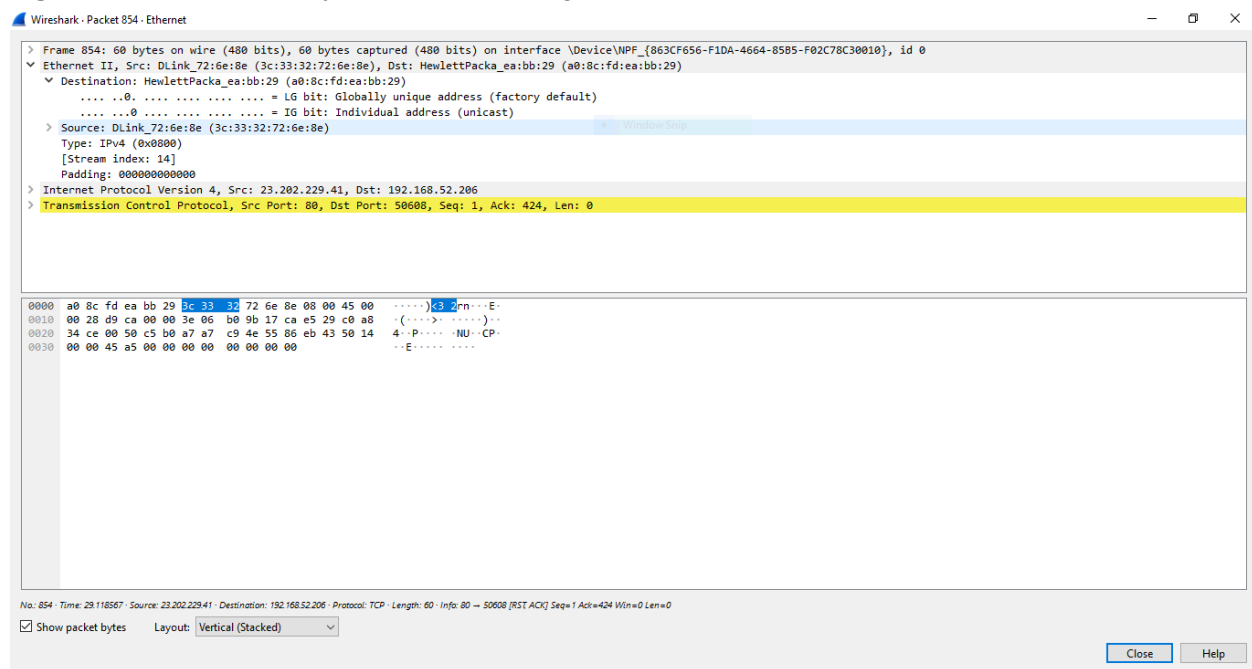


Figure 4. IP Header (Layer-3)

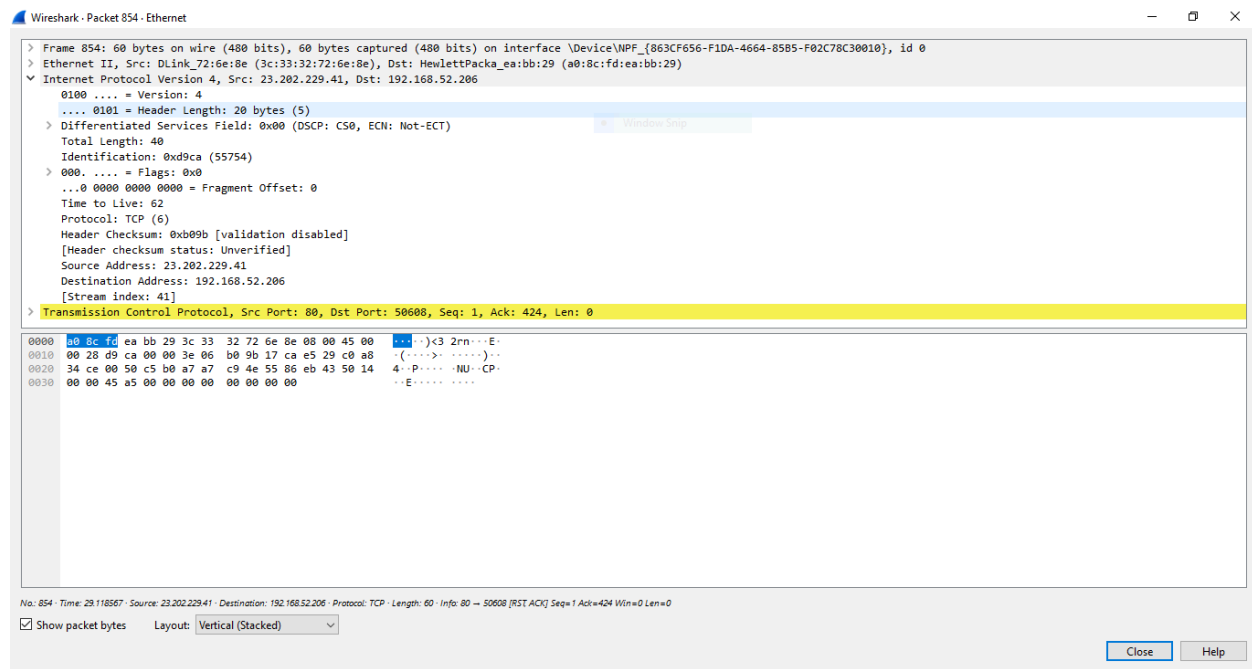
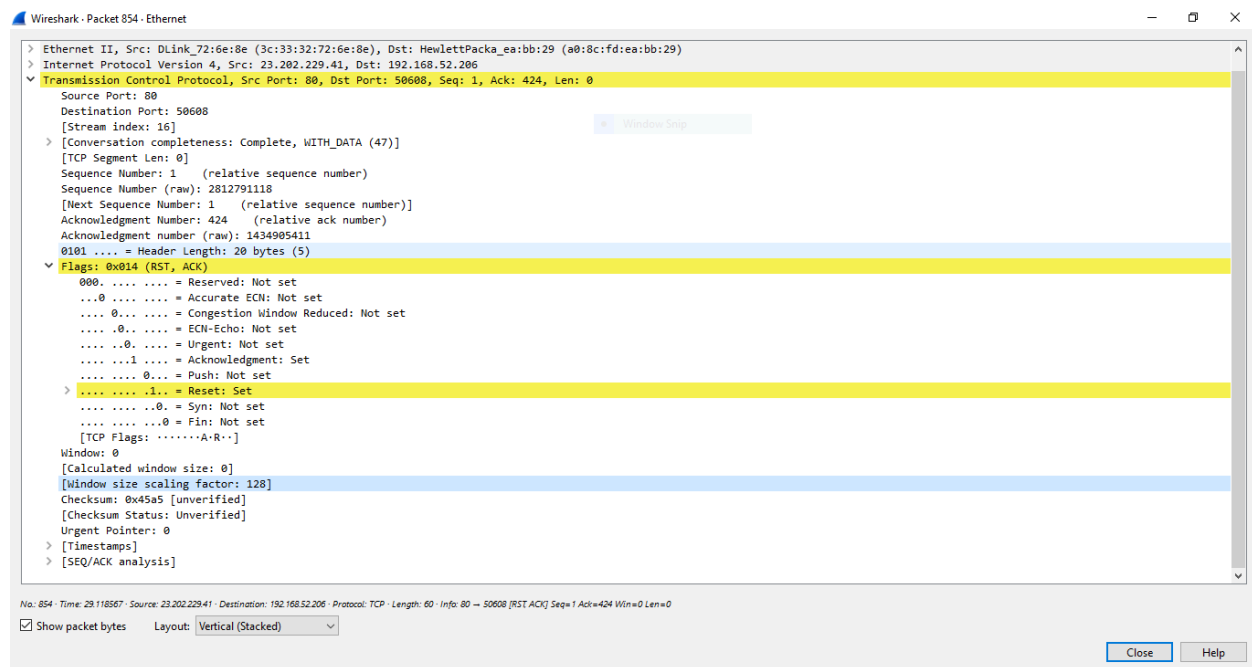


Figure 5. TCP headers.



TCP Three-way Handshake

No.	Time	Source	Destination	Protocol	Length	Info
7272	299.760753	13.107.3.254	192.168.52.206	TCP	60	443 → 50641 [ACK] Seq=6282 Ack=361 Win=4194048 Len=0
7273	299.762675	13.107.3.254	192.168.52.206	TCP	66	[TCP Dup ACK 7272#1] 443 → 50641 [ACK] Seq=6282 Ack=361 Win=4194048 Len=0 SLE=448 SRE=773
7274	299.762675	13.107.3.254	192.168.52.206	TCP	60	443 → 50641 [ACK] Seq=6282 Ack=773 Win=4193792 Len=0
7275	299.763689	13.107.3.254	192.168.52.206	TLSv1.2	396	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
7276	299.763689	13.107.3.254	192.168.52.206	TLSv1.2	123	Application Data
7277	299.763728	192.168.52.206	13.107.3.254	TCP	54	50641 → 443 [ACK] Seq=773 Ack=6693 Win=261632 Len=0
7278	299.764304	192.168.52.206	13.107.3.254	TLSv1.2	92	Application Data
7279	299.766723	13.107.3.254	192.168.52.206	TLSv1.2	607	Application Data, Application Data
7280	299.766723	13.107.3.254	192.168.52.206	TLSv1.2	92	Application Data
7281	299.766761	192.168.52.206	13.107.3.254	TCP	54	50641 → 443 [ACK] Seq=811 Ack=7284 Win=261120 Len=0
7282	299.771801	13.107.3.254	192.168.52.206	TCP	60	443 → 50641 [ACK] Seq=7284 Ack=811 Win=4193536 Len=0
7283	299.775450	192.168.52.206	13.107.3.254	TLSv1.2	136	Application Data
7284	299.782309	13.107.3.254	192.168.52.206	TCP	60	443 → 50641 [ACK] Seq=7284 Ack=893 Win=4193536 Len=0
7285	299.786516	13.107.3.254	192.168.52.206	TLSv1.2	254	Application Data
7286	299.786516	13.107.3.254	192.168.52.206	TLSv1.2	92	Application Data
7287	299.786551	192.168.52.206	13.107.3.254	TCP	54	50641 → 443 [ACK] Seq=893 Ack=7522 Win=260864 Len=0

> Frame 7274: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF...

> Ethernet II, Src: DLink_72:6e:8e (3c:33:32:72:6e:8e), Dst: HewlettPacka_ea:bb:29 (a0:8c:fd:15:5a:2d)

> Internet Protocol Version 4, Src: 13.107.3.254, Dst: 192.168.52.206

> Transmission Control Protocol, Src Port: 443, Dst Port: 50641, Seq: 6282, Ack: 773, Len: 0

Source Port: 443

Destination Port: 50641

[Stream index: 69]

> [Conversation completeness: Incomplete, DATA (15)]

[TCP Segment Len: 0]

Sequence Number: 6282 (relative sequence number)

Sequence Number (raw): 877499652

[Next Sequence Number: 6282 (relative sequence number)]

Acknowledgment Number: 773 (relative ack number)

Acknowledgment number (raw): 309502018

0101 = Header Length: 20 bytes (5)

Flags: 0x010 (ACK)

0000 = Reserved: Not set

0000 a0 8c fd ea bb 29 3c 33 32 72 6e 8e 08 00 45 00<3 2n...E-

0010 00 28 5a 2d 40 00 75 06 a4 c3 0d 6b 03 fe c0 a8 ..(Z:@u...k....

0020 34 ce 01 bb c5 d1 34 4d 95 04 12 72 a0 42 50 10 4.....4M...nBP-

0030 3f fe 25 64 00 00 00 00 00 00 00 00 00 00 00 00 ?%d.....

Ethernet: <live capture in progress> Packets: 9459 Profile: Default