

Internship day-3 Report

19-01-2026

1. Wireshark Packet Capture File (PCAP)

The image displays the Wireshark network protocol analyzer interface. The top pane shows a list of captured packets with columns for No., Delta, Time, Source, Destination, Protocol, Length, and Info. The middle pane shows the details of the selected packet (No. 14857), including Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Data (1250 bytes). The bottom pane shows the packet's structure as a diagram with Source and Destination fields.

No.	Delta	Time	Source	Destination	Protocol	Length	Info
14825	0.000000	26.785581	23.223.243.67	172.20.10.4	TCP	1394	443 → 49410 [ACK] Seq=8695208 Ack=1 Win=501 Len=1340 [TCP PDU reassembled in 14828]
14826	0.000000	26.785581	23.223.243.67	172.20.10.4	TCP	1394	443 → 49410 [PSH, ACK] Seq=8695548 Ack=1 Win=501 Len=1340 [TCP PDU reassembled in 14828]
14827	0.000091	26.785672	172.20.10.4	23.223.243.67	TCP	54	49410 → 443 [ACK] Seq=1 Ack=8697888 Win=4095 Len=0
14828	0.005825	26.791497	23.223.243.67	172.20.10.4	SSLv2	1394	Encrypted Data
14829	0.000000	26.791497	23.223.243.67	172.20.10.4	TCP	1394	443 → 49410 [PSH, ACK] Seq=8699228 Ack=1 Win=501 Len=1340 [TCP PDU reassembled in 14835]
14830	0.000074	26.791571	172.20.10.4	23.223.243.67	TCP	54	49410 → 443 [ACK] Seq=1 Ack=8700568 Win=4095 Len=0
14831	0.000046	26.797617	42.105.255.12	172.20.10.4	UDP	1292	443 → 56295 Len=1250
14832	0.000000	26.797617	42.105.255.12	172.20.10.4	UDP	1292	443 → 56295 Len=1250
14833	0.000000	26.797617	42.105.255.12	172.20.10.4	UDP	1292	443 → 56295 Len=1250
14834	0.000000	26.797617	23.223.243.67	172.20.10.4	TCP	1394	443 → 49410 [ACK] Seq=8700568 Ack=1 Win=501 Len=1340 [TCP PDU reassembled in 14835]
14835	0.003941	26.801558	23.223.243.67	172.20.10.4	SSLv2	1394	Encrypted Data
14836	0.000000	26.801558	23.223.243.67	172.20.10.4	TCP	1394	443 → 49410 [ACK] Seq=8703248 Ack=1 Win=501 Len=1340 [TCP PDU reassembled in 14838]
14837	0.000000	26.801558	23.223.243.67	172.20.10.4	TCP	1394	443 → 49410 [PSH, ACK] Seq=8704588 Ack=1 Win=501 Len=1340 [TCP PDU reassembled in 14838]
14838	0.000000	26.801558	23.223.243.67	172.20.10.4	SSLv2	1394	Encrypted Data
14839	0.000153	26.801711	172.20.10.4	23.223.243.67	TCP	54	49410 → 443 [ACK] Seq=1 Ack=8707268 Win=4095 Len=0
14840	0.000721	26.808432	23.223.243.67	172.20.10.4	TCP	1394	443 → 49410 [PSH, ACK] Seq=8707268 Ack=1 Win=501 Len=1340 [TCP PDU reassembled in 14844]
14841	0.000091	26.808523	172.20.10.4	23.223.243.67	TCP	54	49410 → 443 [ACK] Seq=1 Ack=8708608 Win=4095 Len=0
14842	0.003292	26.811815	172.20.10.4	42.105.255.12	UDP	78	56295 → 443 Len=36
14843	0.001704	26.813519	142.251.222.206	172.20.10.4	UDP	67	443 → 49974 Len=25
14844	0.000000	26.813519	23.223.243.67	172.20.10.4	SSLv2	1394	Encrypted Data
14845	0.000000	26.813519	23.223.243.67	172.20.10.4	TCP	1394	443 → 49410 [PSH, ACK] Seq=8709948 Ack=1 Win=501 Len=1340 [TCP PDU reassembled in 14856]
14846	0.000000	26.813519	42.105.255.12	172.20.10.4	UDP	1292	443 → 56295 Len=1250
14847	0.000128	26.813647	172.20.10.4	23.223.243.67	TCP	54	49410 → 443 [ACK] Seq=1 Ack=8711288 Win=4095 Len=0
14848	0.002594	26.816241	23.223.243.67	172.20.10.4	TCP	1394	443 → 49410 [ACK] Seq=8711288 Ack=1 Win=501 Len=1340 [TCP PDU reassembled in 14856]
14849	0.000000	26.816241	23.223.243.67	172.20.10.4	TCP	1394	443 → 49410 [PSH, ACK] Seq=8712628 Ack=1 Win=501 Len=1340 [TCP PDU reassembled in 14856]
14850	0.000000	26.816241	23.223.243.67	172.20.10.4	TCP	1394	443 → 49410 [ACK] Seq=8713968 Ack=1 Win=501 Len=1340 [TCP PDU reassembled in 14856]
14851	0.000094	26.816355	172.20.10.4	23.223.243.67	TCP	54	49410 → 443 [ACK] Seq=1 Ack=8715308 Win=4095 Len=0
14852	0.005165	26.821500	23.223.243.67	172.20.10.4	TCP	1394	443 → 49410 [PSH, ACK] Seq=8715308 Ack=1 Win=501 Len=1340 [TCP PDU reassembled in 14856]
14853	0.000000	26.821500	142.250.207.206	172.20.10.4	UDP	328	443 → 55752 Len=286
14854	0.000000	26.821500	142.250.207.206	172.20.10.4	UDP	67	443 → 55752 Len=25
14855	0.000000	26.821500	23.223.243.67	172.20.10.4	TCP	1394	443 → 49410 [ACK] Seq=8716648 Ack=1 Win=501 Len=1340 [TCP PDU reassembled in 14856]
14856	0.000000	26.821500	23.223.243.67	172.20.10.4	SSLv2	1394	Encrypted Data
14857	0.000116	26.821616	172.20.10.4	23.223.243.67	TCP	54	49410 → 443 [ACK] Seq=1 Ack=8716648 Win=4095 Len=0

2. HTTP Filter Packets

No.	Delta	Time	Source	Destination	Protocol	Length	Info
45.	0.00060	18.738	14.102	172.20.10.4	TCP	1346	80 → 49826 [PSH, ACK] Seq=217681 Ack=1 Win=22 Len=1280 TSval=3293457814 TSecr=747155
46.	0.0000	18.738	14.102	172.20.10.4	TCP	1346	80 → 49826 [ACK] Seq=218881 Ack=1 Win=22 Len=1280 TSval=3293457814 TSecr=747155
47.	0.0000	18.738	14.102	172.20.10.4	TCP	1346	80 → 49826 [PSH, ACK] Seq=2208161 Ack=1 Win=22 Len=1280 TSval=3293457814 TSecr=747156
48.	0.0000	18.738	14.102	172.20.10.4	TCP	1346	80 → 49826 [ACK] Seq=221441 Ack=1 Win=22 Len=1280 TSval=3293457814 TSecr=747156
49.	0.0000	18.738	172.20	14.102.231.2	TCP	66	49826 → 80 [ACK] Seq=1 Ack=222721 Win=33 Len=0 TSval=747964 TSecr=3293457814
50.	0.0018	18.740	14.102	172.20.10.4	TCP	1346	80 → 49826 [PSH, ACK] Seq=222721 Ack=1 Win=22 Len=1280 TSval=3293457814 TSecr=747156
51.	0.0059	18.746	14.102	172.20.10.4	TCP	1346	80 → 49826 [ACK] Seq=224001 Ack=1 Win=22 Len=1280 TSval=3293457814 TSecr=747156
52.	0.0000	18.746	14.102	172.20.10.4	TCP	1346	80 → 49826 [PSH, ACK] Seq=225281 Ack=1 Win=22 Len=1280 TSval=3293457814 TSecr=747156
53.	0.0000	18.746	172.20	14.102.231.2	TCP	66	49826 → 80 [ACK] Seq=1 Ack=226561 Win=18 Len=0 TSval=747972 TSecr=3293457814
54.	0.0059	18.752	14.102	172.20.10.4	TCP	1346	80 → 49826 [ACK] Seq=226561 Ack=1 Win=22 Len=1280 TSval=3293457814 TSecr=747156
55.	0.0000	18.752	172.20	14.102.231.2	TCP	1346	80 → 49826 [PSH, ACK] Seq=227841 Ack=1 Win=22 Len=1280 TSval=3293457814 TSecr=747156
56.	0.0000	18.752	172.20	14.102.231.2	TCP	66	49826 → 80 [ACK] Seq=1 Ack=229121 Win=17 Len=0 TSval=747978 TSecr=3293457814
57.	0.0017	18.754	14.102	172.20.10.4	TCP	1346	80 → 49826 [ACK] Seq=229121 Ack=1 Win=22 Len=1280 TSval=3293457814 TSecr=747156
58.	0.0000	18.754	172.20	14.102.231.2	TCP	66	49826 → 80 [ACK] Seq=1 Ack=230401 Win=17 Len=0 TSval=747980 TSecr=3293457814
59.	0.0069	18.931	172.20	23.192.115.98	TCP	54	50706 → 80 [FIN, ACK] Seq=1 Ack=1 Win=254 Len=0
60.	0.0000	19.022	23.192	172.20.10.4	TCP	54	80 → 50706 [FIN, ACK] Seq=1 Ack=2 Win=501 Len=0
61.	0.0000	19.022	172.20	23.192.115.98	TCP	54	50706 → 80 [ACK] Seq=2 Ack=2 Win=254 Len=0
62.	0.0015	19.058	14.102	172.20.10.4	TCP	1346	80 → 49826 [PSH, ACK] Seq=230401 Ack=1 Win=22 Len=1280 TSval=3293458652 TSecr=747978
63.	0.0054	19.064	14.102	172.20.10.4	TCP	1346	80 → 49826 [ACK] Seq=231681 Ack=1 Win=22 Len=1280 TSval=3293458652 TSecr=747978
64.	0.0000	19.064	14.102	172.20.10.4	TCP	1346	80 → 49826 [PSH, ACK] Seq=232961 Ack=1 Win=22 Len=1280 TSval=3293458652 TSecr=747980
65.	0.0000	19.064	172.20	14.102.231.2	TCP	66	49826 → 80 [ACK] Seq=1 Ack=234241 Win=17 Len=0 TSval=748290 TSecr=3293458652
66.	0.0058	20.414	14.102	172.20.10.4	TCP	1346	80 → 49826 [ACK] Seq=234241 Ack=1 Win=22 Len=1280 TSval=3293458961 TSecr=748290
67.	0.0000	20.414	14.102	172.20.10.4	TCP	1346	80 → 49826 [PSH, ACK] Seq=235521 Ack=1 Win=22 Len=1280 TSval=3293458961 TSecr=748290
68.	0.0000	20.414	172.20	14.102.231.2	TCP	66	49826 → 80 [ACK] Seq=1 Ack=236801 Win=16 Len=0 TSval=749640 TSecr=3293458961
69.	0.0059	20.420	14.102	172.20.10.4	TCP	1346	80 → 49826 [ACK] Seq=236801 Ack=1 Win=22 Len=1280 TSval=3293458961 TSecr=748290
70.	0.0004	20.464	172.20	14.102.231.2	TCP	66	49826 → 80 [ACK] Seq=1 Ack=238081 Win=16 Len=0 TSval=749690 TSecr=3293458961
71.	0.0000	20.606	14.102	172.20.10.4	TCP	1346	[TCP Spurious Retransmission] 80 → 49826 [ACK] Seq=238081 Ack=1 Win=22 Len=1280 TSval=3293460125 TSecr=748290
72.	0.0000	20.606	172.20	14.102.231.2	TCP	78	[TCP Dup ACK 493161] 49826 → 80 [ACK] Seq=1 Ack=238081 Win=16 Len=0 TSval=749832 TSecr=3293458961 SLE=236801 SRE=238081
73.	0.0111	20.702	14.102	172.20.10.4	TCP	1346	80 → 49826 [PSH, ACK] Seq=238081 Ack=1 Win=22 Len=1280 TSval=3293460294 TSecr=749640
74.	0.0060	20.708	14.102	172.20.10.4	TCP	1346	80 → 49826 [ACK] Seq=239361 Ack=1 Win=22 Len=1280 TSval=3293460294 TSecr=749640
75.	0.0000	20.708	172.20	14.102.231.2	TCP	66	49826 → 80 [ACK] Seq=1 Ack=240641 Win=16 Len=0 TSval=749934 TSecr=3293460294
76.	0.0000	20.708	14.102	172.20.10.4	TCP	1346	80 → 49826 [PSH, ACK] Seq=240641 Ack=1 Win=22 Len=1280 TSval=3293460349 TSecr=749690
77.	0.0001	20.845	172.20	14.102.231.2	TCP	66	49826 → 80 [ACK] Seq=1 Ack=241031 Win=31 Len=0 TSval=750071 TSecr=3293460349

3. TCP Filter Packets

tcp port => 80							
No.	Delta	Time	Source	Destination	Protocol	Length	Info
1	0.0000	14.102...	172.20.10.4	TCP	1346	80 + 49826	[PSH, ACK] Seq=1 Acks1 Win=22 Len=1280 Tsva1=3293439504 TSecr=728848
2	0.0045	0.0045	14.102...	172.20.10.4	TCP	1346	80 + 49826 [ACK] Seq=1281 Acks1 Win=22 Len=1280 Tsva1=3293439504 TSecr=728848
3	0.0045	0.0045	14.102...	172.20.10.4	TCP	66	49826 + 0 [ACK] Seq=1281 Acks1 Win=22 Len=1280 Tsva1=3293439504 TSecr=728848
20	0.0055	0.2824	14.102...	172.20.10.4	TCP	1346	80 + 49826 [PSH, ACK] Seq=2561 Acks1 Win=22 Len=1280 Tsva1=3293439885 TSecr=729231
21	0.0080	0.2905	14.102...	172.20.10.4	TCP	1346	80 + 49826 [ACK] Seq=3841 Acks1 Win=22 Len=1280 Tsva1=3293439885 TSecr=729231
22	0.0000	0.2905	14.102...	172.20.10.4	TCP	1346	80 + 49826 [PSH, ACK] Seq=5121 Acks1 Win=22 Len=1280 Tsva1=3293439885 TSecr=729231
23	0.0000	0.2906	172.20...	14.102.231.2	TCP	66	49826 + 0 [ACK] Seq=1 Acks=6401 Win=15 Len=0 Tsva1=729517 TSecr=393439885
196	0.0000	0.7106	172.20...	14.102.231.2	TCP	1346	80 + 49826 [ACK] Seq=6401 Acks1 Win=22 Len=1280 Tsva1=3293440175 TSecr=729517
197	0.0000	0.7106	172.20...	14.102.231.2	TCP	1346	80 + 49826 [ACK] Seq=8961 Acks1 Win=22 Len=1280 Tsva1=3293440175 TSecr=729517
198	0.0001	0.7107	172.20...	14.102.231.2	TCP	66	49826 + 0 [ACK] Seq=1 Acks=10241 Win=20 Len=0 Tsva1=729937 TSecr=3293440175
406	0.0009	1.1175	172.20...	14.102.231.2	TCP	1346	80 + 49826 [ACK] Seq=10241 Acks1 Win=22 Len=1280 Tsva1=3293440594 TSecr=729937
407	0.0001	1.1176	172.20...	14.102.231.2	TCP	1346	80 + 49826 [ACK] Seq=11521 Acks1 Win=22 Len=1280 Tsva1=3293440594 TSecr=729937
408	0.0001	1.1175	172.20...	14.102.231.2	TCP	1346	80 + 49826 [PSH, ACK] Seq=12801 Acks1 Win=22 Len=1280 Tsva1=3293440594 TSecr=729937 [TCP PDU reassembled in 409]
409	0.0001	1.1175	172.20...	14.102.231.2	TCP	1346	80 + 49826 [ACK] Seq=14081 Acks1 Win=22 Len=1280 Tsva1=3293440594 TSecr=729937
410	0.0001	1.1176	172.20...	14.102.231.2	TCP	66	49826 + 0 [ACK] Seq=1 Acks=15361 Win=26 Len=0 Tsva1=730344 TSecr=3293440594
631	0.0000	1.5383	172.20...	14.102.231.2	TCP	1346	80 + 49826 [ACK] Seq=15361 Acks1 Win=22 Len=1280 Tsva1=3293441006 TSecr=730344
632	0.0001	1.5384	172.20...	14.102.231.2	TCP	1346	80 + 49826 [ACK] Seq=15361 Acks1 Win=22 Len=1280 Tsva1=3293441006 TSecr=730344
633	0.0000	1.5384	172.20...	14.102.231.2	TCP	1346	80 + 49826 [PSH, ACK] Seq=17921 Acks1 Win=22 Len=1280 Tsva1=3293441006 TSecr=730344
634	0.0000	1.5385	172.20...	14.102.231.2	TCP	66	49826 + 0 [ACK] Seq=1 Acks=19201 Win=31 Len=0 Tsva1=730764 TSecr=3293441006
635	0.0059	1.5444	172.20...	14.102.231.2	TCP	1346	80 + 49826 [ACK] Seq=19201 Acks1 Win=22 Len=1280 Tsva1=3293441006 TSecr=730344
636	0.0000	1.5444	172.20...	14.102.231.2	TCP	1346	80 + 49826 [ACK] Seq=20481 Acks1 Win=22 Len=1280 Tsva1=3293441006 TSecr=730344
716	0.0157	1.8666	172.20...	14.102.231.2	TCP	66	49826 + 0 [ACK] Seq=1 Acks=21761 Win=31 Len=0 Tsva1=730770 TSecr=3293441006
717	0.0060	1.8726	172.20...	14.102.231.2	TCP	1346	80 + 49826 [PSH, ACK] Seq=23041 Acks1 Win=22 Len=1280 Tsva1=3293441421 TSecr=730764
718	0.0000	1.8726	172.20...	14.102.231.2	TCP	1346	80 + 49826 [ACK] Seq=24321 Acks1 Win=22 Len=1280 Tsva1=3293441421 TSecr=730770
719	0.0001	1.8727	172.20...	14.102.231.2	TCP	66	49826 + 0 [ACK] Seq=1 Acks=25601 Win=21 Len=0 Tsva1=731099 TSecr=3293441421
720	0.0001	1.8726	172.20...	14.102.231.2	TCP	1346	80 + 49826 [PSH, ACK] Seq=25601 Acks1 Win=22 Len=1280 Tsva1=3293441421 TSecr=730770
721	0.0000	1.8786	172.20...	14.102.231.2	TCP	1346	80 + 49826 [ACK] Seq=26881 Acks1 Win=22 Len=1280 Tsva1=3293441422 TSecr=731071
722	0.0000	1.8786	172.20...	14.102.231.2	TCP	1346	80 + 49826 [PSH, ACK] Seq=28161 Acks1 Win=22 Len=1280 Tsva1=3293441422 TSecr=730770
724	0.0000	1.8787	172.20...	14.102.231.2	TCP	66	49826 + 0 [ACK] Seq=1 Acks=29441 Win=21 Len=0 Tsva1=731105 TSecr=3293441422
745	0.6742	2.2327	14.102...	172.20.10.4	TCP	1346	80 + 49826 [ACK] Seq=29441 Acks1 Win=22 Len=1280 Tsva1=3293441768 TSecr=731099
746	0.0036	2.2369	14.102...	172.20.10.4	TCP	1346	80 + 49826 [PSH, ACK] Seq=30721 Acks1 Win=22 Len=1280 Tsva1=3293441762 TSecr=731105
747	0.0000	2.2366	172.20...	14.102.231.2	TCP	1346	80 + 49826 [ACK] Seq=32001 Acks1 Win=22 Len=1280 Tsva1=3293441762 TSecr=731105

4. UDP Filter Packets

udp port		udp port		https UN W		SYN		Flags	
No.	Delta	Time	Source	Destination	Protocol	Length	Info		
10.	0.0000.	358.13.	42.105...	172.20.10.4	UDP	1292	443 + 55956 Len=1250		
10.	0.0000.	358.13.	42.105...	172.20.10.4	UDP	1292	443 + 55956 Len=1250		
10.	0.0001.	358.13.	42.105...	172.20.10.4	UDP	1292	443 + 55956 Len=1250		
10.	0.0000.	358.13.	42.105...	172.20.10.4	UDP	1292	443 + 55956 Len=1250		
10.	0.0000.	358.13.	42.105...	172.20.10.4	UDP	1292	443 + 55956 Len=1250		
10.	0.0000.	358.13.	42.105...	172.20.10.4	UDP	1292	443 + 55956 Len=1250		
10.	0.0005.	358.13.	42.105...	172.20.10.4	UDP	1292	443 + 55956 Len=1250		
10.	0.0000.	358.13.	42.105...	172.20.10.4	UDP	1292	443 + 55956 Len=1250		
10.	0.0000.	358.13.	42.105...	172.20.10.4	UDP	1292	443 + 55956 Len=1250		
10.	0.0000.	358.13.	42.105...	172.20.10.4	UDP	1292	443 + 55956 Len=1250		
10.	0.0000.	358.13.	42.105...	172.20.10.4	UDP	1292	443 + 55956 Len=1250		
10.	0.0000.	358.13.	42.105...	172.20.10.4	UDP	1292	443 + 55956 Len=1250		
10.	0.0000.	358.13.	42.105...	172.20.10.4	UDP	1292	443 + 55956 Len=1250		
10.	0.0000.	358.13.	42.105...	172.20.10.4	UDP	1292	443 + 55956 Len=1250		
10.	0.0000.	358.13.	42.105...	172.20.10.4	UDP	1292	443 + 55956 Len=1250		
10.	0.0000.	358.13.	42.105...	172.20.10.4	UDP	388	443 + 55956 Len=346		
10.	0.0001.	358.13.	172.20...	42.105.255.12	UDP	77	55956 + 443 Len=35		
10.	0.0041.	358.13.	142.250...	172.20.10.4	UDP	122	443 + 60695 Len=80		
10.	0.0000.	358.13.	142.251...	172.20.10.4	QUIC	76	Protected Payload (KPo)		
10.	0.0003.	358.13.	172.20...	142.258.206...	UDP	76	60695 + 443 Len=34		
10.	0.0005.	358.14.	142.251...	172.20.10.4	QUIC	69	Protected Payload (KPo)		
10.	0.0000.	358.14.	142.251...	172.20.10.4	QUIC	69	Protected Payload (KPo)		
10.	0.0000.	358.14.	142.251...	172.20.10.4	QUIC	71	Protected Payload (KPo)		
10.	0.0144.	358.15.	172.20...	42.105.255.12	UDP	78	55956 + 443 Len=36		
10.	0.0001.	358.15.	172.20...	142.251.223...	QUIC	75	Protected Payload (KPo), DCID=eadad98ea8a6cc9		
10.	0.0077.	358.16.	142.251...	172.20.10.4	QUIC	69	Protected Payload (KPo)		
10.	0.0249.	358.19.	142.251...	172.20.10.4	QUIC	932	Protected Payload (KPo)		
10.	0.0041.	358.19.	142.251...	172.20.10.4	QUIC	244	Protected Payload (KPo)		
10.	0.0262.	358.22.	172.20...	142.251.223...	QUIC	82	Protected Payload (KPo), DCID=eadad98ea8a6cc9		
10.	0.0538.	358.27.	42.105...	172.20.10.4	UDP	1292	443 + 55956 Len=1250		
10.	0.0004.	358.27.	172.20...	42.105.255.12	UDP	84	55956 + 443 Len=42		
10.	0.0260.	358.30.	142.250...	172.20.10.4	UDP	122	443 + 60695 Len=80		
10.	0.0004.	358.30.	172.20...	142.258.206...	UDP	78	60695 + 443 Len=36		
10.	0.0867.	358.39.	142.251...	172.20.10.4	QUIC	68	Protected Payload (KPo)		

5. Conclusion

Wireshark packet analysis provides deep visibility into network traffic, enabling identification of:

- Insecure protocols
- Reconnaissance activity
- Potential attack vectors

Packet capture and analysis are critical skills for:

- Penetration
- testingIncident response
- Network forensics