

Part.1

Part.2(task1)

No.	Time	Source	Destination	Protocol	Length	Info
486	11.389507	10.90.71.154	13.107.22.239	TCP	66	59453 → 443 [ACK] Seq=16196 Ack=11778 Win=131584 Len=0 SLE=12802 SRE=12840
487	11.411513	13.107.22.239	10.90.71.154	TCP	1078	[TCP Retransmission] 443 → 59453 [PSH, ACK] Seq=11778 Ack=16196 Win=4195328 Len=0
488	11.411582	10.90.71.154	13.107.22.239	TCP	54	59453 → 443 [ACK] Seq=16196 Ack=12840 Win=130560 Len=0
489	11.431736	10.90.71.154	23.209.113.35	TCP	55	59427 → 443 [ACK] Seq=1 Ack=1 Win=514 Len=1
492	11.454747	10.90.71.154	79.139.94.107	TCP	66	59455 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
493	11.462125	23.209.113.35	10.90.71.154	TCP	66	443 → 59427 [ACK] Seq=1 Ack=2 Win=501 Len=0 SLE=1 SRE=2
494	11.466639	79.139.94.107	10.90.71.154	TCP	66	80 → 59455 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1386 SACK_PERM WS=128
495	11.466754	10.90.71.154	79.139.94.107	TCP	54	59455 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=0
496	11.466992	10.90.71.154	79.139.94.107	HTTP	403	HEAD /filestreamingservice/files/9b9f8fb4-8a65-41e4-bda3-5416858f0aeb?P1=17390875
497	11.478507	79.139.94.107	10.90.71.154	TCP	60	80 → 59455 [ACK] Seq=1 Ack=350 Win=64128 Len=0
498	11.481137	79.139.94.107	10.90.71.154	HTTP	658	HTTP/1.1 200 OK
503	11.515305	10.90.71.154	79.139.94.107	HTTP	475	GET /filestreamingservice/files/9b9f8fb4-8a65-41e4-bda3-5416858f0aeb?P1=17390875
504	11.525663	79.139.94.107	10.90.71.154	TCP	60	80 → 59455 [ACK] Seq=605 Ack=771 Win=64128 Len=0
505	11.529076	79.139.94.107	10.90.71.154	TCP	1440	80 → 59455 [ACK] Seq=605 Ack=771 Win=64128 Len=1386 [TCP PDU reassembled in 506]
506	11.529076	79.139.94.107	10.90.71.154	HTTP	439	HTTP/1.1 206 Partial Content (application/x-chrome-extension)
507	11.529129	10.90.71.154	79.139.94.107	TCP	54	59455 → 80 [ACK] Seq=771 Ack=2376 Win=131584 Len=0
510	11.760945	10.90.71.154	44.240.19.242	TCP	55	58835 → 443 [ACK] Seq=1 Ack=1 Win=508 Len=1
512	11.871286	10.90.71.154	172.217.19.46	TCP	55	59250 → 443 [ACK] Seq=1 Ack=1 Win=510 Len=1
513	11.944305	172.217.19.46	10.90.71.154	TCP	66	443 → 59250 [ACK] Seq=1 Ack=2 Win=1048 Len=0 SLE=1 SRE=2
520	12.225601	10.90.71.154	20.42.65.85	TCP	66	59456 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM

> 010. = Flags: 0x2, Don't fragment

...0 0000 0000 0000 = Fragment Offset: 0

Time to Live: 128

Protocol: TCP (6)

Header Checksum: 0x0000 [validation disabled]

[Header checksum status: Unverified]

Source Address: 10.90.71.154

Destination Address: 13.107.22.239

[Stream index: 0]

✖ Transmission Control Protocol, Src Port: 59453, Dst Port: 443, Seq: 16196, Ack: 12840, Len: 0

Source Port: 59453

Destination Port: 443

[Stream index: 40]

> [Conversation completeness: Complete, WITH_DATA (31)]

[TCP Segment Len: 0]

Sequence Number: 16196 (relative sequence number)

Sequence Number (raw): 1052714709

[Next Sequence Number: 16196 (relative sequence number)]

Acknowledgment Number: 12840 (relative ack number)

Acknowledgment number (raw): 2575736988

0101 = Header Length: 20 bytes (5)

0000 e0 23 ff 5d fc 8a 70 32 17 b0 4b cc 08 00 45

0010 00 28 ac e5 40 00 80 06 00 00 0a 5a 47 9a 0d

0020 0e ef e8 3d 01 bb 3e 3f 26 d5 99 86 a0 9c 50

0030 01 fe 76 68 00 00

Part.2(task2)

✓ [Conversation completeness: Complete, WITH_DATA (31)]

```

...0. .... = RST: Absent
...1 .... = FIN: Present
.... 1... = Data: Present
.... .1.. = ACK: Present
.... ..1. = SYN-ACK: Present
.... ...1 = SYN: Present
[Completeness Flags: ·FDASS]

```

Part.3

No.	Time	Source	Destination	Protocol	Length	Info
509	11.713449	10.90.18.178	224.0.0.252	LLMNR	66	Standard query 0x2c40 A tmosce
511	11.813683	10.90.18.178	10.90.255.255	NBNS	92	Name query NB IMAC-8BF77C<00>
514	12.120672	10.90.18.178	10.90.255.255	NBNS	92	Name query NB TMOSE<00>
515	12.221430	10.90.71.154	10.90.100.20	DNS	96	Standard query 0x6e18 A functional.events.data.microsoft.com
516	12.221720	10.90.71.154	10.90.100.20	DNS	96	Standard query 0x8573 HTTPS functional.events.data.microsoft.com
517	12.223582	10.90.6.236	10.90.255.255	NBNS	92	Name query NB DESKTOP-B07RJA2C1<
518	12.224709	10.90.100.20	10.90.71.154	DNS	223	Standard query response 0x6e18 A functional.events.data.microsoft.com CNAME global.asimov.events.data.traff
519	12.224709	10.90.100.20	10.90.71.154	DNS	267	Standard query response 0x8573 HTTPS functional.events.data.microsoft.com CNAME global.asimov.events.data.t
521	12.325221	10.90.19.153	10.90.255.255	NBNS	92	Name query NB ISATAP<00>
527	12.427664	10.90.19.4	224.0.0.252	LLMNR	75	Standard query 0xbfad ANY DESKTOP-JAVSIQD
528	12.530842	10.90.17.210	10.90.255.255	UDP	106	7551 → 7551 Len=64
529	12.530842	10.90.61.87	255.255.255.255	UDP	69	2008 → 2008 Len=27
530	12.530842	10.90.2.89	230.0.0.1	UDP	92	51217 → 6666 Len=50
533	12.632370	10.90.18.178	10.90.255.255	NBNS	92	Name query NB IMAC-8BF77C<00>
534	12.632370	10.90.10.37	10.90.255.255	UDP	86	57621 → 57621 Len=44
535	12.735403	10.90.3.42	10.90.255.255	UDP	86	57621 → 57621 Len=44
546	12.837555	10.90.23.232	10.90.255.255	BROWSER	243	Host Announcement LAPTOP-GF59HEL7, Workstation, Server, NT Workstation, Potential Browser
547	12.839486	10.90.18.178	10.90.255.255	NBNS	92	Name query NB TMOSE<00>
548	12.879275	10.90.71.154	10.90.100.20	DNS	79	Standard query 0xd32b A aefd.nelreports.net
549	12.879550	10.90.71.154	10.90.100.20	DNS	79	Standard query 0x59b1 HTTPS aefd.nelreports.net

Part.4(task1)

	TCP or UDP	Reasons
Reliability and Connection Establishment	TCP	TCP provides reliable data transfer with error checking
Data Integrity and Ordering	TCP	TCP ensures data is received in the correct order

Part.4(task2)

	TCP	UDP
Use cases	- Web browsing (HTTP/HTTPS) - Email (SMTP, IMAP, POP3) - File transfer (FTP, SFTP) - Remote access (SSH, Telnet) - Secure transactions	- Streaming (audio/video) - Online gaming - VoIP (Voice over IP) - DNS lookups - IoT and sensor data transmission
Performance	- Reliable but slower due to error checking, retransmission, and connection overhead - Ensures data integrity and order	- Faster and lightweight since it lacks reliability mechanisms - No retransmissions or acknowledgments, reducing latency