Wireshark Task 5 - Capture & Analysis Report

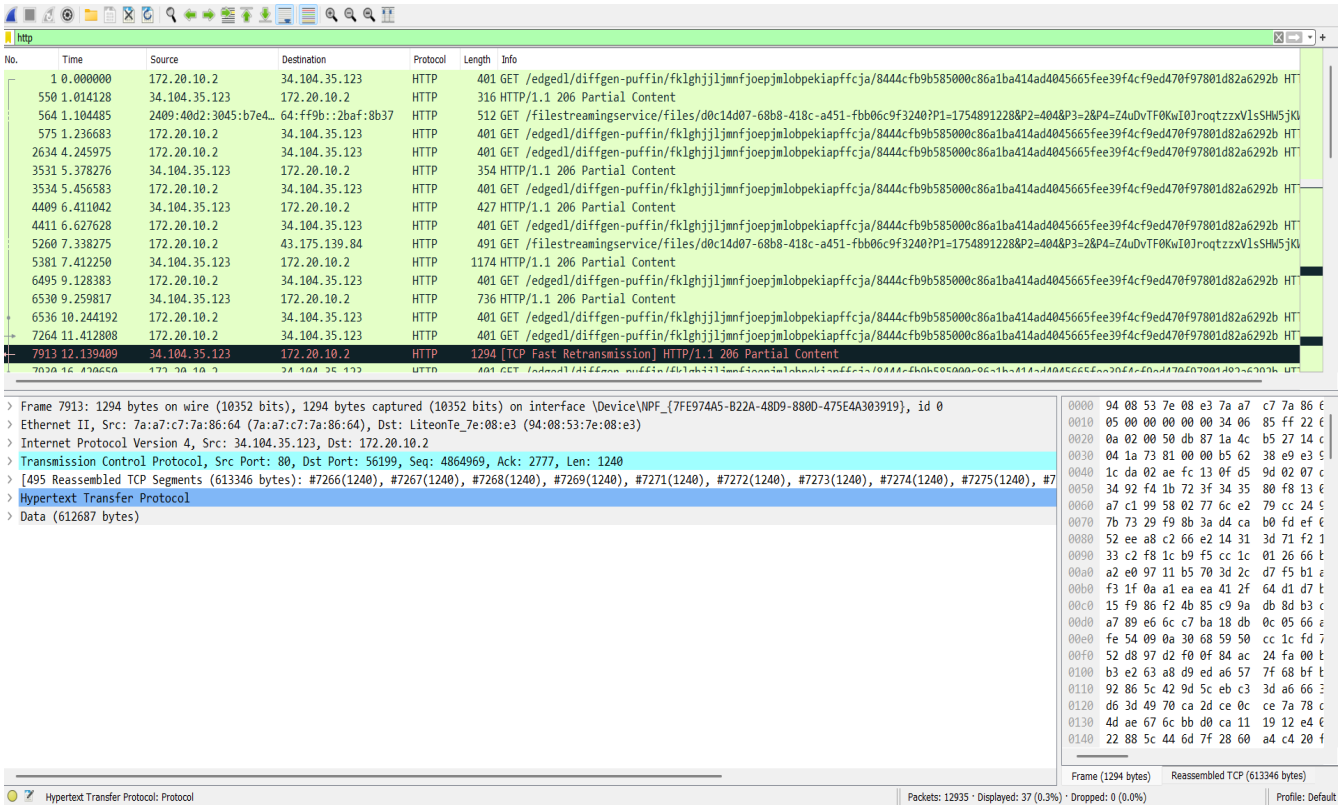
This report documents the process and results of Task 5, which involves capturing network packets using Wireshark, identifying protocols, analyzing selected packets, and documenting findings. Attached are packet capture files and screenshots from the analysis.

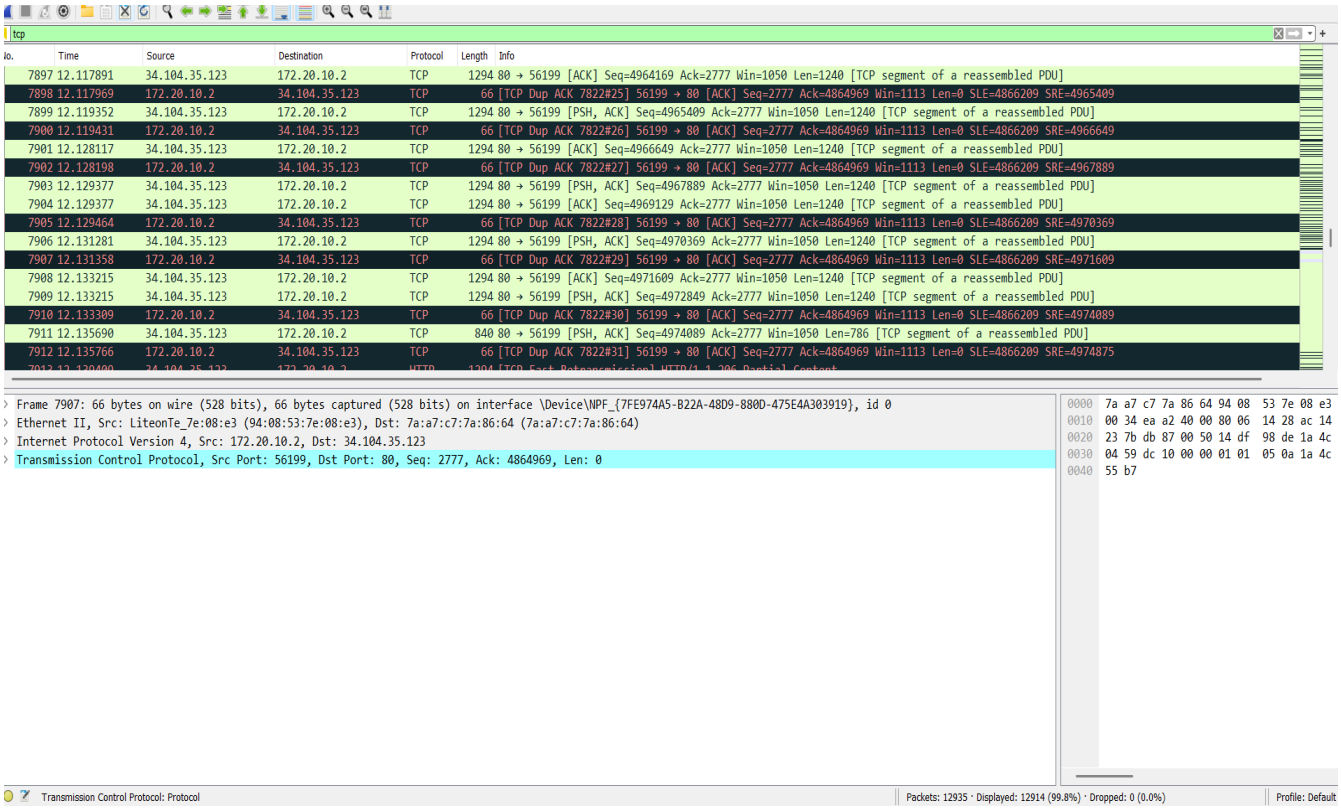
Methodology:
1. Started Wireshark capture on the active network interface.
2. Generated network traffic by browsing websites and triggering DNS lookups.
3. Used display filters (http, tcp, dns) to isolate relevant packets.
4. Saved capture file as 'packet.pcapng'.
5. Collected screenshots of protocol-specific analysis.

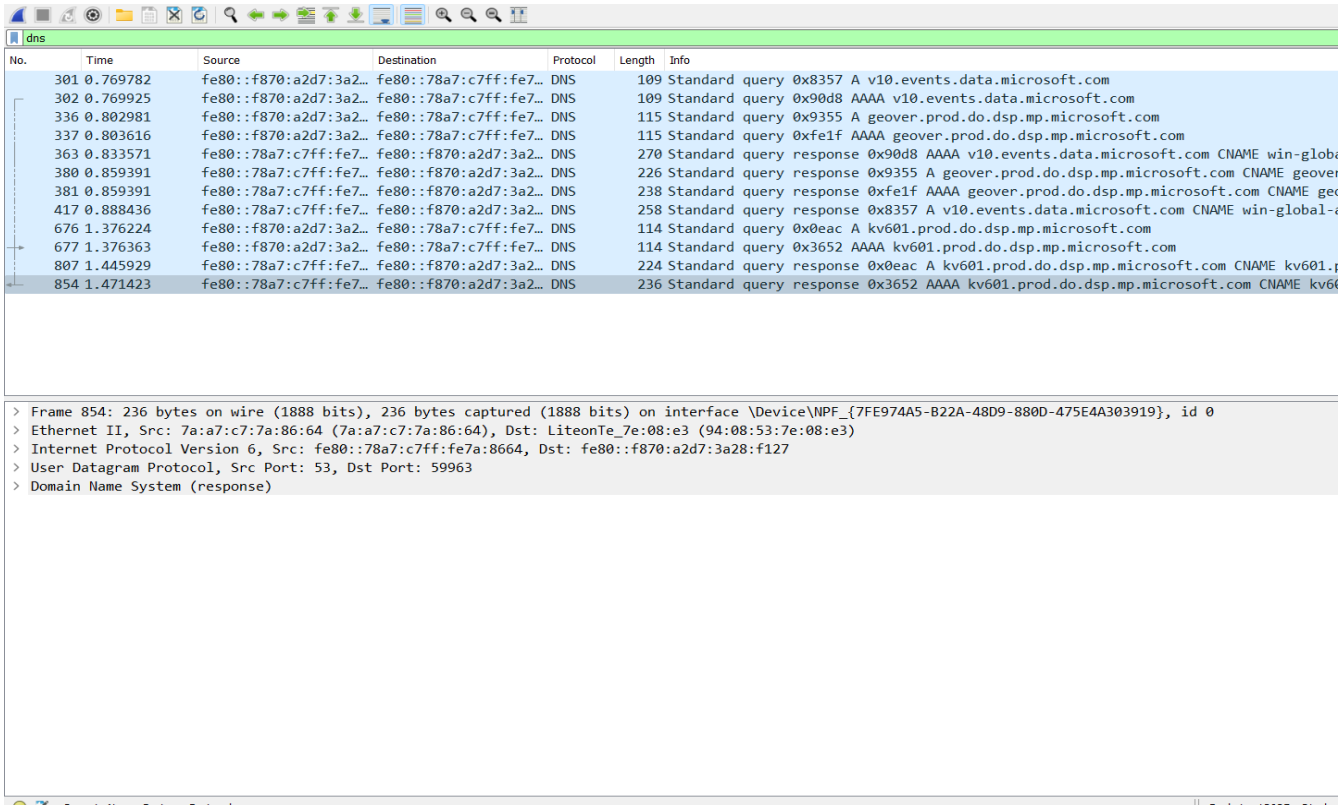
Protocol	Description	Observed Count (approx.)
HTTP	Hypertext Transfer Protocol - application layer web traffic	Multiple GET/Partial Content requests
TCP	Transmission Control Protocol - reliable transport	Multiple PSH/ACK and reassembled s
DNS	Domain Name System - resolves domain names to IP addresses	Multiple AAAA and A record lookups/r

Packet Analysis:
1. HTTP Packet (#550): GET request to /edgedl/diffgen-puffin/... with HTTP/1.1 206 Partial Content response. Large reassembled TCP segment (612,687 bytes) observed.
2. TCP Packet (#7907): ACK packet in a TCP stream from 172.20.10.2 to 34.104.35.123, Seq=2777, Ack=4864969, Len=0.
3. DNS Packet (#854): Standard query response AAAA kv601.prod.do.dsp.mp.microsoft.com, resolved to multiple addresses.

Screenshots of Analysis:


http
No. Time Source Destination Protocol Length Info
1 0.000000 172.20.10.2 34.104.35.123 HTTP 401 GET /edgedl/diffgen-puffin/fklghjjljmnfjoepjmlobpekiapffcja/8444cfb9b585000c86a1ba414ad4045665fee39f4cf9ed470f97801d82a6292b HT
550 1.014128 34.104.35.123 172.20.10.2 HTTP 316 HTTP/1.1 206 Partial Content
564 1.104485 2409:40d2:3045:b7e4… 64:ff9b::2baf:8b37 HTTP 512 GET /filestreamingservice/files/d0c14d07-68b8-418c-a451-fbb06c9f3240?P1=1754891228&P2=404&P3=2&P4=Z4uDvTF0KwI0JroqtzzxVlsSHW5jKl
575 1.236683 172.20.10.2 34.104.35.123 HTTP 401 GET /edgedl/diffgen-puffin/fklghjjljmnfjoepjmlobpekiapffcja/8444cfb9b585000c86a1ba414ad4045665fee39f4cf9ed470f97801d82a6292b HT
2634 4.245975 172.20.10.2 34.104.35.123 HTTP 401 GET /edgedl/diffgen-puffin/fklghjjljmnfjoepjmlobpekiapffcja/8444cfb9b585000c86a1ba414ad4045665fee39f4cf9ed470f97801d82a6292b HT
3531 5.378276 34.104.35.123 172.20.10.2 HTTP 354 HTTP/1.1 206 Partial Content
3534 5.456583 172.20.10.2 34.104.35.123 HTTP 401 GET /edgedl/diffgen-puffin/fklghjjljmnfjoepjmlobpekiapffcja/8444cfb9b585000c86a1ba414ad4045665fee39f4cf9ed470f97801d82a6292b HT
4409 6.411042 34.104.35.123 172.20.10.2 HTTP 427 HTTP/1.1 206 Partial Content
4411 6.627628 172.20.10.2 34.104.35.123 HTTP 401 GET /edgedl/diffgen-puffin/fklghjjljmnfjoepjmlobpekiapffcja/8444cfb9b585000c86a1ba414ad4045665fee39f4cf9ed470f97801d82a6292b HT
5260 7.338275 172.20.10.2 43.175.139.84 HTTP 491 GET /filestreamingservice/files/d0c14d07-68b8-418c-a451-fbb06c9f3240?P1=1754891228&P2=404&P3=2&P4=Z4uDvTF0KwI0JroqtzzxVlsSHW5jKl
5381 7.412250 34.104.35.123 172.20.10.2 HTTP 1174 HTTP/1.1 206 Partial Content
6495 9.128383 172.20.10.2 34.104.35.123 HTTP 401 GET /edgedl/diffgen-puffin/fklghjjljmnfjoepjmlobpekiapffcja/8444cfb9b585000c86a1ba414ad4045665fee39f4cf9ed470f97801d82a6292b HT
6530 9.259817 34.104.35.123 172.20.10.2 HTTP 736 HTTP/1.1 206 Partial Content
6536 10.244192 172.20.10.2 34.104.35.123 HTTP 401 GET /edgedl/diffgen-puffin/fklghjjljmnfjoepjmlobpekiapffcja/8444cfb9b585000c86a1ba414ad4045665fee39f4cf9ed470f97801d82a6292b HT
7264 11.412808 172.20.10.2 34.104.35.123 HTTP 401 GET /edgedl/diffgen-puffin/fklghjjljmnfjoepjmlobpekiapffcja/8444cfb9b585000c86a1ba414ad4045665fee39f4cf9ed470f97801d82a6292b HT
7913 12.139409 34.104.35.123 172.20.10.2 HTTP 1294 [TCP Fast Retransmission] HTTP/1.1 206 Partial Content
Frame 7913: 1294 bytes on wire (10352 bits), 1294 bytes captured (10352 bits) on interface \Device\NPF_{7FE974A5-B22A-48D9-880D-475E4A303919}, id 0
Ethernet II, Src: 7a:a7:c7:7a:86:64 (7a:a7:c7:7a:86:64), Dst: LiteonTe_7e:08:e3 (94:08:53:7e:08:e3)
Internet Protocol Version 4, Src: 34.104.35.123, Dst: 172.20.10.2
Transmission Control Protocol, Src Port: 80, Dst Port: 56199, Seq: 4864969, Ack: 2777, Len: 1240
[495 Reassembled TCP Segments (613346 bytes): #7266(1240), #7267(1240), #7268(1240), #7269(1240), #7271(1240), #7272(1240), #7273(1240), #7274(1240), #7275(1240), #7
Hypertext Transfer Protocol
Data (612687 bytes)
0000 94 08 53 7e 08 e3 7a a7 c7 7a 86 6
0010 05 00 00 00 00 00 34 06 85 ff 22 6
0020 0a 02 00 50 db 87 1a 4c b5 27 14 c
0030 04 1a 73 81 00 00 b5 62 38 e9 e3 9
0040 1c da 02 ae fc 13 0f d5 9d 02 07 c
0050 34 92 f4 1b 72 3f 34 35 80 f8 13 6
0060 a7 c1 99 58 02 77 6c e2 79 cc 24 9
0070 7b 73 29 f9 8b 3a d4 ca b0 fd ef 6
0080 52 ee a8 c2 66 e2 14 31 3d 71 f2 1
0090 33 c2 f8 1c b9 f5 cc 1c 01 26 66 b
00a0 a2 e0 97 11 b5 70 3d 2c d7 f5 b1 a
00b0 f3 1f 0a a1 ea ea 41 2f 64 d1 d7 b
00c0 15 f9 86 f2 4b 85 c9 9a db 8d b3 c
00d0 a7 89 e6 6c c7 ba 18 db 0c 05 66 a
00e0 fe 54 09 0a 30 68 59 50 cc 1c fd 7
00f0 52 d8 97 d2 f0 0f 84 ac 24 fa 00 b
0100 b3 e2 63 a8 d9 ed a6 57 7f 68 bf b
0110 92 86 5c 42 9d 5c eb c3 3d a6 66 3
0120 d6 3d 49 70 ca 2d ce 0c ce 7a 78 c
0130 4d ae 67 6c bb d0 ca 11 19 12 e4 6
0140 22 88 5c 44 6d 7f 28 60 a4 c4 20 f
Frame (1294 bytes)
Reassembled TCP (613346 bytes)
Hypertext Transfer Protocol: Protocol
Packets: 12935 · Displayed: 37 (0.3%) · Dropped: 0 (0.0%)
Profile: Default


tcp
Time Source Destination Protocol Length Info
7897 12.117891 34.104.35.123 172.20.10.2 TCP 1294 80 → 56199 [ACK] Seq=4964169 Ack=2777 Win=1050 Len=1240 [TCP segment of a reassembled PDU]
7898 12.117969 172.20.10.2 34.104.35.123 TCP 66 [TCP Dup ACK 7822#25] 56199 → 80 [ACK] Seq=2777 Ack=4864969 Win=1113 Len=0 SLE=4866209 SRE=4965409
7899 12.119352 34.104.35.123 172.20.10.2 TCP 1294 80 → 56199 [PSH, ACK] Seq=4965409 Ack=2777 Win=1050 Len=1240 [TCP segment of a reassembled PDU]
7900 12.119431 172.20.10.2 34.104.35.123 TCP 66 [TCP Dup ACK 7822#26] 56199 → 80 [ACK] Seq=2777 Ack=4864969 Win=1113 Len=0 SLE=4866209 SRE=4966649
7901 12.128117 34.104.35.123 172.20.10.2 TCP 1294 80 → 56199 [ACK] Seq=4966649 Ack=2777 Win=1050 Len=1240 [TCP segment of a reassembled PDU]
7902 12.128198 172.20.10.2 34.104.35.123 TCP 66 [TCP Dup ACK 7822#27] 56199 → 80 [ACK] Seq=2777 Ack=4864969 Win=1113 Len=0 SLE=4866209 SRE=4967889
7903 12.129377 34.104.35.123 172.20.10.2 TCP 1294 80 → 56199 [PSH, ACK] Seq=4967889 Ack=2777 Win=1050 Len=1240 [TCP segment of a reassembled PDU]
7904 12.129377 34.104.35.123 172.20.10.2 TCP 1294 80 → 56199 [ACK] Seq=4969129 Ack=2777 Win=1050 Len=1240 [TCP segment of a reassembled PDU]
7905 12.129464 172.20.10.2 34.104.35.123 TCP 66 [TCP Dup ACK 7822#28] 56199 → 80 [ACK] Seq=2777 Ack=4864969 Win=1113 Len=0 SLE=4866209 SRE=4970369
7906 12.131281 34.104.35.123 172.20.10.2 TCP 1294 80 → 56199 [PSH, ACK] Seq=4970369 Ack=2777 Win=1050 Len=1240 [TCP segment of a reassembled PDU]
7907 12.131358 172.20.10.2 34.104.35.123 TCP 66 [TCP Dup ACK 7822#29] 56199 → 80 [ACK] Seq=2777 Ack=4864969 Win=1113 Len=0 SLE=4866209 SRE=4971609
7908 12.133215 34.104.35.123 172.20.10.2 TCP 1294 80 → 56199 [ACK] Seq=4971609 Ack=2777 Win=1050 Len=1240 [TCP segment of a reassembled PDU]
7909 12.133215 34.104.35.123 172.20.10.2 TCP 1294 80 → 56199 [PSH, ACK] Seq=4972849 Ack=2777 Win=1050 Len=1240 [TCP segment of a reassembled PDU]
7910 12.133309 172.20.10.2 34.104.35.123 TCP 66 [TCP Dup ACK 7822#30] 56199 → 80 [ACK] Seq=2777 Ack=4864969 Win=1113 Len=0 SLE=4866209 SRE=4974089
7911 12.135690 34.104.35.123 172.20.10.2 TCP 840 80 → 56199 [PSH, ACK] Seq=4974089 Ack=2777 Win=1050 Len=786 [TCP segment of a reassembled PDU]
7912 12.135766 172.20.10.2 34.104.35.123 TCP 66 [TCP Dup ACK 7822#31] 56199 → 80 [ACK] Seq=2777 Ack=4864969 Win=1113 Len=0 SLE=4866209 SRE=4974875
Frame 7907: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{7FE974A5-B22A-48D9-880D-475E4A303919}, id 0
Ethernet II, Src: LiteonTe_7e:08:e3 (94:08:53:7e:08:e3), Dst: 7a:a7:c7:7a:86:64 (7a:a7:c7:7a:86:64)
Internet Protocol Version 4, Src: 172.20.10.2, Dst: 34.104.35.123
Transmission Control Protocol, Src Port: 56199, Dst Port: 80, Seq: 2777, Ack: 4864969, Len: 0
0000 7a a7 c7 7a 86 64 94 08 53 7e 08 e3
0010 00 34 ea a2 40 00 80 06 14 28 ac 14
0020 23 7b db 87 00 50 14 df 98 de 1a 4c
0030 04 59 dc 10 00 00 01 01 05 0a 1a 4c
0040 55 b7
Transmission Control Protocol: Protocol
Packets: 12935 · Displayed: 12914 (99.8%) · Dropped: 0 (0.0%)
Profile: Default



Conclusion:
The capture contained common protocols such as HTTP, TCP, and DNS. Analysis showed partial content HTTP responses, reassembled TCP segments indicating large file transfers, and DNS lookups to Microsoft-related domains. No suspicious or malicious traffic was detected in this session.