Experiment - 23

Transport Layer protocol Header analysis using Wire Shark TCP & UDP

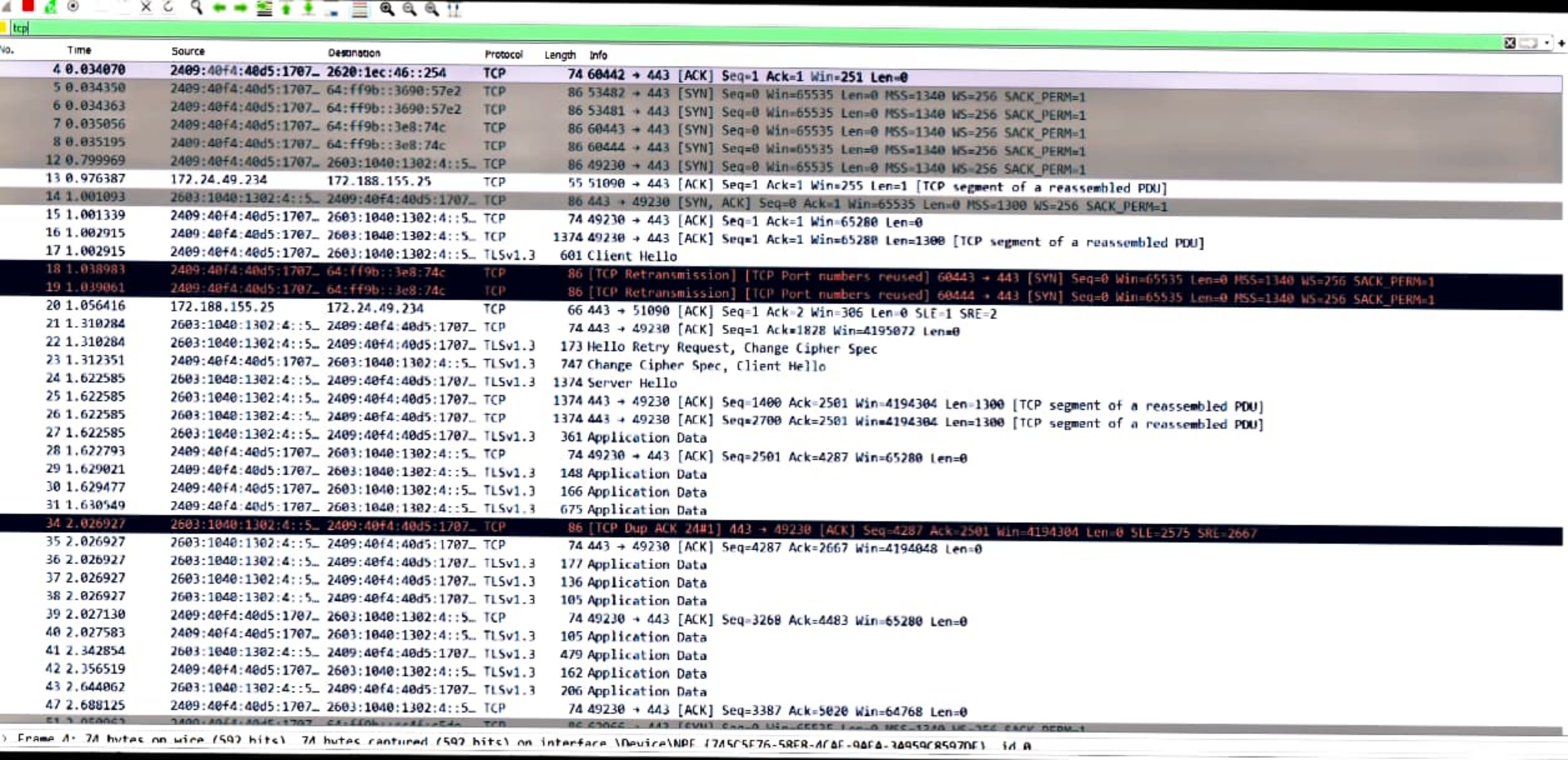
Aim: To analyse capturing transport layer protocol header analysis using wire shark TCP & UDP.

Software: Wire shark Network Analyzer

Procedure:

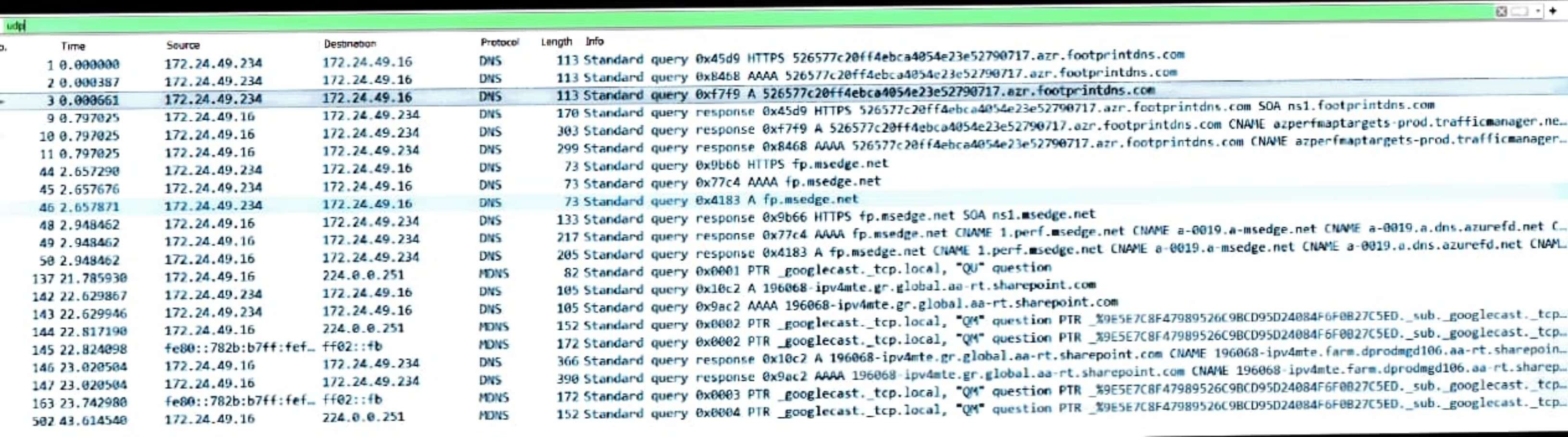
1. open wire shark
2. Click on capture interface
3. Choose LAN interface
4. Click on start button
5. Active packets will be displayed
6. capture the packets & select IP address
7. Click on the expression & select IPv4-
8. Select the double equals.
9. Click on apply button.
10. All the packets will be filtered

Result: Hence the capturing on packets using Shark network analyser for TCP & UDP



tcp

```
No.     Time      Source                   Destination              Protocol  Length Info
     4 0.034070  2409:40f4:40d5:1707…  2620:1ec:46::254        TCP       74 60442 → 443 [ACK] Seq=1 Ack=1 Win=251 Len=0
     5 0.034350  2409:40f4:40d5:1707…  64:ff9b::3690:57e2      TCP       86 53482 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1340 WS=256 SACK_PERM=1
     6 0.034363  2409:40f4:40d5:1707…  64:ff9b::3690:57e2      TCP       86 53481 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1340 WS=256 SACK_PERM=1
     7 0.035056  2409:40f4:40d5:1707…  64:ff9b::3e8:74c        TCP       86 60443 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1340 WS=256 SACK_PERM=1
     8 0.035195  2409:40f4:40d5:1707…  64:ff9b::3e8:74c        TCP       86 60444 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1340 WS=256 SACK_PERM=1
    12 0.799969  2409:40f4:40d5:1707…  2603:1040:1302:4::5…    TCP       86 49230 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1340 WS=256 SACK_PERM=1
    13 0.976387  172.24.49.234         172.188.155.25          TCP       55 51090 → 443 [ACK] Seq=1 Ack=1 Win=255 Len=1 [TCP segment of a reassembled PDU]
    14 1.001093  2603:1040:1302:4::5…  2409:40f4:40d5:1707…    TCP       86 443 → 49230 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1300 WS=256 SACK_PERM=1
    15 1.001339  2409:40f4:40d5:1707…  2603:1040:1302:4::5…    TCP       74 49230 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=0
    16 1.002915  2409:40f4:40d5:1707…  2603:1040:1302:4::5…    TCP     1374 49230 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=1300 [TCP segment of a reassembled PDU]
    17 1.002915  2409:40f4:40d5:1707…  2603:1040:1302:4::5…    TLSv1.3  601 Client Hello
    18 1.038983  2409:40f4:40d5:1707…  64:ff9b::3e8:74c        TCP       86 [TCP Retransmission] [TCP Port numbers reused] 60443 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1340 WS=256 SACK_PERM=1
    19 1.039061  2409:40f4:40d5:1707…  64:ff9b::3e8:74c        TCP       86 [TCP Retransmission] [TCP Port numbers reused] 60444 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1340 WS=256 SACK_PERM=1
    20 1.056416  172.188.155.25        172.24.49.234           TCP       66 443 → 51090 [ACK] Seq=1 Ack=2 Win=306 Len=0 SLE=1 SRE=2
    21 1.310284  2603:1040:1302:4::5…  2409:40f4:40d5:1707…    TCP       74 443 → 49230 [ACK] Seq=1 Ack=1828 Win=4195072 Len=0
    22 1.310284  2603:1040:1302:4::5…  2409:40f4:40d5:1707…    TLSv1.3  173 Hello Retry Request, Change Cipher Spec
    23 1.312351  2409:40f4:40d5:1707…  2603:1040:1302:4::5…    TLSv1.3  747 Change Cipher Spec, Client Hello
    24 1.622585  2603:1040:1302:4::5…  2409:40f4:40d5:1707…    TLSv1.3 1374 Server Hello
    25 1.622585  2603:1040:1302:4::5…  2409:40f4:40d5:1707…    TCP     1374 443 → 49230 [ACK] Seq=1400 Ack=2501 Win=4194304 Len=1300 [TCP segment of a reassembled PDU]
    26 1.622585  2603:1040:1302:4::5…  2409:40f4:40d5:1707…    TCP     1374 443 → 49230 [ACK] Seq=2700 Ack=2501 Win=4194304 Len=1300 [TCP segment of a reassembled PDU]
    27 1.622585  2603:1040:1302:4::5…  2409:40f4:40d5:1707…    TLSv1.3  361 Application Data
    28 1.622793  2409:40f4:40d5:1707…  2603:1040:1302:4::5…    TCP       74 49230 → 443 [ACK] Seq=2501 Ack=4287 Win=65280 Len=0
    29 1.629021  2409:40f4:40d5:1707…  2603:1040:1302:4::5…    TLSv1.3  148 Application Data
    30 1.629477  2409:40f4:40d5:1707…  2603:1040:1302:4::5…    TLSv1.3  166 Application Data
    31 1.630549  2409:40f4:40d5:1707…  2603:1040:1302:4::5…    TLSv1.3  675 Application Data
    34 2.026927  2603:1040:1302:4::5…  2409:40f4:40d5:1707…    TCP       86 [TCP Dup ACK 24#1] 443 → 49230 [ACK] Seq=4287 Ack=2501 Win=4194304 Len=0 SLE=2575 SRE=2667
    35 2.026927  2603:1040:1302:4::5…  2409:40f4:40d5:1707…    TCP       74 443 → 49230 [ACK] Seq=4287 Ack=2667 Win=4194048 Len=0
    36 2.026927  2603:1040:1302:4::5…  2409:40f4:40d5:1707…    TLSv1.3  177 Application Data
    37 2.026927  2603:1040:1302:4::5…  2409:40f4:40d5:1707…    TLSv1.3  136 Application Data
    38 2.026927  2603:1040:1302:4::5…  2409:40f4:40d5:1707…    TLSv1.3  105 Application Data
    39 2.027130  2409:40f4:40d5:1707…  2603:1040:1302:4::5…    TCP       74 49230 → 443 [ACK] Seq=3268 Ack=4483 Win=65280 Len=0
    40 2.027583  2409:40f4:40d5:1707…  2603:1040:1302:4::5…    TLSv1.3  105 Application Data
    41 2.342854  2603:1040:1302:4::5…  2409:40f4:40d5:1707…    TLSv1.3  479 Application Data
    42 2.356519  2409:40f4:40d5:1707…  2603:1040:1302:4::5…    TLSv1.3  162 Application Data
    43 2.644062  2603:1040:1302:4::5…  2409:40f4:40d5:1707…    TLSv1.3  206 Application Data
    47 2.688125  2409:40f4:40d5:1707…  2603:1040:1302:4::5…    TCP       74 49230 → 443 [ACK] Seq=3387 Ack=5020 Win=64768 Len=0
    51 2.050062  2409:40f4:40d5:1707…  64:ff9b::a8f:c5da       TCP       86 52066 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1340 WS=256 SACK_PERM=1
> Frame 4: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{745C5F76-58E8-4CAE-9AEA-34959C8597DE}, id 0
```



```
udp
o.      Time          Source                   Destination        Protocol  Length  Info
      1 0.000000      172.24.49.234            172.24.49.16       DNS       113 Standard query 0x45d9 HTTPS 526577c20ff4ebca4054e23e52790717.azr.footprintdns.com
      2 0.000387      172.24.49.234            172.24.49.16       DNS       113 Standard query 0x8468 AAAA 526577c20ff4ebca4054e23e52790717.azr.footprintdns.com
      3 0.000661      172.24.49.234            172.24.49.16       DNS       113 Standard query 0xf7f9 A 526577c20ff4ebca4054e23e52790717.azr.footprintdns.com
      9 0.797025      172.24.49.16             172.24.49.234      DNS       170 Standard query response 0x45d9 HTTPS 526577c20ff4ebca4054e23e52790717.azr.footprintdns.com SOA ns1.footprintdns.com
     10 0.797025      172.24.49.16             172.24.49.234      DNS       303 Standard query response 0xf7f9 A 526577c20ff4ebca4054e23e52790717.azr.footprintdns.com CNAME azperfmaptargets-prod.trafficmanager.ne…
     11 0.797025      172.24.49.16             172.24.49.234      DNS       299 Standard query response 0x8468 AAAA 526577c20ff4ebca4054e23e52790717.azr.footprintdns.com CNAME azperfmaptargets-prod.trafficmanager…
     44 2.657290      172.24.49.234            172.24.49.16       DNS        73 Standard query 0x9b66 HTTPS fp.msedge.net
     45 2.657676      172.24.49.234            172.24.49.16       DNS        73 Standard query 0x77c4 AAAA fp.msedge.net
     46 2.657871      172.24.49.234            172.24.49.16       DNS        73 Standard query 0x4183 A fp.msedge.net
     48 2.948462      172.24.49.16             172.24.49.234      DNS       133 Standard query response 0x9b66 HTTPS fp.msedge.net SOA ns1.msedge.net
     49 2.948462      172.24.49.16             172.24.49.234      DNS       217 Standard query response 0x77c4 AAAA fp.msedge.net CNAME 1.perf.msedge.net CNAME a-0019.a-msedge.net CNAME a-0019.a.dns.azurefd.net C…
     50 2.948462      172.24.49.16             172.24.49.234      DNS       205 Standard query response 0x4183 A fp.msedge.net CNAME 1.perf.msedge.net CNAME a-0019.a-msedge.net CNAME a-0019.a.dns.azurefd.net CNAM…
    137 21.785930     172.24.49.16             224.0.0.251        MDNS       82 Standard query 0x0001 PTR _googlecast._tcp.local, "QU" question
    142 22.629867     172.24.49.234            172.24.49.16       DNS       105 Standard query 0x10c2 A 196068-ipv4mte.gr.global.aa-rt.sharepoint.com
    143 22.629946     172.24.49.234            172.24.49.16       DNS       105 Standard query 0x9ac2 AAAA 196068-ipv4mte.gr.global.aa-rt.sharepoint.com
    144 22.817190     172.24.49.16             224.0.0.251        MDNS      152 Standard query 0x0002 PTR _googlecast._tcp.local, "QM" question PTR _%9E5E7C8F47989526C9BCD95D24084F6F0B27C5ED._sub._googlecast._tcp…
    145 22.824098     fe80::782b:b7ff:fef…     ff02::fb           MDNS      172 Standard query 0x0002 PTR _googlecast._tcp.local, "QM" question PTR _%9E5E7C8F47989526C9BCD95D24084F6F0027C5ED._sub._googlecast._tcp…
    146 23.020504     172.24.49.16             172.24.49.234      DNS       366 Standard query response 0x10c2 A 196068-ipv4mte.gr.global.aa-rt.sharepoint.com CNAME 196068-ipv4mte.farm.dprodmgd106.aa-rt.sharepoin…
    147 23.020504     172.24.49.16             172.24.49.234      DNS       390 Standard query response 0x9ac2 AAAA 196068-ipv4mte.gr.global.aa-rt.sharepoint.com CNAME 196068-ipv4mte.farm.dprodmgd106.aa-rt.sharep…
    163 23.742980     fe80::782b:b7ff:fef…     ff02::fb           MDNS      172 Standard query 0x0003 PTR _googlecast._tcp.local, "QM" question PTR _%9E5E7C8F47989526C9BCD95D24084F6F0B27C5ED._sub._googlecast._tcp…
    502 43.614540     172.24.49.16             224.0.0.251        MDNS      152 Standard query 0x0004 PTR _googlecast._tcp.local, "QM" question PTR _%9E5E7C8F47989526C9BCD95D24084F6F0B27C5ED._sub._googlecast._tcp…
```