EXPERIMENT 10

Aim

Study of Wireshark and understand its functionality

Prerequisite

Nil

Outcome

To impart knowledge of Computer Networking Technology

Theory

Wireshark is a popular and powerful open-source network protocol analyser that allows users to capture, inspect, and analyse data traffic on a computer network. It is widely used by network administrators, security professionals, and developers to troubleshoot network issues, monitor network performance, and identify potential security vulnerabilities.

Wireshark boasts support for a wide array of network protocols, including common ones like TCP, IP, UDP, HTTP, and HTTPS, as well as less common or proprietary protocols. The tool can decode and display information about each packet, allowing users to understand the contents of network traffic and identify potential issues.

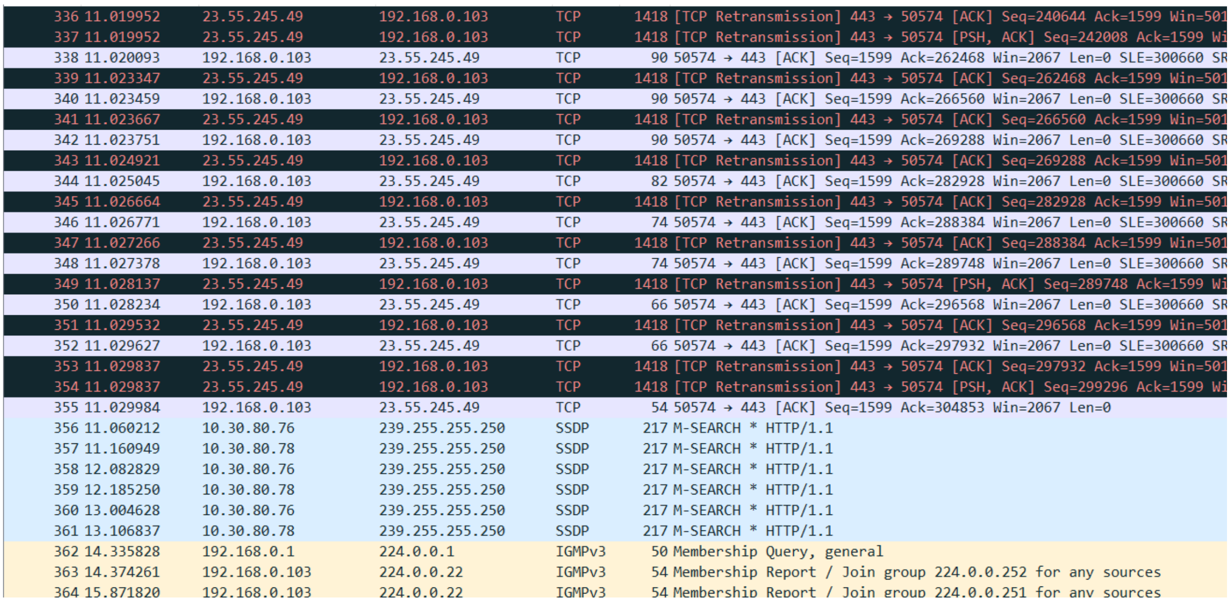
Here are some key aspects of Wireshark:

- Packet Capture
- Protocol Support
- Live Capture and Offline Analysis
- Display Filters
- Packet Inspection
- Statistics and Graphs
- Colour Coding
- Extensibility
- Cross-Platform
- Community and Support
- Security Analysis
- Educational Tool

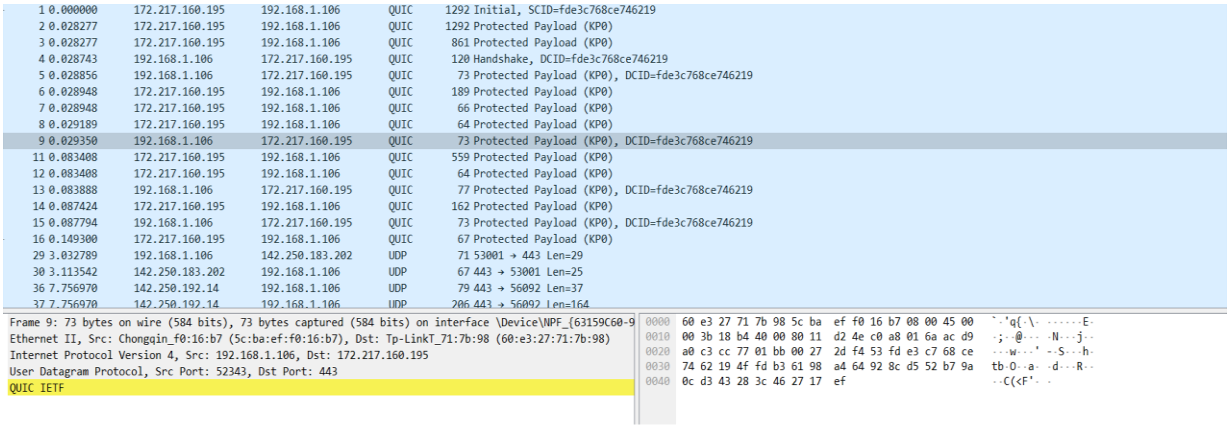
Procedure

1. Install the Wireshark and integrate it with network simulator
2. Analyse the traffic using Wireshark

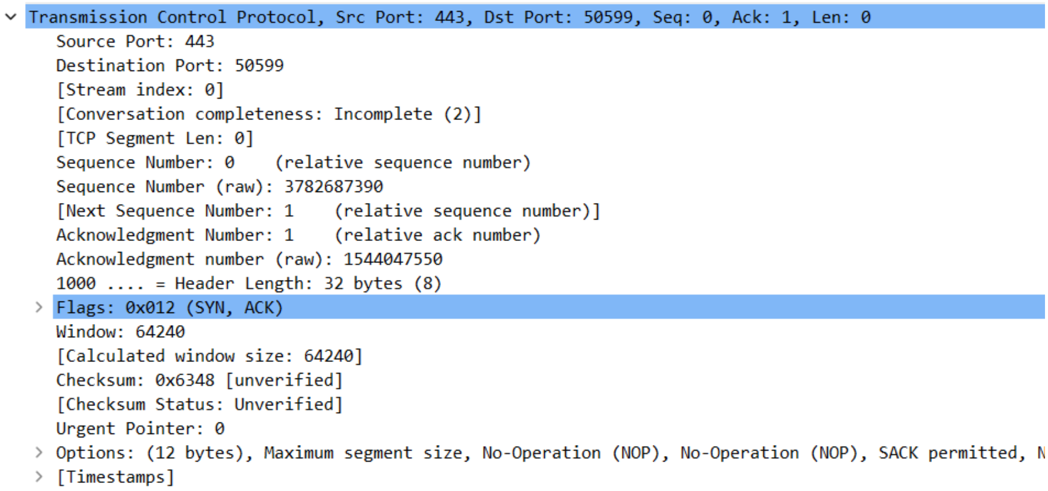
Output



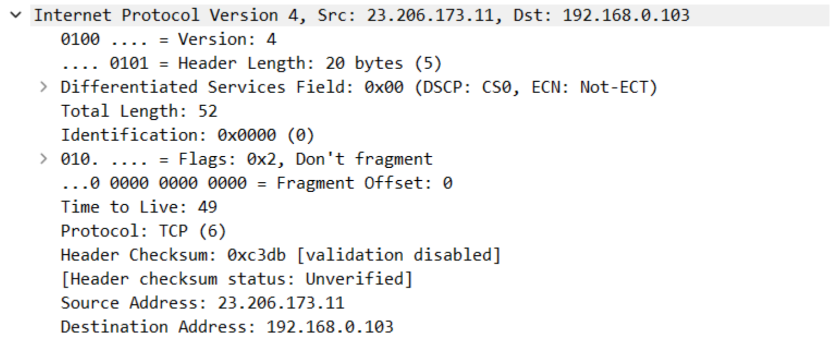
```
336 11.019952   23.55.245.49    192.168.0.103     TCP     1418 [TCP Retransmission] 443 → 50574 [ACK] Seq=240644 Ack=1599 Win=501
337 11.019952   23.55.245.49    192.168.0.103     TCP     1418 [TCP Retransmission] 443 → 50574 [PSH, ACK] Seq=242008 Ack=1599 Wi
338 11.020093   192.168.0.103   23.55.245.49      TCP       90 50574 → 443 [ACK] Seq=1599 Ack=262468 Win=2067 Len=0 SLE=300660 SR
339 11.023347   23.55.245.49    192.168.0.103     TCP     1418 [TCP Retransmission] 443 → 50574 [ACK] Seq=262468 Ack=1599 Win=501
340 11.023459   192.168.0.103   23.55.245.49      TCP       90 50574 → 443 [ACK] Seq=1599 Ack=266560 Win=2067 Len=0 SLE=300660 SR
341 11.023667   23.55.245.49    192.168.0.103     TCP     1418 [TCP Retransmission] 443 → 50574 [ACK] Seq=266560 Ack=1599 Win=501
342 11.023751   192.168.0.103   23.55.245.49      TCP       90 50574 → 443 [ACK] Seq=1599 Ack=269288 Win=2067 Len=0 SLE=300660 SR
343 11.024921   23.55.245.49    192.168.0.103     TCP     1418 [TCP Retransmission] 443 → 50574 [ACK] Seq=269288 Ack=1599 Win=501
344 11.025045   192.168.0.103   23.55.245.49      TCP       82 50574 → 443 [ACK] Seq=1599 Ack=282928 Win=2067 Len=0 SLE=300660 SR
345 11.026664   23.55.245.49    192.168.0.103     TCP     1418 [TCP Retransmission] 443 → 50574 [ACK] Seq=282928 Ack=1599 Win=501
346 11.026771   192.168.0.103   23.55.245.49      TCP       74 50574 → 443 [ACK] Seq=1599 Ack=288384 Win=2067 Len=0 SLE=300660 SR
347 11.027266   23.55.245.49    192.168.0.103     TCP     1418 [TCP Retransmission] 443 → 50574 [ACK] Seq=288384 Ack=1599 Win=501
348 11.027378   192.168.0.103   23.55.245.49      TCP       74 50574 → 443 [ACK] Seq=1599 Ack=289748 Win=2067 Len=0 SLE=300660 SR
349 11.028137   23.55.245.49    192.168.0.103     TCP     1418 [TCP Retransmission] 443 → 50574 [PSH, ACK] Seq=289748 Ack=1599 Wi
350 11.028234   192.168.0.103   23.55.245.49      TCP       66 50574 → 443 [ACK] Seq=1599 Ack=296568 Win=2067 Len=0 SLE=300660 SR
351 11.029532   23.55.245.49    192.168.0.103     TCP     1418 [TCP Retransmission] 443 → 50574 [ACK] Seq=296568 Ack=1599 Win=501
352 11.029627   192.168.0.103   23.55.245.49      TCP       66 50574 → 443 [ACK] Seq=1599 Ack=297932 Win=2067 Len=0 SLE=300660 SR
353 11.029837   23.55.245.49    192.168.0.103     TCP     1418 [TCP Retransmission] 443 → 50574 [ACK] Seq=297932 Ack=1599 Win=501
354 11.029837   23.55.245.49    192.168.0.103     TCP     1418 [TCP Retransmission] 443 → 50574 [PSH, ACK] Seq=299296 Ack=1599 Wi
355 11.029984   192.168.0.103   23.55.245.49      TCP       54 50574 → 443 [ACK] Seq=1599 Ack=304853 Win=2067 Len=0
356 11.060212   10.30.80.76     239.255.255.250   SSDP     217 M-SEARCH * HTTP/1.1
357 11.160949   10.30.80.78     239.255.255.250   SSDP     217 M-SEARCH * HTTP/1.1
358 12.082829   10.30.80.76     239.255.255.250   SSDP     217 M-SEARCH * HTTP/1.1
359 12.185250   10.30.80.78     239.255.255.250   SSDP     217 M-SEARCH * HTTP/1.1
360 13.004628   10.30.80.76     239.255.255.250   SSDP     217 M-SEARCH * HTTP/1.1
361 13.106837   10.30.80.78     239.255.255.250   SSDP     217 M-SEARCH * HTTP/1.1
362 14.335828   192.168.0.1     224.0.0.1         IGMPv3    50 Membership Query, general
363 14.374261   192.168.0.103   224.0.0.22        IGMPv3    54 Membership Report / Join group 224.0.0.252 for any sources
364 15.871820   192.168.0.103   224.0.0.22        IGMPv3    54 Membership Report / Join group 224.0.0.251 for any sources
```



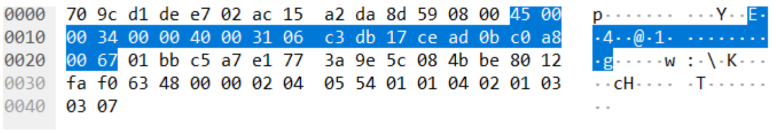
```
 1 0.000000   172.217.160.195   192.168.1.106     QUIC   1292 Initial, SCID=fde3c768ce746219
 2 0.028277   172.217.160.195   192.168.1.106     QUIC   1292 Protected Payload (KP0)
 3 0.028277   172.217.160.195   192.168.1.106     QUIC    861 Protected Payload (KP0)
 4 0.028743   192.168.1.106     172.217.160.195   QUIC    120 Handshake, DCID=fde3c768ce746219
 5 0.028856   192.168.1.106     172.217.160.195   QUIC     73 Protected Payload (KP0), DCID=fde3c768ce746219
 6 0.028948   172.217.160.195   192.168.1.106     QUIC    189 Protected Payload (KP0)
 7 0.028948   172.217.160.195   192.168.1.106     QUIC     66 Protected Payload (KP0)
 8 0.029189   172.217.160.195   192.168.1.106     QUIC     64 Protected Payload (KP0)
 9 0.029350   192.168.1.106     172.217.160.195   QUIC     73 Protected Payload (KP0), DCID=fde3c768ce746219
11 0.083408   172.217.160.195   192.168.1.106     QUIC    559 Protected Payload (KP0)
12 0.083408   172.217.160.195   192.168.1.106     QUIC     64 Protected Payload (KP0)
13 0.083888   192.168.1.106     172.217.160.195   QUIC     77 Protected Payload (KP0), DCID=fde3c768ce746219
14 0.087424   172.217.160.195   192.168.1.106     QUIC    162 Protected Payload (KP0)
15 0.087794   192.168.1.106     172.217.160.195   QUIC     73 Protected Payload (KP0), DCID=fde3c768ce746219
16 0.149300   172.217.160.195   192.168.1.106     QUIC     67 Protected Payload (KP0)
29 3.032789   192.168.1.106     142.250.183.202   UDP      71 53001 → 443 Len=29
30 3.113542   142.250.183.202   192.168.1.106     UDP      67 443 → 53001 Len=25
36 7.756970   142.250.192.14    192.168.1.106     UDP      79 443 → 56092 Len=37
37 7.756970   142.250.192.14    192.168.1.106     UDP     206 443 → 56092 Len=164

Frame 9: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface \Device\NPF_{63159C60-9
Ethernet II, Src: Chongqin_f0:16:b7 (5c:ba:ef:f0:16:b7), Dst: Tp-LinkT_71:7b:98 (60:e3:27:71:7b:98)
Internet Protocol Version 4, Src: 192.168.1.106, Dst: 172.217.160.195
User Datagram Protocol, Src Port: 52343, Dst Port: 443
QUIC IETF

0000  60 e3 27 71 7b 98 5c ba  ef f0 16 b7 08 00 45 00   `·'q{·\· ······E·
0010  00 3b 18 b4 40 00 80 11  d2 4e c0 a8 01 6a ac d9   ·;··@··· ·N···j··
0020  a0 c3 cc 77 01 bb 00 27  2d f4 53 fd e3 c7 68 ce   ···w···' -·S···h·
0030  74 62 19 4f fd b3 61 98  a4 64 92 8c d5 52 b7 9a   tb·O··a· ·d···R··
0040  0c d3 43 28 3c 46 27 17  ef                        ··C(<F'· ·
```



```
⌄ Transmission Control Protocol, Src Port: 443, Dst Port: 50599, Seq: 0, Ack: 1, Len: 0
     Source Port: 443
     Destination Port: 50599
     [Stream index: 0]
     [Conversation completeness: Incomplete (2)]
     [TCP Segment Len: 0]
     Sequence Number: 0    (relative sequence number)
     Sequence Number (raw): 3782687390
     [Next Sequence Number: 1    (relative sequence number)]
     Acknowledgment Number: 1    (relative ack number)
     Acknowledgment number (raw): 1544047550
     1000 .... = Header Length: 32 bytes (8)
  >  Flags: 0x012 (SYN, ACK)
     Window: 64240
     [Calculated window size: 64240]
     Checksum: 0x6348 [unverified]
     [Checksum Status: Unverified]
     Urgent Pointer: 0
  >  Options: (12 bytes), Maximum segment size, No-Operation (NOP), No-Operation (NOP), SACK permitted, N
  >  [Timestamps]
```



```
⌄ Internet Protocol Version 4, Src: 23.206.173.11, Dst: 192.168.0.103
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  › Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 52
    Identification: 0x0000 (0)
  › 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 49
    Protocol: TCP (6)
    Header Checksum: 0xc3db [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 23.206.173.11
    Destination Address: 192.168.0.103
```



```
0000  70 9c d1 de e7 02 ac 15  a2 da 8d 59 08 00 45 00   p·······  ···Y··E·
0010  00 34 00 00 40 00 31 06  c3 db 17 ce ad 0b c0 a8   ·4··@·1·  ········
0020  00 67 01 bb c5 a7 e1 77  3a 9e 5c 08 4b be 80 12   ·g·····w  :·\·K···
0030  fa f0 63 48 00 00 02 04  05 54 01 01 04 02 01 03   ··cH····  ·T······
0040  03 07                                              ··
```

Observation & Learning

- **Packet Capture**: Wireshark effectively captured network traffic on the specified interface, allowing us to monitor the data packets as they passed through the network.

- **Protocol Diversity**: Wireshark identified and displayed a wide variety of network protocols, including common ones like TCP, IP, UDP, HTTP, and HTTPS. This diversity is essential for understanding the different types of traffic on the network.

- **Packet Analysis**: The tool enabled us to inspect individual packets, revealing detailed information about each one. This included source and destination IP addresses, port numbers, protocol-specific details, and the content of data payloads.

- **Real-time Analysis**: Wireshark's live capture feature provided real-time data, allowing us to monitor network activity as it happened. This proved valuable for troubleshooting and identifying issues promptly.

- **Display Filters**: The use of display filters made it easy to isolate and focus on specific aspects of network traffic, helping us pinpoint relevant information amid a large volume of data.

Conclusion

The use of Wireshark for analysing network traffic has proven to be an indispensable practice for maintaining a well-functioning and secure network. This tool not only provides a comprehensive view of network activity but also empowers us to diagnose issues, optimize network performance, and enhance our network's overall reliability and security. The insights gained from this analysis will be invaluable in our ongoing efforts to manage and improve our network infrastructure.