Batch: D-2 Roll No.: 16010122151

Experiment / assignment / tutorial No.________

Grade: AA / AB / BB / BC / CC / CD /DD

Signature of the Staff In-charge with date

Experiment No.:10

TITLE: Study of Packet Analyzer tool: Wireshark

AIM: To study and analyse various Protocols using Packet Analyzer tool: Wireshark

Expected Outcome of Experiment:

CO:

Books/ Journals/ Websites referred:

1. A. S. Tanenbaum, “Computer Networks”, Pearson Education, Fourth Edition
2. B. A. Forouzan, “Data Communications and Networking”, TMH, Fourth Edition

Pre Lab/ Prior Concepts:

IPv4 Addressing, Subnetting, Link State Protocol, Router configuration Commands

New Concepts to be learned: Packet Analyzer tool: Wireshark.

THEORY:

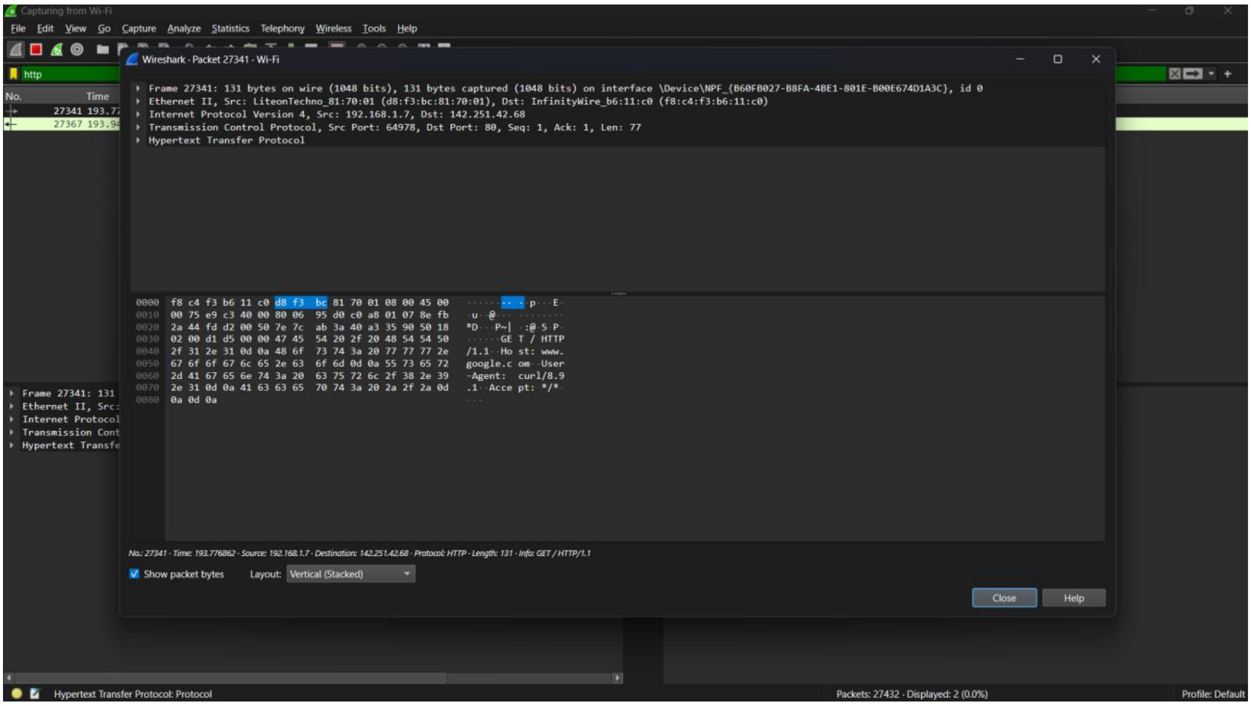
A packet analyzer, or network sniffer, like Wireshark, captures data packets traveling over a network and provides information that can be crucial for analyzing network health, troubleshooting issues, and detecting malicious activities.

Key Features of Wireshark:

1. **Protocol Analysis**: Wireshark can analyze over 2000 protocols and is updated frequently to include the latest protocol definitions.
2. **Packet Capture and Display**: Captures real-time data packets and displays them with detailed information, including source and destination IP, protocol type, and payload content.
3. **Filters and Color Coding**: Uses display filters (e.g., ip.addr == 192.168.1.1) to isolate specific traffic and color coding to distinguish protocols at a glance.
4. **Expert Information**: Highlights network anomalies like duplicate packets, retransmissions, and out-of-order packets.
5. **Graphical Analysis Tools**: Provides tools to graphically analyze data flows, packet lengths, and time-based activity.

IMPLEMENTATION:

1.HTTP


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Packet 27341 · Wi-Fi
Close
Help
Hypertext Transfer Protocol: Protocol
Packets: 27432 · Displayed: 2 (0.0%)
Profile: Default

http

No.	Time
27341	193.77
27367	193.94

```
Frame 27341: 131 bytes on wire (1048 bits), 131 bytes captured (1048 bits) on interface \Device\NPF_{B60FB027-B8FA-4BE1-801E-B00E674D1A3C}, id 0
Ethernet II, Src: LiteonTechno_81:70:01 (d8:f3:bc:81:70:01), Dst: InfinityWire_b6:11:c0 (f8:c4:f3:b6:11:c0)
Internet Protocol Version 4, Src: 192.168.1.7, Dst: 142.251.42.68
Transmission Control Protocol, Src Port: 64978, Dst Port: 80, Seq: 1, Ack: 1, Len: 77
Hypertext Transfer Protocol
```

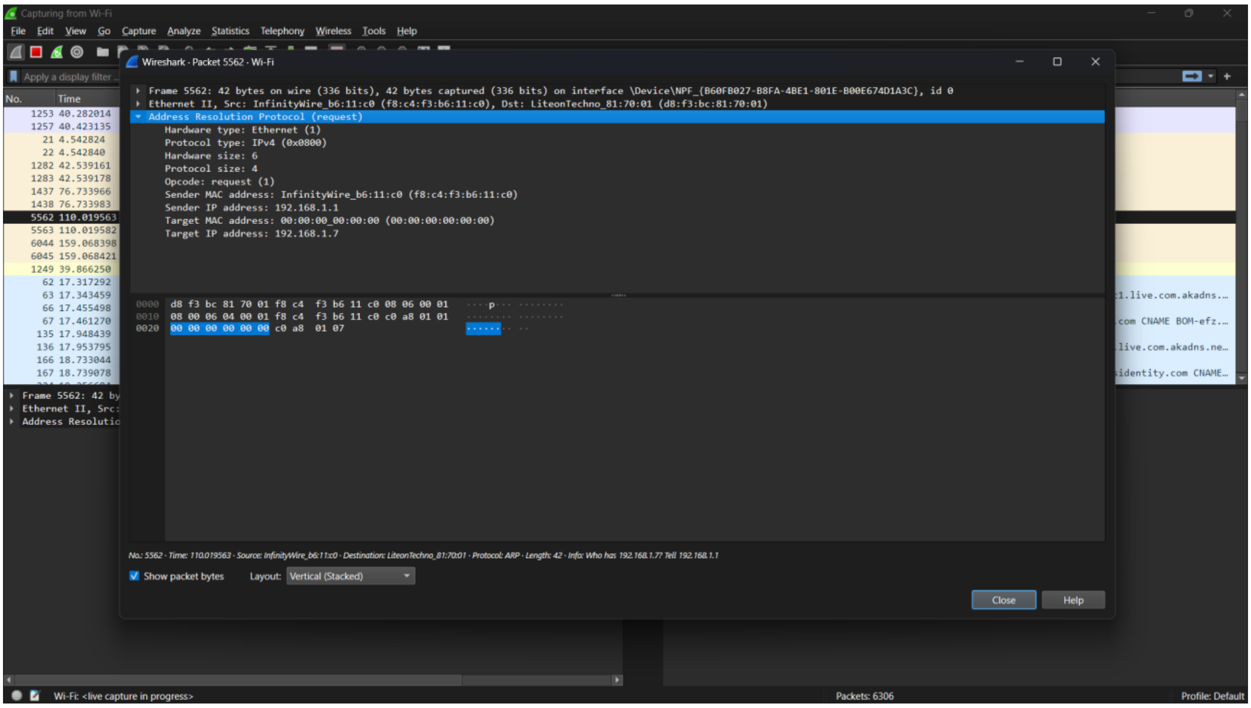
```
0000  f8 c4 f3 b6 11 c0 d8 f3  bc 81 70 01 08 00 45 00   ······ ·· ·p··E·
0010  00 75 e9 c3 40 00 80 06  95 d0 c0 a8 01 07 8e fb   ·u··@··· ········
0020  2a 44 fd d2 00 50 7e 7c  ab 3a 40 a3 35 90 50 18   *D···P~| ·:@·5·P·
0030  02 00 d1 d5 00 00 47 45  54 20 2f 20 48 54 54 50   ······GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 77 77 77 2e   /1.1··Ho st: www.
0050  67 6f 6f 67 6c 65 2e 63  6f 6d 0d 0a 55 73 65 72   google.c om··User
0060  2d 41 67 65 6e 74 3a 20  63 75 72 6c 2f 38 2e 39   -Agent:  curl/8.9
0070  2e 31 0d 0a 41 63 63 65  70 74 3a 20 2a 2f 2a 0d   .1··Acce pt: */*·
0080  0a 0d 0a                                           ···
```

```
Frame 27341: 131
Ethernet II, Src:
Internet Protocol
Transmission Cont
Hypertext Transfe
```

No.: 27341 · Time: 193.776862 · Source: 192.168.1.7 · Destination: 142.251.42.68 · Protocol: HTTP · Length: 131 · Info: GET / HTTP/1.1

☑ Show packet bytes Layout: Vertical (Stacked)

2.ARP



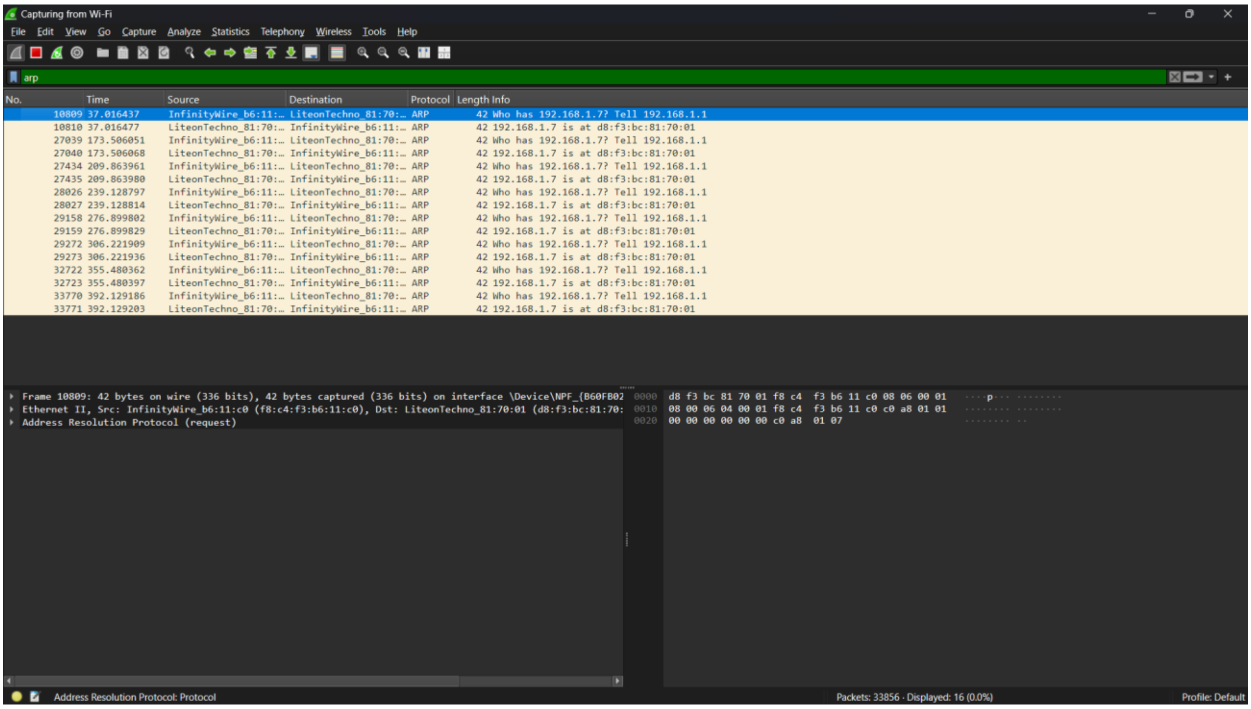
Wireshark · Packet 5562 · Wi-Fi

```
Frame 5562: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{B60FB027-B8FA-4BE1-801E-B00E674D1A3C}, id 0
Ethernet II, Src: InfinityWire_b6:11:c0 (f8:c4:f3:b6:11:c0), Dst: LiteonTechno_81:70:01 (d8:f3:bc:81:70:01)
Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: InfinityWire_b6:11:c0 (f8:c4:f3:b6:11:c0)
    Sender IP address: 192.168.1.1
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.1.7

0000  d8 f3 bc 81 70 01 f8 c4  f3 b6 11 c0 08 06 00 01   ····p··· ········
0010  08 00 06 04 00 01 f8 c4  f3 b6 11 c0 c0 a8 01 01   ········ ········
0020  00 00 00 00 00 00 c0 a8  01 07                     ········ ··
```

No.: 5562 · Time: 110.019563 · Source: InfinityWire_b6:11:c0 · Destination: LiteonTechno_81:70:01 · Protocol: ARP · Length: 42 · Info: Who has 192.168.1.7? Tell 192.168.1.1

☑ Show packet bytes   Layout: Vertical (Stacked)

Wi-Fi: <live capture in progress>   Packets: 6306   Profile: Default



Capturing from Wi-Fi

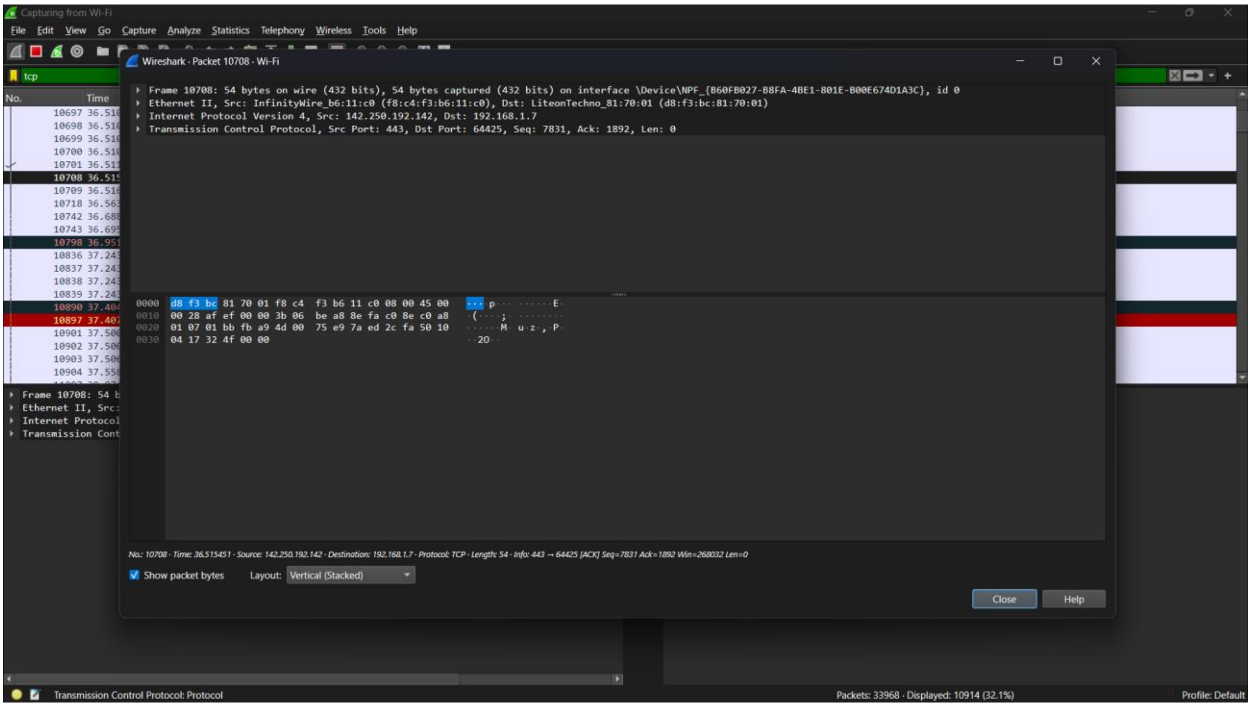
arp

```
No.    Time        Source                 Destination            Protocol Length Info
10809  37.016437   InfinityWire_b6:11:…   LiteonTechno_81:70:…   ARP      42 Who has 192.168.1.7? Tell 192.168.1.1
10810  37.016477   LiteonTechno_81:70:…   InfinityWire_b6:11:…   ARP      42 192.168.1.7 is at d8:f3:bc:81:70:01
27039  173.506051  InfinityWire_b6:11:…   LiteonTechno_81:70:…   ARP      42 Who has 192.168.1.7? Tell 192.168.1.1
27040  173.506068  LiteonTechno_81:70:…   InfinityWire_b6:11:…   ARP      42 192.168.1.7 is at d8:f3:bc:81:70:01
27434  209.863961  InfinityWire_b6:11:…   LiteonTechno_81:70:…   ARP      42 Who has 192.168.1.7? Tell 192.168.1.1
27435  209.863980  LiteonTechno_81:70:…   InfinityWire_b6:11:…   ARP      42 192.168.1.7 is at d8:f3:bc:81:70:01
28026  239.128797  InfinityWire_b6:11:…   LiteonTechno_81:70:…   ARP      42 Who has 192.168.1.7? Tell 192.168.1.1
28027  239.128814  LiteonTechno_81:70:…   InfinityWire_b6:11:…   ARP      42 192.168.1.7 is at d8:f3:bc:81:70:01
29158  276.899802  InfinityWire_b6:11:…   LiteonTechno_81:70:…   ARP      42 Who has 192.168.1.7? Tell 192.168.1.1
29159  276.899829  LiteonTechno_81:70:…   InfinityWire_b6:11:…   ARP      42 192.168.1.7 is at d8:f3:bc:81:70:01
29272  306.221909  InfinityWire_b6:11:…   LiteonTechno_81:70:…   ARP      42 Who has 192.168.1.7? Tell 192.168.1.1
29273  306.221936  LiteonTechno_81:70:…   InfinityWire_b6:11:…   ARP      42 192.168.1.7 is at d8:f3:bc:81:70:01
32722  355.480362  InfinityWire_b6:11:…   LiteonTechno_81:70:…   ARP      42 Who has 192.168.1.7? Tell 192.168.1.1
32723  355.480397  LiteonTechno_81:70:…   InfinityWire_b6:11:…   ARP      42 192.168.1.7 is at d8:f3:bc:81:70:01
33770  392.129186  InfinityWire_b6:11:…   LiteonTechno_81:70:…   ARP      42 Who has 192.168.1.7? Tell 192.168.1.1
33771  392.129203  LiteonTechno_81:70:…   InfinityWire_b6:11:…   ARP      42 192.168.1.7 is at d8:f3:bc:81:70:01
```

```
Frame 10809: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{B60FB02
Ethernet II, Src: InfinityWire_b6:11:c0 (f8:c4:f3:b6:11:c0), Dst: LiteonTechno_81:70:01 (d8:f3:bc:81:70:
Address Resolution Protocol (request)

0000  d8 f3 bc 81 70 01 f8 c4  f3 b6 11 c0 08 06 00 01   ····p··· ········
0010  08 00 06 04 00 01 f8 c4  f3 b6 11 c0 c0 a8 01 01   ········ ········
0020  00 00 00 00 00 00 c0 a8  01 07                     ········ ··
```

Address Resolution Protocol: Protocol   Packets: 33856 · Displayed: 16 (0.0%)   Profile: Default

3.TCP

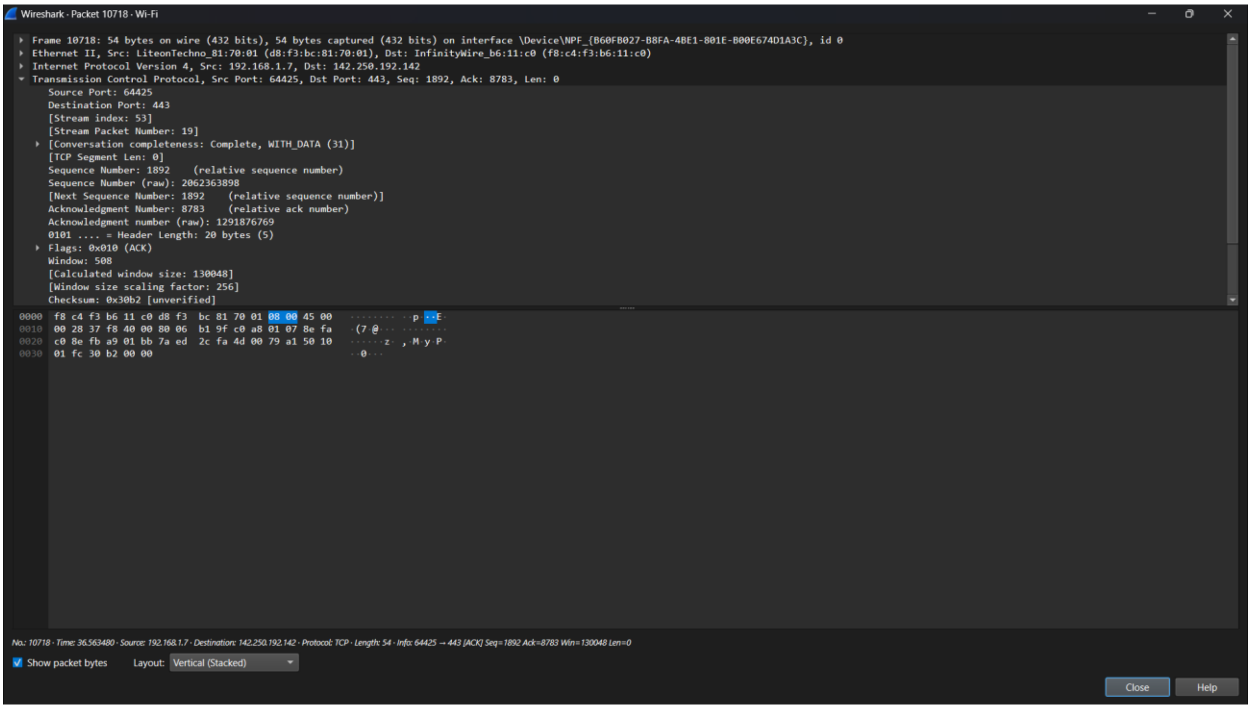

Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
Wireshark · Packet 10708 · Wi-Fi
Close
Help
Transmission Control Protocol: Protocol
Packets: 33968 · Displayed: 10914 (32.1%)
Profile: Default

```
No.     Time
10697 36.51
10698 36.51
10699 36.51
10700 36.51
10701 36.51
10708 36.51
10709 36.51
10718 36.56
10742 36.68
10743 36.69
10798 36.95
10836 37.24
10837 37.24
10838 37.24
10839 37.24
10890 37.40
10897 37.40
10901 37.50
10902 37.50
10903 37.50
10904 37.55

Frame 10708: 54 b
Ethernet II, Src:
Internet Protocol
Transmission Cont
```

```
Frame 10708: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{B60FB027-B8FA-4BE1-801E-B00E674D1A3C}, id 0
Ethernet II, Src: InfinityWire_b6:11:c0 (f8:c4:f3:b6:11:c0), Dst: LiteonTechno_81:70:01 (d8:f3:bc:81:70:01)
Internet Protocol Version 4, Src: 142.250.192.142, Dst: 192.168.1.7
Transmission Control Protocol, Src Port: 443, Dst Port: 64425, Seq: 7831, Ack: 1892, Len: 0

0000  d8 f3 bc 81 70 01 f8 c4  f3 b6 11 c0 08 00 45 00   ····p··· ······E·
0010  00 28 af ef 00 00 3b 06  be a8 8e fa c0 8e c0 a8   ·(····;· ········
0020  01 07 01 bb fb a9 4d 00  75 e9 7a ed 2c fa 50 10   ······M· u·z·,·P·
0030  04 17 32 4f 00 00                                  ··2O··
```

No.: 10708 · Time: 36.515451 · Source: 142.250.192.142 · Destination: 192.168.1.7 · Protocol: TCP · Length: 54 · Info: 443 → 64425 [ACK] Seq=7831 Ack=1892 Win=268032 Len=0

☑ Show packet bytes   Layout: Vertical (Stacked)

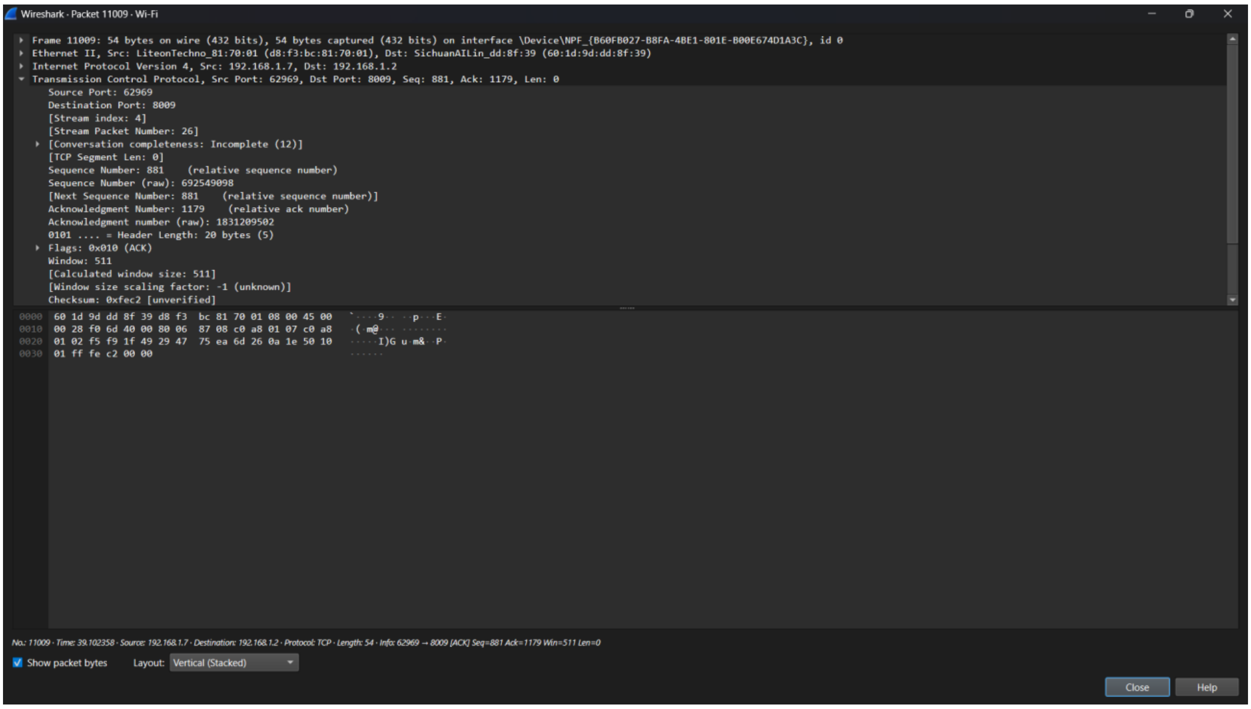


```
Frame 10718: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{B60FB027-B8FA-4BE1-801E-B00E674D1A3C}, id 0
Ethernet II, Src: LiteonTechno_81:70:01 (d8:f3:bc:81:70:01), Dst: InfinityWire_b6:11:c0 (f8:c4:f3:b6:11:c0)
Internet Protocol Version 4, Src: 192.168.1.7, Dst: 142.250.192.142
Transmission Control Protocol, Src Port: 64425, Dst Port: 443, Seq: 1892, Ack: 8783, Len: 0
    Source Port: 64425
    Destination Port: 443
    [Stream index: 53]
    [Stream Packet Number: 19]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 0]
    Sequence Number: 1892    (relative sequence number)
    Sequence Number (raw): 2062363898
    [Next Sequence Number: 1892    (relative sequence number)]
    Acknowledgment Number: 8783    (relative ack number)
    Acknowledgment number (raw): 1291876769
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x010 (ACK)
    Window: 508
    [Calculated window size: 130048]
    [Window size scaling factor: 256]
    Checksum: 0x30b2 [unverified]

0000  f8 c4 f3 b6 11 c0 d8 f3  bc 81 70 01 08 00 45 00   ········ ··p···E·
0010  00 28 37 f8 40 00 80 06  b1 9f c0 a8 01 07 8e fa   ·(7·@··· ········
0020  c0 8e fb a9 01 bb 7a ed  2c fa 4d 00 79 a1 50 10   ······z· ,·M·y·P·
0030  01 fc 30 b2 00 00                                  ··0···
```

No.: 10718 · Time: 36.563480 · Source: 192.168.1.7 · Destination: 142.250.192.142 · Protocol: TCP · Length: 54 · Info: 64425 → 443 [ACK] Seq=1892 Ack=8783 Win=130048 Len=0

☑ Show packet bytes   Layout: Vertical (Stacked)

4.IPv4



Wireshark · Packet 11009 · Wi-Fi

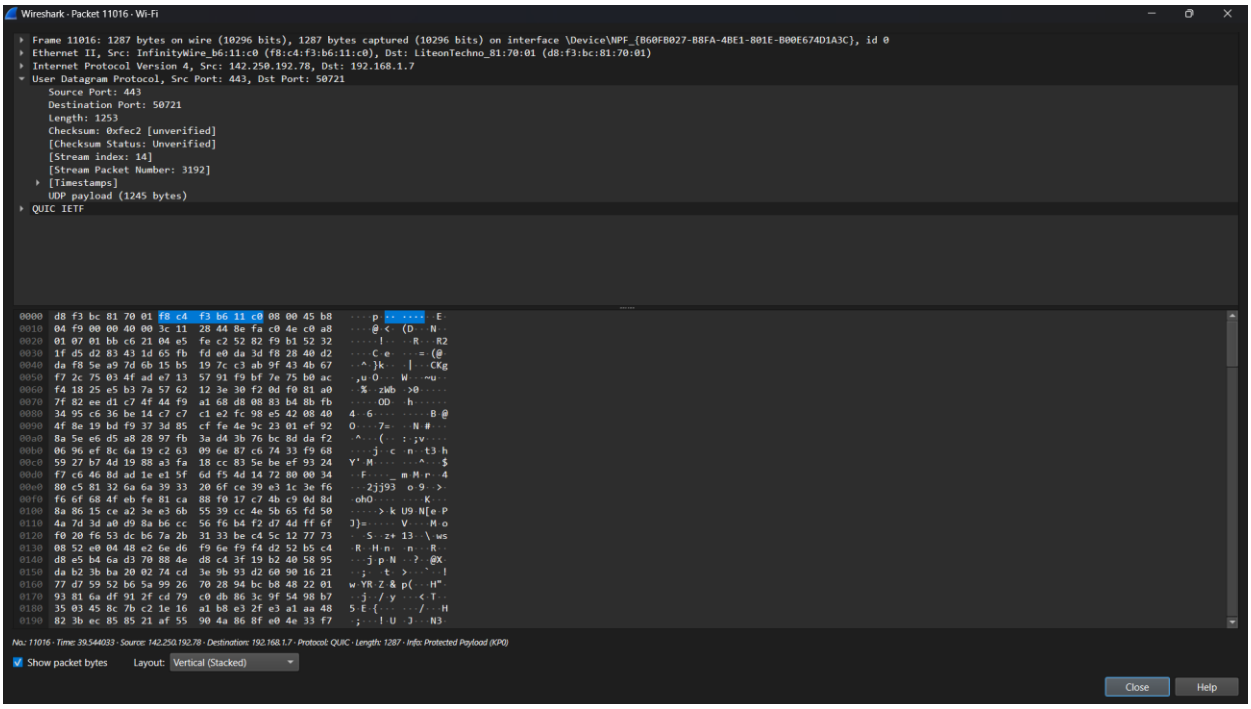
```
▸ Frame 11009: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{B60FB027-B8FA-4BE1-801E-B00E674D1A3C}, id 0
▸ Ethernet II, Src: LiteonTechno_81:70:01 (d8:f3:bc:81:70:01), Dst: SichuanAILin_dd:8f:39 (60:1d:9d:dd:8f:39)
▸ Internet Protocol Version 4, Src: 192.168.1.7, Dst: 192.168.1.2
▾ Transmission Control Protocol, Src Port: 62969, Dst Port: 8009, Seq: 881, Ack: 1179, Len: 0
     Source Port: 62969
     Destination Port: 8009
     [Stream index: 4]
     [Stream Packet Number: 26]
   ▸ [Conversation completeness: Incomplete (12)]
     [TCP Segment Len: 0]
     Sequence Number: 881    (relative sequence number)
     Sequence Number (raw): 692549098
     [Next Sequence Number: 881    (relative sequence number)]
     Acknowledgment Number: 1179    (relative ack number)
     Acknowledgment number (raw): 1831209502
     0101 .... = Header Length: 20 bytes (5)
   ▸ Flags: 0x010 (ACK)
     Window: 511
     [Calculated window size: 511]
     [Window size scaling factor: -1 (unknown)]
     Checksum: 0xfec2 [unverified]
```

```
0000  60 1d 9d dd 8f 39 d8 f3  bc 81 70 01 08 00 45 00   `····9·· ··p···E·
0010  00 28 f0 6d 40 00 80 06  87 08 c0 a8 01 07 c0 a8   ·(·m@··· ········
0020  01 02 f5 f9 1f 49 29 47  75 ea 6d 26 0a 1e 50 10   ·····I)G u·m&··P·
0030  01 ff fe c2 00 00                                  ······
```

No.: 11009 · Time: 39.102358 · Source: 192.168.1.7 · Destination: 192.168.1.2 · Protocol: TCP · Length: 54 · Info: 62969 → 8009 [ACK] Seq=881 Ack=1179 Win=511 Len=0

☑ Show packet bytes   Layout: Vertical (Stacked)

5.UDP



Wireshark · Packet 11016 · Wi-Fi

```
▸ Frame 11016: 1287 bytes on wire (10296 bits), 1287 bytes captured (10296 bits) on interface \Device\NPF_{B60FB027-B8FA-4BE1-801E-B00E674D1A3C}, id 0
▸ Ethernet II, Src: InfinityWire_b6:11:c0 (f8:c4:f3:b6:11:c0), Dst: LiteonTechno_81:70:01 (d8:f3:bc:81:70:01)
▸ Internet Protocol Version 4, Src: 142.250.192.78, Dst: 192.168.1.7
▾ User Datagram Protocol, Src Port: 443, Dst Port: 50721
     Source Port: 443
     Destination Port: 50721
     Length: 1253
     Checksum: 0xfec2 [unverified]
     [Checksum Status: Unverified]
     [Stream index: 14]
     [Stream Packet Number: 3192]
   ▸ [Timestamps]
     UDP payload (1245 bytes)
▸ QUIC IETF
```

```
0000  d8 f3 bc 81 70 01 f8 c4  f3 b6 11 c0 08 00 45 b8   ····p··· ······E·
0010  04 f9 00 00 40 00 3c 11  28 44 8e fa c0 4e c0 a8   ····@·<· (D···N··
0020  01 07 01 bb c6 21 04 e5  fe c2 52 82 f9 b1 52 32   ·····!·· ··R···R2
0030  1f d5 d2 83 43 1d 65 fb  fd e0 da 3d f8 28 40 d2   ····C·e· ···=·(@·
0040  da f8 5e a9 7d 6b 15 b5  19 7c c3 ab 9f 43 4b 67   ··^·}k·· ·|···CKg
0050  f7 2c 75 03 4f ad e7 13  57 91 f9 bf 7e 75 b0 ac   ·,u·O··· W···~u··
0060  f4 18 25 e5 b3 7a 57 62  12 3e 30 f2 0d f0 81 a0   ··%··zWb ·>0·····
0070  7f 82 ee d1 c7 4f 44 f9  a1 68 d8 08 83 b4 8b fb   ·····OD· ·h······
0080  34 95 c6 36 be 14 c7 c7  c1 e2 fc 98 e5 42 08 40   4··6···· ·····B·@
0090  4f 8e 19 bd f9 37 3d 85  cf fe 4e 9c 23 01 ef 92   O····7=· ··N·#···
00a0  8a 5e e6 d5 a8 28 97 fb  3a d4 3b 76 bc 8d da f2   ·^···(·· :·;v····
00b0  06 96 ef 8c 6a 19 c2 63  09 6e 87 c6 74 33 f9 68   ····j··c ·n··t3·h
00c0  59 27 b7 4d 19 88 a3 fa  18 cc 83 5e be ef 93 24   Y'·M···· ···^···$
00d0  f7 c6 46 8d ad 1e e1 5f  6d f5 4d 14 72 80 00 34   ··F····_ m·M·r··4
00e0  80 c5 81 32 6a 6a 39 33  20 6f ce 39 e3 1c 3e f6   ···2jj93  o·9··>·
00f0  f6 6f 68 4f eb fe 81 ca  88 f0 17 c7 4b c9 0d 8d   ·ohO···· ····K···
0100  8a 86 15 ce a2 3e e3 6b  55 39 cc 4e 5b 65 fd 50   ·····>·k U9·N[e·P
0110  4a 7d 3d a0 d9 8a b6 cc  56 f6 b4 f2 d7 4d ff 6f   J}=····· V····M·o
0120  f0 20 f6 53 dc b6 7a 2b  31 33 be c4 5c 12 77 73   · ·S··z+ 13··\·ws
0130  08 52 e0 04 48 e2 6e d6  f9 6e f9 f4 d2 52 b5 c4   ·R··H·n· ·n···R··
0140  d8 e5 b4 6a d3 70 88 4e  d8 c4 3f 19 b2 40 58 95   ···j·p·N ··?··@X·
0150  da b2 3b ba 20 02 74 cd  3e 9b 93 d2 60 90 16 21   ··;· ·t· >···`··!
0160  77 d7 59 52 b6 5a 99 26  70 28 94 bc b8 48 22 01   w·YR·Z·& p(···H"·
0170  93 81 6a df 91 2f cd 79  c0 db 86 3c 9f 54 98 b7   ··j··/·y ···<·T··
0180  35 03 45 8c 7b c2 1e 16  a1 b8 e3 2f e3 a1 aa 48   5·E·{··· ···/···H
0190  82 3b ec 85 85 21 af 55  90 4a 86 8f e0 4e 33 f7   ·;···!·U ·J···N3·
```

No.: 11016 · Time: 39.544033 · Source: 142.250.192.78 · Destination: 192.168.1.7 · Protocol: QUIC · Length: 1287 · Info: Protected Payload (KP0)

☑ Show packet bytes   Layout: Vertical (Stacked)

CONCLUSION:

We learned how to analyse the web protocols with wireshark, and got to know in detail how the computer network works

Date: 11-11-2024 **Signature of faculty in-charge**