NAME : PRERNA SUNIL JADHAV

SAPID: 60004220127

BATCH : COMPUTER ENGINEERING

COURSE: INFORMATION SECURITY LABORATORY

COURSE CODE: DJ19CEL603

EXPERIMENT10

AIM: Perform Packet capture & sniffing IP traffic using wireshark.

THEORY: Packet sniffers intercept packets of data flowing across a computer network in order to view their content in. This act is called packet sniffing.

webpages and emails are not sent through the Internet as one document rather, the sending side breaks them down into many little data packets. These packets are then addressed to an IP address at the receiving end, which has to send back an acknowledgement of each packet it receives.

These packets are not transferred from the sender to the receiver through a single ~~to~~ direct connection. Instead as each packet traverses, the internet enroute to its destination, it passes through a no. of traffic control devices such as routers and switches. Each time a a packet poses through one of these traffic control devices, it is suspectible to capture & analysis. Wireshark smart sniff are examples of packet sniffing tools.

CONCLUSION: Thus, we have performed packet capture & sniffed IP traffic using wireshalk.

Name:	Prerna Sunil Jadhav
Sap Id:	60004220127
Class:	T. Y. B. Tech (Computer Engineering)
Course:	Information Security Laboratory
Course Code:	DJ19CEL603
Experiment No.:	10

AIM: Perform Packet Capture and Sniff IP traffic using Wireshark.

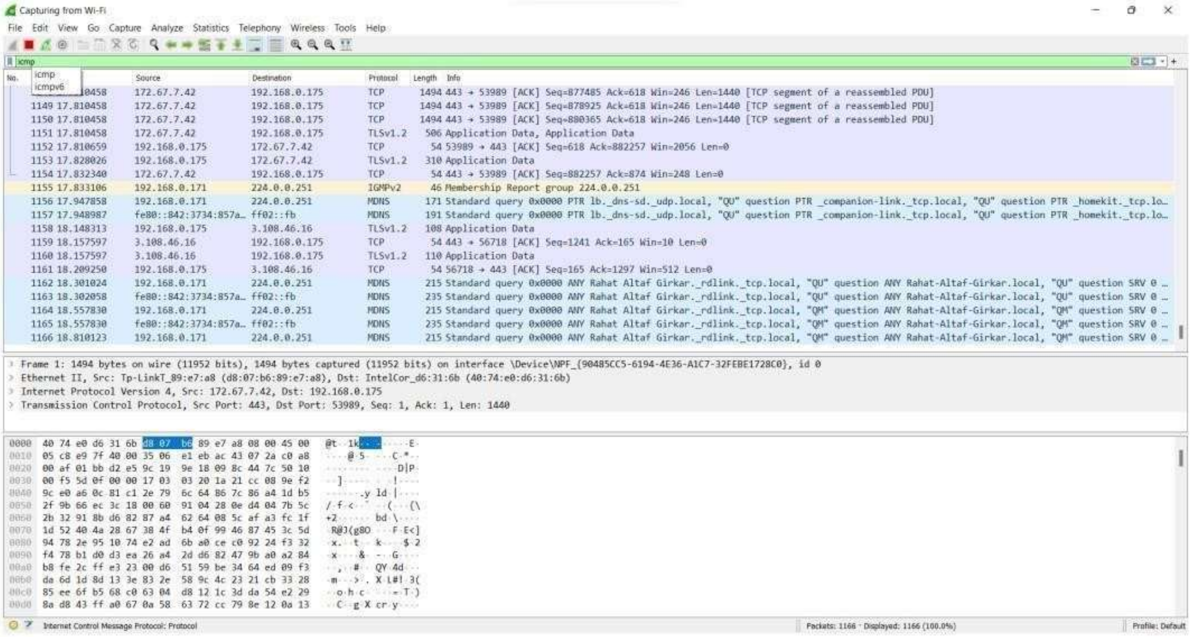
<u>Capturing ICMP Packets:</u>

C:\Users\Marwin Shroff>ping 8.8.8.8 Pinging 8.8.8.8 with 32 bytes of data: Reply from 8.8.8.8: bytes=32 time=5ms TTL=119

Reply from 8.8.8.8: bytes=32 time=6ms TTL=119 Reply from 8.8.8.8: bytes=32 time=2ms TTL=119

Reply from 8.8.8.8: bytes=32 time=3ms TTL=119 Ping statistics for 8.8.8.8:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 2ms, Maximum = 6ms, Average = 4ms


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
icmp
icmpv6

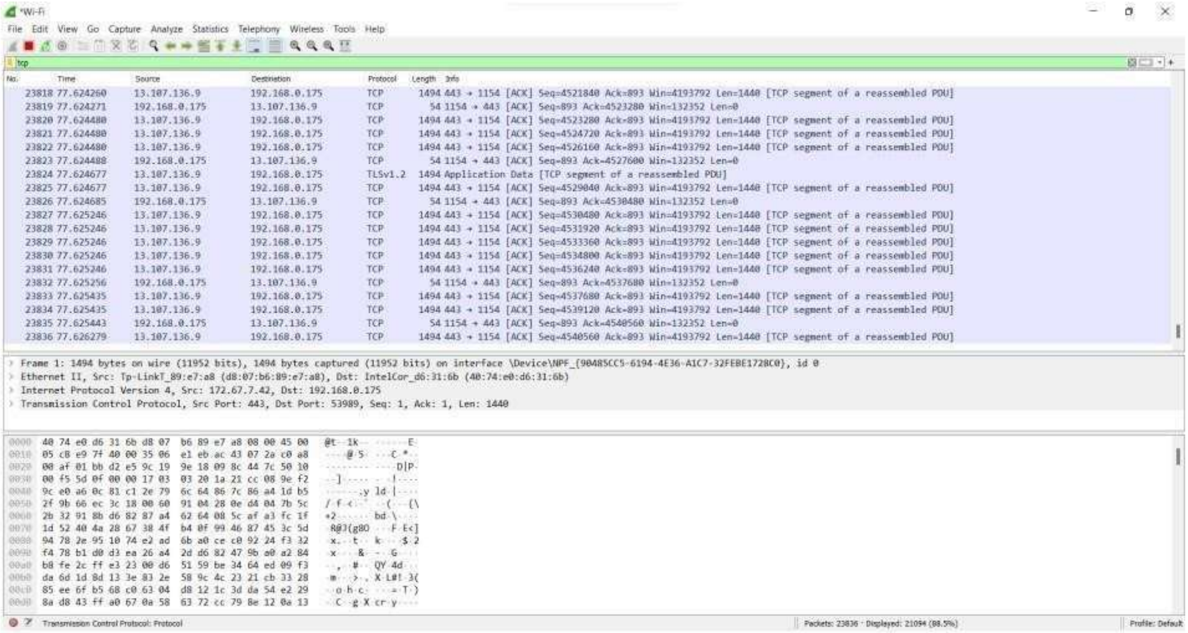
```
No.          Source               Destination       Protocol  Length Info
        0458 172.67.7.42          192.168.0.175     TCP       1494 443 → 53989 [ACK] Seq=877485 Ack=618 Win=246 Len=1440 [TCP segment of a reassembled PDU]
1149 17.810458 172.67.7.42        192.168.0.175     TCP       1494 443 → 53989 [ACK] Seq=878925 Ack=618 Win=246 Len=1440 [TCP segment of a reassembled PDU]
1150 17.810458 172.67.7.42        192.168.0.175     TCP       1494 443 → 53989 [ACK] Seq=880365 Ack=618 Win=246 Len=1440 [TCP segment of a reassembled PDU]
1151 17.810458 172.67.7.42        192.168.0.175     TLSv1.2    506 Application Data, Application Data
1152 17.810659 192.168.0.175      172.67.7.42       TCP         54 53989 → 443 [ACK] Seq=618 Ack=882257 Win=2056 Len=0
1153 17.828026 192.168.0.175      172.67.7.42       TLSv1.2    310 Application Data
1154 17.832340 172.67.7.42        192.168.0.175     TCP         54 443 → 53989 [ACK] Seq=882257 Ack=874 Win=248 Len=0
1155 17.833106 192.168.0.171      224.0.0.251       IGMPv2      46 Membership Report group 224.0.0.251
1156 17.947858 192.168.0.171      224.0.0.251       MDNS       171 Standard query 0x0000 PTR lb._dns-sd._udp.local, "QU" question PTR _companion-link._tcp.local, "QU" question PTR _homekit._tcp.lo…
1157 17.948987 fe80::842:3734:857a… ff02::fb        MDNS       191 Standard query 0x0000 PTR lb._dns-sd._udp.local, "QU" question PTR _companion-link._tcp.local, "QU" question PTR _homekit._tcp.lo…
1158 18.148313 192.168.0.175      3.108.46.16       TLSv1.2    108 Application Data
1159 18.157597 3.108.46.16        192.168.0.175     TCP         54 443 → 56718 [ACK] Seq=1241 Ack=165 Win=10 Len=0
1160 18.157597 3.108.46.16        192.168.0.175     TLSv1.2    110 Application Data
1161 18.209250 192.168.0.175      3.108.46.16       TCP         54 56718 → 443 [ACK] Seq=165 Ack=1297 Win=512 Len=0
1162 18.301024 192.168.0.171      224.0.0.251       MDNS       215 Standard query 0x0000 ANY Rahat Altaf Girkar._rdlink._tcp.local, "QU" question ANY Rahat-Altaf-Girkar.local, "QU" question SRV 0 …
1163 18.302058 fe80::842:3734:857a… ff02::fb        MDNS       235 Standard query 0x0000 ANY Rahat Altaf Girkar._rdlink._tcp.local, "QU" question ANY Rahat-Altaf-Girkar.local, "QU" question SRV 0 …
1164 18.557830 192.168.0.171      224.0.0.251       MDNS       215 Standard query 0x0000 ANY Rahat Altaf Girkar._rdlink._tcp.local, "QM" question ANY Rahat-Altaf-Girkar.local, "QM" question SRV 0 …
1165 18.557830 fe80::842:3734:857a… ff02::fb        MDNS       235 Standard query 0x0000 ANY Rahat Altaf Girkar._rdlink._tcp.local, "QM" question ANY Rahat-Altaf-Girkar.local, "QM" question SRV 0 …
1166 18.810123 192.168.0.171      224.0.0.251       MDNS       215 Standard query 0x0000 ANY Rahat Altaf Girkar._rdlink._tcp.local, "QM" question ANY Rahat-Altaf-Girkar.local, "QM" question SRV 0 …
```

```
> Frame 1: 1494 bytes on wire (11952 bits), 1494 bytes captured (11952 bits) on interface \Device\NPF_{90485CC5-6194-4E36-A1C7-32FEBE1728C0}, id 0
> Ethernet II, Src: Tp-LinkT_89:e7:a8 (d8:07:b6:89:e7:a8), Dst: IntelCor_d6:31:6b (40:74:e0:d6:31:6b)
> Internet Protocol Version 4, Src: 172.67.7.42, Dst: 192.168.0.175
> Transmission Control Protocol, Src Port: 443, Dst Port: 53989, Seq: 1, Ack: 1, Len: 1440
```

```
0000  40 74 e0 d6 31 6b d8 07  b6 89 e7 a8 08 00 45 00   @t··1k········E·
0010  05 c8 e9 7f 40 00 35 06  e1 eb ac 43 07 2a c0 a8   ····@·5····C·*··
0020  00 af 01 bb d2 e5 9c 19  9e 18 09 8c 44 7c 50 10   ············D|P·
0030  00 f5 5d 0f 00 00 17 03  03 20 1a 21 cc 08 9e f2   ··]······ ·!····
0040  9c e0 a6 0c 81 c1 2e 79  6c 64 86 7c 86 a4 1d b5   ·······yld·|····
0050  2f 9b 66 ec 3c 18 00 60  91 04 28 0e d4 04 7b 5c   /·f·<··`··(···{\
0060  2b 32 91 8b d6 82 87 a4  62 64 08 5c af a3 fc 1f   +2······bd·\····
0070  1d 52 40 4a 28 67 38 4f  b4 0f 99 46 87 45 3c 5d   ·R@J(g8O···F·E<]
0080  94 78 2e 95 10 74 e2 ad  6b a0 ce c0 92 24 f3 32   ·x.··t··k····$·2
0090  f4 78 b1 d0 d3 ea 26 a4  2d d6 82 47 9b a0 a2 84   ·x····&·-··G····
00a0  b8 fe 2c ff e3 23 00 d6  51 59 be 34 64 ed 09 f3   ··,··#··QY·4d···
00b0  da 6d 1d 8d 13 3e 83 2e  58 9c 4c 23 21 cb 33 28   ·m···>·.X·L#!·3(
00c0  85 ee 6f b5 68 c0 63 04  d8 12 1c 3d da 54 e2 29   ··o·h·c····=·T·)
00d0  8a d8 43 ff a0 67 0a 58  63 72 cc 79 8e 12 0a 13   ··C··g·Xcr·y····
```

Internet Control Message Protocol: Protocol
Packets: 1166 · Displayed: 1166 (100.0%)
Profile: Default

Capturing TCP Packets:


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp

```
No.   Time       Source          Destination     Protocol Length Info
23818 77.624260  13.107.136.9    192.168.0.175   TCP      1494 443 → 1154 [ACK] Seq=4521840 Ack=893 Win=4193792 Len=1440 [TCP segment of a reassembled PDU]
23819 77.624271  192.168.0.175   13.107.136.9    TCP        54 1154 → 443 [ACK] Seq=893 Ack=4523280 Win=132352 Len=0
23820 77.624480  13.107.136.9    192.168.0.175   TCP      1494 443 → 1154 [ACK] Seq=4523280 Ack=893 Win=4193792 Len=1440 [TCP segment of a reassembled PDU]
23821 77.624480  13.107.136.9    192.168.0.175   TCP      1494 443 → 1154 [ACK] Seq=4524720 Ack=893 Win=4193792 Len=1440 [TCP segment of a reassembled PDU]
23822 77.624480  13.107.136.9    192.168.0.175   TCP      1494 443 → 1154 [ACK] Seq=4526160 Ack=893 Win=4193792 Len=1440 [TCP segment of a reassembled PDU]
23823 77.624488  192.168.0.175   13.107.136.9    TCP        54 1154 → 443 [ACK] Seq=893 Ack=4527600 Win=132352 Len=0
23824 77.624677  13.107.136.9    192.168.0.175   TLSv1.2  1494 Application Data [TCP segment of a reassembled PDU]
23825 77.624677  13.107.136.9    192.168.0.175   TCP      1494 443 → 1154 [ACK] Seq=4529040 Ack=893 Win=4193792 Len=1440 [TCP segment of a reassembled PDU]
23826 77.624685  192.168.0.175   13.107.136.9    TCP        54 1154 → 443 [ACK] Seq=893 Ack=4530480 Win=132352 Len=0
23827 77.625246  13.107.136.9    192.168.0.175   TCP      1494 443 → 1154 [ACK] Seq=4530480 Ack=893 Win=4193792 Len=1440 [TCP segment of a reassembled PDU]
23828 77.625246  13.107.136.9    192.168.0.175   TCP      1494 443 → 1154 [ACK] Seq=4531920 Ack=893 Win=4193792 Len=1440 [TCP segment of a reassembled PDU]
23829 77.625246  13.107.136.9    192.168.0.175   TCP      1494 443 → 1154 [ACK] Seq=4533360 Ack=893 Win=4193792 Len=1440 [TCP segment of a reassembled PDU]
23830 77.625246  13.107.136.9    192.168.0.175   TCP      1494 443 → 1154 [ACK] Seq=4534800 Ack=893 Win=4193792 Len=1440 [TCP segment of a reassembled PDU]
23831 77.625246  13.107.136.9    192.168.0.175   TCP      1494 443 → 1154 [ACK] Seq=4536240 Ack=893 Win=4193792 Len=1440 [TCP segment of a reassembled PDU]
23832 77.625256  192.168.0.175   13.107.136.9    TCP        54 1154 → 443 [ACK] Seq=893 Ack=4537680 Win=132352 Len=0
23833 77.625435  13.107.136.9    192.168.0.175   TCP      1494 443 → 1154 [ACK] Seq=4537680 Ack=893 Win=4193792 Len=1440 [TCP segment of a reassembled PDU]
23834 77.625435  13.107.136.9    192.168.0.175   TCP      1494 443 → 1154 [ACK] Seq=4539120 Ack=893 Win=4193792 Len=1440 [TCP segment of a reassembled PDU]
23835 77.625443  192.168.0.175   13.107.136.9    TCP        54 1154 → 443 [ACK] Seq=893 Ack=4540560 Win=132352 Len=0
23836 77.626279  13.107.136.9    192.168.0.175   TCP      1494 443 → 1154 [ACK] Seq=4540560 Ack=893 Win=4193792 Len=1440 [TCP segment of a reassembled PDU]
```

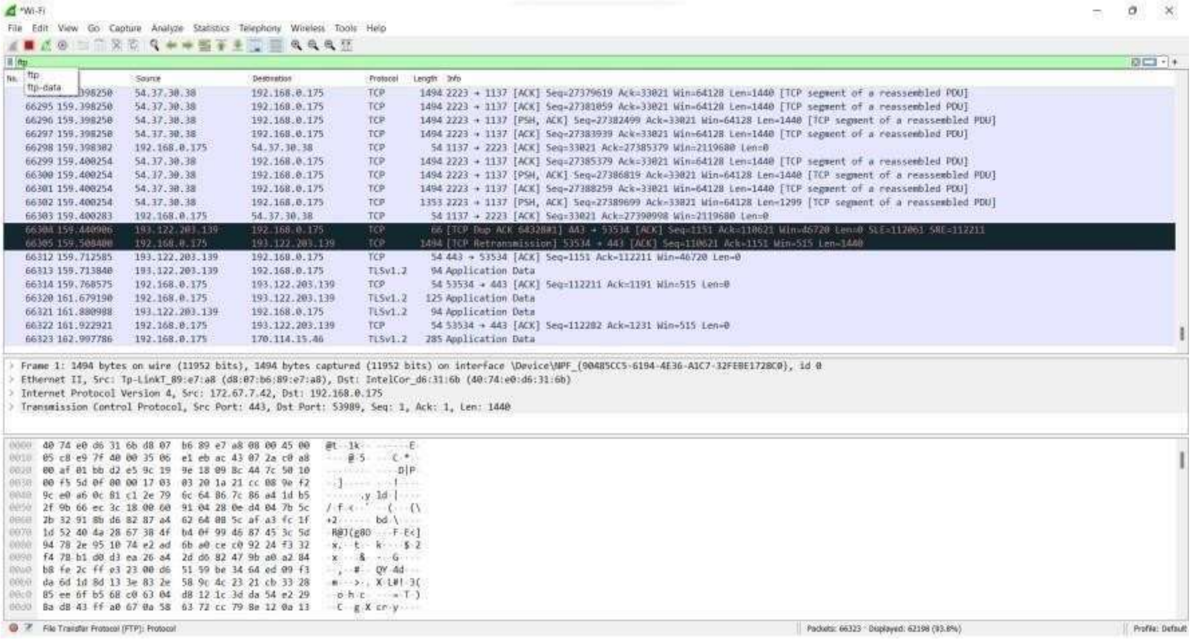
```
> Frame 1: 1494 bytes on wire (11952 bits), 1494 bytes captured (11952 bits) on interface \Device\NPF_{90485CC5-6194-4E36-A1C7-32FEBE1728C0}, id 0
> Ethernet II, Src: Tp-LinkT_89:e7:a8 (d8:07:b6:89:e7:a8), Dst: IntelCor_d6:31:6b (40:74:e0:d6:31:6b)
> Internet Protocol Version 4, Src: 172.67.7.42, Dst: 192.168.0.175
> Transmission Control Protocol, Src Port: 443, Dst Port: 53989, Seq: 1, Ack: 1, Len: 1440
```

```
0000  40 74 e0 d6 31 6b d8 07  b6 89 e7 a8 08 00 45 00   @t··1k········E·
0010  05 c8 e9 7f 40 00 35 06  e1 eb ac 43 07 2a c0 a8   ····@·5····C·*··
0020  00 af 01 bb d2 e5 9c 19  9e 18 09 8c 44 7c 50 10   ············D|P·
0030  00 f5 5d 0f 00 00 17 03  03 20 1a 21 cc 08 9e f2   ··]······ ·!····
0040  9c e0 a6 0c 81 c1 2e 79  6c 64 86 7c 86 a4 1d b5   ·······.yld·|····
0050  2f 9b 66 ec 3c 18 00 60  91 04 28 0e d4 04 7b 5c   /·f·<··`··(···{\
0060  2b 32 91 8b d6 82 87 a4  62 64 08 5c af a3 fc 1f   +2······bd·\····
0070  1d 52 40 4a 28 67 38 4f  b4 0f 99 46 87 45 3c 5d   ·R@J(g8O···F·E<]
0080  94 78 2e 95 10 74 e2 ad  6b a0 ce c0 92 24 f3 32   ·x.··t··k····$·2
0090  f4 78 b1 d0 d3 ea 26 a4  2d d6 82 47 9b a0 a2 84   ·x····&·-··G····
00a0  b8 fe 2c ff e3 23 00 d6  51 59 be 34 64 ed 09 f3   ··,··#··QY·4d···
00b0  da 6d 1d 8d 13 3e 83 2e  58 9c 4c 23 21 cb 33 28   ·m···>·.X·L#!·3(
00c0  85 ee 6f b5 68 c0 63 04  d8 12 1c 3d da 54 e2 29   ··o·h·c····=·T·)
00d0  8a d8 43 ff a0 67 0a 58  63 72 cc 79 8e 12 0a 13   ··C··g·Xcr·y····
```

Transmission Control Protocol: Protocol
Packets: 23836 · Displayed: 21094 (88.5%)
Profile: Default

Capturing FTP Packets:

```
C:\Users\Marwin Shroff>ftp ftp.cdc.gov Connected to ftp.cdc.gov. 220 Microsoft FTP Service
200 OPTS UTF8 command successful - UTF8 encoding now ON. User (ftp.cdc.gov:(none)):
        anonymous
331 Anonymous access allowed, send identity (e-mail name) as password. Password: 230 User
        logged in.
ftp> ls
200 PORT command successful.
150 Opening ASCII mode data connection.
.change.dir .message pub Readme
Siteinfo w3c welcome.msg 226 Transfer complete. ftp: 67 bytes received in 0.03Seconds
        2.03Kbytes/sec.
```


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ftp
ftp
ftp-data

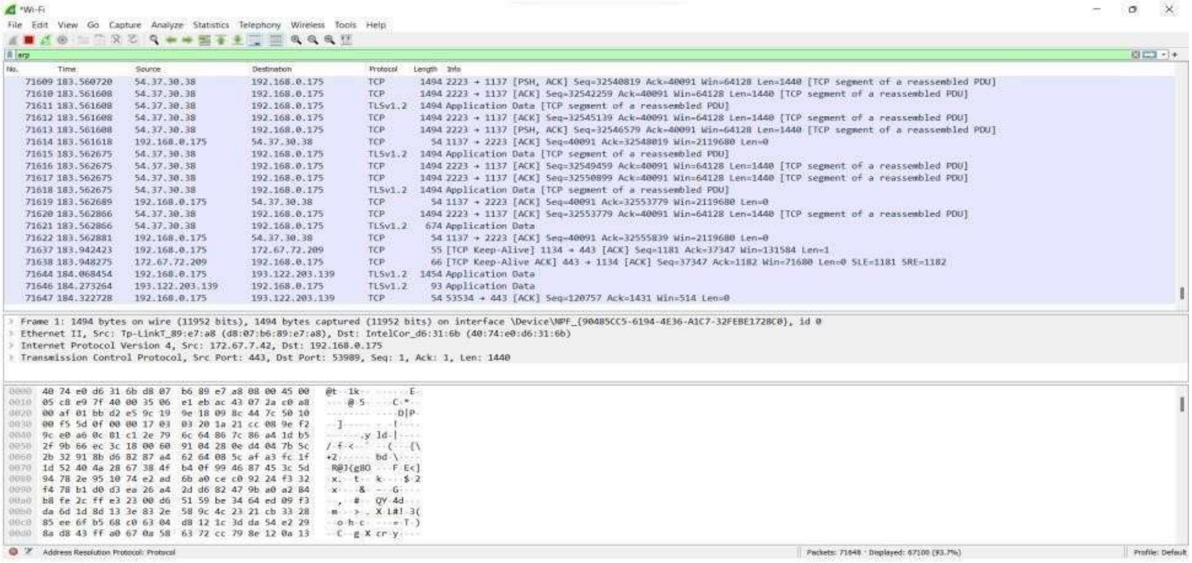
```
No.   Time           Source           Destination      Protocol  Length Info
      ...398250      54.37.30.38      192.168.0.175    TCP       1494 2223 → 1137 [ACK] Seq=27379619 Ack=33021 Win=64128 Len=1440 [TCP segment of a reassembled PDU]
66295 159.398250     54.37.30.38      192.168.0.175    TCP       1494 2223 → 1137 [ACK] Seq=27381059 Ack=33021 Win=64128 Len=1440 [TCP segment of a reassembled PDU]
66296 159.398250     54.37.30.38      192.168.0.175    TCP       1494 2223 → 1137 [PSH, ACK] Seq=27382499 Ack=33021 Win=64128 Len=1440 [TCP segment of a reassembled PDU]
66297 159.398250     54.37.30.38      192.168.0.175    TCP       1494 2223 → 1137 [ACK] Seq=27383939 Ack=33021 Win=64128 Len=1440 [TCP segment of a reassembled PDU]
66298 159.398382     192.168.0.175    54.37.30.38      TCP         54 1137 → 2223 [ACK] Seq=33021 Ack=27385379 Win=2119680 Len=0
66299 159.400254     54.37.30.38      192.168.0.175    TCP       1494 2223 → 1137 [ACK] Seq=27385379 Ack=33021 Win=64128 Len=1440 [TCP segment of a reassembled PDU]
66300 159.400254     54.37.30.38      192.168.0.175    TCP       1494 2223 → 1137 [PSH, ACK] Seq=27386819 Ack=33021 Win=64128 Len=1440 [TCP segment of a reassembled PDU]
66301 159.400254     54.37.30.38      192.168.0.175    TCP       1494 2223 → 1137 [ACK] Seq=27388259 Ack=33021 Win=64128 Len=1440 [TCP segment of a reassembled PDU]
66302 159.400254     54.37.30.38      192.168.0.175    TCP       1353 2223 → 1137 [PSH, ACK] Seq=27389699 Ack=33021 Win=64128 Len=1299 [TCP segment of a reassembled PDU]
66303 159.400283     192.168.0.175    54.37.30.38      TCP         54 1137 → 2223 [ACK] Seq=33021 Ack=27390998 Win=2119680 Len=0
66304 159.440906     193.122.203.139  192.168.0.175    TCP         66 [TCP Dup ACK 64328#1] 443 → 53534 [ACK] Seq=1151 Ack=110621 Win=46720 Len=0 SLE=112061 SRE=112211
66305 159.508400     192.168.0.175    193.122.203.139  TCP       1494 [TCP Retransmission] 53534 → 443 [ACK] Seq=110621 Ack=1151 Win=515 Len=1440
66312 159.712585     193.122.203.139  192.168.0.175    TCP         54 443 → 53534 [ACK] Seq=1151 Ack=112211 Win=46720 Len=0
66313 159.713840     193.122.203.139  192.168.0.175    TLSv1.2     94 Application Data
66314 159.768575     192.168.0.175    193.122.203.139  TCP         54 53534 → 443 [ACK] Seq=112211 Ack=1191 Win=515 Len=0
66320 161.679190     192.168.0.175    193.122.203.139  TLSv1.2    125 Application Data
66321 161.880988     193.122.203.139  192.168.0.175    TLSv1.2     94 Application Data
66322 161.922921     192.168.0.175    193.122.203.139  TCP         54 53534 → 443 [ACK] Seq=112282 Ack=1231 Win=515 Len=0
66323 162.997786     192.168.0.175    170.114.15.46    TLSv1.2    285 Application Data
```

```
> Frame 1: 1494 bytes on wire (11952 bits), 1494 bytes captured (11952 bits) on interface \Device\NPF_{90485CC5-6194-4E36-A1C7-32FEBE1728C0}, id 0
> Ethernet II, Src: Tp-LinkT_89:e7:a8 (d8:07:b6:89:e7:a8), Dst: IntelCor_d6:31:6b (40:74:e0:d6:31:6b)
> Internet Protocol Version 4, Src: 172.67.7.42, Dst: 192.168.0.175
> Transmission Control Protocol, Src Port: 443, Dst Port: 53989, Seq: 1, Ack: 1, Len: 1440
```

```
0000  40 74 e0 d6 31 6b d8 07  b6 89 e7 a8 08 00 45 00   @t··1k········E·
0010  05 c8 e9 7f 40 00 35 06  e1 eb ac 43 07 2a c0 a8   ····@·5····C·*··
0020  00 af 01 bb d2 e5 9c 19  9e 18 09 8c 44 7c 50 10   ············D|P·
0030  00 f5 5d 0f 00 00 17 03  03 20 1a 21 cc 08 9e f2   ··]······ ·!····
0040  9c e0 a6 0c 81 c1 2e 79  6c 64 86 7c 86 a4 1d b5   ·······yld·|····
0050  2f 9b 66 ec 3c 18 00 60  91 04 28 0e d4 04 7b 5c   /·f·<··`··(···{\
0060  2b 32 91 8b d6 82 87 a4  62 64 08 5c af a3 fc 1f   +2······bd·\····
0070  1d 52 40 4a 28 67 38 4f  b4 0f 99 46 87 45 3c 5d   ·R@J(g8O···F·E<]
0080  94 78 2e 95 10 74 e2 ad  6b a0 ce c0 92 24 f3 32   ·x.··t··k····$·2
0090  f4 78 b1 d0 d3 ea 26 a4  2d d6 82 47 9b a0 a2 84   ·x····&·-··G····
00a0  b8 fe 2c ff e3 23 00 d6  51 59 be 34 64 ed 09 f3   ··,··#··QY·4d···
00b0  da 6d 1d 8d 13 3e 83 2e  58 9c 4c 23 21 cb 33 28   ·m···>·.X·L#!·3(
00c0  85 ee 6f b5 68 c0 63 04  d8 12 1c 3d da 54 e2 29   ··o·h·c····=·T·)
00d0  8a d8 43 ff a0 67 0a 58  63 72 cc 79 8e 12 0a 13   ··C··g·Xcr·y····
```

File Transfer Protocol (FTP): Protocol | Packets: 66323 · Displayed: 62198 (93.8%) | Profile: Default

Capturing ARP Packets:


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
arp

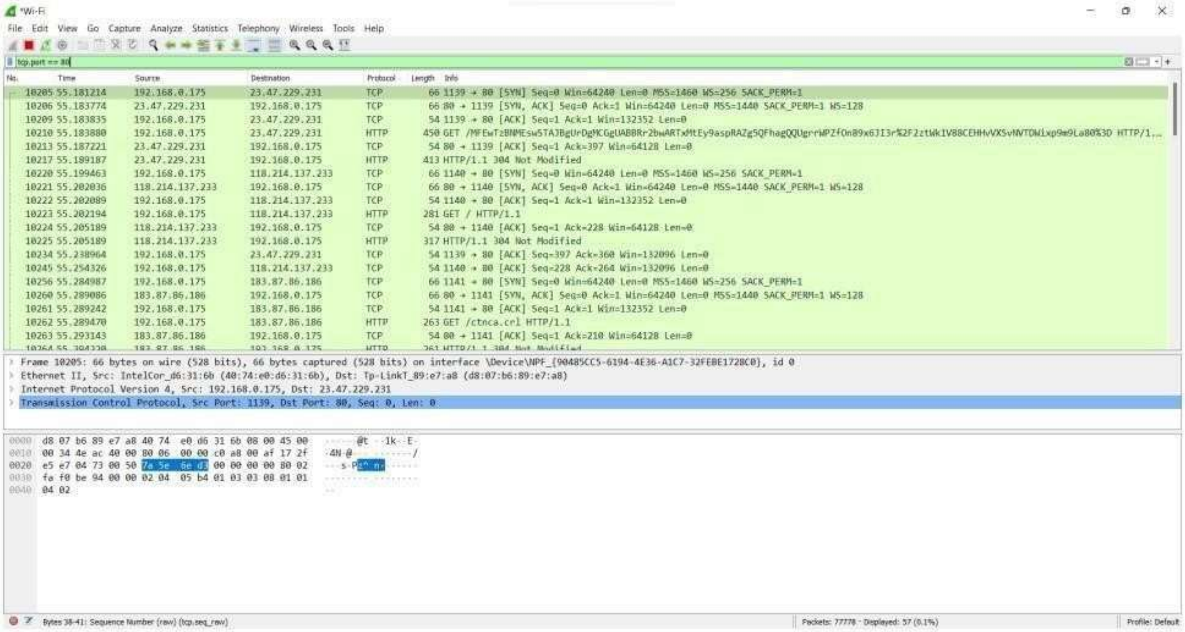
```
No.   Time           Source           Destination      Protocol  Length Info
71609 183.560720     54.37.30.38      192.168.0.175    TCP       1494 2223 → 1137 [PSH, ACK] Seq=32540819 Ack=40091 Win=64128 Len=1440 [TCP segment of a reassembled PDU]
71610 183.561608     54.37.30.38      192.168.0.175    TCP       1494 2223 → 1137 [ACK] Seq=32542259 Ack=40091 Win=64128 Len=1440 [TCP segment of a reassembled PDU]
71611 183.561608     54.37.30.38      192.168.0.175    TLSv1.2   1494 Application Data [TCP segment of a reassembled PDU]
71612 183.561608     54.37.30.38      192.168.0.175    TCP       1494 2223 → 1137 [ACK] Seq=32545139 Ack=40091 Win=64128 Len=1440 [TCP segment of a reassembled PDU]
71613 183.561608     54.37.30.38      192.168.0.175    TCP       1494 2223 → 1137 [PSH, ACK] Seq=32546579 Ack=40091 Win=64128 Len=1440 [TCP segment of a reassembled PDU]
71614 183.561618     192.168.0.175    54.37.30.38      TCP         54 1137 → 2223 [ACK] Seq=40091 Ack=32548019 Win=2119680 Len=0
71615 183.562675     54.37.30.38      192.168.0.175    TLSv1.2   1494 Application Data [TCP segment of a reassembled PDU]
71616 183.562675     54.37.30.38      192.168.0.175    TCP       1494 2223 → 1137 [ACK] Seq=32549459 Ack=40091 Win=64128 Len=1440 [TCP segment of a reassembled PDU]
71617 183.562675     54.37.30.38      192.168.0.175    TCP       1494 2223 → 1137 [ACK] Seq=32550899 Ack=40091 Win=64128 Len=1440 [TCP segment of a reassembled PDU]
71618 183.562675     54.37.30.38      192.168.0.175    TLSv1.2   1494 Application Data [TCP segment of a reassembled PDU]
71619 183.562689     192.168.0.175    54.37.30.38      TCP         54 1137 → 2223 [ACK] Seq=40091 Ack=32553779 Win=2119680 Len=0
71620 183.562866     54.37.30.38      192.168.0.175    TCP       1494 2223 → 1137 [ACK] Seq=32553779 Ack=40091 Win=64128 Len=1440 [TCP segment of a reassembled PDU]
71621 183.562866     54.37.30.38      192.168.0.175    TLSv1.2    674 Application Data
71622 183.562881     192.168.0.175    54.37.30.38      TCP         54 1137 → 2223 [ACK] Seq=40091 Ack=32555839 Win=2119680 Len=0
71637 183.942423     192.168.0.175    172.67.72.209    TCP         55 [TCP Keep-Alive] 1134 → 443 [ACK] Seq=1181 Ack=37347 Win=131584 Len=1
71638 183.948275     172.67.72.209    192.168.0.175    TCP         66 [TCP Keep-Alive ACK] 443 → 1134 [ACK] Seq=37347 Ack=1182 Win=71680 Len=0 SLE=1181 SRE=1182
71644 184.068454     192.168.0.175    193.122.203.139  TLSv1.2   1454 Application Data
71646 184.273264     193.122.203.139  192.168.0.175    TLSv1.2     93 Application Data
71647 184.322728     192.168.0.175    193.122.203.139  TCP         54 53534 → 443 [ACK] Seq=120757 Ack=1431 Win=514 Len=0
```

```
> Frame 1: 1494 bytes on wire (11952 bits), 1494 bytes captured (11952 bits) on interface \Device\NPF_{90485CC5-6194-4E36-A1C7-32FEBE1728C0}, id 0
> Ethernet II, Src: Tp-LinkT_89:e7:a8 (d8:07:b6:89:e7:a8), Dst: IntelCor_d6:31:6b (40:74:e0:d6:31:6b)
> Internet Protocol Version 4, Src: 172.67.7.42, Dst: 192.168.0.175
> Transmission Control Protocol, Src Port: 443, Dst Port: 53989, Seq: 1, Ack: 1, Len: 1440
```

```
0000  40 74 e0 d6 31 6b d8 07  b6 89 e7 a8 08 00 45 00   @t··1k········E·
0010  05 c8 e9 7f 40 00 35 06  e1 eb ac 43 07 2a c0 a8   ····@·5····C·*··
0020  00 af 01 bb d2 e5 9c 19  9e 18 09 8c 44 7c 50 10   ············D|P·
0030  00 f5 5d 0f 00 00 17 03  03 20 1a 21 cc 08 9e f2   ··]······ ·!····
0040  9c e0 a6 0c 81 c1 2e 79  6c 64 86 7c 86 a4 1d b5   ·······yld·|····
0050  2f 9b 66 ec 3c 18 00 60  91 04 28 0e d4 04 7b 5c   /·f·<··`··(···{\
0060  2b 32 91 8b d6 82 87 a4  62 64 08 5c af a3 fc 1f   +2······bd·\····
0070  1d 52 40 4a 28 67 38 4f  b4 0f 99 46 87 45 3c 5d   ·R@J(g8O···F·E<]
0080  94 78 2e 95 10 74 e2 ad  6b a0 ce c0 92 24 f3 32   ·x.··t··k····$·2
0090  f4 78 b1 d0 d3 ea 26 a4  2d d6 82 47 9b a0 a2 84   ·x····&·-··G····
00a0  b8 fe 2c ff e3 23 00 d6  51 59 be 34 64 ed 09 f3   ··,··#··QY·4d···
00b0  da 6d 1d 8d 13 3e 83 2e  58 9c 4c 23 21 cb 33 28   ·m···>·.X·L#!·3(
00c0  85 ee 6f b5 68 c0 63 04  d8 12 1c 3d da 54 e2 29   ··o·h·c····=·T·)
00d0  8a d8 43 ff a0 67 0a 58  63 72 cc 79 8e 12 0a 13   ··C··g·Xcr·y····
```

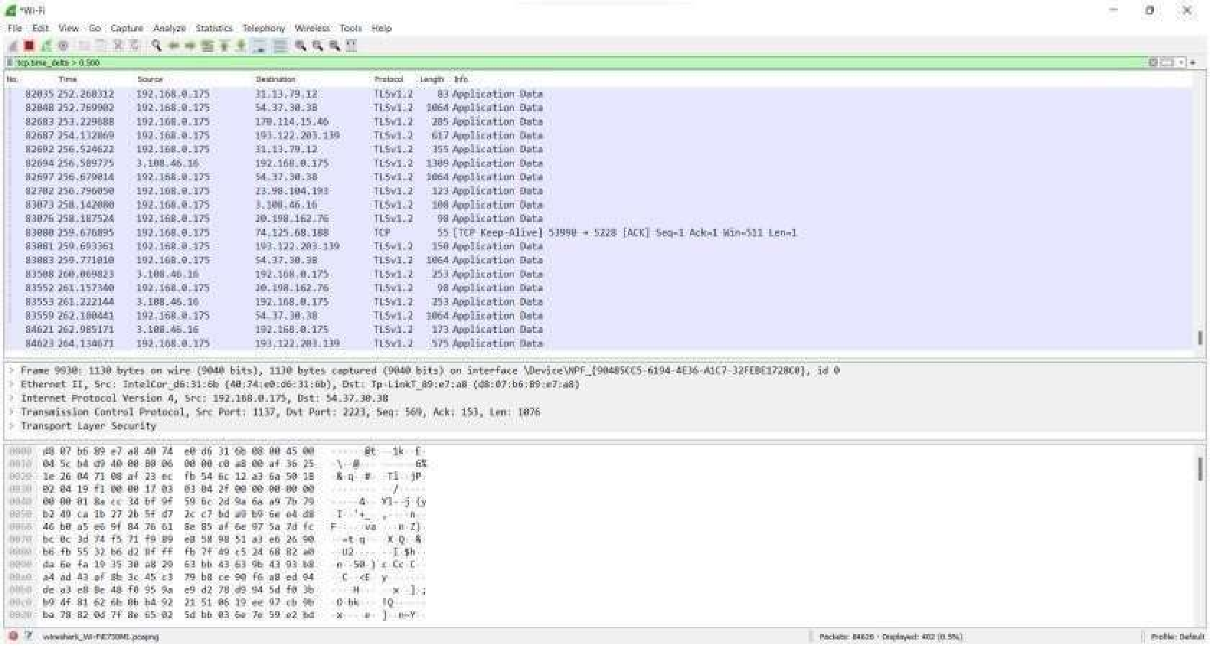
Address Resolution Protocol: Protocol | Packets: 71648 · Displayed: 67100 (93.7%) | Profile: Default

B] Tracing Packets based on filters: 1] Filter Results by Port:
Traces all packets related to Port 80.


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp.port == 80
No.   Time      Source           Destination      Protocol Length Info
10205 55.181214 192.168.0.175    23.47.229.231    TCP       66 1139 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
10206 55.183774 23.47.229.231    192.168.0.175    TCP       66 80 → 1139 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1440 SACK_PERM=1 WS=128
10209 55.183835 192.168.0.175    23.47.229.231    TCP       54 1139 → 80 [ACK] Seq=1 Ack=1 Win=132352 Len=0
10210 55.183880 192.168.0.175    23.47.229.231    HTTP     450 GET /MFEwTzBNMEsw5TAJBgUrDgMCGgUABBRr2bwARTxMtEy9aspRAZg5QFhagQQUgrrWPZfOn89x6JI3r%2F2ztWk1V88CEHHvVXSvNVTDWixp9m9La80%3D HTTP/1…
10213 55.187221 23.47.229.231    192.168.0.175    TCP       54 80 → 1139 [ACK] Seq=1 Ack=397 Win=64128 Len=0
10217 55.189187 23.47.229.231    192.168.0.175    HTTP     413 HTTP/1.1 304 Not Modified
10220 55.199463 192.168.0.175    118.214.137.233  TCP       66 1140 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
10221 55.202036 118.214.137.233  192.168.0.175    TCP       66 80 → 1140 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1440 SACK_PERM=1 WS=128
10222 55.202089 192.168.0.175    118.214.137.233  TCP       54 1140 → 80 [ACK] Seq=1 Ack=1 Win=132352 Len=0
10223 55.202194 192.168.0.175    118.214.137.233  HTTP     281 GET / HTTP/1.1
10224 55.205189 118.214.137.233  192.168.0.175    TCP       54 80 → 1140 [ACK] Seq=1 Ack=228 Win=64128 Len=0
10225 55.205189 118.214.137.233  192.168.0.175    HTTP     317 HTTP/1.1 304 Not Modified
10234 55.238964 192.168.0.175    23.47.229.231    TCP       54 1139 → 80 [ACK] Seq=397 Ack=360 Win=132096 Len=0
10245 55.254326 192.168.0.175    118.214.137.233  TCP       54 1140 → 80 [ACK] Seq=228 Ack=264 Win=132096 Len=0
10256 55.284987 192.168.0.175    183.87.86.186    TCP       66 1141 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
10260 55.289086 183.87.86.186    192.168.0.175    TCP       66 80 → 1141 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1440 SACK_PERM=1 WS=128
10261 55.289242 192.168.0.175    183.87.86.186    TCP       54 1141 → 80 [ACK] Seq=1 Ack=1 Win=132352 Len=0
10262 55.289470 192.168.0.175    183.87.86.186    HTTP     263 GET /ctnca.crl HTTP/1.1
10263 55.293143 183.87.86.186    192.168.0.175    TCP       54 80 → 1141 [ACK] Seq=1 Ack=210 Win=64128 Len=0
10264 55.294120 183.87.86.186    192.168.0.175    HTTP     261 HTTP/1.1 304 Not Modified

> Frame 10205: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{90485CC5-6194-4E36-A1C7-32FEBE1728C0}, id 0
> Ethernet II, Src: IntelCor_d6:31:6b (40:74:e0:d6:31:6b), Dst: Tp-LinkT_89:e7:a8 (d8:07:b6:89:e7:a8)
> Internet Protocol Version 4, Src: 192.168.0.175, Dst: 23.47.229.231
> Transmission Control Protocol, Src Port: 1139, Dst Port: 80, Seq: 0, Len: 0

0000  d8 07 b6 89 e7 a8 40 74  e0 d6 31 6b 08 00 45 00   ······@t ··1k··E·
0010  00 34 4e ac 40 00 80 06  00 00 c0 a8 00 af 17 2f   ·4N·@··· ·······/
0020  e5 e7 04 73 00 50 7a 5e  6e d3 00 00 00 00 80 02   ···s·Pz^ n·······
0030  fa f0 be 94 00 00 02 04  05 b4 01 03 03 08 01 01   ········ ········
0040  04 02                                              ··

Bytes 38-41: Sequence Number (raw) (tcp.seq_raw)    Packets: 77778 · Displayed: 57 (0.1%)    Profile: Default
```

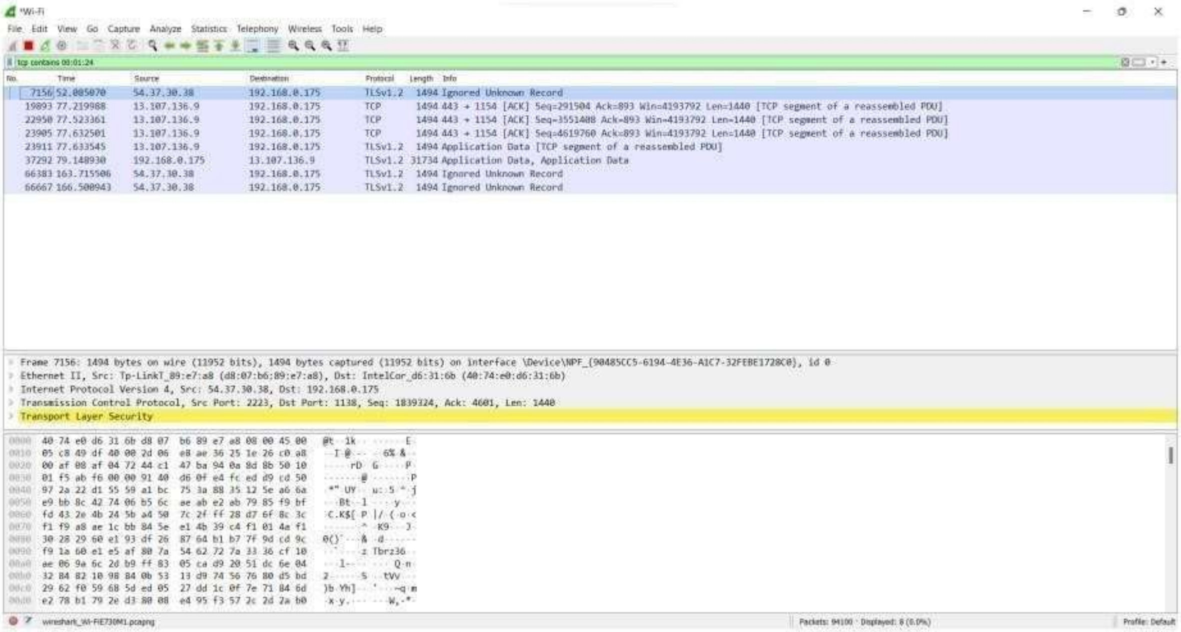
2] Filter by Delta Time :
Displays tcp packets with delta time of greater than 0.500 sec


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp.time_delta > 0.500
No.   Time       Source           Destination      Protocol Length Info
82035 252.268312 192.168.0.175    31.13.79.12      TLSv1.2    83 Application Data
82048 252.769902 192.168.0.175    54.37.30.38      TLSv1.2  1064 Application Data
82683 253.229088 192.168.0.175    170.114.15.46    TLSv1.2   285 Application Data
82687 254.132869 192.168.0.175    193.122.203.130  TLSv1.2   617 Application Data
82692 256.524622 192.168.0.175    31.13.79.12      TLSv1.2   355 Application Data
82694 256.589775 3.108.46.16      192.168.0.175    TLSv1.2  1309 Application Data
82697 256.679814 192.168.0.175    54.37.30.38      TLSv1.2  1064 Application Data
82702 256.796050 192.168.0.175    23.98.104.193    TLSv1.2   123 Application Data
83073 258.142080 192.168.0.175    3.108.46.16      TLSv1.2   108 Application Data
83076 258.187524 192.168.0.175    20.198.162.76    TLSv1.2    98 Application Data
83080 259.676895 192.168.0.175    74.125.68.188    TCP        55 [TCP Keep-Alive] 53990 → 5228 [ACK] Seq=1 Ack=1 Win=511 Len=1
83081 259.693361 192.168.0.175    193.122.203.130  TLSv1.2   150 Application Data
83083 259.771010 192.168.0.175    54.37.30.38      TLSv1.2  1064 Application Data
83508 260.069823 3.108.46.16      192.168.0.175    TLSv1.2   253 Application Data
83552 261.157340 192.168.0.175    20.198.162.76    TLSv1.2    98 Application Data
83553 261.222144 3.108.46.16      192.168.0.175    TLSv1.2   253 Application Data
83559 262.180441 192.168.0.175    54.37.30.38      TLSv1.2  1064 Application Data
84621 262.985171 3.108.46.16      192.168.0.175    TLSv1.2   173 Application Data
84623 264.134671 192.168.0.175    193.122.203.130  TLSv1.2   575 Application Data

> Frame 9930: 1130 bytes on wire (9040 bits), 1130 bytes captured (9040 bits) on interface \Device\NPF_{90485CC5-6194-4E36-A1C7-32FEBE1728C0}, id 0
> Ethernet II, Src: IntelCor_d6:31:6b (40:74:e0:d6:31:6b), Dst: Tp-LinkT_89:e7:a8 (d8:07:b6:89:e7:a8)
> Internet Protocol Version 4, Src: 192.168.0.175, Dst: 54.37.30.38
> Transmission Control Protocol, Src Port: 1137, Dst Port: 2223, Seq: 569, Ack: 153, Len: 1076
> Transport Layer Security

0000  d8 07 b6 89 e7 a8 40 74  e0 d6 31 6b 08 00 45 00   ······@t ··1k··E·
0010  04 5c b4 d9 40 00 80 06  00 00 c0 a8 00 af 36 25   ·\··@··· ······6%
0020  1e 26 04 71 08 af 23 ec  fb 54 6c 12 a3 6a 50 18   ·&·q··#· ·Tl··jP·
0030  02 04 19 f1 00 00 17 03  03 04 2f 00 00 00 00 00   ········ ··/·····
0040  00 00 01 8a cc 34 bf 9f  59 6c 2d 9a 6a a9 7b 79   ·····4·· Yl-·j·{y
0050  b2 49 ca 1b 27 2b 5f d7  2c c7 bd a0 b9 6e e4 d8   ·I··'+_· ,····n··
0060  46 b0 a5 e6 9f 84 76 61  8e 85 af 6e 97 5a 7d fc   F·····va ···n·Z}·
0070  bc 0c 3d 74 f5 71 f9 89  e8 58 98 51 a3 e6 26 90   ··=t·q·· ·X·Q··&·
0080  b6 fb 55 32 b6 d2 8f ff  fb 7f 49 c5 24 68 82 a0   ··U2···· ··I·$h··
0090  da 6e fa 19 35 30 a8 29  63 bb 43 63 9b 43 93 b8   ·n··50·) c·Cc·C··
00a0  a4 ad 43 af 8b 3c 45 c3  79 b8 ce 90 f6 a8 ed 94   ··C··<E· y·······
00b0  de a3 e8 8e 48 f0 95 9a  e9 d2 78 d9 94 5d f0 3b   ····H··· ··x··]·;
00c0  b9 4f 81 62 6b 0b b4 92  21 51 06 19 ee 97 cb 9b   ·O·bk··· !Q······
00d0  ba 78 82 0d 7f 8e 65 02  5d bb 03 6e 7e 59 e2 bd   ·x····e· ]··n~Y··

wireshark_Wi-FiE7S0M1.pcapng    Packets: 84626 · Displayed: 402 (0.5%)    Profile: Default
```

3] Filter by Byte Sequence:

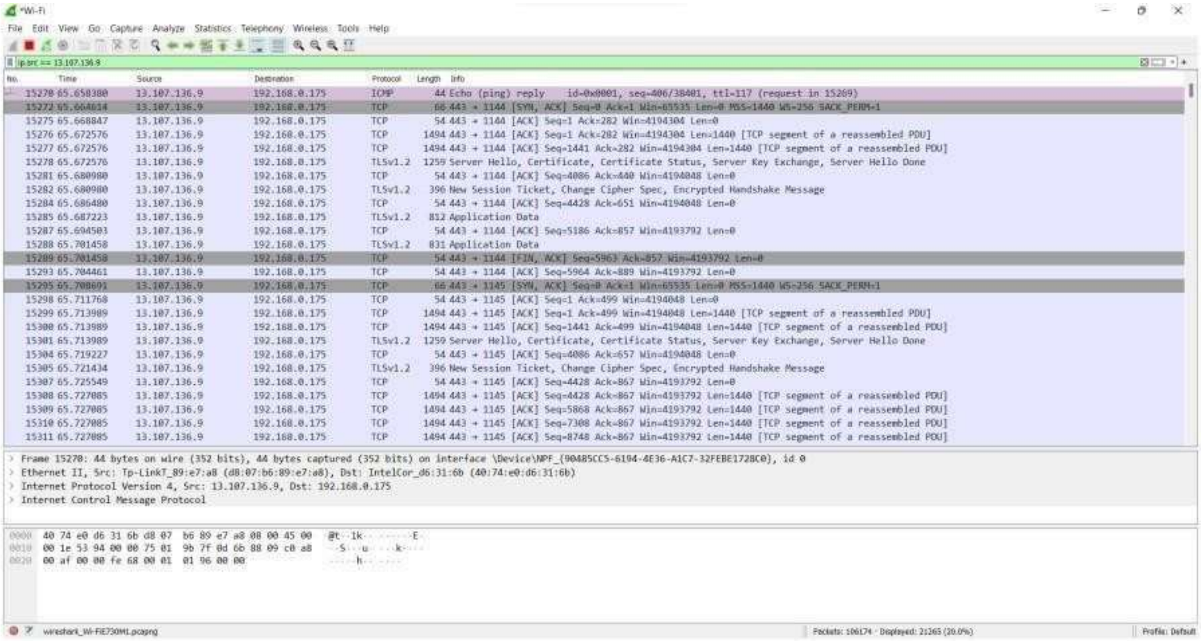
Displays packets which contain a particular byte sequence.


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp contains 00:01:24

No.    Time        Source          Destination     Protocol Length Info
 7156 52.085070   54.37.30.38     192.168.0.175   TLSv1.2  1494 Ignored Unknown Record
19893 77.219988   13.107.136.9    192.168.0.175   TCP      1494 443 → 1154 [ACK] Seq=291504 Ack=893 Win=4193792 Len=1440 [TCP segment of a reassembled PDU]
22950 77.523361   13.107.136.9    192.168.0.175   TCP      1494 443 → 1154 [ACK] Seq=3551408 Ack=893 Win=4193792 Len=1440 [TCP segment of a reassembled PDU]
23905 77.632501   13.107.136.9    192.168.0.175   TCP      1494 443 → 1154 [ACK] Seq=4619760 Ack=893 Win=4193792 Len=1440 [TCP segment of a reassembled PDU]
23911 77.633545   13.107.136.9    192.168.0.175   TLSv1.2  1494 Application Data [TCP segment of a reassembled PDU]
37292 79.148930   192.168.0.175   13.107.136.9    TLSv1.2 31734 Application Data, Application Data
66383 163.715506  54.37.30.38     192.168.0.175   TLSv1.2  1494 Ignored Unknown Record
66667 166.508943  54.37.30.38     192.168.0.175   TLSv1.2  1494 Ignored Unknown Record

> Frame 7156: 1494 bytes on wire (11952 bits), 1494 bytes captured (11952 bits) on interface \Device\NPF_{90485CC5-6194-4E36-A1C7-32FEBE1728C0}, id 0
> Ethernet II, Src: Tp-LinkT_89:e7:a8 (d8:07:b6:89:e7:a8), Dst: IntelCor_d6:31:6b (40:74:e0:d6:31:6b)
> Internet Protocol Version 4, Src: 54.37.30.38, Dst: 192.168.0.175
> Transmission Control Protocol, Src Port: 2223, Dst Port: 1138, Seq: 1839324, Ack: 4601, Len: 1440
> Transport Layer Security

0000  40 74 e0 d6 31 6b d8 07  b6 89 e7 a8 08 00 45 00   @t··1k········E·
0010  05 c8 49 df 40 00 2d 06  e8 ae 36 25 1e 26 c0 a8   ··I·@·-···6%·&··
0020  00 af 08 af 04 72 44 c1  47 ba 94 0a 8d 8b 50 10   ·····rD·G·····P·
0030  01 f5 ab f6 00 00 91 40  d6 0f e4 fc ed d9 cd 50   ·······@·······P
0040  97 2a 22 d1 55 59 a1 bc  75 3a 88 35 12 5e a6 6a   ·*"·UY··u:·5·^·j
0050  e9 bb 8c 42 74 06 b5 6c  ae ab e2 ab 79 85 f9 bf   ···Bt··l····y···
0060  fd 43 2e 4b 24 5b a4 50  7c 2f ff 28 d7 6f 8c 3c   ·C.K$[·P|/·(·o·<
0070  f1 f9 a8 ae 1c bb 84 5e  e1 4b 39 c4 f1 01 4a f1   ·······^·K9···J·
0080  30 28 29 60 e1 93 df 26  87 64 b1 b7 7f 9d cd 9c   0()`···&·d······
0090  f9 1a 60 e1 e5 af 80 7a  54 62 72 7a 33 36 cf 10   ··`····zTbrz36··
00a0  ae 06 9a 6c 2d b9 ff 83  05 ca d9 20 51 dc 6e 04   ···l-······ Q·n·
00b0  32 84 82 10 98 84 0b 53  13 d9 74 56 76 80 d5 bd   2······S··tVv···
00c0  29 62 f0 59 68 5d ed 05  27 dd 1c 0f 7e 71 84 6d   )b·Yh]··'···~q·m
00d0  e2 78 b1 79 2e d3 80 08  e4 95 f3 57 2c 2d 2a b0   ·x·y.······W,-*·

wireshark_Wi-FiE730M1.pcapng          Packets: 94100 · Displayed: 8 (0.0%)          Profile: Default
```

4] Filter by Source IP Address:

Displays packets which have source IP address same as the one provided in the argument.


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.src == 13.107.136.9

No.    Time        Source          Destination     Protocol Length Info
15270 65.658380   13.107.136.9    192.168.0.175   ICMP       44 Echo (ping) reply    id=0x0001, seq=406/38401, ttl=117 (request in 15269)
15272 65.664614   13.107.136.9    192.168.0.175   TCP        66 443 → 1144 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM=1
15275 65.668847   13.107.136.9    192.168.0.175   TCP        54 443 → 1144 [ACK] Seq=1 Ack=282 Win=4194304 Len=0
15276 65.672576   13.107.136.9    192.168.0.175   TCP      1494 443 → 1144 [ACK] Seq=1 Ack=282 Win=4194304 Len=1440 [TCP segment of a reassembled PDU]
15277 65.672576   13.107.136.9    192.168.0.175   TCP      1494 443 → 1144 [ACK] Seq=1441 Ack=282 Win=4194304 Len=1440 [TCP segment of a reassembled PDU]
15278 65.672576   13.107.136.9    192.168.0.175   TLSv1.2  1259 Server Hello, Certificate, Certificate Status, Server Key Exchange, Server Hello Done
15281 65.680980   13.107.136.9    192.168.0.175   TCP        54 443 → 1144 [ACK] Seq=4086 Ack=440 Win=4194048 Len=0
15282 65.680980   13.107.136.9    192.168.0.175   TLSv1.2   396 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
15284 65.686480   13.107.136.9    192.168.0.175   TCP        54 443 → 1144 [ACK] Seq=4428 Ack=651 Win=4194048 Len=0
15285 65.687223   13.107.136.9    192.168.0.175   TLSv1.2   812 Application Data
15287 65.694503   13.107.136.9    192.168.0.175   TCP        54 443 → 1144 [ACK] Seq=5186 Ack=857 Win=4193792 Len=0
15288 65.701458   13.107.136.9    192.168.0.175   TLSv1.2   831 Application Data
15289 65.701458   13.107.136.9    192.168.0.175   TCP        54 443 → 1144 [FIN, ACK] Seq=5963 Ack=857 Win=4193792 Len=0
15293 65.704461   13.107.136.9    192.168.0.175   TCP        54 443 → 1144 [ACK] Seq=5964 Ack=889 Win=4193792 Len=0
15295 65.708691   13.107.136.9    192.168.0.175   TCP        66 443 → 1145 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM=1
15298 65.711768   13.107.136.9    192.168.0.175   TCP        54 443 → 1145 [ACK] Seq=1 Ack=499 Win=4194048 Len=0
15299 65.713989   13.107.136.9    192.168.0.175   TCP      1494 443 → 1145 [ACK] Seq=1 Ack=499 Win=4194048 Len=1440 [TCP segment of a reassembled PDU]
15300 65.713989   13.107.136.9    192.168.0.175   TCP      1494 443 → 1145 [ACK] Seq=1441 Ack=499 Win=4194048 Len=1440 [TCP segment of a reassembled PDU]
15301 65.713989   13.107.136.9    192.168.0.175   TLSv1.2  1259 Server Hello, Certificate, Certificate Status, Server Key Exchange, Server Hello Done
15304 65.719227   13.107.136.9    192.168.0.175   TCP        54 443 → 1145 [ACK] Seq=4086 Ack=657 Win=4194048 Len=0
15305 65.721434   13.107.136.9    192.168.0.175   TLSv1.2   396 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
15307 65.725549   13.107.136.9    192.168.0.175   TCP        54 443 → 1145 [ACK] Seq=4428 Ack=867 Win=4193792 Len=0
15308 65.727085   13.107.136.9    192.168.0.175   TCP      1494 443 → 1145 [ACK] Seq=4428 Ack=867 Win=4193792 Len=1440 [TCP segment of a reassembled PDU]
15309 65.727085   13.107.136.9    192.168.0.175   TCP      1494 443 → 1145 [ACK] Seq=5868 Ack=867 Win=4193792 Len=1440 [TCP segment of a reassembled PDU]
15310 65.727085   13.107.136.9    192.168.0.175   TCP      1494 443 → 1145 [ACK] Seq=7308 Ack=867 Win=4193792 Len=1440 [TCP segment of a reassembled PDU]
15311 65.727085   13.107.136.9    192.168.0.175   TCP      1494 443 → 1145 [ACK] Seq=8748 Ack=867 Win=4193792 Len=1440 [TCP segment of a reassembled PDU]

> Frame 15270: 44 bytes on wire (352 bits), 44 bytes captured (352 bits) on interface \Device\NPF_{90485CC5-6194-4E36-A1C7-32FEBE1728C0}, id 0
> Ethernet II, Src: Tp-LinkT_89:e7:a8 (d8:07:b6:89:e7:a8), Dst: IntelCor_d6:31:6b (40:74:e0:d6:31:6b)
> Internet Protocol Version 4, Src: 13.107.136.9, Dst: 192.168.0.175
> Internet Control Message Protocol

0000  40 74 e0 d6 31 6b d8 07  b6 89 e7 a8 08 00 45 00   @t··1k········E·
0010  00 1e 53 94 00 00 75 01  9b 7f 0d 6b 88 09 c0 a8   ··S···u····k····
0020  00 af 00 00 fe 68 00 01  01 96 00 00               ·····h······

wireshark_Wi-FiE730M1.pcapng          Packets: 106174 · Displayed: 21265 (20.0%)          Profile: Default
```

CONCLUSION: Thus, we have successfully studied packet sniffing tools (Wireshark) and explored how packets can be traced based on different filters