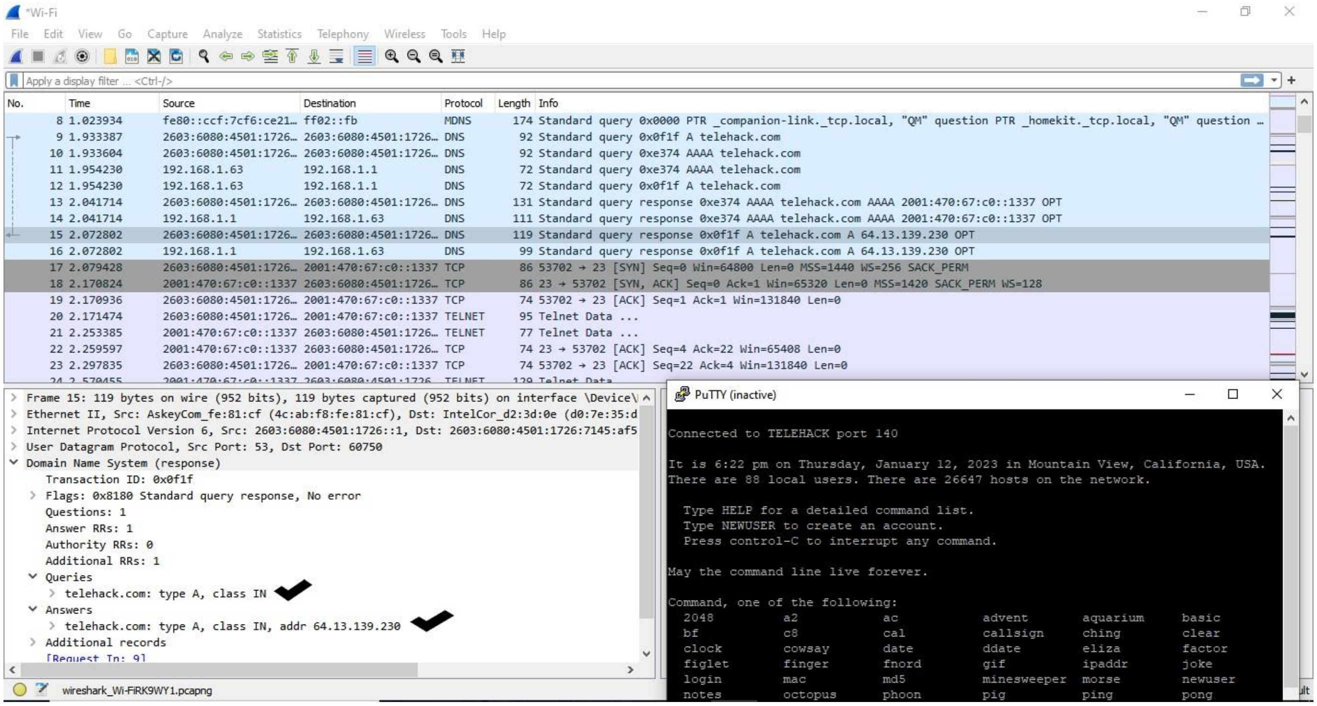
Project-1

1. What are the IP addresses of “telehack.com” and “sdf.org”?

A. The IP Address of **telehack.com is 64.13.139.230**. We can see that clearly in Wireshark. PFB Screenshots of PuTTy and Wireshark for your reference.

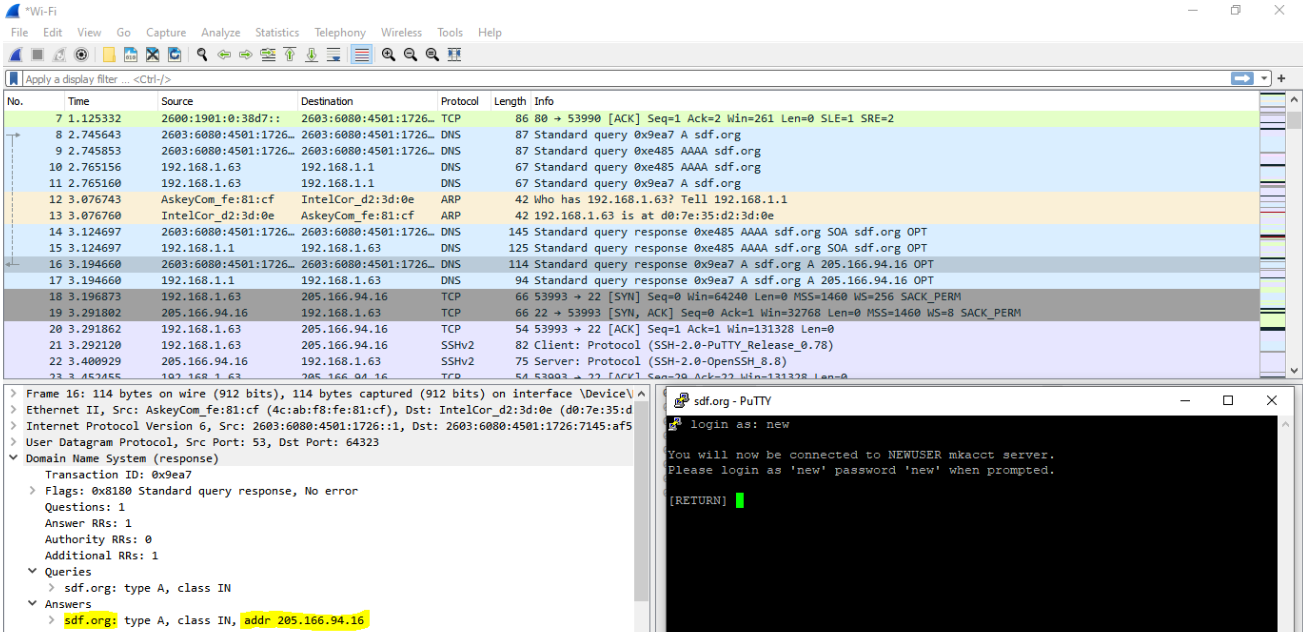

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
8	1.023934	fe80::ccf:7cf6:ce21…	ff02::fb	MDNS	174	Standard query 0x0000 PTR _companion-link._tcp.local, "QM" question PTR _homekit._tcp.local, "QM" question …
9	1.933387	2603:6080:4501:1726…	2603:6080:4501:1726…	DNS	92	Standard query 0x0f1f A telehack.com
10	1.933604	2603:6080:4501:1726…	2603:6080:4501:1726…	DNS	92	Standard query 0xe374 AAAA telehack.com
11	1.954230	192.168.1.63	192.168.1.1	DNS	72	Standard query 0xe374 AAAA telehack.com
12	1.954230	192.168.1.63	192.168.1.1	DNS	72	Standard query 0x0f1f A telehack.com
13	2.041714	2603:6080:4501:1726…	2603:6080:4501:1726…	DNS	131	Standard query response 0xe374 AAAA telehack.com AAAA 2001:470:67:c0::1337 OPT
14	2.041714	192.168.1.1	192.168.1.63	DNS	111	Standard query response 0xe374 AAAA telehack.com AAAA 2001:470:67:c0::1337 OPT
15	2.072802	2603:6080:4501:1726…	2603:6080:4501:1726…	DNS	119	Standard query response 0x0f1f A telehack.com A 64.13.139.230 OPT
16	2.072802	192.168.1.1	192.168.1.63	DNS	99	Standard query response 0x0f1f A telehack.com A 64.13.139.230 OPT
17	2.079428	2603:6080:4501:1726…	2001:470:67:c0::1337	TCP	86	53702 → 23 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM
18	2.170824	2001:470:67:c0::1337	2603:6080:4501:1726…	TCP	86	23 → 53702 [SYN, ACK] Seq=0 Ack=1 Win=65320 Len=0 MSS=1420 SACK_PERM WS=128
19	2.170936	2603:6080:4501:1726…	2001:470:67:c0::1337	TCP	74	53702 → 23 [ACK] Seq=1 Ack=1 Win=131840 Len=0
20	2.171474	2603:6080:4501:1726…	2001:470:67:c0::1337	TELNET	95	Telnet Data ...
21	2.253385	2001:470:67:c0::1337	2603:6080:4501:1726…	TELNET	77	Telnet Data ...
22	2.259597	2001:470:67:c0::1337	2603:6080:4501:1726…	TCP	74	23 → 53702 [ACK] Seq=4 Ack=22 Win=65408 Len=0
23	2.297835	2603:6080:4501:1726…	2001:470:67:c0::1337	TCP	74	53702 → 23 [ACK] Seq=22 Ack=4 Win=131840 Len=0
24	2.570455	2001:470:67:c0::1337	2603:6080:4501:1726	TELNET	129	Telnet Data

```
> Frame 15: 119 bytes on wire (952 bits), 119 bytes captured (952 bits) on interface \Device\
> Ethernet II, Src: AskeyCom_fe:81:cf (4c:ab:f8:fe:81:cf), Dst: IntelCor_d2:3d:0e (d0:7e:35:d
> Internet Protocol Version 6, Src: 2603:6080:4501:1726::1, Dst: 2603:6080:4501:1726:7145:af5
> User Datagram Protocol, Src Port: 53, Dst Port: 60750
v Domain Name System (response)
    Transaction ID: 0x0f1f
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 1
  v Queries
    > telehack.com: type A, class IN ✓
  v Answers
    > telehack.com: type A, class IN, addr 64.13.139.230 ✓
  > Additional records
    [Request In: 9]
```

```
Connected to TELEHACK port 140

It is 6:22 pm on Thursday, January 12, 2023 in Mountain View, California, USA.
There are 88 local users. There are 26647 hosts on the network.

  Type HELP for a detailed command list.
  Type NEWUSER to create an account.
  Press control-C to interrupt any command.

May the command line live forever.

Command, one of the following:
  2048         a2           ac           advent       aquarium     basic
  bf           c8           cal          callsign     ching        clear
  clock        cowsay       date         ddate        eliza        factor
  figlet       finger       fnord        gif          ipaddr       joke
  login        mac          md5          minesweeper  morse        newuser
  notes        octopus      phoon        pig          ping         pong
```

The IP Address of **<u>sdf.org is 205.166.94.16</u>**. We can see that clearly in Wireshark. PFB Screenshots of PuTTy and Wireshark for your reference


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
sdf.org - PuTTY

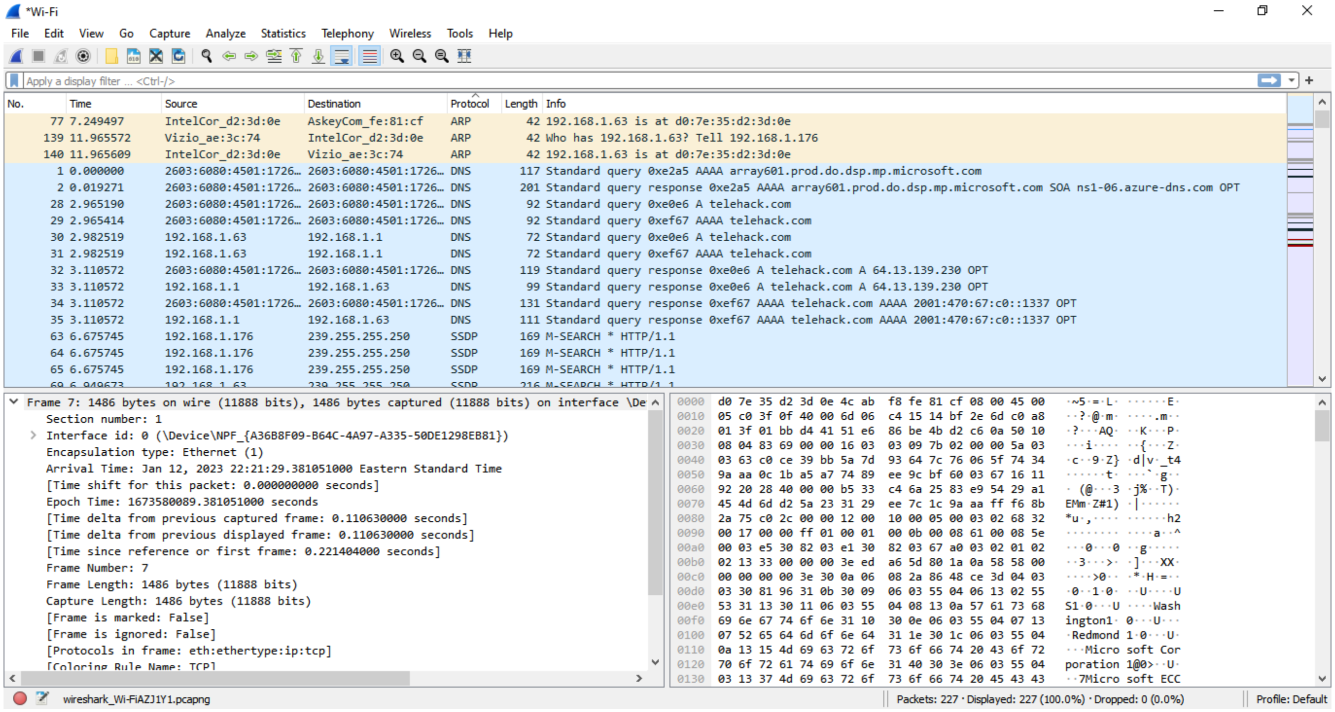
```
No.   Time      Source                 Destination            Protocol Length Info
    7 1.125332  2600:1901:0:38d7::     2603:6080:4501:1726…  TCP      86 80 → 53990 [ACK] Seq=1 Ack=2 Win=261 Len=0 SLE=1 SRE=2
    8 2.745643  2603:6080:4501:1726…  2603:6080:4501:1726…  DNS      87 Standard query 0x9ea7 A sdf.org
    9 2.745853  2603:6080:4501:1726…  2603:6080:4501:1726…  DNS      87 Standard query 0xe485 AAAA sdf.org
   10 2.765156  192.168.1.63           192.168.1.1            DNS      67 Standard query 0xe485 AAAA sdf.org
   11 2.765160  192.168.1.63           192.168.1.1            DNS      67 Standard query 0x9ea7 A sdf.org
   12 3.076743  AskeyCom_fe:81:cf      IntelCor_d2:3d:0e      ARP      42 Who has 192.168.1.63? Tell 192.168.1.1
   13 3.076760  IntelCor_d2:3d:0e      AskeyCom_fe:81:cf      ARP      42 192.168.1.63 is at d0:7e:35:d2:3d:0e
   14 3.124697  2603:6080:4501:1726…  2603:6080:4501:1726…  DNS     145 Standard query response 0xe485 AAAA sdf.org SOA sdf.org OPT
   15 3.124697  192.168.1.1            192.168.1.63           DNS     125 Standard query response 0xe485 AAAA sdf.org SOA sdf.org OPT
   16 3.194660  2603:6080:4501:1726…  2603:6080:4501:1726…  DNS     114 Standard query response 0x9ea7 A sdf.org A 205.166.94.16 OPT
   17 3.194660  192.168.1.1            192.168.1.63           DNS      94 Standard query response 0x9ea7 A sdf.org A 205.166.94.16 OPT
   18 3.196873  192.168.1.63           205.166.94.16          TCP      66 53993 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
   19 3.291802  205.166.94.16          192.168.1.63           TCP      66 22 → 53993 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460 WS=8 SACK_PERM
   20 3.291862  192.168.1.63           205.166.94.16          TCP      54 53993 → 22 [ACK] Seq=1 Ack=1 Win=131328 Len=0
   21 3.292120  192.168.1.63           205.166.94.16          SSHv2    82 Client: Protocol (SSH-2.0-PuTTY_Release_0.78)
   22 3.400929  205.166.94.16          192.168.1.63           SSHv2    75 Server: Protocol (SSH-2.0-OpenSSH_8.8)
   23 3.452455  192.168.1.63           205.166.94.16          TCP      54 53993 → 22 [ACK] Seq=29 Ack=22 Win=131328 Len=0
```

```
> Frame 16: 114 bytes on wire (912 bits), 114 bytes captured (912 bits) on interface \Device\
> Ethernet II, Src: AskeyCom_fe:81:cf (4c:ab:f8:fe:81:cf), Dst: IntelCor_d2:3d:0e (d0:7e:35:d
> Internet Protocol Version 6, Src: 2603:6080:4501:1726::1, Dst: 2603:6080:4501:1726:7145:af5
> User Datagram Protocol, Src Port: 53, Dst Port: 64323
v Domain Name System (response)
    Transaction ID: 0x9ea7
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 1
  v Queries
    > sdf.org: type A, class IN
  v Answers
    > sdf.org: type A, class IN, addr 205.166.94.16
```

```
login as: new

You will now be connected to NEWUSER mkacct server.
Please login as 'new' password 'new' when prompted.

[RETURN]
```

2. Screenshots of the packet dump for the TELNET operation and the SSH operation. Please choose the packets with relatively large size so that we can see the data contents.

<u>TELNET Packet Dump</u>.


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

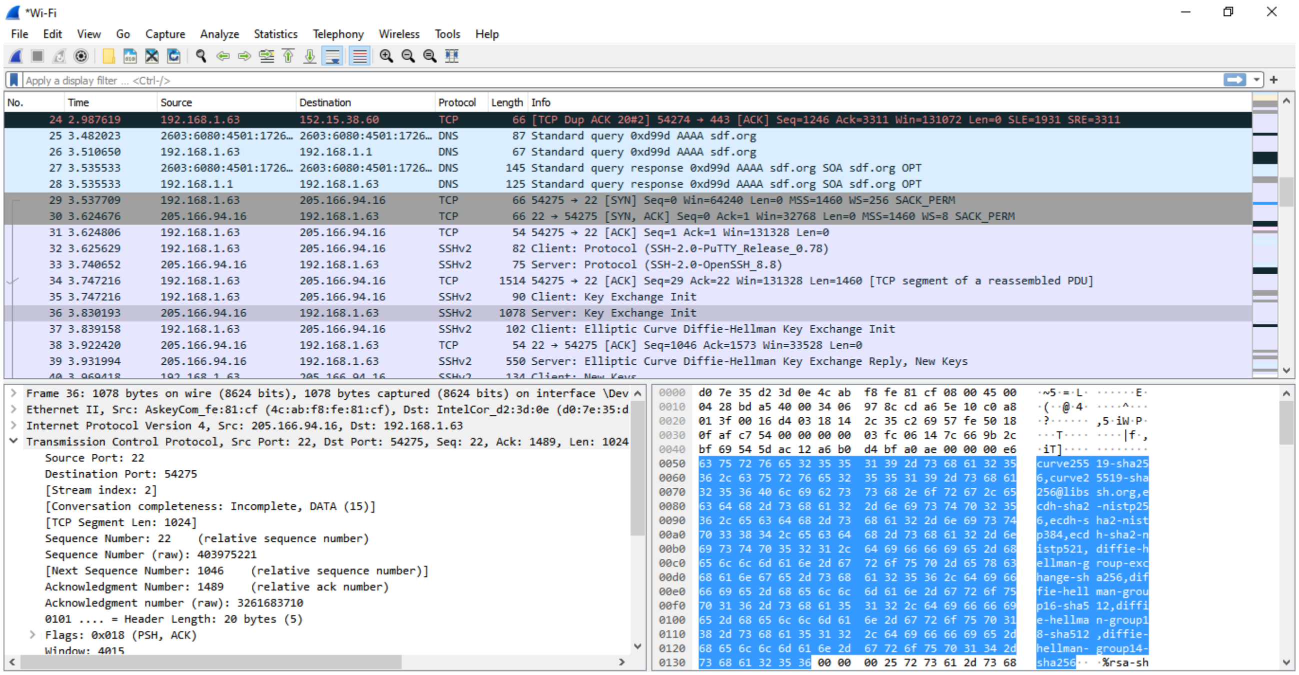
```
No.   Time       Source                 Destination            Protocol Length Info
   77 7.249497   IntelCor_d2:3d:0e      AskeyCom_fe:81:cf      ARP      42 192.168.1.63 is at d0:7e:35:d2:3d:0e
  139 11.965572  Vizio_ae:3c:74         IntelCor_d2:3d:0e      ARP      42 Who has 192.168.1.63? Tell 192.168.1.176
  140 11.965609  IntelCor_d2:3d:0e      Vizio_ae:3c:74         ARP      42 192.168.1.63 is at d0:7e:35:d2:3d:0e
    1 0.000000   2603:6080:4501:1726…  2603:6080:4501:1726…  DNS     117 Standard query 0xe2a5 AAAA array601.prod.do.dsp.mp.microsoft.com
    2 0.019271   2603:6080:4501:1726…  2603:6080:4501:1726…  DNS     201 Standard query response 0xe2a5 AAAA array601.prod.do.dsp.mp.microsoft.com SOA ns1-06.azure-dns.com OPT
   28 2.965190   2603:6080:4501:1726…  2603:6080:4501:1726…  DNS      92 Standard query 0xe0e6 A telehack.com
   29 2.965414   2603:6080:4501:1726…  2603:6080:4501:1726…  DNS      92 Standard query 0xef67 AAAA telehack.com
   30 2.982519   192.168.1.63           192.168.1.1            DNS      72 Standard query 0xe0e6 A telehack.com
   31 2.982519   192.168.1.63           192.168.1.1            DNS      72 Standard query 0xef67 AAAA telehack.com
   32 3.110572   2603:6080:4501:1726…  2603:6080:4501:1726…  DNS     119 Standard query response 0xe0e6 A telehack.com A 64.13.139.230 OPT
   33 3.110572   192.168.1.1            192.168.1.63           DNS      99 Standard query response 0xe0e6 A telehack.com A 64.13.139.230 OPT
   34 3.110572   2603:6080:4501:1726…  2603:6080:4501:1726…  DNS     131 Standard query response 0xef67 AAAA telehack.com AAAA 2001:470:67:c0::1337 OPT
   35 3.110572   192.168.1.1            192.168.1.63           DNS     111 Standard query response 0xef67 AAAA telehack.com AAAA 2001:470:67:c0::1337 OPT
   63 6.675745   192.168.1.176          239.255.255.250        SSDP    169 M-SEARCH * HTTP/1.1
   64 6.675745   192.168.1.176          239.255.255.250        SSDP    169 M-SEARCH * HTTP/1.1
   65 6.675745   192.168.1.176          239.255.255.250        SSDP    169 M-SEARCH * HTTP/1.1
   69 6.949673   192.168.1.63           239.255.255.250        SSDP    216 M-SEARCH * HTTP/1.1
```

```
v Frame 7: 1486 bytes on wire (11888 bits), 1486 bytes captured (11888 bits) on interface \De
    Section number: 1
  > Interface id: 0 (\Device\NPF_{A36B8F09-B64C-4A97-A335-50DE1298EB81})
    Encapsulation type: Ethernet (1)
    Arrival Time: Jan 12, 2023 22:21:29.381051000 Eastern Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1673580089.381051000 seconds
    [Time delta from previous captured frame: 0.110630000 seconds]
    [Time delta from previous displayed frame: 0.110630000 seconds]
    [Time since reference or first frame: 0.221404000 seconds]
    Frame Number: 7
    Frame Length: 1486 bytes (11888 bits)
    Capture Length: 1486 bytes (11888 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp]
    [Coloring Rule Name: TCP]
```

```
0000  d0 7e 35 d2 3d 0e 4c ab  f8 fe 81 cf 08 00 45 00   ·~5·=·L· ······E·
0010  05 c0 3f 0f 40 00 6d 06  c4 15 14 bf 2e 6d c0 a8   ··?·@·m· ····.m··
0020  01 3f 01 bb d4 41 51 e6  86 be 4b d2 c6 0a 50 10   ·?···AQ· ··K···P·
0030  08 04 83 69 00 00 16 03  03 09 7b 02 00 00 5a 03   ···i···· ··{···Z·
0040  03 63 c0 ce 39 bb 5a 7d  93 64 7c 76 06 5f 74 34   ·c··9·Z} ·d|v·_t4
0050  9a aa 0c 1b a5 a7 74 89  ee 9c bf 60 03 67 16 11   ······t· ···`·g··
0060  92 20 28 40 00 00 b5 33  c4 6a 25 83 e9 54 29 a1   · (@···3 ·j%··T)·
0070  45 4d 6d d2 5a 23 31 29  ee 7c 1c 9a aa ff f6 8b   EMm·Z#1) ·|······
0080  2a 75 c0 2c 00 00 12 00  10 00 05 00 03 02 68 32   *u·,···· ······h2
0090  00 17 00 00 ff 01 00 01  00 0b 00 08 61 00 08 5e   ········ ····a··^
00a0  00 03 e5 30 82 03 e1 30  82 03 67 a0 03 02 01 02   ···0···0 ··g·····
00b0  02 13 33 00 00 00 3e ed  a6 5d 80 1a 0a 58 58 00   ··3···>· ·]···XX·
00c0  00 00 00 00 3e 30 0a 06  08 2a 86 48 ce 3d 04 03   ····>0·· ·*·H·=··
00d0  03 30 81 96 31 0b 30 09  06 03 55 04 06 13 02 55   ·0··1·0· ··U····U
00e0  53 31 13 30 11 06 03 55  04 08 13 0a 57 61 73 68   S1·0···U ····Wash
00f0  69 6e 67 74 6f 6e 31 10  30 0e 06 03 55 04 07 13   ington1· 0···U···
0100  07 52 65 64 6d 6f 6e 64  31 1e 30 1c 06 03 55 04   ·Redmond 1·0···U·
0110  0a 13 15 4d 69 63 72 6f  73 6f 66 74 20 43 6f 72   ···Micro soft Cor
0120  70 6f 72 61 74 69 6f 6e  31 40 30 3e 06 03 55 04   poration 1@0>··U·
0130  03 13 37 4d 69 63 72 6f  73 6f 66 74 20 45 43 43   ··7Micro soft ECC
```

```
wireshark_Wi-FiAZJ1Y1.pcapng    Packets: 227 · Displayed: 227 (100.0%) · Dropped: 0 (0.0%)    Profile: Default
```

SSH Packet Dump.



*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

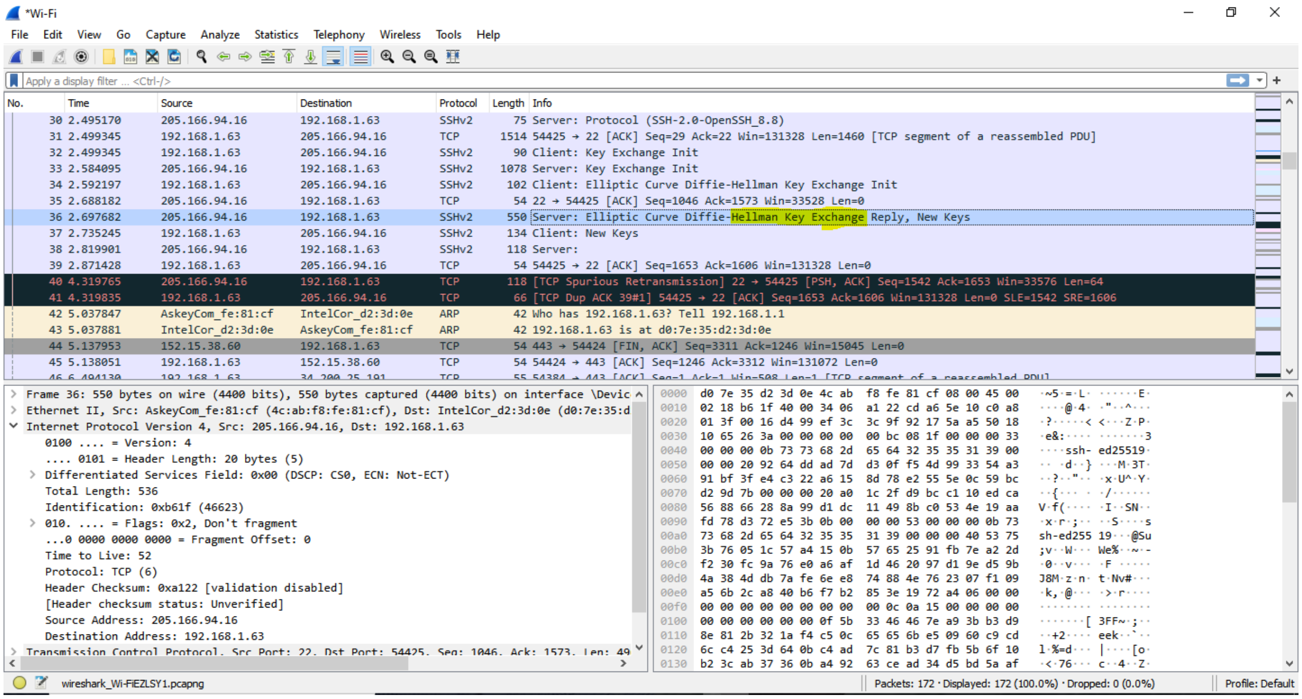
```
No.   Time      Source                Destination           Protocol Length Info
   24 2.987619  192.168.1.63          152.15.38.60          TCP        66 [TCP Dup ACK 20#2] 54274 → 443 [ACK] Seq=1246 Ack=3311 Win=131072 Len=0 SLE=1931 SRE=3311
   25 3.482023  2603:6080:4501:1726…  2603:6080:4501:1726…  DNS        87 Standard query 0xd99d AAAA sdf.org
   26 3.510650  192.168.1.63          192.168.1.1           DNS        67 Standard query 0xd99d AAAA sdf.org
   27 3.535533  2603:6080:4501:1726…  2603:6080:4501:1726…  DNS       145 Standard query response 0xd99d AAAA sdf.org SOA sdf.org OPT
   28 3.535533  192.168.1.1           192.168.1.63          DNS       125 Standard query response 0xd99d AAAA sdf.org SOA sdf.org OPT
   29 3.537709  192.168.1.63          205.166.94.16         TCP        66 54275 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
   30 3.624676  205.166.94.16         192.168.1.63          TCP        66 22 → 54275 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460 WS=8 SACK_PERM
   31 3.624806  192.168.1.63          205.166.94.16         TCP        54 54275 → 22 [ACK] Seq=1 Ack=1 Win=131328 Len=0
   32 3.625629  192.168.1.63          205.166.94.16         SSHv2      82 Client: Protocol (SSH-2.0-PuTTY_Release_0.78)
   33 3.740652  205.166.94.16         192.168.1.63          SSHv2      75 Server: Protocol (SSH-2.0-OpenSSH_8.8)
   34 3.747216  192.168.1.63          205.166.94.16         TCP      1514 54275 → 22 [ACK] Seq=29 Ack=22 Win=131328 Len=1460 [TCP segment of a reassembled PDU]
   35 3.747216  192.168.1.63          205.166.94.16         SSHv2      90 Client: Key Exchange Init
   36 3.830193  205.166.94.16         192.168.1.63          SSHv2    1078 Server: Key Exchange Init
   37 3.839158  192.168.1.63          205.166.94.16         SSHv2     102 Client: Elliptic Curve Diffie-Hellman Key Exchange Init
   38 3.922420  205.166.94.16         192.168.1.63          TCP        54 22 → 54275 [ACK] Seq=1046 Ack=1573 Win=33528 Len=0
   39 3.931994  205.166.94.16         192.168.1.63          SSHv2     550 Server: Elliptic Curve Diffie-Hellman Key Exchange Reply, New Keys
   40 3.969418  192.168.1.63          205.166.94.16         SSHv2     134 Client: New Keys
```

```
> Frame 36: 1078 bytes on wire (8624 bits), 1078 bytes captured (8624 bits) on interface \Dev
> Ethernet II, Src: AskeyCom_fe:81:cf (4c:ab:f8:fe:81:cf), Dst: IntelCor_d2:3d:0e (d0:7e:35:d
> Internet Protocol Version 4, Src: 205.166.94.16, Dst: 192.168.1.63
v Transmission Control Protocol, Src Port: 22, Dst Port: 54275, Seq: 22, Ack: 1489, Len: 1024
    Source Port: 22
    Destination Port: 54275
    [Stream index: 2]
    [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 1024]
    Sequence Number: 22    (relative sequence number)
    Sequence Number (raw): 403975221
    [Next Sequence Number: 1046    (relative sequence number)]
    Acknowledgment Number: 1489    (relative ack number)
    Acknowledgment number (raw): 3261683710
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window: 4015
```

```
0000  d0 7e 35 d2 3d 0e 4c ab  f8 fe 81 cf 08 00 45 00   ·~5·=·L· ······E·
0010  04 28 bd a5 40 00 34 06  97 8c cd a6 5e 10 c0 a8   ·(··@·4· ····^···
0020  01 3f 00 16 d4 03 18 14  2c 35 c2 69 57 fe 50 18   ·?······ ,5·iW·P·
0030  0f af c7 54 00 00 00 00  03 fc 06 14 7c 66 9b 2c   ···T···· ····|f·,
0040  bf 69 54 5d ac 12 a6 b0  d4 bf a0 ae 00 00 00 e6   ·iT]···· ········
0050  63 75 72 76 65 32 35 35  31 39 2d 73 68 61 32 35   curve255 19-sha25
0060  36 2c 63 75 72 76 65 32  35 35 31 39 2d 73 68 61   6,curve2 5519-sha
0070  32 35 36 40 6c 69 62 73  73 68 2e 6f 72 67 2c 65   256@libs sh.org,e
0080  63 64 68 2d 73 68 61 32  2d 6e 69 73 74 70 32 35   cdh-sha2 -nistp25
0090  36 2c 65 63 64 68 2d 73  68 61 32 2d 6e 69 73 74   6,ecdh-s ha2-nist
00a0  70 33 38 34 2c 65 63 64  68 2d 73 68 61 32 2d 6e   p384,ecd h-sha2-n
00b0  69 73 74 70 35 32 31 2c  64 69 66 66 69 65 2d 68   istp521, diffie-h
00c0  65 6c 6c 6d 61 6e 2d 67  72 6f 75 70 2d 65 78 63   ellman-g roup-exc
00d0  68 61 6e 67 65 2d 73 68  61 32 35 36 2c 64 69 66   hange-sh a256,dif
00e0  66 69 65 2d 68 65 6c 6c  6d 61 6e 2d 67 72 6f 75   fie-hell man-grou
00f0  70 31 36 2d 73 68 61 35  31 32 2c 64 69 66 66 69   p16-sha5 12,diffi
0100  65 2d 68 65 6c 6c 6d 61  6e 2d 67 72 6f 75 70 31   e-hellma n-group1
0110  38 2d 73 68 61 35 31 32  2c 64 69 66 66 69 65 2d   8-sha512 ,diffie-
0120  68 65 6c 6c 6d 61 6e 2d  67 72 6f 75 70 31 34 2d   hellman- group14-
0130  73 68 61 32 35 36 00 00  00 25 72 73 61 2d 73 68   sha256·· ·%rsa-sh
```

3. which protocol does PuTTY use to establish encryption key with the SSH server?

As we can in the below screenshot by using puTTY SSH, Algorithm used is **Elliptic Curve Diffie-Hellman Key Exchange.**



*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.   Time      Source             Destination        Protocol Length Info
   30 2.495170  205.166.94.16      192.168.1.63       SSHv2      75 Server: Protocol (SSH-2.0-OpenSSH_8.8)
   31 2.499345  192.168.1.63       205.166.94.16      TCP      1514 54425 → 22 [ACK] Seq=29 Ack=22 Win=131328 Len=1460 [TCP segment of a reassembled PDU]
   32 2.499345  192.168.1.63       205.166.94.16      SSHv2      90 Client: Key Exchange Init
   33 2.584095  205.166.94.16      192.168.1.63       SSHv2    1078 Server: Key Exchange Init
   34 2.592197  192.168.1.63       205.166.94.16      SSHv2     102 Client: Elliptic Curve Diffie-Hellman Key Exchange Init
   35 2.688182  205.166.94.16      192.168.1.63       TCP        54 22 → 54425 [ACK] Seq=1046 Ack=1573 Win=33528 Len=0
   36 2.697682  205.166.94.16      192.168.1.63       SSHv2     550 Server: Elliptic Curve Diffie-Hellman Key Exchange Reply, New Keys
   37 2.735245  192.168.1.63       205.166.94.16      SSHv2     134 Client: New Keys
   38 2.819901  205.166.94.16      192.168.1.63       SSHv2     118 Server:
   39 2.871428  192.168.1.63       205.166.94.16      TCP        54 54425 → 22 [ACK] Seq=1653 Ack=1606 Win=131328 Len=0
   40 4.319765  205.166.94.16      192.168.1.63       TCP       118 [TCP Spurious Retransmission] 22 → 54425 [PSH, ACK] Seq=1542 Ack=1653 Win=33576 Len=64
   41 4.319835  192.168.1.63       205.166.94.16      TCP        66 [TCP Dup ACK 39#1] 54425 → 22 [ACK] Seq=1653 Ack=1606 Win=131328 Len=0 SLE=1542 SRE=1606
   42 5.037847  AskeyCom_fe:81:cf  IntelCor_d2:3d:0e  ARP        42 Who has 192.168.1.63? Tell 192.168.1.1
   43 5.037881  IntelCor_d2:3d:0e  AskeyCom_fe:81:cf  ARP        42 192.168.1.63 is at d0:7e:35:d2:3d:0e
   44 5.137953  152.15.38.60       192.168.1.63       TCP        54 443 → 54424 [FIN, ACK] Seq=3311 Ack=1246 Win=15045 Len=0
   45 5.138051  192.168.1.63       152.15.38.60       TCP        54 54424 → 443 [ACK] Seq=1246 Ack=3312 Win=131072 Len=0
   46 6.494130  192.168.1.63       34.200.25.191      TCP        55 54384 → 443 [ACK] Seq=1 Ack=1 Win=508 Len=1 [TCP segment of a reassembled PDU]
```

```
> Frame 36: 550 bytes on wire (4400 bits), 550 bytes captured (4400 bits) on interface \Devic
> Ethernet II, Src: AskeyCom_fe:81:cf (4c:ab:f8:fe:81:cf), Dst: IntelCor_d2:3d:0e (d0:7e:35:d
v Internet Protocol Version 4, Src: 205.166.94.16, Dst: 192.168.1.63
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 536
    Identification: 0xb61f (46623)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 52
    Protocol: TCP (6)
    Header Checksum: 0xa122 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 205.166.94.16
    Destination Address: 192.168.1.63
> Transmission Control Protocol, Src Port: 22, Dst Port: 54425, Seq: 1046, Ack: 1573, Len: 49
```

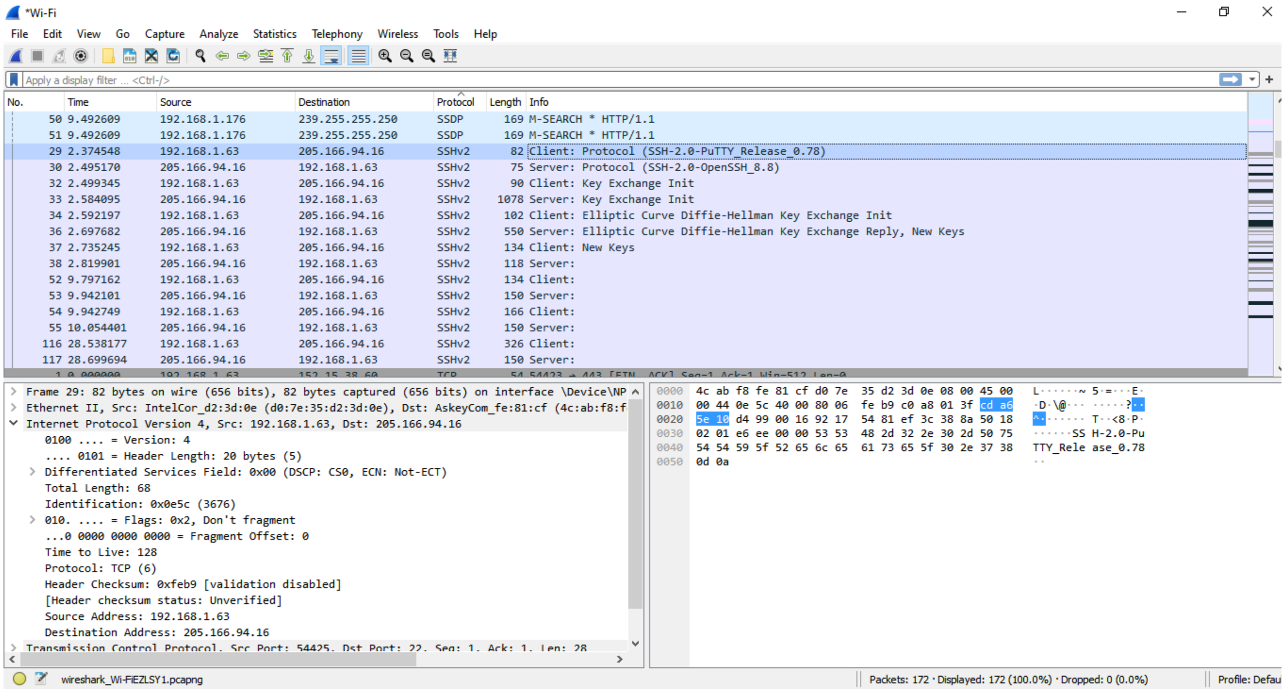
```
0000  d0 7e 35 d2 3d 0e 4c ab  f8 fe 81 cf 08 00 45 00   ·~5·=·L· ······E·
0010  02 18 b6 1f 40 00 34 06  a1 22 cd a6 5e 10 c0 a8   ····@·4· ·"··^···
0020  01 3f 00 16 d4 99 ef 3c  3c 9f 92 17 5a a5 50 18   ·?·····< <···Z·P·
0030  10 65 26 3a 00 00 00 00  00 bc 08 1f 00 00 00 33   ·e&:···· ·······3
0040  00 00 00 0b 73 73 68 2d  65 64 32 35 35 31 39 00   ····ssh- ed25519·
0050  00 00 20 92 64 dd ad 7d  d3 0f f5 4d 99 33 54 a3   ·· ·d··} ···M·3T·
0060  91 bf 3f e4 c3 22 a6 15  8d 78 e2 55 5e 0c 59 bc   ··?··"·· ·x·U^·Y·
0070  d2 9d 7b 00 00 00 20 a0  1c 2f d9 bc c1 10 ed ca   ··{··· · ·/······
0080  56 88 66 28 8a 99 d1 dc  11 49 8b c0 53 4e 19 aa   V·f(···· ·I··SN··
0090  fd 78 d3 72 e5 3b 0b 00  00 00 53 00 00 00 0b 73   ·x·r·;·· ··S····s
00a0  73 68 2d 65 64 32 35 35  31 39 00 00 00 40 53 75   sh-ed255 19···@Su
00b0  3b 76 05 1c 57 a4 15 0b  57 65 25 91 fb 7e a2 2d   ;v··W··· We%··~·-
00c0  f2 30 fc 9a 76 e0 a6 af  1d 46 20 97 d1 9e d5 9b   ·0··v··· ·F ·····
00d0  4a 38 4d db 7a fe 6e e8  74 88 4e 76 23 07 f1 09   J8M·z·n· t·Nv#···
00e0  a5 6b 2c a8 40 b6 f7 b2  85 3e 19 72 a4 06 00 00   ·k,·@··· ·>·r····
00f0  00 00 00 00 00 00 00 00  00 0c 0a 15 00 00 00 00   ········ ········
0100  00 00 00 00 00 00 0f 5b  33 46 46 7e a9 3b b3 d9   ·······[ 3FF~·;··
0110  8e 81 2b 32 1a f4 c5 0c  65 65 6b e5 09 60 c9 cd   ··+2···· eek··`··
0120  6c c4 25 3d 64 0b c4 ad  7c 81 b3 d7 fb 5b 6f 10   l·%=d··· |····[o·
0130  b2 3c ab 37 36 0b a4 92  63 ce ad 34 d5 bd 5a af   ·<·76··· c··4··Z·
```

Packets: 172 · Displayed: 172 (100.0%) · Dropped: 0 (0.0%)

Profile: Default

4. Analysis – packet dump out and explain why SSH is more secure than TELNET.

As per the Analysis from the TELNET and SSH, SSH Uses Encryption which means all data transferred on the network is protected from eavesdropping which makes it hard to decrypt. Data sent into the internet using this protocol will be out of confidentiality. SSH Protocol uses public key encryption for authentication.


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.     Time       Source           Destination       Protocol  Length Info
     50 9.492609   192.168.1.176    239.255.255.250   SSDP      169 M-SEARCH * HTTP/1.1
     51 9.492609   192.168.1.176    239.255.255.250   SSDP      169 M-SEARCH * HTTP/1.1
     29 2.374548   192.168.1.63     205.166.94.16     SSHv2      82 Client: Protocol (SSH-2.0-PuTTY_Release_0.78)
     30 2.495170   205.166.94.16    192.168.1.63      SSHv2      75 Server: Protocol (SSH-2.0-OpenSSH_8.8)
     32 2.499345   192.168.1.63     205.166.94.16     SSHv2      90 Client: Key Exchange Init
     33 2.584095   205.166.94.16    192.168.1.63      SSHv2    1078 Server: Key Exchange Init
     34 2.592197   192.168.1.63     205.166.94.16     SSHv2     102 Client: Elliptic Curve Diffie-Hellman Key Exchange Init
     36 2.697682   205.166.94.16    192.168.1.63      SSHv2     550 Server: Elliptic Curve Diffie-Hellman Key Exchange Reply, New Keys
     37 2.735245   192.168.1.63     205.166.94.16     SSHv2     134 Client: New Keys
     38 2.819901   205.166.94.16    192.168.1.63      SSHv2     118 Server:
     52 9.797162   192.168.1.63     205.166.94.16     SSHv2     134 Client:
     53 9.942101   205.166.94.16    192.168.1.63      SSHv2     150 Server:
     54 9.942749   192.168.1.63     205.166.94.16     SSHv2     166 Client:
     55 10.054401  205.166.94.16    192.168.1.63      SSHv2     150 Server:
    116 28.538177  192.168.1.63     205.166.94.16     SSHv2     326 Client:
    117 28.699694  205.166.94.16    192.168.1.63      SSHv2     150 Server:
      1 0.000000   192.168.1.63     152.15.38.60      TCP        54 54423 → 443 [FIN, ACK] Seq=1 Ack=1 Win=512 Len=0
```

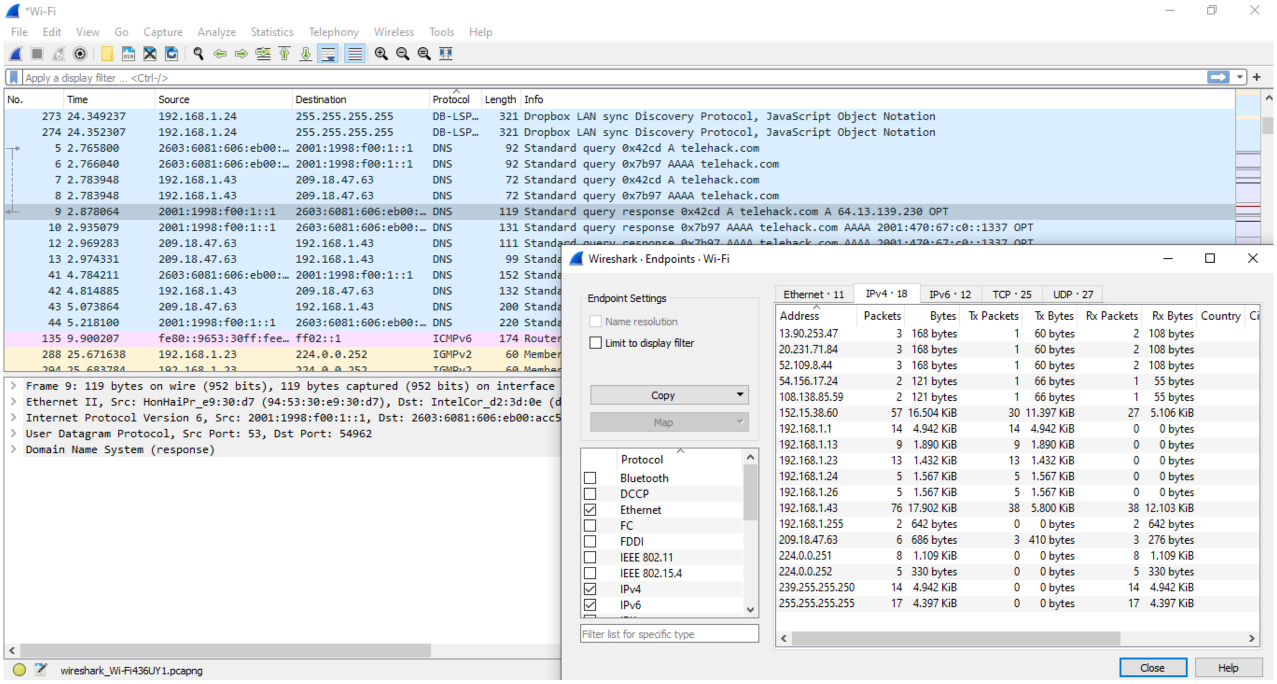
```
> Frame 29: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface \Device\NP
> Ethernet II, Src: IntelCor_d2:3d:0e (d0:7e:35:d2:3d:0e), Dst: AskeyCom_fe:81:cf (4c:ab:f8:f
v Internet Protocol Version 4, Src: 192.168.1.63, Dst: 205.166.94.16
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 68
    Identification: 0x0e5c (3676)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0xfeb9 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.63
    Destination Address: 205.166.94.16
> Transmission Control Protocol, Src Port: 54425, Dst Port: 22, Seq: 1, Ack: 1, Len: 28
```

```
0000  4c ab f8 fe 81 cf d0 7e  35 d2 3d 0e 08 00 45 00   L······~ 5·=···E·
0010  00 44 0e 5c 40 00 80 06  fe b9 c0 a8 01 3f cd a6   ·D·\@··· ·····?··
0020  5e 10 d4 99 00 16 92 17  54 81 ef 3c 38 8a 50 18   ^······· T··<8·P·
0030  02 01 e6 ee 00 00 53 53  48 2d 32 2e 30 2d 50 75   ······SS H-2.0-Pu
0040  54 54 59 5f 52 65 6c 65  61 73 65 5f 30 2e 37 38   TTY_Rele ase_0.78
0050  0d 0a                                              ··
```

```
wireshark_Wi-FiEZLSY1.pcapng    Packets: 172 · Displayed: 172 (100.0%) · Dropped: 0 (0.0%)    Profile: Defau
```

5. IP Addresses in Captured Packets

- **List all different IP addresses that you see in these captured packets:**


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.   Time       Source                Destination           Protocol Length Info
  273 24.349237  192.168.1.24          255.255.255.255       DB-LSP…    321 Dropbox LAN sync Discovery Protocol, JavaScript Object Notation
  274 24.352307  192.168.1.24          255.255.255.255       DB-LSP…    321 Dropbox LAN sync Discovery Protocol, JavaScript Object Notation
    5 2.765800   2603:6081:606:eb00:… 2001:1998:f00:1::1     DNS         92 Standard query 0x42cd A telehack.com
    6 2.766040   2603:6081:606:eb00:… 2001:1998:f00:1::1     DNS         92 Standard query 0x7b97 AAAA telehack.com
    7 2.783948   192.168.1.43          209.18.47.63          DNS         72 Standard query 0x42cd A telehack.com
    8 2.783948   192.168.1.43          209.18.47.63          DNS         72 Standard query 0x7b97 AAAA telehack.com
    9 2.878064   2001:1998:f00:1::1    2603:6081:606:eb00:… DNS        119 Standard query response 0x42cd A telehack.com A 64.13.139.230 OPT
   10 2.935079   2001:1998:f00:1::1    2603:6081:606:eb00:… DNS        131 Standard query response 0x7b97 AAAA telehack.com AAAA 2001:470:67:c0::1337 OPT
   12 2.969283   209.18.47.63          192.168.1.43          DNS        111 Standard query response 0x7b97 AAAA telehack.com AAAA 2001:470:67:c0::1337 OPT
   13 2.974331   209.18.47.63          192.168.1.43          DNS         99 Standa
   41 4.784211   2603:6081:606:eb00:… 2001:1998:f00:1::1     DNS        152 Standa
   42 4.814885   192.168.1.43          209.18.47.63          DNS        132 Standa
   43 5.073864   209.18.47.63          192.168.1.43          DNS        200 Standa
   44 5.218100   2001:1998:f00:1::1    2603:6081:606:eb00:… DNS        220 Standa
  135 9.900207   fe80::9653:30ff:fee…  ff02::1               ICMPv6     174 Router
  288 25.671638  192.168.1.23          224.0.0.252           IGMPv2      60 Member
  294 25.683784  192.168.1.23          224.0.0.252           IGMPv2      60 Member

> Frame 9: 119 bytes on wire (952 bits), 119 bytes captured (952 bits) on interface
> Ethernet II, Src: HonHaiPr_e9:30:d7 (94:53:30:e9:30:d7), Dst: IntelCor_d2:3d:0e (d
> Internet Protocol Version 6, Src: 2001:1998:f00:1::1, Dst: 2603:6081:606:eb00:acc5
> User Datagram Protocol, Src Port: 53, Dst Port: 54962
> Domain Name System (response)
```

wireshark_Wi-Fi436UY1.pcapng

Wireshark · Endpoints · Wi-Fi

Endpoint Settings

□ Name resolution
□ Limit to display filter

Copy ▾ Map

Protocol
□ Bluetooth
□ DCCP
☑ Ethernet
□ FC
□ FDDI
□ IEEE 802.11
□ IEEE 802.15.4
☑ IPv4
☑ IPv6

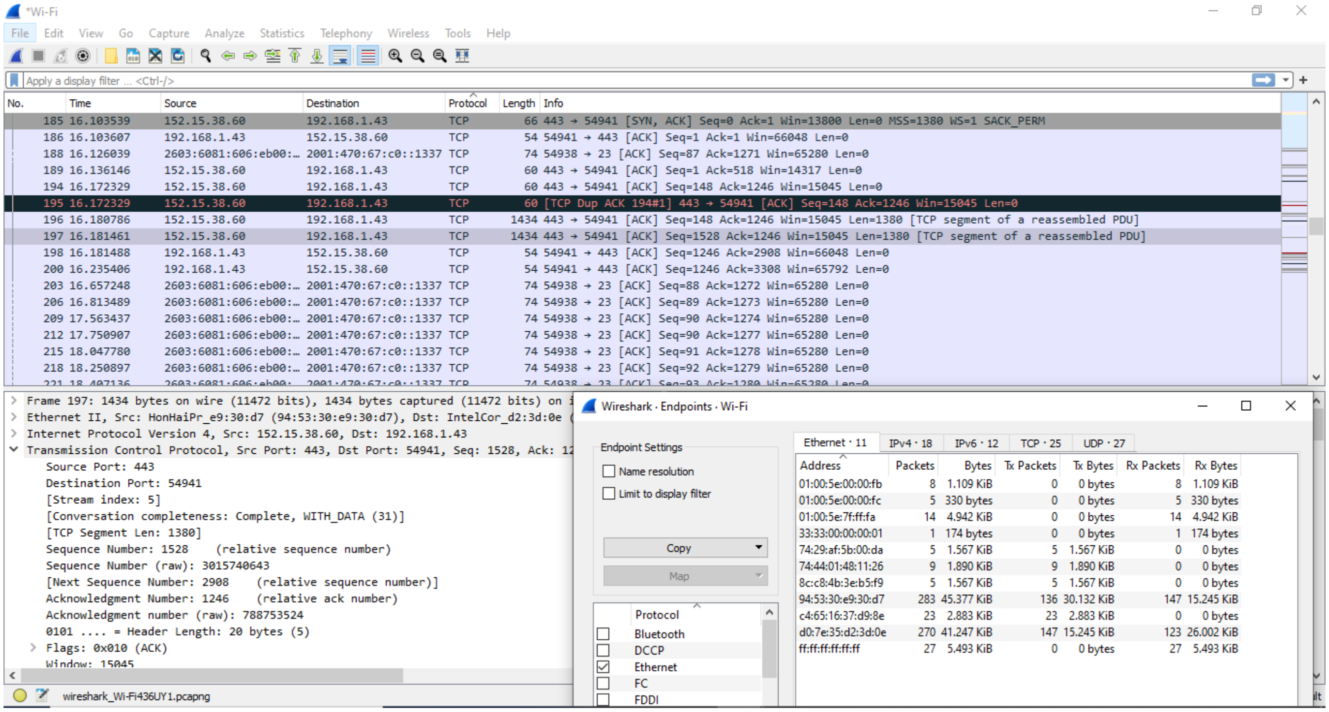
Filter list for specific type

Ethernet · 11 | IPv4 · 18 | IPv6 · 12 | TCP · 25 | UDP · 27

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	Ci
13.90.253.47	3	168 bytes	1	60 bytes	2	108 bytes		
20.231.71.84	3	168 bytes	1	60 bytes	2	108 bytes		
52.109.8.44	3	168 bytes	1	60 bytes	2	108 bytes		
54.156.17.24	2	121 bytes	1	66 bytes	1	55 bytes		
108.138.85.59	2	121 bytes	1	66 bytes	1	55 bytes		
152.15.38.60	57	16.504 KiB	30	11.397 KiB	27	5.106 KiB		
192.168.1.1	14	4.942 KiB	14	4.942 KiB	0	0 bytes		
192.168.1.13	9	1.890 KiB	9	1.890 KiB	0	0 bytes		
192.168.1.23	13	1.432 KiB	13	1.432 KiB	0	0 bytes		
192.168.1.24	5	1.567 KiB	5	1.567 KiB	0	0 bytes		
192.168.1.26	5	1.567 KiB	5	1.567 KiB	0	0 bytes		
192.168.1.43	76	17.902 KiB	38	5.800 KiB	38	12.103 KiB		
192.168.1.255	2	642 bytes	0	0 bytes	2	642 bytes		
209.18.47.63	6	686 bytes	3	410 bytes	3	276 bytes		
224.0.0.251	8	1.109 KiB	0	0 bytes	8	1.109 KiB		
224.0.0.252	5	330 bytes	0	0 bytes	5	330 bytes		
239.255.255.250	14	4.942 KiB	0	0 bytes	14	4.942 KiB		
255.255.255.255	17	4.397 KiB	0	0 bytes	17	4.397 KiB		

Close Help

❖ **List all the MAC addresses that you see in these captured packets**


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.   Time       Source                Destination           Protocol Length Info
  185 16.103539  152.15.38.60          192.168.1.43          TCP        66 443 → 54941 [SYN, ACK] Seq=0 Ack=1 Win=13800 Len=0 MSS=1380 WS=1 SACK_PERM
  186 16.103607  192.168.1.43          152.15.38.60          TCP        54 54941 → 443 [ACK] Seq=1 Ack=1 Win=66048 Len=0
  188 16.126039  2603:6081:606:eb00:… 2001:470:67:c0::1337  TCP        74 54938 → 23 [ACK] Seq=87 Ack=1271 Win=65280 Len=0
  189 16.136146  152.15.38.60          192.168.1.43          TCP        60 443 → 54941 [ACK] Seq=1 Ack=518 Win=14317 Len=0
  194 16.172329  152.15.38.60          192.168.1.43          TCP        60 443 → 54941 [ACK] Seq=148 Ack=1246 Win=15045 Len=0
  195 16.172329  152.15.38.60          192.168.1.43          TCP        60 [TCP Dup ACK 194#1] 443 → 54941 [ACK] Seq=148 Ack=1246 Win=15045 Len=0
  196 16.180786  152.15.38.60          192.168.1.43          TCP      1434 443 → 54941 [ACK] Seq=148 Ack=1246 Win=15045 Len=1380 [TCP segment of a reassembled PDU]
  197 16.181461  152.15.38.60          192.168.1.43          TCP      1434 443 → 54941 [ACK] Seq=1528 Ack=1246 Win=15045 Len=1380 [TCP segment of a reassembled PDU]
  198 16.181488  192.168.1.43          152.15.38.60          TCP        54 54941 → 443 [ACK] Seq=1246 Ack=2908 Win=66048 Len=0
  200 16.235406  192.168.1.43          152.15.38.60          TCP        54 54941 → 443 [ACK] Seq=1246 Ack=3308 Win=65792 Len=0
  203 16.657248  2603:6081:606:eb00:… 2001:470:67:c0::1337  TCP        74 54938 → 23 [ACK] Seq=88 Ack=1272 Win=65280 Len=0
  206 16.813489  2603:6081:606:eb00:… 2001:470:67:c0::1337  TCP        74 54938 → 23 [ACK] Seq=89 Ack=1273 Win=65280 Len=0
  209 17.563437  2603:6081:606:eb00:… 2001:470:67:c0::1337  TCP        74 54938 → 23 [ACK] Seq=90 Ack=1274 Win=65280 Len=0
  212 17.750907  2603:6081:606:eb00:… 2001:470:67:c0::1337  TCP        74 54938 → 23 [ACK] Seq=90 Ack=1277 Win=65280 Len=0
  215 18.047780  2603:6081:606:eb00:… 2001:470:67:c0::1337  TCP        74 54938 → 23 [ACK] Seq=91 Ack=1278 Win=65280 Len=0
  218 18.250897  2603:6081:606:eb00:… 2001:470:67:c0::1337  TCP        74 54938 → 23 [ACK] Seq=92 Ack=1279 Win=65280 Len=0
  221 18.407136  2603:6081:606:eb00:… 2001:470:67:c0::1337  TCP        74 54938 → 23 [ACK] Seq=93 Ack=1280 Win=65280 Len=0

> Frame 197: 1434 bytes on wire (11472 bits), 1434 bytes captured (11472 bits) on i
> Ethernet II, Src: HonHaiPr_e9:30:d7 (94:53:30:e9:30:d7), Dst: IntelCor_d2:3d:0e (
> Internet Protocol Version 4, Src: 152.15.38.60, Dst: 192.168.1.43
v Transmission Control Protocol, Src Port: 443, Dst Port: 54941, Seq: 1528, Ack: 12
    Source Port: 443
    Destination Port: 54941
    [Stream index: 5]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 1380]
    Sequence Number: 1528    (relative sequence number)
    Sequence Number (raw): 3015740643
    [Next Sequence Number: 2908    (relative sequence number)]
    Acknowledgment Number: 1246    (relative ack number)
    Acknowledgment number (raw): 788753524
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x010 (ACK)
    Window: 15045
```

wireshark_Wi-Fi436UY1.pcapng

Wireshark · Endpoints · Wi-Fi

Endpoint Settings

□ Name resolution
□ Limit to display filter

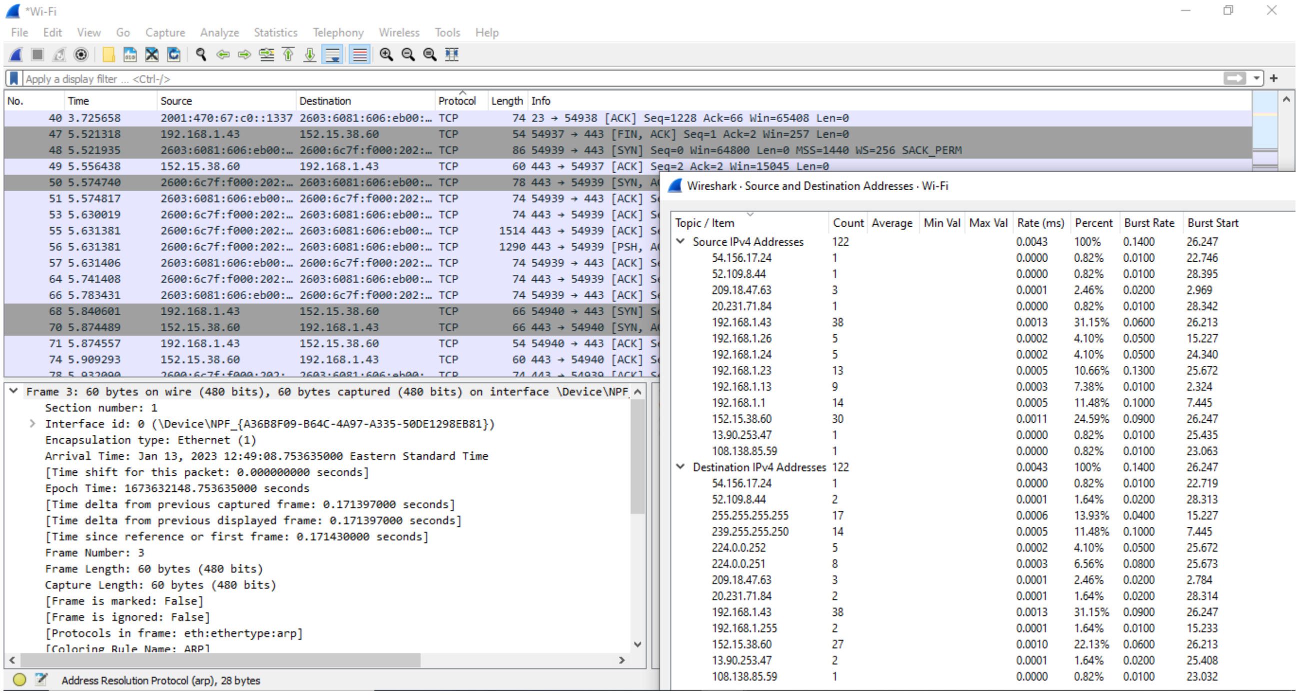
Copy ▾ Map

Protocol
□ Bluetooth
□ DCCP
☑ Ethernet
□ FC
□ FDDI

Ethernet · 11 | IPv4 · 18 | IPv6 · 12 | TCP · 25 | UDP · 27

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
01:00:5e:00:00:fb	8	1.109 KiB	0	0 bytes	8	1.109 KiB
01:00:5e:00:00:fc	5	330 bytes	0	0 bytes	5	330 bytes
01:00:5e:7f:ff:fa	14	4.942 KiB	0	0 bytes	14	4.942 KiB
33:33:00:00:00:01	1	174 bytes	0	0 bytes	1	174 bytes
74:29:af:5b:00:da	5	1.567 KiB	5	1.567 KiB	0	0 bytes
74:44:01:48:11:26	9	1.890 KiB	9	1.890 KiB	0	0 bytes
8c:c8:4b:3e:b5:f9	5	1.567 KiB	5	1.567 KiB	0	0 bytes
94:53:30:e9:30:d7	283	45.377 KiB	136	30.132 KiB	147	15.245 KiB
c4:65:16:37:d9:8e	23	2.883 KiB	23	2.883 KiB	0	0 bytes
d0:7e:35:d2:3d:0e	270	41.247 KiB	147	15.245 KiB	123	26.002 KiB
ff:ff:ff:ff:ff:ff	27	5.493 KiB	0	0 bytes	27	5.493 KiB

- **List all TCP connections between the IP addresses that you capture. Please note that for a TCP connection, you need to provide (Source IP, Source PORT, Destination IP, Destination PORT)**


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

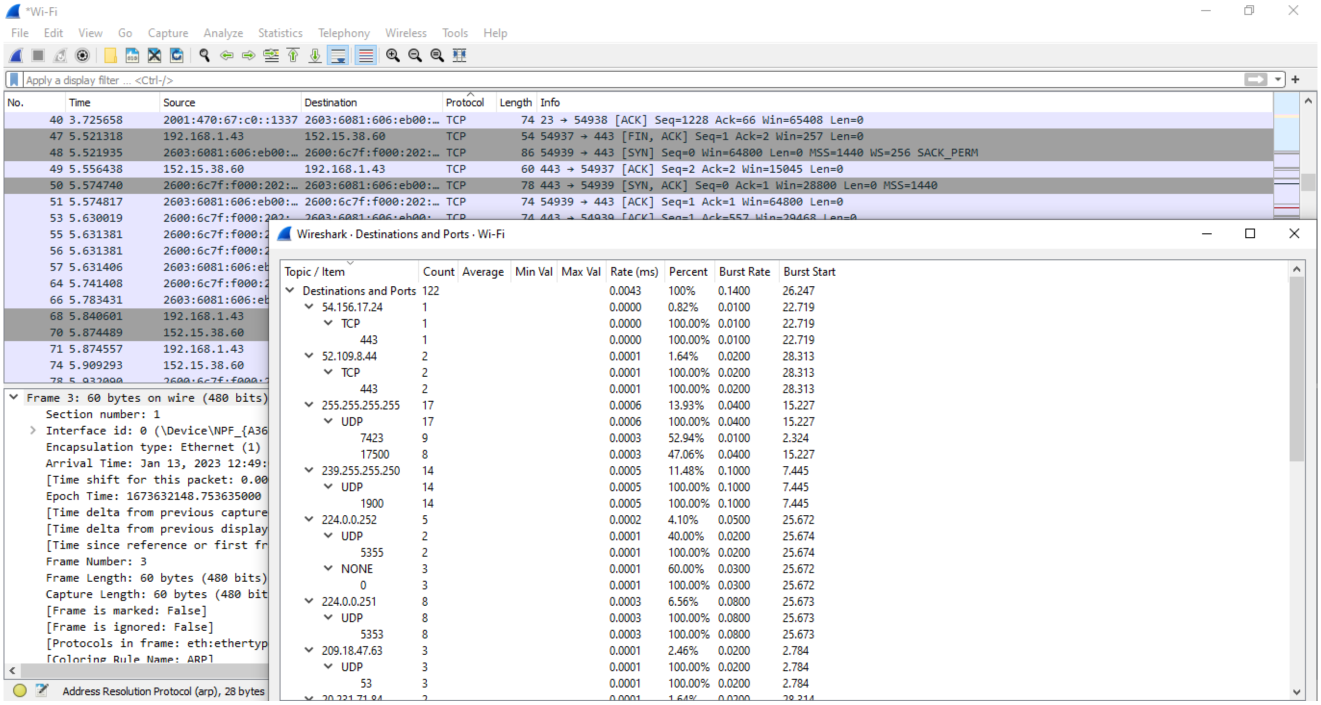
```
No.   Time      Source                 Destination            Protocol Length Info
   40 3.725658  2001:470:67:c0::1337   2603:6081:606:eb00:…   TCP        74 23 → 54938 [ACK] Seq=1228 Ack=66 Win=65408 Len=0
   47 5.521318  192.168.1.43           152.15.38.60           TCP        54 54937 → 443 [FIN, ACK] Seq=1 Ack=2 Win=257 Len=0
   48 5.521935  2603:6081:606:eb00:…   2600:6c7f:f000:202:…   TCP        86 54939 → 443 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM
   49 5.556438  152.15.38.60           192.168.1.43           TCP        60 443 → 54937 [ACK] Seq=2 Ack=2 Win=15045 Len=0
   50 5.574740  2600:6c7f:f000:202:…   2603:6081:606:eb00:…   TCP        78 443 → 54939 [SYN, A
   51 5.574817  2603:6081:606:eb00:…   2600:6c7f:f000:202:…   TCP        74 54939 → 443 [ACK] S
   53 5.630019  2600:6c7f:f000:202:…   2603:6081:606:eb00:…   TCP        74 443 → 54939 [ACK] S
   55 5.631381  2600:6c7f:f000:202:…   2603:6081:606:eb00:…   TCP      1514 443 → 54939 [ACK] S
   56 5.631381  2600:6c7f:f000:202:…   2603:6081:606:eb00:…   TCP      1290 443 → 54939 [PSH, A
   57 5.631406  2603:6081:606:eb00:…   2600:6c7f:f000:202:…   TCP        74 54939 → 443 [ACK] S
   64 5.741408  2600:6c7f:f000:202:…   2603:6081:606:eb00:…   TCP        74 443 → 54939 [ACK] S
   66 5.783431  2603:6081:606:eb00:…   2600:6c7f:f000:202:…   TCP        74 54939 → 443 [ACK] S
   68 5.840601  192.168.1.43           152.15.38.60           TCP        66 54940 → 443 [SYN] S
   70 5.874489  152.15.38.60           192.168.1.43           TCP        66 443 → 54940 [SYN, A
   71 5.874557  192.168.1.43           152.15.38.60           TCP        54 54940 → 443 [ACK] S
   74 5.909293  152.15.38.60           192.168.1.43           TCP        60 443 → 54940 [ACK] S
   78 5.932090  2600:6c7f:f000:202:    2603:6081:606:eb00:    TCP        74 443 → 54939 [ACK] S
```

```
∨ Frame 3: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_
    Section number: 1
  > Interface id: 0 (\Device\NPF_{A36B8F09-B64C-4A97-A335-50DE1298EB81})
    Encapsulation type: Ethernet (1)
    Arrival Time: Jan 13, 2023 12:49:08.753635000 Eastern Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1673632148.753635000 seconds
    [Time delta from previous captured frame: 0.171397000 seconds]
    [Time delta from previous displayed frame: 0.171397000 seconds]
    [Time since reference or first frame: 0.171430000 seconds]
    Frame Number: 3
    Frame Length: 60 bytes (480 bits)
    Capture Length: 60 bytes (480 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:arp]
    [Coloring Rule Name: ARP]
```

Address Resolution Protocol (arp), 28 bytes

Wireshark · Source and Destination Addresses · Wi-Fi

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
∨ Source IPv4 Addresses	122				0.0043	100%	0.1400	26.247
54.156.17.24	1				0.0000	0.82%	0.0100	22.746
52.109.8.44	1				0.0000	0.82%	0.0100	28.395
209.18.47.63	3				0.0001	2.46%	0.0200	2.969
20.231.71.84	1				0.0000	0.82%	0.0100	28.342
192.168.1.43	38				0.0013	31.15%	0.0600	26.213
192.168.1.26	5				0.0002	4.10%	0.0500	15.227
192.168.1.24	5				0.0002	4.10%	0.0500	24.340
192.168.1.23	13				0.0005	10.66%	0.1300	25.672
192.168.1.13	9				0.0003	7.38%	0.0100	2.324
192.168.1.1	14				0.0005	11.48%	0.1000	7.445
152.15.38.60	30				0.0011	24.59%	0.0900	26.247
13.90.253.47	1				0.0000	0.82%	0.0100	25.435
108.138.85.59	1				0.0000	0.82%	0.0100	23.063
∨ Destination IPv4 Addresses	122				0.0043	100%	0.1400	26.247
54.156.17.24	1				0.0000	0.82%	0.0100	22.719
52.109.8.44	2				0.0001	1.64%	0.0200	28.313
255.255.255.255	17				0.0006	13.93%	0.0400	15.227
239.255.255.250	14				0.0005	11.48%	0.1000	7.445
224.0.0.252	5				0.0002	4.10%	0.0500	25.672
224.0.0.251	8				0.0003	6.56%	0.0800	25.673
209.18.47.63	3				0.0001	2.46%	0.0200	2.784
20.231.71.84	2				0.0001	1.64%	0.0200	28.314
192.168.1.43	38				0.0013	31.15%	0.0900	26.247
192.168.1.255	2				0.0001	1.64%	0.0100	15.233
152.15.38.60	27				0.0010	22.13%	0.0600	26.213
13.90.253.47	2				0.0001	1.64%	0.0200	25.408
108.138.85.59	1				0.0000	0.82%	0.0100	23.032


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time      Source                 Destination            Protocol Length Info
   40 3.725658  2001:470:67:c0::1337   2603:6081:606:eb00:…   TCP        74 23 → 54938 [ACK] Seq=1228 Ack=66 Win=65408 Len=0
   47 5.521318  192.168.1.43           152.15.38.60           TCP        54 54937 → 443 [FIN, ACK] Seq=1 Ack=2 Win=257 Len=0
   48 5.521935  2603:6081:606:eb00:…   2600:6c7f:f000:202:…   TCP        86 54939 → 443 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM
   49 5.556438  152.15.38.60           192.168.1.43           TCP        60 443 → 54937 [ACK] Seq=2 Ack=2 Win=15045 Len=0
   50 5.574740  2600:6c7f:f000:202:…   2603:6081:606:eb00:…   TCP        78 443 → 54939 [SYN, ACK] Seq=0 Ack=1 Win=28800 Len=0 MSS=1440
   51 5.574817  2603:6081:606:eb00:…   2600:6c7f:f000:202:…   TCP        74 54939 → 443 [ACK] Seq=1 Ack=1 Win=64800 Len=0
   53 5.630019  2600:6c7f:f000:202:…   2603:6081:606:eb00:…   TCP        74 443 → 54939 [ACK] Seq=1 Ack=557 Win=29468 Len=0
   55 5.631381  2600:6c7f:f000:2
   56 5.631381  2600:6c7f:f000:2
   57 5.631406  2603:6081:606:eb
   64 5.741408  2600:6c7f:f000:2
   66 5.783431  2603:6081:606:eb
   68 5.840601  192.168.1.43
   70 5.874489  152.15.38.60
   71 5.874557  192.168.1.43
   74 5.909293  152.15.38.60
```

```
∨ Frame 3: 60 bytes on wire (480 bits)
    Section number: 1
  > Interface id: 0 (\Device\NPF_{A36
    Encapsulation type: Ethernet (1)
    Arrival Time: Jan 13, 2023 12:49:
    [Time shift for this packet: 0.00
    Epoch Time: 1673632148.753635000
    [Time delta from previous capture
    [Time delta from previous display
    [Time since reference or first fr
    Frame Number: 3
    Frame Length: 60 bytes (480 bits)
    Capture Length: 60 bytes (480 bit
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertyp
    [Coloring Rule Name: ARP]
```

Address Resolution Protocol (arp), 28 bytes

Wireshark · Destinations and Ports · Wi-Fi

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
∨ Destinations and Ports	122				0.0043	100%	0.1400	26.247
∨ 54.156.17.24	1				0.0000	0.82%	0.0100	22.719
∨ TCP	1				0.0000	100.00%	0.0100	22.719
443	1				0.0000	100.00%	0.0100	22.719
∨ 52.109.8.44	2				0.0001	1.64%	0.0200	28.313
∨ TCP	2				0.0001	100.00%	0.0200	28.313
443	2				0.0001	100.00%	0.0200	28.313
∨ 255.255.255.255	17				0.0006	13.93%	0.0400	15.227
∨ UDP	17				0.0006	100.00%	0.0400	15.227
7423	9				0.0003	52.94%	0.0100	2.324
17500	8				0.0003	47.06%	0.0400	15.227
∨ 239.255.255.250	14				0.0005	11.48%	0.1000	7.445
∨ UDP	14				0.0005	100.00%	0.1000	7.445
1900	14				0.0005	100.00%	0.1000	7.445
∨ 224.0.0.252	5				0.0002	4.10%	0.0500	25.672
∨ UDP	2				0.0001	40.00%	0.0200	25.674
5355	2				0.0001	100.00%	0.0200	25.674
∨ NONE	3				0.0001	60.00%	0.0300	25.672
0	3				0.0001	100.00%	0.0300	25.672
∨ 224.0.0.251	8				0.0003	6.56%	0.0800	25.673
∨ UDP	8				0.0003	100.00%	0.0800	25.673
5353	8				0.0003	100.00%	0.0800	25.673
∨ 209.18.47.63	3				0.0001	2.46%	0.0200	2.784
∨ UDP	3				0.0001	100.00%	0.0200	2.784
53	3				0.0001	100.00%	0.0200	2.784
∨ 20.231.71.84	2				0.0001	1.64%	0.0200	28.314

Ports.txt