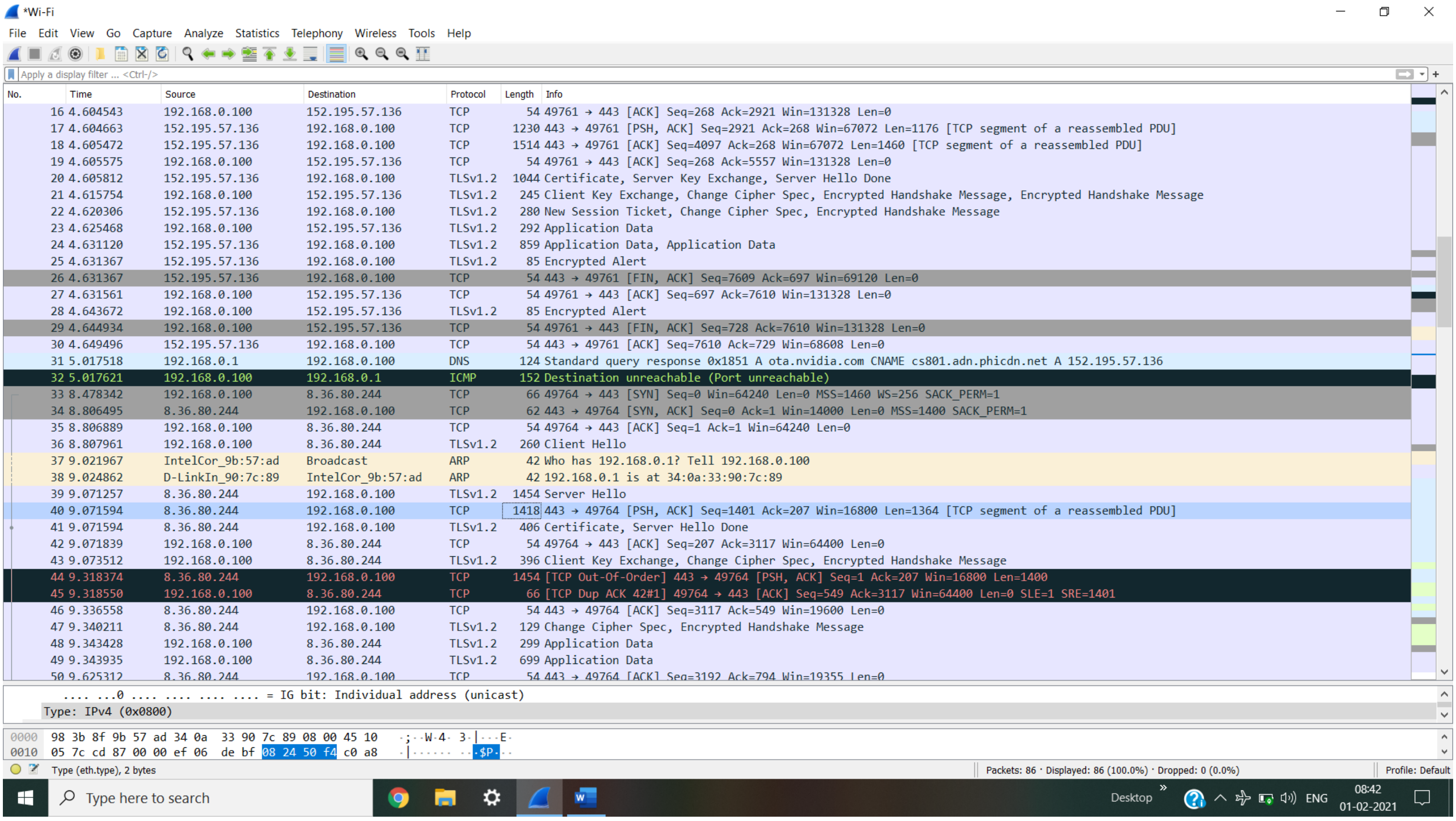
NETWORKS LAB EXPERIMENT – 2

YACHA VENKATA RAKESH

B180427CS

1.


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Type here to search
Desktop
ENG
08:42
01-02-2021

```
No.  Time      Source             Destination        Protocol  Length Info
  16 4.604543  192.168.0.100      152.195.57.136     TCP         54 49761 → 443 [ACK] Seq=268 Ack=2921 Win=131328 Len=0
  17 4.604663  152.195.57.136     192.168.0.100      TCP       1230 443 → 49761 [PSH, ACK] Seq=2921 Ack=268 Win=67072 Len=1176 [TCP segment of a reassembled PDU]
  18 4.605472  152.195.57.136     192.168.0.100      TCP       1514 443 → 49761 [ACK] Seq=4097 Ack=268 Win=67072 Len=1460 [TCP segment of a reassembled PDU]
  19 4.605575  192.168.0.100      152.195.57.136     TCP         54 49761 → 443 [ACK] Seq=268 Ack=5557 Win=131328 Len=0
  20 4.605812  152.195.57.136     192.168.0.100      TLSv1.2   1044 Certificate, Server Key Exchange, Server Hello Done
  21 4.615754  192.168.0.100      152.195.57.136     TLSv1.2    245 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message, Encrypted Handshake Message
  22 4.620306  152.195.57.136     192.168.0.100      TLSv1.2    280 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
  23 4.625468  192.168.0.100      152.195.57.136     TLSv1.2    292 Application Data
  24 4.631120  152.195.57.136     192.168.0.100      TLSv1.2    859 Application Data, Application Data
  25 4.631367  152.195.57.136     192.168.0.100      TLSv1.2     85 Encrypted Alert
  26 4.631367  152.195.57.136     192.168.0.100      TCP         54 443 → 49761 [FIN, ACK] Seq=7609 Ack=697 Win=69120 Len=0
  27 4.631561  192.168.0.100      152.195.57.136     TCP         54 49761 → 443 [ACK] Seq=697 Ack=7610 Win=131328 Len=0
  28 4.643672  192.168.0.100      152.195.57.136     TLSv1.2     85 Encrypted Alert
  29 4.644934  192.168.0.100      152.195.57.136     TCP         54 49761 → 443 [FIN, ACK] Seq=728 Ack=7610 Win=131328 Len=0
  30 4.649496  152.195.57.136     192.168.0.100      TCP         54 443 → 49761 [ACK] Seq=7610 Ack=729 Win=68608 Len=0
  31 5.017518  192.168.0.1        192.168.0.100      DNS        124 Standard query response 0x1851 A ota.nvidia.com CNAME cs801.adn.phicdn.net A 152.195.57.136
  32 5.017621  192.168.0.100      192.168.0.1        ICMP       152 Destination unreachable (Port unreachable)
  33 8.478342  192.168.0.100      8.36.80.244        TCP         66 49764 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  34 8.806495  8.36.80.244        192.168.0.100      TCP         62 443 → 49764 [SYN, ACK] Seq=0 Ack=1 Win=14000 Len=0 MSS=1400 SACK_PERM=1
  35 8.806889  192.168.0.100      8.36.80.244        TCP         54 49764 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
  36 8.807961  192.168.0.100      8.36.80.244        TLSv1.2    260 Client Hello
  37 9.021967  IntelCor_9b:57:ad  Broadcast          ARP         42 Who has 192.168.0.1? Tell 192.168.0.100
  38 9.024862  D-LinkIn_90:7c:89  IntelCor_9b:57:ad  ARP         42 192.168.0.1 is at 34:0a:33:90:7c:89
  39 9.071257  8.36.80.244        192.168.0.100      TLSv1.2   1454 Server Hello
  40 9.071594  8.36.80.244        192.168.0.100      TCP       1418 443 → 49764 [PSH, ACK] Seq=1401 Ack=207 Win=16800 Len=1364 [TCP segment of a reassembled PDU]
  41 9.071594  8.36.80.244        192.168.0.100      TLSv1.2    406 Certificate, Server Hello Done
  42 9.071839  192.168.0.100      8.36.80.244        TCP         54 49764 → 443 [ACK] Seq=207 Ack=3117 Win=64400 Len=0
  43 9.073512  192.168.0.100      8.36.80.244        TLSv1.2    396 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
  44 9.318374  8.36.80.244        192.168.0.100      TCP       1454 [TCP Out-Of-Order] 443 → 49764 [PSH, ACK] Seq=1 Ack=207 Win=16800 Len=1400
  45 9.318550  192.168.0.100      8.36.80.244        TCP         66 [TCP Dup ACK 42#1] 49764 → 443 [ACK] Seq=549 Ack=3117 Win=64400 Len=0 SLE=1 SRE=1401
  46 9.336558  8.36.80.244        192.168.0.100      TCP         54 443 → 49764 [ACK] Seq=3117 Ack=549 Win=19600 Len=0
  47 9.340211  8.36.80.244        192.168.0.100      TLSv1.2    129 Change Cipher Spec, Encrypted Handshake Message
  48 9.343428  192.168.0.100      8.36.80.244        TLSv1.2    299 Application Data
  49 9.343935  192.168.0.100      8.36.80.244        TLSv1.2    699 Application Data
  50 9.625312  8.36.80.244        192.168.0.100      TCP         54 443 → 49764 [ACK] Seq=3192 Ack=794 Win=19355 Len=0

    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)

0000  98 3b 8f 9b 57 ad 34 0a  33 90 7c 89 08 00 45 10   ·;··W·4· 3·|···E·
0010  05 7c cd 87 00 00 ef 06  de bf 08 24 50 f4 c0 a8   ·|······ ···$P···

Type (eth.type), 2 bytes          Packets: 86 · Displayed: 86 (100.0%) · Dropped: 0 (0.0%)          Profile: Default
```

Fig 1. Wireshark capturing different packets for 5 seconds

a)

MAC Header: typically referred as an Ethernet Header

This contains 1. Destination MAC address (48 bit size in in hexadecimal format)

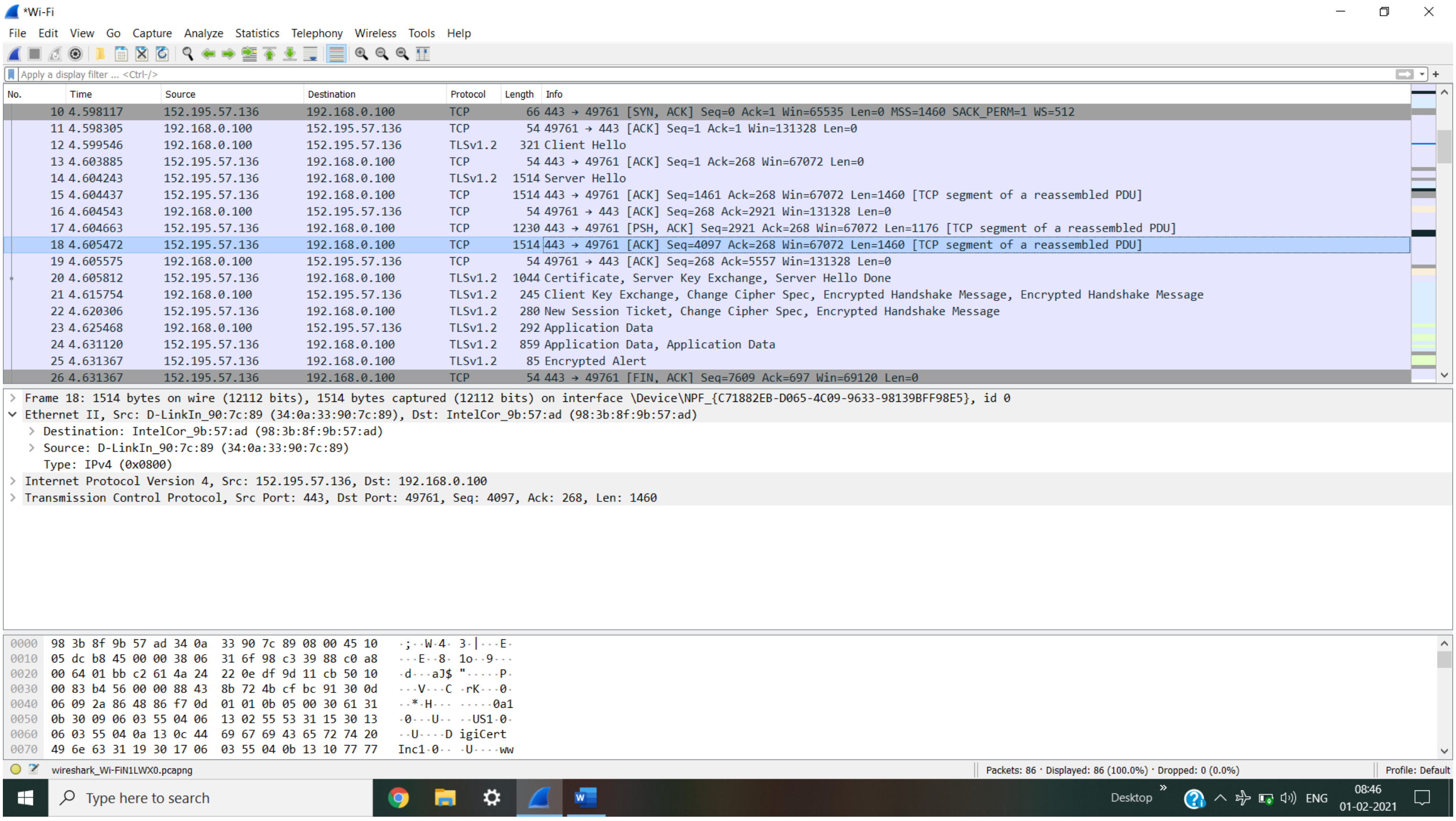
2. Source MAC address (48 bit size in in hexadecimal format)

3. Ether type

These data fields are added at the beginning of a network packet in order to turn it into a frame (Ethernet frame) to be transmitted. This typically refers to an ethernet header. It is part of data link layer which controls access to physical transmission medium.

Protocol ID:

The Protocol ID is a number embedded in the header of the packet to identify the protocol. It is mainly used for protocols which can’t be identified with a port number.


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Type here to search
Desktop
ENG
08:46
01-02-2021

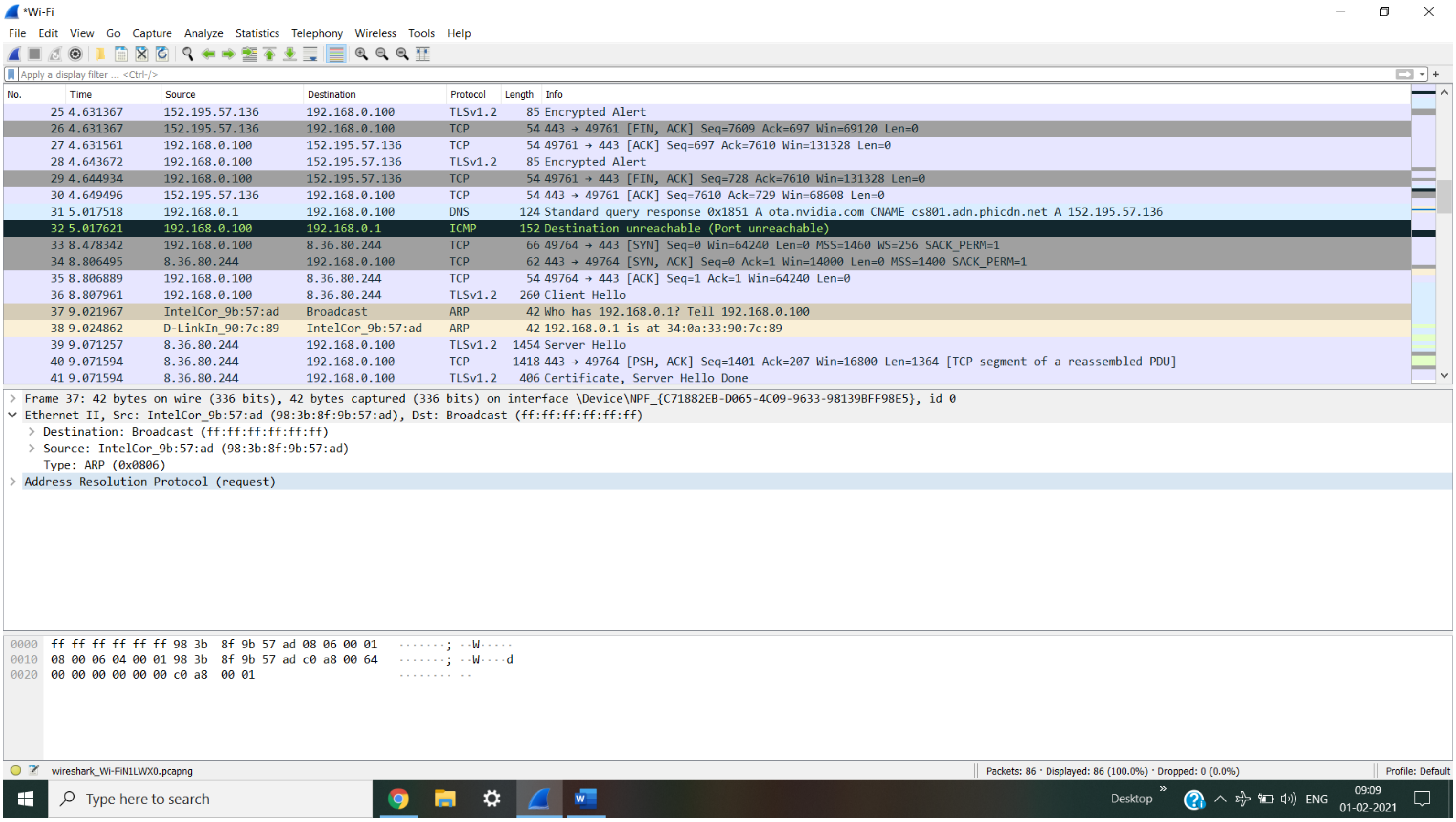
```
No.   Time      Source          Destination     Protocol Length Info
   10 4.598117  152.195.57.136  192.168.0.100   TCP        66 443 → 49761 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 SACK_PERM=1 WS=512
   11 4.598305  192.168.0.100   152.195.57.136  TCP        54 49761 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0
   12 4.599546  192.168.0.100   152.195.57.136  TLSv1.2   321 Client Hello
   13 4.603885  152.195.57.136  192.168.0.100   TCP        54 443 → 49761 [ACK] Seq=1 Ack=268 Win=67072 Len=0
   14 4.604243  152.195.57.136  192.168.0.100   TLSv1.2  1514 Server Hello
   15 4.604437  152.195.57.136  192.168.0.100   TCP      1514 443 → 49761 [ACK] Seq=1461 Ack=268 Win=67072 Len=1460 [TCP segment of a reassembled PDU]
   16 4.604543  192.168.0.100   152.195.57.136  TCP        54 49761 → 443 [ACK] Seq=268 Ack=2921 Win=131328 Len=0
   17 4.604663  152.195.57.136  192.168.0.100   TCP      1230 443 → 49761 [PSH, ACK] Seq=2921 Ack=268 Win=67072 Len=1176 [TCP segment of a reassembled PDU]
   18 4.605472  152.195.57.136  192.168.0.100   TCP      1514 443 → 49761 [ACK] Seq=4097 Ack=268 Win=67072 Len=1460 [TCP segment of a reassembled PDU]
   19 4.605575  192.168.0.100   152.195.57.136  TCP        54 49761 → 443 [ACK] Seq=268 Ack=5557 Win=131328 Len=0
   20 4.605812  152.195.57.136  192.168.0.100   TLSv1.2  1044 Certificate, Server Key Exchange, Server Hello Done
   21 4.615754  192.168.0.100   152.195.57.136  TLSv1.2   245 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message, Encrypted Handshake Message
   22 4.620306  152.195.57.136  192.168.0.100   TLSv1.2   280 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
   23 4.625468  192.168.0.100   152.195.57.136  TLSv1.2   292 Application Data
   24 4.631120  152.195.57.136  192.168.0.100   TLSv1.2   859 Application Data, Application Data
   25 4.631367  152.195.57.136  192.168.0.100   TLSv1.2    85 Encrypted Alert
   26 4.631367  152.195.57.136  192.168.0.100   TCP        54 443 → 49761 [FIN, ACK] Seq=7609 Ack=697 Win=69120 Len=0
```

```
> Frame 18: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{C71882EB-D065-4C09-9633-98139BFF98E5}, id 0
v Ethernet II, Src: D-LinkIn_90:7c:89 (34:0a:33:90:7c:89), Dst: IntelCor_9b:57:ad (98:3b:8f:9b:57:ad)
  > Destination: IntelCor_9b:57:ad (98:3b:8f:9b:57:ad)
  > Source: D-LinkIn_90:7c:89 (34:0a:33:90:7c:89)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 152.195.57.136, Dst: 192.168.0.100
> Transmission Control Protocol, Src Port: 443, Dst Port: 49761, Seq: 4097, Ack: 268, Len: 1460
```

```
0000  98 3b 8f 9b 57 ad 34 0a  33 90 7c 89 08 00 45 10   ·;··W·4· 3·|···E·
0010  05 dc b8 45 00 00 38 06  31 6f 98 c3 39 88 c0 a8   ···E··8· 1o··9···
0020  00 64 01 bb c2 61 4a 24  22 0e df 9d 11 cb 50 10   ·d···aJ$ "·····P·
0030  00 83 b4 56 00 00 88 43  8b 72 4b cf bc 91 30 0d   ···V···C ·rK···0·
0040  06 09 2a 86 48 86 f7 0d  01 01 0b 05 00 30 61 31   ··*·H··· ·····0a1
0050  0b 30 09 06 03 55 04 06  13 02 55 53 31 15 30 13   ·0···U·· ··US1·0·
0060  06 03 55 04 0a 13 0c 44  69 67 69 43 65 72 74 20   ··U····D igiCert
0070  49 6e 63 31 19 30 17 06  03 55 04 0b 13 10 77 77   Inc1·0·· ·U····ww
```

```
wireshark_Wi-FiN1LWX0.pcapng          Packets: 86 · Displayed: 86 (100.0%) · Dropped: 0 (0.0%)          Profile: Default
```

Fig 1.2 MAC header in an IP packet under Ethernet II


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Type here to search
Desktop
ENG
09:09
01-02-2021

```
No.   Time      Source             Destination        Protocol Length Info
   25 4.631367  152.195.57.136     192.168.0.100      TLSv1.2    85 Encrypted Alert
   26 4.631367  152.195.57.136     192.168.0.100      TCP        54 443 → 49761 [FIN, ACK] Seq=7609 Ack=697 Win=69120 Len=0
   27 4.631561  192.168.0.100      152.195.57.136     TCP        54 49761 → 443 [ACK] Seq=697 Ack=7610 Win=131328 Len=0
   28 4.643672  192.168.0.100      152.195.57.136     TLSv1.2    85 Encrypted Alert
   29 4.644934  192.168.0.100      152.195.57.136     TCP        54 49761 → 443 [FIN, ACK] Seq=728 Ack=7610 Win=131328 Len=0
   30 4.649496  152.195.57.136     192.168.0.100      TCP        54 443 → 49761 [ACK] Seq=7610 Ack=729 Win=68608 Len=0
   31 5.017518  192.168.0.1        192.168.0.100      DNS       124 Standard query response 0x1851 A ota.nvidia.com CNAME cs801.adn.phicdn.net A 152.195.57.136
   32 5.017621  192.168.0.100      192.168.0.1        ICMP      152 Destination unreachable (Port unreachable)
   33 8.478342  192.168.0.100      8.36.80.244        TCP        66 49764 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
   34 8.806495  8.36.80.244        192.168.0.100      TCP        62 443 → 49764 [SYN, ACK] Seq=0 Ack=1 Win=14000 Len=0 MSS=1400 SACK_PERM=1
   35 8.806889  192.168.0.100      8.36.80.244        TCP        54 49764 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
   36 8.807961  192.168.0.100      8.36.80.244        TLSv1.2   260 Client Hello
   37 9.021967  IntelCor_9b:57:ad  Broadcast          ARP        42 Who has 192.168.0.1? Tell 192.168.0.100
   38 9.024862  D-LinkIn_90:7c:89  IntelCor_9b:57:ad  ARP        42 192.168.0.1 is at 34:0a:33:90:7c:89
   39 9.071257  8.36.80.244        192.168.0.100      TLSv1.2  1454 Server Hello
   40 9.071594  8.36.80.244        192.168.0.100      TCP      1418 443 → 49764 [PSH, ACK] Seq=1401 Ack=207 Win=16800 Len=1364 [TCP segment of a reassembled PDU]
   41 9.071594  8.36.80.244        192.168.0.100      TLSv1.2   406 Certificate, Server Hello Done
```

```
> Frame 37: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{C71882EB-D065-4C09-9633-98139BFF98E5}, id 0
v Ethernet II, Src: IntelCor_9b:57:ad (98:3b:8f:9b:57:ad), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  > Source: IntelCor_9b:57:ad (98:3b:8f:9b:57:ad)
    Type: ARP (0x0806)
> Address Resolution Protocol (request)
```

```
0000  ff ff ff ff ff ff 98 3b  8f 9b 57 ad 08 06 00 01   ·······; ··W·····
0010  08 00 06 04 00 01 98 3b  8f 9b 57 ad c0 a8 00 64   ·······; ··W····d
0020  00 00 00 00 00 00 c0 a8  00 01                     ········ ··
```

```
wireshark_Wi-FiN1LWX0.pcapng          Packets: 86 · Displayed: 86 (100.0%) · Dropped: 0 (0.0%)          Profile: Default
```

Fig 1.3 MAC Header in an ARP Packet under Ethernet II

We can observe source MAC address being same in the both packets and Destination MAC address is different one is a broadcast (ARP request packet) and other is unicast (IP packet). Ether type is different for IP it is **IPv4 (0x0800)** and for ARP it is **ARP (0x0806).** Hence the MAC headers for both ARP and IP packets are different.

Protocol ID for IP is **0x0800**

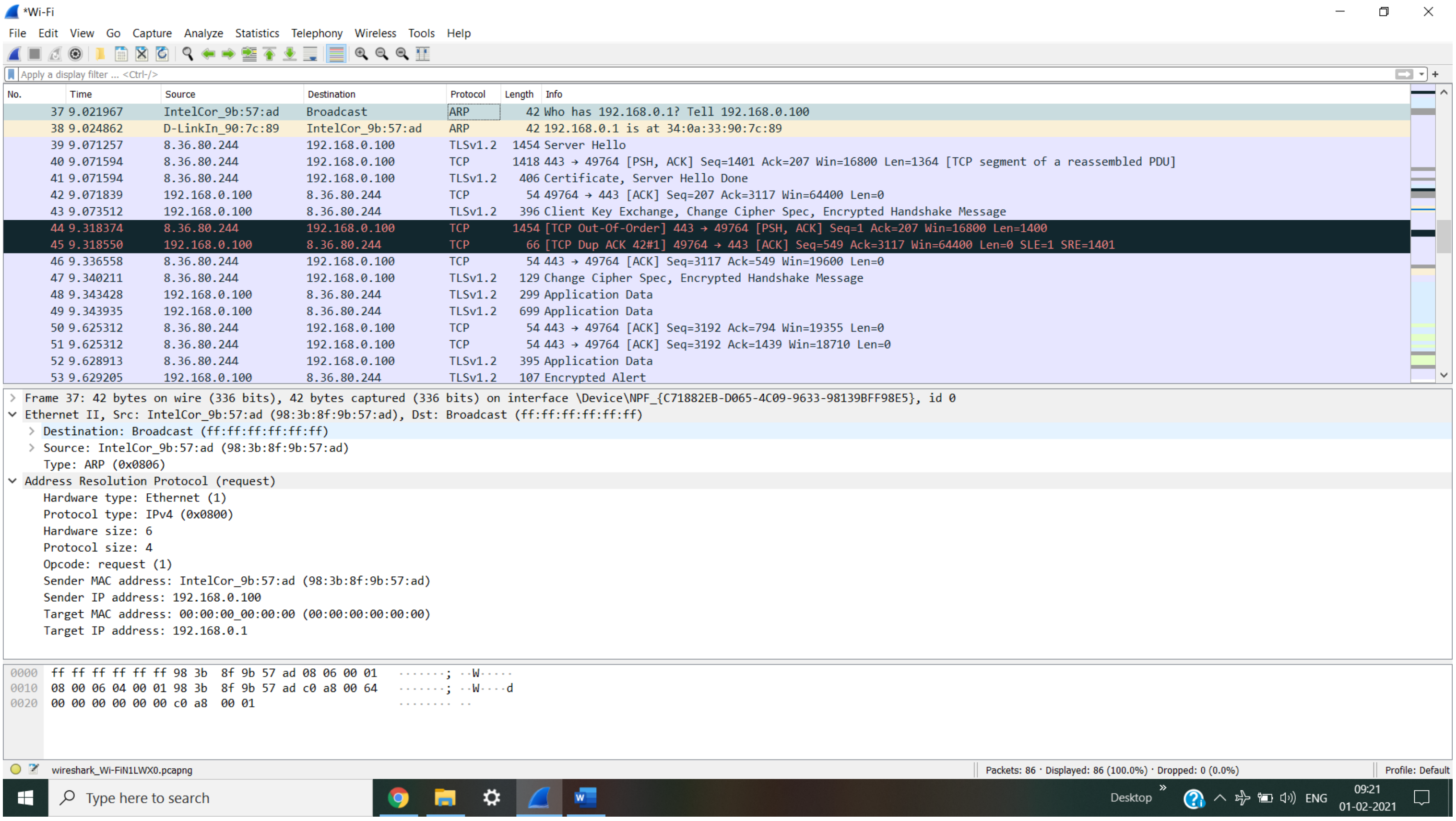
Protocol ID for ARP is **0x0806**

b)

Destination address of the ARP packet can be either broadcast or unicast.

1. Destination address of the ARP request packet is a broadcast (Since the MAC address of the target machine is unknown)

2. Destination address of the ARP reply packet is a unicast address (Since the MAC address there is the source address itself which is known from the ARP packet)


*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
   37 9.021967    IntelCor_9b:57:ad   Broadcast           ARP         42 Who has 192.168.0.1? Tell 192.168.0.100
   38 9.024862    D-LinkIn_90:7c:89   IntelCor_9b:57:ad   ARP         42 192.168.0.1 is at 34:0a:33:90:7c:89
   39 9.071257    8.36.80.244         192.168.0.100       TLSv1.2   1454 Server Hello
   40 9.071594    8.36.80.244         192.168.0.100       TCP       1418 443 → 49764 [PSH, ACK] Seq=1401 Ack=207 Win=16800 Len=1364 [TCP segment of a reassembled PDU]
   41 9.071594    8.36.80.244         192.168.0.100       TLSv1.2    406 Certificate, Server Hello Done
   42 9.071839    192.168.0.100       8.36.80.244         TCP         54 49764 → 443 [ACK] Seq=207 Ack=3117 Win=64400 Len=0
   43 9.073512    192.168.0.100       8.36.80.244         TLSv1.2    396 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
   44 9.318374    8.36.80.244         192.168.0.100       TCP       1454 [TCP Out-Of-Order] 443 → 49764 [PSH, ACK] Seq=1 Ack=207 Win=16800 Len=1400
   45 9.318550    192.168.0.100       8.36.80.244         TCP         66 [TCP Dup ACK 42#1] 49764 → 443 [ACK] Seq=549 Ack=3117 Win=64400 Len=0 SLE=1 SRE=1401
   46 9.336558    8.36.80.244         192.168.0.100       TCP         54 443 → 49764 [ACK] Seq=3117 Ack=549 Win=19600 Len=0
   47 9.340211    8.36.80.244         192.168.0.100       TLSv1.2    129 Change Cipher Spec, Encrypted Handshake Message
   48 9.343428    192.168.0.100       8.36.80.244         TLSv1.2    299 Application Data
   49 9.343935    192.168.0.100       8.36.80.244         TLSv1.2    699 Application Data
   50 9.625312    8.36.80.244         192.168.0.100       TCP         54 443 → 49764 [ACK] Seq=3192 Ack=794 Win=19355 Len=0
   51 9.625312    8.36.80.244         192.168.0.100       TCP         54 443 → 49764 [ACK] Seq=3192 Ack=1439 Win=18710 Len=0
   52 9.628913    8.36.80.244         192.168.0.100       TLSv1.2    395 Application Data
   53 9.629205    192.168.0.100       8.36.80.244         TLSv1.2    107 Encrypted Alert
```

```
> Frame 37: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{C71882EB-D065-4C09-9633-98139BFF98E5}, id 0
v Ethernet II, Src: IntelCor_9b:57:ad (98:3b:8f:9b:57:ad), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  > Source: IntelCor_9b:57:ad (98:3b:8f:9b:57:ad)
    Type: ARP (0x0806)
v Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: IntelCor_9b:57:ad (98:3b:8f:9b:57:ad)
    Sender IP address: 192.168.0.100
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.0.1
```

```
0000  ff ff ff ff ff ff 98 3b  8f 9b 57 ad 08 06 00 01   .......; ..W.....
0010  08 00 06 04 00 01 98 3b  8f 9b 57 ad c0 a8 00 64   .......; ..W....d
0020  00 00 00 00 00 00 c0 a8  00 01                     ........ ..
```

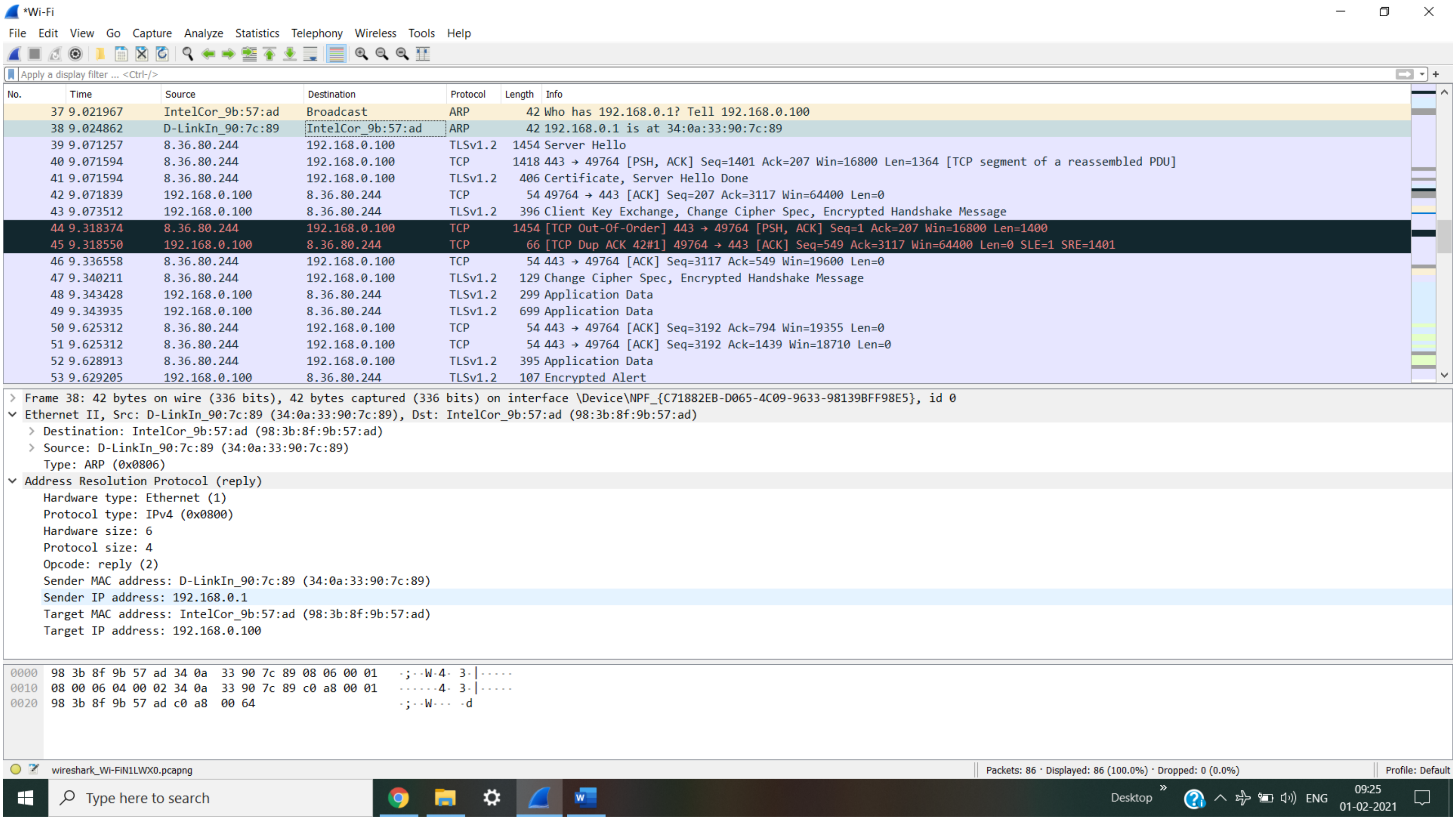
wireshark_Wi-FiN1LWX0.pcapng
Packets: 86 · Displayed: 86 (100.0%) · Dropped: 0 (0.0%)
Profile: Default
Type here to search
Desktop
ENG
09:21
01-02-2021

Fig 1.4 ARP Request with Destination as broadcast

Here for packet number 37 under Ethernet II, You can see the destination address as Broadcast

In the Address Resolution Protocol, You can find the Opcode as request (1).

1 denotes request and 2 denotes reply.



*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
wireshark_Wi-FiN1LWX0.pcapng
Packets: 86 · Displayed: 86 (100.0%) · Dropped: 0 (0.0%)
Profile: Default
Type here to search
Desktop
ENG
09:25
01-02-2021

```
No.   Time       Source              Destination        Protocol Length Info
   37 9.021967   IntelCor_9b:57:ad   Broadcast          ARP        42 Who has 192.168.0.1? Tell 192.168.0.100
   38 9.024862   D-LinkIn_90:7c:89   IntelCor_9b:57:ad  ARP        42 192.168.0.1 is at 34:0a:33:90:7c:89
   39 9.071257   8.36.80.244         192.168.0.100      TLSv1.2  1454 Server Hello
   40 9.071594   8.36.80.244         192.168.0.100      TCP      1418 443 → 49764 [PSH, ACK] Seq=1401 Ack=207 Win=16800 Len=1364 [TCP segment of a reassembled PDU]
   41 9.071594   8.36.80.244         192.168.0.100      TLSv1.2   406 Certificate, Server Hello Done
   42 9.071839   192.168.0.100       8.36.80.244        TCP        54 49764 → 443 [ACK] Seq=207 Ack=3117 Win=64400 Len=0
   43 9.073512   192.168.0.100       8.36.80.244        TLSv1.2   396 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
   44 9.318374   8.36.80.244         192.168.0.100      TCP      1454 [TCP Out-Of-Order] 443 → 49764 [PSH, ACK] Seq=1 Ack=207 Win=16800 Len=1400
   45 9.318550   192.168.0.100       8.36.80.244        TCP        66 [TCP Dup ACK 42#1] 49764 → 443 [ACK] Seq=549 Ack=3117 Win=64400 Len=0 SLE=1 SRE=1401
   46 9.336558   8.36.80.244         192.168.0.100      TCP        54 443 → 49764 [ACK] Seq=3117 Ack=549 Win=19600 Len=0
   47 9.340211   8.36.80.244         192.168.0.100      TLSv1.2   129 Change Cipher Spec, Encrypted Handshake Message
   48 9.343428   192.168.0.100       8.36.80.244        TLSv1.2   299 Application Data
   49 9.343935   192.168.0.100       8.36.80.244        TLSv1.2   699 Application Data
   50 9.625312   8.36.80.244         192.168.0.100      TCP        54 443 → 49764 [ACK] Seq=3192 Ack=794 Win=19355 Len=0
   51 9.625312   8.36.80.244         192.168.0.100      TCP        54 443 → 49764 [ACK] Seq=3192 Ack=1439 Win=18710 Len=0
   52 9.628913   8.36.80.244         192.168.0.100      TLSv1.2   395 Application Data
   53 9.629205   192.168.0.100       8.36.80.244        TLSv1.2   107 Encrypted Alert

> Frame 38: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{C71882EB-D065-4C09-9633-98139BFF98E5}, id 0
v Ethernet II, Src: D-LinkIn_90:7c:89 (34:0a:33:90:7c:89), Dst: IntelCor_9b:57:ad (98:3b:8f:9b:57:ad)
  > Destination: IntelCor_9b:57:ad (98:3b:8f:9b:57:ad)
  > Source: D-LinkIn_90:7c:89 (34:0a:33:90:7c:89)
    Type: ARP (0x0806)
v Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: D-LinkIn_90:7c:89 (34:0a:33:90:7c:89)
    Sender IP address: 192.168.0.1
    Target MAC address: IntelCor_9b:57:ad (98:3b:8f:9b:57:ad)
    Target IP address: 192.168.0.100

0000  98 3b 8f 9b 57 ad 34 0a  33 90 7c 89 08 06 00 01   ·;··W·4· 3·|·····
0010  08 00 06 04 00 02 34 0a  33 90 7c 89 c0 a8 00 01   ······4· 3·|·····
0020  98 3b 8f 9b 57 ad c0 a8  00 64                     ·;··W···  ·d
```

Fig 1.5 ARP reply with destination as unicast

You can see under packet number 38 info, showing MAC address of the previously requested IP address 192.168.0.1

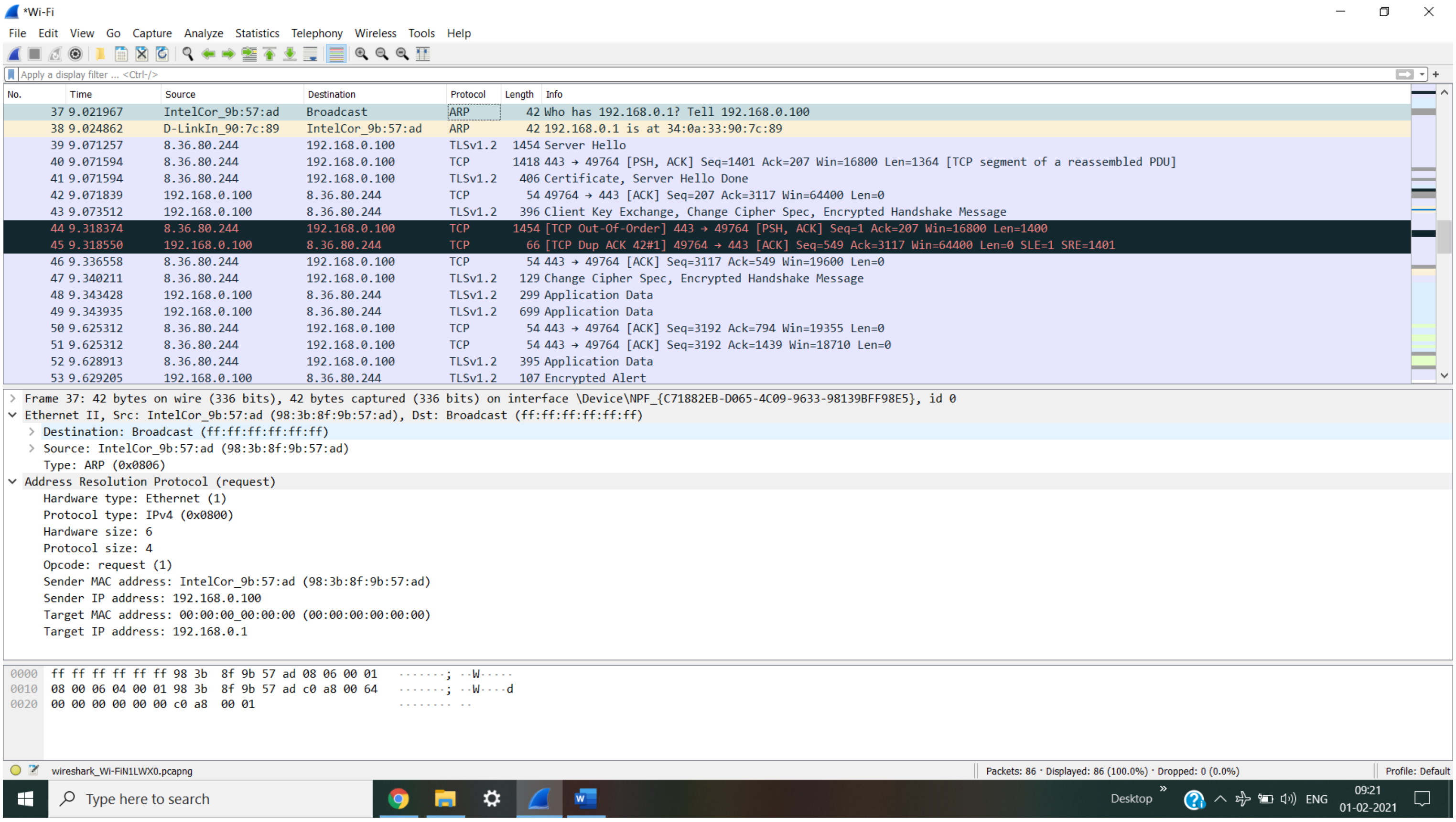
And in the Ethernet II we can see the destination address as unicast address and also it is the source address from which ARP request has been sent

In Address Resolution Protocol, Under Opcode it is shown as reply (2) c)

There are two types of ARP packets. They are: ARP request and ARP reply.

ARP: ARP (Address Resolution Protocol) is used to obtain the Ethernet Address / MAC Address of the target computer from the IP address of the target computer, so that source can send data to the target device. This is because MAC address is required to communicate between any two systems.

Suppose we search for a website, For this initially it checks for MAC address mapping of the IP address of DNS server in the ARP table or ARP cache. If It is not present then the Operating system creates a DNS query message in ‘question section’ of packet and place it in UDP segment with the destination port 53 and the source port as random UDP port number opened by TCP/IP protocol stack on DNS client. Then this is sent to IP datagram along with the headers source and destination IP addresses. The IP address of source is allocated by DHCP protocol along with IP address of the Gateway router and DNS server. Now this is added with source MAC address and Gateway broadcast address and then this ethernet frame is sent to the gateway router. Since, it being a broadcast message it is sent to all the systems and each system by checking the type field in the ethernet frame, ARP request packet is sent to ARP module and then the target IP address is checked and if it matches then ARP reply message is sent by interchanging source and Destination MAC address and now the ARP table adds this IP address and MAC address of the DNS server mapping to it.


*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
   37 9.021967  IntelCor_9b:57:ad   Broadcast          ARP         42 Who has 192.168.0.1? Tell 192.168.0.100
   38 9.024862  D-LinkIn_90:7c:89   IntelCor_9b:57:ad  ARP         42 192.168.0.1 is at 34:0a:33:90:7c:89
   39 9.071257  8.36.80.244         192.168.0.100      TLSv1.2   1454 Server Hello
   40 9.071594  8.36.80.244         192.168.0.100      TCP       1418 443 → 49764 [PSH, ACK] Seq=1401 Ack=207 Win=16800 Len=1364 [TCP segment of a reassembled PDU]
   41 9.071594  8.36.80.244         192.168.0.100      TLSv1.2    406 Certificate, Server Hello Done
   42 9.071839  192.168.0.100       8.36.80.244        TCP         54 49764 → 443 [ACK] Seq=207 Ack=3117 Win=64400 Len=0
   43 9.073512  192.168.0.100       8.36.80.244        TLSv1.2    396 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
   44 9.318374  8.36.80.244         192.168.0.100      TCP       1454 [TCP Out-Of-Order] 443 → 49764 [PSH, ACK] Seq=1 Ack=207 Win=16800 Len=1400
   45 9.318550  192.168.0.100       8.36.80.244        TCP         66 [TCP Dup ACK 42#1] 49764 → 443 [ACK] Seq=549 Ack=3117 Win=64400 Len=0 SLE=1 SRE=1401
   46 9.336558  8.36.80.244         192.168.0.100      TCP         54 443 → 49764 [ACK] Seq=3117 Ack=549 Win=19600 Len=0
   47 9.340211  8.36.80.244         192.168.0.100      TLSv1.2    129 Change Cipher Spec, Encrypted Handshake Message
   48 9.343428  192.168.0.100       8.36.80.244        TLSv1.2    299 Application Data
   49 9.343935  192.168.0.100       8.36.80.244        TLSv1.2    699 Application Data
   50 9.625312  8.36.80.244         192.168.0.100      TCP         54 443 → 49764 [ACK] Seq=3192 Ack=794 Win=19355 Len=0
   51 9.625312  8.36.80.244         192.168.0.100      TCP         54 443 → 49764 [ACK] Seq=3192 Ack=1439 Win=18710 Len=0
   52 9.628913  8.36.80.244         192.168.0.100      TLSv1.2    395 Application Data
   53 9.629205  192.168.0.100       8.36.80.244        TLSv1.2    107 Encrypted Alert
```

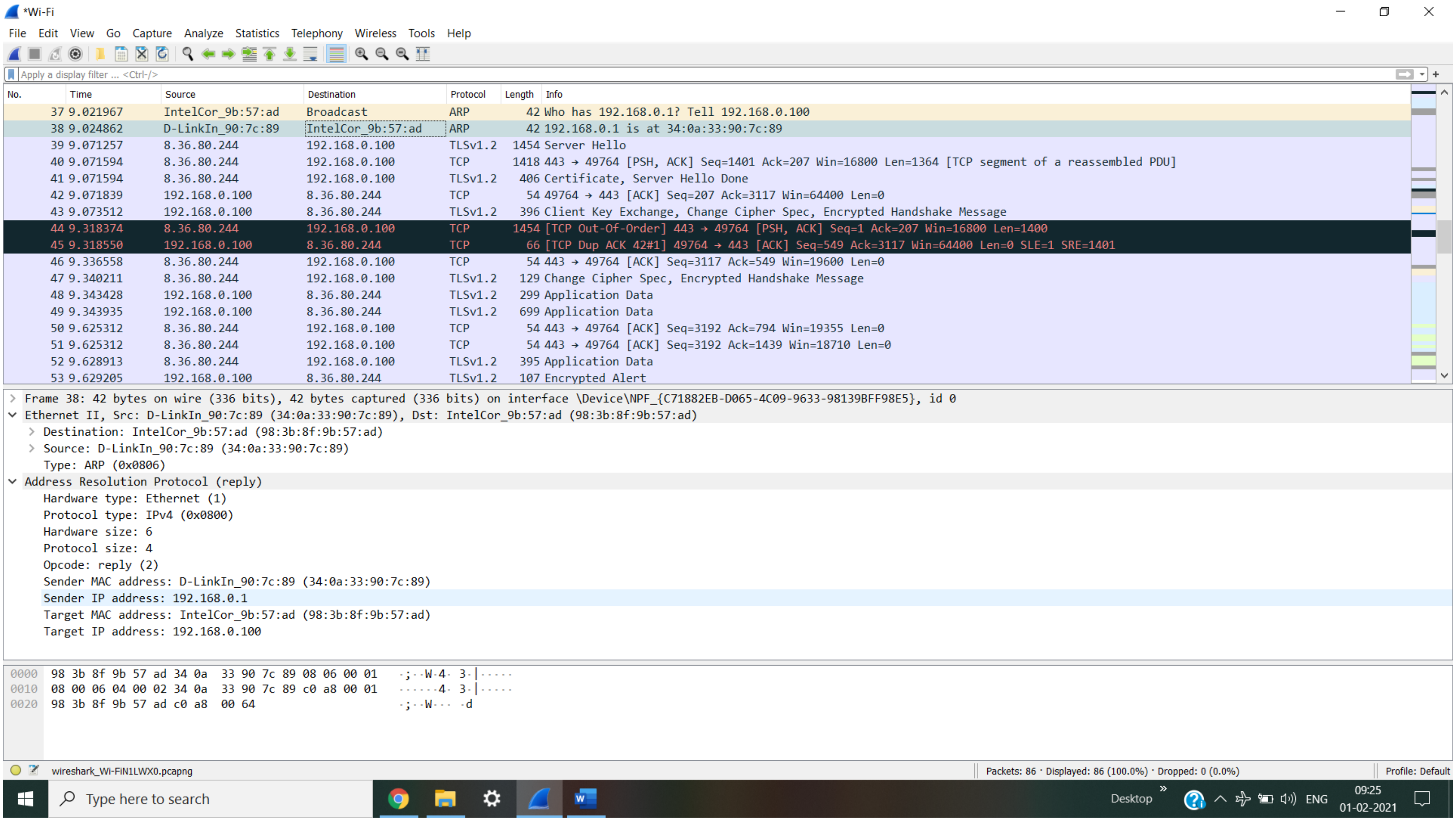
```
> Frame 37: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{C71882EB-D065-4C09-9633-98139BFF98E5}, id 0
v Ethernet II, Src: IntelCor_9b:57:ad (98:3b:8f:9b:57:ad), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  > Source: IntelCor_9b:57:ad (98:3b:8f:9b:57:ad)
    Type: ARP (0x0806)
v Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: IntelCor_9b:57:ad (98:3b:8f:9b:57:ad)
    Sender IP address: 192.168.0.100
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.0.1
```

```
0000  ff ff ff ff ff ff 98 3b  8f 9b 57 ad 08 06 00 01   ·······; ··W·····
0010  08 00 06 04 00 01 98 3b  8f 9b 57 ad c0 a8 00 64   ·······; ··W····d
0020  00 00 00 00 00 00 c0 a8  00 01                     ········ ··
```

wireshark_Wi-FiN1LWX0.pcapng | Packets: 86 · Displayed: 86 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

Fig 1.6 ARP request packet

Here in the Address Resolution Protocol, **Opcode** field represents the type of the message. Here it’s value is 1 representing it as an ARP request message. This is the accurate way of finding but yeah in wireshark that can be seen just at the heading Address Resolution Protocol **(request).**


*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
     37 9.021967   IntelCor_9b:57:ad  Broadcast          ARP         42 Who has 192.168.0.1? Tell 192.168.0.100
     38 9.024862   D-LinkIn_90:7c:89  IntelCor_9b:57:ad  ARP         42 192.168.0.1 is at 34:0a:33:90:7c:89
     39 9.071257   8.36.80.244        192.168.0.100      TLSv1.2   1454 Server Hello
     40 9.071594   8.36.80.244        192.168.0.100      TCP       1418 443 → 49764 [PSH, ACK] Seq=1401 Ack=207 Win=16800 Len=1364 [TCP segment of a reassembled PDU]
     41 9.071594   8.36.80.244        192.168.0.100      TLSv1.2    406 Certificate, Server Hello Done
     42 9.071839   192.168.0.100      8.36.80.244        TCP         54 49764 → 443 [ACK] Seq=207 Ack=3117 Win=64400 Len=0
     43 9.073512   192.168.0.100      8.36.80.244        TLSv1.2    396 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
     44 9.318374   8.36.80.244        192.168.0.100      TCP       1454 [TCP Out-Of-Order] 443 → 49764 [PSH, ACK] Seq=1 Ack=207 Win=16800 Len=1400
     45 9.318550   192.168.0.100      8.36.80.244        TCP         66 [TCP Dup ACK 42#1] 49764 → 443 [ACK] Seq=549 Ack=3117 Win=64400 Len=0 SLE=1 SRE=1401
     46 9.336558   8.36.80.244        192.168.0.100      TCP         54 443 → 49764 [ACK] Seq=3117 Ack=549 Win=19600 Len=0
     47 9.340211   8.36.80.244        192.168.0.100      TLSv1.2    129 Change Cipher Spec, Encrypted Handshake Message
     48 9.343428   192.168.0.100      8.36.80.244        TLSv1.2    299 Application Data
     49 9.343935   192.168.0.100      8.36.80.244        TLSv1.2    699 Application Data
     50 9.625312   8.36.80.244        192.168.0.100      TCP         54 443 → 49764 [ACK] Seq=3192 Ack=794 Win=19355 Len=0
     51 9.625312   8.36.80.244        192.168.0.100      TCP         54 443 → 49764 [ACK] Seq=3192 Ack=1439 Win=18710 Len=0
     52 9.628913   8.36.80.244        192.168.0.100      TLSv1.2    395 Application Data
     53 9.629205   192.168.0.100      8.36.80.244        TLSv1.2    107 Encrypted Alert
```

```
> Frame 38: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{C71882EB-D065-4C09-9633-98139BFF98E5}, id 0
v Ethernet II, Src: D-LinkIn_90:7c:89 (34:0a:33:90:7c:89), Dst: IntelCor_9b:57:ad (98:3b:8f:9b:57:ad)
  > Destination: IntelCor_9b:57:ad (98:3b:8f:9b:57:ad)
  > Source: D-LinkIn_90:7c:89 (34:0a:33:90:7c:89)
    Type: ARP (0x0806)
v Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: D-LinkIn_90:7c:89 (34:0a:33:90:7c:89)
    Sender IP address: 192.168.0.1
    Target MAC address: IntelCor_9b:57:ad (98:3b:8f:9b:57:ad)
    Target IP address: 192.168.0.100
```

```
0000  98 3b 8f 9b 57 ad 34 0a  33 90 7c 89 08 06 00 01   ·;··W·4· 3·|·····
0010  08 00 06 04 00 02 34 0a  33 90 7c 89 c0 a8 00 01   ······4· 3·|·····
0020  98 3b 8f 9b 57 ad c0 a8  00 64                     ·;··W··· ·d
```

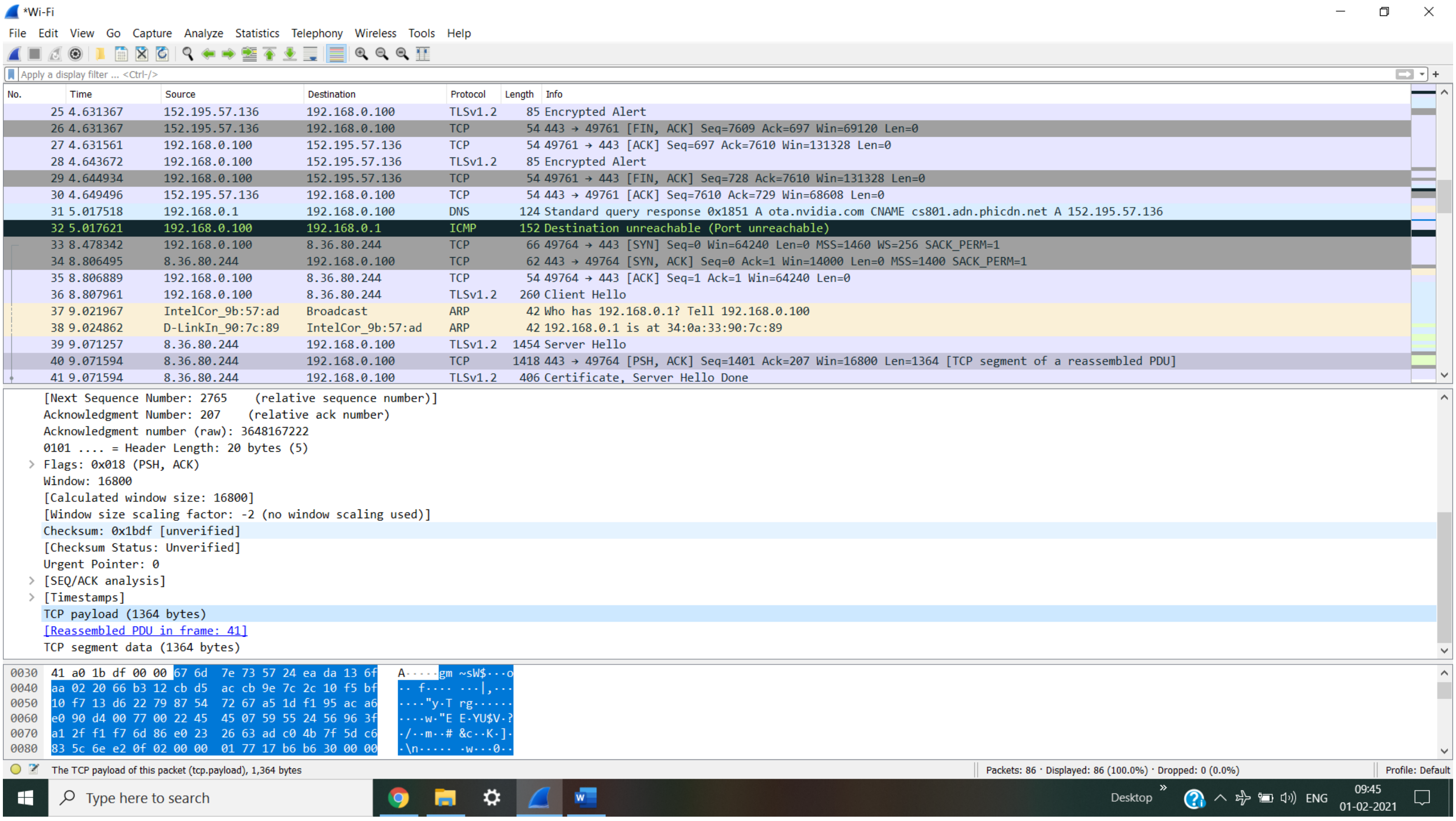
wireshark_Wi-FiN1LWX0.pcapng
Packets: 86 · Displayed: 86 (100.0%) · Dropped: 0 (0.0%)
Profile: Default
Type here to search
Desktop
ENG
09:25
01-02-2021

Fig 1.7 ARP reply packet

Here in the Address Resolution Protocol, **Opcode** field (Operation field) represents the type of the message. Here it’s value is 2 representing it as an ARP reply message. This is the accurate way of finding but yeah in wireshark that can be seen just at the heading Address Resolution Protocol **(reply).**

In short ARP request is initially created by the source system and if the destination protocol address (IP address) matches with any of the system then an ARP reply is sent to the source system giving MAC address of that system.

d)


*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
     25 4.631367   152.195.57.136    192.168.0.100     TLSv1.2     85 Encrypted Alert
     26 4.631367   152.195.57.136    192.168.0.100     TCP         54 443 → 49761 [FIN, ACK] Seq=7609 Ack=697 Win=69120 Len=0
     27 4.631561   192.168.0.100     152.195.57.136    TCP         54 49761 → 443 [ACK] Seq=697 Ack=7610 Win=131328 Len=0
     28 4.643672   192.168.0.100     152.195.57.136    TLSv1.2     85 Encrypted Alert
     29 4.644934   192.168.0.100     152.195.57.136    TCP         54 49761 → 443 [FIN, ACK] Seq=728 Ack=7610 Win=131328 Len=0
     30 4.649496   152.195.57.136    192.168.0.100     TCP         54 443 → 49761 [ACK] Seq=7610 Ack=729 Win=68608 Len=0
     31 5.017518   192.168.0.1       192.168.0.100     DNS        124 Standard query response 0x1851 A ota.nvidia.com CNAME cs801.adn.phicdn.net A 152.195.57.136
     32 5.017621   192.168.0.100     192.168.0.1       ICMP       152 Destination unreachable (Port unreachable)
     33 8.478342   192.168.0.100     8.36.80.244       TCP         66 49764 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
     34 8.806495   8.36.80.244       192.168.0.100     TCP         62 443 → 49764 [SYN, ACK] Seq=0 Ack=1 Win=14000 Len=0 MSS=1400 SACK_PERM=1
     35 8.806889   192.168.0.100     8.36.80.244       TCP         54 49764 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
     36 8.807961   192.168.0.100     8.36.80.244       TLSv1.2    260 Client Hello
     37 9.021967   IntelCor_9b:57:ad Broadcast         ARP         42 Who has 192.168.0.1? Tell 192.168.0.100
     38 9.024862   D-LinkIn_90:7c:89 IntelCor_9b:57:ad ARP         42 192.168.0.1 is at 34:0a:33:90:7c:89
     39 9.071257   8.36.80.244       192.168.0.100     TLSv1.2   1454 Server Hello
     40 9.071594   8.36.80.244       192.168.0.100     TCP       1418 443 → 49764 [PSH, ACK] Seq=1401 Ack=207 Win=16800 Len=1364 [TCP segment of a reassembled PDU]
     41 9.071594   8.36.80.244       192.168.0.100     TLSv1.2    406 Certificate, Server Hello Done
```

```
    [Next Sequence Number: 2765    (relative sequence number)]
    Acknowledgment Number: 207    (relative ack number)
    Acknowledgment number (raw): 3648167222
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window: 16800
    [Calculated window size: 16800]
    [Window size scaling factor: -2 (no window scaling used)]
    Checksum: 0x1bdf [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [SEQ/ACK analysis]
  > [Timestamps]
    TCP payload (1364 bytes)
    [Reassembled PDU in frame: 41]
    TCP segment data (1364 bytes)
```

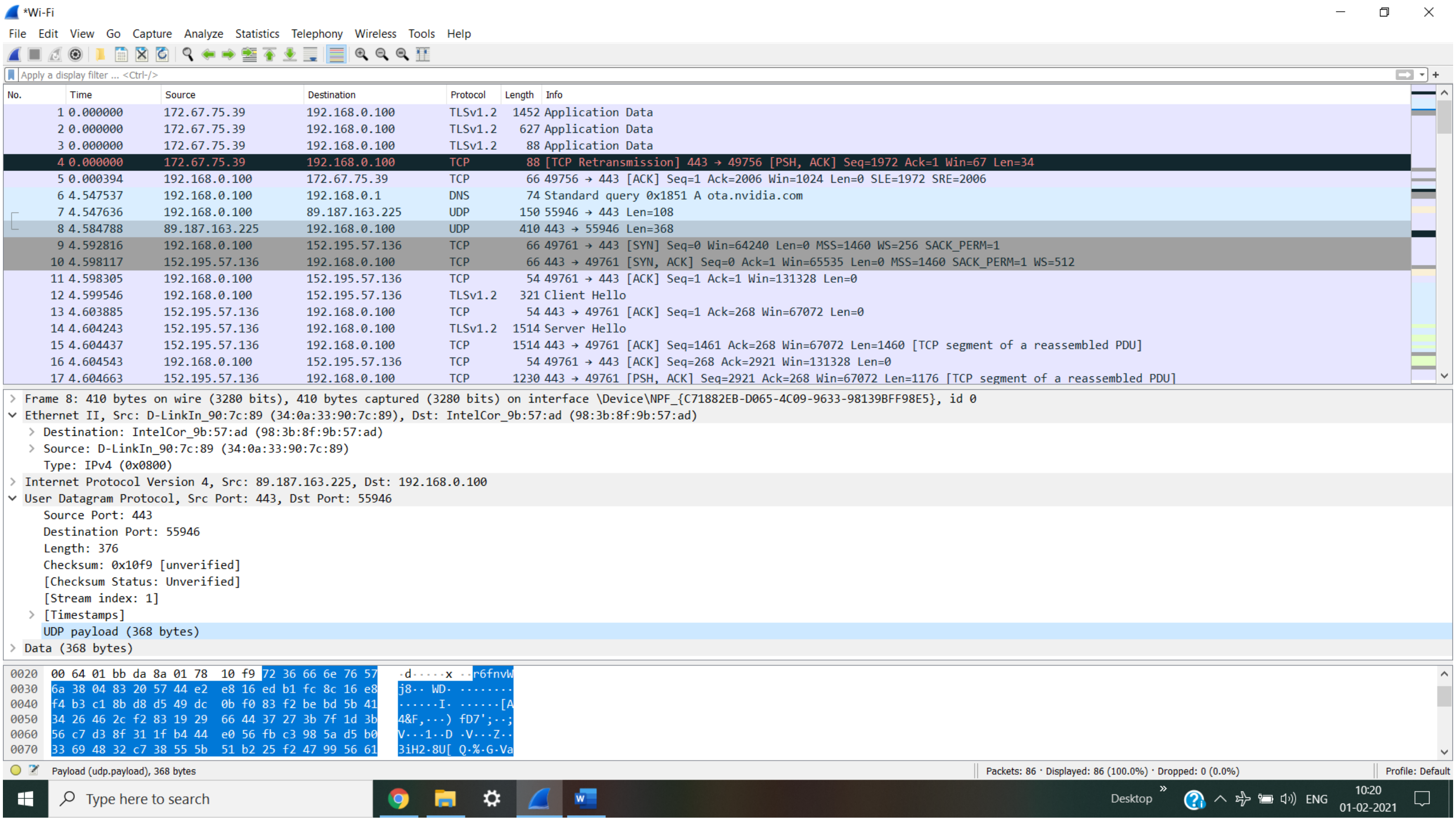
```
0030  41 a0 1b df 00 00 67 6d  7e 73 57 24 ea da 13 6f   A·····gm ~sW$···o
0040  aa 02 20 66 b3 12 cb d5  ac cb 9e 7c 2c 10 f5 bf   ·· f···· ···|,···
0050  10 f7 13 d6 22 79 87 54  72 67 a5 1d f1 95 ac a6   ····"y·T rg······
0060  e0 90 d4 00 77 00 22 45  45 07 59 55 24 56 96 3f   ····w·"E E·YU$V·?
0070  a1 2f f1 f7 6d 86 e0 23  26 63 ad c0 4b 7f 5d c6   ·/··m··# &c··K·]·
0080  83 5c 6e e2 0f 02 00 00  01 77 17 b6 b6 30 00 00   ·\n····· ·w···0··
```

The TCP payload of this packet (tcp.payload), 1,364 bytes | Packets: 86 · Displayed: 86 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

Fig 1.8 Payload of a TCP packet

Payload for an IP packet is the total encapsulated data received from its previous layer. In packet transmission from each layer, the packet includes both the header information and the payload which is received as packet from its previous layer. The header identifies the meta data about the source and destination of the packet, while the actual data is referred to as the payload. Because header information is only used in transmission process, it is stripped from the packet when it reaches its destination. Therefore, the payload is the actual data that is received by the destination system. For an IP packet payload can sometimes be zero since IP packets can be transferred without any actual data. In wireshark it clearly represents the length of the packet and if it's non zero then there is a payload being transmitted.

In the above figure it shows TCP payload (1364 bytes). Data segments from the transport layer are divided into packets and this encapsulated segment is IP payload.


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Type here to search
Desktop
ENG
10:20
01-02-2021

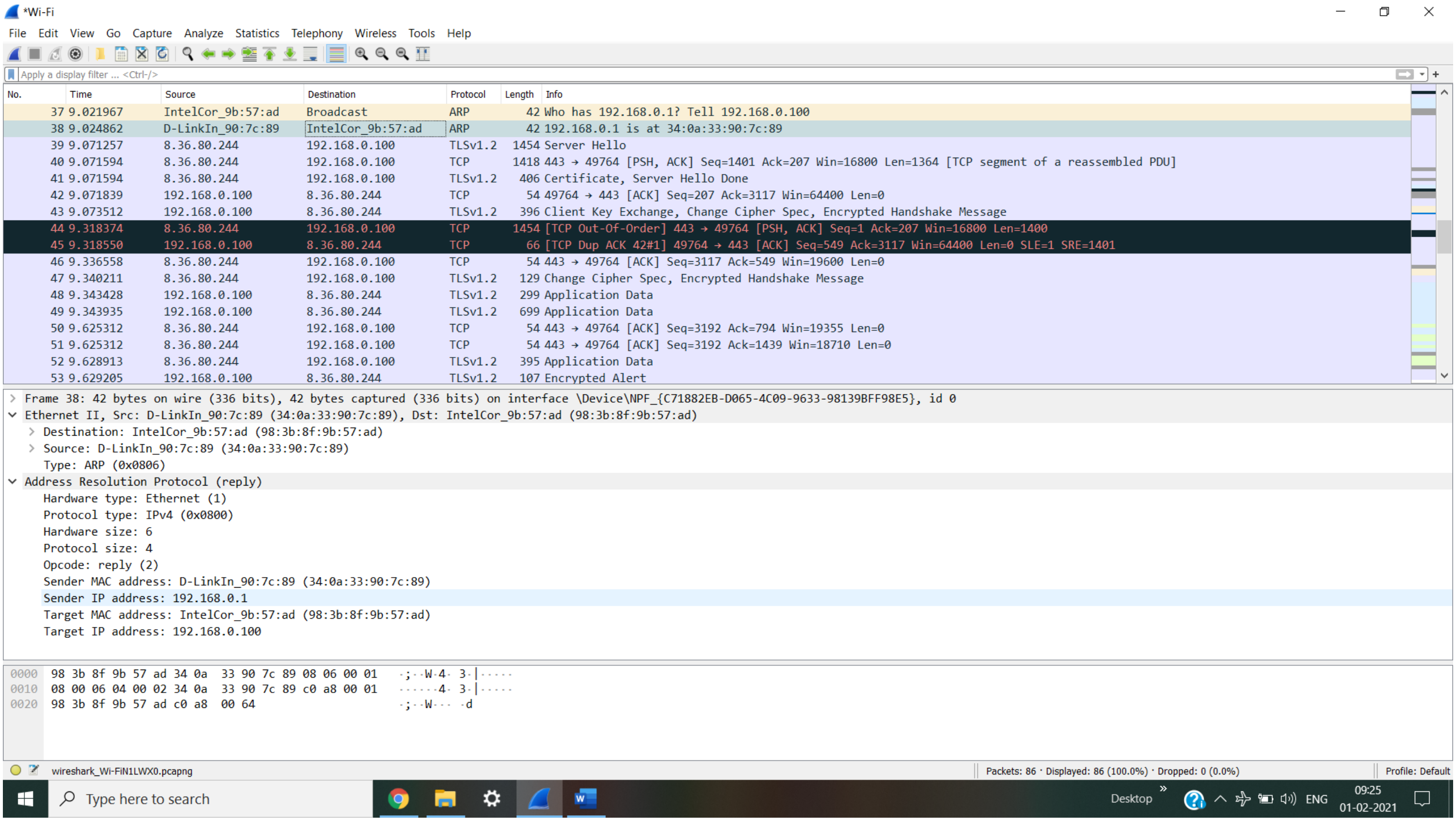
```
No.   Time       Source            Destination      Protocol  Length  Info
    1 0.000000   172.67.75.39      192.168.0.100    TLSv1.2   1452 Application Data
    2 0.000000   172.67.75.39      192.168.0.100    TLSv1.2    627 Application Data
    3 0.000000   172.67.75.39      192.168.0.100    TLSv1.2     88 Application Data
    4 0.000000   172.67.75.39      192.168.0.100    TCP         88 [TCP Retransmission] 443 → 49756 [PSH, ACK] Seq=1972 Ack=1 Win=67 Len=34
    5 0.000394   192.168.0.100     172.67.75.39     TCP         66 49756 → 443 [ACK] Seq=1 Ack=2006 Win=1024 Len=0 SLE=1972 SRE=2006
    6 4.547537   192.168.0.100     192.168.0.1      DNS         74 Standard query 0x1851 A ota.nvidia.com
    7 4.547636   192.168.0.100     89.187.163.225   UDP        150 55946 → 443 Len=108
    8 4.584788   89.187.163.225    192.168.0.100    UDP        410 443 → 55946 Len=368
    9 4.592816   192.168.0.100     152.195.57.136   TCP         66 49761 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
   10 4.598117   152.195.57.136    192.168.0.100    TCP         66 443 → 49761 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 SACK_PERM=1 WS=512
   11 4.598305   192.168.0.100     152.195.57.136   TCP         54 49761 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0
   12 4.599546   192.168.0.100     152.195.57.136   TLSv1.2    321 Client Hello
   13 4.603885   152.195.57.136    192.168.0.100    TCP         54 443 → 49761 [ACK] Seq=1 Ack=268 Win=67072 Len=0
   14 4.604243   152.195.57.136    192.168.0.100    TLSv1.2   1514 Server Hello
   15 4.604437   152.195.57.136    192.168.0.100    TCP       1514 443 → 49761 [ACK] Seq=1461 Ack=268 Win=67072 Len=1460 [TCP segment of a reassembled PDU]
   16 4.604543   192.168.0.100     152.195.57.136   TCP         54 49761 → 443 [ACK] Seq=268 Ack=2921 Win=131328 Len=0
   17 4.604663   152.195.57.136    192.168.0.100    TCP       1230 443 → 49761 [PSH, ACK] Seq=2921 Ack=268 Win=67072 Len=1176 [TCP segment of a reassembled PDU]
```

```
> Frame 8: 410 bytes on wire (3280 bits), 410 bytes captured (3280 bits) on interface \Device\NPF_{C71882EB-D065-4C09-9633-98139BFF98E5}, id 0
v Ethernet II, Src: D-LinkIn_90:7c:89 (34:0a:33:90:7c:89), Dst: IntelCor_9b:57:ad (98:3b:8f:9b:57:ad)
  > Destination: IntelCor_9b:57:ad (98:3b:8f:9b:57:ad)
  > Source: D-LinkIn_90:7c:89 (34:0a:33:90:7c:89)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 89.187.163.225, Dst: 192.168.0.100
v User Datagram Protocol, Src Port: 443, Dst Port: 55946
    Source Port: 443
    Destination Port: 55946
    Length: 376
    Checksum: 0x10f9 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
  > [Timestamps]
    UDP payload (368 bytes)
> Data (368 bytes)
```

```
0020  00 64 01 bb da 8a 01 78  10 f9 72 36 66 6e 76 57   ·d·····x ··r6fnvW
0030  6a 38 04 83 20 57 44 e2  e8 16 ed b1 fc 8c 16 e8   j8·· WD· ········
0040  f4 b3 c1 8b d8 d5 49 dc  0b f0 83 f2 be bd 5b 41   ······I· ······[A
0050  34 26 46 2c f2 83 19 29  66 44 37 27 3b 7f 1d 3b   4&F,···) fD7';··;
0060  56 c7 d3 8f 31 1f b4 44  e0 56 fb c3 98 5a d5 b0   V···1··D ·V···Z··
0070  33 69 48 32 c7 38 55 5b  51 b2 25 f2 47 99 56 61   3iH2·8U[ Q·%·G·Va
```

Payload (udp.payload), 368 bytes | Packets: 86 · Displayed: 86 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

Fig 1.9 Payload of a UDP Packet


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Type here to search
Desktop
ENG
09:25
01-02-2021

```
No.   Time       Source              Destination         Protocol  Length  Info
   37 9.021967   IntelCor_9b:57:ad   Broadcast           ARP         42 Who has 192.168.0.1? Tell 192.168.0.100
   38 9.024862   D-LinkIn_90:7c:89   IntelCor_9b:57:ad   ARP         42 192.168.0.1 is at 34:0a:33:90:7c:89
   39 9.071257   8.36.80.244         192.168.0.100       TLSv1.2   1454 Server Hello
   40 9.071594   8.36.80.244         192.168.0.100       TCP       1418 443 → 49764 [PSH, ACK] Seq=1401 Ack=207 Win=16800 Len=1364 [TCP segment of a reassembled PDU]
   41 9.071594   8.36.80.244         192.168.0.100       TLSv1.2    406 Certificate, Server Hello Done
   42 9.071839   192.168.0.100       8.36.80.244         TCP         54 49764 → 443 [ACK] Seq=207 Ack=3117 Win=64400 Len=0
   43 9.073512   192.168.0.100       8.36.80.244         TLSv1.2    396 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
   44 9.318374   8.36.80.244         192.168.0.100       TCP       1454 [TCP Out-Of-Order] 443 → 49764 [PSH, ACK] Seq=1 Ack=207 Win=16800 Len=1400
   45 9.318550   192.168.0.100       8.36.80.244         TCP         66 [TCP Dup ACK 42#1] 49764 → 443 [ACK] Seq=549 Ack=3117 Win=64400 Len=0 SLE=1 SRE=1401
   46 9.336558   8.36.80.244         192.168.0.100       TCP         54 443 → 49764 [ACK] Seq=3117 Ack=549 Win=19600 Len=0
   47 9.340211   8.36.80.244         192.168.0.100       TLSv1.2    129 Change Cipher Spec, Encrypted Handshake Message
   48 9.343428   192.168.0.100       8.36.80.244         TLSv1.2    299 Application Data
   49 9.343935   192.168.0.100       8.36.80.244         TLSv1.2    699 Application Data
   50 9.625312   8.36.80.244         192.168.0.100       TCP         54 443 → 49764 [ACK] Seq=3192 Ack=794 Win=19355 Len=0
   51 9.625312   8.36.80.244         192.168.0.100       TCP         54 443 → 49764 [ACK] Seq=3192 Ack=1439 Win=18710 Len=0
   52 9.628913   8.36.80.244         192.168.0.100       TLSv1.2    395 Application Data
   53 9.629205   192.168.0.100       8.36.80.244         TLSv1.2    107 Encrypted Alert
```

```
> Frame 38: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{C71882EB-D065-4C09-9633-98139BFF98E5}, id 0
v Ethernet II, Src: D-LinkIn_90:7c:89 (34:0a:33:90:7c:89), Dst: IntelCor_9b:57:ad (98:3b:8f:9b:57:ad)
  > Destination: IntelCor_9b:57:ad (98:3b:8f:9b:57:ad)
  > Source: D-LinkIn_90:7c:89 (34:0a:33:90:7c:89)
    Type: ARP (0x0806)
v Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: D-LinkIn_90:7c:89 (34:0a:33:90:7c:89)
    Sender IP address: 192.168.0.1
    Target MAC address: IntelCor_9b:57:ad (98:3b:8f:9b:57:ad)
    Target IP address: 192.168.0.100
```

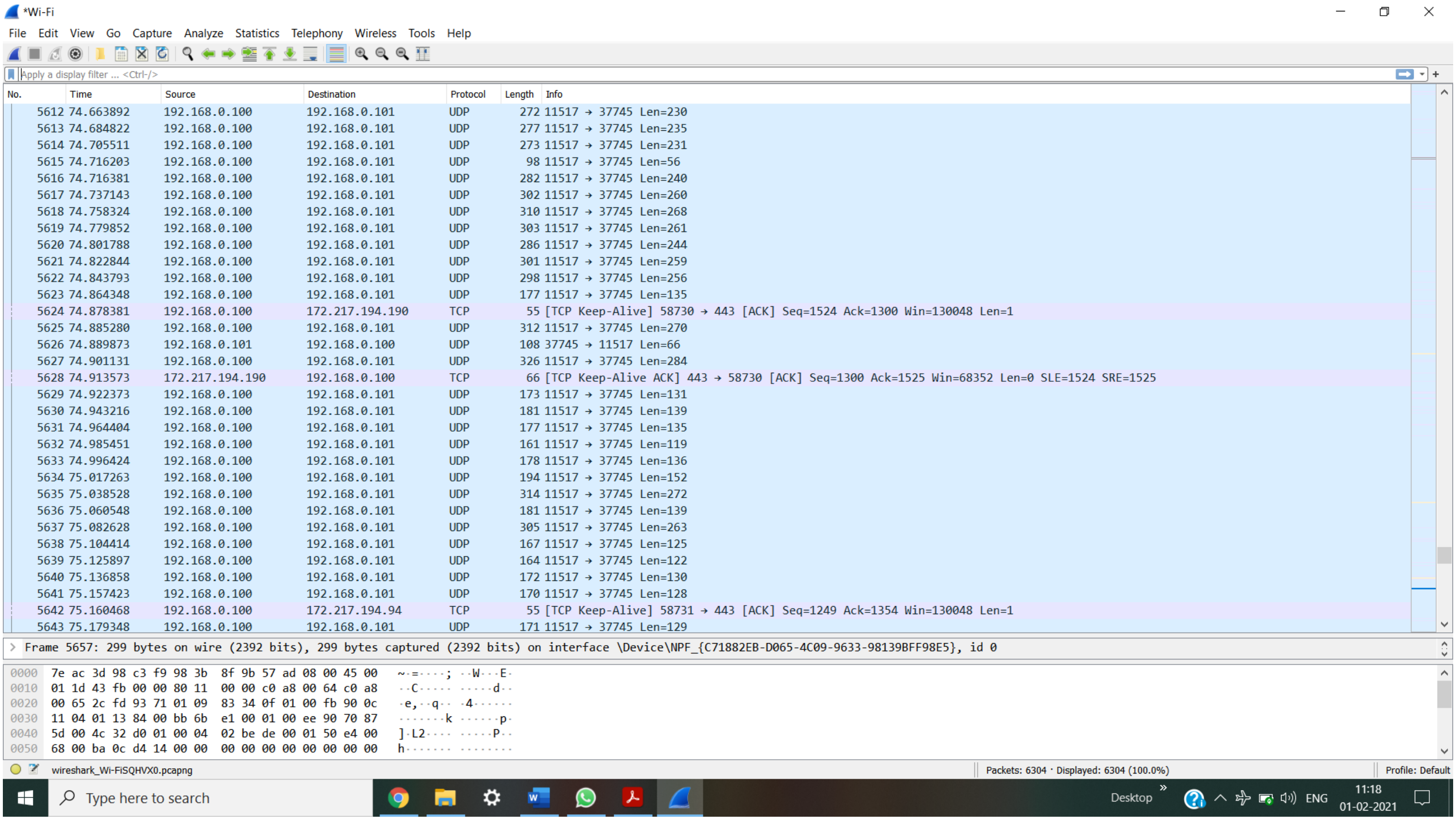
```
0000  98 3b 8f 9b 57 ad 34 0a  33 90 7c 89 08 06 00 01   ·;··W·4· 3·|·····
0010  08 00 06 04 00 02 34 0a  33 90 7c 89 c0 a8 00 01   ······4· 3·|·····
0020  98 3b 8f 9b 57 ad c0 a8  00 64                     ·;··W··· ·d
```

wireshark_Wi-FiN1LWX0.pcapng | Packets: 86 · Displayed: 86 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

Fig 2.0 Payload of an ARP packet

If we follow the previous terminology, we have to say that payload for an ARP packet as zero. Definition of payload slightly changes in case of an ARP packet since there is no actual data being sent and it is just a request of MAC address of a system with a given IP address. So, for this the payload of the packet is defined to consists of four addresses, the Hardware (MAC) addresses and the protocol (IP) addresses of the sender and the receiver hosts. In the above figure all the four addresses are visible under ARP protocol.

e)


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Type here to search
Desktop
ENG
11:18
01-02-2021

```
No.   Time      Source          Destination      Protocol Length Info
 5612 74.663892 192.168.0.100   192.168.0.101    UDP      272 11517 → 37745 Len=230
 5613 74.684822 192.168.0.100   192.168.0.101    UDP      277 11517 → 37745 Len=235
 5614 74.705511 192.168.0.100   192.168.0.101    UDP      273 11517 → 37745 Len=231
 5615 74.716203 192.168.0.100   192.168.0.101    UDP       98 11517 → 37745 Len=56
 5616 74.716381 192.168.0.100   192.168.0.101    UDP      282 11517 → 37745 Len=240
 5617 74.737143 192.168.0.100   192.168.0.101    UDP      302 11517 → 37745 Len=260
 5618 74.758324 192.168.0.100   192.168.0.101    UDP      310 11517 → 37745 Len=268
 5619 74.779852 192.168.0.100   192.168.0.101    UDP      303 11517 → 37745 Len=261
 5620 74.801788 192.168.0.100   192.168.0.101    UDP      286 11517 → 37745 Len=244
 5621 74.822844 192.168.0.100   192.168.0.101    UDP      301 11517 → 37745 Len=259
 5622 74.843793 192.168.0.100   192.168.0.101    UDP      298 11517 → 37745 Len=256
 5623 74.864348 192.168.0.100   192.168.0.101    UDP      177 11517 → 37745 Len=135
 5624 74.878381 192.168.0.100   172.217.194.190  TCP       55 [TCP Keep-Alive] 58730 → 443 [ACK] Seq=1524 Ack=1300 Win=130048 Len=1
 5625 74.885280 192.168.0.100   192.168.0.101    UDP      312 11517 → 37745 Len=270
 5626 74.889873 192.168.0.101   192.168.0.100    UDP      108 37745 → 11517 Len=66
 5627 74.901131 192.168.0.100   192.168.0.101    UDP      326 11517 → 37745 Len=284
 5628 74.913573 172.217.194.190 192.168.0.100    TCP       66 [TCP Keep-Alive ACK] 443 → 58730 [ACK] Seq=1300 Ack=1525 Win=68352 Len=0 SLE=1524 SRE=1525
 5629 74.922373 192.168.0.100   192.168.0.101    UDP      173 11517 → 37745 Len=131
 5630 74.943216 192.168.0.100   192.168.0.101    UDP      181 11517 → 37745 Len=139
 5631 74.964404 192.168.0.100   192.168.0.101    UDP      177 11517 → 37745 Len=135
 5632 74.985451 192.168.0.100   192.168.0.101    UDP      161 11517 → 37745 Len=119
 5633 74.996424 192.168.0.100   192.168.0.101    UDP      178 11517 → 37745 Len=136
 5634 75.017263 192.168.0.100   192.168.0.101    UDP      194 11517 → 37745 Len=152
 5635 75.038528 192.168.0.100   192.168.0.101    UDP      314 11517 → 37745 Len=272
 5636 75.060548 192.168.0.100   192.168.0.101    UDP      181 11517 → 37745 Len=139
 5637 75.082628 192.168.0.100   192.168.0.101    UDP      305 11517 → 37745 Len=263
 5638 75.104414 192.168.0.100   192.168.0.101    UDP      167 11517 → 37745 Len=125
 5639 75.125897 192.168.0.100   192.168.0.101    UDP      164 11517 → 37745 Len=122
 5640 75.136858 192.168.0.100   192.168.0.101    UDP      172 11517 → 37745 Len=130
 5641 75.157423 192.168.0.100   192.168.0.101    UDP      170 11517 → 37745 Len=128
 5642 75.160468 192.168.0.100   172.217.194.94   TCP       55 [TCP Keep-Alive] 58731 → 443 [ACK] Seq=1249 Ack=1354 Win=130048 Len=1
 5643 75.179348 192.168.0.100   192.168.0.101    UDP      171 11517 → 37745 Len=129

> Frame 5657: 299 bytes on wire (2392 bits), 299 bytes captured (2392 bits) on interface \Device\NPF_{C71882EB-D065-4C09-9633-98139BFF98E5}, id 0

0000  7e ac 3d 98 c3 f9 98 3b  8f 9b 57 ad 08 00 45 00   ~·=····; ··W···E·
0010  01 1d 43 fb 00 00 80 11  00 00 c0 a8 00 64 c0 a8   ··C·····  ·····d··
0020  00 65 2c fd 93 71 01 09  83 34 0f 01 00 fb 90 0c   ·e,··q·· ·4······
0030  11 04 01 13 84 00 bb 6b  e1 00 01 00 ee 90 70 87   ·······k ······p·
0040  5d 00 4c 32 d0 01 00 04  02 be de 00 01 50 e4 00   ]·L2···· ·····P··
0050  68 00 ba 0c d4 14 00 00  00 00 00 00 00 00 00 00   h······· ········

wireshark_Wi-FiSQHVX0.pcapng          Packets: 6304 · Displayed: 6304 (100.0%)          Profile: Default
```

Fig 2.1 TCP, UDP packets are shown for a Zoom meeting

Transport layer protocols in Skype and zoom or any other media streaming services are both UDP and TCP.

UDP protocol is used for video and audio streaming because here speed of the data is more important than the accurate delivery of the entire content since we need the live data information. And as UDP doesn’t have such extensive error checking mechanism and also it doesn’t care if the packet is received at receiver’s end, it’s relatively faster.

TCP (Transmission Control Protocol) is used for chat section since messages are important to be delivered completely, maintaining the session details like checking if the user is currently logged in or not and also to check connection status whether it is connected to the network or displaying signal strength and also some of the other details like participants list etc.,