KALINGA INSTITUTE OF
INDUSTRIAL TECHNOLOGY (KIIT)

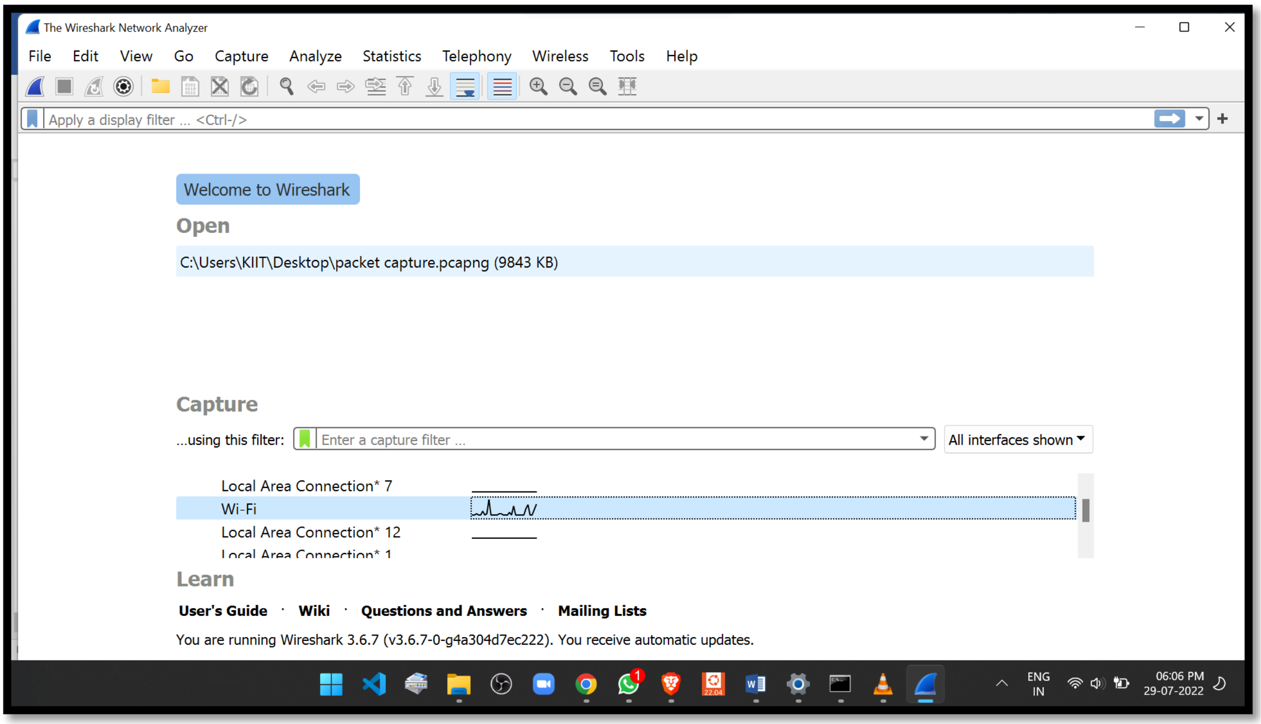
Deemed to be University U/S 3 of UGC Act, 1956

CN LAB-2

WIRESHARK

- Name :HITU RAJ
- Roll no. :2005025
- Branch :CSE-4

1. Screenshot of Wireshark application.



Open

C:\Users\KIIT\Desktop\packet capture.pcapng (9843 KB)

Capture

…using this filter: Enter a capture filter … All interfaces shown

Local Area Connection* 7
Wi-Fi
Local Area Connection* 12
Local Area Connection* 1

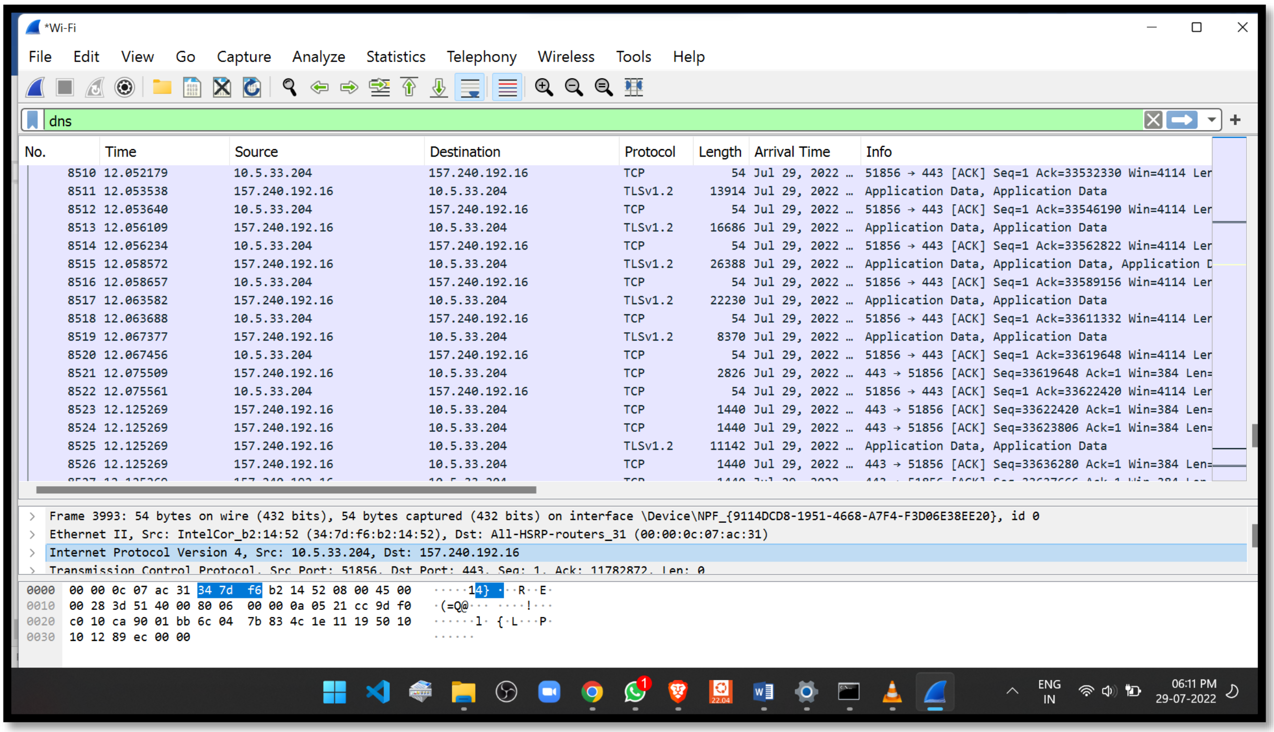
Learn

User's Guide · Wiki · Questions and Answers · Mailing Lists

You are running Wireshark 3.6.7 (v3.6.7-0-g4a304d7ec222). You receive automatic updates.

2. Use "DNS" as a filter.

KIIT WIFI



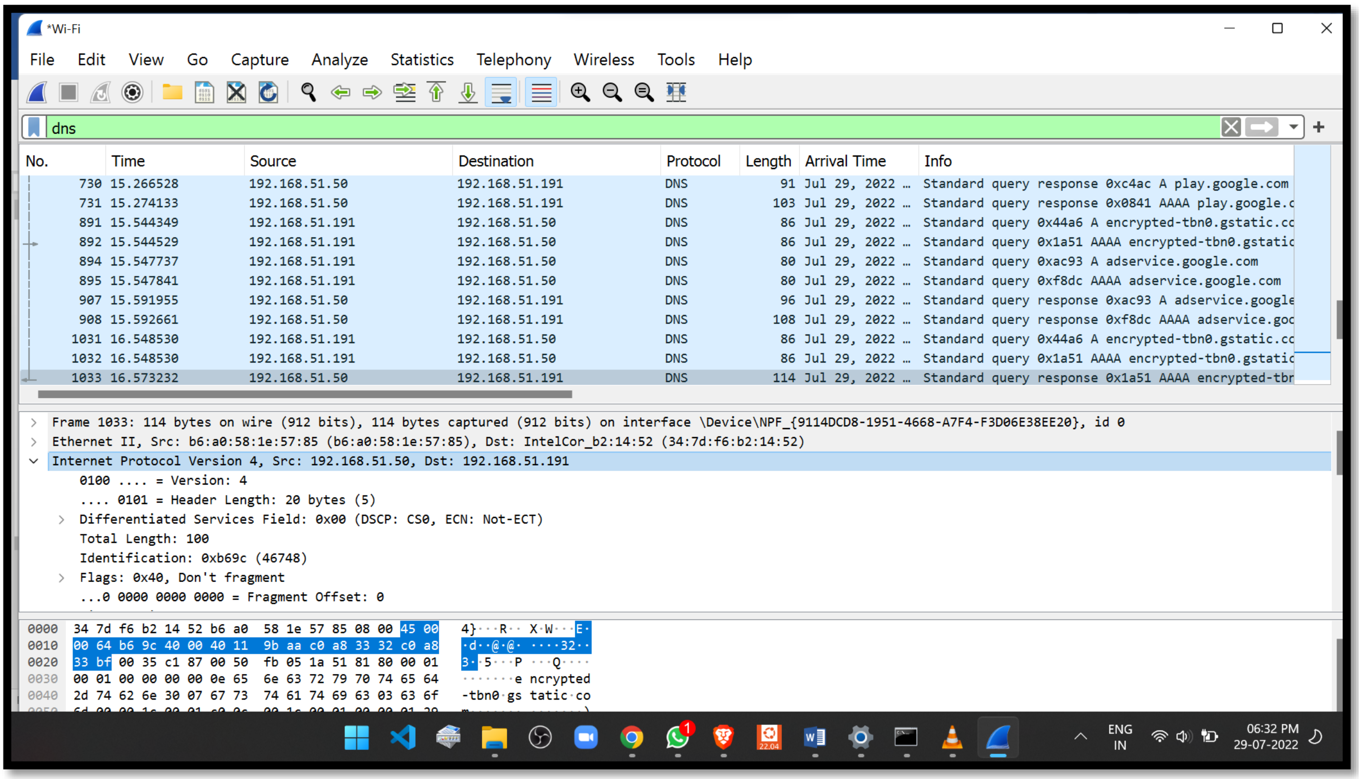
dns

```
No.       Time        Source           Destination      Protocol  Length Arrival Time      Info
    8510 12.052179   10.5.33.204      157.240.192.16   TCP           54 Jul 29, 2022 … 51856 → 443 [ACK] Seq=1 Ack=33532330 Win=4114 Ler
    8511 12.053538   157.240.192.16   10.5.33.204      TLSv1.2    13914 Jul 29, 2022 … Application Data, Application Data
    8512 12.053640   10.5.33.204      157.240.192.16   TCP           54 Jul 29, 2022 … 51856 → 443 [ACK] Seq=1 Ack=33546190 Win=4114 Ler
    8513 12.056109   157.240.192.16   10.5.33.204      TLSv1.2    16686 Jul 29, 2022 … Application Data, Application Data
    8514 12.056234   10.5.33.204      157.240.192.16   TCP           54 Jul 29, 2022 … 51856 → 443 [ACK] Seq=1 Ack=33562822 Win=4114 Ler
    8515 12.058572   157.240.192.16   10.5.33.204      TLSv1.2    26388 Jul 29, 2022 … Application Data, Application Data, Application D
    8516 12.058657   10.5.33.204      157.240.192.16   TCP           54 Jul 29, 2022 … 51856 → 443 [ACK] Seq=1 Ack=33589156 Win=4114 Ler
    8517 12.063582   157.240.192.16   10.5.33.204      TLSv1.2    22230 Jul 29, 2022 … Application Data, Application Data
    8518 12.063688   10.5.33.204      157.240.192.16   TCP           54 Jul 29, 2022 … 51856 → 443 [ACK] Seq=1 Ack=33611332 Win=4114 Ler
    8519 12.067377   157.240.192.16   10.5.33.204      TLSv1.2     8370 Jul 29, 2022 … Application Data, Application Data
    8520 12.067456   10.5.33.204      157.240.192.16   TCP           54 Jul 29, 2022 … 51856 → 443 [ACK] Seq=1 Ack=33619648 Win=4114 Ler
    8521 12.075509   157.240.192.16   10.5.33.204      TCP         2826 Jul 29, 2022 … 443 → 51856 [ACK] Seq=33619648 Ack=1 Win=384 Len=
    8522 12.075561   10.5.33.204      157.240.192.16   TCP           54 Jul 29, 2022 … 51856 → 443 [ACK] Seq=1 Ack=33622420 Win=4114 Ler
    8523 12.125269   157.240.192.16   10.5.33.204      TCP         1440 Jul 29, 2022 … 443 → 51856 [ACK] Seq=33622420 Ack=1 Win=384 Len=
    8524 12.125269   157.240.192.16   10.5.33.204      TCP         1440 Jul 29, 2022 … 443 → 51856 [ACK] Seq=33623806 Ack=1 Win=384 Len=
    8525 12.125269   157.240.192.16   10.5.33.204      TLSv1.2    11142 Jul 29, 2022 … Application Data, Application Data
    8526 12.125269   157.240.192.16   10.5.33.204      TCP         1440 Jul 29, 2022 … 443 → 51856 [ACK] Seq=33636280 Ack=1 Win=384 Len=
```

```
> Frame 3993: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{9114DCD8-1951-4668-A7F4-F3D06E38EE20}, id 0
> Ethernet II, Src: IntelCor_b2:14:52 (34:7d:f6:b2:14:52), Dst: All-HSRP-routers_31 (00:00:0c:07:ac:31)
> Internet Protocol Version 4, Src: 10.5.33.204, Dst: 157.240.192.16
> Transmission Control Protocol, Src Port: 51856, Dst Port: 443, Seq: 1, Ack: 11782872, Len: 0
```

```
0000  00 00 0c 07 ac 31 34 7d  f6 b2 14 52 08 00 45 00   ·····14}···R··E·
0010  00 28 3d 51 40 00 80 06  00 00 0a 05 21 cc 9d f0   ·(=Q@··· ····!···
0020  c0 10 ca 90 01 bb 6c 04  7b 83 4c 1e 11 19 50 10   ······l· {·L···P·
0030  10 12 89 ec 00 00                                  ······
```

HOTSPOT


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ENG
IN
06:32 PM
29-07-2022

```
dns
```

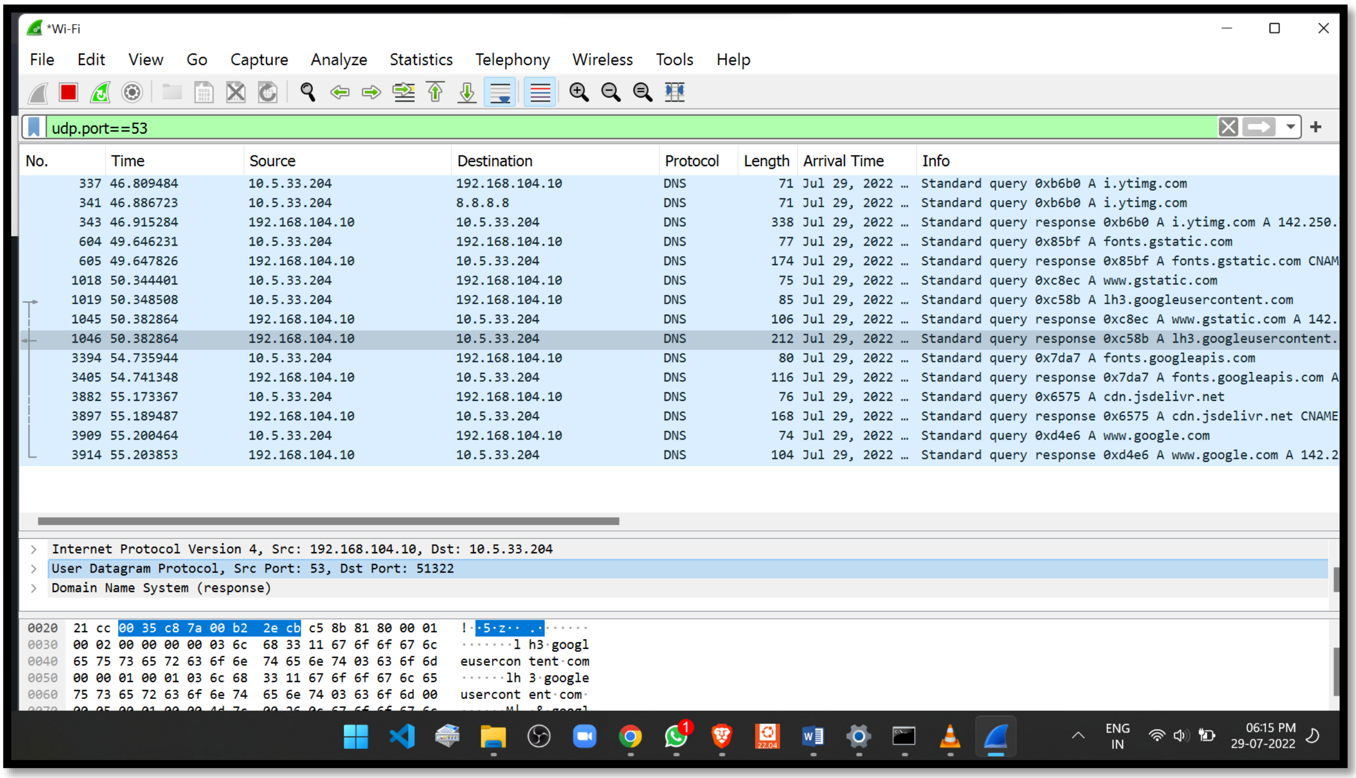
```
No.   Time        Source          Destination     Protocol Length Arrival Time      Info
  730 15.266528   192.168.51.50   192.168.51.191  DNS         91 Jul 29, 2022 … Standard query response 0xc4ac A play.google.com
  731 15.274133   192.168.51.50   192.168.51.191  DNS        103 Jul 29, 2022 … Standard query response 0x0841 AAAA play.google.c
  891 15.544349   192.168.51.191  192.168.51.50   DNS         86 Jul 29, 2022 … Standard query 0x44a6 A encrypted-tbn0.gstatic.cc
  892 15.544529   192.168.51.191  192.168.51.50   DNS         86 Jul 29, 2022 … Standard query 0x1a51 AAAA encrypted-tbn0.gstatic
  894 15.547737   192.168.51.191  192.168.51.50   DNS         80 Jul 29, 2022 … Standard query 0xac93 A adservice.google.com
  895 15.547841   192.168.51.191  192.168.51.50   DNS         80 Jul 29, 2022 … Standard query 0xf8dc AAAA adservice.google.com
  907 15.591955   192.168.51.50   192.168.51.191  DNS         96 Jul 29, 2022 … Standard query response 0xac93 A adservice.google
  908 15.592661   192.168.51.50   192.168.51.191  DNS        108 Jul 29, 2022 … Standard query response 0xf8dc AAAA adservice.goc
 1031 16.548530   192.168.51.191  192.168.51.50   DNS         86 Jul 29, 2022 … Standard query 0x44a6 A encrypted-tbn0.gstatic.cc
 1032 16.548530   192.168.51.191  192.168.51.50   DNS         86 Jul 29, 2022 … Standard query 0x1a51 AAAA encrypted-tbn0.gstatic
 1033 16.573232   192.168.51.50   192.168.51.191  DNS        114 Jul 29, 2022 … Standard query response 0x1a51 AAAA encrypted-tbr
```

```
> Frame 1033: 114 bytes on wire (912 bits), 114 bytes captured (912 bits) on interface \Device\NPF_{9114DCD8-1951-4668-A7F4-F3D06E38EE20}, id 0
> Ethernet II, Src: b6:a0:58:1e:57:85 (b6:a0:58:1e:57:85), Dst: IntelCor_b2:14:52 (34:7d:f6:b2:14:52)
v Internet Protocol Version 4, Src: 192.168.51.50, Dst: 192.168.51.191
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 100
    Identification: 0xb69c (46748)
  > Flags: 0x40, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
```

```
0000  34 7d f6 b2 14 52 b6 a0  58 1e 57 85 08 00 45 00   4}···R·· X·W···E·
0010  00 64 b6 9c 40 00 40 11  9b aa c0 a8 33 32 c0 a8   ·d··@·@· ····32··
0020  33 bf 00 35 c1 87 00 50  fb 05 1a 51 81 80 00 01   3··5···P ···Q····
0030  00 01 00 00 00 00 0e 65  6e 63 72 79 70 74 65 64   ·······e ncrypted
0040  2d 74 62 6e 30 07 67 73  74 61 74 69 63 03 63 6f   -tbn0·gs tatic·co
```

3.Use “port 53” as a filter.

KIIT WIFI


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ENG
IN
06:15 PM
29-07-2022

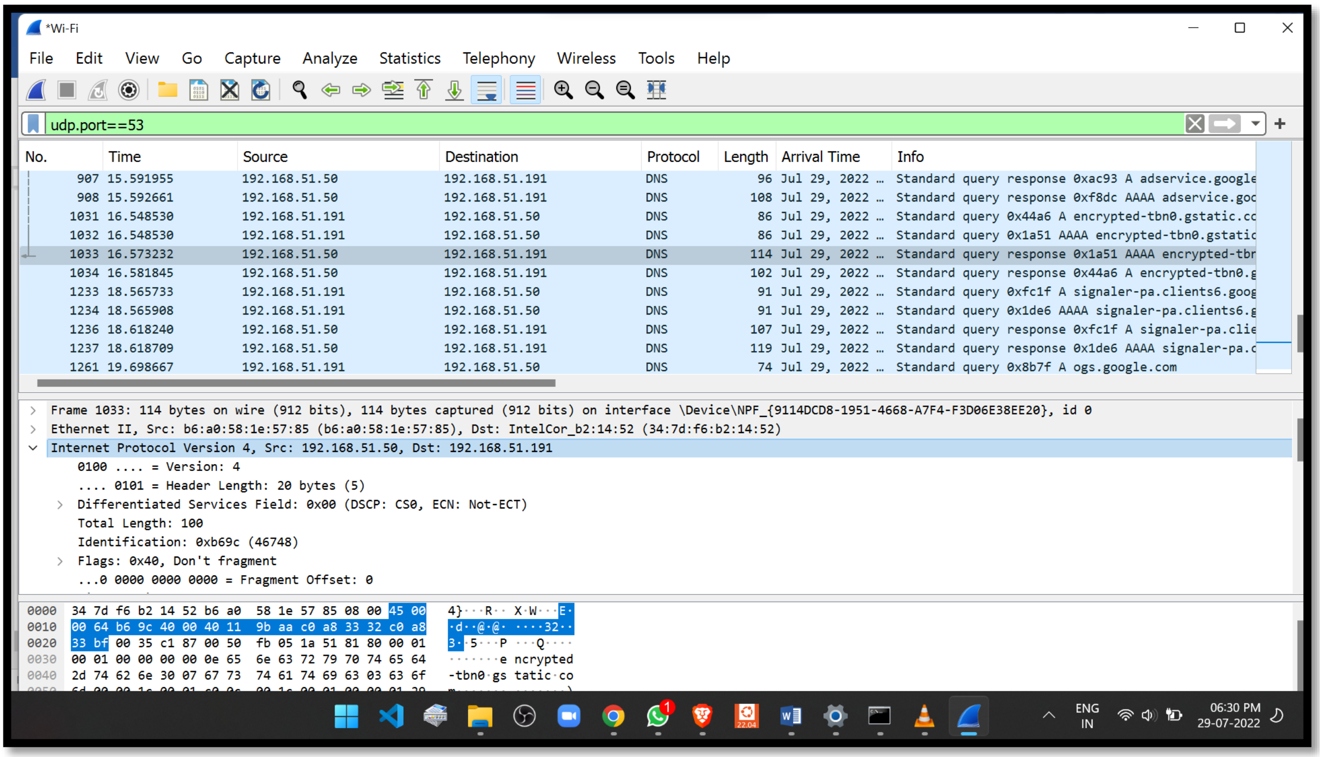
```
udp.port==53
```

```
No.   Time        Source          Destination     Protocol Length Arrival Time      Info
  337 46.809484   10.5.33.204     192.168.104.10  DNS         71 Jul 29, 2022 … Standard query 0xb6b0 A i.ytimg.com
  341 46.886723   10.5.33.204     8.8.8.8         DNS         71 Jul 29, 2022 … Standard query 0xb6b0 A i.ytimg.com
  343 46.915284   192.168.104.10  10.5.33.204     DNS        338 Jul 29, 2022 … Standard query response 0xb6b0 A i.ytimg.com A 142.250.
  604 49.646231   10.5.33.204     192.168.104.10  DNS         77 Jul 29, 2022 … Standard query 0x85bf A fonts.gstatic.com
  605 49.647826   192.168.104.10  10.5.33.204     DNS        174 Jul 29, 2022 … Standard query response 0x85bf A fonts.gstatic.com CNAM
 1018 50.344401   10.5.33.204     192.168.104.10  DNS         75 Jul 29, 2022 … Standard query 0xc8ec A www.gstatic.com
 1019 50.348508   10.5.33.204     192.168.104.10  DNS         85 Jul 29, 2022 … Standard query 0xc58b A lh3.googleusercontent.com
 1045 50.382864   192.168.104.10  10.5.33.204     DNS        106 Jul 29, 2022 … Standard query response 0xc8ec A www.gstatic.com A 142.
 1046 50.382864   192.168.104.10  10.5.33.204     DNS        212 Jul 29, 2022 … Standard query response 0xc58b A lh3.googleusercontent.
 3394 54.735944   10.5.33.204     192.168.104.10  DNS         80 Jul 29, 2022 … Standard query 0x7da7 A fonts.googleapis.com
 3405 54.741348   192.168.104.10  10.5.33.204     DNS        116 Jul 29, 2022 … Standard query response 0x7da7 A fonts.googleapis.com A
 3882 55.173367   10.5.33.204     192.168.104.10  DNS         76 Jul 29, 2022 … Standard query 0x6575 A cdn.jsdelivr.net
 3897 55.189487   192.168.104.10  10.5.33.204     DNS        168 Jul 29, 2022 … Standard query response 0x6575 A cdn.jsdelivr.net CNAME
 3909 55.200464   10.5.33.204     192.168.104.10  DNS         74 Jul 29, 2022 … Standard query 0xd4e6 A www.google.com
 3914 55.203853   192.168.104.10  10.5.33.204     DNS        104 Jul 29, 2022 … Standard query response 0xd4e6 A www.google.com A 142.2
```

```
> Internet Protocol Version 4, Src: 192.168.104.10, Dst: 10.5.33.204
> User Datagram Protocol, Src Port: 53, Dst Port: 51322
> Domain Name System (response)
```

```
0020  21 cc 00 35 c8 7a 00 b2  2e cb c5 8b 81 80 00 01   !··5·z·· .·······
0030  00 02 00 00 00 00 03 6c  68 33 11 67 6f 6f 67 6c   ·······l h3·googl
0040  65 75 73 65 72 63 6f 6e  74 65 6e 74 03 63 6f 6d   eusercon tent·com
0050  00 00 01 00 01 03 6c 68  33 11 67 6f 6f 67 6c 65   ······lh 3·google
0060  75 73 65 72 63 6f 6e 74  65 6e 74 03 63 6f 6d 00   usercont ent·com·
```

HOTSPOT



*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
udp.port==53

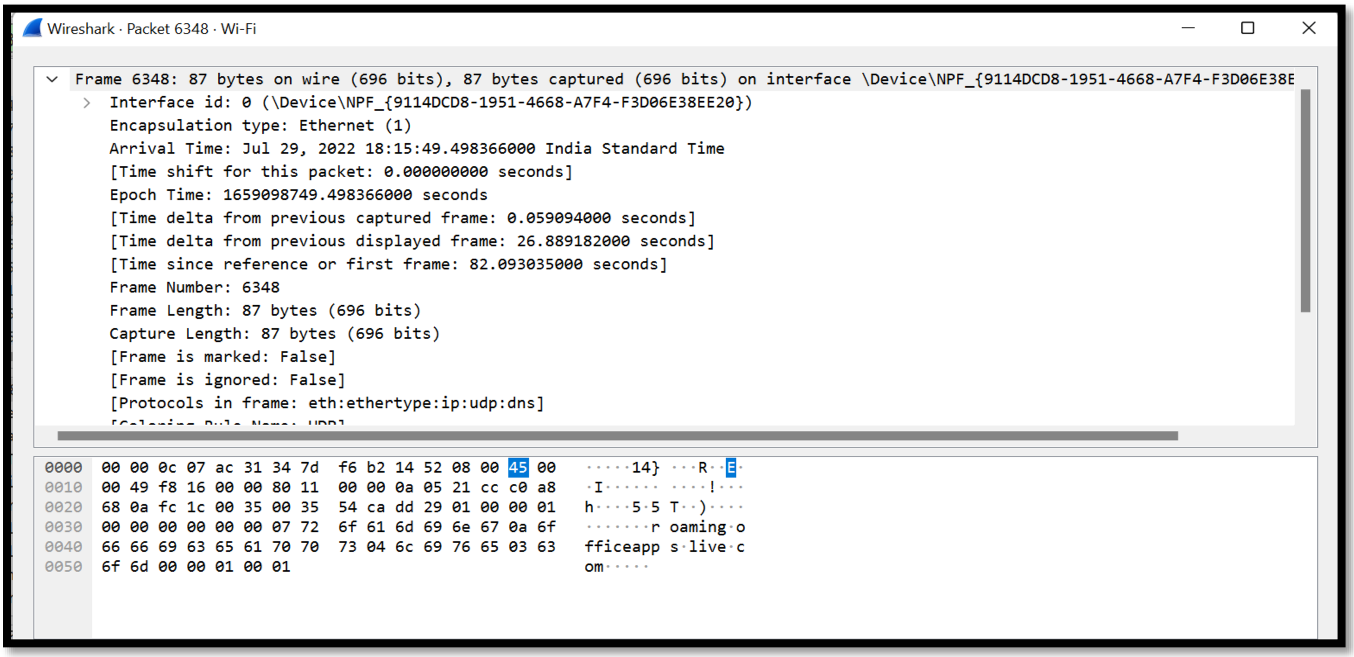
```
No.    Time       Source          Destination     Protocol  Length Arrival Time       Info
  907 15.591955   192.168.51.50   192.168.51.191  DNS           96 Jul 29, 2022 …  Standard query response 0xac93 A adservice.google
  908 15.592661   192.168.51.50   192.168.51.191  DNS          108 Jul 29, 2022 …  Standard query response 0xf8dc AAAA adservice.goc
 1031 16.548530   192.168.51.191  192.168.51.50   DNS           86 Jul 29, 2022 …  Standard query 0x44a6 A encrypted-tbn0.gstatic.cc
 1032 16.548530   192.168.51.191  192.168.51.50   DNS           86 Jul 29, 2022 …  Standard query 0x1a51 AAAA encrypted-tbn0.gstatic
 1033 16.573232   192.168.51.50   192.168.51.191  DNS          114 Jul 29, 2022 …  Standard query response 0x1a51 AAAA encrypted-tbr
 1034 16.581845   192.168.51.50   192.168.51.191  DNS          102 Jul 29, 2022 …  Standard query response 0x44a6 A encrypted-tbn0.g
 1233 18.565733   192.168.51.191  192.168.51.50   DNS           91 Jul 29, 2022 …  Standard query 0xfc1f A signaler-pa.clients6.goog
 1234 18.565908   192.168.51.191  192.168.51.50   DNS           91 Jul 29, 2022 …  Standard query 0x1de6 AAAA signaler-pa.clients6.g
 1236 18.618240   192.168.51.50   192.168.51.191  DNS          107 Jul 29, 2022 …  Standard query response 0xfc1f A signaler-pa.clie
 1237 18.618709   192.168.51.50   192.168.51.191  DNS          119 Jul 29, 2022 …  Standard query response 0x1de6 AAAA signaler-pa.c
 1261 19.698667   192.168.51.191  192.168.51.50   DNS           74 Jul 29, 2022 …  Standard query 0x8b7f A ogs.google.com
```

```
> Frame 1033: 114 bytes on wire (912 bits), 114 bytes captured (912 bits) on interface \Device\NPF_{9114DCD8-1951-4668-A7F4-F3D06E38EE20}, id 0
> Ethernet II, Src: b6:a0:58:1e:57:85 (b6:a0:58:1e:57:85), Dst: IntelCor_b2:14:52 (34:7d:f6:b2:14:52)
v Internet Protocol Version 4, Src: 192.168.51.50, Dst: 192.168.51.191
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 100
    Identification: 0xb69c (46748)
  > Flags: 0x40, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
```

```
0000  34 7d f6 b2 14 52 b6 a0  58 1e 57 85 08 00 45 00   4}···R·· X·W···E·
0010  00 64 b6 9c 40 00 40 11  9b aa c0 a8 33 32 c0 a8   ·d··@·@· ····32··
0020  33 bf 00 35 c1 87 00 50  fb 05 1a 51 81 80 00 01   3··5···P ···Q····
0030  00 01 00 00 00 00 0e 65  6e 63 72 79 70 74 65 64   ·······e ncrypted
0040  2d 74 62 6e 30 07 67 73  74 61 74 69 63 03 63 6f   -tbn0·gs tatic·co
```

4. Encapsulation details screenshots.

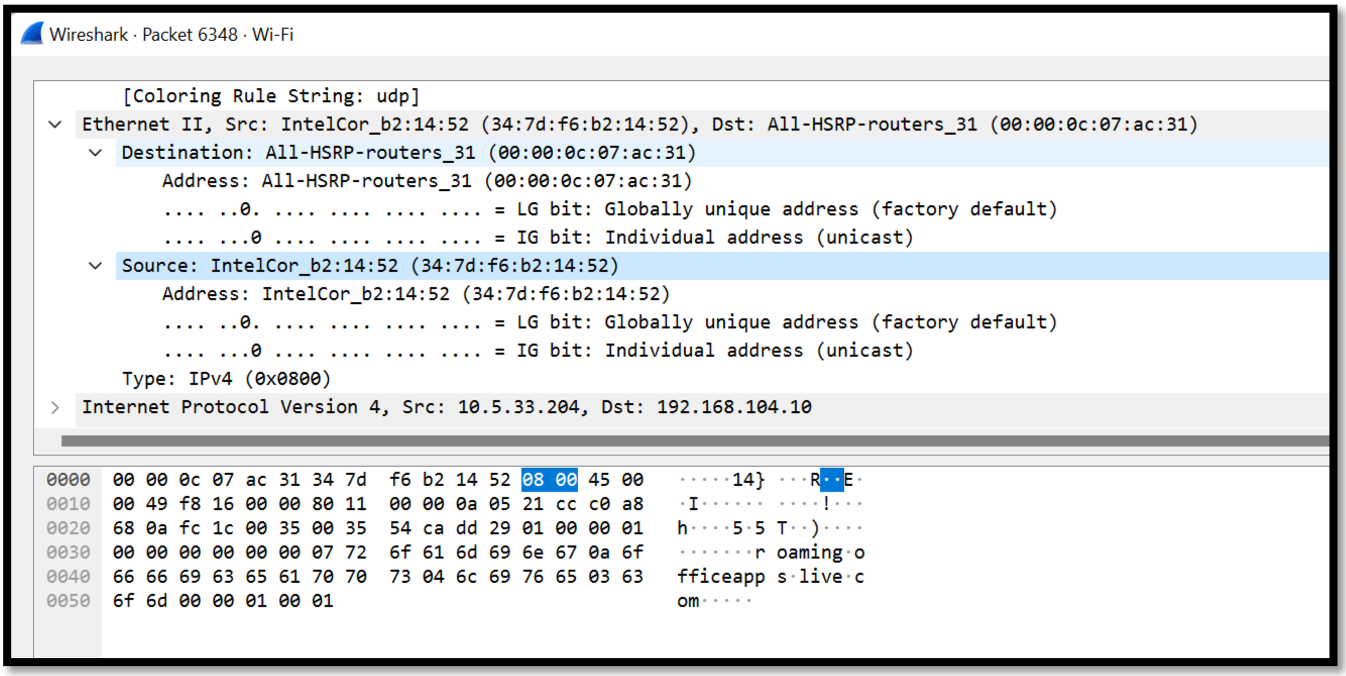
- **Frames**



```
v Frame 6348: 87 bytes on wire (696 bits), 87 bytes captured (696 bits) on interface \Device\NPF_{9114DCD8-1951-4668-A7F4-F3D06E38E
  > Interface id: 0 (\Device\NPF_{9114DCD8-1951-4668-A7F4-F3D06E38EE20})
    Encapsulation type: Ethernet (1)
    Arrival Time: Jul 29, 2022 18:15:49.498366000 India Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1659098749.498366000 seconds
    [Time delta from previous captured frame: 0.059094000 seconds]
    [Time delta from previous displayed frame: 26.889182000 seconds]
    [Time since reference or first frame: 82.093035000 seconds]
    Frame Number: 6348
    Frame Length: 87 bytes (696 bits)
    Capture Length: 87 bytes (696 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:udp:dns]
```

```
0000  00 00 0c 07 ac 31 34 7d  f6 b2 14 52 08 00 45 00   ·····14} ···R··E·
0010  00 49 f8 16 00 00 80 11  00 00 0a 05 21 cc c0 a8   ·I······ ····!···
0020  68 0a fc 1c 00 35 00 35  54 ca dd 29 01 00 00 01   h····5·5 T··)····
0030  00 00 00 00 00 00 07 72  6f 61 6d 69 6e 67 0a 6f   ·······r oaming·o
0040  66 66 69 63 65 61 70 70  73 04 6c 69 76 65 03 63   fficeapp s·live·c
0050  6f 6d 00 00 01 00 01                               om·····
```

- **Ethernet**

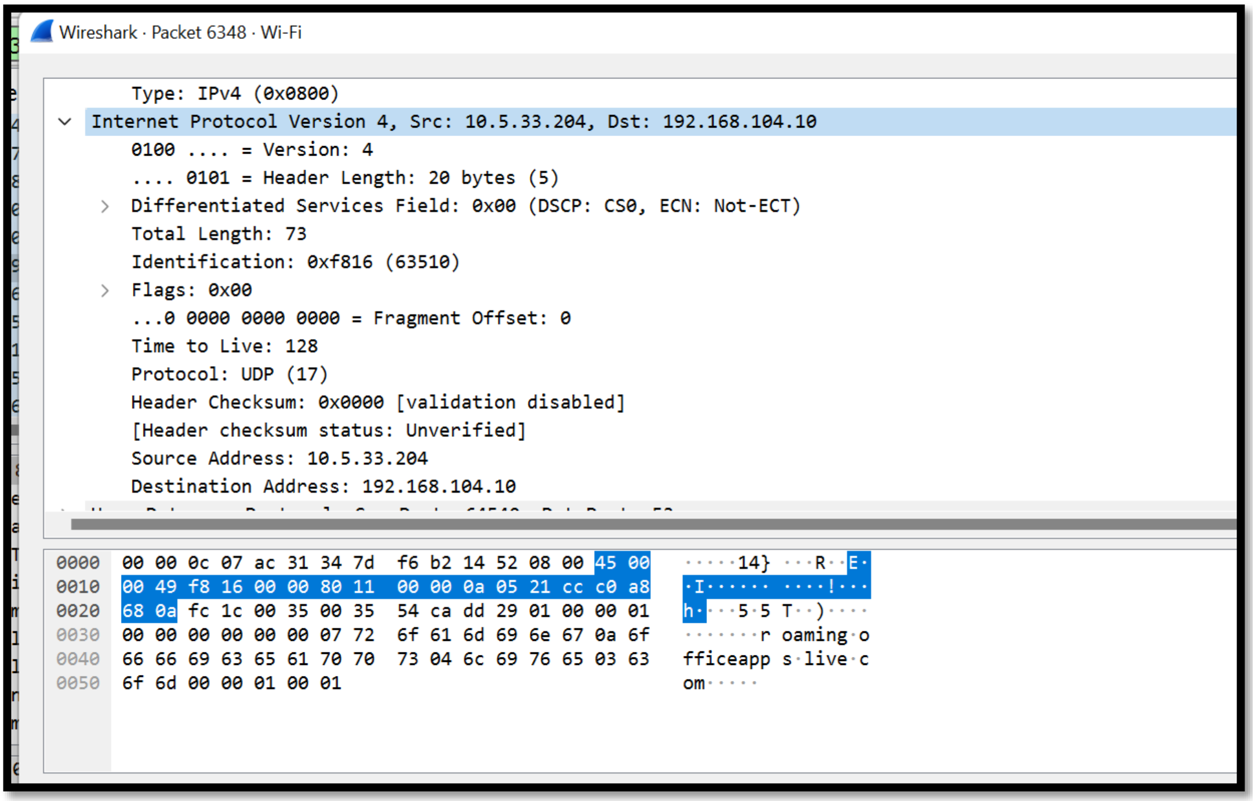


Wireshark · Packet 6348 · Wi-Fi

```
      [Coloring Rule String: udp]
v Ethernet II, Src: IntelCor_b2:14:52 (34:7d:f6:b2:14:52), Dst: All-HSRP-routers_31 (00:00:0c:07:ac:31)
  v Destination: All-HSRP-routers_31 (00:00:0c:07:ac:31)
        Address: All-HSRP-routers_31 (00:00:0c:07:ac:31)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: IntelCor_b2:14:52 (34:7d:f6:b2:14:52)
        Address: IntelCor_b2:14:52 (34:7d:f6:b2:14:52)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
      Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 10.5.33.204, Dst: 192.168.104.10
```

```
0000  00 00 0c 07 ac 31 34 7d  f6 b2 14 52 08 00 45 00   ·····14} ···R··E·
0010  00 49 f8 16 00 00 80 11  00 00 0a 05 21 cc c0 a8   ·I······ ····!···
0020  68 0a fc 1c 00 35 00 35  54 ca dd 29 01 00 00 01   h····5·5 T··)····
0030  00 00 00 00 00 00 07 72  6f 61 6d 69 6e 67 0a 6f   ·······r oaming·o
0040  66 66 69 63 65 61 70 70  73 04 6c 69 76 65 03 63   fficeapp s·live·c
0050  6f 6d 00 00 01 00 01                               om·····
```

- **IP**



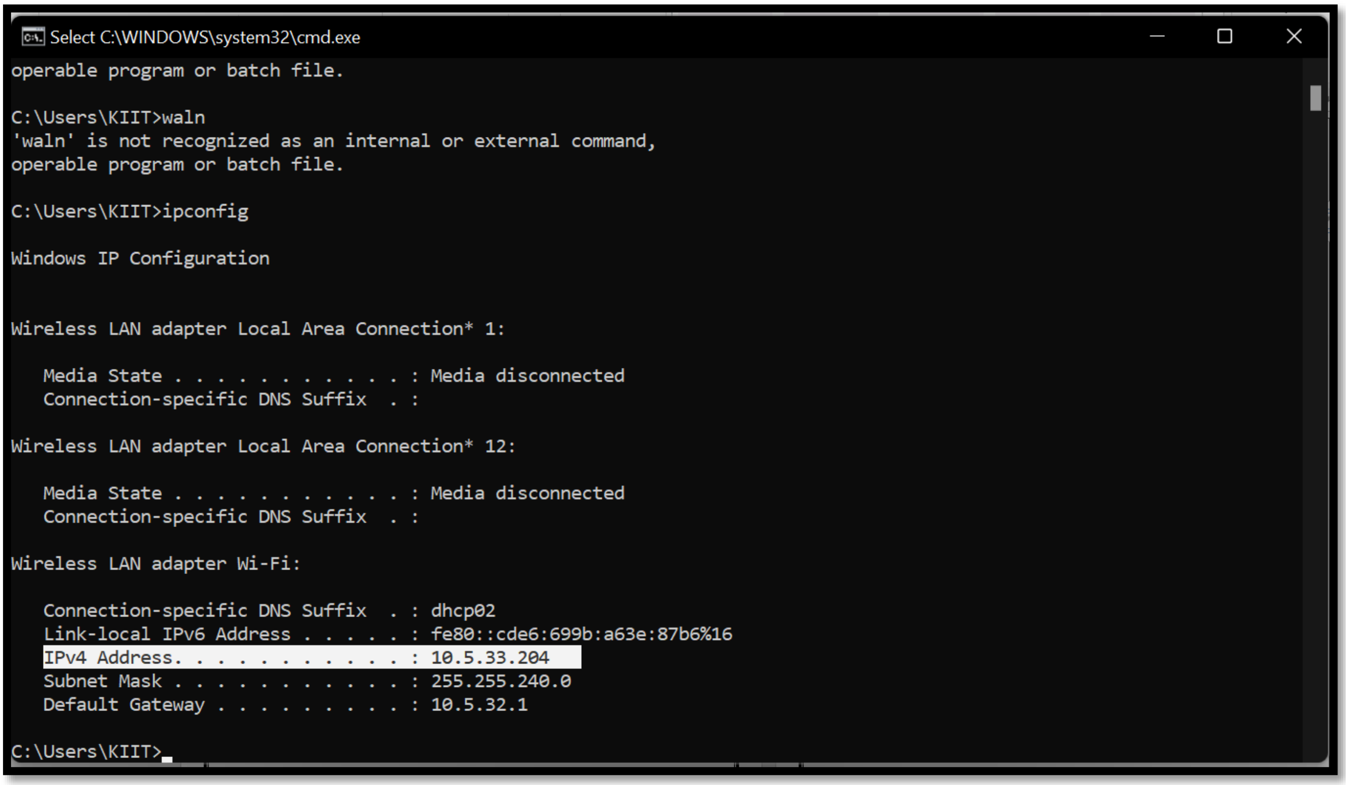
Wireshark · Packet 6348 · Wi-Fi

```
      Type: IPv4 (0x0800)
v Internet Protocol Version 4, Src: 10.5.33.204, Dst: 192.168.104.10
      0100 .... = Version: 4
      .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      Total Length: 73
      Identification: 0xf816 (63510)
    > Flags: 0x00
      ...0 0000 0000 0000 = Fragment Offset: 0
      Time to Live: 128
      Protocol: UDP (17)
      Header Checksum: 0x0000 [validation disabled]
      [Header checksum status: Unverified]
      Source Address: 10.5.33.204
      Destination Address: 192.168.104.10
```

```
0000  00 00 0c 07 ac 31 34 7d  f6 b2 14 52 08 00 45 00   ·····14} ···R··E·
0010  00 49 f8 16 00 00 80 11  00 00 0a 05 21 cc c0 a8   ·I······ ····!···
0020  68 0a fc 1c 00 35 00 35  54 ca dd 29 01 00 00 01   h····5·5 T··)····
0030  00 00 00 00 00 00 07 72  6f 61 6d 69 6e 67 0a 6f   ·······r oaming·o
0040  66 66 69 63 65 61 70 70  73 04 6c 69 76 65 03 63   fficeapp s·live·c
0050  6f 6d 00 00 01 00 01                               om·····
```

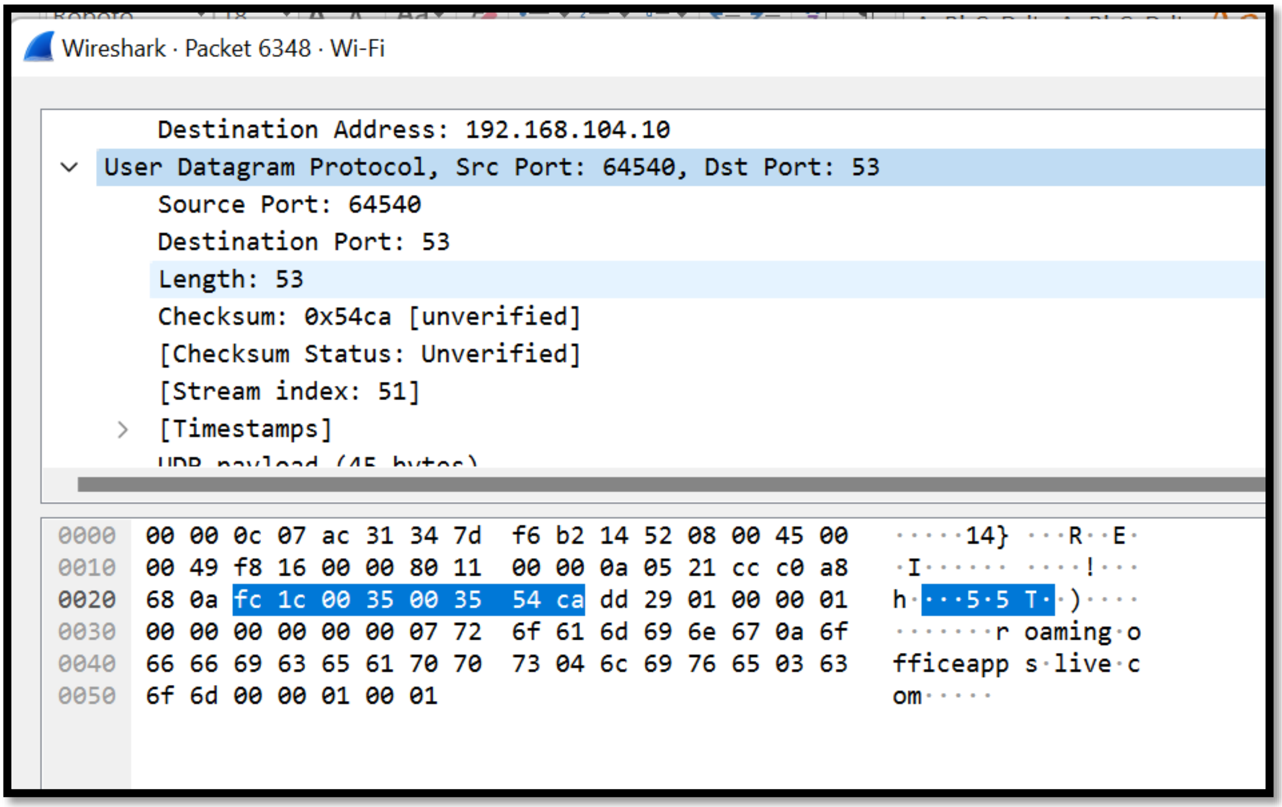
2005025_Hitu raj

IP SHOWING SAME AS THAT OF MY PC



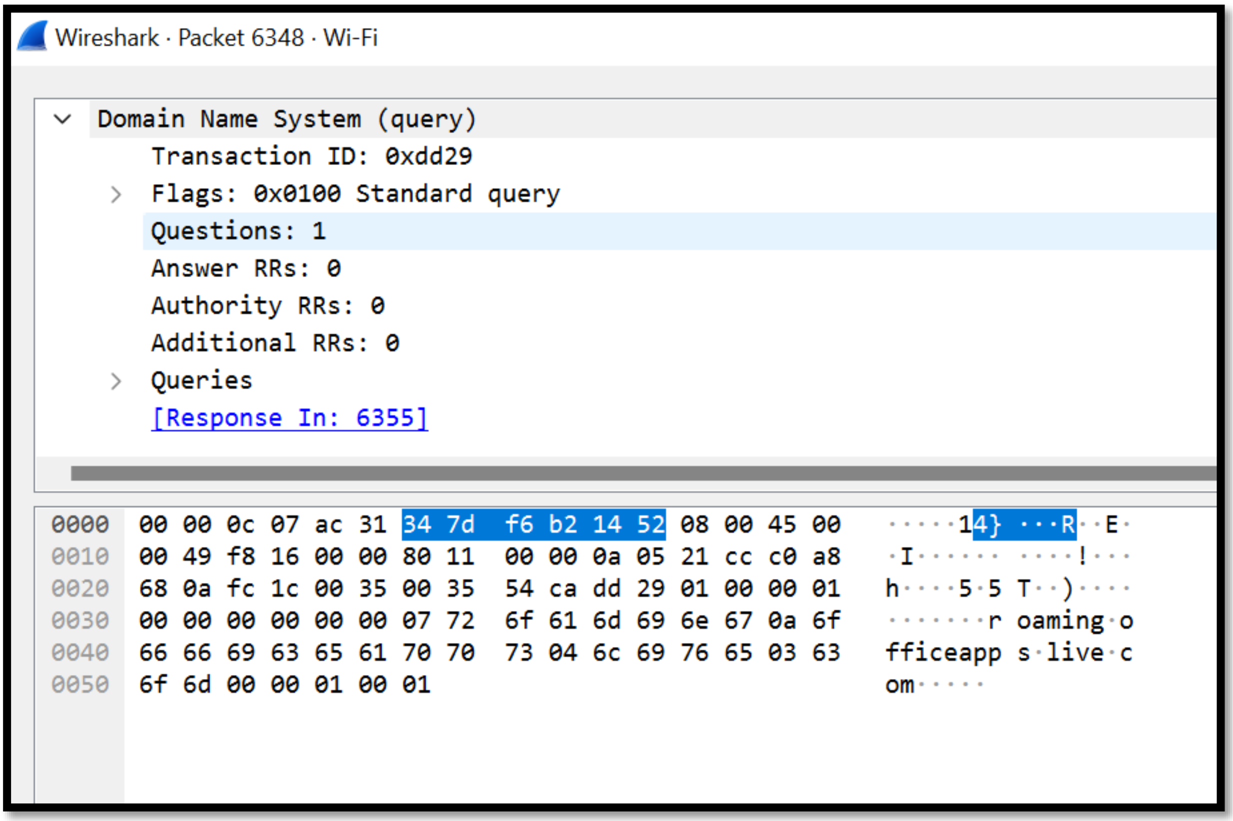
```
operable program or batch file.

C:\Users\KIIT>waln
'waln' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\KIIT>ipconfig

Windows IP Configuration


Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 12:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : dhcp02
   Link-local IPv6 Address . . . . . : fe80::cde6:699b:a63e:87b6%16
   IPv4 Address. . . . . . . . . . . : 10.5.33.204
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . : 10.5.32.1

C:\Users\KIIT>_
```

- UDP



```
    Destination Address: 192.168.104.10
v User Datagram Protocol, Src Port: 64540, Dst Port: 53
    Source Port: 64540
    Destination Port: 53
    Length: 53
    Checksum: 0x54ca [unverified]
    [Checksum Status: Unverified]
    [Stream index: 51]
  > [Timestamps]
    UDP payload (45 bytes)

0000  00 00 0c 07 ac 31 34 7d  f6 b2 14 52 08 00 45 00   ·····14} ···R··E·
0010  00 49 f8 16 00 00 80 11  00 00 0a 05 21 cc c0 a8   ·I······ ····!···
0020  68 0a fc 1c 00 35 00 35  54 ca dd 29 01 00 00 01   h···5·5 T·)····
0030  00 00 00 00 00 00 07 72  6f 61 6d 69 6e 67 0a 6f   ·······r oaming·o
0040  66 66 69 63 65 61 70 70  73 04 6c 69 76 65 03 63   fficeapp s·live·c
0050  6f 6d 00 00 01 00 01                               om·····
```

- DNS



Wireshark · Packet 6348 · Wi-Fi

```
∨ Domain Name System (query)
      Transaction ID: 0xdd29
    > Flags: 0x0100 Standard query
      Questions: 1
      Answer RRs: 0
      Authority RRs: 0
      Additional RRs: 0
    > Queries
      [Response In: 6355]
```

```
0000  00 00 0c 07 ac 31 34 7d  f6 b2 14 52 08 00 45 00   ·····14} ···R··E·
0010  00 49 f8 16 00 00 80 11  00 00 0a 05 21 cc c0 a8   ·I······ ····!···
0020  68 0a fc 1c 00 35 00 35  54 ca dd 29 01 00 00 01   h····5·5 T··)····
0030  00 00 00 00 00 00 07 72  6f 61 6d 69 6e 67 0a 6f   ·······r oaming·o
0040  66 66 69 63 65 61 70 70  73 04 6c 69 76 65 03 63   fficeapp s·live·c
0050  6f 6d 00 00 01 00 01                               om·····
```

Hitu Raj

- Name :HITU RAJ
- Roll no. :2005025
- Branch :CSE-4