Department of Computer Engineering

Class: S.Y. B.Tech. **Semester: IV**

Course Code: DJ19CEL405 **Course Name: Computer Networks Lab**

Name: Vinit Shah	**SAP ID:60004220097**
Date of Performance:9/10/2024	**Date of Submission:16/10/2024**

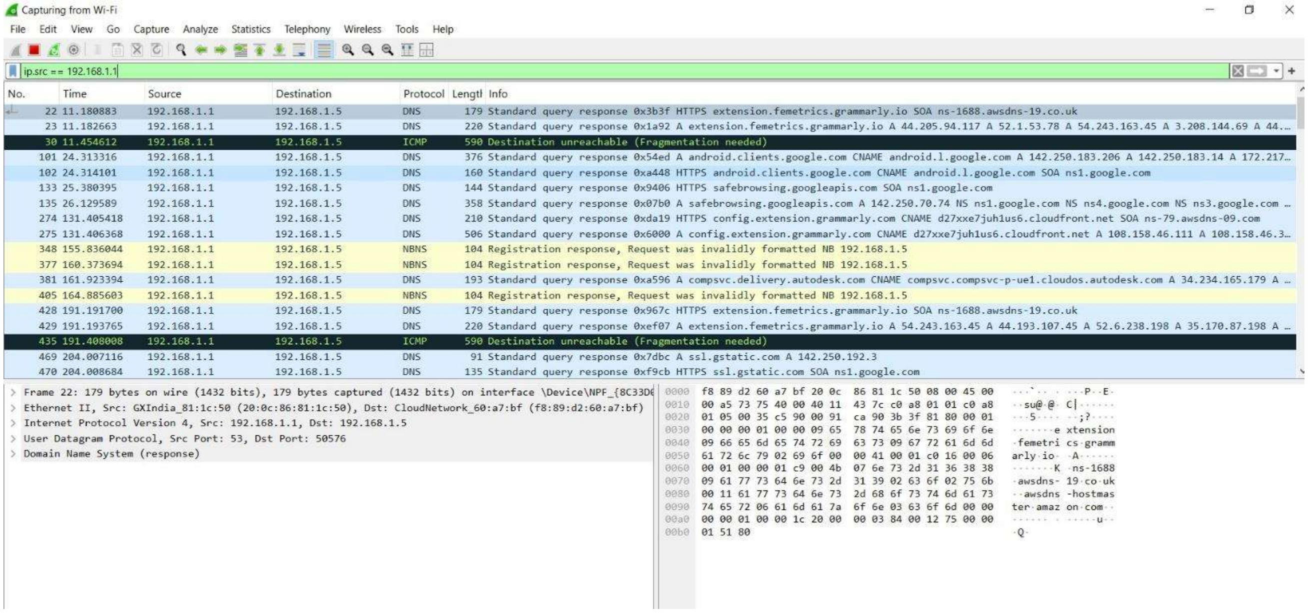
Experiment No: 8

Aim: To implement Packet Capturing Using Wireshark

Theory: Different filters:

1)IP:

a) src:


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

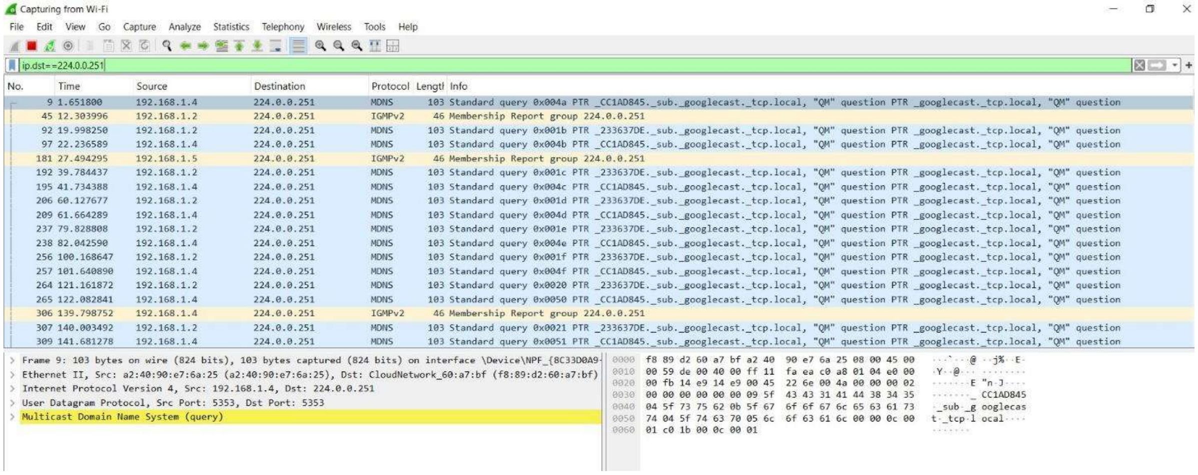
```
ip.src == 192.168.1.1

No.  Time        Source       Destination  Protocol Lengtl Info
 22 11.180883   192.168.1.1  192.168.1.5  DNS      179 Standard query response 0x3b3f HTTPS extension.femetrics.grammarly.io SOA ns-1688.awsdns-19.co.uk
 23 11.182663   192.168.1.1  192.168.1.5  DNS      220 Standard query response 0x1a92 A extension.femetrics.grammarly.io A 44.205.94.117 A 52.1.53.78 A 54.243.163.45 A 3.208.144.69 A 44.…
 30 11.454612   192.168.1.1  192.168.1.5  ICMP     590 Destination unreachable (Fragmentation needed)
101 24.313316   192.168.1.1  192.168.1.5  DNS      376 Standard query response 0x54ed A android.clients.google.com CNAME android.l.google.com A 142.250.183.206 A 142.250.183.14 A 172.217…
102 24.314101   192.168.1.1  192.168.1.5  DNS      160 Standard query response 0xa448 HTTPS android.clients.google.com CNAME android.l.google.com SOA ns1.google.com
133 25.380395   192.168.1.1  192.168.1.5  DNS      144 Standard query response 0x9406 HTTPS safebrowsing.googleapis.com SOA ns1.google.com
135 26.129589   192.168.1.1  192.168.1.5  DNS      358 Standard query response 0x07b0 A safebrowsing.googleapis.com A 142.250.70.74 NS ns1.google.com NS ns4.google.com NS ns3.google.com …
274 131.405418  192.168.1.1  192.168.1.5  DNS      210 Standard query response 0xda19 HTTPS config.extension.grammarly.com CNAME d27xxe7juh1us6.cloudfront.net SOA ns-79.awsdns-09.com
275 131.406368  192.168.1.1  192.168.1.5  DNS      506 Standard query response 0x6000 A config.extension.grammarly.com CNAME d27xxe7juh1us6.cloudfront.net A 108.158.46.111 A 108.158.46.3…
348 155.836044  192.168.1.1  192.168.1.5  NBNS     104 Registration response, Request was invalidly formatted NB 192.168.1.5
377 160.373694  192.168.1.1  192.168.1.5  NBNS     104 Registration response, Request was invalidly formatted NB 192.168.1.5
381 161.923394  192.168.1.1  192.168.1.5  DNS      193 Standard query response 0xa596 A compsvc.delivery.autodesk.com CNAME compsvc.compsvc-p-ue1.cloudos.autodesk.com A 34.234.165.179 A …
405 164.885603  192.168.1.1  192.168.1.5  NBNS     104 Registration response, Request was invalidly formatted NB 192.168.1.5
428 191.191700  192.168.1.1  192.168.1.5  DNS      179 Standard query response 0x967c HTTPS extension.femetrics.grammarly.io SOA ns-1688.awsdns-19.co.uk
429 191.193765  192.168.1.1  192.168.1.5  DNS      220 Standard query response 0xef07 A extension.femetrics.grammarly.io A 54.243.163.45 A 44.193.107.45 A 52.6.238.198 A 35.170.87.198 A …
435 191.408008  192.168.1.1  192.168.1.5  ICMP     590 Destination unreachable (Fragmentation needed)
469 204.007116  192.168.1.1  192.168.1.5  DNS       91 Standard query response 0x7dbc A ssl.gstatic.com A 142.250.192.3
470 204.008684  192.168.1.1  192.168.1.5  DNS      135 Standard query response 0xf9cb HTTPS ssl.gstatic.com SOA ns1.google.com

> Frame 22: 179 bytes on wire (1432 bits), 179 bytes captured (1432 bits) on interface \Device\NPF_{8C33D(
> Ethernet II, Src: GXIndia_81:1c:50 (20:0c:86:81:1c:50), Dst: CloudNetwork_60:a7:bf (f8:89:d2:60:a7:bf)
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.5
> User Datagram Protocol, Src Port: 53, Dst Port: 50576
> Domain Name System (response)

0000  f8 89 d2 60 a7 bf 20 0c  86 81 1c 50 08 00 45 00   ···`·· · ···P··E·
0010  00 a5 73 75 40 00 40 11  43 7c c0 a8 01 01 c0 a8   ··su@·@· C|······
0020  01 05 00 35 c5 90 00 91  ca 90 3b 3f 81 80 00 01   ···5···· ··;?····
0030  00 00 00 01 00 00 09 65  78 74 65 6e 73 69 6f 6e   ·······e xtension
0040  09 66 65 6d 65 74 72 69  63 73 09 67 72 61 6d 6d   ·femetri cs·gramm
0050  61 72 6c 79 02 69 6f 00  00 41 00 01 c0 16 00 06   arly·io· ·A······
0060  00 01 00 00 01 c9 00 4b  07 6e 73 2d 31 36 38 38   ·······K ·ns-1688
0070  09 61 77 73 64 6e 73 2d  31 39 02 63 6f 02 75 6b   ·awsdns- 19·co·uk
0080  00 11 61 77 73 64 6e 73  2d 68 6f 73 74 6d 61 73   ··awsdns -hostmas
0090  74 65 72 06 61 6d 61 7a  6f 6e 03 63 6f 6d 00 00   ter·amaz on·com··
00a0  00 00 01 00 00 1c 20 00  00 03 84 00 12 75 00 00   ······ · ·····u··
00b0  01 51 80                                           ·Q·
```

b) dst:


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

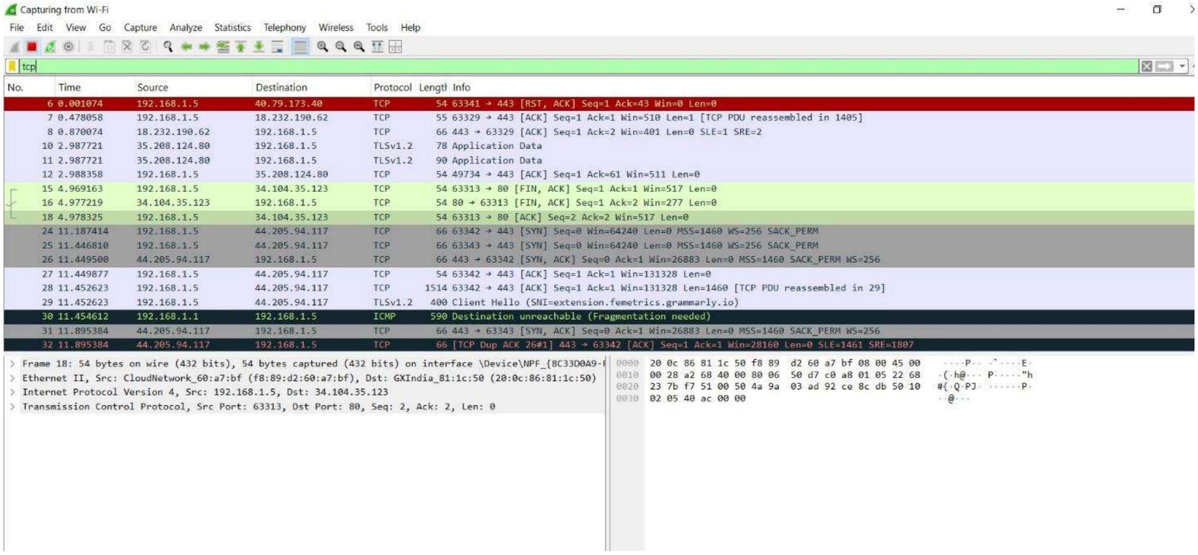
```
ip.dst==224.0.0.251

No.  Time        Source       Destination  Protocol Lengtl Info
  9 1.651800    192.168.1.4  224.0.0.251  MDNS     103 Standard query 0x004a PTR _CC1AD845._sub._googlecast._tcp.local, "QM" question PTR _googlecast._tcp.local, "QM" question
 45 12.303996   192.168.1.2  224.0.0.251  IGMPv2    46 Membership Report group 224.0.0.251
 92 19.998250   192.168.1.2  224.0.0.251  MDNS     103 Standard query 0x001b PTR _233637DE._sub._googlecast._tcp.local, "QM" question PTR _googlecast._tcp.local, "QM" question
 97 22.236589   192.168.1.4  224.0.0.251  MDNS     103 Standard query 0x004b PTR _CC1AD845._sub._googlecast._tcp.local, "QM" question PTR _googlecast._tcp.local, "QM" question
181 27.494295   192.168.1.5  224.0.0.251  IGMPv2    46 Membership Report group 224.0.0.251
192 39.784437   192.168.1.2  224.0.0.251  MDNS     103 Standard query 0x001c PTR _233637DE._sub._googlecast._tcp.local, "QM" question PTR _googlecast._tcp.local, "QM" question
195 41.734388   192.168.1.4  224.0.0.251  MDNS     103 Standard query 0x004c PTR _CC1AD845._sub._googlecast._tcp.local, "QM" question PTR _googlecast._tcp.local, "QM" question
206 60.127677   192.168.1.2  224.0.0.251  MDNS     103 Standard query 0x001d PTR _233637DE._sub._googlecast._tcp.local, "QM" question PTR _googlecast._tcp.local, "QM" question
209 61.664289   192.168.1.4  224.0.0.251  MDNS     103 Standard query 0x004d PTR _CC1AD845._sub._googlecast._tcp.local, "QM" question PTR _googlecast._tcp.local, "QM" question
237 79.828808   192.168.1.2  224.0.0.251  MDNS     103 Standard query 0x001e PTR _233637DE._sub._googlecast._tcp.local, "QM" question PTR _googlecast._tcp.local, "QM" question
238 82.042590   192.168.1.4  224.0.0.251  MDNS     103 Standard query 0x004e PTR _CC1AD845._sub._googlecast._tcp.local, "QM" question PTR _googlecast._tcp.local, "QM" question
256 100.168647  192.168.1.2  224.0.0.251  MDNS     103 Standard query 0x001f PTR _233637DE._sub._googlecast._tcp.local, "QM" question PTR _googlecast._tcp.local, "QM" question
257 101.640890  192.168.1.4  224.0.0.251  MDNS     103 Standard query 0x004f PTR _CC1AD845._sub._googlecast._tcp.local, "QM" question PTR _googlecast._tcp.local, "QM" question
264 121.161872  192.168.1.2  224.0.0.251  MDNS     103 Standard query 0x0020 PTR _233637DE._sub._googlecast._tcp.local, "QM" question PTR _googlecast._tcp.local, "QM" question
265 122.082841  192.168.1.4  224.0.0.251  MDNS     103 Standard query 0x0050 PTR _CC1AD845._sub._googlecast._tcp.local, "QM" question PTR _googlecast._tcp.local, "QM" question
306 139.798752  192.168.1.4  224.0.0.251  IGMPv2    46 Membership Report group 224.0.0.251
307 140.003492  192.168.1.2  224.0.0.251  MDNS     103 Standard query 0x0021 PTR _233637DE._sub._googlecast._tcp.local, "QM" question PTR _googlecast._tcp.local, "QM" question
309 141.681278  192.168.1.4  224.0.0.251  MDNS     103 Standard query 0x0051 PTR _CC1AD845._sub._googlecast._tcp.local, "QM" question PTR _googlecast._tcp.local, "QM" question

> Frame 9: 103 bytes on wire (824 bits), 103 bytes captured (824 bits) on interface \Device\NPF_{8C33D0A9-
> Ethernet II, Src: a2:40:90:e7:6a:25 (a2:40:90:e7:6a:25), Dst: CloudNetwork_60:a7:bf (f8:89:d2:60:a7:bf)
> Internet Protocol Version 4, Src: 192.168.1.4, Dst: 224.0.0.251
> User Datagram Protocol, Src Port: 5353, Dst Port: 5353
> Multicast Domain Name System (query)

0000  f8 89 d2 60 a7 bf a2 40  90 e7 6a 25 08 00 45 00   ···`···@ ··j%··E·
0010  00 59 de 00 40 00 ff 11  fa ea c0 a8 01 04 e0 00   ·Y··@··· ········
0020  00 fb 14 e9 14 e9 00 45  22 6e 00 4a 00 00 00 02   ·······E "n·J····
0030  00 00 00 00 00 00 09 5f  43 43 31 41 44 38 34 35   ·······_ CC1AD845
0040  04 5f 73 75 62 0b 5f 67  6f 6f 67 6c 65 63 61 73   ·_sub·_g ooglecas
0050  74 04 5f 74 63 70 05 6c  6f 63 61 6c 00 00 0c 00   t·_tcp·l ocal····
0060  01 c0 1b 00 0c 00 01                               ·······
```

2)TCP:

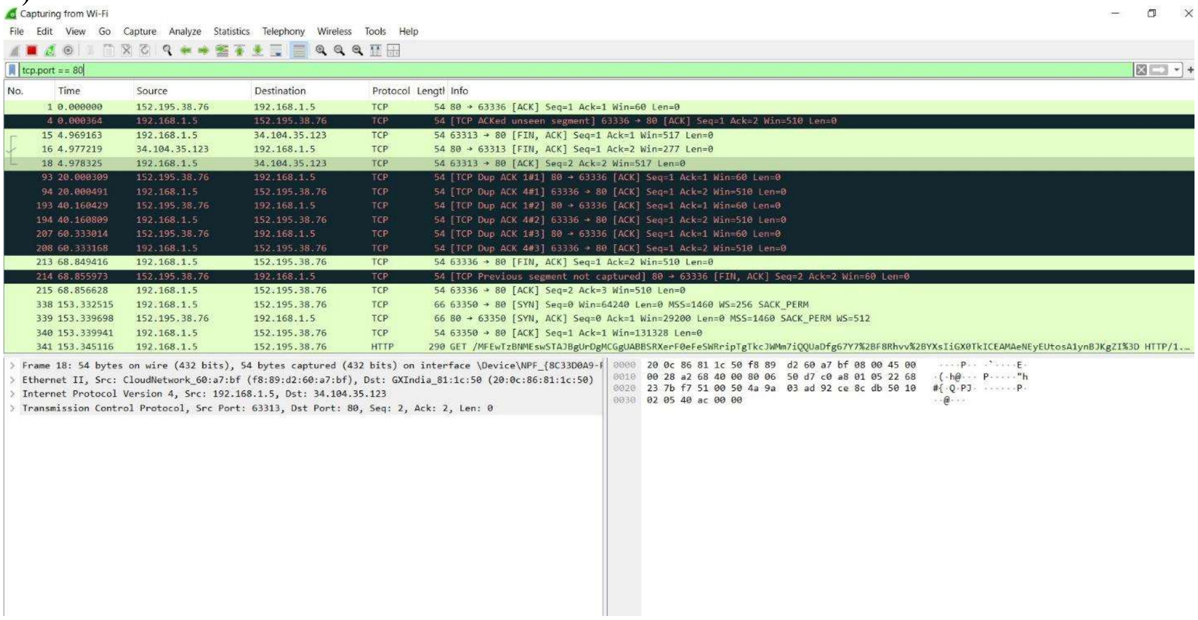


```
tcp
No.   Time       Source          Destination     Protocol Lengtl Info
    6 0.001074   192.168.1.5     40.79.173.40    TCP        54 63341 → 443 [RST, ACK] Seq=1 Ack=43 Win=0 Len=0
    7 0.478058   192.168.1.5     18.232.190.62   TCP        55 63329 → 443 [ACK] Seq=1 Ack=1 Win=510 Len=1 [TCP PDU reassembled in 1405]
    8 0.870074   18.232.190.62   192.168.1.5     TCP        66 443 → 63329 [ACK] Seq=1 Ack=2 Win=401 Len=0 SLE=1 SRE=2
   10 2.987721   35.208.124.80   192.168.1.5     TLSv1.2    78 Application Data
   11 2.987721   35.208.124.80   192.168.1.5     TLSv1.2    90 Application Data
   12 2.988358   192.168.1.5     35.208.124.80   TCP        54 49734 → 443 [ACK] Seq=1 Ack=61 Win=511 Len=0
   15 4.969163   192.168.1.5     34.104.35.123   TCP        54 63313 → 80 [FIN, ACK] Seq=1 Ack=1 Win=517 Len=0
   16 4.977219   34.104.35.123   192.168.1.5     TCP        54 80 → 63313 [FIN, ACK] Seq=1 Ack=2 Win=277 Len=0
   18 4.978325   192.168.1.5     34.104.35.123   TCP        54 63313 → 80 [ACK] Seq=2 Ack=2 Win=517 Len=0
   24 11.187414  192.168.1.5     44.205.94.117   TCP        66 63342 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
   25 11.446810  192.168.1.5     44.205.94.117   TCP        66 63343 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
   26 11.449500  44.205.94.117   192.168.1.5     TCP        66 443 → 63342 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=1460 SACK_PERM WS=256
   27 11.449877  192.168.1.5     44.205.94.117   TCP        54 63342 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0
   28 11.452623  192.168.1.5     44.205.94.117   TCP      1514 63342 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=1460 [TCP PDU reassembled in 29]
   29 11.452623  192.168.1.5     44.205.94.117   TLSv1.2   400 Client Hello (SNI=extension.femetrics.grammarly.io)
   30 11.454612  192.168.1.1     192.168.1.5     ICMP      590 Destination unreachable (Fragmentation needed)
   31 11.895384  44.205.94.117   192.168.1.5     TCP        66 443 → 63343 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=1460 SACK_PERM WS=256
   32 11.895384  44.205.94.117   192.168.1.5     TCP        66 [TCP Dup ACK 26#1] 443 → 63342 [ACK] Seq=1 Ack=1 Win=28160 Len=0 SLE=1461 SRE=1807

> Frame 18: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{8C33D0A9-F
> Ethernet II, Src: CloudNetwork_60:a7:bf (f8:89:d2:60:a7:bf), Dst: GXIndia_81:1c:50 (20:0c:86:81:1c:50)
> Internet Protocol Version 4, Src: 192.168.1.5, Dst: 34.104.35.123
> Transmission Control Protocol, Src Port: 63313, Dst Port: 80, Seq: 2, Ack: 2, Len: 0

0000  20 0c 86 81 1c 50 f8 89  d2 60 a7 bf 08 00 45 00   ····P·· ·`····E·
0010  00 28 a2 68 40 00 80 06  50 d7 c0 a8 01 05 22 68   ·(·h@··· P·····"h
0020  23 7b f7 51 00 50 4a 9a  03 ad 92 ce 8c db 50 10   #{·Q·PJ· ······P·
0030  02 05 40 ac 00 00                                  ··@···
```

a) Port:

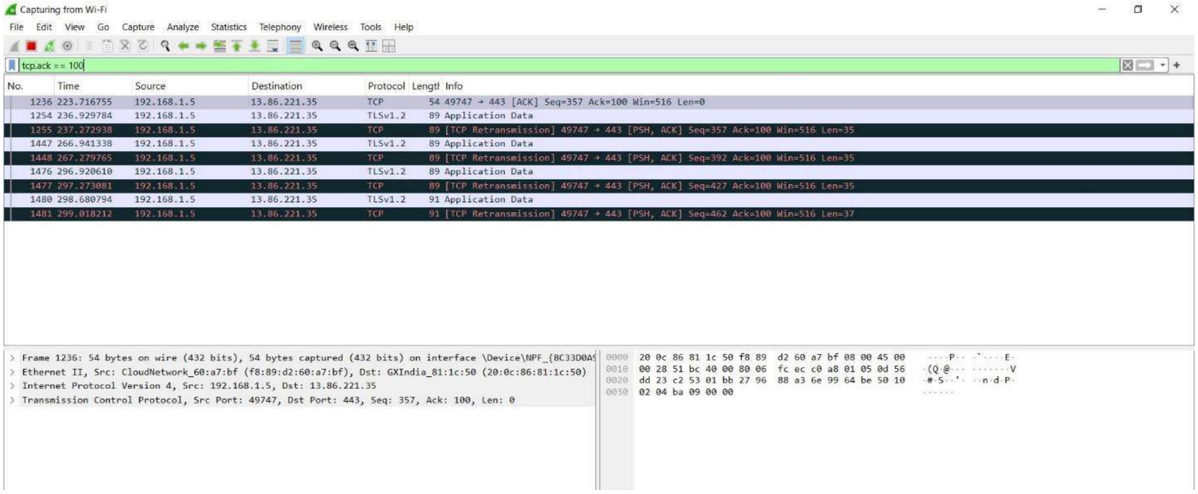


```
tcp.port == 80
No.   Time        Source          Destination     Protocol Lengtl Info
    1 0.000000    152.195.38.76   192.168.1.5     TCP        54 80 → 63336 [ACK] Seq=1 Ack=1 Win=60 Len=0
    4 0.000364    192.168.1.5     152.195.38.76   TCP        54 [TCP ACKed unseen segment] 63336 → 80 [ACK] Seq=1 Ack=2 Win=510 Len=0
   15 4.969163    192.168.1.5     34.104.35.123   TCP        54 63313 → 80 [FIN, ACK] Seq=1 Ack=1 Win=517 Len=0
   16 4.977219    34.104.35.123   192.168.1.5     TCP        54 80 → 63313 [FIN, ACK] Seq=1 Ack=2 Win=277 Len=0
   18 4.978325    192.168.1.5     34.104.35.123   TCP        54 63313 → 80 [ACK] Seq=2 Ack=2 Win=517 Len=0
   93 20.000309   152.195.38.76   192.168.1.5     TCP        54 [TCP Dup ACK 1#1] 80 → 63336 [ACK] Seq=1 Ack=1 Win=60 Len=0
   94 20.000491   192.168.1.5     152.195.38.76   TCP        54 [TCP Dup ACK 4#1] 63336 → 80 [ACK] Seq=1 Ack=2 Win=510 Len=0
  193 40.160429   152.195.38.76   192.168.1.5     TCP        54 [TCP Dup ACK 1#2] 80 → 63336 [ACK] Seq=1 Ack=1 Win=60 Len=0
  194 40.160809   192.168.1.5     152.195.38.76   TCP        54 [TCP Dup ACK 4#2] 63336 → 80 [ACK] Seq=1 Ack=2 Win=510 Len=0
  207 60.333014   152.195.38.76   192.168.1.5     TCP        54 [TCP Dup ACK 1#3] 80 → 63336 [ACK] Seq=1 Ack=1 Win=60 Len=0
  208 60.333168   192.168.1.5     152.195.38.76   TCP        54 [TCP Dup ACK 4#3] 63336 → 80 [ACK] Seq=1 Ack=2 Win=510 Len=0
  213 68.849416   192.168.1.5     152.195.38.76   TCP        54 63336 → 80 [FIN, ACK] Seq=1 Ack=2 Win=510 Len=0
  214 68.855973   152.195.38.76   192.168.1.5     TCP        54 [TCP Previous segment not captured] 80 → 63336 [FIN, ACK] Seq=2 Ack=2 Win=60 Len=0
  215 68.856628   192.168.1.5     152.195.38.76   TCP        54 63336 → 80 [ACK] Seq=2 Ack=3 Win=510 Len=0
  338 153.332515  192.168.1.5     152.195.38.76   TCP        66 63350 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
  339 153.339698  152.195.38.76   192.168.1.5     TCP        66 80 → 63350 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM WS=512
  340 153.339941  192.168.1.5     152.195.38.76   TCP        54 63350 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
  341 153.345116  192.168.1.5     152.195.38.76   HTTP      290 GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBSRXerF0eFeSWRripTgTkcJWMm7iQQUaDfg67Y7%2BF8Rhvv%2BYXsIiGX0TkICEAMAeNEyEUtosA1ynBJKgZI%3D HTTP/1.…

> Frame 18: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{8C33D0A9-F
> Ethernet II, Src: CloudNetwork_60:a7:bf (f8:89:d2:60:a7:bf), Dst: GXIndia_81:1c:50 (20:0c:86:81:1c:50)
> Internet Protocol Version 4, Src: 192.168.1.5, Dst: 34.104.35.123
> Transmission Control Protocol, Src Port: 63313, Dst Port: 80, Seq: 2, Ack: 2, Len: 0

0000  20 0c 86 81 1c 50 f8 89  d2 60 a7 bf 08 00 45 00   ····P·· ·`····E·
0010  00 28 a2 68 40 00 80 06  50 d7 c0 a8 01 05 22 68   ·(·h@··· P·····"h
0020  23 7b f7 51 00 50 4a 9a  03 ad 92 ce 8c db 50 10   #{·Q·PJ· ······P·
0030  02 05 40 ac 00 00                                  ··@···
```

b) ack:

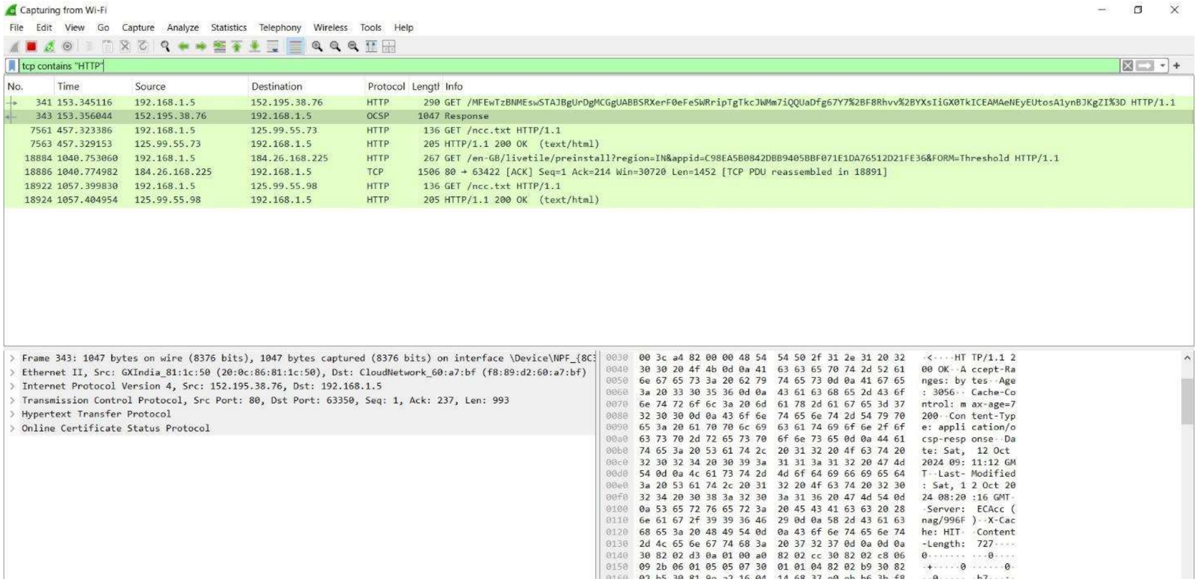

Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.ack == 100

```
No.   Time        Source       Destination   Protocol Length Info
 1236 223.716755  192.168.1.5  13.86.221.35  TCP      54 49747 → 443 [ACK] Seq=357 Ack=100 Win=516 Len=0
 1254 236.929784  192.168.1.5  13.86.221.35  TLSv1.2  89 Application Data
 1255 237.272938  192.168.1.5  13.86.221.35  TCP      89 [TCP Retransmission] 49747 → 443 [PSH, ACK] Seq=357 Ack=100 Win=516 Len=35
 1447 266.941338  192.168.1.5  13.86.221.35  TLSv1.2  89 Application Data
 1448 267.279765  192.168.1.5  13.86.221.35  TCP      89 [TCP Retransmission] 49747 → 443 [PSH, ACK] Seq=392 Ack=100 Win=516 Len=35
 1476 296.920610  192.168.1.5  13.86.221.35  TLSv1.2  89 Application Data
 1477 297.273081  192.168.1.5  13.86.221.35  TCP      89 [TCP Retransmission] 49747 → 443 [PSH, ACK] Seq=427 Ack=100 Win=516 Len=35
 1480 298.680794  192.168.1.5  13.86.221.35  TLSv1.2  91 Application Data
 1481 299.018212  192.168.1.5  13.86.221.35  TCP      91 [TCP Retransmission] 49747 → 443 [PSH, ACK] Seq=462 Ack=100 Win=516 Len=37
```

```
> Frame 1236: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{8C33D0A9
> Ethernet II, Src: CloudNetwork_60:a7:bf (f8:89:d2:60:a7:bf), Dst: GXIndia_81:1c:50 (20:0c:86:81:1c:50)
> Internet Protocol Version 4, Src: 192.168.1.5, Dst: 13.86.221.35
> Transmission Control Protocol, Src Port: 49747, Dst Port: 443, Seq: 357, Ack: 100, Len: 0
```

```
0000  20 0c 86 81 1c 50 f8 89  d2 60 a7 bf 08 00 45 00   ····P·· ·`····E·
0010  00 28 51 bc 40 00 80 06  fc ec c0 a8 01 05 0d 56   ·(Q·@··· ·······V
0020  dd 23 c2 53 01 bb 27 96  88 a3 6e 99 64 be 50 10   ·#·S··'· ··n·d·P·
0030  02 04 ba 09 00 00                                  ······
```


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

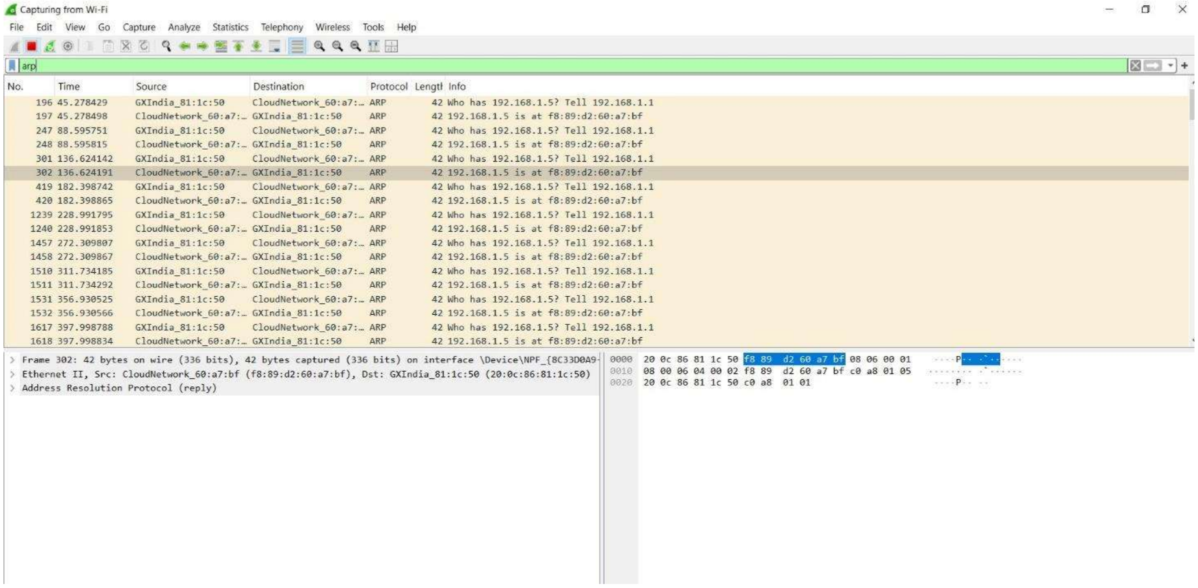
tcp contains "HTTP"

```
No.    Time         Source          Destination     Protocol Length Info
  341  153.345116   192.168.1.5     152.195.38.76   HTTP     290 GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBSRXerF0eFeSWRripTgTkcJWMm7iQQUaDfg67Y7%2BF8Rhvv%2BYXsIiGX0TkICEAMAeNEyEUtosA1ynBJKgZI%3D HTTP/1.1
  343  153.356044   152.195.38.76   192.168.1.5     OCSP     1047 Response
 7561  457.323386   192.168.1.5     125.99.55.73    HTTP     136 GET /ncc.txt HTTP/1.1
 7563  457.329153   125.99.55.73    192.168.1.5     HTTP     205 HTTP/1.1 200 OK  (text/html)
18884  1040.753060  192.168.1.5     184.26.168.225  HTTP     267 GET /en-GB/livetile/preinstall?region=IN&appid=C98EA5B0842DBB9405BBF071E1DA76512D21FE36&FORM=Threshold HTTP/1.1
18886  1040.774982  184.26.168.225  192.168.1.5     TCP      1506 80 → 63422 [ACK] Seq=1 Ack=214 Win=30720 Len=1452 [TCP PDU reassembled in 18891]
18922  1057.399830  192.168.1.5     125.99.55.98    HTTP     136 GET /ncc.txt HTTP/1.1
18924  1057.404954  125.99.55.98    192.168.1.5     HTTP     205 HTTP/1.1 200 OK  (text/html)
```

```
> Frame 343: 1047 bytes on wire (8376 bits), 1047 bytes captured (8376 bits) on interface \Device\NPF_{8C3
> Ethernet II, Src: GXIndia_81:1c:50 (20:0c:86:81:1c:50), Dst: CloudNetwork_60:a7:bf (f8:89:d2:60:a7:bf)
> Internet Protocol Version 4, Src: 152.195.38.76, Dst: 192.168.1.5
> Transmission Control Protocol, Src Port: 80, Dst Port: 63350, Seq: 1, Ack: 237, Len: 993
> Hypertext Transfer Protocol
> Online Certificate Status Protocol
```

```
0030  00 3c a4 82 00 00 48 54  54 50 2f 31 2e 31 20 32   ·<····HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 41  63 63 65 70 74 2d 52 61   00 OK··A ccept-Ra
0050  6e 67 65 73 3a 20 62 79  74 65 73 0d 0a 41 67 65   nges: by tes··Age
0060  3a 20 33 30 35 36 0d 0a  43 61 63 68 65 2d 43 6f   : 3056·· Cache-Co
0070  6e 74 72 6f 6c 3a 20 6d  61 78 2d 61 67 65 3d 37   ntrol: m ax-age=7
0080  32 30 30 0d 0a 43 6f 6e  74 65 6e 74 2d 54 79 70   200··Con tent-Typ
0090  65 3a 20 61 70 70 6c 69  63 61 74 69 6f 6e 2f 6f   e: appli cation/o
00a0  63 73 70 2d 72 65 73 70  6f 6e 73 65 0d 0a 44 61   csp-resp onse··Da
00b0  74 65 3a 20 53 61 74 2c  20 31 32 20 4f 63 74 20   te: Sat,  12 Oct 
00c0  32 30 32 34 20 30 39 3a  31 31 3a 31 32 20 47 4d   2024 09: 11:12 GM
00d0  54 0d 0a 4c 61 73 74 2d  4d 6f 64 69 66 69 65 64   T··Last- Modified
00e0  3a 20 53 61 74 2c 20 31  32 20 4f 63 74 20 32 30   : Sat, 1 2 Oct 20
00f0  32 34 20 30 38 3a 32 30  3a 31 36 20 47 4d 54 0d   24 08:20 :16 GMT·
0100  0a 53 65 72 76 65 72 3a  20 45 43 41 63 63 20 28   ·Server:  ECAcc (
0110  6e 61 67 2f 39 39 36 46  29 0d 0a 58 2d 43 61 63   nag/996F )··X-Cac
0120  68 65 3a 20 48 49 54 0d  0a 43 6f 6e 74 65 6e 74   he: HIT· ·Content
0130  2d 4c 65 6e 67 74 68 3a  20 37 32 37 0d 0a 0d 0a   -Length:  727····
0140  30 82 02 d3 0a 01 00 a0  82 02 cc 30 82 02 c8 06   0······· ···0····
0150  09 2b 06 01 05 05 07 30  01 01 04 82 02 b9 30 82   ·+·····0 ······0·
```

3)ARP:


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

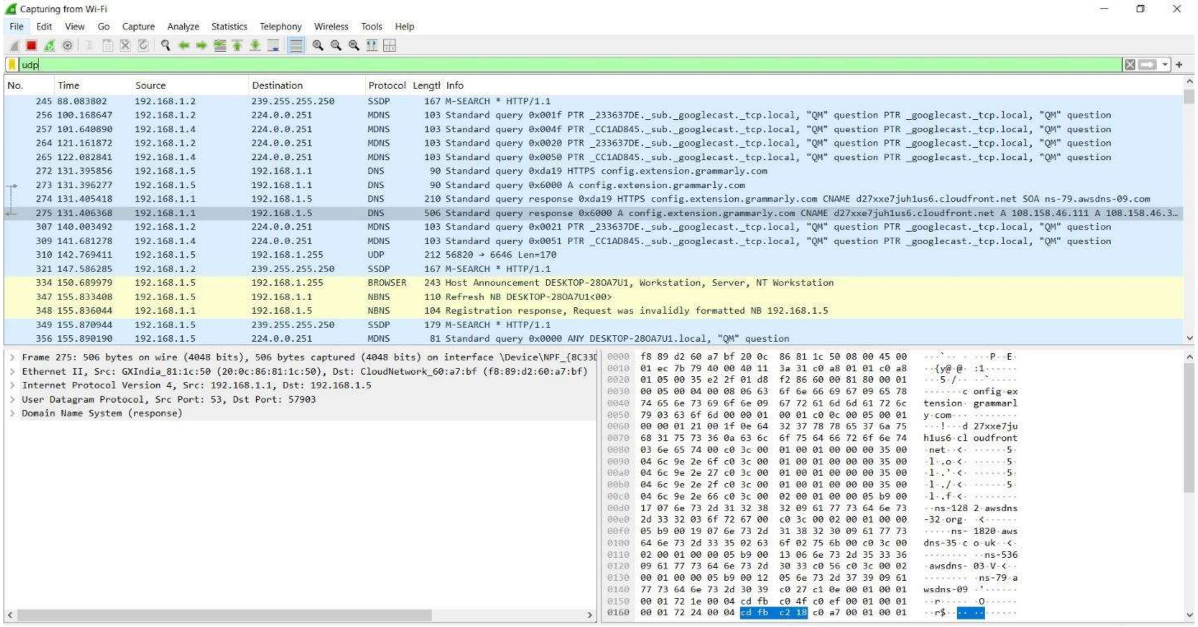
arp

```
No.   Time        Source                Destination           Protocol Lengtl Info
  196 45.278429   GXIndia_81:1c:50      CloudNetwork_60:a7:… ARP      42 Who has 192.168.1.5? Tell 192.168.1.1
  197 45.278498   CloudNetwork_60:a7:… GXIndia_81:1c:50      ARP      42 192.168.1.5 is at f8:89:d2:60:a7:bf
  247 88.595751   GXIndia_81:1c:50      CloudNetwork_60:a7:… ARP      42 Who has 192.168.1.5? Tell 192.168.1.1
  248 88.595815   CloudNetwork_60:a7:… GXIndia_81:1c:50      ARP      42 192.168.1.5 is at f8:89:d2:60:a7:bf
  301 136.624142  GXIndia_81:1c:50      CloudNetwork_60:a7:… ARP      42 Who has 192.168.1.5? Tell 192.168.1.1
  302 136.624191  CloudNetwork_60:a7:… GXIndia_81:1c:50      ARP      42 192.168.1.5 is at f8:89:d2:60:a7:bf
  419 182.398742  GXIndia_81:1c:50      CloudNetwork_60:a7:… ARP      42 Who has 192.168.1.5? Tell 192.168.1.1
  420 182.398865  CloudNetwork_60:a7:… GXIndia_81:1c:50      ARP      42 192.168.1.5 is at f8:89:d2:60:a7:bf
 1239 228.991795  GXIndia_81:1c:50      CloudNetwork_60:a7:… ARP      42 Who has 192.168.1.5? Tell 192.168.1.1
 1240 228.991853  CloudNetwork_60:a7:… GXIndia_81:1c:50      ARP      42 192.168.1.5 is at f8:89:d2:60:a7:bf
 1457 272.309807  GXIndia_81:1c:50      CloudNetwork_60:a7:… ARP      42 Who has 192.168.1.5? Tell 192.168.1.1
 1458 272.309867  CloudNetwork_60:a7:… GXIndia_81:1c:50      ARP      42 192.168.1.5 is at f8:89:d2:60:a7:bf
 1510 311.734185  GXIndia_81:1c:50      CloudNetwork_60:a7:… ARP      42 Who has 192.168.1.5? Tell 192.168.1.1
 1511 311.734292  CloudNetwork_60:a7:… GXIndia_81:1c:50      ARP      42 192.168.1.5 is at f8:89:d2:60:a7:bf
 1531 356.930525  GXIndia_81:1c:50      CloudNetwork_60:a7:… ARP      42 Who has 192.168.1.5? Tell 192.168.1.1
 1532 356.930566  CloudNetwork_60:a7:… GXIndia_81:1c:50      ARP      42 192.168.1.5 is at f8:89:d2:60:a7:bf
 1617 397.998788  GXIndia_81:1c:50      CloudNetwork_60:a7:… ARP      42 Who has 192.168.1.5? Tell 192.168.1.1
 1618 397.998834  CloudNetwork_60:a7:… GXIndia_81:1c:50      ARP      42 192.168.1.5 is at f8:89:d2:60:a7:bf
```

```
> Frame 302: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{8C33D0A9-
> Ethernet II, Src: CloudNetwork_60:a7:bf (f8:89:d2:60:a7:bf), Dst: GXIndia_81:1c:50 (20:0c:86:81:1c:50)
> Address Resolution Protocol (reply)
```

```
0000  20 0c 86 81 1c 50 f8 89  d2 60 a7 bf 08 06 00 01   ····P·· ·`······
0010  08 00 06 04 00 02 f8 89  d2 60 a7 bf c0 a8 01 05   ········ ·`······
0020  20 0c 86 81 1c 50 c0 a8  01 01                     ····P·· ··
```

4)UDP:


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

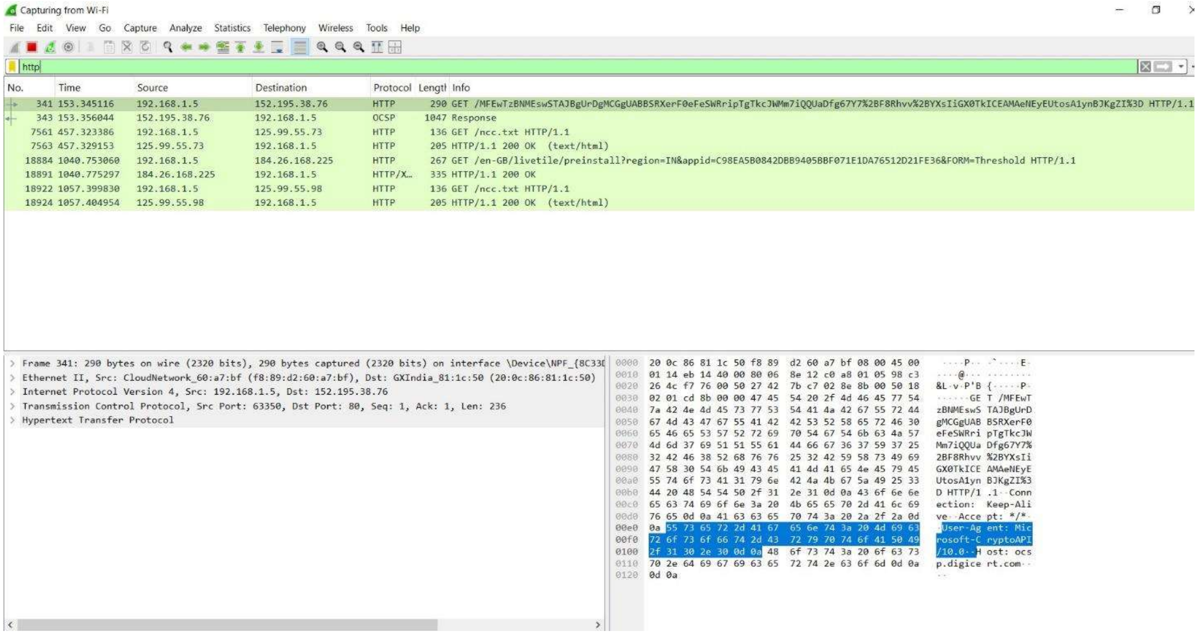
udp

```
No.   Time        Source        Destination      Protocol Lengtl Info
  245 88.083802   192.168.1.2   239.255.255.250  SSDP     167 M-SEARCH * HTTP/1.1
  256 100.168647  192.168.1.2   224.0.0.251      MDNS     103 Standard query 0x001f PTR _233637DE._sub._googlecast._tcp.local, "QM" question PTR _googlecast._tcp.local, "QM" question
  257 101.640890  192.168.1.4   224.0.0.251      MDNS     103 Standard query 0x004f PTR _CC1AD845._sub._googlecast._tcp.local, "QM" question PTR _googlecast._tcp.local, "QM" question
  264 121.161872  192.168.1.2   224.0.0.251      MDNS     103 Standard query 0x0020 PTR _233637DE._sub._googlecast._tcp.local, "QM" question PTR _googlecast._tcp.local, "QM" question
  265 122.082841  192.168.1.4   224.0.0.251      MDNS     103 Standard query 0x0050 PTR _CC1AD845._sub._googlecast._tcp.local, "QM" question PTR _googlecast._tcp.local, "QM" question
  272 131.395856  192.168.1.5   192.168.1.1      DNS       90 Standard query 0xda19 HTTPS config.extension.grammarly.com
  273 131.396277  192.168.1.5   192.168.1.1      DNS       90 Standard query 0x6000 A config.extension.grammarly.com
  274 131.405418  192.168.1.1   192.168.1.5      DNS      210 Standard query response 0xda19 HTTPS config.extension.grammarly.com CNAME d27xxe7juh1us6.cloudfront.net SOA ns-79.awsdns-09.com
  275 131.406368  192.168.1.1   192.168.1.5      DNS      506 Standard query response 0x6000 A config.extension.grammarly.com CNAME d27xxe7juh1us6.cloudfront.net A 108.158.46.111 A 108.158.46.3…
  307 140.003492  192.168.1.2   224.0.0.251      MDNS     103 Standard query 0x0021 PTR _233637DE._sub._googlecast._tcp.local, "QM" question PTR _googlecast._tcp.local, "QM" question
  309 141.681278  192.168.1.4   224.0.0.251      MDNS     103 Standard query 0x0051 PTR _CC1AD845._sub._googlecast._tcp.local, "QM" question PTR _googlecast._tcp.local, "QM" question
  310 142.769411  192.168.1.5   192.168.1.255    UDP      212 56820 → 6646 Len=170
  321 147.586285  192.168.1.2   239.255.255.250  SSDP     167 M-SEARCH * HTTP/1.1
  334 150.689979  192.168.1.5   192.168.1.255    BROWSER  243 Host Announcement DESKTOP-28OA7U1, Workstation, Server, NT Workstation
  347 155.833408  192.168.1.5   192.168.1.1      NBNS     110 Refresh NB DESKTOP-28OA7U1<00>
  348 155.836044  192.168.1.1   192.168.1.5      NBNS     104 Registration response, Request was invalidly formatted NB 192.168.1.5
  349 155.870944  192.168.1.5   239.255.255.250  SSDP     179 M-SEARCH * HTTP/1.1
  356 155.890190  192.168.1.5   224.0.0.251      MDNS      81 Standard query 0x0000 ANY DESKTOP-28OA7U1.local, "QM" question
```

```
> Frame 275: 506 bytes on wire (4048 bits), 506 bytes captured (4048 bits) on interface \Device\NPF_{8C33D
> Ethernet II, Src: GXIndia_81:1c:50 (20:0c:86:81:1c:50), Dst: CloudNetwork_60:a7:bf (f8:89:d2:60:a7:bf)
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.5
> User Datagram Protocol, Src Port: 53, Dst Port: 57903
> Domain Name System (response)
```

```
0000  f8 89 d2 60 a7 bf 20 0c  86 81 1c 50 08 00 45 00   ···`·· · ···P··E·
0010  01 ec 7b 79 40 00 40 11  3a 31 c0 a8 01 01 c0 a8   ··{y@·@· :1······
0020  01 05 00 35 e2 2f 01 d8  f2 86 60 00 81 80 00 01   ···5·/·· ··`·····
0030  00 05 00 04 00 08 06 63  6f 6e 66 69 67 09 65 78   ·······c onfig·ex
0040  74 65 6e 73 69 6f 6e 09  67 72 61 6d 6d 61 72 6c   tension· grammarl
0050  79 03 63 6f 6d 00 00 01  00 01 c0 0c 00 05 00 01   y·com··· ········
0060  00 00 01 21 00 1f 0e 64  32 37 78 78 65 37 6a 75   ···!···d 27xxe7ju
0070  68 31 75 73 36 0a 63 6c  6f 75 64 66 72 6f 6e 74   h1us6·cl oudfront
0080  03 6e 65 74 00 c0 3c 00  01 00 01 00 00 00 35 00   ·net··<· ······5·
0090  04 6c 9e 2e 6f c0 3c 00  01 00 01 00 00 00 35 00   ·l·.o·<· ······5·
00a0  04 6c 9e 2e 27 c0 3c 00  01 00 01 00 00 00 35 00   ·l·.'·<· ······5·
00b0  04 6c 9e 2e 2f c0 3c 00  01 00 01 00 00 00 35 00   ·l·./·<· ······5·
00c0  04 6c 9e 2e 66 c0 3c 00  02 00 01 00 00 05 b9 00   ·l·.f·<· ········
00d0  17 07 6e 73 2d 31 32 38  32 09 61 77 73 64 6e 73   ··ns-128 2·awsdns
00e0  2d 33 32 03 6f 72 67 00  c0 3c 00 02 00 01 00 00   -32·org· ·<······
00f0  05 b9 00 19 07 6e 73 2d  31 38 32 30 09 61 77 73   ·····ns- 1820·aws
0100  64 6e 73 2d 33 35 02 63  6f 02 75 6b 00 c0 3c 00   dns-35·c o·uk··<·
0110  02 00 01 00 00 05 b9 00  13 06 6e 73 2d 35 33 36   ········ ··ns-536
0120  09 61 77 73 64 6e 73 2d  30 33 c0 56 c0 3c 00 02   ·awsdns- 03·V·<··
0130  00 01 00 00 05 b9 00 12  05 6e 73 2d 37 39 09 61   ········ ·ns-79·a
0140  77 73 64 6e 73 2d 30 39  c0 27 c1 0e 00 01 00 01   wsdns-09 ·'······
0150  00 01 72 1e 00 04 cd fb  c0 4f c0 ef 00 01 00 01   ··r····· ·O······
0160  00 01 72 24 00 04 cd fb  c2 18 c0 a7 00 01 00 01   ··r$···· ········
```

5)HTTP:


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

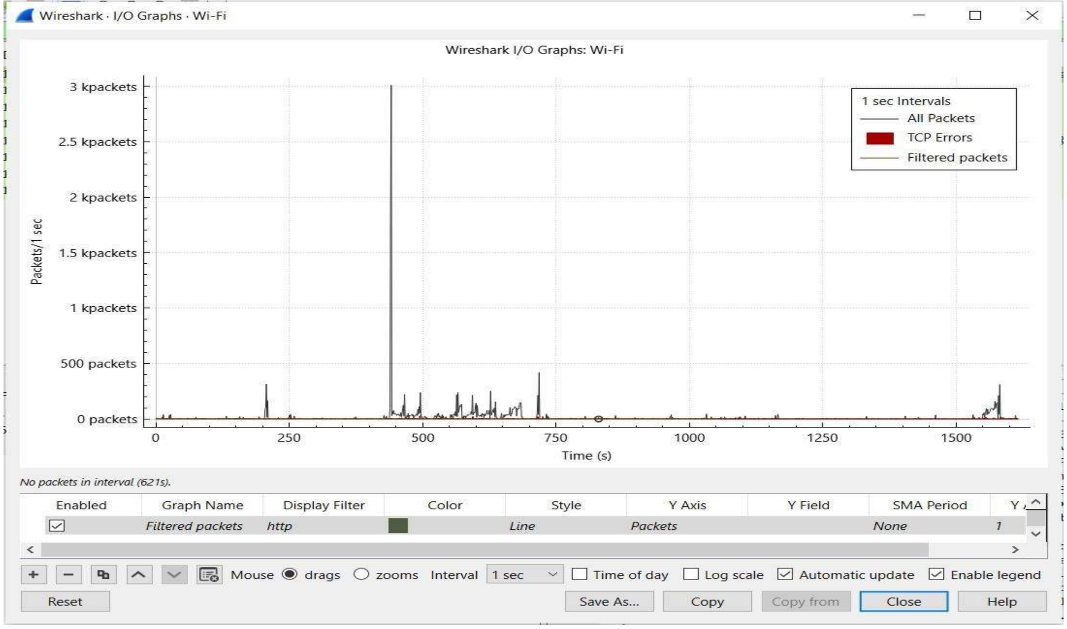
http

```
No.    Time         Source          Destination     Protocol Length Info
  341  153.345116   192.168.1.5     152.195.38.76   HTTP     290 GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBSRXerF0eFeSWRripTgTkcJWMm7iQQUaDfg67Y7%2BF8Rhvv%2BYXsIiGX0TkICEAMAeNEyEUtosA1ynBJKgZI%3D HTTP/1.1
  343  153.356044   152.195.38.76   192.168.1.5     OCSP     1047 Response
 7561  457.323386   192.168.1.5     125.99.55.73    HTTP     136 GET /ncc.txt HTTP/1.1
 7563  457.329153   125.99.55.73    192.168.1.5     HTTP     205 HTTP/1.1 200 OK  (text/html)
18884 1040.753060   192.168.1.5     184.26.168.225  HTTP     267 GET /en-GB/livetile/preinstall?region=IN&appid=C98EA5B0842DBB9405BBF071E1DA76512D21FE36&FORM=Threshold HTTP/1.1
18891 1040.775297   184.26.168.225  192.168.1.5     HTTP/X…  335 HTTP/1.1 200 OK
18922 1057.399830   192.168.1.5     125.99.55.98    HTTP     136 GET /ncc.txt HTTP/1.1
18924 1057.404954   125.99.55.98    192.168.1.5     HTTP     205 HTTP/1.1 200 OK  (text/html)
```

```
> Frame 341: 290 bytes on wire (2320 bits), 290 bytes captured (2320 bits) on interface \Device\NPF_{8C33D
> Ethernet II, Src: CloudNetwork_60:a7:bf (f8:89:d2:60:a7:bf), Dst: GXIndia_81:1c:50 (20:0c:86:81:1c:50)
> Internet Protocol Version 4, Src: 192.168.1.5, Dst: 152.195.38.76
> Transmission Control Protocol, Src Port: 63350, Dst Port: 80, Seq: 1, Ack: 1, Len: 236
> Hypertext Transfer Protocol
```

```
0000  20 0c 86 81 1c 50 f8 89  d2 60 a7 bf 08 00 45 00   ····P·· ·`····E·
0010  01 14 eb 14 40 00 80 06  8e 12 c0 a8 01 05 98 c3   ····@··· ········
0020  26 4c f7 76 00 50 27 42  7b c7 02 8e 8b 00 50 18   &L·v·P'B {·····P·
0030  02 01 cd 8b 00 00 47 45  54 20 2f 4d 46 45 77 54   ······GE T /MFEwT
0040  7a 42 4e 4d 45 73 77 53  54 41 4a 42 67 55 72 44   zBNMEswS TAJBgUrD
0050  67 4d 43 47 67 55 41 42  42 53 52 58 65 72 46 30   gMCGgUAB BSRXerF0
0060  65 46 65 53 57 52 72 69  70 54 67 54 6b 63 4a 57   eFeSWRri pTgTkcJW
0070  4d 6d 37 69 51 51 55 61  44 66 67 36 37 59 37 25   Mm7iQQUa Dfg67Y7%
0080  32 42 46 38 52 68 76 76  25 32 42 59 58 73 49 69   2BF8Rhvv %2BYXsIi
0090  47 58 30 54 6b 49 43 45  41 4d 41 65 4e 45 79 45   GX0TkICE AMAeNEyE
00a0  55 74 6f 73 41 31 79 6e  42 4a 4b 67 5a 49 25 33   UtosA1yn BJKgZI%3
00b0  44 20 48 54 54 50 2f 31  2e 31 0d 0a 43 6f 6e 6e   D HTTP/1 .1··Conn
00c0  65 63 74 69 6f 6e 3a 20  4b 65 65 70 2d 41 6c 69   ection:  Keep-Ali
00d0  76 65 0d 0a 41 63 63 65  70 74 3a 20 2a 2f 2a 0d   ve··Acce pt: */*·
00e0  0a 55 73 65 72 2d 41 67  65 6e 74 3a 20 4d 69 63   ·User-Ag ent: Mic
00f0  72 6f 73 6f 66 74 2d 43  72 79 70 74 6f 41 50 49   rosoft-C ryptoAPI
0100  2f 31 30 2e 30 0d 0a 48  6f 73 74 3a 20 6f 63 73   /10.0··H ost: ocs
0110  70 2e 64 69 67 69 63 65  72 74 2e 63 6f 6d 0d 0a   p.digice rt.com··
0120  0d 0a                                              ··
```

6)I/O GRAPH:



No packets in interval (621s).

Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field	SMA Period	Y
☑	Filtered packets	http	■	Line	Packets		None	1

Mouse ● drags ○ zooms Interval 1 sec ☐ Time of day ☐ Log scale ☑ Automatic update ☑ Enable legend

Conclusion:

Thus, we successfully implemented Packet Capturing Using Wireshark.