Name : Anish Kumar **Roll No : 2300290120041**

Basic Packet Inspection Using Wireshark

Objective

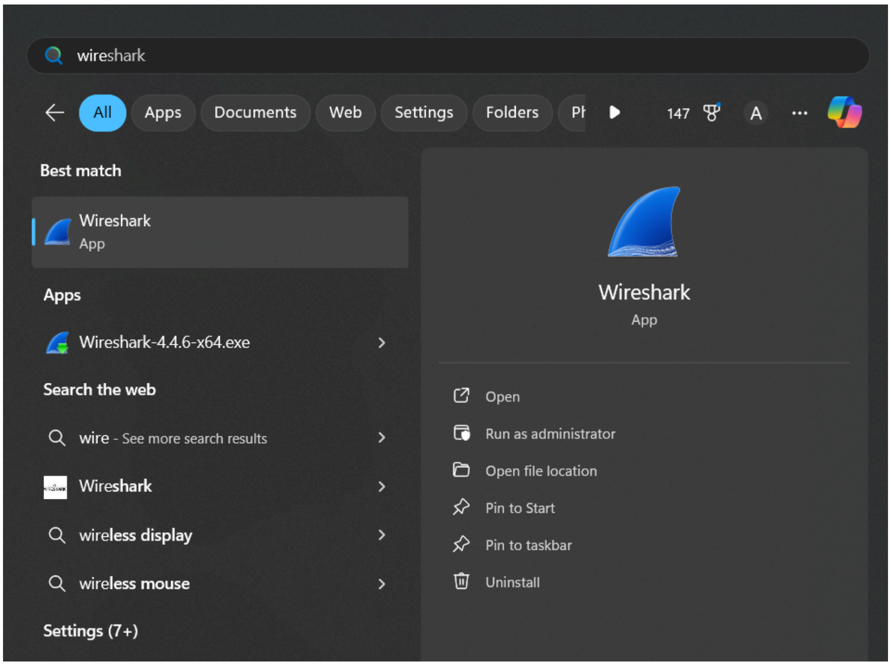
To capture and analyze network traffic using **Wireshark** to understand how common protocols (HTTP, DNS, ARP, TCP, UDP, FTP, IP, SMTP) work and how data is transmitted and received.

1. Tools Used

- **Wireshark** (a free and open-source packet analyzer)
- A working internet connection
- Optional: a web browser or command-line tools to generate protocol traffic (e.g., `ping`, `ftp`, `telnet`, email clients)

2. Capturing Packets with Wireshark

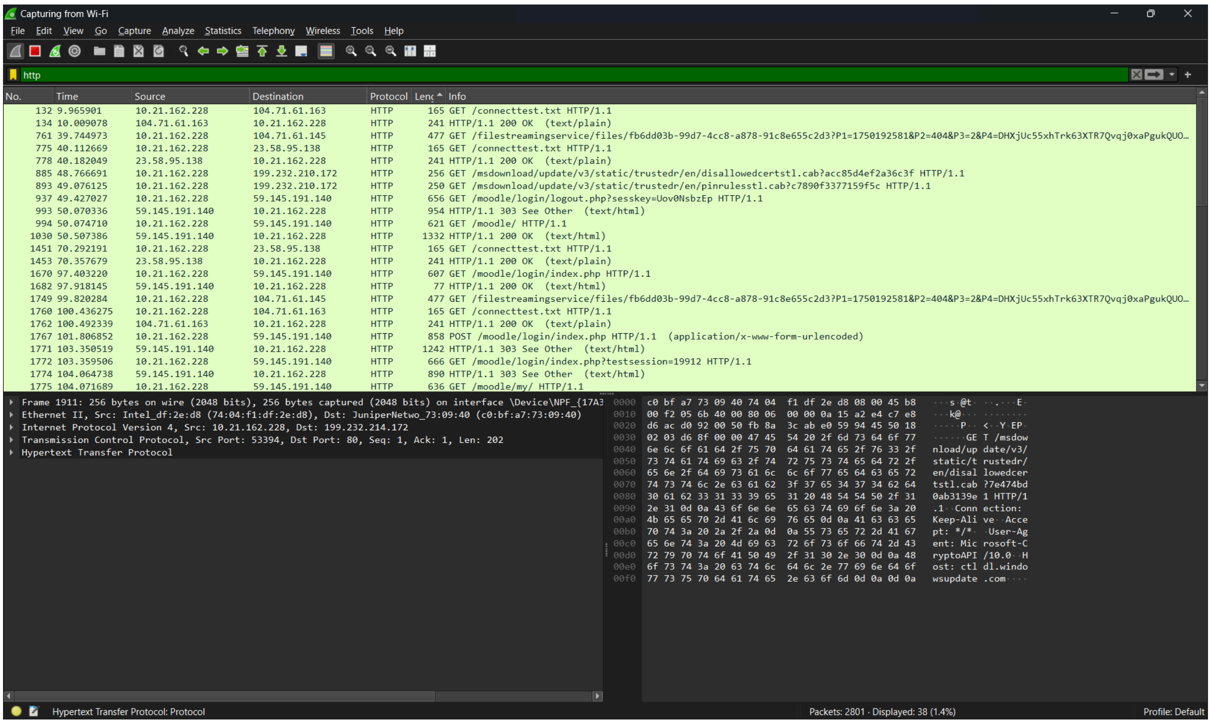
1. Open Wireshark.
2. Select the active network interface (e.g., Wi-Fi or Ethernet).
3. Click **Start Capturing Packets**.
4. Perform actions like visiting websites, sending emails, or using FTP to generate protocol traffic.
5. Click **Stop** after collecting sufficient data.



3. Protocol Analysis

A. HTTP (Hypertext Transfer Protocol)

- **Port:** 80
- **Use:** Web browsing (fetching websites)
- **How to identify in Wireshark:** Filter by `http`
- **Look for:**
    - GET/POST requests
    - Response headers (e.g., `200 OK`)
    - Hostname and URI



http

```
No.   Time        Source           Destination      Protocol Leng Info
  132 9.965901    10.21.162.228    104.71.61.163    HTTP      165 GET /connecttest.txt HTTP/1.1
  134 10.009078   104.71.61.163    10.21.162.228    HTTP      241 HTTP/1.1 200 OK  (text/plain)
  761 39.744973   10.21.162.228    104.71.61.145    HTTP      477 GET /filestreamingservice/files/fb6dd03b-99d7-4cc8-a878-91c8e655c2d3?P1=1750192581&P2=404&P3=2&P4=DHXjUc55xhTrk63XTR7Qvqj0xaPgukQUO…
  775 40.112669   10.21.162.228    23.58.95.138     HTTP      165 GET /connecttest.txt HTTP/1.1
  778 40.182049   23.58.95.138     10.21.162.228    HTTP      241 HTTP/1.1 200 OK  (text/plain)
  885 48.766691   10.21.162.228    199.232.210.172  HTTP      256 GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?acc85d4ef2a36c3f HTTP/1.1
  893 49.076125   10.21.162.228    199.232.210.172  HTTP      250 GET /msdownload/update/v3/static/trustedr/en/pinrulesstl.cab?c7890f3377159f5c HTTP/1.1
  937 49.427027   10.21.162.228    59.145.191.140   HTTP      656 GET /moodle/login/logout.php?sesskey=Uov0NsbzEp HTTP/1.1
  993 50.070336   59.145.191.140   10.21.162.228    HTTP      954 HTTP/1.1 303 See Other  (text/html)
  994 50.074710   10.21.162.228    59.145.191.140   HTTP      621 GET /moodle/ HTTP/1.1
 1030 50.507386   59.145.191.140   10.21.162.228    HTTP     1332 HTTP/1.1 200 OK  (text/html)
 1451 70.292191   10.21.162.228    23.58.95.138     HTTP      165 GET /connecttest.txt HTTP/1.1
 1453 70.357679   23.58.95.138     10.21.162.228    HTTP      241 HTTP/1.1 200 OK  (text/plain)
 1670 97.403220   10.21.162.228    59.145.191.140   HTTP      607 GET /moodle/login/index.php HTTP/1.1
 1682 97.918145   59.145.191.140   10.21.162.228    HTTP       77 HTTP/1.1 200 OK  (text/html)
 1749 99.820284   10.21.162.228    104.71.61.145    HTTP      477 GET /filestreamingservice/files/fb6dd03b-99d7-4cc8-a878-91c8e655c2d3?P1=1750192581&P2=404&P3=2&P4=DHXjUc55xhTrk63XTR7Qvqj0xaPgukQUO…
 1760 100.436275  10.21.162.228    104.71.61.163    HTTP      165 GET /connecttest.txt HTTP/1.1
 1762 100.492339  104.71.61.163    10.21.162.228    HTTP      241 HTTP/1.1 200 OK  (text/plain)
 1767 101.806852  10.21.162.228    59.145.191.140   HTTP      858 POST /moodle/login/index.php HTTP/1.1  (application/x-www-form-urlencoded)
 1771 103.350519  59.145.191.140   10.21.162.228    HTTP     1242 HTTP/1.1 303 See Other  (text/html)
 1772 103.359506  10.21.162.228    59.145.191.140   HTTP      666 GET /moodle/login/index.php?testsession=19912 HTTP/1.1
 1774 104.064738  59.145.191.140   10.21.162.228    HTTP      890 HTTP/1.1 303 See Other  (text/html)
 1775 104.071689  10.21.162.228    59.145.191.140   HTTP      636 GET /moodle/my/ HTTP/1.1
```

```
▸ Frame 1911: 256 bytes on wire (2048 bits), 256 bytes captured (2048 bits) on interface \Device\NPF_{17A3
▸ Ethernet II, Src: Intel_df:2e:d8 (74:04:f1:df:2e:d8), Dst: JuniperNetwo_73:09:40 (c0:bf:a7:73:09:40)
▸ Internet Protocol Version 4, Src: 10.21.162.228, Dst: 199.232.214.172
▸ Transmission Control Protocol, Src Port: 53394, Dst Port: 80, Seq: 1, Ack: 1, Len: 202
▸ Hypertext Transfer Protocol
```

```
0000  c0 bf a7 73 09 40 74 04  f1 df 2e d8 08 00 45 b8   ···s·@t· ··.···E·
0010  00 f2 05 6b 40 00 80 06  00 00 0a 15 a2 e4 c7 e8   ···k@··· ········
0020  d6 ac d0 92 00 50 fb 8a  3c ab e0 59 94 45 50 18   ·····P·· <··Y·EP·
0030  02 03 d6 8f 00 00 47 45  54 20 2f 6d 73 64 6f 77   ······GE T /msdow
0040  6e 6c 6f 61 64 2f 75 70  64 61 74 65 2f 76 33 2f   nload/up date/v3/
0050  73 74 61 74 69 63 2f 74  72 75 73 74 65 64 72 2f   static/t rustedr/
0060  65 6e 2f 64 69 73 61 6c  6c 6f 77 65 64 63 65 72   en/disal lowedcer
0070  74 73 74 6c 2e 63 61 62  3f 37 65 34 37 34 62 64   tstl.cab ?7e474bd
0080  30 61 62 33 31 33 39 65  31 20 48 54 54 50 2f 31   0ab3139e 1 HTTP/1
0090  2e 31 0d 0a 43 6f 6e 6e  65 63 74 69 6f 6e 3a 20   .1··Conn ection: 
00a0  4b 65 65 70 2d 41 6c 69  76 65 0d 0a 41 63 63 65   Keep-Ali ve··Acce
00b0  70 74 3a 20 2a 2f 2a 0d  0a 55 73 65 72 2d 41 67   pt: */*· ·User-Ag
00c0  65 6e 74 3a 20 4d 69 63  72 6f 73 6f 66 74 2d 43   ent: Mic rosoft-C
00d0  72 79 70 74 6f 41 50 49  2f 31 30 2e 30 0d 0a 48   ryptoAPI /10.0··H
00e0  6f 73 74 3a 20 63 74 6c  64 6c 2e 77 69 6e 64 6f   ost: ctl dl.windo
00f0  77 73 75 70 64 61 74 65  2e 63 6f 6d 0d 0a 0d 0a   wsupdate .com····
```

Hypertext Transfer Protocol: Protocol

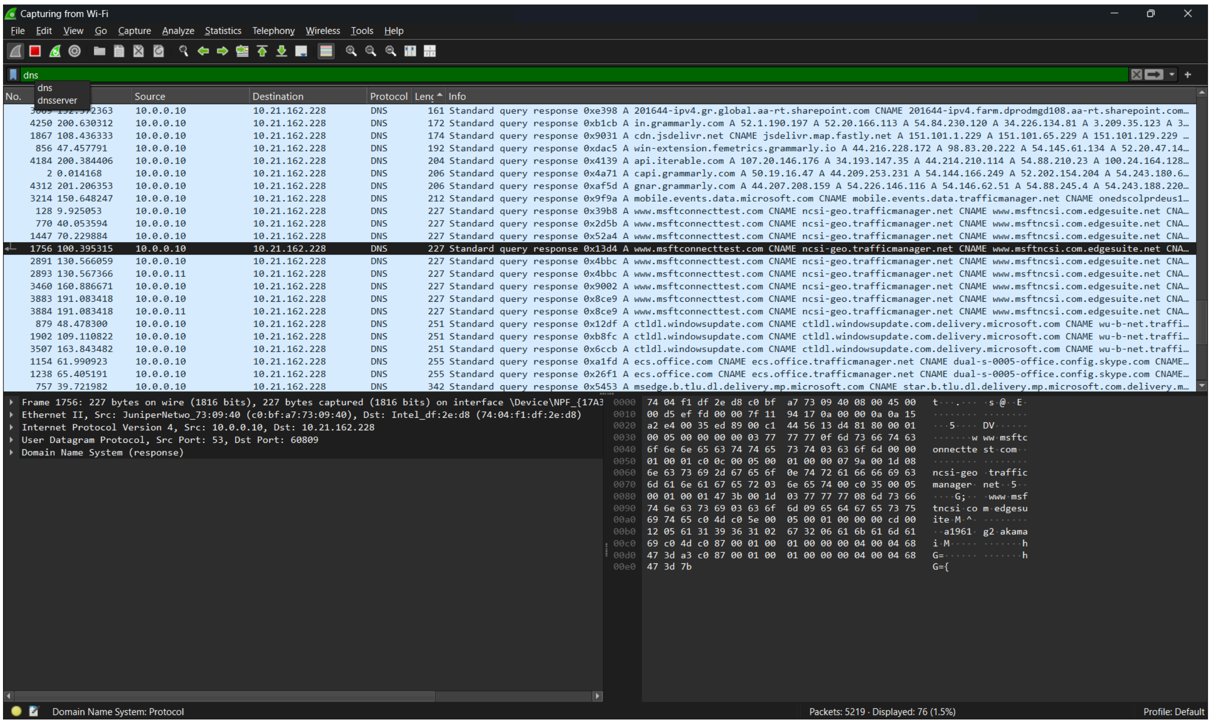
Packets: 2801 · Displayed: 38 (1.4%)

Profile: Default

B. DNS (Domain Name System)

- **Port:** 53 (UDP or TCP)
- **Use:** Translates domain names to IP addresses

- **Filter:** `dns`
- **Look for:**
    - DNS queries (`Standard query`)
    - Responses with IP addresses



Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
dns
dnsserver
Domain Name System: Protocol
Packets: 5219 · Displayed: 76 (1.5%)
Profile: Default

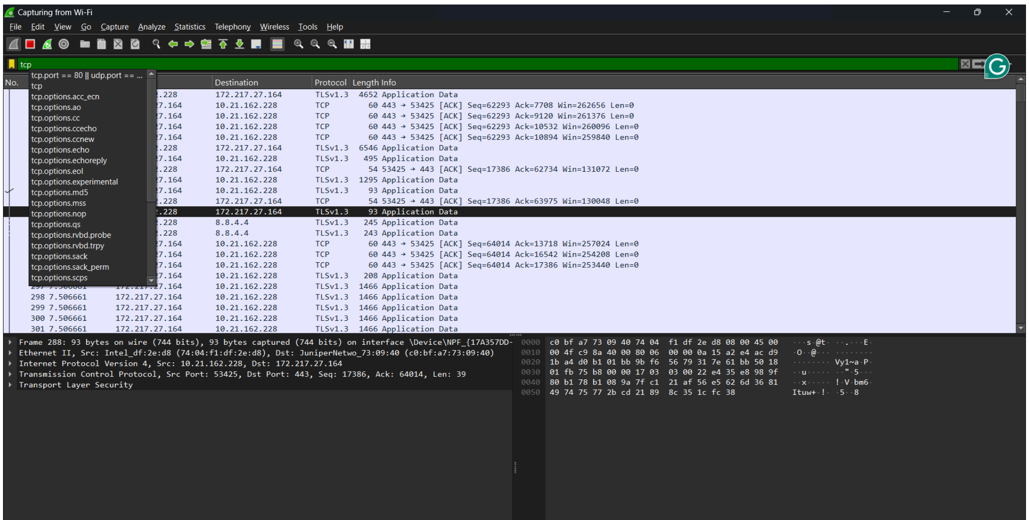
```
No.                 Source        Destination      Protocol Leng Info
        72363       10.0.0.10     10.21.162.228    DNS      161 Standard query response 0xe398 A 201644-ipv4.gr.global.aa-rt.sharepoint.com CNAME 201644-ipv4.farm.dprodmgd108.aa-rt.sharepoint.com…
   4250 200.630312  10.0.0.10     10.21.162.228    DNS      172 Standard query response 0xb1cb A in.grammarly.com A 52.1.190.197 A 52.20.166.113 A 54.84.230.120 A 34.226.134.81 A 3.209.35.123 A 3…
   1867 108.436333  10.0.0.10     10.21.162.228    DNS      174 Standard query response 0x9031 A cdn.jsdelivr.net CNAME jsdelivr.map.fastly.net A 151.101.1.229 A 151.101.65.229 A 151.101.129.229 …
    856 47.457791   10.0.0.10     10.21.162.228    DNS      192 Standard query response 0xdac5 A win-extension.femetrics.grammarly.io A 44.216.228.172 A 98.83.20.222 A 54.145.61.134 A 52.20.47.14…
   4184 200.384406  10.0.0.10     10.21.162.228    DNS      204 Standard query response 0x4139 A api.iterable.com A 107.20.146.176 A 34.193.147.35 A 44.214.210.114 A 54.88.210.23 A 100.24.164.128…
      2 0.014168    10.0.0.10     10.21.162.228    DNS      206 Standard query response 0x4a71 A capi.grammarly.com A 50.19.16.47 A 44.209.253.231 A 54.144.166.249 A 52.202.154.204 A 54.243.180.6…
   4312 201.206353  10.0.0.10     10.21.162.228    DNS      206 Standard query response 0xaf5d A gnar.grammarly.com A 44.207.208.159 A 54.226.146.116 A 54.146.62.51 A 54.88.245.4 A 54.243.188.220…
   3214 150.648247  10.0.0.10     10.21.162.228    DNS      212 Standard query response 0x9f9a A mobile.events.data.microsoft.com CNAME mobile.events.data.trafficmanager.net CNAME onedscolprdeus1…
    128 9.925053    10.0.0.10     10.21.162.228    DNS      227 Standard query response 0x39b8 A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME www.msftncsi.com.edgesuite.net CNA…
    770 40.053594   10.0.0.10     10.21.162.228    DNS      227 Standard query response 0x2d5b A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME www.msftncsi.com.edgesuite.net CNA…
   1447 70.229884   10.0.0.10     10.21.162.228    DNS      227 Standard query response 0x52a4 A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME www.msftncsi.com.edgesuite.net CNA…
   1756 100.395315  10.0.0.10     10.21.162.228    DNS      227 Standard query response 0x13d4 A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME www.msftncsi.com.edgesuite.net CNA…
   2891 130.566059  10.0.0.10     10.21.162.228    DNS      227 Standard query response 0x4bbc A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME www.msftncsi.com.edgesuite.net CNA…
   2893 130.567366  10.0.0.11     10.21.162.228    DNS      227 Standard query response 0x4bbc A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME www.msftncsi.com.edgesuite.net CNA…
   3460 160.886671  10.0.0.10     10.21.162.228    DNS      227 Standard query response 0x9002 A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME www.msftncsi.com.edgesuite.net CNA…
   3883 191.083418  10.0.0.10     10.21.162.228    DNS      227 Standard query response 0x8ce9 A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME www.msftncsi.com.edgesuite.net CNA…
   3884 191.083418  10.0.0.11     10.21.162.228    DNS      227 Standard query response 0x8ce9 A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME www.msftncsi.com.edgesuite.net CNA…
    879 48.478300   10.0.0.10     10.21.162.228    DNS      251 Standard query response 0x12df A ctldl.windowsupdate.com CNAME ctldl.windowsupdate.com.delivery.microsoft.com CNAME wu-b-net.traffi…
   1902 109.110822  10.0.0.10     10.21.162.228    DNS      251 Standard query response 0xb8fc A ctldl.windowsupdate.com CNAME ctldl.windowsupdate.com.delivery.microsoft.com CNAME wu-b-net.traffi…
   3507 163.843482  10.0.0.10     10.21.162.228    DNS      251 Standard query response 0x6ccb A ctldl.windowsupdate.com CNAME ctldl.windowsupdate.com.delivery.microsoft.com CNAME wu-b-net.traffi…
   1154 61.990923   10.0.0.10     10.21.162.228    DNS      255 Standard query response 0xa1fd A ecs.office.com CNAME ecs.office.trafficmanager.net CNAME dual-s-0005-office.config.skype.com CNAME…
   1238 65.405191   10.0.0.10     10.21.162.228    DNS      255 Standard query response 0x26f1 A ecs.office.com CNAME ecs.office.trafficmanager.net CNAME dual-s-0005-office.config.skype.com CNAME…
    757 39.721982   10.0.0.10     10.21.162.228    DNS      342 Standard query response 0x5453 A msedge.b.tlu.dl.delivery.mp.microsoft.com CNAME star.b.tlu.dl.delivery.mp.microsoft.com.delivery.m…
```

```
▸ Frame 1756: 227 bytes on wire (1816 bits), 227 bytes captured (1816 bits) on interface \Device\NPF_{17A3
▸ Ethernet II, Src: JuniperNetwo_73:09:40 (c0:bf:a7:73:09:40), Dst: Intel_df:2e:d8 (74:04:f1:df:2e:d8)
▸ Internet Protocol Version 4, Src: 10.0.0.10, Dst: 10.21.162.228
▸ User Datagram Protocol, Src Port: 53, Dst Port: 60809
▸ Domain Name System (response)
```

```
0000  74 04 f1 df 2e d8 c0 bf  a7 73 09 40 08 00 45 00   t···.··· ·s·@··E·
0010  00 d5 ef fd 00 00 7f 11  94 17 0a 00 00 0a 0a 15   ········ ········
0020  a2 e4 00 35 ed 89 00 c1  44 56 13 d4 81 80 00 01   ···5···· DV······
0030  00 05 00 00 00 00 03 77  77 77 0f 6d 73 66 74 63   ·······w ww·msftc
0040  6f 6e 6e 65 63 74 74 65  73 74 03 63 6f 6d 00 00   onnectte st·com··
0050  01 00 01 c0 0c 00 05 00  01 00 00 07 9a 00 1d 08   ········ ········
0060  6e 63 73 69 2d 67 65 6f  0e 74 72 61 66 66 69 63   ncsi-geo ·traffic
0070  6d 61 6e 61 67 65 72 03  6e 65 74 00 c0 35 00 05   manager· net··5··
0080  00 01 00 01 47 3b 00 1d  03 77 77 77 08 6d 73 66   ····G;·· ·www·msf
0090  74 6e 63 73 69 03 63 6f  6d 09 65 64 67 65 73 75   tncsi·co m·edgesu
00a0  69 74 65 c0 4d c0 5e 00  05 00 01 00 00 00 cd 00   ite·M·^· ········
00b0  12 05 61 31 39 36 31 02  67 32 06 61 6b 61 6d 61   ··a1961· g2·akama
00c0  69 c0 4d c0 87 00 01 00  01 00 00 00 04 00 04 68   i·M····· ·······h
00d0  47 3d a3 c0 87 00 01 00  01 00 00 00 04 00 04 68   G=······ ·······h
00e0  47 3d 7b                                           G={
```

D. TCP (Transmission Control Protocol)

- **Use:** Reliable, connection-oriented communication
- **Filter:** `tcp`
- **Look for:**
    - 3-way handshake (`SYN`, `SYN-ACK`, `ACK`)
    - Sequence and acknowledgment numbers



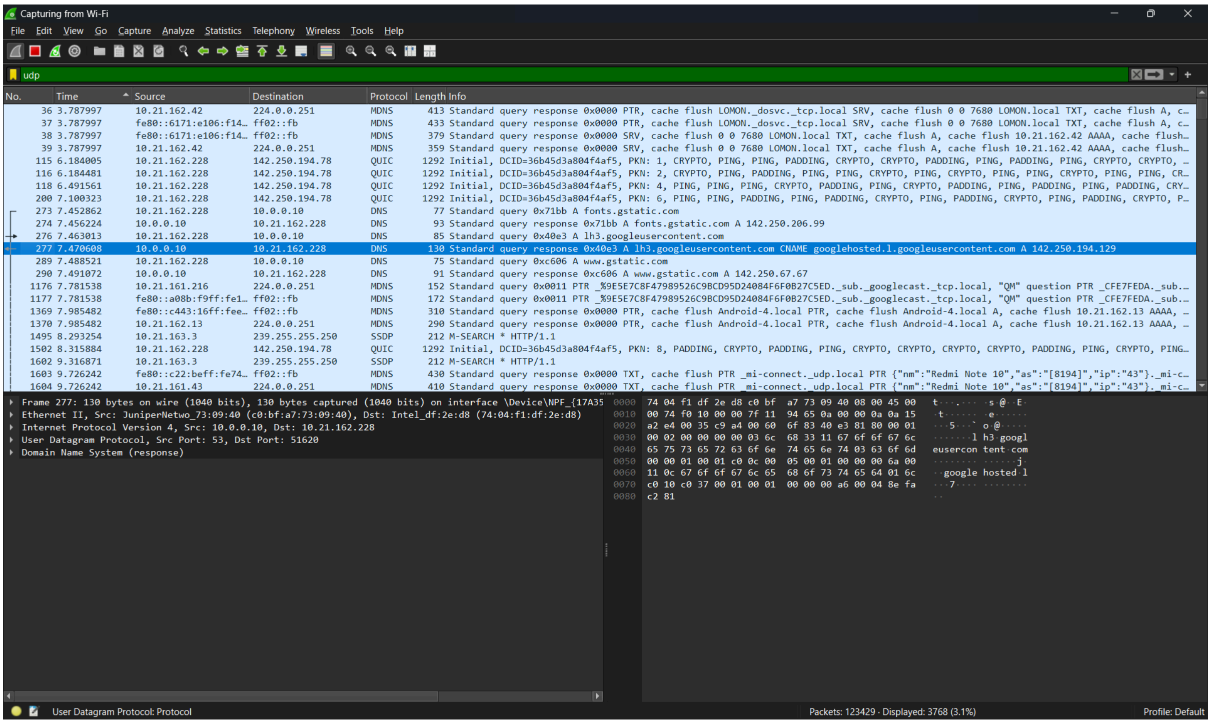
```
No.                          Destination      Protocol Length Info
                    .228     172.217.27.164   TLSv1.3  4652 Application Data
                    7.164    10.21.162.228    TCP        60 443 → 53425 [ACK] Seq=62293 Ack=7708 Win=262656 Len=0
                    7.164    10.21.162.228    TCP        60 443 → 53425 [ACK] Seq=62293 Ack=9120 Win=261376 Len=0
                    7.164    10.21.162.228    TCP        60 443 → 53425 [ACK] Seq=62293 Ack=10532 Win=260096 Len=0
                    7.164    10.21.162.228    TCP        60 443 → 53425 [ACK] Seq=62293 Ack=10894 Win=259840 Len=0
                    .228     172.217.27.164   TLSv1.3  6546 Application Data
                    7.164    10.21.162.228    TLSv1.3   495 Application Data
                    .228     172.217.27.164   TCP        54 53425 → 443 [ACK] Seq=17386 Ack=62734 Win=131072 Len=0
                    7.164    10.21.162.228    TLSv1.3  1295 Application Data
                    7.164    10.21.162.228    TLSv1.3    93 Application Data
                    .228     172.217.27.164   TCP        54 53425 → 443 [ACK] Seq=17386 Ack=63975 Win=130048 Len=0
                    .228     172.217.27.164   TLSv1.3    93 Application Data
                    .228     8.8.4.4          TLSv1.3   245 Application Data
                    .228     8.8.4.4          TLSv1.3   243 Application Data
                    7.164    10.21.162.228    TCP        60 443 → 53425 [ACK] Seq=64014 Ack=13718 Win=257024 Len=0
                    7.164    10.21.162.228    TCP        60 443 → 53425 [ACK] Seq=64014 Ack=16542 Win=254208 Len=0
                    7.164    10.21.162.228    TCP        60 443 → 53425 [ACK] Seq=64014 Ack=17386 Win=253440 Len=0
                    7.164    10.21.162.228    TLSv1.3   208 Application Data
                    7.164    10.21.162.228    TLSv1.3  1466 Application Data
  298 7.506661  172.217.27.164   10.21.162.228    TLSv1.3  1466 Application Data
  299 7.506661  172.217.27.164   10.21.162.228    TLSv1.3  1466 Application Data
  300 7.506661  172.217.27.164   10.21.162.228    TLSv1.3  1466 Application Data
  301 7.506661  172.217.27.164   10.21.162.228    TLSv1.3  1466 Application Data
```

```
▸ Frame 288: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface \Device\NPF_{17A357DD-
▸ Ethernet II, Src: Intel_df:2e:d8 (74:04:f1:df:2e:d8), Dst: JuniperNetwo_73:09:40 (c0:bf:a7:73:09:40)
▸ Internet Protocol Version 4, Src: 10.21.162.228, Dst: 172.217.27.164
▸ Transmission Control Protocol, Src Port: 53425, Dst Port: 443, Seq: 17386, Ack: 64014, Len: 39
▸ Transport Layer Security
```

```
0000  c0 bf a7 73 09 40 74 04  f1 df 2e d8 08 00 45 00   ···s·@t· ··.···E·
0010  00 4f c9 8a 40 00 80 06  00 00 0a 15 a2 e4 ac d9   ·O··@··· ········
0020  1b a4 d0 b1 01 bb 9b f6  56 79 31 7e 61 bb 50 18   ········ Vy1~a·P·
0030  01 fb 75 b8 00 00 17 03  03 00 22 e4 35 e8 98 9f   ··u····· ··"·5···
0040  80 b1 78 b1 08 9a 7f c1  21 af 56 e5 62 6d 36 81   ··x····· !·V·bm6·
0050  49 74 75 77 2b cd 21 89  8c 35 1c fc 38            Ituw+·!· ·5··8
```

E. UDP (User Datagram Protocol)

- **Use:** Faster, connectionless communication (e.g., video streaming)
- **Filter:** `udp`
- **Look for:**
  - Lightweight packets without handshakes
  - Often used with DNS, VoIP, streaming services



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

```
No.   Time       Source               Destination      Protocol Length Info
   36 3.787997   10.21.162.42         224.0.0.251      MDNS      413 Standard query response 0x0000 PTR, cache flush LOMON._dosvc._tcp.local SRV, cache flush 0 0 7680 LOMON.local TXT, cache flush A, c…
   37 3.787997   fe80::6171:e106:f14… ff02::fb         MDNS      433 Standard query response 0x0000 PTR, cache flush LOMON._dosvc._tcp.local SRV, cache flush 0 0 7680 LOMON.local TXT, cache flush A, c…
   38 3.787997   fe80::6171:e106:f14… ff02::fb         MDNS      379 Standard query response 0x0000 SRV, cache flush 0 0 7680 LOMON.local TXT, cache flush A, cache flush 10.21.162.42 AAAA, cache flush…
   39 3.787997   10.21.162.42         224.0.0.251      MDNS      359 Standard query response 0x0000 SRV, cache flush 0 0 7680 LOMON.local TXT, cache flush A, cache flush 10.21.162.42 AAAA, cache flush…
  115 6.184005   10.21.162.228        142.250.194.78   QUIC     1292 Initial, DCID=36b45d3a804f4af5, PKN: 1, CRYPTO, PING, PING, PADDING, CRYPTO, CRYPTO, PADDING, PING, PADDING, PING, CRYPTO, CRYPTO, …
  116 6.184481   10.21.162.228        142.250.194.78   QUIC     1292 Initial, DCID=36b45d3a804f4af5, PKN: 2, CRYPTO, PING, PADDING, PING, PING, CRYPTO, PING, CRYPTO, PING, PING, CRYPTO, PING, PING, CR…
  118 6.491561   10.21.162.228        142.250.194.78   QUIC     1292 Initial, DCID=36b45d3a804f4af5, PKN: 4, PING, PING, PING, CRYPTO, PADDING, PING, CRYPTO, PADDING, PING, PADDING, PING, PADDING, CRY…
  200 7.100323   10.21.162.228        142.250.194.78   QUIC     1292 Initial, DCID=36b45d3a804f4af5, PKN: 6, PING, PING, PADDING, PING, PADDING, CRYPTO, PING, PADDING, CRYPTO, PING, PADDING, CRYPTO, P…
  273 7.452862   10.21.162.228        10.0.0.10        DNS        77 Standard query 0x71bb A fonts.gstatic.com
  274 7.456224   10.0.0.10            10.21.162.228    DNS        93 Standard query response 0x71bb A fonts.gstatic.com A 142.250.206.99
  276 7.463013   10.21.162.228        10.0.0.10        DNS        85 Standard query 0x40e3 A lh3.googleusercontent.com
  277 7.470608   10.0.0.10            10.21.162.228    DNS       130 Standard query response 0x40e3 A lh3.googleusercontent.com CNAME googlehosted.l.googleusercontent.com A 142.250.194.129
  289 7.488521   10.21.162.228        10.0.0.10        DNS        75 Standard query 0xc606 A www.gstatic.com
  290 7.491072   10.0.0.10            10.21.162.228    DNS        91 Standard query response 0xc606 A www.gstatic.com A 142.250.67.67
 1176 7.781538   10.21.161.216        224.0.0.251      MDNS      152 Standard query 0x0011 PTR _%9E5E7C8F47989526C9BCD95D24084F6F0B27C5ED._sub._googlecast._tcp.local, "QM" question PTR _CFE7FEDA._sub.…
 1177 7.781538   fe80::a08b:f9ff:fe1… ff02::fb         MDNS      172 Standard query 0x0011 PTR _%9E5E7C8F47989526C9BCD95D24084F6F0B27C5ED._sub._googlecast._tcp.local, "QM" question PTR _CFE7FEDA._sub.…
 1369 7.985482   fe80::c443:16ff:fee… ff02::fb         MDNS      310 Standard query response 0x0000 PTR, cache flush Android-4.local PTR, cache flush Android-4.local A, cache flush 10.21.162.13 AAAA, …
 1370 7.985482   10.21.162.13         224.0.0.251      MDNS      290 Standard query response 0x0000 PTR, cache flush Android-4.local PTR, cache flush Android-4.local A, cache flush 10.21.162.13 AAAA, …
 1495 8.293254   10.21.163.3          239.255.255.250  SSDP      212 M-SEARCH * HTTP/1.1
 1502 8.315884   10.21.162.228        142.250.194.78   QUIC     1292 Initial, DCID=36b45d3a804f4af5, PKN: 8, PADDING, CRYPTO, PADDING, PING, CRYPTO, CRYPTO, CRYPTO, CRYPTO, PADDING, PING, CRYPTO, PING…
 1602 9.316871   10.21.163.3          239.255.255.250  SSDP      212 M-SEARCH * HTTP/1.1
 1603 9.726242   fe80::c22:beff:fe74… ff02::fb         MDNS      430 Standard query response 0x0000 TXT, cache flush PTR _mi-connect._udp.local PTR {"nm":"Redmi Note 10","as":"[8194]","ip":"43"}._mi-c…
 1604 9.726242   10.21.161.43         224.0.0.251      MDNS      410 Standard query response 0x0000 TXT, cache flush PTR _mi-connect._udp.local PTR {"nm":"Redmi Note 10","as":"[8194]","ip":"43"}._mi-c…
```

```
> Frame 277: 130 bytes on wire (1040 bits), 130 bytes captured (1040 bits) on interface \Device\NPF_{17A35
> Ethernet II, Src: JuniperNetwo_73:09:40 (c0:bf:a7:73:09:40), Dst: Intel_df:2e:d8 (74:04:f1:df:2e:d8)
> Internet Protocol Version 4, Src: 10.0.0.10, Dst: 10.21.162.228
> User Datagram Protocol, Src Port: 53, Dst Port: 51620
> Domain Name System (response)
```

```
0000  74 04 f1 df 2e d8 c0 bf  a7 73 09 40 08 00 45 00   t···.··· ·s·@··E·
0010  00 74 f0 10 00 00 7f 11  94 65 0a 00 00 0a 0a 15   ·t······ ·e······
0020  a2 e4 00 35 c9 a4 00 60  6f 83 40 e3 81 80 00 01   ···5···` o·@·····
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 c0 0c 00  05 00 01 00 00 00 6a 00   ········ ······j·
0060  11 0c 67 6f 6f 67 6c 65  68 6f 73 74 65 64 01 6c   ··google hosted·l
0070  c0 10 c0 37 00 01 00 01  00 00 00 a6 00 04 8e fa   ···7···· ········
0080  c2 81                                              ··
```

User Datagram Protocol: Protocol
Packets: 123429 · Displayed: 3768 (3.1%)
Profile: Default

F. FTP (File Transfer Protocol)

- **Port:** 21 (control), 20 (data)
- **Use:** File transfers between client and server
- **Filter:** `ftp`
- **Look for:**
  - Login commands (`USER`, `PASS`)

  - File upload/download commands (`STOR`, `RETR`)
  -

G. IP (Internet Protocol)

- **Use:** Logical addressing for routing packets
- **Filter:** `ip`
- **Look for:**
  - Source and destination IP addresses
  - IP version, header length, TTL, checksum

H. SMTP (Simple Mail Transfer Protocol)

- **Port:** 25 (sometimes 587 or 465)
- **Use:** Sending emails from client to server
- **Filter:** `smtp`
- **Look for:**
  - Commands like `HELO`, `MAIL FROM`, `RCPT TO`, `DATA`
  - Email content in plain text

---

4. Example Workflow

1. Visit `http://example.com` in your browser.
2. Use `nslookup example.com` to trigger DNS request.
3. Send a test email via command-line or client.
4. Use FTP client to upload/download a file.
5. Analyze each protocol using Wireshark filters.

---

5. Observations and Insights

- **DNS** typically precedes HTTP as domains are resolved before browsing.

- **TCP handshakes** establish a reliable session before actual data (HTTP, FTP) is sent.
- **SMTP traffic** is often readable in plain text unless encrypted with TLS.
- **ARP** shows how local MAC addresses are resolved.
- **UDP** lacks acknowledgment, suitable for speed-critical applications.