Experiment – 9

Aim: To capture and analyze DNS (Domain Name System) queries and understand how domain names are resolved to IP addresses.

Objective: Monitor the DNS queries generated when accessing websites and analyze how the DNS resolution process works.

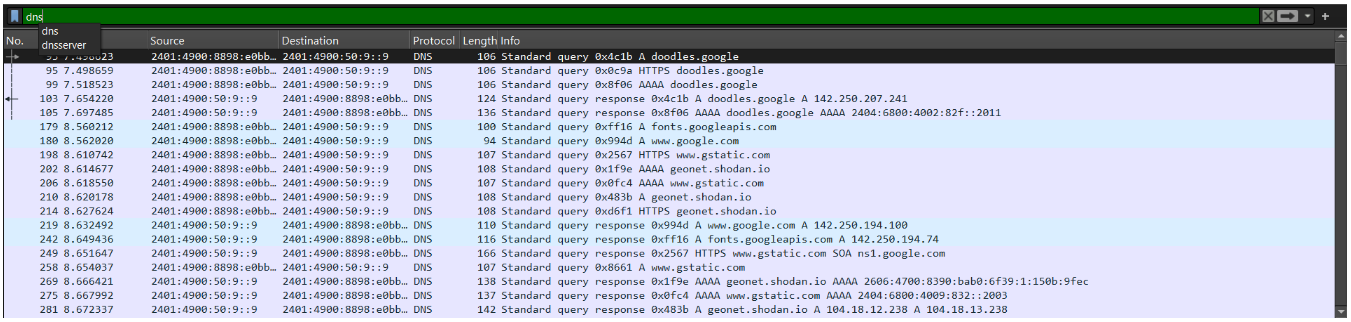
Theory:

When you enter a website address (e.g., www.example.com) in your browser, a DNS query is made to resolve the domain name to its corresponding IP address. DNS servers respond with the IP address, allowing the browser to connect to the server.

Used **Commands** in Wireshark:

1. Capture DNS Traffic:

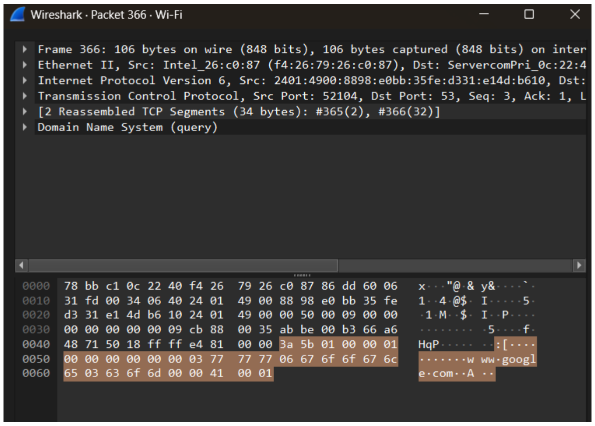
- Start capturing packets and use the display filter dns to capture only DNS packets.



```
dns
No.   Time         Source                   Destination              Protocol Length Info
 93 7.498023      2401:4900:8898:e0bb…     2401:4900:50:9::9        DNS      106 Standard query 0x4c1b A doodles.google
 95 7.498659      2401:4900:8898:e0bb…     2401:4900:50:9::9        DNS      106 Standard query 0x0c9a HTTPS doodles.google
 99 7.518523      2401:4900:8898:e0bb…     2401:4900:50:9::9        DNS      106 Standard query 0x8f06 AAAA doodles.google
103 7.654220      2401:4900:50:9::9        2401:4900:8898:e0bb…     DNS      124 Standard query response 0x4c1b A doodles.google A 142.250.207.241
105 7.697485      2401:4900:50:9::9        2401:4900:8898:e0bb…     DNS      136 Standard query response 0x8f06 AAAA doodles.google AAAA 2404:6800:4002:82f::2011
179 8.560212      2401:4900:8898:e0bb…     2401:4900:50:9::9        DNS      100 Standard query 0xff16 A fonts.googleapis.com
180 8.562020      2401:4900:8898:e0bb…     2401:4900:50:9::9        DNS       94 Standard query 0x994d A www.google.com
198 8.610742      2401:4900:8898:e0bb…     2401:4900:50:9::9        DNS      107 Standard query 0x2567 HTTPS www.gstatic.com
202 8.614677      2401:4900:8898:e0bb…     2401:4900:50:9::9        DNS      108 Standard query 0x1f9e AAAA geonet.shodan.io
206 8.618550      2401:4900:8898:e0bb…     2401:4900:50:9::9        DNS      107 Standard query 0x0fc4 AAAA www.gstatic.com
210 8.620178      2401:4900:8898:e0bb…     2401:4900:50:9::9        DNS      108 Standard query 0x483b A geonet.shodan.io
214 8.627624      2401:4900:8898:e0bb…     2401:4900:50:9::9        DNS      108 Standard query 0xd6f1 HTTPS geonet.shodan.io
219 8.632492      2401:4900:50:9::9        2401:4900:8898:e0bb…     DNS      110 Standard query response 0x994d A www.google.com A 142.250.194.100
242 8.649436      2401:4900:50:9::9        2401:4900:8898:e0bb…     DNS      116 Standard query response 0xff16 A fonts.googleapis.com A 142.250.194.74
249 8.651647      2401:4900:50:9::9        2401:4900:8898:e0bb…     DNS      166 Standard query response 0x2567 HTTPS www.gstatic.com SOA ns1.google.com
258 8.654037      2401:4900:8898:e0bb…     2401:4900:50:9::9        DNS      107 Standard query 0x8661 A www.gstatic.com
269 8.666421      2401:4900:50:9::9        2401:4900:8898:e0bb…     DNS      138 Standard query response 0x1f9e AAAA geonet.shodan.io AAAA 2606:4700:8390:bab0:6f39:1:150b:9fec
275 8.667992      2401:4900:50:9::9        2401:4900:8898:e0bb…     DNS      137 Standard query response 0x0fc4 AAAA www.gstatic.com AAAA 2404:6800:4009:832::2003
281 8.672337      2401:4900:50:9::9        2401:4900:8898:e0bb…     DNS      142 Standard query response 0x483b A geonet.shodan.io A 104.18.12.238 A 104.18.13.238
```

2. Filter DNS Queries:

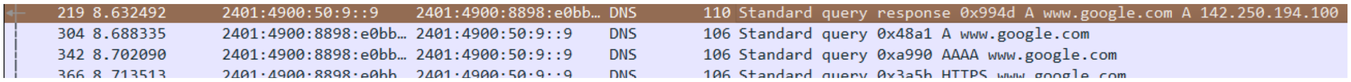
- Look for DNS query packets that contain requests like A www.example.com, which indicates a request for the IP address of the domain www.example.com.



Wireshark · Packet 366 · Wi-Fi

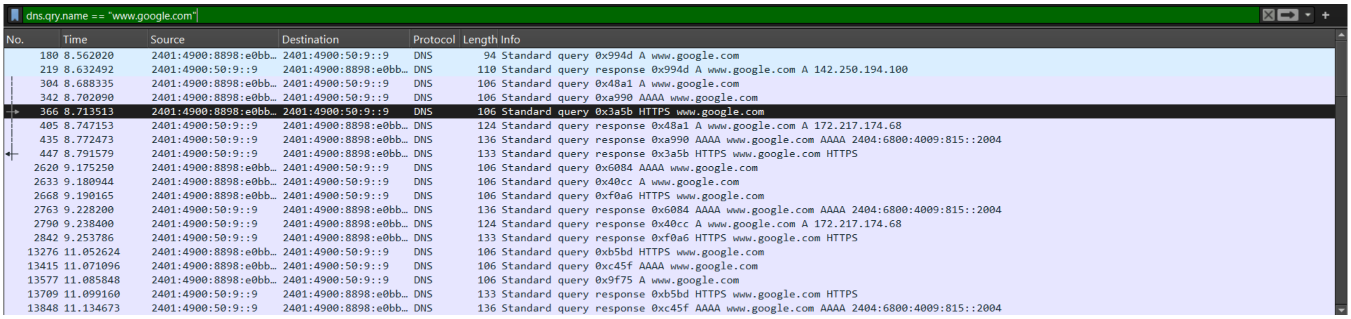
```
Frame 366: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on inter
Ethernet II, Src: Intel_26:c0:87 (f4:26:79:26:c0:87), Dst: ServercomPri_0c:22:4
Internet Protocol Version 6, Src: 2401:4900:8898:e0bb:35fe:d331:e14d:b610, Dst:
Transmission Control Protocol, Src Port: 52104, Dst Port: 53, Seq: 3, Ack: 1, L
[2 Reassembled TCP Segments (34 bytes): #365(2), #366(32)]
Domain Name System (query)

0000  78 bb c1 0c 22 40 f4 26  79 26 c0 87 86 dd 60 06   x···"@·& y&····`·
0010  31 fd 00 34 06 40 24 01  49 00 88 98 e0 bb 35 fe   1··4·@$· I·····5·
0020  d3 31 e1 4d b6 10 24 01  49 00 00 50 00 09 00 00   ·1·M··$· I··P····
0030  00 00 00 00 00 09 cb 88  00 35 ab be 00 b3 66 a6   ········ ·5····f·
0040  48 71 50 18 ff ff e4 81  00 00 3a 5b 01 00 00 01   HqP····· ··:[····
0050  00 00 00 00 00 00 03 77  77 77 06 67 6f 6f 67 6c   ·······w ww·googl
0060  65 03 63 6f 6d 00 00 41  00 01                     e·com··A ··
```

3. Analyze DNS Response:
- Look for DNS response packets that will provide the IP address for the requested domain name, e.g., www.example.com -> 93.184.216.34.



```
219 8.632492   2401:4900:50:9::9      2401:4900:8898:e0bb… DNS   110 Standard query response 0x994d A www.google.com A 142.250.194.100
304 8.688335   2401:4900:8898:e0bb…   2401:4900:50:9::9    DNS   106 Standard query 0x48a1 A www.google.com
342 8.702090   2401:4900:8898:e0bb…   2401:4900:50:9::9    DNS   106 Standard query 0xa990 AAAA www.google.com
366 8.713513   2401:4900:8898:e0bb…   2401:4900:50:9::9    DNS   106 Standard query 0x3a5b HTTPS www.google.com
```

4. Filter by DNS Query:
- Use a filter like dns.qry.name == "example.com" to see the DNS query for a specific domain.



```
dns.qry.name == "www.google.com"

No.   Time      Source                Destination           Protocol Length Info
  180 8.562020  2401:4900:8898:e0bb…  2401:4900:50:9::9     DNS       94 Standard query 0x994d A www.google.com
  219 8.632492  2401:4900:50:9::9     2401:4900:8898:e0bb…  DNS      110 Standard query response 0x994d A www.google.com A 142.250.194.100
  304 8.688335  2401:4900:8898:e0bb…  2401:4900:50:9::9     DNS      106 Standard query 0x48a1 A www.google.com
  342 8.702090  2401:4900:8898:e0bb…  2401:4900:50:9::9     DNS      106 Standard query 0xa990 AAAA www.google.com
  366 8.713513  2401:4900:8898:e0bb…  2401:4900:50:9::9     DNS      106 Standard query 0x3a5b HTTPS www.google.com
  405 8.747153  2401:4900:50:9::9     2401:4900:8898:e0bb…  DNS      124 Standard query response 0x48a1 A www.google.com A 172.217.174.68
  435 8.772473  2401:4900:50:9::9     2401:4900:8898:e0bb…  DNS      136 Standard query response 0xa990 AAAA www.google.com AAAA 2404:6800:4009:815::2004
  447 8.791579  2401:4900:50:9::9     2401:4900:8898:e0bb…  DNS      133 Standard query response 0x3a5b HTTPS www.google.com HTTPS
 2620 9.175250  2401:4900:8898:e0bb…  2401:4900:50:9::9     DNS      106 Standard query 0x6084 AAAA www.google.com
 2633 9.180944  2401:4900:8898:e0bb…  2401:4900:50:9::9     DNS      106 Standard query 0x40cc A www.google.com
 2668 9.190165  2401:4900:8898:e0bb…  2401:4900:50:9::9     DNS      106 Standard query 0xf0a6 HTTPS www.google.com
 2763 9.228200  2401:4900:50:9::9     2401:4900:8898:e0bb…  DNS      136 Standard query response 0x6084 AAAA www.google.com AAAA 2404:6800:4009:815::2004
 2790 9.238400  2401:4900:50:9::9     2401:4900:8898:e0bb…  DNS      124 Standard query response 0x40cc A www.google.com A 172.217.174.68
 2842 9.253786  2401:4900:50:9::9     2401:4900:8898:e0bb…  DNS      133 Standard query response 0xf0a6 HTTPS www.google.com HTTPS
13276 11.052624 2401:4900:8898:e0bb…  2401:4900:50:9::9     DNS      106 Standard query 0xb5bd HTTPS www.google.com
13415 11.071096 2401:4900:8898:e0bb…  2401:4900:50:9::9     DNS      106 Standard query 0xc45f AAAA www.google.com
13577 11.085848 2401:4900:8898:e0bb…  2401:4900:50:9::9     DNS      106 Standard query 0x9f75 A www.google.com
13709 11.099160 2401:4900:50:9::9     2401:4900:8898:e0bb…  DNS      133 Standard query response 0xb5bd HTTPS www.google.com HTTPS
13848 11.134673 2401:4900:50:9::9     2401:4900:8898:e0bb…  DNS      136 Standard query response 0xc45f AAAA www.google.com AAAA 2404:6800:4009:815::2004
```

Conclusion: In this experiment, we successfully captured and analyzed **DNS (Domain Name System)** traffic using Wireshark to understand how domain names are resolved to IP addresses. By monitoring DNS queries and responses, we gained insights into the DNS resolution process, which is a fundamental part of how the internet operates