

Week 4-Computer Networks LAB

No.	Time	Source	Destination	Protocol	Length	Info
10	0.005820	172.17.64.216	172.16.100.210	DNS	78	Standard query 0x8384 A capi.grammarly.com
31	0.031335	172.17.64.216	172.16.100.211	DNS	78	Standard query 0x8384 A capi.grammarly.com
33	0.076753	172.17.64.216	172.16.100.210	DNS	76	Standard query 0x1801 A api.iterable.com
34	0.082564	172.16.100.211	172.17.64.216	DNS	206	Standard query response 0x8384 A capi.grammarly.com A 54.85.149.157 A 3.225.33.98 A 50.16.1.199 A 3.92.154.43 A 3.224.228.228 A...
39	0.082564	172.16.100.210	172.17.64.216	DNS	206	Standard query response 0x8384 A capi.grammarly.com A 3.93.104.104 A 35.172.90.242 A 3.229.153.114 A 34.229.25.10 A 3.230.107.1...
40	0.082564	172.16.100.210	172.17.64.216	DNS	204	Standard query response 0x1801 A api.iterable.com A 3.90.132.173 A 52.6.29.79 A 34.196.61.219 A 3.214.176.41 A 52.207.76.97 A 5...
105	0.435007	172.17.64.216	172.16.100.210	DNS	78	Standard query 0x6779 A gnar.grammarly.com
107	0.472013	172.17.64.216	172.16.100.211	DNS	78	Standard query 0x6779 A gnar.grammarly.com
110	0.500081	172.16.100.210	172.17.64.216	DNS	206	Standard query response 0x6779 A gnar.grammarly.com A 18.204.100.20 A 50.19.150.221 A 18.213.145.220 A 34.235.231.103 A 34.193...
113	0.524927	172.16.100.211	172.17.64.216	DNS	206	Standard query response 0x6779 A gnar.grammarly.com A 34.235.231.103 A 52.204.99.156 A 34.193.30.8 A 3.224.47.162 A 52.206.201...
982	6.179850	172.17.64.216	172.16.100.210	DNS	78	Standard query 0x1fa3 TXT wmail-endpoint.com
983	6.210001	172.17.64.216	172.16.100.211	DNS	78	Standard query 0x1fa3 TXT wmail-endpoint.com
1082	7.214633	172.17.64.216	8.8.8.8	DNS	78	Standard query 0x1fa3 TXT wmail-endpoint.com
1105	7.343600	8.8.8.8	172.17.64.216	DNS	102	Standard query response 0x1fa3 TXT wmail-endpoint.com TXT
1106	7.345105	172.17.64.216	172.16.100.210	DNS	74	Standard query 0x4f3d TXT wmail-blog.com
1119	7.371822	172.16.100.210	172.17.64.216	DNS	98	Standard query response 0x4f3d TXT wmail-blog.com TXT
1122	7.374248	172.17.64.216	172.16.100.210	DNS	74	Standard query 0x7b7a TXT wmail-chat.com
1148	7.389021	172.16.100.210	172.17.64.216	DNS	154	Standard query response 0x7b7a TXT wmail-chat.com SOA ns1.sinkhole.caad.fkie.fraunhofer.de
1157	7.391035	172.17.64.216	172.16.100.210	DNS	73	Standard query 0x2447 TXT wmail-cdn.com
1169	7.419626	172.16.100.210	172.17.64.216	DNS	153	Standard query response 0x2447 TXT wmail-cdn.com SOA ns1.sinkhole.caad.fkie.fraunhofer.de
1171	7.421699	172.17.64.216	172.16.100.210	DNS	80	Standard query 0x25b1 TXT wmail-schnellvpn.com
1173	7.453158	172.17.64.216	8.8.8.8	DNS	80	Standard query 0x25b1 TXT wmail-schnellvpn.com
1179	7.470390	172.16.100.210	172.17.64.216	DNS	160	Standard query response 0x25b1 TXT wmail-schnellvpn.com SOA ns1.sinkhole.caad.fkie.fraunhofer.de
1189	7.473113	172.17.64.216	172.16.100.210	DNS	78	Standard query 0xa50e TXT fairu-endpoint.com
1192	7.490628	8.8.8.8	172.17.64.216	DNS	160	Standard query response 0x25b1 TXT wmail-schnellvpn.com SOA ns1.sinkhole.caad.fkie.fraunhofer.de
1193	7.500191	172.17.64.216	8.8.8.8	DNS	78	Standard query 0xa50e TXT fairu-endpoint.com
1200	7.532948	172.16.100.210	172.17.64.216	DNS	142	Standard query response 0xa50e TXT fairu-endpoint.com SOA ns1.namecheapapi.com

Frame 105: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface \Device\NPF_{F56A2E66-6924-4...}

Ethernet II, Src: Intel_b2:b0:88 (60:f6:77:b2:b0:88), Dst: HewlettPacka_d0:48:00 (08:97:34:d0:48:00)

Internet Protocol Version 4, Src: 172.17.64.216, Dst: 172.16.100.210

User Datagram Protocol, Src Port: 58683, Dst Port: 53

Domain Name System (query)

Transaction ID: 0x6779

Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

Queries

[Response In: 110]

```

0000 08 97 34 d0 48 00 60 f6 77 b2 b0 88 08 00 45 00  : 4 H...w....E...
0010 00 40 f4 52 00 00 80 11 48 8e ac 11 40 d8 ac 10  : @ R...H...@...
0020 64 d2 e5 3b 00 35 00 2c dc e9 67 79 01 00 00 01  : d.;5,...gy...
0030 00 00 00 00 00 04 67 6e 61 72 09 67 72 61 6d  : .....g nar.gram
0040 6d 61 72 6c 79 03 63 6f 6d 00 00 01 00 01      : marly.co m.....

```

Domain Name System: Protocol

Packets: 2077 - Displayed: 164 (7.9%) - Dropped: 0 (0.0%)

Profile: Default

Task#1

1. The Record Type of DNS is 'A'.
2. The Domain Name used by the server was **gnar.grammarly.com**: type A, class IN.
3. DNS query is using **UDP** as the transport protocol.
4. The IP address of the response server is **172.16.100.210**.
5. Yes, the IP was included in the response packet of the queried server.

dns.flags.rcode==3					
No.	Time	Source	Destination	Protocol	Length Info
1751	9.440012	172.16.100.210	172.17.64.216	DNS	145 Standard query response 0x57d5 No such name TXT bideo-schnellvpn.xyz SOA ns0.centralnic.net
1753	9.484149	8.8.8.8	172.17.64.216	DNS	145 Standard query response 0x57d5 No such name TXT bideo-schnellvpn.xyz SOA ns0.centralnic.net

6. There were 2 packets for **dns.flags.rcode==3**.

- Transaction ID: 0x37d3
Flags: 0x8183 Standard query response, No such name
- 1... .. = Response: Message is a response
 - .000 0... .. = Opcode: Standard query (0)
 - 0... .. = Authoritative: Server is not an authority for domain
 - 0... .. = Truncated: Message is not truncated
 - 1... .. = Recursion desired: Do query recursively
 - 1... .. = Recursion available: Server can do recursive queries
 - 0... .. = Z: reserved (0)
 - 0... .. = Answer authenticated: Answer/authority portion was not authenticated by the serv
 - 0... .. = Non-authenticated data: Unacceptable
 - 0011 = Reply code: No such name (3)
7. Internet Protocol Version 4, Src: 172.16.100.210, Dst: 172.17.64.216
- 0100 = Version: 4
 - 0101 = Header Length: 20 bytes (5)
 - Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 - Total Length: 131
 - Identification: 0x79f3 (31219)
 - 000. = Flags: 0x0
 - ...0 0000 0000 0000 = Fragment Offset: 0
 - Time to Live: 127
 - Protocol: UDP (17)
 - Header Checksum: 0xc3aa [validation disabled]
[Header checksum status: Unverified]
 - Source Address: 172.16.100.210
 - Destination Address: 172.17.64.216
- 8.