

HACETTEPE UNIVERSITY
COMPUTER ENGINEERING DEPARTMENT
COMPUTER NETWORKS LABORATORY



EXPERIMENT : DNS

Deniz Ece AKTAŞ 21626901

Ece OMURTAY 21627543

GROUP NUMBER : 12

IP ADDRESS OF OUR COMPUTER : 192.168.1.53

nslookup

1. We performed nslookup for www.frc.org.uk which is the UK based Financial Reporting Council's website. Its IP Address is; 159.253.211.139

```
C:\Users\pc>nslookup www.frc.org.uk
Server: UnKnown
Address: 192.168.1.1

Non-authoritative answer:
Name: www.frc.org.uk
Address: 159.253.211.139
```

2. We performed nslookup -type=NS command for Stanford University in United States.

```
C:\Users\pc>nslookup -type=NS stanford.edu ns5.dnsmadeeasy.com
Server: UnKnown
Address: 208.94.148.13

stanford.edu    nameserver = atalante.stanford.edu
stanford.edu    nameserver = avallone.stanford.edu
stanford.edu    nameserver = ns6.dnsmadeeasy.com
stanford.edu    nameserver = ns7.dnsmadeeasy.com
stanford.edu    nameserver = argus.stanford.edu
stanford.edu    nameserver = ns5.dnsmadeeasy.com
Argus.stanford.edu    internet address = 171.64.7.115
Atalante.stanford.edu    internet address = 171.64.7.61
avallone.stanford.edu    internet address = 171.66.32.8
Argus.stanford.edu    AAAA IPv6 address = 2607:f6d0:0:9113::ab40:773
Atalante.stanford.edu    AAAA IPv6 address = 2607:f6d0:0:d32::ab40:73d
avallone.stanford.edu    AAAA IPv6 address = 2607:f6d0:8000:0:172:26:32:8
```

To be sure, we looked up another DNS Server which is ns7.dnsmadeeasy.com Results are same.

```
C:\Users\pc>nslookup -type=NS stanford.edu ns7.dnsmadeeasy.com
Server: UnKnown
Address: 208.80.126.13

stanford.edu    nameserver = ns5.dnsmadeeasy.com
stanford.edu    nameserver = ns6.dnsmadeeasy.com
stanford.edu    nameserver = avallone.stanford.edu
stanford.edu    nameserver = argus.stanford.edu
stanford.edu    nameserver = atalante.stanford.edu
stanford.edu    nameserver = ns7.dnsmadeeasy.com
Argus.stanford.edu    internet address = 171.64.7.115
Atalante.stanford.edu    internet address = 171.64.7.61
avallone.stanford.edu    internet address = 171.66.32.8
Argus.stanford.edu    AAAA IPv6 address = 2607:f6d0:0:9113::ab40:773
Atalante.stanford.edu    AAAA IPv6 address = 2607:f6d0:0:d32::ab40:73d
avallone.stanford.edu    AAAA IPv6 address = 2607:f6d0:8000:0:172:26:32:8
```

3. We used Google's DNS server for performing nslookup which is queried for mail server: Yahoo! Mail. One of its IP address is 87.248.118.22

```
C:\Users\pc>nslookup mail.yahoo.com dns.google
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:     edge.gycpi.b.yahoodns.net
Addresses: 2a00:1288:80:800::7001
          2a00:1288:80:800::7000
          87.248.118.22
          87.248.118.23
Aliases:  mail.yahoo.com
```

Tracing DNS with Wireshark

We answered the following questions according to analytics.ietf.org

No.	Time	Source	Destination	Protocol	Length	Info
242	3.954556	192.168.1.53	192.168.1.1	DNS	72	Standard query 0x72da A www.ietf.org
244	3.960057	192.168.1.53	192.168.1.1	DNS	78	Standard query 0xdd51 A www.googleapis.com
245	3.970806	192.168.1.1	192.168.1.53	DNS	254	Standard query response 0xdd51 A www.googleapis.com A 172.217.169.202 A 172.217.17.170 A 216.58.212.10 A 172.217.17.202 A 216...
248	3.981101	192.168.1.1	192.168.1.53	DNS	149	Standard query response 0x72da A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.44.99 A 104.16.45.99
299	4.172219	192.168.1.53	192.168.1.1	DNS	83	Standard query 0x36aa A safebrowsing.google.com
306	4.178182	192.168.1.1	192.168.1.53	DNS	118	Standard query response 0x36aa A safebrowsing.google.com CNAME sb.l.google.com A 172.217.169.206
634	4.760236	192.168.1.53	192.168.1.1	DNS	78	Standard query 0xb803 A analytics.ietf.org
676	5.006836	192.168.1.1	192.168.1.53	DNS	108	Standard query response 0xb803 A analytics.ietf.org CNAME ietf.org A 4.31.198.44
260	3.998008	192.168.1.53	104.16.44.99	HTTP	527	GET / HTTP/1.1
265	4.025080	104.16.44.99	192.168.1.53	HTTP	406	HTTP/1.1 301 Moved Permanently
178	3.178069	192.168.1.53	224.0.0.252	LLMNR	64	Standard query 0x664b A wpad
219	3.602437	192.168.1.53	224.0.0.252	LLMNR	64	Standard query 0x664b A wpad
305	4.175877	192.168.1.53	224.0.0.252	LLMNR	64	Standard query 0xa8ca A wpad
419	4.593652	192.168.1.53	224.0.0.252	LLMNR	64	Standard query 0xa8ca A wpad
157	2.789783	192.168.1.36	224.0.0.251	MDNS	411	Standard query response 0x0000 PTR HiTV-AESP0-131b6ba8eb72eff1e087001e47081b3f._googlecast._tcp.local TXT, cache flush SRV, ca...
175	3.177158	192.168.1.53	224.0.0.251	MDNS	70	Standard query 0x0000 A wpad.local, "QM" question
301	4.175349	192.168.1.53	224.0.0.251	MDNS	70	Standard query 0x0000 A wpad.local, "QM" question

> Frame 242: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{2F86FA23-1860-4715-9568-3A40F810F6C4}, id 0
> Ethernet II, Src: IntelCor_83:5e:f5 (f8:94:c2:83:5e:f5), Dst: Tp-LinkT_62:5c:80 (1c:44:19:62:5c:80)
> Internet Protocol Version 4, Src: 192.168.1.53, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 56277, Dst Port: 53
> Domain Name System (query)

4. Query and response messages are sent over UDP.
5. Source port for DNS response: 56277 and Destination port for DNS query: 53. They are shown in the picture above.

- > Frame 242: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{2F86FA23-1860-4715-9568-3A40F810F6C4}, id 0
- > Ethernet II, Src: IntelCor_83:5e:f5 (f8:94:c2:83:5e:f5), Dst: Tp-LinkT_62:5c:80 (1c:44:19:62:5c:80)
- ✓ Internet Protocol Version 4, Src: 192.168.1.53, Dst: 192.168.1.1
 - 0100 = Version: 4
 - 0101 = Header Length: 20 bytes (5)
 - > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 - Total Length: 58
 - Identification: 0x1b7a (7034)
 - > Flags: 0x0000
 - Fragment offset: 0
 - Time to live: 128
 - Protocol: UDP (17)
 - Header checksum: 0x9bb2 [validation disabled]
 - [Header checksum status: Unverified]
 - Source: 192.168.1.53
 - Destination: 192.168.1.1
 - > User Datagram Protocol, Src Port: 56277, Dst Port: 53
 - > Domain Name System (query)

6. As it shows in both of images, one of our local DNS Servers is 192.168.1.1. ipconfig results and Wireshark screenshot show the same address.

```

DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Yerel Ağ Bağlantısı* 1:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix  . :
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
Physical Address. . . . . : F8-94-C2-83-5E-F6
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Yerel Ağ Bağlantısı* 3:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix  . :
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
Physical Address. . . . . : FA-94-C2-83-5E-F5
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix  . :
Description . . . . . : Intel(R) Dual Band Wireless-AC 7265
Physical Address. . . . . : F8-94-C2-83-5E-F5
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::f83b:dbee:82ff:c081%6(Preferred)
IPv4 Address. . . . . : 192.168.1.53(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Thursday, November 5, 2020 1:18:33 PM
Lease Expires . . . . . : Thursday, November 5, 2020 2:18:33 PM
Default Gateway . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DHCPv6 IAID . . . . . : 66622658
DHCPv6 Client DUID. . . . . : 00-01-00-01-21-AD-83-81-AC-E2-D3-66-6A-CE
DNS Servers . . . . . : 192.168.1.1
NetBIOS over Tcpip. . . . . : Enabled

```

7. Type A query. It does not conclude any answer.

242	3.954556	192.168.1.53	192.168.1.1	DNS	72 Standard query 0x72da A www.ietf.org
244	3.960057	192.168.1.53	192.168.1.1	DNS	78 Standard query 0xdd51 A www.googleapis.com
245	3.970806	192.168.1.1	192.168.1.53	DNS	254 Standard query response 0xdd51 A www.googleapis.com A 172.217.169.202 A 172.217.17.
248	3.981101	192.168.1.1	192.168.1.53	DNS	149 Standard query response 0x72da A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net
299	4.172219	192.168.1.53	192.168.1.1	DNS	83 Standard query 0x36aa A safebrowsing.google.com
306	4.178182	192.168.1.1	192.168.1.53	DNS	118 Standard query response 0x36aa A safebrowsing.google.com CNAME sb.l.google.com A 17
634	4.760236	192.168.1.53	192.168.1.1	DNS	78 Standard query 0xb803 A analytics.ietf.org
676	5.006836	192.168.1.1	192.168.1.53	DNS	108 Standard query response 0xb803 A analytics.ietf.org CNAME ietf.org A 4.31.198.44
260	3.998008	192.168.1.53	104.16.44.99	HTTP	527 GET / HTTP/1.1
265	4.025000	104.16.44.99	192.168.1.53	HTTP	406 HTTP/1.1 301 Moved Permanently
178	3.178069	192.168.1.53	224.0.0.252	LLMNR	64 Standard query 0x664b A wpad
219	3.602437	192.168.1.53	224.0.0.252	LLMNR	64 Standard query 0x664b A wpad
305	4.175877	192.168.1.53	224.0.0.252	LLMNR	64 Standard query 0xa8ca A wpad
419	4.593652	192.168.1.53	224.0.0.252	LLMNR	64 Standard query 0xa8ca A wpad
157	2.789783	192.168.1.36	224.0.0.251	MDNS	411 Standard query response 0x0000 PTR MiTV-AESP0-131b6ba8eb72eff1e087001e47081b3f._goo
175	3.177158	192.168.1.53	224.0.0.251	MDNS	70 Standard query 0x0000 A wpad.local, "QM" question
301	4.175349	192.168.1.53	224.0.0.251	MDNS	70 Standard query 0x0000 A wpad.local, "QM" question
308	4.190731	192.168.1.53	224.0.0.251	MDNS	70 Standard query 0x0000 A wpad.local, "QM" question


```

> Frame 242: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{2F86FA23-1860-4715-956B-3A40FB10F6C4}, id 0
> Ethernet II, Src: IntelCor_83:5e:f5 (f8:94:c2:83:5e:f5), Dst: Tp-LinkT_62:5c:80 (1c:44:19:62:5c:80)
> Internet Protocol Version 4, Src: 192.168.1.53, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 56277, Dst Port: 53
  > Domain Name System (query)
    Transaction ID: 0x72da
    > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
    > Queries
      > www.ietf.org: type A, class IN
      [Response In: 248]

```


8. There are 3 answers. Messages contain the IP address, class and type information.

No.	Time	Source	Destination	Protocol	Length	Info
242	3.954556	192.168.1.53	192.168.1.1	DNS	72	Standard query 0x72da A www.ietf.org
244	3.960057	192.168.1.53	192.168.1.1	DNS	78	Standard query 0xdd51 A www.googleapis.com
245	3.970806	192.168.1.1	192.168.1.53	DNS	254	Standard query response 0xdd51 A www.googleapis.com A 172.217.169.202 A 172.217.17.170 A 216.58.212.10 A 172.217.17.202 A
248	3.981101	192.168.1.1	192.168.1.53	DNS	149	Standard query response 0x72da A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.44.99 A 104.16.45.99
299	4.172219	192.168.1.53	192.168.1.1	DNS	83	Standard query 0x36aa A safebrowsing.google.com
306	4.178182	192.168.1.1	192.168.1.53	DNS	118	Standard query response 0x36aa A safebrowsing.google.com CNAME sb.l.google.com A 172.217.169.206
634	4.760236	192.168.1.53	192.168.1.1	DNS	78	Standard query 0xb803 A analytics.ietf.org
676	5.006836	192.168.1.1	192.168.1.53	DNS	108	Standard query response 0xb803 A analytics.ietf.org CNAME ietf.org A 4.31.198.44
260	3.998008	192.168.1.53	104.16.44.99	HTTP	527	GET / HTTP/1.1
265	4.025080	104.16.44.99	192.168.1.53	HTTP	406	HTTP/1.1 301 Moved Permanently
178	3.178069	192.168.1.53	224.0.0.252	LLMNR	64	Standard query 0x664b A upad
219	3.602437	192.168.1.53	224.0.0.252	LLMNR	64	Standard query 0x664b A upad
305	4.175877	192.168.1.53	224.0.0.252	LLMNR	64	Standard query 0xa8ca A upad
419	4.593652	192.168.1.53	224.0.0.252	LLMNR	64	Standard query 0xa8ca A upad
157	2.789783	192.168.1.36	224.0.0.251	MDNS	411	Standard query response 0x0000 PTR MITV-AESP0-131b6a8eb72eff1e087001e47081b3f._googlecast._tcp.local TXT, cache flush SRV
175	3.177158	192.168.1.53	224.0.0.251	MDNS	70	Standard query 0x0000 A upad.local, "QM" question
301	4.175349	192.168.1.53	224.0.0.251	MDNS	70	Standard query 0x0000 A upad.local, "QM" question

Frame 248: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface \Device\NPF_{2F86FA23-1860-4715-9568-3A40F810F6C4}, id 0
Ethernet II, Src: Tp-LinkT_62:5c:80 (1c:44:19:62:5c:80), Dst: IntelCor_83:5e:f5 (f8:94:c2:83:5e:f5)
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.53
User Datagram Protocol, Src Port: 53, Dst Port: 56277
Domain Name System (response)
Transaction ID: 0x72da
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 3
Authority RRs: 0
Additional RRs: 0
Queries
www.ietf.org: type A, class IN
Answers
www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.44.99
www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.45.99
[Request In: 242]
[Time: 0.026545000 seconds]

9. IP addresses are matched with each other. Destination address is 104.16.44.99

249	3.981713	192.168.1.53	104.16.44.99	TCP	66	60044 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
250	3.982116	192.168.1.53	104.16.44.99	TCP	66	60045 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
251	3.990348	192.168.1.53	192.168.1.36	TCP	164	60009 → 80009 [PSH, ACK] Seq=1 Ack=1 Win=508 Len=110 [TCP segment of a reassembled PDU]
252	3.992982	172.217.169.202	192.168.1.53	TCP	66	443 → 60043 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1430 SACK_PERM=1 WS=256
253	3.993062	192.168.1.53	172.217.169.202	TCP	54	60043 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0

Frame 248: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface \Device\NPF_{2F86FA23-1860-4715-9568-3A40F810F6C4}, id 0
Ethernet II, Src: Tp-LinkT_62:5c:80 (1c:44:19:62:5c:80), Dst: IntelCor_83:5e:f5 (f8:94:c2:83:5e:f5)
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.53
User Datagram Protocol, Src Port: 53, Dst Port: 56277
Domain Name System (response)
Transaction ID: 0x72da
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 3
Authority RRs: 0
Additional RRs: 0
Queries
www.ietf.org: type A, class IN
Answers
www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.44.99
www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.45.99
[Request In: 242]
[Time: 0.026545000 seconds]

10. Yes, it calls for googleapis DNS server. So, it issues new DNS queries.

242	3.954556	192.168.1.53	192.168.1.1	DNS	72	Standard query 0x72da A www.ietf.org
244	3.960057	192.168.1.53	192.168.1.1	DNS	78	Standard query 0xdd51 A www.googleapis.com
245	3.970806	192.168.1.1	192.168.1.53	DNS	254	Standard query response 0xdd51 A www.googleapis.com A 172.217.169.202 A 172.217.17.170 A 216.58.212.10 A 172.217.17.202 A 216...
248	3.981101	192.168.1.1	192.168.1.53	DNS	149	Standard query response 0x72da A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.44.99 A 104.16.45.99

11.

```
C:\Users\pc>nslookup www.mit.edu
Server: UnKnown
Address: 192.168.1.1

Non-authoritative answer:
Name: e9566.dscb.akamaiedge.net
Addresses: 2a02:26f0:fa00:1b1::255e
           2a02:26f0:fa00:1a9::255e
           23.7.207.228
Aliases: www.mit.edu
          www.mit.edu.edgekey.net
```

We run the nslookup command

Destination port for DNS query message: 53.

No.	Time	Source	Destination	Protocol	Length	Info
398	9.756903	0.0.0.0	255.255.255.255	DHCP	340	DHCP Discover - Transaction ID 0xc67904c3
399	9.858630	0.0.0.0	255.255.255.255	DHCP	352	DHCP Request - Transaction ID 0xc67904c3
789	20.347363	192.168.1.53	192.168.1.1	DNS	84	Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
792	20.364740	192.168.1.1	192.168.1.53	DNS	139	Standard query response 0x0001 No such name PTR 1.1.168.192.in-addr.arpa SOA 168.192.IN-ADDR.ARPA
793	20.366757	192.168.1.53	192.168.1.1	DNS	71	Standard query 0x0002 A www.mit.edu
794	20.535355	192.168.1.1	192.168.1.53	DNS	160	Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 23.7.207.228
795	20.538057	192.168.1.53	192.168.1.1	DNS	71	Standard query 0x0003 AAAA www.mit.edu
797	20.673349	192.168.1.1	192.168.1.53	DNS	200	Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net AAAA 2a02:26f0:f...
928	24.186551	192.168.1.53	192.168.1.1	DNS	70	Standard query 0x49f7 A piazza.com
930	24.203028	192.168.1.1	192.168.1.53	DNS	198	Standard query response 0x49f7 A piazza.com A 52.55.158.156 A 3.228.26.56 A 34.224.199.66 A 52.72.175.212 A 34.230.125.68 A 34...
1035	25.518104	192.168.1.53	192.168.1.1	DNS	94	Standard query 0x9908 A oauthaccountmanager.googleapis.com
1036	25.539571	192.168.1.1	192.168.1.53	DNS	110	Standard query response 0x9908 A oauthaccountmanager.googleapis.com A 172.217.169.138
983	24.715532	192.168.1.1	192.168.1.53	ICMP	590	Destination unreachable (Fragmentation needed)
25	0.363438	192.168.1.53	224.0.0.22	IGMPv3	54	Membership Report / Join group 239.255.255.250 for any sources
30	0.452463	192.168.1.53	224.0.0.22	IGMPv3	54	Membership Report / Join group 239.255.255.250 for any sources
80	1.358680	192.168.1.53	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.251 for any sources
87	1.467666	192.168.1.53	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.251 for any sources

> Frame 793: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF_{2F86FA23-1860-4715-956B-3A40FB10F6C4}, id 0
> Ethernet II, Src: IntelCor_83:5e:f5 (f8:94:c2:83:5e:f5), Dst: Tp-LinkT_62:5c:80 (1c:44:19:62:5c:80)
> Internet Protocol Version 4, Src: 192.168.1.53, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 65212, Dst Port: 53
Domain Name System (query)

Source port for DNS response message: 53.

793	20.366757	192.168.1.53	192.168.1.1	DNS	71	Standard query 0x0002 A www.mit.edu
794	20.535355	192.168.1.1	192.168.1.53	DNS	160	Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 23.7.207.228
795	20.538057	192.168.1.53	192.168.1.1	DNS	71	Standard query 0x0003 AAAA www.mit.edu
797	20.673349	192.168.1.1	192.168.1.53	DNS	200	Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net AAAA 2a02:26f0:f...
928	24.186551	192.168.1.53	192.168.1.1	DNS	70	Standard query 0x49f7 A piazza.com
930	24.203028	192.168.1.1	192.168.1.53	DNS	198	Standard query response 0x49f7 A piazza.com A 52.55.158.156 A 3.228.26.56 A 34.224.199.66 A 52.72.175.212 A 34.230.125.68 A 34...
1035	25.518104	192.168.1.53	192.168.1.1	DNS	94	Standard query 0x9908 A oauthaccountmanager.googleapis.com
1036	25.539571	192.168.1.1	192.168.1.53	DNS	110	Standard query response 0x9908 A oauthaccountmanager.googleapis.com A 172.217.169.138
983	24.715532	192.168.1.1	192.168.1.53	ICMP	590	Destination unreachable (Fragmentation needed)
25	0.363438	192.168.1.53	224.0.0.22	IGMPv3	54	Membership Report / Join group 239.255.255.250 for any sources
30	0.452463	192.168.1.53	224.0.0.22	IGMPv3	54	Membership Report / Join group 239.255.255.250 for any sources
80	1.358680	192.168.1.53	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.251 for any sources
87	1.467666	192.168.1.53	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.251 for any sources

> Frame 794: 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits) on interface \Device\NPF_{2F86FA23-1860-4715-956B-3A40FB10F6C4}, id 0
> Ethernet II, Src: Tp-LinkT_62:5c:80 (1c:44:19:62:5c:80), Dst: IntelCor_83:5e:f5 (f8:94:c2:83:5e:f5)
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.53
> User Datagram Protocol, Src Port: 53, Dst Port: 65212
Domain Name System (response)

12. 192.168.1.1 is our local DNS server. DNS query messages is sent to this IP address

793	20.366757	192.168.1.53	192.168.1.1	DNS	71	Standard query 0x0002 A www.mit.edu
794	20.535355	192.168.1.1	192.168.1.53	DNS	160	Standard query response 0x0002 A www.mit.e
795	20.538057	192.168.1.53	192.168.1.1	DNS	71	Standard query 0x0003 AAAA www.mit.edu
797	20.673349	192.168.1.1	192.168.1.53	DNS	200	Standard query response 0x0003 AAAA www.mi
928	24.186551	192.168.1.53	192.168.1.1	DNS	70	Standard query 0x49f7 A piazza.com
930	24.203028	192.168.1.1	192.168.1.53	DNS	198	Standard query response 0x49f7 A piazza.co
1035	25.518104	192.168.1.53	192.168.1.1	DNS	94	Standard query 0x9908 A oauthaccountmanage
1036	25.539571	192.168.1.1	192.168.1.53	DNS	110	Standard query response 0x9908 A oauthacco
983	24.715532	192.168.1.1	192.168.1.53	ICMP	590	Destination unreachable (Fragmentation nee
25	0.363438	192.168.1.53	224.0.0.22	IGMPv3	54	Membership Report / Join group 239.255.255
30	0.452463	192.168.1.53	224.0.0.22	IGMPv3	54	Membership Report / Join group 239.255.255
80	1.358680	192.168.1.53	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.251
87	1.467666	192.168.1.53	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.251

> Internet Protocol Version 4, Src: 192.168.1.53, Dst: 192.168.1.1
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 57
Identification: 0x1c20 (7200)
> Flags: 0x0000
Fragment offset: 0
Time to live: 128
Protocol: UDP (17)
Header checksum: 0x9b0d [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.1.53
Destination: 192.168.1.1

13. Type A. There is no answer, only query.

793	20.366757	192.168.1.53	192.168.1.1	DNS	71 Standard query 0x0002 A www.mit.edu
794	20.535355	192.168.1.1	192.168.1.53	DNS	160 Standard query response 0x0002 A www.

> Frame 793: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF_{2F86FA23-1860-4715-956B-3A40F810F6C4}, id 0

> Ethernet II, Src: IntelCor_83:5e:f5 (f8:94:c2:83:5e:f5), Dst: Tp-LinkT_62:5c:80 (1c:44:19:62:5c:80)

> Internet Protocol Version 4, Src: 192.168.1.53, Dst: 192.168.1.1

> User Datagram Protocol, Src Port: 65212, Dst Port: 53

▼ Domain Name System (query)

Transaction ID: 0x0002

> Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

▼ Queries

> www.mit.edu: type A, class IN

[Response In: 794]

14. There are 3 answers as shown in the picture below. 2 type CNAME and 1 Host address.

793	20.366757	192.168.1.53	192.168.1.1	DNS	71 Standard query 0x0002 A www.mit.edu
794	20.535355	192.168.1.1	192.168.1.53	DNS	160 Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 23.7.207.228

> Frame 794: 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits) on interface \Device\NPF_{2F86FA23-1860-4715-956B-3A40F810F6C4}, id 0

> Ethernet II, Src: Tp-LinkT_62:5c:80 (1c:44:19:62:5c:80), Dst: IntelCor_83:5e:f5 (f8:94:c2:83:5e:f5)

> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.53

> User Datagram Protocol, Src Port: 53, Dst Port: 65212

▼ Domain Name System (response)

Transaction ID: 0x0002

> Flags: 0x8180 Standard query response, No error

Questions: 1

Answer RRs: 3

Authority RRs: 0

Additional RRs: 0

▼ Queries

> www.mit.edu: type A, class IN

▼ Answers

> www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net

> www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net

> e9566.dscb.akamaiedge.net: type A, class IN, addr 23.7.207.228

[Request In: 793]

[Time: 0.168598000 seconds]

16. IP address of DNS query message sent is our default local DNS server.

```
C:\Users\pc>nslookup -type=NS mit.edu
Server: UnKnown
Address: 192.168.1.1

Non-authoritative answer:
mit.edu nameserver = usw2.akam.net
mit.edu nameserver = use2.akam.net
mit.edu nameserver = ns1-173.akam.net
mit.edu nameserver = use5.akam.net
mit.edu nameserver = ns1-37.akam.net
mit.edu nameserver = asia1.akam.net
mit.edu nameserver = asia2.akam.net
mit.edu nameserver = eur5.akam.net
```


559	17.900943	192.168.1.53	192.168.1.1	DNS	67 Standard query 0x0002 NS mit.edu
564	17.976267	192.168.1.1	192.168.1.53	DNS	234 Standard query response 0x0002 NS mit.edu NS usw2.akam.net NS use2.akam.net NS ns1-173.akam.net NS use5.akam.net NS ns1-37.akam.net
189	3.483755	192.168.1.53	188.122.83.151	RTCP	102 Sender Report
190	3.489744	192.168.1.53	188.122.83.151	RTCP	70 Receiver Report

> Frame 564: 234 bytes on wire (1872 bits), 234 bytes captured (1872 bits) on interface \Device\NPF_{2F86FA23-1860-4715-956B-3A40FB10F6C4}, id 0
 > Ethernet II, Src: Tp-LinkT_62:5c:80 (1c:44:19:62:5c:80), Dst: IntelCor_83:5e:f5 (f8:94:c2:83:5e:f5)
 > Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.53
 > User Datagram Protocol, Src Port: 53, Dst Port: 49746
 > Domain Name System (response)
 Transaction ID: 0x0002
 > Flags: 0x8100 Standard query response, No error
 Questions: 1
 Answer RRs: 8
 Authority RRs: 0
 Additional RRs: 0
 > Queries
 > mit.edu: type NS, class IN
 > Answers
 > mit.edu: type NS, class IN, ns usw2.akam.net
 > mit.edu: type NS, class IN, ns use2.akam.net
 > mit.edu: type NS, class IN, ns ns1-173.akam.net
 > mit.edu: type NS, class IN, ns use5.akam.net
 > mit.edu: type NS, class IN, ns ns1-37.akam.net
 > mit.edu: type NS, class IN, ns asia1.akam.net
 > mit.edu: type NS, class IN, ns asia2.akam.net
 > mit.edu: type NS, class IN, ns eur5.akam.net
[\[Request In: 559\]](#)
 [Time: 0.075324000 seconds]

17. Its type is NS. There is no answer.

559	17.900943	192.168.1.53	192.168.1.1	DNS	67 Standard query 0x0002 NS mit.edu
564	17.976267	192.168.1.1	192.168.1.53	DNS	234 Standard query response 0x0002 NS mit.edu NS usw2.akam.net NS use2.akam.net NS ns1-173.akam.net NS use5.akam.net NS ns1-37.akam.net
189	3.483755	192.168.1.53	188.122.83.151	RTCP	102 Sender Report
190	3.489744	192.168.1.53	188.122.83.151	RTCP	70 Receiver Report

> Frame 559: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface \Device\NPF_{2F86FA23-1860-4715-956B-3A40FB10F6C4}, id 0
 > Ethernet II, Src: IntelCor_83:5e:f5 (f8:94:c2:83:5e:f5), Dst: Tp-LinkT_62:5c:80 (1c:44:19:62:5c:80)
 > Internet Protocol Version 4, Src: 192.168.1.53, Dst: 192.168.1.1
 > User Datagram Protocol, Src Port: 49746, Dst Port: 53
 > Domain Name System (query)
 Transaction ID: 0x0002
 > Flags: 0x0100 Standard query
 Questions: 1
 Answer RRs: 0
 Authority RRs: 0
 Additional RRs: 0
 > Queries
 > mit.edu: type NS, class IN
[\[Response In: 564\]](#)

18. The answers provide name servers. There are 8 name servers. It doesn't provide IP addresses.

559	17.900943	192.168.1.53	192.168.1.1	DNS	67 Standard query 0x0002 NS mit.edu
564	17.976267	192.168.1.1	192.168.1.53	DNS	234 Standard query response 0x0002 NS mit.edu NS usw2.akam.net NS use2.akam.net NS ns1-173.akam.net NS use5.akam.net NS ns1-37.akam.net
189	3.483755	192.168.1.53	188.122.83.151	RTCP	102 Sender Report
190	3.489744	192.168.1.53	188.122.83.151	RTCP	70 Receiver Report

> Frame 564: 234 bytes on wire (1872 bits), 234 bytes captured (1872 bits) on interface \Device\NPF_{2F86FA23-1860-4715-956B-3A40FB10F6C4}, id 0
 > Ethernet II, Src: Tp-LinkT_62:5c:80 (1c:44:19:62:5c:80), Dst: IntelCor_83:5e:f5 (f8:94:c2:83:5e:f5)
 > Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.53
 > User Datagram Protocol, Src Port: 53, Dst Port: 49746
 > Domain Name System (response)
 Transaction ID: 0x0002
 > Flags: 0x8100 Standard query response, No error
 Questions: 1
 Answer RRs: 8
 Authority RRs: 0
 Additional RRs: 0
 > Queries
 > mit.edu: type NS, class IN
 > Answers
 > mit.edu: type NS, class IN, ns usw2.akam.net
 > mit.edu: type NS, class IN, ns use2.akam.net
 > mit.edu: type NS, class IN, ns ns1-173.akam.net
 > mit.edu: type NS, class IN, ns use5.akam.net
 > mit.edu: type NS, class IN, ns ns1-37.akam.net
 > mit.edu: type NS, class IN, ns asia1.akam.net
 > mit.edu: type NS, class IN, ns asia2.akam.net
 > mit.edu: type NS, class IN, ns eur5.akam.net
[\[Request In: 559\]](#)
 [Time: 0.075324000 seconds]

20. We used Google DNS Server which is 8.8.8.8 because school's server does not work.

```
C:\Users\pc>nslookup www.aiit.or.kr 8.8.8.8
Server:      dns.google
Address:     8.8.8.8

Non-authoritative answer:
Name:   www.aiit.or.kr
Address: 58.229.6.225
```

Query sent to 8.8.8.8

ip.addr == 192.168.1.53						
No.	Time	Source	Destination	Protocol	Length	Info
214	3.687486	192.168.1.53	8.8.8.8	DNS	80	Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
217	3.714068	8.8.8.8	192.168.1.53	DNS	104	Standard query response 0x0001 PTR 8.8.8.8.in-addr.arpa PTR dns.google
219	3.716154	192.168.1.53	8.8.8.8	DNS	74	Standard query 0x0002 A www.aiit.or.kr
223	3.764014	8.8.8.8	192.168.1.53	DNS	90	Standard query response 0x0002 A www.aiit.or.kr A 58.229.6.225
224	3.767373	192.168.1.53	8.8.8.8	DNS	74	Standard query 0x0003 AAAA www.aiit.or.kr

> Frame 223: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface \Device\NPF_{2F86FA23-1860-4715-956B-3A40FB10F6C4}, id 0
> Ethernet II, Src: Tp-LinkT_62:5c:80 (1c:44:19:62:5c:80), Dst: IntelCor_83:5e:f5 (f8:94:c2:83:5e:f5)
> Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.1.53

21. Type A. There is no answer.

219	3.716154	192.168.1.53	8.8.8.8	DNS	74	Standard query 0x0002 A www.aiit.or.kr
223	3.764014	8.8.8.8	192.168.1.53	DNS	90	Standard query response 0x0002 A www.aiit.or.kr A 58.229.6.225
224	3.767373	192.168.1.53	8.8.8.8	DNS	74	Standard query 0x0003 AAAA www.aiit.or.kr

> Frame 219: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{2F86FA23-1860-4715-956B-3A40FB10F6C4}, id 0
> Ethernet II, Src: IntelCor_83:5e:f5 (f8:94:c2:83:5e:f5), Dst: Tp-LinkT_62:5c:80 (1c:44:19:62:5c:80)
> Internet Protocol Version 4, Src: 192.168.1.53, Dst: 8.8.8.8
> User Datagram Protocol, Src Port: 62104, Dst Port: 53
▼ Domain Name System (query)
Transaction ID: 0x0002
> Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
▼ Queries
> www.aiit.or.kr: type A, class IN
[\[Response In: 223\]](#)

22. The answer is shown in the picture below.

219	3.716154	192.168.1.53	8.8.8.8	DNS	74	Standard query 0x0002 A www.aiit.or.kr
223	3.764014	8.8.8.8	192.168.1.53	DNS	90	Standard query response 0x0002 A www.aiit.or.kr A 58.229.6.225
224	3.767373	192.168.1.53	8.8.8.8	DNS	74	Standard query 0x0003 AAAA www.aiit.or.kr

> Frame 223: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface \Device\NPF_{2F86FA23-1860-4715-956B-3A40FB10F6C4}, id 0
> Ethernet II, Src: Tp-LinkT_62:5c:80 (1c:44:19:62:5c:80), Dst: IntelCor_83:5e:f5 (f8:94:c2:83:5e:f5)
> Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.1.53
> User Datagram Protocol, Src Port: 53, Dst Port: 62104
▼ Domain Name System (response)
Transaction ID: 0x0002
> Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
▼ Queries
> www.aiit.or.kr: type A, class IN
▼ Answers
▼ www.aiit.or.kr: type A, class IN, addr 58.229.6.225
Name: www.aiit.or.kr
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 3571 (59 minutes, 31 seconds)
Data length: 4
Address: 58.229.6.225
[\[Request In: 219\]](#)
[Time: 0.047860000 seconds]