

EEM-413

BİLGİ SAYAR AĞLARI

LABORATUVAR 2 - DNS

Nslookup www.mit.edu yazıldığında ;

```
Microsoft Windows [Sürüm 6.1.7600]
Telif Hakkı (c) 2009 Microsoft Corporation. Tüm hakları saklıdır.

C:\Users\NASA>nslookup www.mit.edu
Sunucu: RT
Address: 192.168.2.1

Güvenilir olmayan yanıt:
Ad: e7086.b.akamaiedge.net
Address: 2.23.182.151
Aliases: www.mit.edu
          www.mit.edu.edgekey.net

C:\Users\NASA>_
```

Nslookup -type = NS mit.edu yazıldığında ;

```
C:\Users\NASA>nslookup www.mit.edu
Sunucu: RT
Address: 192.168.2.1

Güvenilir olmayan yanıt:
Ad: e7086.b.akamaiedge.net
Address: 2.23.182.151
Aliases: www.mit.edu
          www.mit.edu.edgekey.net

C:\Users\NASA>nslookup -type=NS mit.edu
Sunucu: RT
Address: 192.168.2.1

DNS request timed out.
  timeout was 2 seconds.
DNS request timed out.
  timeout was 2 seconds.
*** RT yapilmasi istegi zaman asimina ugradi

C:\Users\NASA>_
```

Nslookup www.aiit.or.kr bitsy.mit.edu

```

C:\Users\NASA>nslookup -type=NS mit.edu
Sunucu: RT
Address: 192.168.2.1

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** RT yapilmasi istegi zaman asimina ugradi

C:\Users\NASA>nslookup www.aiit.or.kr bitsy.mit.edu
DNS request timed out.
    timeout was 2 seconds.
Sunucu: UnKnown
Address: 18.72.0.3

```

```

bilgi göster

C:\Users\NASA>ipconfig

Windows IP Yapilandirmas

Ethernet bagdastirci LAN-verbinding 3:

    Medya Durumu . . . . . : Medya Baglantisi kesildi
    Baglantiya özgü DNS Soneki . . . . . :

Ethernet bagdastirci LAN-verbinding 2:

    Medya Durumu . . . . . : Medya Baglantisi kesildi
    Baglantiya özgü DNS Soneki . . . . . :

Ethernet bagdastirci LAN-verbinding:

    Baglantiya özgü DNS Soneki . . . . . :
    Baglant Yerel IPv6 Adresi . . . . . : fe80::7568:b485:107f:edab%14
    IPv4 Adresi . . . . . : 192.168.2.3
    Alt Ag Maskesi . . . . . : 255.255.255.0
    Varsayilan Ag Geçidi . . . . . : 192.168.2.1

Kablosuz LAN bagdastircisi Draadloze netwerkverbinding 3:

    Medya Durumu . . . . . : Medya Baglantisi kesildi
    Baglantiya özgü DNS Soneki . . . . . :

Kablosuz LAN bagdastircisi Draadloze netwerkverbinding 2:

    Medya Durumu . . . . . : Medya Baglantisi kesildi
    Baglantiya özgü DNS Soneki . . . . . :

Kablosuz LAN bagdastircisi Draadloze netwerkverbinding:

    Medya Durumu . . . . . : Medya Baglantisi kesildi

```

ipconfig/flushdns

```

Tunnel bagdastircisi isatap.{F0F9010A-BE8A-4C4E-94BE-96FA43D7195D}:

    Medya Durumu . . . . . : Medya Baglantisi kesildi
    Baglantiya özgü DNS Soneki . . . . . :

C:\Users\NASA>ipconfig/flushdns

Windows IP Yapilandirmas

DNS Çözücü önbellegi basariyla temizlendi.

C:\Users\NASA>

```

1-)Asia için www.rediff.com denendiğinde nslookup aşağıdaki gibi olmaktadır.

```

Microsoft Windows [Sürüm 6.1.7600]
Telif Hakkı (c) 2009 Microsoft Corporation. Tüm haklar saklıdır.

C:\Users\NASA>nslookup www.rediff.com
Sunucu: RT
Address: 192.168.2.1

Güvenilir olmayan yanıt:
Ad: a1586.w3.akamai.net
Addresses: 80.239.247.68
           80.239.247.31
Aliases: www.rediff.com
          www-b.rediff.com.edgesuite.net

C:\Users\NASA>_

```

2-) nslookup -type=NS.udi.org Avrupadaki bi üniversite sitesi

```

Microsoft Windows [Sürüm 6.1.7600]
Telif Hakkı (c) 2009 Microsoft Corporation. Tüm haklar saklıdır.

C:\Users\NASA>nslookup www.rediff.com
Sunucu: RT
Address: 192.168.2.1

Güvenilir olmayan yanıt:
Ad: a1586.w3.akamai.net
Addresses: 80.239.247.68
           80.239.247.31
Aliases: www.rediff.com
          www-b.rediff.com.edgesuite.net

C:\Users\NASA>nslookup -type=NS.udi.edu
unknown query type: NS.udi.edu
Varsayılan Sunucu: RT
Address: 192.168.2.1

> _

```

3-) nslookup mail.yahoo.com ya baktığımızda ;

```

Ad: a1586.w3.akamai.net
Addresses: 80.239.247.68
           80.239.247.31
Aliases: www.rediff.com
          www-b.rediff.com.edgesuite.net

C:\Users\NASA>nslookup -type=NS.udi.edu
unknown query type: NS.udi.edu
Varsayılan Sunucu: RT
Address: 192.168.2.1

> nslookup mail.yahoo.com
Sunucu: login.lga1.b.yahoo.com
Address: 98.139.237.162
Aliases: mail.yahoo.com
          login.yahoo.com
          login-global.lgg1.b.yahoo.com

DNS request timed out.
  timeout was 2 seconds.
DNS request timed out.
  timeout was 2 seconds.
*** mail.yahoo.com yapilnasi istegi zaman asimina ugradi
>

```

4-) www.ietf.com için wireshark ta bakıldığında aşağıda kırmızıyla belirttiğim gibi User Datagram Protocol yani UDP kullanılmıştır.

No.	Time	Source	Destination	Protocol	Length	Info
1	3.156456900	85.138.111.29	192.168.2.3	UDP	72	Source port: 59345 Destination port: 26125
2	3.510192000	192.168.2.3	4.31.198.44	TCP	78	59345 → 59345 [PSH, ACK] Seq=1 Ack=25 Win=260 Len=24
3	3.589337000	87.210.155.78	192.168.2.3	TCP	78	59345 → 59345 [ACK] Seq=25 Ack=25 Win=260 Len=0
4	3.797220000	192.168.2.3	4.31.198.44	TCP	62	59345 → 59345 [ACK] Seq=25 Ack=25 Win=260 Len=0
5	3.804500000	4.31.198.44	192.168.2.3	TCP	62	59345 → 59345 [ACK] Seq=25 Ack=25 Win=260 Len=0
6	3.804500000	4.31.198.44	192.168.2.3	TCP	62	59345 → 59345 [ACK] Seq=25 Ack=25 Win=260 Len=0
7	3.804500000	4.31.198.44	192.168.2.3	TCP	62	59345 → 59345 [ACK] Seq=25 Ack=25 Win=260 Len=0
8	3.804500000	4.31.198.44	192.168.2.3	TCP	62	59345 → 59345 [ACK] Seq=25 Ack=25 Win=260 Len=0
9	3.804500000	4.31.198.44	192.168.2.3	TCP	62	59345 → 59345 [ACK] Seq=25 Ack=25 Win=260 Len=0
10	3.804500000	4.31.198.44	192.168.2.3	TCP	62	59345 → 59345 [ACK] Seq=25 Ack=25 Win=260 Len=0
11	3.804500000	4.31.198.44	192.168.2.3	TCP	62	59345 → 59345 [ACK] Seq=25 Ack=25 Win=260 Len=0
12	3.804500000	4.31.198.44	192.168.2.3	TCP	62	59345 → 59345 [ACK] Seq=25 Ack=25 Win=260 Len=0
13	3.804500000	4.31.198.44	192.168.2.3	TCP	62	59345 → 59345 [ACK] Seq=25 Ack=25 Win=260 Len=0
14	3.804500000	4.31.198.44	192.168.2.3	TCP	62	59345 → 59345 [ACK] Seq=25 Ack=25 Win=260 Len=0
15	3.804500000	4.31.198.44	192.168.2.3	TCP	62	59345 → 59345 [ACK] Seq=25 Ack=25 Win=260 Len=0
16	3.804500000	4.31.198.44	192.168.2.3	TCP	62	59345 → 59345 [ACK] Seq=25 Ack=25 Win=260 Len=0
17	3.804500000	4.31.198.44	192.168.2.3	TCP	62	59345 → 59345 [ACK] Seq=25 Ack=25 Win=260 Len=0
18	3.804500000	4.31.198.44	192.168.2.3	TCP	62	59345 → 59345 [ACK] Seq=25 Ack=25 Win=260 Len=0
19	3.804500000	4.31.198.44	192.168.2.3	TCP	62	59345 → 59345 [ACK] Seq=25 Ack=25 Win=260 Len=0
20	3.804500000	4.31.198.44	192.168.2.3	TCP	62	59345 → 59345 [ACK] Seq=25 Ack=25 Win=260 Len=0

Frame 10: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface 0
 Ethernet II, Src: WistronT_bb:66:cb (f0:de:f1:bb:66:cb), Dst: Arcadyan_02:4b:ed (00:1a:2a:02:4b:ed)
 Internet Protocol version 4, Src: 192.168.2.3 (192.168.2.3), Dst: 192.168.2.1 (192.168.2.1)
 User Datagram Protocol, Src port: 65292 (65292), Dst port: domain (53)
 Source port: 65292 (65292)
 Destination port: domain (53)
 Length: 38
 checksum: 0x858c [validation disabled]
 Domain Name System (query)

```

0000 00 1a 2a 02 4b ed f0 de f1 bb 66 cb 08 00 45 00  ...K...f...E.
0010 00 1a 2a 02 4b ed f0 de f1 bb 66 cb 08 00 45 00  ...K...f...E.
0020 00 03 ff 0c 00 35 00 26 85 8c ce e0 01 00 00 01  ....5.6.....
0030 00 00 00 00 00 00 00 00 77 77 04 69 65 74 66 03  ....www.ietf.
0040 8f 72 67 00 00 01 00 01 00 00 00 00 00 00 00 00  org....

```

5) Yukarıdaki screenshotta da görüldüğü gibi Source port (Src port) = 65292 ve Destination port yani Dst = 53 üçüncü porttadır.

6) Aşağıda da gösterdiğim gibi Varsayılan ağ geçidi ve DHCP sunucusu IP si 192.168.2.1 dir. Wire shar ta da görülmektedir. Benim Ip adresimde 192.168.2.3 dür.

```

Ethernet bagdast1r3c1 LAN-verbinding:
  Baglant1ya özgü DNS Soneki . . . . . :
  Aç1klama . . . . . : Realtek PCIe FE Family Controller
  Fiziksel Adres . . . . . : F0-DE-F1-BB-66-CB
  Dhcp Etkin . . . . . : Evet
  Otomatik Yap1land1rma Etkin . . . . . : Evet
  Baglant1 Yerel IPv6 Adresi . . . . . : fe80::7568:b485:107f:edab%14(Tercih Edilen)
  IPv4 Adresi . . . . . : 192.168.2.3(Tercih Edilen)
  Alt Ağ Maskesi . . . . . : 255.255.255.0
  Kira Sağlanan . . . . . : 03 Aral1k 2013 Sal1 22:28:11
  Kira Bitisi . . . . . : 04 Aral1k 2013 Çarşamba 00:58:10
  Varsay1lan Ağ Geçidi . . . . . : 192.168.2.1
  DHCP Sunucusu . . . . . : 192.168.2.1
  DHCPv6 IAID . . . . . : 519102193
  DHCPv6 İstemcisi DUID'si . . . . . : 00-01-00-01-19-48-A6-E9-74-E5-0B-69-30-DA
  DNS Sunucusu . . . . . : 192.168.2.1
  Tcpip üzerinden NetBIOS . . . . . : Etkin

Kablosuz LAN bagdast1r3c1s1 Draadloze netwerkverbinding 3:
  Medya Durumu . . . . . : Medya Baglant1s1 kesildi

```

7) Bu standart bir query mesaj ve herhangi bir veri içermemektedir. Yukarıdaki screenshotta da görülmektedir.

8) Aşağıda da gösterildiği gibi TYPE A class IN adres 4.31.198.44 ve DNS sekmesini açtığımızda answer =1 görülmektedir.

No.	Time	Source	Destination	Protocol	Length	Info
3	1.56456900	85.138.11.29	192.168.2.3	UDP	72	Source port: 59345 Destination port: 26325
6	2.58953700	87.230.55.78	192.168.2.3	TCP	78	5938 > 50565 [PSH, ACK] Seq=1 Ack=25 Win=260 Len=24
7	2.79722000	192.168.2.3	87.230.55.78	TCP	54	50565 > 5938 [ACK] Seq=25 Ack=25 Win=0 Len=0
9	3.00430000	85.73.242.100	192.168.2.3	UDP	62	Source port: 46107 Destination port: 26325
10	3.77018600	192.168.2.3	192.168.2.1	DNS	72	Standard query 0xee0 A www.ietf.org
11	3.86343100	192.168.2.1	192.168.2.3	DNS	481	Standard query response 0xee0 A 4.31.198.44
12	3.86343100	192.168.2.3	4.31.198.44	TCP	62	http > 53832 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1452 SACK_PERM=1
14	4.06914300	4.31.198.44	192.168.2.3	TCP	62	http > 53832 [ACK] Seq=1 Ack=1 Win=65340 Len=0
15	4.06920000	192.168.2.3	4.31.198.44	TCP	54	53832 > http [ACK] Seq=1 Ack=1 Win=65340 Len=0
16	4.07024000	192.168.2.3	4.31.198.44	HTTP	585	GET / HTTP/1.1
17	4.27868500	4.31.198.44	192.168.2.3	TCP	60	http > 53832 [ACK] Seq=1 Ack=532 Win=15544 Len=0
18	4.28231300	4.31.198.44	192.168.2.3	TCP	1506	[TCP segment of a reassembled PDU]
19	4.28468400	4.31.198.44	192.168.2.3	TCP	1506	[TCP segment of a reassembled PDU]
20	4.28471100	192.168.2.3	4.31.198.44	TCP	54	53832 > http [ACK] Seq=532 Ack=2905 Win=65340 Len=0

Questions: 1
Answer RRs: 1
Authority RRs: 6
Additional RRs: 11
Queries
Answers
www.ietf.org: type A, class IN, addr 4.31.198.44
Name: www.ietf.org
Type: A (host address)
Class: IN (0x0001)
Time to live: 30 minutes
Data length: 4
Addr: 4.31.198.44 (4.31.198.44)
Authoritative nameservers
Additional records

0000	10 de f1 bb 66 cb 00 1a 29 02 4b 0e 08 00 45 00	f1..bb.66.cb.00.1a.29.02.4b.0e.08.00.45.00
0010	01 d3 00 00 40 00 40 11 b3 c5 c0 a8 02 01 c0 a8	01.d3.00.00.40.00.40.11.b3.c5.c0.a8.02.01.c0.a8
0020	02 00 00 3f ff 0c 01 8f aa 95 ce 60 81 80 00 01	02.00.00.3f.ff.0c.01.8f.aa.95.ce.60.81.80.00.01
0030	00 01 00 06 00 0b 03 77 77 64 63 74 66 03	00.01.00.06.00.0b.03.77.77.64.63.74.66.03
0040	0f 72 67 00 00 01 00 01 c0 0c 00 01 00 00 00	0f.72.67.00.00.01.00.01.c0.0c.00.01.00.00.00
0050	07 08 00 00 04 1f c6 2c c0 10 00 02 00 00 00	07.08.00.00.04.1f.c6.2c.c0.10.00.02.00.00.00
0060	00 84 00 15 01 ae 73 11 04 64 69 61 31 0b 09 69	00.84.00.15.01.ae.73.11.04.64.69.61.31.0b.09.69
0070	49 6c 69 81 73 7d 6a 73 74 01 69 6e 66 8f 00 c0	49.6c.69.81.73.7d.6a.73.74.01.69.6e.66.8f.00.c0

9) ilk SYN paketinde 4.31.198.44 IP adresinden cevap gönderilmiştir.

No.	Time	Source	Destination	Protocol	Length	Info
3	1.56456900	85.138.11.29	192.168.2.3	UDP	72	Source port: 59345 Destination port: 26325
6	2.58953700	87.230.55.78	192.168.2.3	TCP	78	5938 > 50565 [PSH, ACK] Seq=1 Ack=25 Win=260 Len=24
7	2.79722000	192.168.2.3	87.230.55.78	TCP	54	50565 > 5938 [ACK] Seq=25 Ack=25 Win=0 Len=0
9	3.00430000	85.73.242.100	192.168.2.3	UDP	62	Source port: 46107 Destination port: 26325
10	3.77018600	192.168.2.3	192.168.2.1	DNS	72	Standard query 0xee0 A www.ietf.org
11	3.86343100	192.168.2.1	192.168.2.3	DNS	481	Standard query response 0xee0 A 4.31.198.44
12	3.86343100	192.168.2.3	4.31.198.44	TCP	62	http > 53832 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1452 SACK_PERM=1
14	4.06914300	4.31.198.44	192.168.2.3	TCP	62	http > 53832 [ACK] Seq=1 Ack=1 Win=65340 Len=0
15	4.06920000	192.168.2.3	4.31.198.44	TCP	54	53832 > http [ACK] Seq=1 Ack=1 Win=65340 Len=0
16	4.07024000	192.168.2.3	4.31.198.44	HTTP	585	GET / HTTP/1.1
17	4.27868500	4.31.198.44	192.168.2.3	TCP	60	http > 53832 [ACK] Seq=1 Ack=532 Win=15544 Len=0
18	4.28231300	4.31.198.44	192.168.2.3	TCP	1506	[TCP segment of a reassembled PDU]
19	4.28468400	4.31.198.44	192.168.2.3	TCP	1506	[TCP segment of a reassembled PDU]
20	4.28471100	192.168.2.3	4.31.198.44	TCP	54	53832 > http [ACK] Seq=532 Ack=2905 Win=65340 Len=0

Frame 12: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface 0
Ethernet II, Src: Wlstront1_b6:66:cb (00:1a:2a:02:4b:ed), Dst: Arcadyan_02:4b:ed (00:1a:2a:02:4b:ed)
Internet Protocol Version 4, Src: 192.168.2.3 (192.168.2.3), Dst: 4.31.198.44 (4.31.198.44)
Version: 4
Header Length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECT-Capable Transport))
Total Length: 48
Identification: 0x7dda (32218)

10) Aşağıda da görüldüğü gibi web sitesindeki resimler için yeni bir DNS query oluşturulmamıştır.

Filter: ip.addr==192.168.2.3		Expression: Clear Apply Save				
No.	Time	Source	Destination	Protocol	Length	Info
53	4.96375300	4.31.198.44	192.168.2.3	HTTP	1335	HTTP/1.1 200 OK (text/css)
54	4.96376400	4.31.198.44	192.168.2.3	TCP	62	http > 53837 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1452 SACK_PERM=1
55	4.96383900	192.168.2.3	4.31.198.44	TCP	54	53837 > http [ACK] Seq=1 Ack=1 Win=65340 Len=0
56	4.96551100	192.168.2.3	4.31.198.44	HTTP	429	GET /images/letflogotrans.gif HTTP/1.1
57	4.96570000	4.31.198.44	192.168.2.3	TCP	62	http > 53840 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1452 SACK_PERM=1
58	4.96700000	192.168.2.3	4.31.198.44	TCP	54	53840 > http [ACK] Seq=1 Ack=1 Win=65340 Len=0
59	4.96703400	4.31.198.44	192.168.2.3	TCP	62	http > 53838 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1452 SACK_PERM=1
60	4.96703500	4.31.198.44	192.168.2.3	TCP	62	http > 53839 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1452 SACK_PERM=1
61	4.96706000	192.168.2.3	4.31.198.44	TCP	54	53838 > http [ACK] Seq=1 Ack=1 Win=65340 Len=0
62	4.96707300	192.168.2.3	4.31.198.44	TCP	54	53839 > http [ACK] Seq=1 Ack=1 Win=65340 Len=0
63	4.96920200	192.168.2.3	4.31.198.44	HTTP	429	GET /images/london-tower-bridge.jpg HTTP/1.1
64	4.97102100	192.168.2.3	4.31.198.44	HTTP	429	GET /images/chat-trans.png HTTP/1.1
65	4.97121000	4.31.198.44	192.168.2.3	TCP	62	http > 53841 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1452 SACK_PERM=1
66	4.97124800	192.168.2.3	4.31.198.44	TCP	54	53841 > http [ACK] Seq=1 Ack=1 Win=65340 Len=0
67	4.97240000	192.168.2.3	4.31.198.44	HTTP	429	GET /images/robotics-and-robot-robot.jpg HTTP/1.1
Frame 63: 457 bytes on wire (3656 bits), 457 bytes captured (3656 bits) on interface 0						
Ethernet II, Src: wiStront_bb:66:cb (f0:de:f1:bb:66:cb), Dst: Arcadyan_02:4b:ed (00:1a:2a:02:4b:ed)						
Internet Protocol Version 4, Src: 192.168.2.3 (192.168.2.3), Dst: 4.31.198.44 (4.31.198.44)						
Version: 4						
Header Length: 20 bytes						
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECT-Capable Transport))						
Total Length: 443						
Identification: 0xdf9 (32249)						
Flags: 0x02 (Don't Fragment)						
Fragment offset: 0						
Time to live: 128						
Protocol: TCP (6)						
Header checksum: 0x0000 (Incorrect, should be 0xe61c (may be caused by 'IP checksum offload'))						
<pre>0000 00 1a 2a 02 4b ed f0 de f1 bb 66 cb 08 00 45 00 ...R...f...E. 0010 01 bb 7d f9 40 00 80 06 00 00 c0 a8 02 03 04 1f ...B... 0020 c0 2c d2 50 00 30 1e f1 3d 9d 6e b1 30 c0 50 18 ...P.P...n.P.P. 0030 ff 3e 84 00 67 45 20 2f 69 68 61 67 65 00 00 00 ...<...GK T /image 0040 73 2f 4c 6f 6e 64 6f 6e 2d 6f 65 72 42 72 2f 2f s/London -Tower br 0050 69 64 67 65 2e 6a 70 67 20 48 34 34 30 2f 31 2e dge.jpg HTTP/1. 0060 31 0d 04 65 73 65 70 2a 3a 20 2f 2a 0d 0a 2f 2f l..Accept t: /i/ 0070 52 65 66 65 72 65 72 3a 20 68 74 74 70 3a 2f 2f Referer: http://</pre>						

nslookup cmd kismından www.mit.edu yaptığımızda aşağıdaki çıktıyı görmekteyiz.

Filter: ip.address:192.168.2.3

Expression: Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
3	1.56725700	192.168.2.3	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
4	3.56070600	192.168.2.1	192.168.2.3	UDP	324	Source port: sonus-logging Destination port: 51296
5	4.56314600	192.168.2.3	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
6	5.56074500	192.168.2.1	192.168.2.3	UDP	324	Source port: sonus-logging Destination port: 51296
7	7.56322300	192.168.2.3	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
9	9.56074700	192.168.2.1	192.168.2.3	UDP	324	Source port: sonus-logging Destination port: 51296
11	10.67461000	192.168.2.3	192.168.2.1	DNS	64	Standard query 0x0001 PTR 192.168.192.10.in-addr.arpa
12	10.67515000	192.168.2.1	192.168.2.3	DNS	100	Standard query response 0x0001 PTR RT
13	10.67665200	192.168.2.3	192.168.2.1	DNS	71	Standard query 0x0002 A www.mit.edu
14	10.75616800	192.168.2.1	192.168.2.3	DNS	429	Standard query response 0x0002 CNAME www.mit.edu.edgekey.net CNAME e7086.b.akamaiedge.net
15	10.75719100	192.168.2.3	192.168.2.1	DNS	71	Standard query 0x0003 AAAA www.mit.edu
16	10.76014000	192.168.2.1	192.168.2.3	DNS	202	Standard query response 0x0003 CNAME www.mit.edu.edgekey.net CNAME e7086.b.akamaiedge.net

Frame 13: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface 0

Ethernet II, Src: WiStront_bb:66:cb (f0:de:f1:bb:66:cb), Dst: Arcadyan_02:4b:ed (00:1a:2a:02:4b:ed)

Internet Protocol Version 4, Src: 192.168.2.3 (192.168.2.3), Dst: 192.168.2.1 (192.168.2.1)

User Datagram Protocol, Src Port: 55516 (55516), Dst Port: domain (53)

Domain Name System (query)

[Response in: 1]

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

Name: www.mit.edu

Type: A (host address)

Class: IN (0x0001)

0000 00 1a 2a 02 4b ed f0 de f1 bb 66 cb 08 00 45 00 ...R...f...E.
0010 00 39 7f bc 00 00 80 11 00 00 c0 a8 02 03 c0 a8 ...9...
0020 02 01 88 dc 00 35 00 25 85 80 00 02 01 00 00 01 5...
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ...0...
0040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ...0...

11) Source port 55516 ve Destination Port ta 53 dür. Yukarıdaki screen shottada görülmektedir.

12) Daha önce ipconfig / all yaptığımızda da gördüğümüz gibi 192.168.2.1 IP adresi benim local default DNS server IP adresimdir.

13) Yukarıdaki screenshottada görüldüğü gibi TYPE A DNS türüdür. Ve Answer veya bi içerik içermez.

14) Aşağıdaki screenshottada görüldüğü gibi 1 cevap gelmiş ve içeriğide aşağıda belirtilmiştir.

Filter: ip.addr== 192.168.2.3

No.	Time	Source	Destination
11	10.6746100	192.168.2.3	192.168.2.1
12	10.6761540	192.168.2.1	192.168.2.3
13	10.6773680	192.168.2.1	192.168.2.3
14	10.6785820	192.168.2.3	192.168.2.1
15	10.7573440	192.168.2.3	192.168.2.1
16	10.7801400	192.168.2.1	192.168.2.3

Flag: 0x0000 Standard query response, no error

Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0

Queries

- 1.2.168.192.in-addr.arpa: type PTR, class IN
Name: 1.2.168.192.in-addr.arpa
Type: PTR (Domain name pointer)
Class: IN (0x0001)

Answers

- 1.2.168.192.in-addr.arpa: type PTR, class IN, RT
Name: 1.2.168.192.in-addr.arpa
Type: PTR (Domain name pointer)
Class: IN (0x0001)
Time to live: 2 hours, 46 minutes, 40 seconds
Data length: 4
Domain Name: RT

16) Kendi bilgisayarımdan ve farklı bir bilgisayardan denememe rağmen nslookup-type=NS mit.edu DNS için timeout vermektedir. Bundan dolayı lab föyünden trace indirme kısmından edindiğim tracelerle devam etmekte dolayısıyla IP adreslerinde farklılıklar bulunmaktadır. Aşağıdaki screenshot a göre DNS query mesajının IP adresi 128.238.29.22 dir.

Time	Source	Destination	Proto	Length	Info
493.30	918636	128.238.29.22	DNS	176	Standard query response 0x0003 NS bitsy.mit.edu NS strawb.mit.edu NS w20ns.mit.edu
492.30	918275	128.238.38.160	DNS	67	Standard query 0x0003 NS mit.edu
491.30	918044	128.238.29.22	DNS	135	Standard query response 0x0002 no such name
490.30	917700	128.238.38.160	DNS	76	Standard query 0x0002 NS mit.edu.poly.edu
489.30	916859	128.238.29.22	DNS	118	Standard query response 0x0001 PTR dns-prime.poly.edu
488.30	916492	128.238.38.160	DNS	86	Standard query 0x0001 PTR 22.29.238.128.in-addr.arpa
389.25	565607	128.238.38.154	DHCP	342	DHCP Inform - Transaction ID 0x7e7caa5e
325.21	564095	128.238.38.154	DHCP	342	DHCP Inform - Transaction ID 0x7e7caa5e
8.0	514535	cisco_fc:f0:de	CDP/VTP/DTCP/PagP/UCDP	371	Device ID: D8221C Port ID: FastEthernet0/30
553.34	289153	128.238.38.252	BROWSE	243	Host Announcement POLYME, workstation, Server, NT workstation, Potential Browser
571.32	918867	128.238.38.31	BROWSE	248	Host Announcement STAYUP-1 FROM workstation Server NT workstation Potential Browser

[Request ID: 488]
[Time: 0.000367000 seconds]
Transaction ID: 0x0001
Flags: 0x8580 standard query response, No error
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
Queries
Answers
22.29.238.128.in-addr.arpa: type PTR, class IN, dns-prime.poly.edu
Name: 22.29.238.128.in-addr.arpa
Type: PTR (Domain name pointer)
Class: IN (0x0001)
Time to live: 1 hour
Data length: 20
Domain Name: dns-prime.poly.edu

0000 00 09 6b 10 60 99 00 b0 8a 83 ea 54 08 00 45 00 . . k T . . E .
0010 00 68 00 55 00 00 7e 11 f6 9d 80 ee 1d 16 80 ee . h . u
0020 26 a0 00 35 0e a0 00 54 25 35 00 01 85 80 00 01 & . 5 T NS
0030 00 01 00 00 00 00 02 32 02 32 39 03 22 33 38 2 2 29 238
0040 03 31 32 38 07 69 6e 2d 61 64 64 72 04 61 72 70 . 128 . in - addr . arp
0050 61 00 00 0c 00 01 c0 0c 00 0c 00 01 00 00 0e 10 a
0060 00 14 09 64 6e 73 2d 70 72 69 6d 65 04 70 6f 6c . . . dns - p rime . pol
0070 79 03 65 64 75 00 y . edu .

17)Type NS ve answer yani bir içerik bulunmamaktadır.

18)İsim serverı bitsy, strawb and w20ns. Additional kısmına bakar isek Ip adresini buluruz.

Answers

mit.edu: type NS, class inet, ns bitsy.mit.edu
mit.edu: type NS, class inet, ns strawb.mit.edu
mit.edu: type NS, class inet, ns w20ns.mit.edu

Additional records

bitsy.mit.edu: type A, class inet, addr 18.72.0.3
strawb.mit.edu: type A, class inet, addr 18.71.0.151
w20ns.mit.edu: type A, class inet, addr 18.70.0.160

20)Aşağıdaki screeshotta da belirtildiği gibi IP = 18.72.0.3 dur.
Hayır benim default local DNS serverım değil. Bu bitsy.mit.edu ya ait.

No.	Time	Source	Destination	Protocol	Length	Info
7	0.230878	128.238.38.177	128.238.38.255	BROWSE	216	Get backup List Request
97	4.186743	128.238.38.207	128.238.38.255	BROWSE	254	Domain/workgroup Announcement MSHOME, NT workstation, Domain Enum
113	4.480689	128.238.38.177	128.238.38.255	BROWSE	216	Get backup List Request
100	4.265296	128.238.38.160	18.72.0.3	DNS	82	Standard query 0x0001 PTR 3.0.72.18.in-addr.arpa
101	4.278516	18.72.0.3	128.238.38.160	DNS	212	Standard query response 0x0001 PTR 3.0.72.18.in-addr.arpa
102	4.279430	128.238.38.160	18.72.0.3	DNS	83	Standard query 0x0002 A www.aift.or.kr.poly.edu
103	4.293283	18.72.0.3	128.238.38.160	DNS	135	Standard query response 0x0002 No such name
104	4.293517	128.238.38.160	18.72.0.3	DNS	74	Standard query 0x0003 A www.aift.or.kr
105	4.307859	18.72.0.3	128.238.38.160	DNS	156	Standard query response 0x0003 A 218.36.94.200
41	1.860140	128.238.38.2	224.0.0.2	HSRP	62	hello (state Active)
114	1.860168	128.238.38.2	224.0.0.2	HSRP	62	hello (state Active)

Frame 102: 83 bytes on wire (664 bits), 83 bytes captured (664 bits)

Ethernet II, Src: Zbn10:60:99 (00:09:6b:10:60:99), Dst: All-HSRP-routers_00 (00:00:0c:07:ac:00)

Internet Protocol Version 4, Src: 128.238.38.160 (128.238.38.160), Dst: 18.72.0.3 (18.72.0.3)

User Datagram Protocol, Src Port: vlmoteagent (3752), Dst Port: domain (53)

Domain Name System (query)

Response in: 1011

Transaction ID: 0x0002

Flags: 0x0100 standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

Queries

www.aift.or.kr.poly.edu: type A, class IN

Name: www.aift.or.kr.poly.edu

Type: A (Host address)

Class: IN (0x0001)

21) Yukarıda da görüldüğü gibi DNS TYPE A dir. Ve answer yoktur.

22-23) Aşağıdaki screenshot tada görüldüğü gibi 1 answer var ve içeriğide screenshotta gösterilmiştir.

No.	Time	Source	Destination	Protocol	Length	Info
7	0.230878	128.238.38.177	128.238.38.255	BROWSE	216	Get Backup List Request
97	4.186743	128.238.38.207	128.238.38.255	BROWSE	254	Domain/workgroup Announcement MSHOME, NT workstation, Domain Enum
113	4.480689	128.238.38.177	128.238.38.255	BROWSE	216	Get backup List Request
100	4.265296	128.238.38.160	18.72.0.3	DNS	82	Standard query 0x0001 PTR 3.0.72.18.in-addr.arpa
101	4.278516	18.72.0.3	128.238.38.160	DNS	212	Standard query response 0x0001 PTR 3.0.72.18.in-addr.arpa
102	4.279430	128.238.38.160	18.72.0.3	DNS	83	Standard query 0x0002 A www.aift.or.kr.poly.edu
103	4.293283	18.72.0.3	128.238.38.160	DNS	135	Standard query response 0x0002 No such name
104	4.293517	128.238.38.160	18.72.0.3	DNS	74	Standard query 0x0003 A www.aift.or.kr
105	4.307859	18.72.0.3	128.238.38.160	DNS	156	Standard query response 0x0003 A 218.36.94.200
41	1.860140	128.238.38.2	224.0.0.2	HSRP	62	hello (state Active)
114	1.860168	128.238.38.2	224.0.0.2	HSRP	62	hello (state Active)

Frame 102: 83 bytes on wire (664 bits), 83 bytes captured (664 bits)

Ethernet II, Src: Zbn10:60:99 (00:09:6b:10:60:99), Dst: All-HSRP-routers_00 (00:00:0c:07:ac:00)

Internet Protocol Version 4, Src: 128.238.38.160 (128.238.38.160), Dst: 18.72.0.3 (18.72.0.3)

User Datagram Protocol, Src Port: vlmoteagent (3752), Dst Port: domain (53)

Domain Name System (query)

Response in: 1011

Transaction ID: 0x0002

Flags: 0x0100 standard query

Questions: 1

Answer RRs: 0

Authority RRs: 2

Additional RRs: 2

Queries

www.aift.or.kr: type A, class IN

Name: www.aift.or.kr

Type: A (Host address)

Class: IN (0x0001)

Answers

www.aift.or.kr: type A, class IN, addr 218.36.94.200

Name: www.aift.or.kr

Type: A (Host address)

Class: IN (0x0001)

Time to live: 55 minutes, 38 seconds

Data length: 4

Addr: 218.36.94.200 (218.36.94.200)

Authoritative nameservers

Additional records