

22100011015 Nursena Taşköprü

Bilgisayar Ağları Ödev 3

ip.addr == 192.168.1.1						
No.	Time	Source	Destination	Protocol	Length	Info
8	1.408684	192.168.1.102	192.168.1.1	DNS	75	Standard query 0x3846 A shftr.adnxs.net
9	1.408883	192.168.1.102	192.168.1.1	DNS	75	Standard query 0x6083 HTTPS shftr.adnxs.net
31	1.435673	192.168.1.102	192.168.1.1	DNS	87	Standard query 0x827d A browser.events.data.msn.com
32	1.435859	192.168.1.102	192.168.1.1	DNS	87	Standard query 0xd652 HTTPS browser.events.data.msn.com
88	1.436875	192.168.1.1	192.168.1.102	DNS	132	Standard query response 0x3846 A shftr.adnxs.net CNAME xandr-shftr.trafficmanager.net A 68.67.153.38
89	1.436875	192.168.1.1	192.168.1.102	DNS	177	Standard query response 0x6083 HTTPS shftr.adnxs.net CNAME xandr-shftr.trafficmanager.net SOA tml.dns-tm.com
98	1.460691	192.168.1.1	192.168.1.102	DNS	214	Standard query response 0x827d A browser.events.data.msn.com CNAME global.asimov.events.data.trafficmanager.net
99	1.461659	192.168.1.1	192.168.1.102	DNS	280	Standard query response 0xd652 HTTPS browser.events.data.msn.com CNAME global.asimov.events.data.trafficmanager.net
346	1.600034	192.168.1.102	192.168.1.1	DNS	72	Standard query 0x3527 A www.bing.com
348	1.600297	192.168.1.102	192.168.1.1	DNS	72	Standard query 0xa2ba HTTPS www.bing.com
399	1.624800	192.168.1.1	192.168.1.102	DNS	337	Standard query response 0x3527 A www.bing.com CNAME www-www.bing.com.trafficmanager.net CNAME www.bing.com
401	1.625452	192.168.1.1	192.168.1.102	DNS	254	Standard query response 0xa2ba HTTPS www.bing.com CNAME www-www.bing.com.trafficmanager.net CNAME www.bing.com
872	1.758893	192.168.1.102	192.168.1.1	DNS	84	Standard query 0xeb57 A ecn.dev.virtualearth.net
873	1.759027	192.168.1.102	192.168.1.1	DNS	84	Standard query 0xf07f HTTPS ecn.dev.virtualearth.net
10...	1.789297	192.168.1.102	192.168.1.1	DNS	96	Standard query 0x9d36 A functional.events.data.microsoft.com
10...	1.789483	192.168.1.102	192.168.1.1	DNS	96	Standard query 0xae90 HTTPS functional.events.data.microsoft.com
10...	1.793291	192.168.1.1	192.168.1.102	DNS	186	Standard query response 0xeb57 A ecn.dev.virtualearth.net CNAME ssl2.tiles.virtualearth.net.edgekey.net CNAME
10...	1.793291	192.168.1.1	192.168.1.102	DNS	234	Standard query response 0xf07f HTTPS ecn.dev.virtualearth.net CNAME ssl2.tiles.virtualearth.net.edgekey.net
12...	1.834116	192.168.1.1	192.168.1.102	DNS	223	Standard query response 0x9d36 A functional.events.data.microsoft.com CNAME global.asimov.events.data.trafficmanager.net

dns						
No.	Time	Source	Destination	Protocol	Length	Info
8	1.408684	192.168.1.102	192.168.1.1	DNS	75	Standard query 0x3846 A shftr.adnxs.net
9	1.408883	192.168.1.102	192.168.1.1	DNS	75	Standard query 0x6083 HTTPS shftr.adnxs.net
31	1.435673	192.168.1.102	192.168.1.1	DNS	87	Standard query 0x827d A browser.events.data.msn.com
32	1.435859	192.168.1.102	192.168.1.1	DNS	87	Standard query 0xd652 HTTPS browser.events.data.msn.com
88	1.436875	192.168.1.1	192.168.1.102	DNS	132	Standard query response 0x3846 A shftr.adnxs.net CNAME xandr-shftr.trafficmanager.net A 68.67.153.38
89	1.436875	192.168.1.1	192.168.1.102	DNS	177	Standard query response 0x6083 HTTPS shftr.adnxs.net CNAME xandr-shftr.trafficmanager.net SOA tml.dns-tm.com
98	1.460691	192.168.1.1	192.168.1.102	DNS	214	Standard query response 0x827d A browser.events.data.msn.com CNAME global.asimov.events.data.trafficmanager.net
99	1.461659	192.168.1.1	192.168.1.102	DNS	280	Standard query response 0xd652 HTTPS browser.events.data.msn.com CNAME global.asimov.events.data.trafficmanager.net
346	1.600034	192.168.1.102	192.168.1.1	DNS	72	Standard query 0x3527 A www.bing.com
348	1.600297	192.168.1.102	192.168.1.1	DNS	72	Standard query 0xa2ba HTTPS www.bing.com
399	1.624800	192.168.1.1	192.168.1.102	DNS	337	Standard query response 0x3527 A www.bing.com CNAME www-www.bing.com.trafficmanager.net CNAME www.bing.com
401	1.625452	192.168.1.1	192.168.1.102	DNS	254	Standard query response 0xa2ba HTTPS www.bing.com CNAME www-www.bing.com.trafficmanager.net CNAME www.bing.com
872	1.758893	192.168.1.102	192.168.1.1	DNS	84	Standard query 0xeb57 A ecn.dev.virtualearth.net
873	1.759027	192.168.1.102	192.168.1.1	DNS	84	Standard query 0xf07f HTTPS ecn.dev.virtualearth.net
10...	1.789297	192.168.1.102	192.168.1.1	DNS	96	Standard query 0x9d36 A functional.events.data.microsoft.com
10...	1.789483	192.168.1.102	192.168.1.1	DNS	96	Standard query 0xae90 HTTPS functional.events.data.microsoft.com

a. DNS sorgu (query) ve cevap (response) mesajlarını bulunuz. Bu mesajlar TCP veya UDP protokollerinden hangisi ile gönderilmiştir? Ekran görüntüsü ile gösteriniz.

Filtreye dns yazdığımızda info kısmında dns query mi response mu olduğunu görüyoruz.

dns						
No.	Time	Source	Destination	Protocol	Length	Info
8	1.408684	192.168.1.102	192.168.1.1	DNS	75	Standard query 0x3846 A shftr.adnxs.net
9	1.408883	192.168.1.102	192.168.1.1	DNS	75	Standard query 0x6083 HTTPS shftr.adnxs.net
31	1.435673	192.168.1.102	192.168.1.1	DNS	87	Standard query 0x827d A browser.events.data.msn.com
32	1.435859	192.168.1.102	192.168.1.1	DNS	87	Standard query 0xd652 HTTPS browser.events.data.msn.com
88	1.436875	192.168.1.1	192.168.1.102	DNS	132	Standard query response 0x3846 A shftr.adnxs.net CNAME xandr-shftr.trafficmanager.net A 68.67.153.38
89	1.436875	192.168.1.1	192.168.1.102	DNS	177	Standard query response 0x6083 HTTPS shftr.adnxs.net CNAME xandr-shftr.trafficmanager.net SOA tml.dns-tm.com
98	1.460691	192.168.1.1	192.168.1.102	DNS	214	Standard query response 0x827d A browser.events.data.msn.com CNAME global.asimov.events.data.trafficmanager.net
99	1.461659	192.168.1.1	192.168.1.102	DNS	280	Standard query response 0xd652 HTTPS browser.events.data.msn.com CNAME global.asimov.events.data.trafficmanager.net
346	1.600034	192.168.1.102	192.168.1.1	DNS	72	Standard query 0x3527 A www.bing.com
348	1.600297	192.168.1.102	192.168.1.1	DNS	72	Standard query 0xa2ba HTTPS www.bing.com

Frame, Ethernet II, Internet Protocol Version 4, User Datagram Protocol (UDP) veya Transmission Control Protocol (TCP), Domain Name System (query/response) kısımlarını görüyoruz. Burda User Datagram Protocol yazıyorsa paket UDP kullanıyor,

Transmission Control Protocol yazıyorsa paket TCP kullanıyor demektir.

```
Frame 8: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF_{4E4E1912-FCDB-4A9B-989A-C6F8092200A9}, id 0
Ethernet II, Src: AzureWaveTec_50:07:ef (b4:8c:9d:50:07:ef), Dst: TplinkTechno_e4:29:08 (5c:63:bf:e4:29:08)
Internet Protocol Version 4, Src: 192.168.1.102, 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: 61
    Identification: 0x22ea (8938)
  000. .... = Flags: 0x0
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 128
  Protocol: UDP (17)
  Header Checksum: 0x940e [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.1.102
  Destination Address: 192.168.1.1
  [Stream index: 3]
User Datagram Protocol, Src Port: 61318, Dst Port: 53
  Source Port: 61318
  Destination Port: 53
  Length: 41
  Checksum: 0x2370 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 3]
  [Stream Packet Number: 1]
  [Timestamps]
  UDP payload (33 bytes)
Domain Name System (query)
```

b. DNS sorgu mesajının port numarası nedir? Ekran görüntüsü ile gösteriniz.

```
Frame 8: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF_{4E4E1912-FCDB-4A9B-989A-C6F8092200A9}, id 0
Ethernet II, Src: AzureWaveTec_50:07:ef (b4:8c:9d:50:07:ef), Dst: TplinkTechno_e4:29:08 (5c:63:bf:e4:29:08)
Internet Protocol Version 4, Src: 192.168.1.102, 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: 61
    Identification: 0x22ea (8938)
  000. .... = Flags: 0x0
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 128
  Protocol: UDP (17)
  Header Checksum: 0x940e [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.1.102
  Destination Address: 192.168.1.1
  [Stream index: 3]
User Datagram Protocol, Src Port: 61318, Dst Port: 53
  Source Port: 61318
  Destination Port: 53
  Length: 41
  Checksum: 0x2370 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 3]
  [Stream Packet Number: 1]
  [Timestamps]
  UDP payload (33 bytes)
Domain Name System (query)
```

Bilgisayarım bu portu kullanarak DNS sunucusuna sorgu yollar.

c. DNS cevap mesajının port numarası nedir? Ekran görüntüsü ile gösteriniz.

```
Frame 8: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF_{4E4E1912-FCDB-4A9B-989A-C6F8092200A9}, i
Ethernet II, Src: AzureWaveTec_50:07:ef (b4:8c:9d:50:07:ef), Dst: TpLinkTechno_e4:29:08 (5c:63:bf:e4:29:08)
Internet Protocol Version 4, Src: 192.168.1.102, 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: 61
  Identification: 0x22ea (8938)
  000. .... = Flags: 0x0
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 128
  Protocol: UDP (17)
  Header Checksum: 0x940e [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.1.102
  Destination Address: 192.168.1.1
  [Stream index: 3]
User Datagram Protocol, Src Port: 61318, Dst Port: 53
  Source Port: 61318
  Destination Port: 53
  Length: 41
  Checksum: 0x2370 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 3]
  [Stream Packet Number: 1]
  [Timestamps]
  UDP payload (33 bytes)
Domain Name System (query)
```

Bilgisayarımda DNS yanıtının ulaştığı port.

d. DNS sorgu mesajını inceleyiniz. Bu sorgu mesajı herhangi bir cevap (answer) içermekte midir? İçeriyorsa bu cevabın içeriği nedir? Ekran görüntüsü ile gösteriniz.

Normalde DNS sorgu mesajları (query), cevap içermez. Ama bazı durumlarda önceden cache'te varsa veya "additional records" gibi bölümler varsa, bir şeyler içerebilir. İlk resimde answer yok. İkinci resimde var.

```
Wireshark - Paket 8 - 22100011015_Odev3.pcapng
  ▶ Frame 8: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF_{4...
  ▶ Ethernet II, Src: AzureWaveTec_50:07:ef (b4:8c:9d:50:07:ef), Dst: TpLinkTechno_e4:29:08 (5c:63:bf:e4:29:08)
  ▶ Internet Protocol Version 4, Src: 192.168.1.102, Dst: 192.168.1.1
  ▶ User Datagram Protocol, Src Port: 61318, Dst Port: 53
  ▼ Domain Name System (query)
    Transaction ID: 0x3846
    ▶ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
    ▶ Queries
      [Response In: 88]

Wireshark - Paket 1022 - 22100011015_Odev3.pcapng
  ▶ Frame 1022: 234 bytes on wire (1872 bits), 234 bytes captured (1872 bits) on interface \Device\NPF_{4E4E1912-FCDB-4A9B-989A-C6F...
  ▶ Ethernet II, Src: TpLinkTechno_e4:29:08 (5c:63:bf:e4:29:08), Dst: AzureWaveTec_50:07:ef (b4:8c:9d:50:07:ef)
  ▶ Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.102
  ▶ User Datagram Protocol, Src Port: 53, Dst Port: 64237
  ▼ Domain Name System (response)
    Transaction ID: 0xf07f
    ▶ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 1
    Additional RRs: 0
    ▶ Queries
      ▶ ecn.dev.virtualearth.net: type HTTPS, class IN
    ▶ Answers
      ▶ ecn.dev.virtualearth.net: type CNAME, class IN, cname ssl2.tiles.virtualearth.net.edgekey.net
      ▶ ssl2.tiles.virtualearth.net.edgekey.net: type CNAME, class IN, cname e4113.dscd.akamaiedge.net
    ▶ Authoritative nameservers
    [Request In: 873]
    [Time: 0.034264000 seconds]
```

e. DNS cevap mesajını inceleyiniz. Kaç tane cevap (answer) içermektedir? Bu cevapların her birinin içeriği nedir? Ekran görüntüsü ile gösteriniz.

Cevaba tıklandığında içerikler gözüküyor. CNAME (alan adı yönlendirme) işlemi.

İlkinde ecn.dev.virtualearth.net adresi aslında ssl2.tiles.virtualearth.net.edgekey.net alan adına yönlendirilmiş.

İkincisinde önceki yönlendirme başka bir adrese yönlenmiş: e4113.dscd.akamaiedge.net

```
Answers
  ▼ ecn.dev.virtualearth.net: type CNAME, class IN, cname ssl2.tiles.virtualearth.net.edgekey.net
    Name: ecn.dev.virtualearth.net
    Type: CNAME (5) (Canonical NAME for an alias)
    Class: IN (0x0001)
    Time to live: 1556 (25 minutes, 56 seconds)
    Data length: 38
    CNAME: ssl2.tiles.virtualearth.net.edgekey.net
  ▼ ssl2.tiles.virtualearth.net.edgekey.net: type CNAME, class IN, cname e4113.dscd.akamaiedge.net
    Name: ssl2.tiles.virtualearth.net.edgekey.net
    Type: CNAME (5) (Canonical NAME for an alias)
    Class: IN (0x0001)
    Time to live: 139 (2 minutes, 19 seconds)
    Data length: 24
    CNAME: e4113.dscd.akamaiedge.net
```