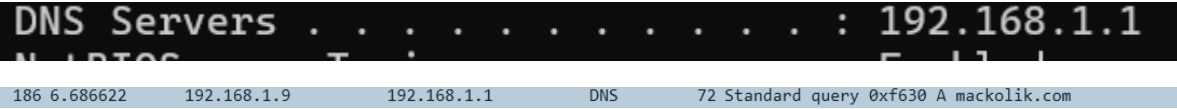
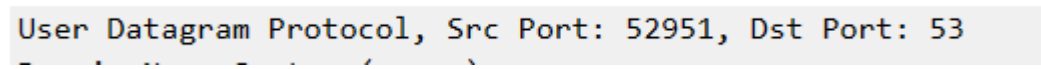
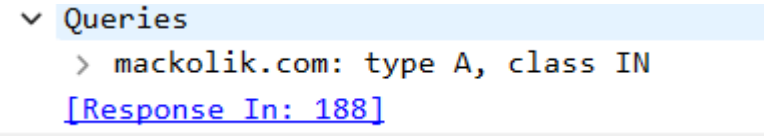
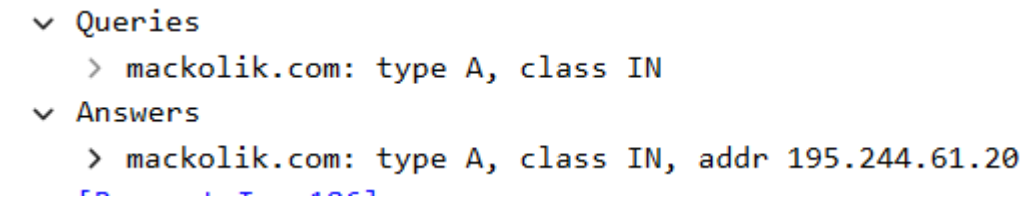
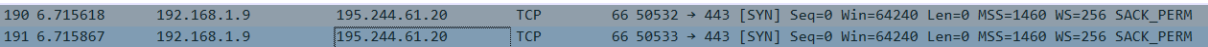


Bilgisayar Ağları LAB5

- 1- 

Cmd ve wireshark üzerinden baktığımda iki adresin de aynı olduğunu görüyorum. 192.168.1.1 adresine gönderilmiş.
- 2- Benim gördüğüm işlemlerde genellikle UDP (User Datagram Protocol) kullanılıyor.
 

Fakat eğer boyutu UDP maksimum paket boyutundan büyük mesajlar gönderilirse TCP de kullanılabilir.
- 3- Bir önceki sorudaki ekran görüntüsünde görüldüğü gibi 53 numaralı port hedef porttur.
- 4- Tarafımdan gönderilen ilk sorgu mesajının Type A türü olduğu görünüyor. Sitenin Ip adresini öğrenmek istiyorum anlamına geliyor. Herhangi bir cevap içermiyor.
 
- 5- Response mesajında görülen sorgu 1 tane cevap içeriyor. Type A olduğunu görüyorum DNS Query türünün. Cevapta ise sitenin IP adresi bulunuyor. Type A olması, sitenin domain adının Ip adresine çevrilmesi anlamına geliyor. (mackolik.com->195.244.61.20)
 
- 6- TCP SYN dosyaları bir önceki sorunun cevabındaki adrese gönderiliyor.
 

Böylece o adresin sitenin Ip adresi olduğunu anlamış olduk.

- 7- Evet her bir resim için ayrı bir sorgu yapma ihtimali bulunuyor. Resmin kaynağı ile şu anda bulunduğumuz site aynı olmayabilir. Aşağıdaki ekran görüntüsünde görüldüğü gibi :

use.fontawesome.com

fonts.gstatic.com

im.mackolik.com

cm.mackolik.com.edgesuite.net

fundingchoicesmessages.google.com

cdn.taboola.com

sitelerine ayrı ayrı sorgu gönderilmiş.

320 7.167973	192.168.1.1	192.168.1.9	DNS	183 Standard query response 0x95a HTTP use.fontawesome.com CNAME use.fontawesome.com.cdn.cloudflare.net A 104.21.47.132 A 172.07.142.1...
321 7.169093	192.168.1.1	192.168.1.9	DNS	204 Standard query response 0x795a HTTP use.fontawesome.com CNAME use.fontawesome.com.cdn.cloudflare.net HTTP
324 7.172421	192.168.1.1	192.168.1.9	DNS	184 Standard query response 0x7bff A im.mackolik.com CNAME im.mackolik.com.edgesuite.net CNAME a763.dscb.akamai.net A 212.252.126.1...
325 7.172656	192.168.1.1	192.168.1.9	DNS	226 Standard query response 0x6e1a HTTP im.mackolik.com CNAME im.mackolik.com.edgesuite.net CNAME a763.dscb.akamai.net SOA n0dscb...
344 7.190283	192.168.1.1	192.168.1.9	DNS	184 Standard query response 0x52bd A cm.mackolik.com CNAME cm.mackolik.com.edgesuite.net CNAME a662.dscb.akamai.net A 212.252.126.1...
974 7.366282	192.168.1.9	192.168.1.1	DNS	77 Standard query 0xe28d A fonts.gstatic.com
975 7.366411	192.168.1.9	192.168.1.1	DNS	77 Standard query 0x9e9d HTTP fonts.gstatic.com
976 7.368076	192.168.1.1	192.168.1.9	DNS	93 Standard query response 0xe28d A fonts.gstatic.com A 142.251.148.3
985 7.380725	192.168.1.9	192.168.1.1	DNS	75 Standard query 0xaa7 A hm.mackolik.com
986 7.380887	192.168.1.9	192.168.1.1	DNS	75 Standard query 0x66d5 HTTP hm.mackolik.com
988 7.381627	192.168.1.1	192.168.1.9	DNS	137 Standard query response 0x9e9d HTTP fonts.gstatic.com SOA ns1.google.com
989 7.381627	192.168.1.1	192.168.1.9	DNS	137 Standard query response 0x9e9d HTTP fonts.gstatic.com SOA ns1.google.com
1043 7.394963	192.168.1.1	192.168.1.9	DNS	184 Standard query response 0xaa7 A hm.mackolik.com CNAME hm.mackolik.com.edgesuite.net CNAME a527.dscb.akamai.net A 212.252.126.1...
1054 7.399132	192.168.1.1	192.168.1.9	DNS	226 Standard query response 0x66d5 HTTP hm.mackolik.com CNAME hm.mackolik.com.edgesuite.net CNAME a527.dscb.akamai.net SOA n0dscb...
1371 7.546556	192.168.1.9	192.168.1.1	DNS	84 Standard query 0xa5c8 A sb.scorecardresearch.com
1372 7.546678	192.168.1.9	192.168.1.1	DNS	84 Standard query 0xb248 HTTP sb.scorecardresearch.com
1415 7.565463	192.168.1.1	192.168.1.9	DNS	148 Standard query response 0xa5c8 A sb.scorecardresearch.com A 18.244.18.27 A 18.244.18.38 A 18.244.18.32 A 18.244.18.122
1425 7.565463	192.168.1.1	192.168.1.9	DNS	168 Standard query response 0xb248 HTTP sb.scorecardresearch.com SOA ns-905.amsdns-49.net
1432 7.565463	192.168.1.1	192.168.1.9	DNS	168 Standard query response 0xb248 HTTP sb.scorecardresearch.com SOA ns-905.amsdns-49.net
1612 7.755956	192.168.1.9	192.168.1.1	DNS	93 Standard query 0xf9b94 A fundingchoicesmessages.google.com
1613 7.756222	192.168.1.9	192.168.1.1	DNS	93 Standard query 0x7635 HTTP fundingchoicesmessages.google.com
1614 7.757048	192.168.1.9	192.168.1.1	DNS	75 Standard query 0x6261 A cdn.taboola.com

- 8- Sorgu benim yerel DNS adresime gönderilmiş.

388 6.751712	192.168.1.9	192.168.1.1	DNS	80 Standard query 0x0003 AAAA http://www.nmsu.edu/
--------------	-------------	-------------	-----	--

- 9- Son cevap iklim ekran görüntüsünde böyle görünüyor.

53 6.924730	192.168.1.9	192.168.1.1	DNS	80 Standard query 0x0004 A http://www.nmsu.edu/
54 8.900155	192.168.1.1	192.168.1.9	DNS	96 Standard query response 0x0002 A http://www.nmsu.edu/ A 192.168.1.1
55 8.937606	192.168.1.9	192.168.1.1	DNS	80 Standard query 0x0005 AAAA http://www.nmsu.edu/
60 12.899545	192.168.1.1	192.168.1.9	DNS	96 Standard query response 0x0004 A http://www.nmsu.edu/ A 192.168.1.1

Yine önceki sorularda karşıma çıktığı gibi A tipi bir sorgu var, domain adı www.nmsu.edu olan sitenin ipv4 adresini istiyor. Herhangi bir cevap yok ama cevap bekliyor diyebiliriz.

10- Cevap olarak domain adını verdiğimiz sitenin IPv4 adresini içeren bir response görünüyor. Yine Type A. Sadece 1 cevap var.

```

  Domain Name System (response)
    Transaction ID: 0x0004
    > Flags: 0x8580 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  Queries
    > http://www.nmsu.edu/: type A, class IN
  Answers
    > http://www.nmsu.edu/: type A, class IN, addr 192.168.1.1
\[Request In: 53\]
[Time: 5.974815000 seconds]
```

11- Yine bana ait olan yerel DNS adresine gönderilmiş.

Source	Destination
192.168.1.9	192.168.1.1

12- Bu sefer sorgu tipi olarak NS görünüyor. Cevap içermiyor, cevap bekliyor. Hangi yetkili sunucular tarafından yönetildiğini öğrenmek istiyoruz.

```

  Domain Name System (query)
    Transaction ID: 0x0002
    > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  Queries
    > nmsu.edu: type NS, class IN
\[Response In: 415\]
```

13- Cevap yerel DNS adresimden gelmiş.

192.168.1.1	192.168.1.9	DNS	138 Standard query response 0x0002 NS nmsu.edu NS dns1.nmsu.edu NS dns2.nmsu.edu A 128.123.3.3 A 128.123.2.2
-------------	-------------	-----	--

Cevap olarak tüm DNS adreslerimi emin değilim fakat yetkili olan bazı adresler verilmiş.

```
✓ nmsu.edu: type NS, class IN
✓ Answers
  > nmsu.edu: type NS, class IN, ns dns1.nmsu.edu
  > nmsu.edu: type NS, class IN, ns dns2.nmsu.edu
✓ Additional records
  > dns1.nmsu.edu: type A, class IN, addr 128.123.3.3
  > dns2.nmsu.edu: type A, class IN, addr 128.123.2.2
\[Request In: 362\]
```

14- Bu sefer hedef olarak 8.8.8.8 adresine gönderilmiş. Bu benim yerel sunucum değil Google'ın kullandığı dns adresidir.

```
192.168.1.9 8.8.8.8
```

15- AAAA tipi bir DNS sorgusudur. IPv6 formatında bir ip adresi cevabı beklemektedir yani cevap içermiyor şu anda.

```
✓ Domain Name System (query)
  Transaction ID: 0x0003
  > Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  ✓ Queries
    > nmsu.edu: type AAAA, class IN
    \[Response In: 115\]
```

16- Sadece 1 adet yanıt bulunuyor. Bu görüntü bana nmsu.edu sitesinin bir IPv6 adresine sahip olmadığını gösteriyor. SOA tipindeki cevap yetkili dns sunucusunu

gösteriyor.

- ✓ Domain Name System (response)
 - Transaction ID: 0x0003
 - › Flags: 0x8180 Standard query response, No error
 - Questions: 1
 - Answer RRs: 0
 - Authority RRs: 1
 - Additional RRs: 0
 - ✓ Queries
 - › nmsu.edu: type AAAA, class IN
 - ✓ Authoritative nameservers
 - › nmsu.edu: type SOA, class IN, mname dns1.nmsu.edu
- [\[Request In: 108\]](#)
[Time: 0.200176000 seconds]
-