

## Dig Nedir ? Nasıl Kullanılır?

Dig, herhangi alan adı için bir dizi dns sorgusu yapılabilmesini sağlayan kullanışlı bir network yazılımıdır. Dig'i işlevleri itibari ile windows sistemlerdeki nslookup'a benzetebilirsiniz.Linux/Unix sistemler de, default olarak network toolari ile beraber sistemde kurulu olarak bulunabildiği gibi, Bind-utils paketi ile de sisteme harici olarak yüklenebilmektedir.Şimdi client dns'imiz üzerinden youtube.com adresinin A,MX,SPF(TXT),NS,SOA.PTR recordlarını sorgulayacağız.Bu işlemleri [google'nin public dns serverlarını](#) kullanarak yapmak durumundayız çünkü telekom'un dns serverları Youtube'nin real IP'lerini dönmemektedir. (Sebebini herkes biliyor.)Client dns sunucum, youtube.com'un IP adresini > Turktelekom'un dns serverlarına soruyor

```
root@localroot:/home/ugur# dig A youtube.com +short +answer  
88.255.41.21
```

88.255.41 subneti tabiki youtube.com'a ait değil.

[http://www.db.ripe.net/whois?form\\_type=simple&full\\_query\\_string=&searchtext=88.255.41.21&submit.x=13&submit.y=6&submit.z=1](http://www.db.ripe.net/whois?form_type=simple&full_query_string=&searchtext=88.255.41.21&submit.x=13&submit.y=6&submit.z=1)

```
inetnum: 88.224.0.0 - 88.255.255.255  
netname: TR-TELEKOM-20051027  
descr: PROVIDER Local Registry  
descr: Turk Telekom  
country: TR  
org: ORG-TT3-RIPE  
admin-c: TTBA1-RIPE  
tech-c: TTBA1-RIPE
```

Bu sebeple resolv.conf isimli dosyama google'nin public ettiği dns adreslerini giriyorum.

```
/etc/resolv.conf
```

```
; generated by /sbin/dhclient-script  
search localdomain  
#nameserver 10.0.0.1  
nameserver 8.8.8.8  
nameserver 8.8.4.4
```

Artık Dig ile youtube.com üzerinde çalışmaya başlayabiliriz.

```
[root@labs ~]# dig  
;<<>> DiG 9.3.6-P1-RedHat-9.3.6-4.P1.el5_4.1 <<>>  
;; global options: printcmd  
;; Got answer:
```

```
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21992
;; flags: qr rd ra; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;.          IN  NS
;; ANSWER SECTION: (THERE ARE 13 ROOT DNS SERVERS IN WORLD)
. 5 IN NS a.root-servers.net.
. 5 IN NS b.root-servers.net.
. 5 IN NS c.root-servers.net.
. 5 IN NS d.root-servers.net.
. 5 IN NS e.root-servers.net.
. 5 IN NS f.root-servers.net.
. 5 IN NS g.root-servers.net.
. 5 IN NS h.root-servers.net.
. 5 IN NS i.root-servers.net.
. 5 IN NS j.root-servers.net.
. 5 IN NS k.root-servers.net.
. 5 IN NS l.root-servers.net.
. 5 IN NS m.root-servers.net.
```

Eğer request'lerimizin sonuçlarını istatistikleri ile görmek istiyorsak (MX,NS,SOA ve TXT kayıtları için)

dig A siteismi.com şeklinde bir komut çalıştırabiliriz. Dig, her ayrı request için ayrıntılı bir istatistik veriyor. (Bakınız A kaydı için yapılan request)

```
[root@labs ~]# dig A youtube.com
```

```
; <<>> DiG 9.3.6-P1-RedHat-9.3.6-4.P1.el5_4.1 <<>> A youtube.com
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43647
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL:
;; QUESTION SECTION:
;youtube.com.          IN  A
;; ANSWER SECTION:
youtube.com.          300 IN  A   74.125.127.100
youtube.com.          300 IN  A   74.125.45.100
youtube.com.          300 IN  A   74.125.67.100

;; Query time: 67 msec
;; SERVER: 8.8.4.4#53(8.8.4.4)
;; WHEN: Sat Mar 20 03:02:05 2010
;; MSG SIZE rcvd: 77
```

Dönen requestleri sadeleştirmek için aşağıdaki parametleri sorgularımıza dahil edebiliriz.

```
+noall
+short
+nostats
```

```
[root@labs ~]# dig A youtube.com +noall +short +nostats
```

```
74.125.127.100
74.125.45.100
74.125.67.100
```

```
[root@labs ~]# dig MX youtube.com +noall +short +nostats +answer
```

```
10 sjl-mbox1.sjl.youtube.com.
```

```
[root@labs ~]# dig NS youtube.com +noall +short +nostats +answer
```

```
ns1.google.com.  
ns3.google.com.  
ns2.google.com.  
ns4.google.com.
```

```
[root@labs ~]# dig SOA youtube.com +noall +short +nostats +answer
```

```
sjl-ins1.sjl.youtube.com. dns-admin.youtube.com. 1410044 10800 3600 604800 600
```

```
[root@labs ~]# dig TXT youtube.com +noall +short +nostats +answer
```

```
"v=spf1 ip4:208.117.224.0/19 ip4:208.65.152.0/22 ip4:64.15.112.0/20 include:google.com  
mx ~all"
```

```
[root@labs ~]# dig any youtube.com +noall +short +answer
```

```
ns2.google.com.  
ns1.google.com.  
ns4.google.com.  
74.125.45.100  
74.125.67.100  
ns3.google.com.  
10 sjl-mbox1.sjl.youtube.com.  
"v=spf1 ip4:208.117.224.0/19 ip4:208.65.152.0/22 ip4:64.15.112.0/20 include:google.com  
mx ~all"  
74.125.127.100  
sjl-ins1.sjl.youtube.com. dns-admin.youtube.com. 1410051 10800 3600 604800 600
```

Şimdi direk youtube.com'un host edildiği dns serverlara A kaydı requesti yapacağız. Amacımız youtube'nin A kayıtlarını görmek.

```
[root@labs ~]# dig @ns1.google.com www.youtube.com +noall +short +answer +nostats
```

```
youtube-ui.l.google.com.  
209.85.229.101  
209.85.229.102  
209.85.229.100
```

```
[root@labs ~]# dig @ns2.google.com A youtube.com +noall +short +answer
```

```
74.125.45.100  
74.125.67.100  
74.125.127.100
```

```
[root@labs ~]# dig @ns2.google.com youtube.com +noall +short +answer
```

```
74.125.45.100  
74.125.67.100  
74.125.127.100
```

Sadece 2 name server dan 6 adet IP adresi elde ettik.Bu durumda bir kac dakika icerisinde yukaridaki IP adreslerine istinaden youtube'nin, subnet araligini tespit edip yuzlerce IP adresi de elde ederiz(Subnets: 74.125 / 209.85) daha sonra gene dig ile PTR sorgusu yapip IP adreslerine karsilik gelen alan adi isimlerini de bulabiliriz.

```
[root@labs ~]# dig -x 74.125.45.100 +short +answer
```

Umarım, dig'in gizemli ve işlevsel gücünü anlatabilmişimdir.

Konuyla bağlantılı olan aşağıdaki referans linkini ayrıca zaman ayırıp okuyabilirsiniz.

<http://code.google.com/speed/public-dns/docs/security.html>

Yazar: Uğur Engin

<http://www.ugurengin.com>

İletişim: mail[at]ugurengin[dat]com