

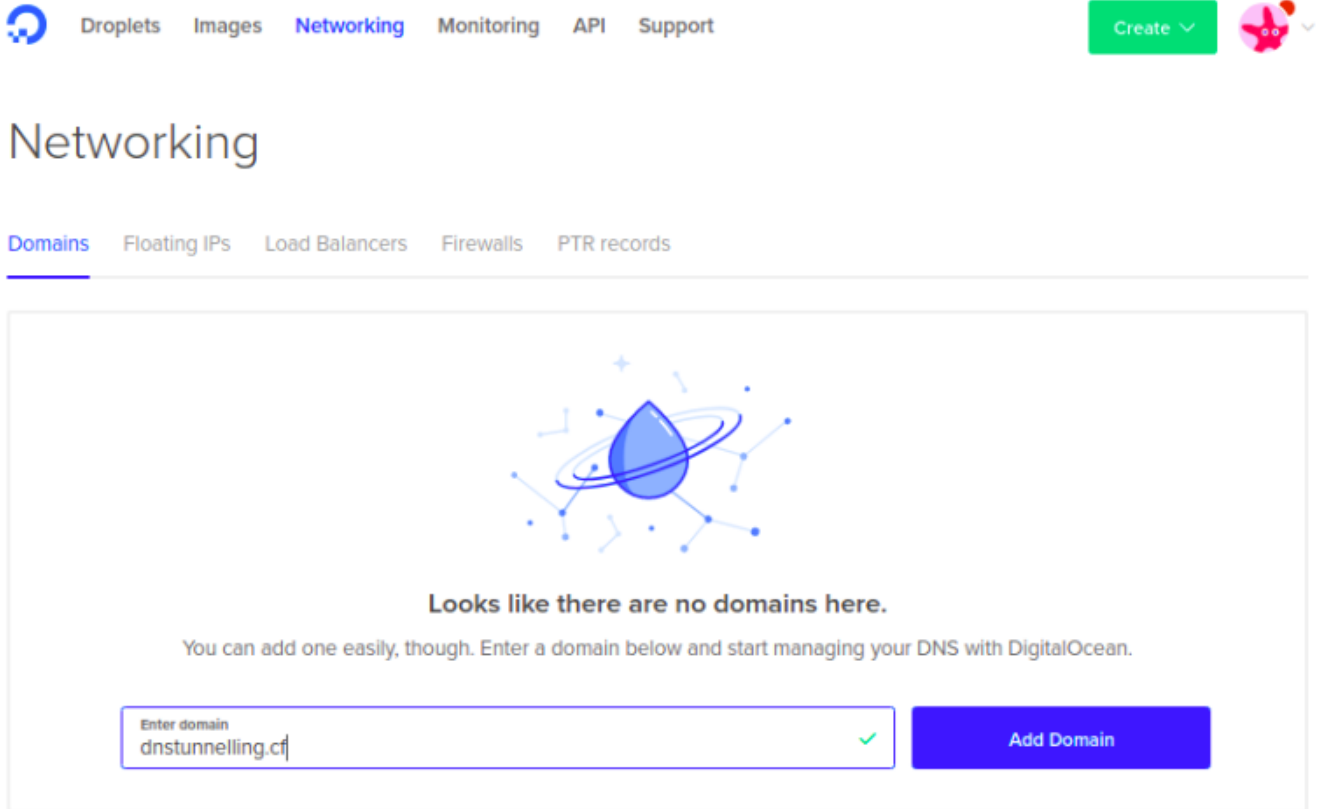
# Iodine Aracı Kullanarak Dns Tünelleme

Iodine aracı kullanarak dns tünelleme nasıl yapılır inceleyelim.

Bize kontrolümüzde olan bir sunucu lazım bunun için ben digitalocean da oluşturduğum sunucuyu kullanacağım. Ve bu sunucuya bağlı bir domain adına ihtiyacımız var. Domain adını ücretsiz olarak edinebileceğiniz bir çok seçenek mevcut. Alan adını alırken dns ayarlarında “use your own DNS” sekmesinden nameserver kısmına digitalocean nameserver adlarını yazıyoruz ve devam ettikten sonra onaylıyoruz.



Digitalocean hesabımızda networking sekmesinden domains sekmesine tıklıyoruz. Oraya aldığımız domain adını ekliyoruz.



Sonrasında hostname verip sunucu ip adresini giriyoruz.

## Create new record

A AAAA CNAME MX TXT NS SRV

Use @ to create the record at the root of the domain or enter a hostname to create it elsewhere. A records are for IPv4 addresses only and tell a request where your domain should direct to.

HOSTNAME	WILL DIRECT TO	TTL (SECONDS)	
<input type="text" value="Enter @ or hostname"/> test	<input type="text" value="Select resource or enter custom IP"/> 37.139.26.240	<input type="text" value="Enter TTL"/> 3600	<button>Create Record</button>

Gerekli olan sunucu dns ayarlaması yapıldıktan sonra aldığımız test.dnstunnelling.cf adresine ping atıp bakabiliriz.

```
root@night:/home/zehra# ping test.dnstunnelling.cf
PING test.dnstunnelling.cf (37.139.26.240) 56(84) bytes of data.
64 bytes from 37.139.26.240: icmp_seq=1 ttl=51 time=49.9 ms
64 bytes from 37.139.26.240: icmp_seq=2 ttl=51 time=49.1 ms
64 bytes from 37.139.26.240: icmp_seq=3 ttl=51 time=49.6 ms
64 bytes from 37.139.26.240: icmp_seq=4 ttl=51 time=49.0 ms
64 bytes from 37.139.26.240: icmp_seq=5 ttl=51 time=49.0 ms
64 bytes from 37.139.26.240: icmp_seq=6 ttl=51 time=49.1 ms
64 bytes from 37.139.26.240: icmp_seq=7 ttl=51 time=49.2 ms
64 bytes from 37.139.26.240: icmp_seq=8 ttl=51 time=52.7 ms
64 bytes from 37.139.26.240: icmp_seq=9 ttl=51 time=49.2 ms
64 bytes from 37.139.26.240: icmp_seq=10 ttl=51 time=49.2 ms
64 bytes from 37.139.26.240: icmp_seq=11 ttl=51 time=49.2 ms
```

Gelelim dns tünellemede bize eşlik edecek olan iodine aracına. Iodine aracını hem server tarafına hem de client tarafına kuruyoruz. Benim her ikisi de ubuntu işletim sistemi olduğu için direkt aşağıdaki komut ile iki tarafın da kurulumunu gerçekleştirdim.

```
sudo apt-get install iodine
```

Şimdi **server** tarafında aşağıdaki komutu yazalım.

```
iodined -f -P password 10.0.0.1 test.dnstunnelling.cf
```

Burada yazan  oluşturulan bağlantıya atanacak olan parola. Client tarafında bağlanılacağı zaman bu parola kullanılır.

10.0.0.1 yerine ise sunucunun dns0 bacağına atamak istediğiniz ip verilir.

test.dnstunnelling.cf yerinede sunucuya eklenen domain adı gelir.

```
root@moonlight:~# iodined -fP pass 10.0.0.1 test.dnstunnelling.cf
Opened dns0
Setting IP of dns0 to 10.0.0.1
Setting MTU of dns0 to 1130
Opened IPv4 UDP socket
Listening to dns for domain test.dnstunnelling.cf
```

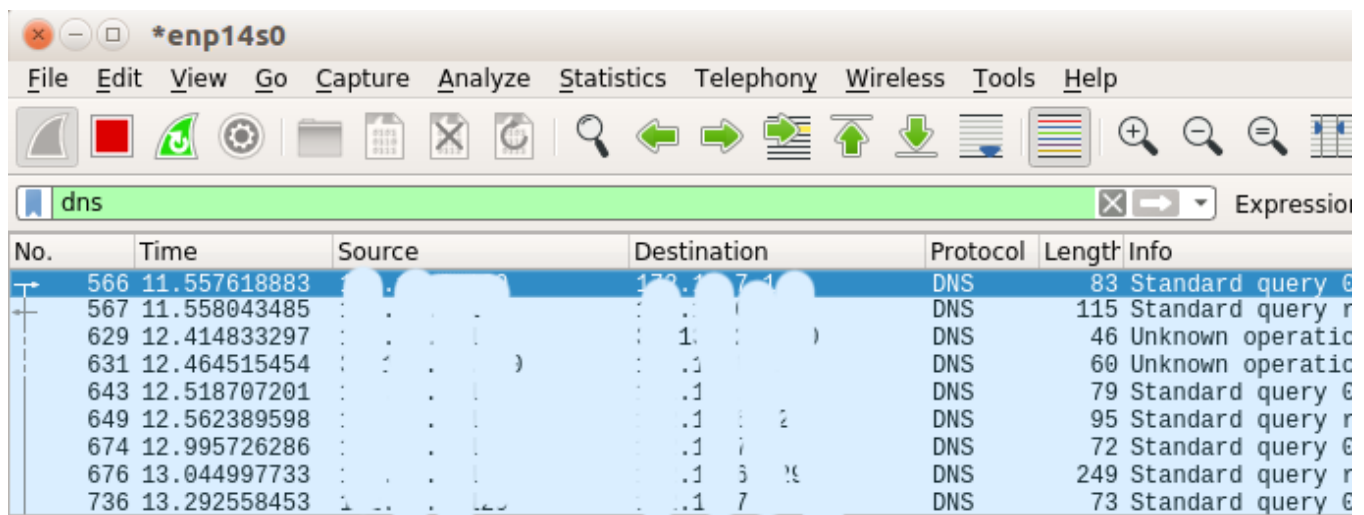
**Client** tarafında ise

```
iodine -fP password 37.139.26.240 test.dnstunnelling.cf
```

komutu çalıştırılır. (37.139.26.240→server ip)

```
root@night:/home/zehra# iodine -f -P pass 37.139.26.240 test.dnstunnelling.cf
Opened dns0
Opened IPv4 UDP socket
Sending DNS queries for test.dnstunnelling.cf to 37.139.26.240
Autodetecting DNS query type (use -T to override).
Using DNS type NULL queries
Version ok, both using protocol v 0x00000502. You are user #0
Setting IP of dns0 to 10.0.0.2
Setting MTU of dns0 to 1130
Server tunnel IP is 10.0.0.1
Testing raw UDP data to the server (skip with -r)
Server is at 37.139.26.240, trying raw login: OK
Sending raw traffic directly to 37.139.26.240
Connection setup complete, transmitting data.
```

Dns tünel bağlantısı tamamlandı. İnternete bağlı olduğunuz ağ arayüzünü wireshark ile dinlemeye aldığınızda dns protokollü paketleri görebirsiniz.



No.	Time	Source	Destination	Protocol	Length	Info
566	11.557618883	10.0.0.1	10.0.0.2	DNS	83	Standard query 0
567	11.558043485	10.0.0.2	10.0.0.1	DNS	115	Standard query r
629	12.414833297	10.0.0.1	10.0.0.2	DNS	46	Unknown operatic
631	12.464515454	10.0.0.2	10.0.0.1	DNS	60	Unknown operatic
643	12.518707201	10.0.0.1	10.0.0.2	DNS	79	Standard query 0
649	12.562389598	10.0.0.2	10.0.0.1	DNS	95	Standard query r
674	12.995726286	10.0.0.1	10.0.0.2	DNS	72	Standard query 0
676	13.044997733	10.0.0.2	10.0.0.1	DNS	249	Standard query r
736	13.292558453	10.0.0.1	10.0.0.2	DNS	73	Standard query 0

Aynı zamanda iki tarafta da ping atıp, dns0 arayüzünü dinleyelim.

```
root@moonlight:~# ping 10.0.0.2
PING 10.0.0.2 (10.0.0.2) 56(84) bytes of data.
64 bytes from 10.0.0.2: icmp_seq=1 ttl=64 time=51.0 ms
64 bytes from 10.0.0.2: icmp_seq=2 ttl=64 time=49.5 ms
64 bytes from 10.0.0.2: icmp_seq=3 ttl=64 time=50.0 ms
64 bytes from 10.0.0.2: icmp_seq=4 ttl=64 time=49.7 ms
64 bytes from 10.0.0.2: icmp_seq=5 ttl=64 time=49.7 ms
```

