Yardımcı Ağ Komutları

Komut Satırı Nedir?

Komut satırı (diğer adıyla komut satırı arayüzü), bir bilgisayar kullanıcısının, belirli metinleri (komutları) girerek, bilgisayarla iletişime geçmesini sağlar.

Komut satırı arayüzleri; konsol, kabuk, terminal veya uçbirim diye de adlandırılır.

Neden Komut Satırı Kullanıyoruz?

- Grafik arayüzde yapılan işlemleri konsolda daha hızlı yapabiliyoruz.
- Bazı durumlarda grafik arayüzün sunmadığı imkanlara erişebiliyoruz.
- Kullandığımız sistem grafik arayüz sunmayabilir. (Örneğin: Sunucular)

Komut Satırını Açma

- Windows 10 işletim sisteminde "Başlat" menüsü yanındaki arama yerine "cmd" yazarsanız "Komut İstemi" uygulamasına erişim sağlayabilirsiniz.
- Ubuntu işletim sisteminde ise masaüstü olarak Gnome kullanıyorsanız "Alt + F2" tuşlarına basıp gelen pencereye "gnome-terminal" yazarsanız konsola erişebilirsiniz.

Ağ ile İlgili Komutlar

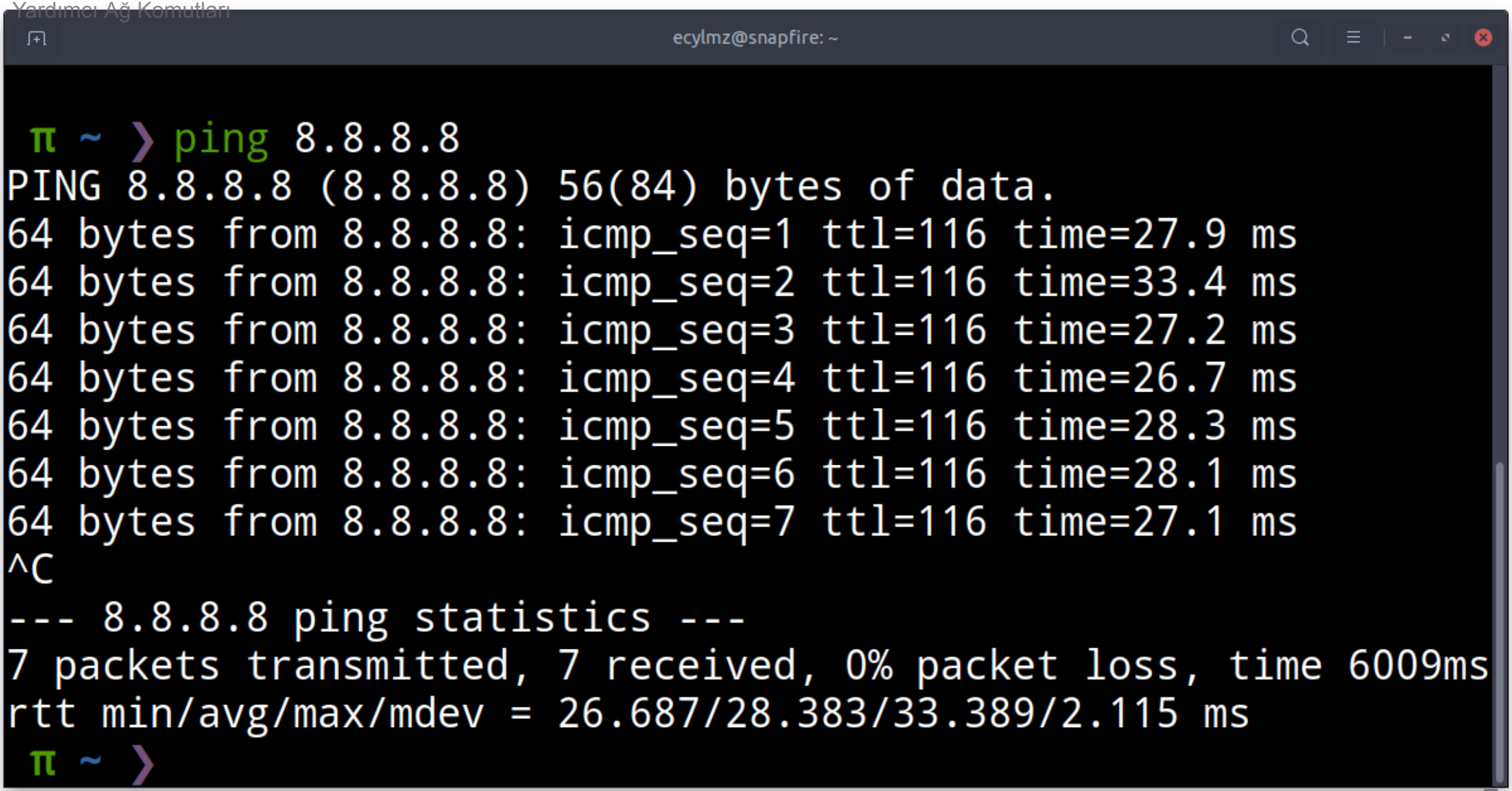
- ping
- ip, ipconfig
- nslookup, dig, host
- route
- arp
- tracert, traceroute, mtr
- netstat, ss
- wireshark, tcpdump

ping

Çalışma prensibi hedefe 32 baytlık bir ICMP paketi göndermek ve aynı paketin geri gelmesini beklemek üzerine kuruludur. Sunucu istemciye ne kadar uzak ise, bekleme süresi o kadar artmaktadır.

Kısaca 2 amaçla kullanılır;

- Bilgisayarın ulaşılabilir durumda olduğunu kontrol etmek
- Ağdaki gecikme süresini tespit etmek


ecylmz@snapfire: ~
π ~ ❯ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=116 time=27.9 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=116 time=33.4 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=116 time=27.2 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=116 time=26.7 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=116 time=28.3 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=116 time=28.1 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=116 time=27.1 ms
^C
--- 8.8.8.8 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6009ms
rtt min/avg/max/mdev = 26.687/28.383/33.389/2.115 ms
π ~ ❯

ip, ipconfig

Ubuntu işletim sistemindeki `ip` komutu, Windows işletim sistemindeki `ipconfig` komutu, bilgisayarınızın TCP/IP ağ yapılandırmasını görüntülemek ve düzenlemek için kullanılan komutlardır.

Komutlar hakkında detaylı bilgi almak için:

Windows'ta `ipconfig /?` Ubuntu'da `man ip` komutlarını kullanabilirsiniz.

ecylmz@snapfire: ~

```
π ~ ❯ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defa
ult qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s31f6: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq_codel stat
e DOWN group default qlen 1000
    link/ether [redacted] brd ff:ff:ff:ff:ff:ff
3: wlp2s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP g
roup default qlen 1000
    link/ether [redacted] brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.105/24 brd 192.168.1.255 scope global dynamic noprefixroute
 wlp2s0
       valid_lft 3320sec preferred_lft 3320sec
    inet6 [redacted] scope link noprefixroute
       valid_lft forever preferred_lft forever
4: lxcbr0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DO
```

nslookup, host, dig

Hem Ubuntu'da hem Windows'ta `nslookup` komutu istenilen alan adı için DNS sorguları yapmaya yarayan bir komut satırı aracıdır.

Ubuntu'da bu komuta alternatif olarak `host` ve `dig` komutları vardır.

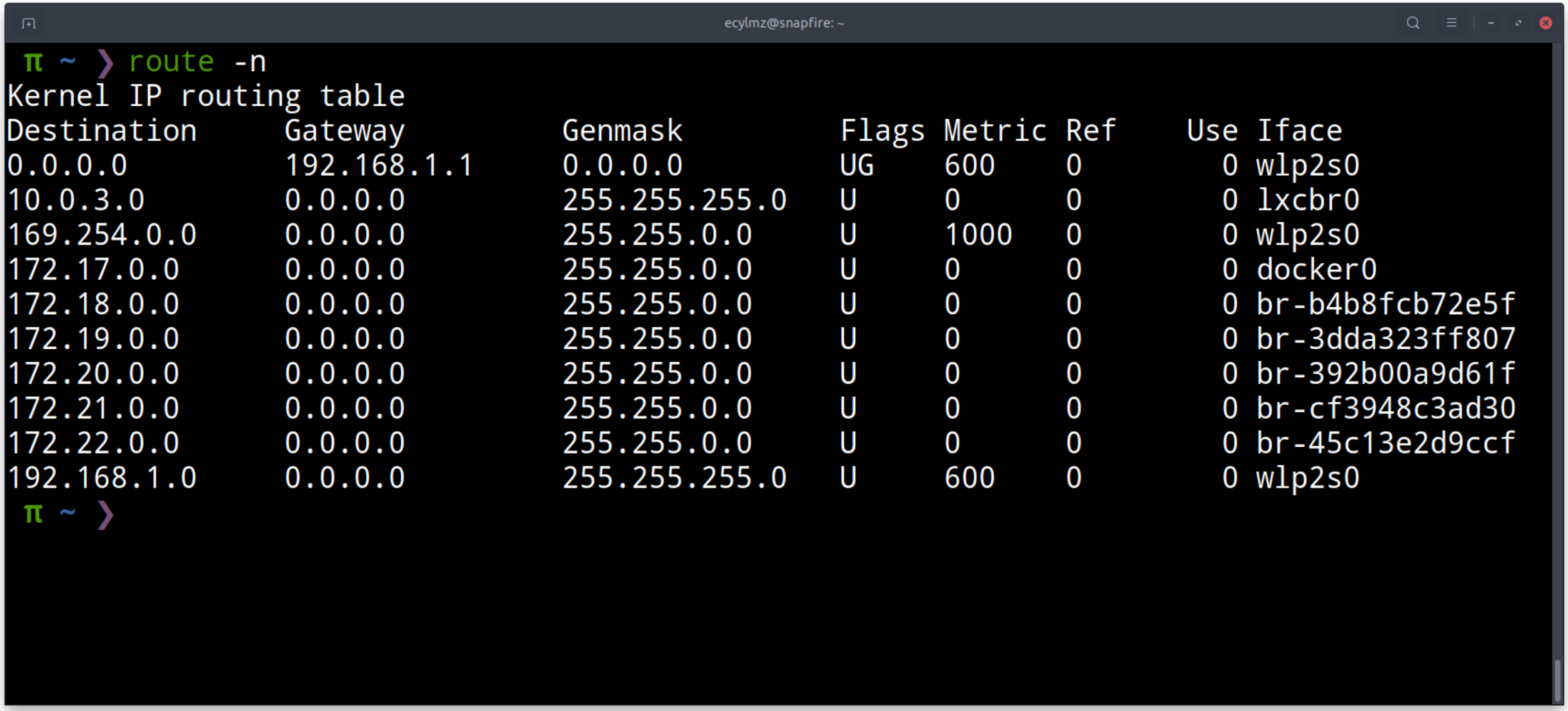
ecylmz@snapfire: ~

```
π ~ ❯ nslookup omu.edu.tr
unknown query class: IN
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   omu.edu.tr
Address: 193.140.28.8

π ~ ❯ host omu.edu.tr
omu.edu.tr has address 193.140.28.8
omu.edu.tr mail is handled by 5 mx.omu.edu.tr.
π ~ ❯
```

route

Yönlendirme Tablosu (Routing Table), yönlendiriciye (router) veya ağdaki bir bilgisayara bir paket geldiğinde, yönlendiricinin veya bilgisayarın o paketi nereye yönlendirmesi gerektiğine dair rotaları içeren tablodur.

Bilgisayardaki rotaları görüntülemek ve düzenlemek için `route` komutu kullanılır.


ecylmz@snapfire: ~
π ~ ❯ route -n
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
0.0.0.0 192.168.1.1 0.0.0.0 UG 600 0 0 wlp2s0
10.0.3.0 0.0.0.0 255.255.255.0 U 0 0 0 lxcbr0
169.254.0.0 0.0.0.0 255.255.0.0 U 1000 0 0 wlp2s0
172.17.0.0 0.0.0.0 255.255.0.0 U 0 0 0 docker0
172.18.0.0 0.0.0.0 255.255.0.0 U 0 0 0 br-b4b8fcb72e5f
172.19.0.0 0.0.0.0 255.255.0.0 U 0 0 0 br-3dda323ff807
172.20.0.0 0.0.0.0 255.255.0.0 U 0 0 0 br-392b00a9d61f
172.21.0.0 0.0.0.0 255.255.0.0 U 0 0 0 br-cf3948c3ad30
172.22.0.0 0.0.0.0 255.255.0.0 U 0 0 0 br-45c13e2d9ccf
192.168.1.0 0.0.0.0 255.255.255.0 U 600 0 0 wlp2s0
π ~ ❯

arp

Adres çözümleme protokolü(ARP) için yazılmış bir programdır. Bu program ağdaki cihazların IP adreslerinden MAC adreslerini bulmaya yarar.

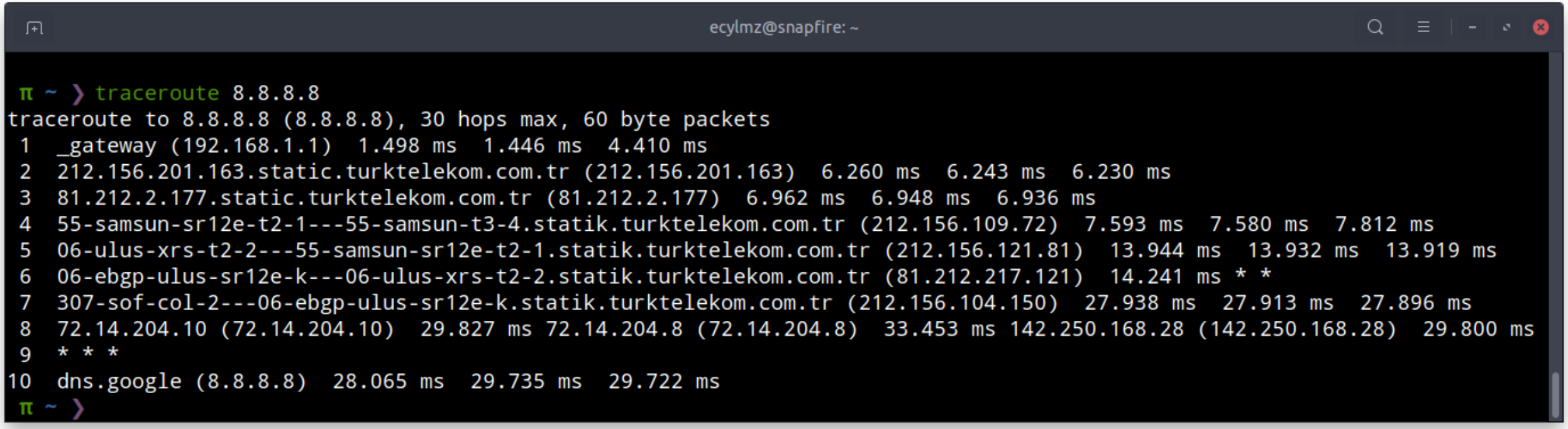
Komut İstemi

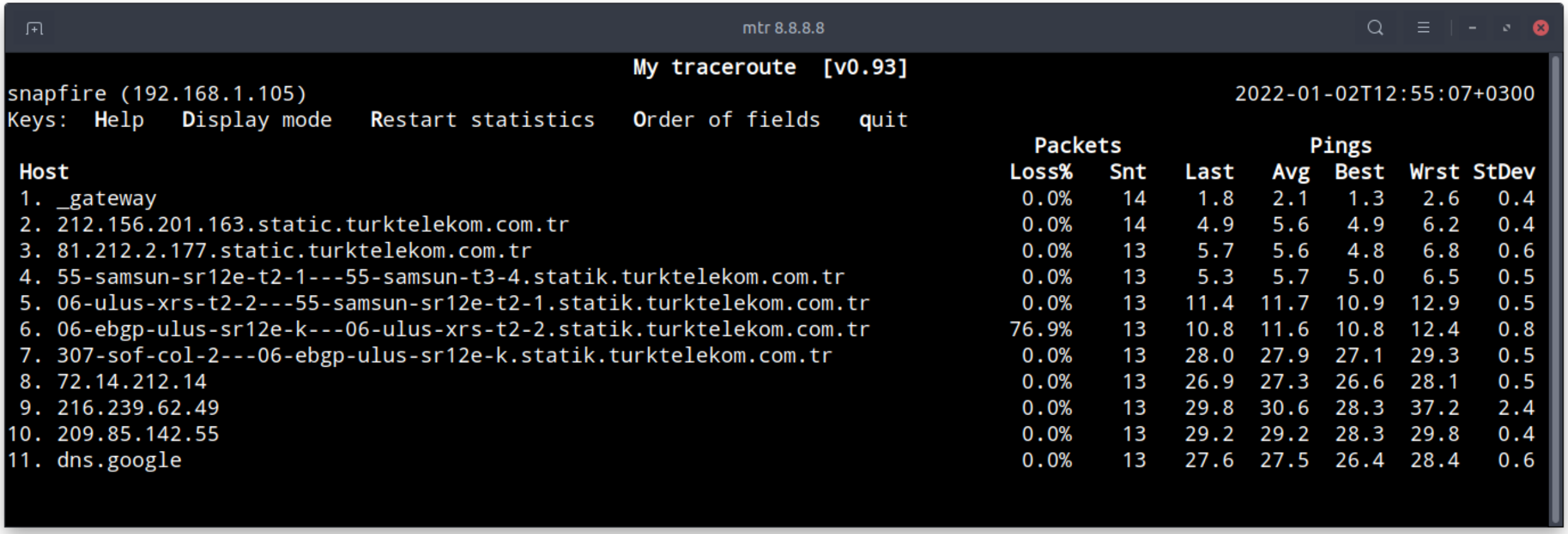
```
C:\Users\Emre Can Yılmaz>arp -a

Interface: 192.168.1.102 --- 0xf
  Internet Address      Physical Address      Type
  192.168.1.1           [redacted]            dynamic
  192.168.1.255                               static
  224.0.0.22                                  static
  224.0.0.251                                 static
  224.0.0.252                                 static
  239.255.255.250                             static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Users\Emre Can Yılmaz>
```

tracert, traceroute, mtr

Windows'ta `tracert` Ubuntu'da `traceroute` komutu, TCP/IP ağlarında kaynak bilgisayardan hedef bilgisayara giden paketlerin hangi rotayı takip ettiğinin anlaşılması ve bu rotalardan geçerken meydana gelen gecikmelerin görülebilmesini sağlayan bir ağ aracıdır.

Ubuntu'da bulunan `mtr` komutu ise `traceroute` ve `ping` komutlarının birleşimi şeklinde çalışır.


ecylmz@snapfire: ~
π ~ ❯ traceroute 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
1 _gateway (192.168.1.1) 1.498 ms 1.446 ms 4.410 ms
2 212.156.201.163.static.turktelekom.com.tr (212.156.201.163) 6.260 ms 6.243 ms 6.230 ms
3 81.212.2.177.static.turktelekom.com.tr (81.212.2.177) 6.962 ms 6.948 ms 6.936 ms
4 55-samsun-sr12e-t2-1---55-samsun-t3-4.statik.turktelekom.com.tr (212.156.109.72) 7.593 ms 7.580 ms 7.812 ms
5 06-ulus-xrs-t2-2---55-samsun-sr12e-t2-1.statik.turktelekom.com.tr (212.156.121.81) 13.944 ms 13.932 ms 13.919 ms
6 06-ebgp-ulus-sr12e-k---06-ulus-xrs-t2-2.statik.turktelekom.com.tr (81.212.217.121) 14.241 ms * *
7 307-sof-col-2---06-ebgp-ulus-sr12e-k.statik.turktelekom.com.tr (212.156.104.150) 27.938 ms 27.913 ms 27.896 ms
8 72.14.204.10 (72.14.204.10) 29.827 ms 72.14.204.8 (72.14.204.8) 33.453 ms 142.250.168.28 (142.250.168.28) 29.800 ms
9 * * *
10 dns.google (8.8.8.8) 28.065 ms 29.735 ms 29.722 ms
π ~ ❯


mtr 8.8.8.8
My traceroute [v0.93]
snapfire (192.168.1.105) 2022-01-02T12:55:07+0300
Keys: Help Display mode Restart statistics Order of fields quit
Packets Pings
Host Loss% Snt Last Avg Best Wrst StDev
1. _gateway 0.0% 14 1.8 2.1 1.3 2.6 0.4
2. 212.156.201.163.static.turktelekom.com.tr 0.0% 14 4.9 5.6 4.9 6.2 0.4
3. 81.212.2.177.static.turktelekom.com.tr 0.0% 13 5.7 5.6 4.8 6.8 0.6
4. 55-samsun-sr12e-t2-1---55-samsun-t3-4.statik.turktelekom.com.tr 0.0% 13 5.3 5.7 5.0 6.5 0.5
5. 06-ulus-xrs-t2-2---55-samsun-sr12e-t2-1.statik.turktelekom.com.tr 0.0% 13 11.4 11.7 10.9 12.9 0.5
6. 06-ebgp-ulus-sr12e-k---06-ulus-xrs-t2-2.statik.turktelekom.com.tr 76.9% 13 10.8 11.6 10.8 12.4 0.8
7. 307-sof-col-2---06-ebgp-ulus-sr12e-k.statik.turktelekom.com.tr 0.0% 13 28.0 27.9 27.1 29.3 0.5
8. 72.14.212.14 0.0% 13 26.9 27.3 26.6 28.1 0.5
9. 216.239.62.49 0.0% 13 29.8 30.6 28.3 37.2 2.4
10. 209.85.142.55 0.0% 13 29.2 29.2 28.3 29.8 0.4
11. dns.google 0.0% 13 27.6 27.5 26.4 28.4 0.6

netstat, ss

netstat (network statistics); ağ bağlantıları (hem gelen hem giden), yönlendirme tabloları ve ağ arayüzü istatistiklerini görüntüleyen bir komut satırı aracıdır.

netstat komutu ağdaki problemleri bulma ve ağ üzerindeki trafiğin miktarını belirlemek için kullanılır.

`ss` programı ise Ubuntu'da öntanımlı olarak `netstat` yerine kullanılmaya başlayan komut satırı aracıdır. İşlevsel olarak `netstat` ile benzerdir.

Örnek netstat kullanımları

- Sadece TCP ve UDP protokollerine ait istatistikleri görmek için:
  `netstat -sp tcp` veya `netstat -sp udp`
- Açık TCP bağlantılarını, durumlarını ve bağlantıları kullanan süreçleri görmek için:
  `netstat -antp`
- TCP 443. porta yapılan bağlantı sayısına ulaşmak için:
  `netstat -antp | grep ":443.*ESTABLISHED" | wc -l`

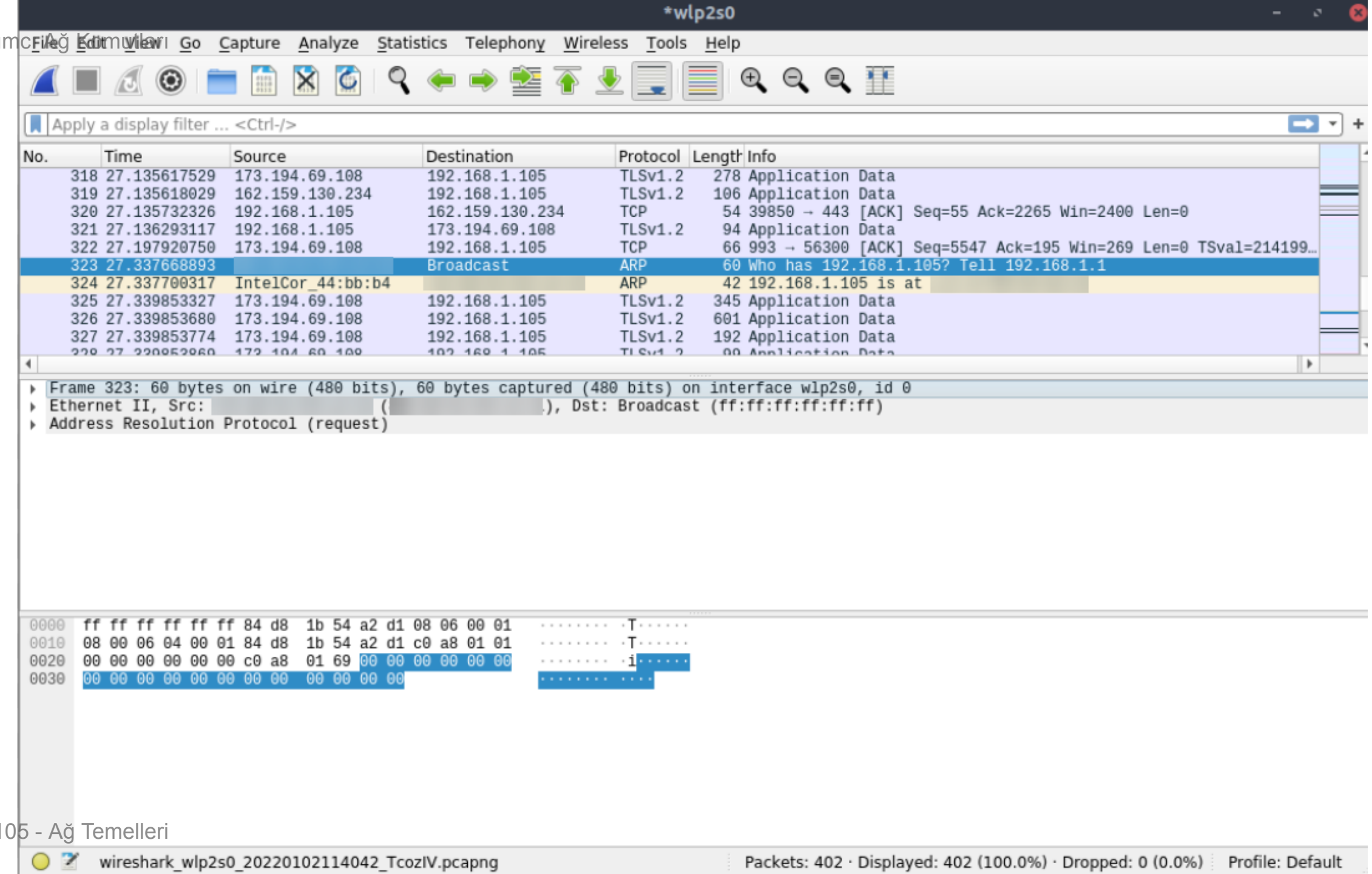
ecylmz@snapfire: ~

```
π ~ ❯ netstat -antp
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Aktif internet bağlantıları (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:631           0.0.0.0:*               DİNLE       -
tcp        0      0 0.0.0.0:17500           0.0.0.0:*               DİNLE       3026/dropbox
tcp        0      0 127.0.0.1:6463          0.0.0.0:*               DİNLE       3470/Discord --type
tcp        0      0 127.0.0.1:17600         0.0.0.0:*               DİNLE       3026/dropbox
tcp        0      0 127.0.0.1:17603         0.0.0.0:*               DİNLE       3026/dropbox
tcp        0      0 127.0.0.1:5939          0.0.0.0:*               DİNLE       -
tcp        0      0 10.0.3.1:53             0.0.0.0:*               DİNLE       -
tcp        0      0 127.0.0.53:53           0.0.0.0:*               DİNLE       -
tcp        0      1 192.168.1.105:38556     142.250.184.129:443     FIN_WAIT1    -
tcp        1      1 192.168.1.105:44502     142.250.184.129:443     LAST_ACK     -
tcp        1      1 192.168.1.105:48254     142.250.184.129:443     LAST_ACK     -
tcp        1      1 10.49.1.119:47850       142.250.186.33:443      LAST_ACK     -
tcp        1      1 192.168.1.105:35386     142.250.184.129:443     LAST_ACK     -
tcp        1      1 192.168.1.105:46048     142.250.184.129:443     LAST_ACK     -
tcp        1      1 10.49.1.119:60570       142.250.186.33:443      LAST_ACK     -
tcp        1      1 192.168.1.105:41246     142.250.184.129:443     LAST_ACK     -
tcp        1      1 192.168.1.105:43830     142.250.184.129:443     LAST_ACK     -
tcp        1      1 192.168.1.105:40166     172.217.17.193:443      LAST_ACK     -
tcp        1      1 192.168.1.105:42894     142.250.184.129:443     LAST_ACK     -
```

tcpdump, wireshark

tcpdump, komut satırından çalışan genel bir paket analiz aracıdır, *bilgisayara gelen veri paketlerini kaydetmeye, incelemeye, filtrelemeye* yardımcı bir sistemdir.

Kullanıcıya bağlı bulunduğu bir ağ üzerinden iletilen veya alınan TCP/IP paketlerini veya diğer paketleri yakalama ve gözlemleme olanağı sunar.


*wlp2s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
318 27.135617529 173.194.69.108 192.168.1.105 TLSv1.2 278 Application Data
319 27.135618029 162.159.130.234 192.168.1.105 TLSv1.2 106 Application Data
320 27.135732326 192.168.1.105 162.159.130.234 TCP 54 39850 → 443 [ACK] Seq=55 Ack=2265 Win=2400 Len=0
321 27.136293117 192.168.1.105 173.194.69.108 TLSv1.2 94 Application Data
322 27.197920750 173.194.69.108 192.168.1.105 TCP 66 993 → 56300 [ACK] Seq=5547 Ack=195 Win=269 Len=0 TSval=214199…
323 27.337668893 Broadcast ARP 60 Who has 192.168.1.105? Tell 192.168.1.1
324 27.337700317 IntelCor_44:bb:b4 ARP 42 192.168.1.105 is at
325 27.339853327 173.194.69.108 192.168.1.105 TLSv1.2 345 Application Data
326 27.339853680 173.194.69.108 192.168.1.105 TLSv1.2 601 Application Data
327 27.339853774 173.194.69.108 192.168.1.105 TLSv1.2 192 Application Data
Frame 323: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface wlp2s0, id 0
Ethernet II, Src:
), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)
0000 ff ff ff ff ff ff 84 d8 1b 54 a2 d1 08 06 00 01
0010 08 00 06 04 00 01 84 d8 1b 54 a2 d1 c0 a8 01 01
0020 00 00 00 00 00 00 c0 a8 01 69 00 00 00 00 00 00
0030 00 00 00 00 00 00 00 00 00 00 00 00
wireshark_wlp2s0_20220102114042_TcozIV.pcapng
Packets: 402 · Displayed: 402 (100.0%) · Dropped: 0 (0.0%)
Profile: Default

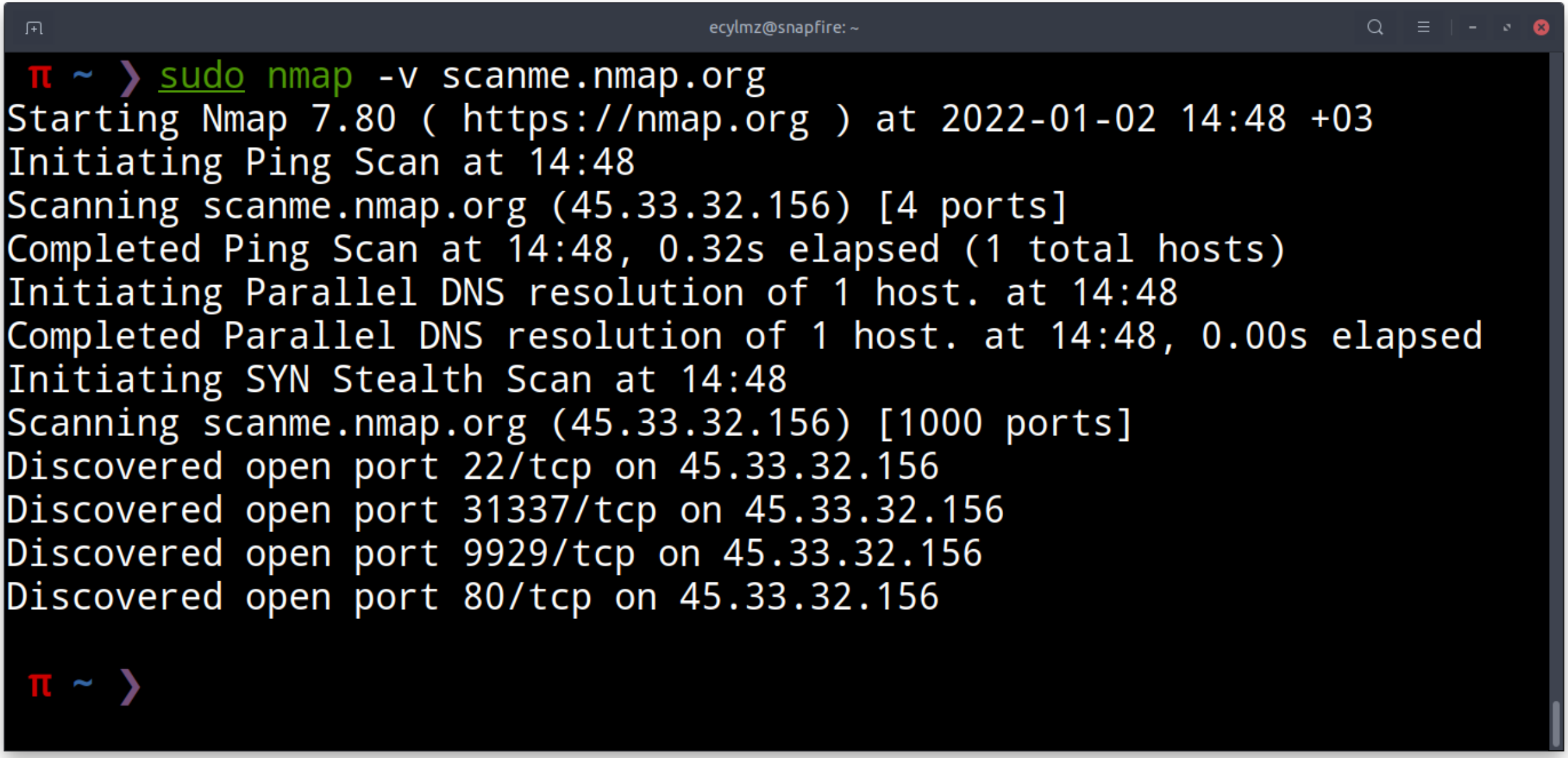
Nmap

Nmap, bilgisayar ağları uzmanı Gordon Lyon (Fyodor) tarafından geliştirilmiş bir **güvenlik tarayıcısıdır**. Taranan ağın haritasını çıkarabilir ve ağ makinalarında çalışan servislerin durumlarını, işletim sistemlerini, portların durumlarını gözlemleyebilir.

Nmap kullanarak ağa bağlı herhangi bir bilgisayarın işletim sistemi, çalışan fiziksel aygıt tipleri, çalışma süresi, yazılımların hangi servisleri kullandığı, yazılımların sürüm numaraları, bilgisayarın güvenlik duvarına sahip olup olmadığı, ağ kartının üreticisinin adı gibi bilgiler öğrenilebilmektedir.

Örnek: Ağdaki tüm istemcileri bulmak için:

```
sudo nmap -sP 192.168.1.0/24
```


ecylmz@snapfire: ~
π ~ ❯ sudo nmap -v scanme.nmap.org
Starting Nmap 7.80 (https://nmap.org) at 2022-01-02 14:48 +03
Initiating Ping Scan at 14:48
Scanning scanme.nmap.org (45.33.32.156) [4 ports]
Completed Ping Scan at 14:48, 0.32s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:48
Completed Parallel DNS resolution of 1 host. at 14:48, 0.00s elapsed
Initiating SYN Stealth Scan at 14:48
Scanning scanme.nmap.org (45.33.32.156) [1000 ports]
Discovered open port 22/tcp on 45.33.32.156
Discovered open port 31337/tcp on 45.33.32.156
Discovered open port 9929/tcp on 45.33.32.156
Discovered open port 80/tcp on 45.33.32.156
π ~ ❯