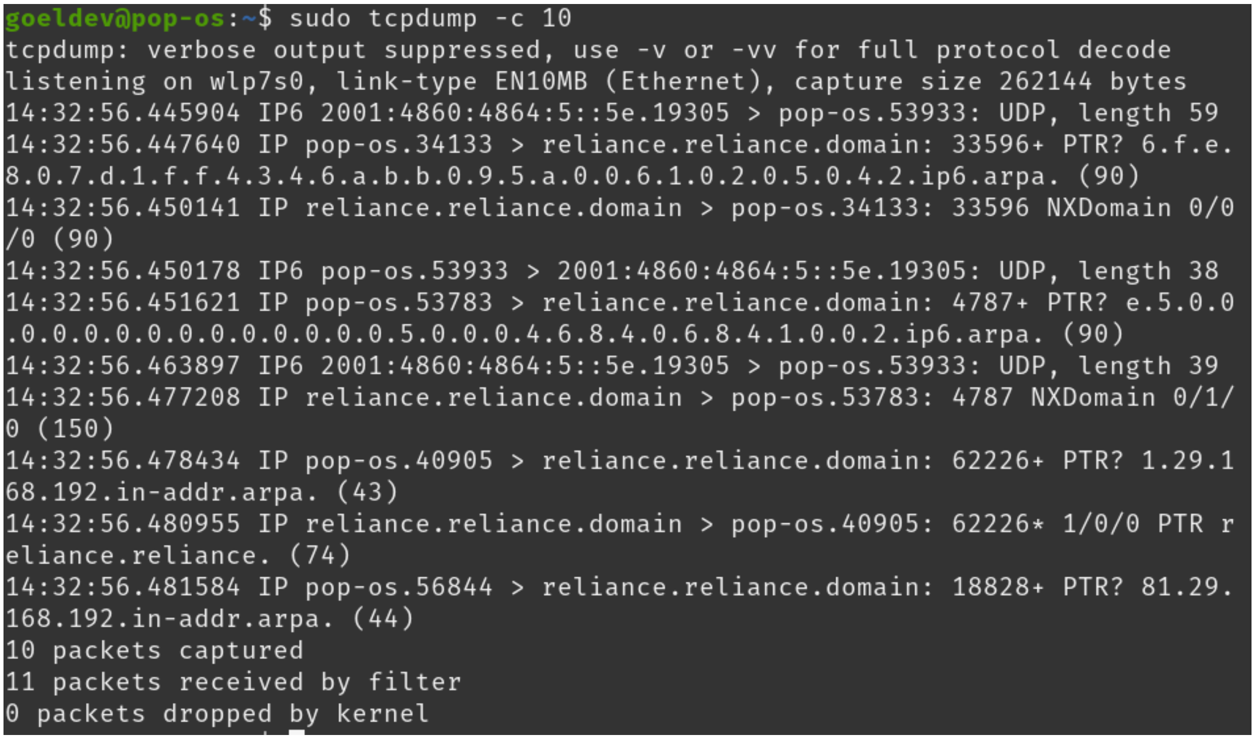
LAB 1 - Network Commands

NAME - DEV GOEL
ID - 2019A7PS0236G

- **tcpdump**

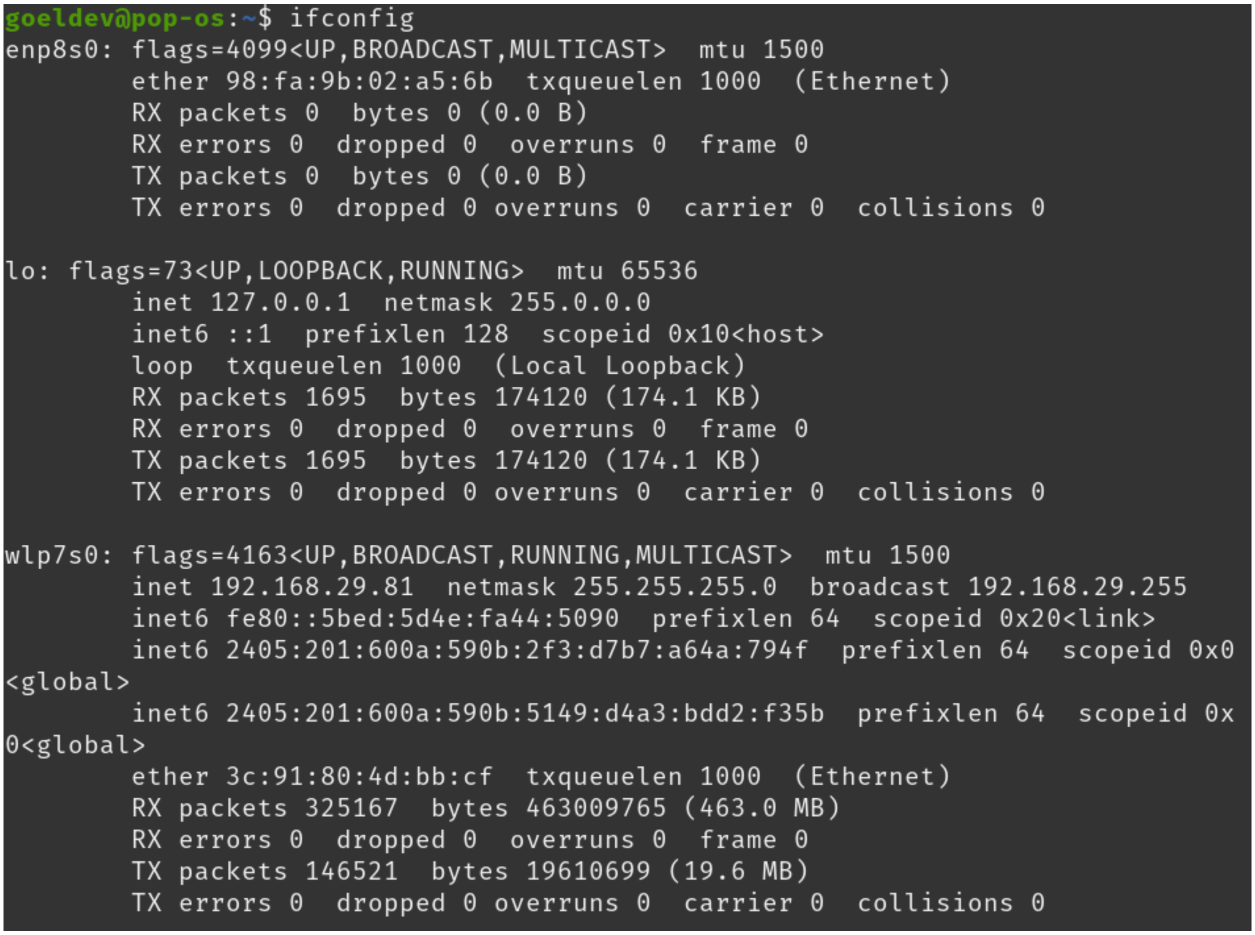
Dumps traffic on a network.
tcpdump outputs a description of the contents of packets on a network interface.
The ‘-c’ flag used in the command below restricts the count of packets to the specified value.



```
goeldev@pop-os:~$ sudo tcpdump -c 10
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wlp7s0, link-type EN10MB (Ethernet), capture size 262144 bytes
14:32:56.445904 IP6 2001:4860:4864:5::5e.19305 > pop-os.53933: UDP, length 59
14:32:56.447640 IP pop-os.34133 > reliance.reliance.domain: 33596+ PTR? 6.f.e.
8.0.7.d.1.f.f.4.3.4.6.a.b.b.0.9.5.a.0.0.6.1.0.2.0.5.0.4.2.ip6.arpa. (90)
14:32:56.450141 IP reliance.reliance.domain > pop-os.34133: 33596 NXDomain 0/0
/0 (90)
14:32:56.450178 IP6 pop-os.53933 > 2001:4860:4864:5::5e.19305: UDP, length 38
14:32:56.451621 IP pop-os.53783 > reliance.reliance.domain: 4787+ PTR? e.5.0.0
.0.0.0.0.0.0.0.0.0.0.0.0.0.5.0.0.0.4.6.8.4.0.6.8.4.1.0.0.2.ip6.arpa. (90)
14:32:56.463897 IP6 2001:4860:4864:5::5e.19305 > pop-os.53933: UDP, length 39
14:32:56.477208 IP reliance.reliance.domain > pop-os.53783: 4787 NXDomain 0/1/
0 (150)
14:32:56.478434 IP pop-os.40905 > reliance.reliance.domain: 62226+ PTR? 1.29.1
68.192.in-addr.arpa. (43)
14:32:56.480955 IP reliance.reliance.domain > pop-os.40905: 62226* 1/0/0 PTR r
eliance.reliance. (74)
14:32:56.481584 IP pop-os.56844 > reliance.reliance.domain: 18828+ PTR? 81.29.
168.192.in-addr.arpa. (44)
10 packets captured
11 packets received by filter
0 packets dropped by kernel
```

- **ifconfig**

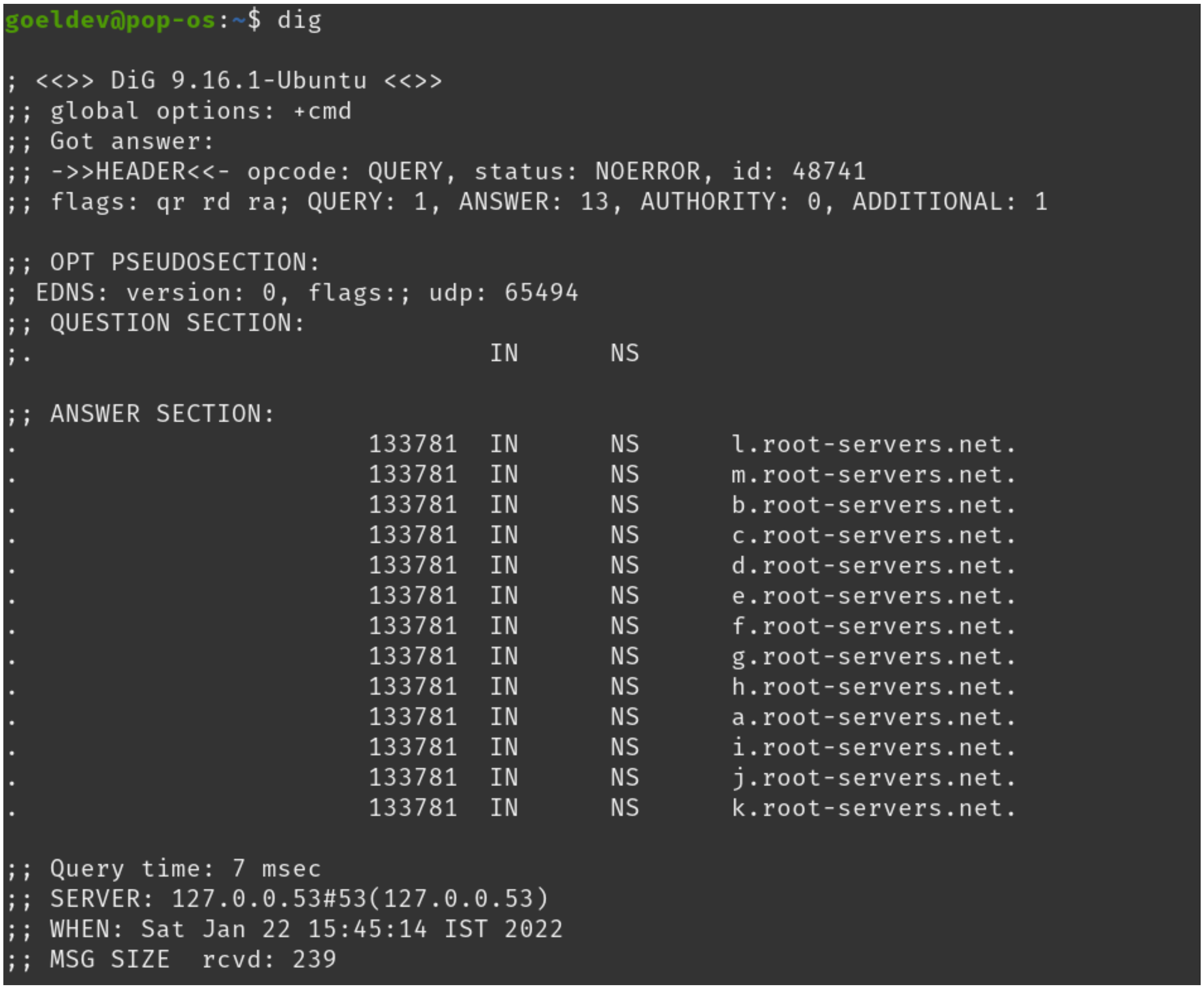
This command is used for configuring the kernel-resident network interfaces.
In the absence of any additional argument, this command is used to display the status of the currently active interfaces.



```
goeldev@pop-os:~$ ifconfig
enp8s0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 98:fa:9b:02:a5:6b  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 1695  bytes 174120 (174.1 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1695  bytes 174120 (174.1 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlp7s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.29.81  netmask 255.255.255.0  broadcast 192.168.29.255
        inet6 fe80::5bed:5d4e:fa44:5090  prefixlen 64  scopeid 0x20<link>
        inet6 2405:201:600a:590b:2f3:d7b7:a64a:794f  prefixlen 64  scopeid 0x0
<global>
        inet6 2405:201:600a:590b:5149:d4a3:bdd2:f35b  prefixlen 64  scopeid 0x
0<global>
        ether 3c:91:80:4d:bb:cf  txqueuelen 1000  (Ethernet)
        RX packets 325167  bytes 463009765 (463.0 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 146521  bytes 19610699 (19.6 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

- **dig**

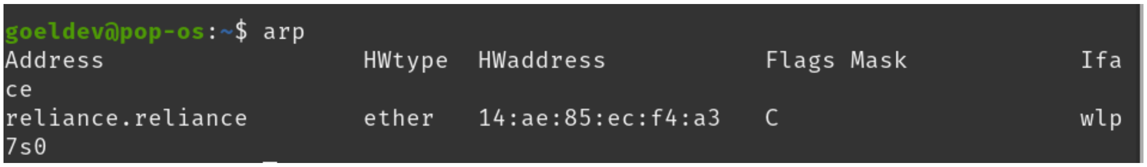
dig is a DNS lookup utility.
It is used to perform DNS lookups and display the answers that are returned from the name servers that were queried.



```
goeldev@pop-os:~$ dig

; <<>> DiG 9.16.1-Ubuntu <<>>
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 48741
;; flags: qr rd ra; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;.                              IN      NS

;; ANSWER SECTION:
.                       133781  IN      NS      l.root-servers.net.
.                       133781  IN      NS      m.root-servers.net.
.                       133781  IN      NS      b.root-servers.net.
.                       133781  IN      NS      c.root-servers.net.
.                       133781  IN      NS      d.root-servers.net.
.                       133781  IN      NS      e.root-servers.net.
.                       133781  IN      NS      f.root-servers.net.
.                       133781  IN      NS      g.root-servers.net.
.                       133781  IN      NS      h.root-servers.net.
.                       133781  IN      NS      a.root-servers.net.
.                       133781  IN      NS      i.root-servers.net.
.                       133781  IN      NS      j.root-servers.net.
.                       133781  IN      NS      k.root-servers.net.

;; Query time: 7 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Sat Jan 22 15:45:14 IST 2022
;; MSG SIZE  rcvd: 239
```

- **arp**

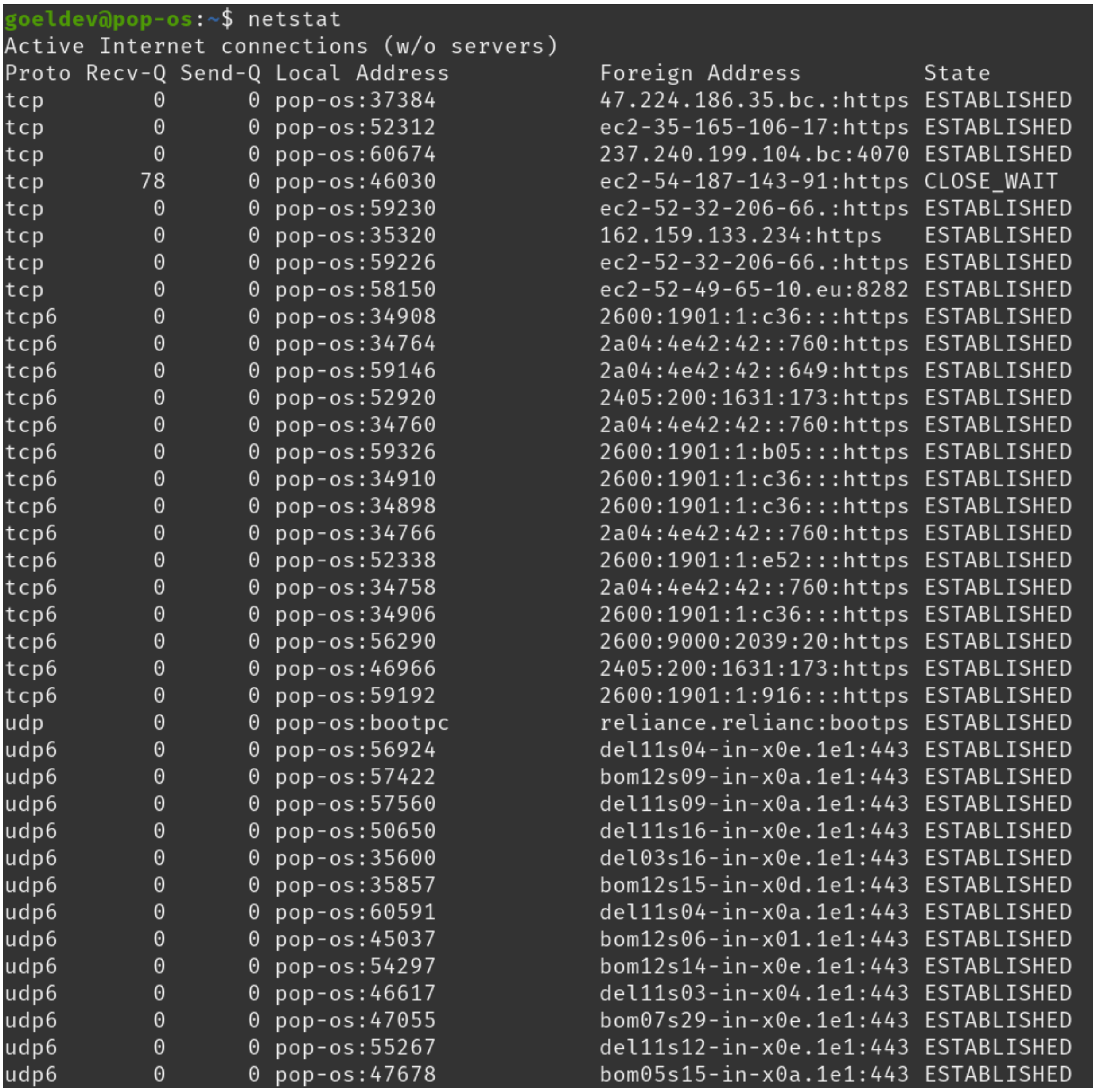
ARP stands for Address Resolution Protocol. **arp** command is used to manipulate or display the kernel’s IPv4 network neighbor cache. With no argument, the command outputs the current content of the ARP table.



```
goeldev@pop-os:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Ifa
ce
reliance.reliance        ether   14:ae:85:ec:f4:a3   C                     wlp
7s0
```

- **netstat**

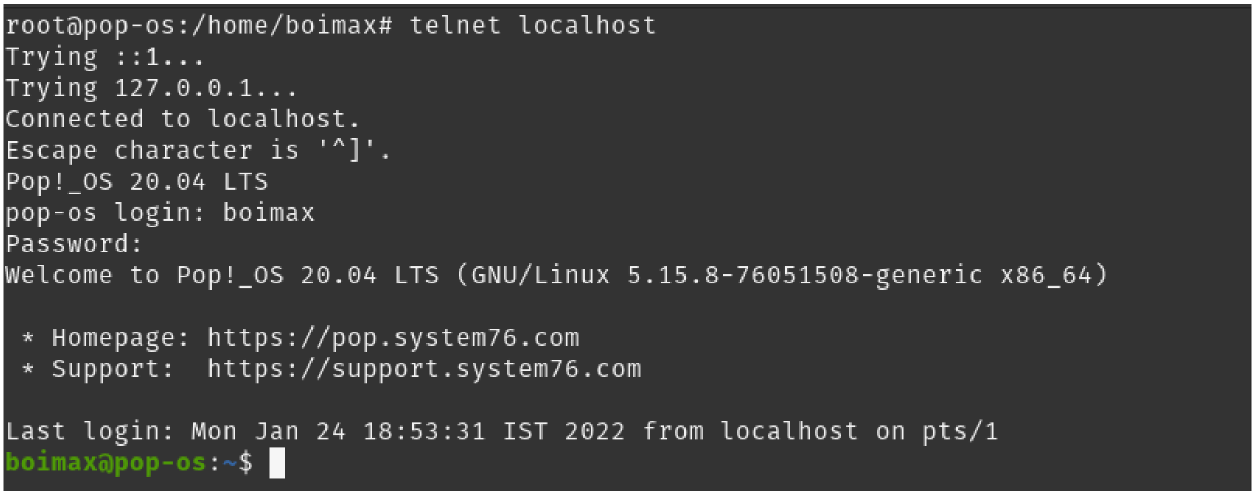
Print network connections, routing tables, interface statistics, masquerade connections, and multicast memberships. With no argument specified, **netstat** displays a list of open sockets.



```
goeldev@pop-os:~$ netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 pop-os:37384            47.224.186.35.bc.:https ESTABLISHED
tcp        0      0 pop-os:52312            ec2-35-165-106-17:https ESTABLISHED
tcp        0      0 pop-os:60674            237.240.199.104.bc:4070 ESTABLISHED
tcp       78      0 pop-os:46030            ec2-54-187-143-91:https CLOSE_WAIT
tcp        0      0 pop-os:59230            ec2-52-32-206-66.:https ESTABLISHED
tcp        0      0 pop-os:35320            162.159.133.234:https   ESTABLISHED
tcp        0      0 pop-os:59226            ec2-52-32-206-66.:https ESTABLISHED
tcp        0      0 pop-os:58150            ec2-52-49-65-10.eu:8282 ESTABLISHED
tcp6       0      0 pop-os:34908            2600:1901:1:c36:::https ESTABLISHED
tcp6       0      0 pop-os:34764            2a04:4e42:42::760:https ESTABLISHED
tcp6       0      0 pop-os:59146            2a04:4e42:42::649:https ESTABLISHED
tcp6       0      0 pop-os:52920            2405:200:1631:173:https ESTABLISHED
tcp6       0      0 pop-os:34760            2a04:4e42:42::760:https ESTABLISHED
tcp6       0      0 pop-os:59326            2600:1901:1:b05:::https ESTABLISHED
tcp6       0      0 pop-os:34910            2600:1901:1:c36:::https ESTABLISHED
tcp6       0      0 pop-os:34898            2600:1901:1:c36:::https ESTABLISHED
tcp6       0      0 pop-os:34766            2a04:4e42:42::760:https ESTABLISHED
tcp6       0      0 pop-os:52338            2600:1901:1:e52:::https ESTABLISHED
tcp6       0      0 pop-os:34758            2a04:4e42:42::760:https ESTABLISHED
tcp6       0      0 pop-os:34906            2600:1901:1:c36:::https ESTABLISHED
tcp6       0      0 pop-os:56290            2600:9000:2039:20:https ESTABLISHED
tcp6       0      0 pop-os:46966            2405:200:1631:173:https ESTABLISHED
tcp6       0      0 pop-os:59192            2600:1901:1:916:::https ESTABLISHED
udp        0      0 pop-os:bootpc           reliance.relianc:bootps ESTABLISHED
udp6       0      0 pop-os:56924            del11s04-in-x0e.1e1:443 ESTABLISHED
udp6       0      0 pop-os:57422            bom12s09-in-x0a.1e1:443 ESTABLISHED
udp6       0      0 pop-os:57560            del11s09-in-x0a.1e1:443 ESTABLISHED
udp6       0      0 pop-os:50650            del11s16-in-x0e.1e1:443 ESTABLISHED
udp6       0      0 pop-os:35600            del03s16-in-x0e.1e1:443 ESTABLISHED
udp6       0      0 pop-os:35857            bom12s15-in-x0d.1e1:443 ESTABLISHED
udp6       0      0 pop-os:60591            del11s04-in-x0a.1e1:443 ESTABLISHED
udp6       0      0 pop-os:45037            bom12s06-in-x01.1e1:443 ESTABLISHED
udp6       0      0 pop-os:54297            bom12s14-in-x0e.1e1:443 ESTABLISHED
udp6       0      0 pop-os:46617            del11s03-in-x04.1e1:443 ESTABLISHED
udp6       0      0 pop-os:47055            bom07s29-in-x0e.1e1:443 ESTABLISHED
udp6       0      0 pop-os:55267            del11s12-in-x0e.1e1:443 ESTABLISHED
udp6       0      0 pop-os:47678            bom05s15-in-x0a.1e1:443 ESTABLISHED
```

- **telnet**

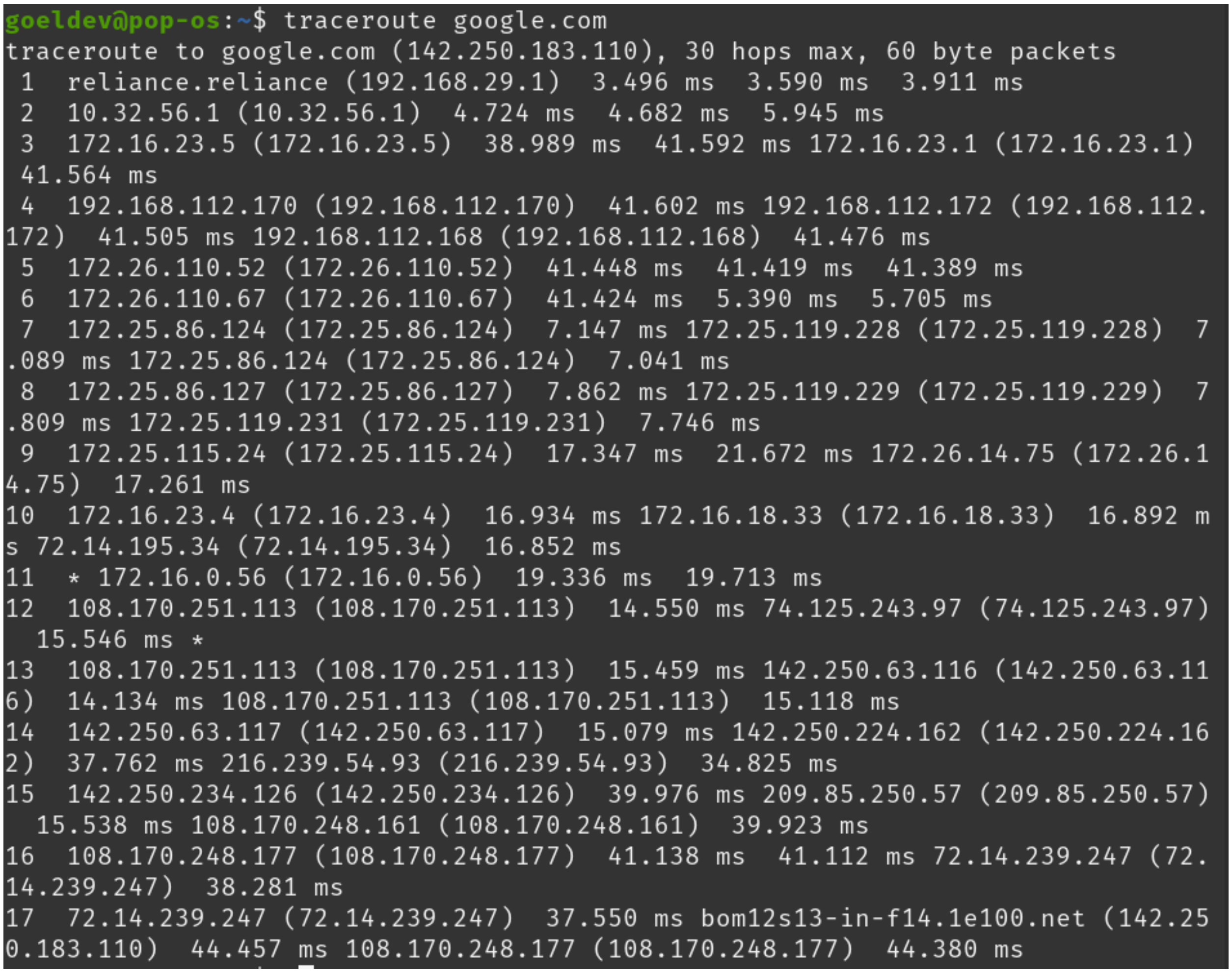
User interface to the TELNET protocol.
This command is used for interactive communication with another host using TELNET protocol. In the below given command execution, we connect via **telnet** to the localhost of the system. The command prompts for username and password, and after connecting, we can execute the commands as done before. The only difference is that the machine is now treated as a remote machine.



```
root@pop-os:/home/boimax# telnet localhost
Trying ::1...
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
Pop!_OS 20.04 LTS
pop-os login: boimax
Password:
Welcome to Pop!_OS 20.04 LTS (GNU/Linux 5.15.8-76051508-generic x86_64)

 * Homepage: https://pop.system76.com
 * Support:  https://support.system76.com

Last login: Mon Jan 24 18:53:31 IST 2022 from localhost on pts/1
boimax@pop-os:~$ 
```

- **traceroute**

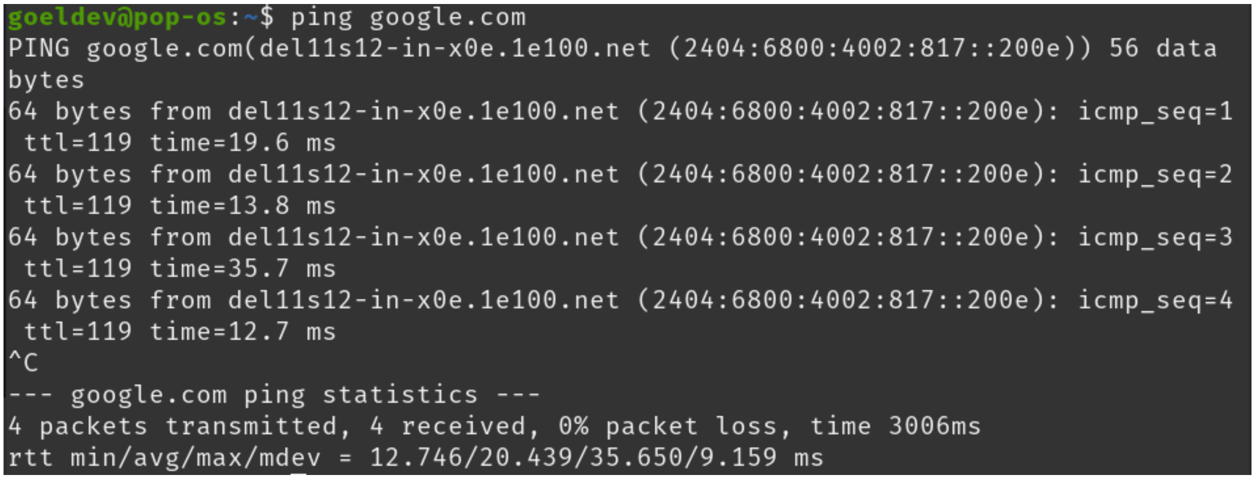
Prints the route packets trace to the network host.
This command tracks the route packets taken from an IP network on their way to a given host.



```
goeldev@pop-os:~$ traceroute google.com
traceroute to google.com (142.250.183.110), 30 hops max, 60 byte packets
 1  reliance.reliance (192.168.29.1)  3.496 ms  3.590 ms  3.911 ms
 2  10.32.56.1 (10.32.56.1)  4.724 ms  4.682 ms  5.945 ms
 3  172.16.23.5 (172.16.23.5)  38.989 ms  41.592 ms 172.16.23.1 (172.16.23.1)
 41.564 ms
 4  192.168.112.170 (192.168.112.170)  41.602 ms 192.168.112.172 (192.168.112.
172)  41.505 ms 192.168.112.168 (192.168.112.168)  41.476 ms
 5  172.26.110.52 (172.26.110.52)  41.448 ms  41.419 ms  41.389 ms
 6  172.26.110.67 (172.26.110.67)  41.424 ms  5.390 ms  5.705 ms
 7  172.25.86.124 (172.25.86.124)  7.147 ms 172.25.119.228 (172.25.119.228)  7
.089 ms 172.25.86.124 (172.25.86.124)  7.041 ms
 8  172.25.86.127 (172.25.86.127)  7.862 ms 172.25.119.229 (172.25.119.229)  7
.809 ms 172.25.119.231 (172.25.119.231)  7.746 ms
 9  172.25.115.24 (172.25.115.24)  17.347 ms  21.672 ms 172.26.14.75 (172.26.1
4.75)  17.261 ms
10  172.16.23.4 (172.16.23.4)  16.934 ms 172.16.18.33 (172.16.18.33)  16.892 m
s 72.14.195.34 (72.14.195.34)  16.852 ms
11  * 172.16.0.56 (172.16.0.56)  19.336 ms  19.713 ms
12  108.170.251.113 (108.170.251.113)  14.550 ms 74.125.243.97 (74.125.243.97)
  15.546 ms *
13  108.170.251.113 (108.170.251.113)  15.459 ms 142.250.63.116 (142.250.63.11
6)  14.134 ms 108.170.251.113 (108.170.251.113)  15.118 ms
14  142.250.63.117 (142.250.63.117)  15.079 ms 142.250.224.162 (142.250.224.16
2)  37.762 ms 216.239.54.93 (216.239.54.93)  34.825 ms
15  142.250.234.126 (142.250.234.126)  39.976 ms 209.85.250.57 (209.85.250.57)
  15.538 ms 108.170.248.161 (108.170.248.161)  39.923 ms
16  108.170.248.177 (108.170.248.177)  41.138 ms  41.112 ms 72.14.239.247 (72.
14.239.247)  38.281 ms
17  72.14.239.247 (72.14.239.247)  37.550 ms bom12s13-in-f14.1e100.net (142.25
0.183.110)  44.457 ms 108.170.248.177 (108.170.248.177)  44.380 ms
```

- **ping**

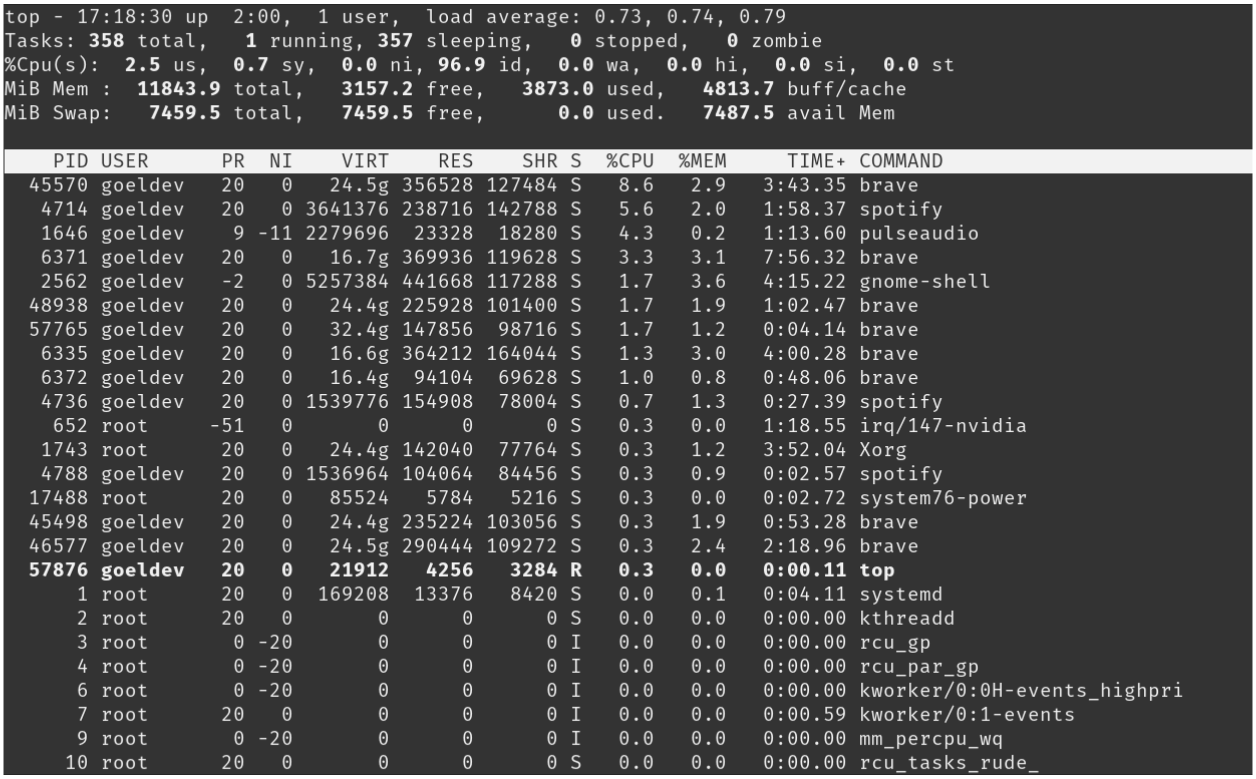
This command uses the ICMP protocol’s ECHO_REQUEST to get an ICMP ECHO_RESPONSE from a host or gateway. It works with both IPv4 and IPv6. Below, we use the command to send and receive requests from google.com.



```
goeldev@pop-os:~$ ping google.com
PING google.com(del11s12-in-x0e.1e100.net (2404:6800:4002:817::200e)) 56 data
bytes
64 bytes from del11s12-in-x0e.1e100.net (2404:6800:4002:817::200e): icmp_seq=1
 ttl=119 time=19.6 ms
64 bytes from del11s12-in-x0e.1e100.net (2404:6800:4002:817::200e): icmp_seq=2
 ttl=119 time=13.8 ms
64 bytes from del11s12-in-x0e.1e100.net (2404:6800:4002:817::200e): icmp_seq=3
 ttl=119 time=35.7 ms
64 bytes from del11s12-in-x0e.1e100.net (2404:6800:4002:817::200e): icmp_seq=4
 ttl=119 time=12.7 ms
^C
--- google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 12.746/20.439/35.650/9.159 ms
```

- **top**

Displays Linux processes in a dynamic real-time view. It can display system summary info as well as a list of processes and threads currently being managed by the kernel.

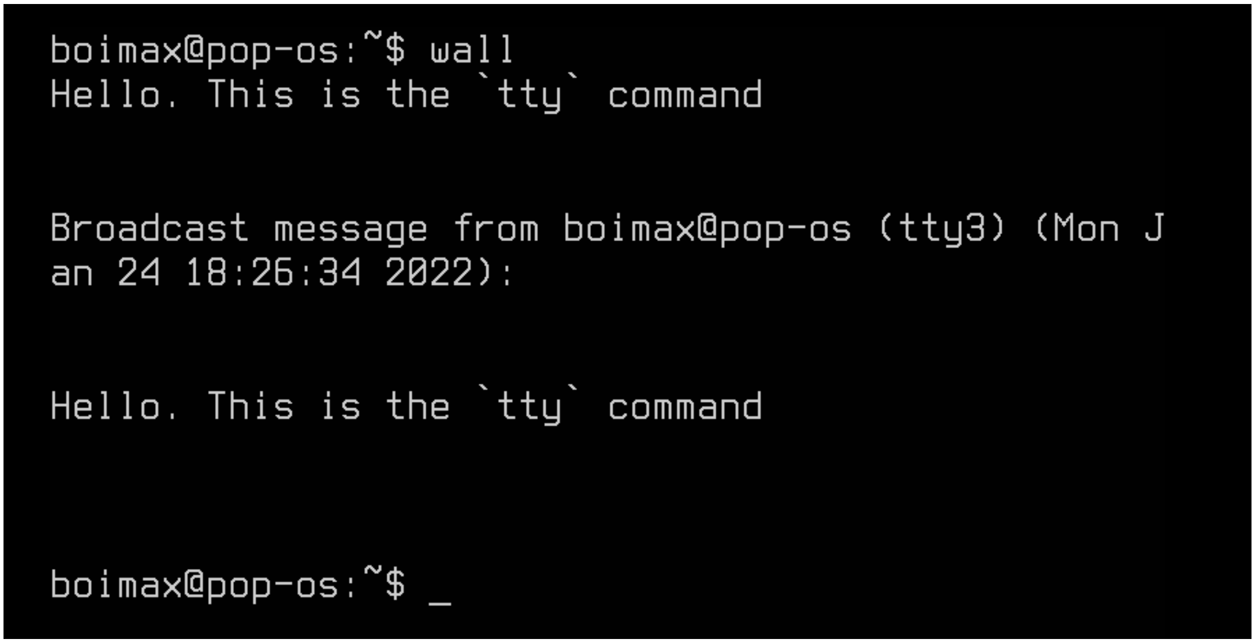


```
top - 17:18:30 up  2:00,  1 user,  load average: 0.73, 0.74, 0.79
Tasks: 358 total,   1 running, 357 sleeping,   0 stopped,   0 zombie
%Cpu(s):  2.5 us,  0.7 sy,  0.0 ni, 96.9 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
MiB Mem :  11843.9 total,   3157.2 free,   3873.0 used,   4813.7 buff/cache
MiB Swap:   7459.5 total,   7459.5 free,      0.0 used.   7487.5 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
  45570 goeldev   20   0   24.5g 356528 127484 S   8.6   2.9   3:43.35 brave
   4714 goeldev   20   0 3641376 238716 142788 S   5.6   2.0   1:58.37 spotify
   1646 goeldev    9 -11 2279696  23328  18280 S   4.3   0.2   1:13.60 pulseaudio
   6371 goeldev   20   0   16.7g 369936 119628 S   3.3   3.1   7:56.32 brave
   2562 goeldev   -2   0 5257384 441668 117288 S   1.7   3.6   4:15.22 gnome-shell
  48938 goeldev   20   0   24.4g 225928 101400 S   1.7   1.9   1:02.47 brave
  57765 goeldev   20   0   32.4g 147856  98716 S   1.7   1.2   0:04.14 brave
   6335 goeldev   20   0   16.6g 364212 164044 S   1.3   3.0   4:00.28 brave
   6372 goeldev   20   0   16.4g  94104  69628 S   1.0   0.8   0:48.06 brave
   4736 goeldev   20   0 1539776 154908  78004 S   0.7   1.3   0:27.39 spotify
    652 root     -51   0       0      0      0 S   0.3   0.0   1:18.55 irq/147-nvidia
   1743 root      20   0   24.4g 142040  77764 S   0.3   1.2   3:52.04 Xorg
   4788 goeldev   20   0 1536964 104064  84456 S   0.3   0.9   0:02.57 spotify
  17488 root      20   0   85524   5784   5216 S   0.3   0.0   0:02.72 system76-power
  45498 goeldev   20   0   24.4g 235224 103056 S   0.3   1.9   0:53.28 brave
  46577 goeldev   20   0   24.5g 290444 109272 S   0.3   2.4   2:18.96 brave
  57876 goeldev   20   0   21912   4256   3284 R   0.3   0.0   0:00.11 top
      1 root      20   0  169208  13376   8420 S   0.0   0.1   0:04.11 systemd
      2 root      20   0       0      0      0 S   0.0   0.0   0:00.00 kthreadd
      3 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_gp
      4 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_par_gp
      6 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/0:0H-events_highpri
      7 root      20   0       0      0      0 I   0.0   0.0   0:00.59 kworker/0:1-events
      9 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 mm_percpu_wq
     10 root      20   0       0      0      0 S   0.0   0.0   0:00.00 rcu_tasks_rude_
```

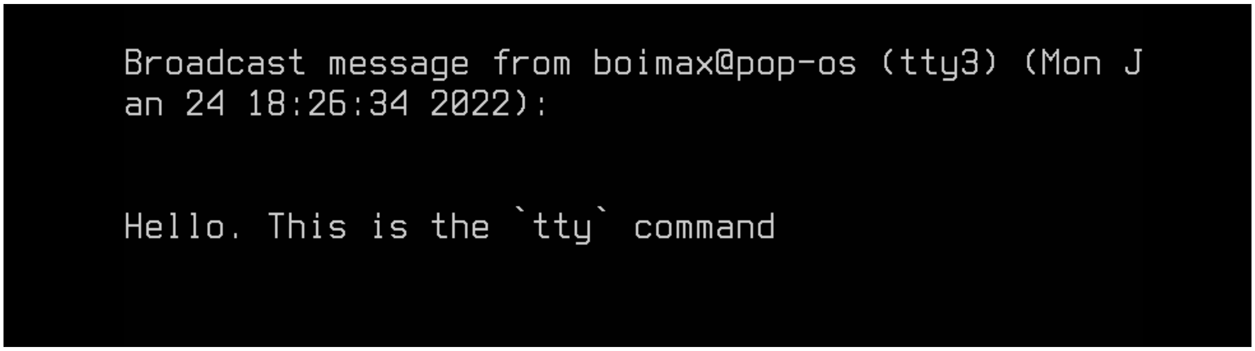
- **wall**

This command is used for writing a message to all logged in users. Only the superuser can write on the terminals of users who have chosen to deny messages.

In the below images, the **wall** command is executed from tty3 terminal to broadcast a message which is then received by the user logged in tty4 terminal.



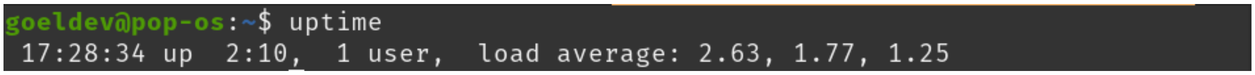
```
boimax@pop-os:~$ wall
Hello. This is the `tty` command


Broadcast message from boimax@pop-os (tty3) (Mon J
an 24 18:26:34 2022):


Hello. This is the `tty` command



boimax@pop-os:~$ _
```



```
Broadcast message from boimax@pop-os (tty3) (Mon J
an 24 18:26:34 2022):


Hello. This is the `tty` command
```

- **uptime**

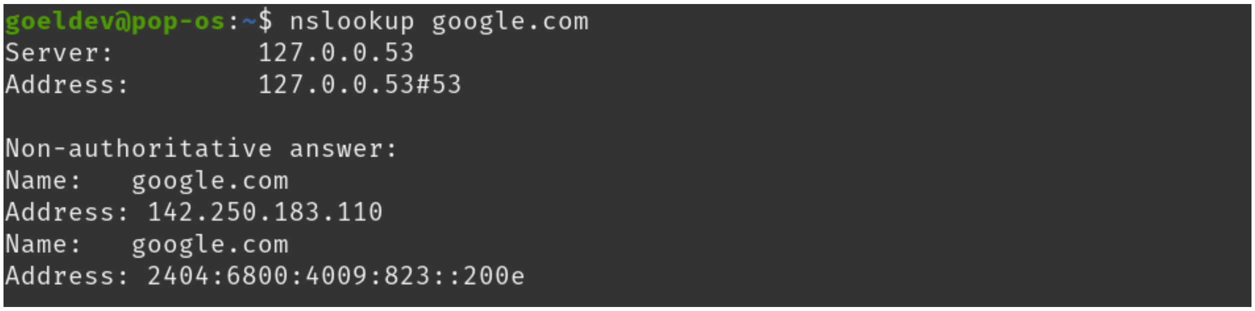
Displays how long the system has been active in a single line output. Also shows currently logged on users and system load averages for the past 1, 5 and 15 minutes.



```
goeldev@pop-os:~$ uptime
 17:28:34 up  2:10,  1 user,  load average: 2.63, 1.77, 1.25
```

- **nslookup**

Queries internet name servers interactively.
This program queries Internet domain name servers. The below given screenshot shows the command executed in non-interactive mode, where just the name and requested info for the host or domain is shown.



```
goeldev@pop-os:~$ nslookup google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   google.com
Address: 142.250.183.110
Name:   google.com
Address: 2404:6800:4009:823::200e
```