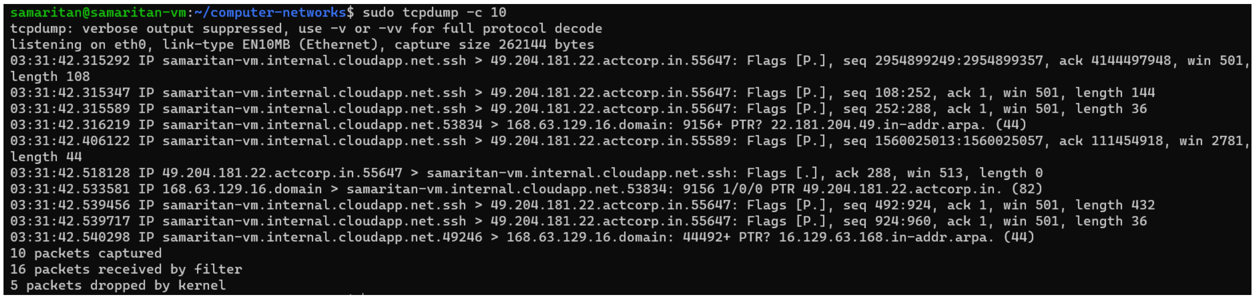
1) tcpdump

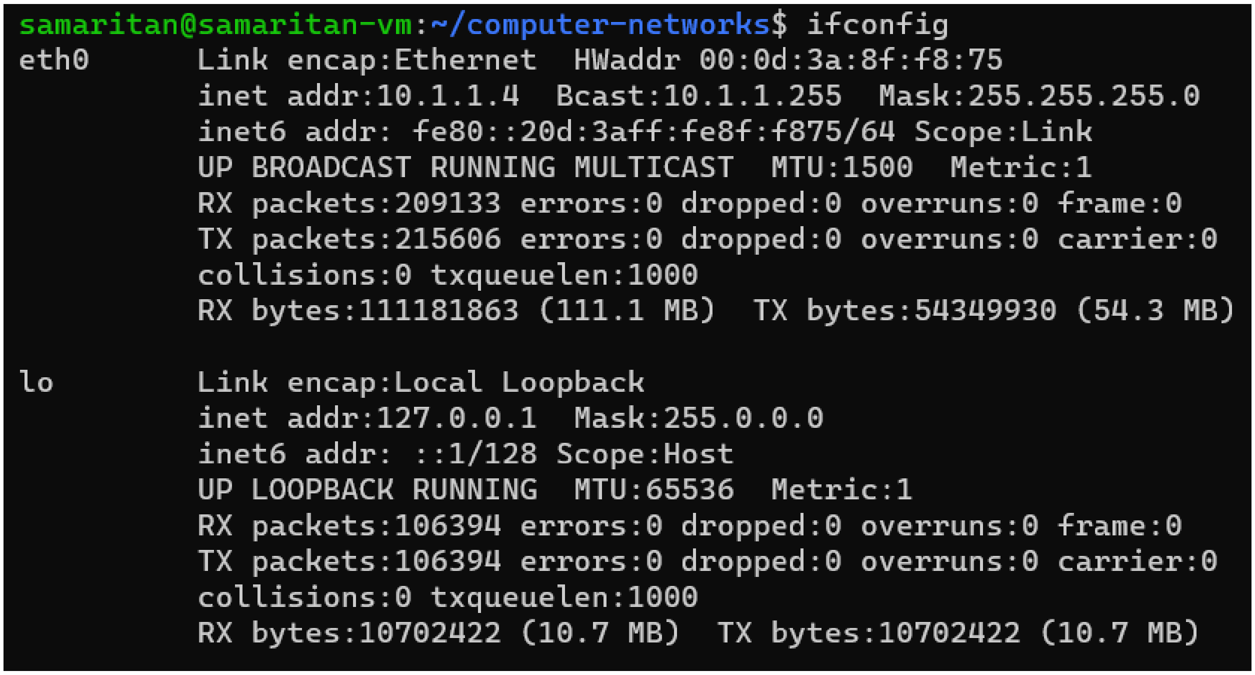
Tcpdump prints out a description of the contents of packets on a network interface that match the boolean expression; the description is preceded by a timestamp, printed, by default, as hours, minutes, seconds, and fractions of a second since midnight. It can also be run with the -w flag, which causes it to save the packet data to a file for later analysis, and/or with the -r flag, which causes it to read from a saved packet file rather than to read packets from a network interface (please note tcpdump is protected via an enforcing apparmor(7) profile in Ubuntu which limits the files tcpdump may access). It can also be run with the -V flag, which causes it to read a list of saved packet files. In all cases, only packets that match expressions will be processed by tcpdump.



```
samaritan@samaritan-vm:~/computer-networks$ sudo tcpdump -c 10
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
03:31:42.315292 IP samaritan-vm.internal.cloudapp.net.ssh > 49.204.181.22.actcorp.in.55647: Flags [P.], seq 2954899249:2954899357, ack 4144497948, win 501,
length 108
03:31:42.315347 IP samaritan-vm.internal.cloudapp.net.ssh > 49.204.181.22.actcorp.in.55647: Flags [P.], seq 108:252, ack 1, win 501, length 144
03:31:42.315589 IP samaritan-vm.internal.cloudapp.net.ssh > 49.204.181.22.actcorp.in.55647: Flags [P.], seq 252:288, ack 1, win 501, length 36
03:31:42.316219 IP samaritan-vm.internal.cloudapp.net.53834 > 168.63.129.16.domain: 9156+ PTR? 22.181.204.49.in-addr.arpa. (44)
03:31:42.406122 IP samaritan-vm.internal.cloudapp.net.ssh > 49.204.181.22.actcorp.in.55589: Flags [P.], seq 1560025013:1560025057, ack 111454918, win 2781,
length 44
03:31:42.518128 IP 49.204.181.22.actcorp.in.55647 > samaritan-vm.internal.cloudapp.net.ssh: Flags [.], ack 288, win 513, length 0
03:31:42.533581 IP 168.63.129.16.domain > samaritan-vm.internal.cloudapp.net.53834: 9156 1/0/0 PTR 49.204.181.22.actcorp.in. (82)
03:31:42.539456 IP samaritan-vm.internal.cloudapp.net.ssh > 49.204.181.22.actcorp.in.55647: Flags [P.], seq 492:924, ack 1, win 501, length 432
03:31:42.539717 IP samaritan-vm.internal.cloudapp.net.ssh > 49.204.181.22.actcorp.in.55647: Flags [P.], seq 924:960, ack 1, win 501, length 36
03:31:42.540298 IP samaritan-vm.internal.cloudapp.net.49246 > 168.63.129.16.domain: 44492+ PTR? 16.129.63.168.in-addr.arpa. (44)
10 packets captured
16 packets received by filter
5 packets dropped by kernel
```

2) ifconfig

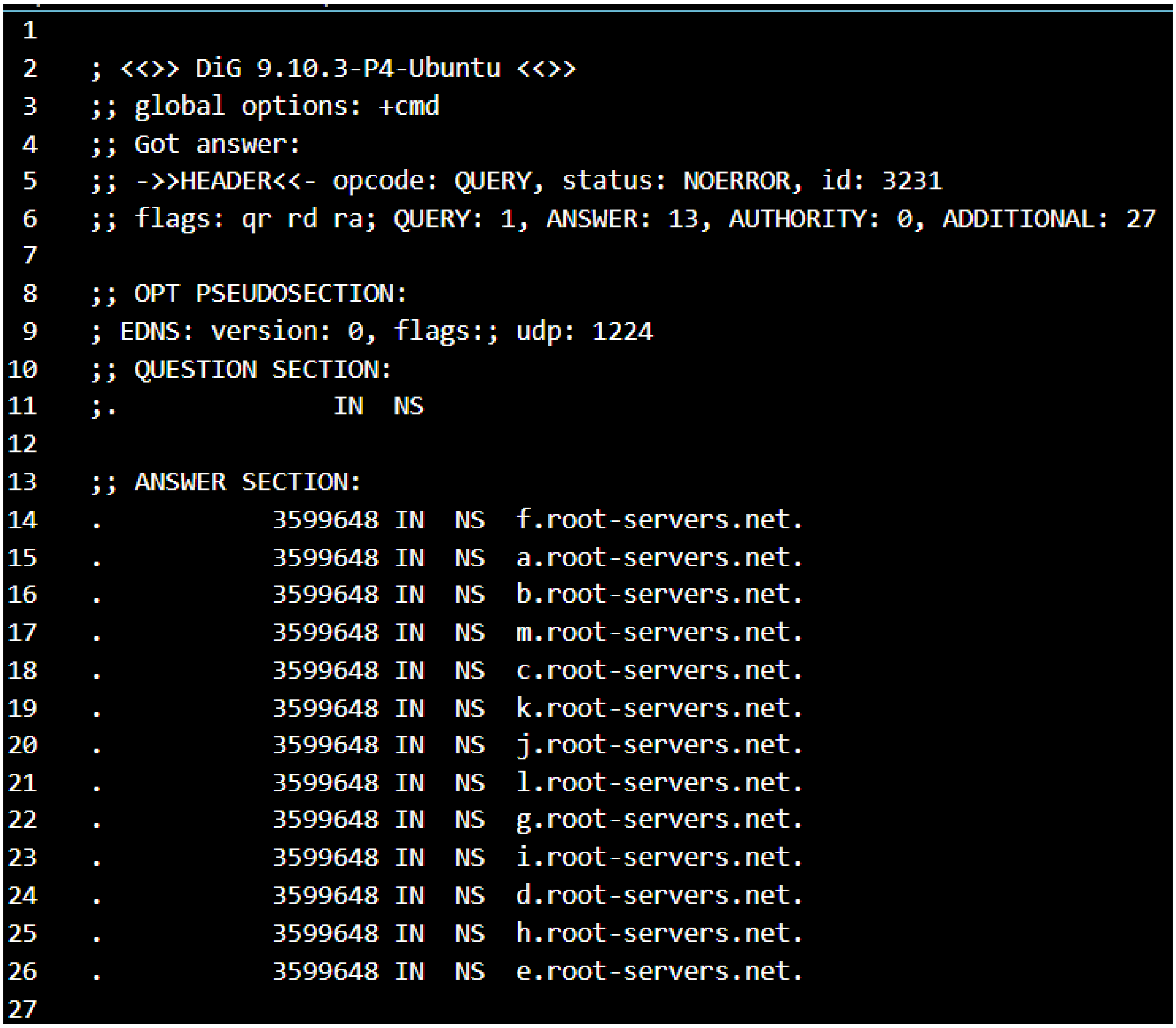
Ifconfig is used to configure the kernel-resident network interfaces. It is used at boot time to set up interfaces as necessary. After that, it is usually only needed when debugging or when system tuning is needed.



```
samaritan@samaritan-vm:~/computer-networks$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0d:3a:8f:f8:75
          inet addr:10.1.1.4  Bcast:10.1.1.255  Mask:255.255.255.0
          inet6 addr: fe80::20d:3aff:fe8f:f875/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:209133 errors:0 dropped:0 overruns:0 frame:0
          TX packets:215606 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:111181863 (111.1 MB)  TX bytes:54349930 (54.3 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:106394 errors:0 dropped:0 overruns:0 frame:0
          TX packets:106394 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:10702422 (10.7 MB)  TX bytes:10702422 (10.7 MB)
```

3) dig

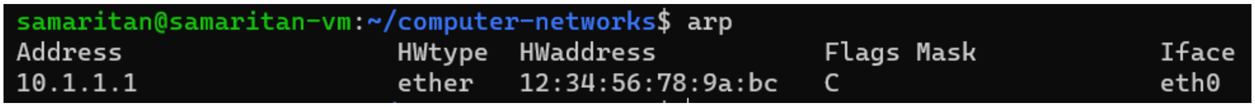
dig (domain information groper) is a flexible tool for interrogating DNS name servers. It performs DNS lookups and displays the answers that are returned from the name server(s) that were queried. Most DNS administrators use dig to troubleshoot DNS problems because of its flexibility, ease of use and clarity of output. Other lookup tools tend to have less functionality than dig.



```

; <<>> DiG 9.10.3-P4-Ubuntu <<>>
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3231
;; flags: qr rd ra; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 27

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1224
;; QUESTION SECTION:
;.              IN  NS

;; ANSWER SECTION:
.           3599648 IN  NS  f.root-servers.net.
.           3599648 IN  NS  a.root-servers.net.
.           3599648 IN  NS  b.root-servers.net.
.           3599648 IN  NS  m.root-servers.net.
.           3599648 IN  NS  c.root-servers.net.
.           3599648 IN  NS  k.root-servers.net.
.           3599648 IN  NS  j.root-servers.net.
.           3599648 IN  NS  l.root-servers.net.
.           3599648 IN  NS  g.root-servers.net.
.           3599648 IN  NS  i.root-servers.net.
.           3599648 IN  NS  d.root-servers.net.
.           3599648 IN  NS  h.root-servers.net.
.           3599648 IN  NS  e.root-servers.net.

```

4) arp

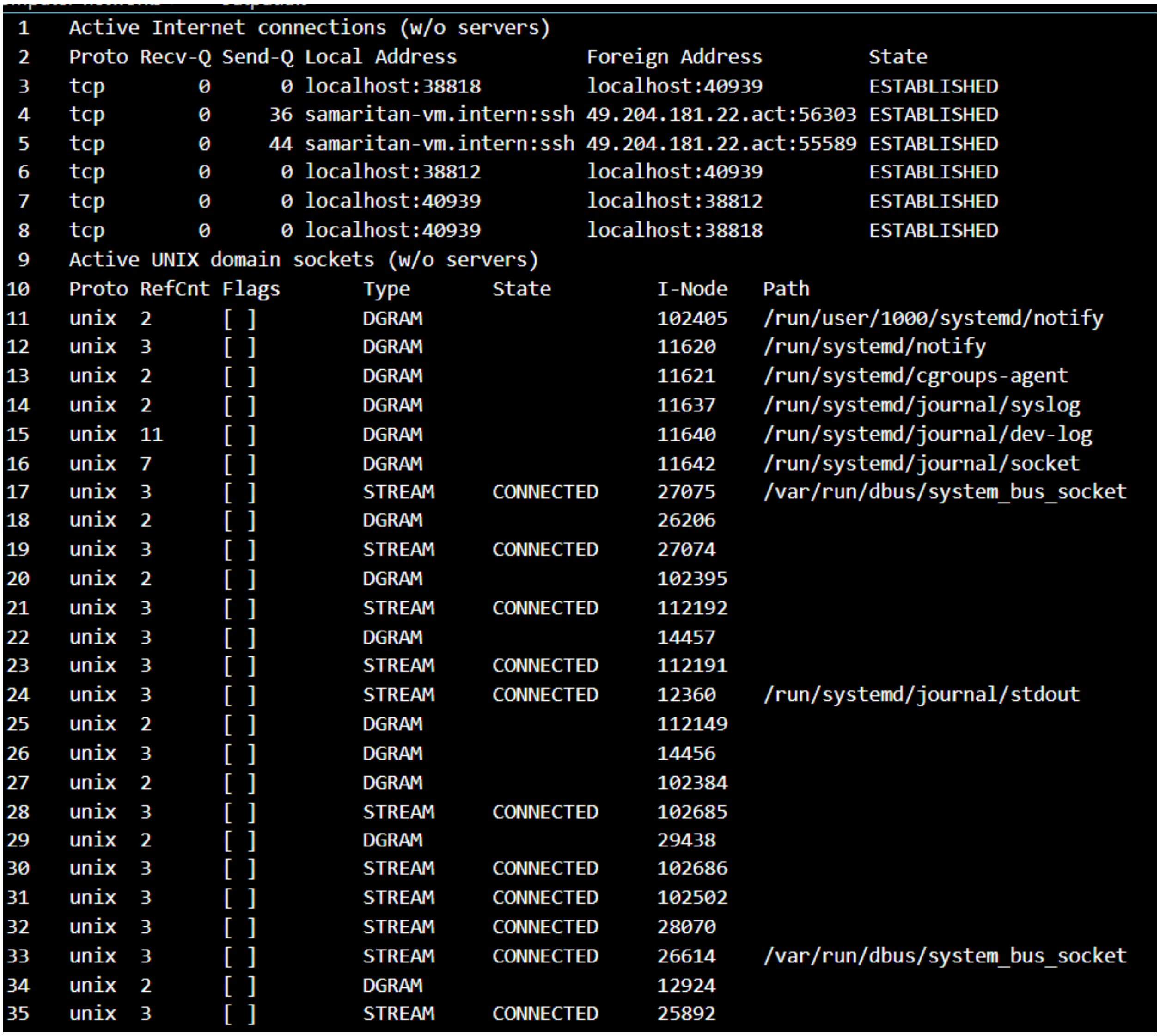
Arp manipulates or displays the kernel's IPv4 network neighbour cache. It can add entries to the table, delete one or display the current content. ARP stands for Address Protocol, which is used to find the media access control address of a network neighbour for a given IPv4 Address.



```
samaritan@samaritan-vm:~/computer-networks$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
10.1.1.1                 ether   12:34:56:78:9a:bc   C                     eth0
```

5) netstat

Netstat prints information about the Linux networking subsystem.



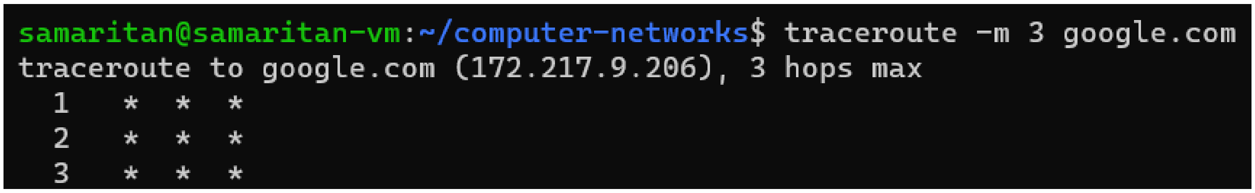
```
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:38818         localhost:40939         ESTABLISHED
tcp        0     36 samaritan-vm.intern:ssh 49.204.181.22.act:56303 ESTABLISHED
tcp        0     44 samaritan-vm.intern:ssh 49.204.181.22.act:55589 ESTABLISHED
tcp        0      0 localhost:38812         localhost:40939         ESTABLISHED
tcp        0      0 localhost:40939         localhost:38812         ESTABLISHED
tcp        0      0 localhost:40939         localhost:38818         ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ]         DGRAM                    102405   /run/user/1000/systemd/notify
unix  3      [ ]         DGRAM                    11620    /run/systemd/notify
unix  2      [ ]         DGRAM                    11621    /run/systemd/cgroups-agent
unix  2      [ ]         DGRAM                    11637    /run/systemd/journal/syslog
unix  11     [ ]         DGRAM                    11640    /run/systemd/journal/dev-log
unix  7      [ ]         DGRAM                    11642    /run/systemd/journal/socket
unix  3      [ ]         STREAM     CONNECTED     27075    /var/run/dbus/system_bus_socket
unix  2      [ ]         DGRAM                    26206
unix  3      [ ]         STREAM     CONNECTED     27074
unix  2      [ ]         DGRAM                    102395
unix  3      [ ]         STREAM     CONNECTED     112192
unix  3      [ ]         DGRAM                    14457
unix  3      [ ]         STREAM     CONNECTED     112191
unix  3      [ ]         STREAM     CONNECTED     12360    /run/systemd/journal/stdout
unix  2      [ ]         DGRAM                    112149
unix  3      [ ]         DGRAM                    14456
unix  2      [ ]         DGRAM                    102384
unix  3      [ ]         STREAM     CONNECTED     102685
unix  2      [ ]         DGRAM                    29438
unix  3      [ ]         STREAM     CONNECTED     102686
unix  3      [ ]         STREAM     CONNECTED     102502
unix  3      [ ]         STREAM     CONNECTED     28070
unix  3      [ ]         STREAM     CONNECTED     26614    /var/run/dbus/system_bus_socket
unix  2      [ ]         DGRAM                    12924
unix  3      [ ]         STREAM     CONNECTED     25892
```

6) telnet

The telnet command is used for interactive communication with another host using the TELNET protocol. It begins in command mode, where it prints a telnet prompt ("telnet> "). If telnet is invoked with a host argument, it performs an open command implicitly.

7) traceroute

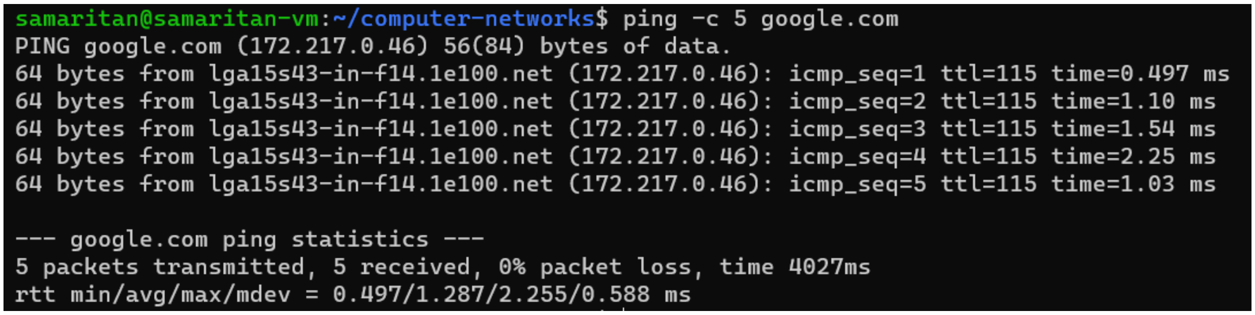
Print the route packets trace to network host.



```
samaritan@samaritan-vm:~/computer-networks$ traceroute -m 3 google.com
traceroute to google.com (172.217.9.206), 3 hops max
  1   *  *  *
  2   *  *  *
  3   *  *  *
```

8) ping

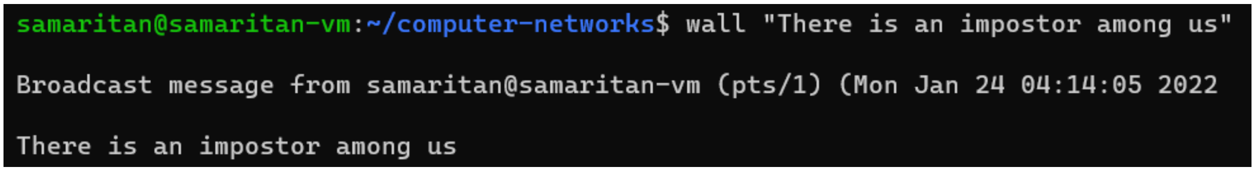
ping uses the ICMP protocol's mandatory ECHO_REQUEST datagram to elicit an ICMP ECHO_RESPONSE from a host or gateway. ECHO_REQUEST datagrams (``pings") have an IP and ICMP header, followed by a struct timeval and then an arbitrary number of ``pad" bytes used to fill out the packet.



```
samaritan@samaritan-vm:~/computer-networks$ ping -c 5 google.com
PING google.com (172.217.0.46) 56(84) bytes of data.
64 bytes from lga15s43-in-f14.1e100.net (172.217.0.46): icmp_seq=1 ttl=115 time=0.497 ms
64 bytes from lga15s43-in-f14.1e100.net (172.217.0.46): icmp_seq=2 ttl=115 time=1.10 ms
64 bytes from lga15s43-in-f14.1e100.net (172.217.0.46): icmp_seq=3 ttl=115 time=1.54 ms
64 bytes from lga15s43-in-f14.1e100.net (172.217.0.46): icmp_seq=4 ttl=115 time=2.25 ms
64 bytes from lga15s43-in-f14.1e100.net (172.217.0.46): icmp_seq=5 ttl=115 time=1.03 ms

--- google.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4027ms
rtt min/avg/max/mdev = 0.497/1.287/2.255/0.588 ms
```

9) wall

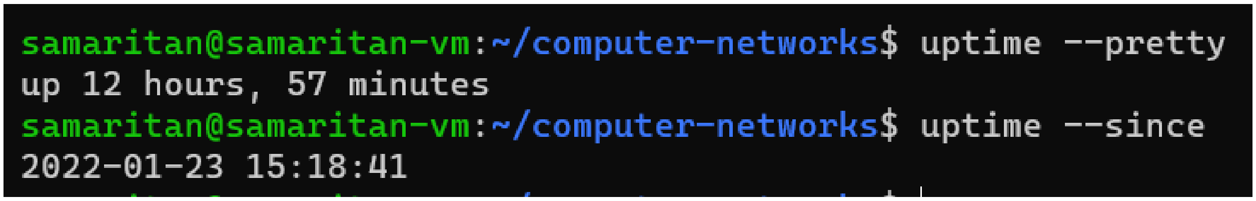
wall displays a message, or the contents of a file, or otherwise its standard input, on the terminals of all currently logged in users. The command will wrap lines that are longer than 79 characters. Short lines are whitespace padded to have 79 characters. The command will always put a carriage return and new line at the end of each line.



```
samaritan@samaritan-vm:~/computer-networks$ wall "There is an impostor among us"

Broadcast message from samaritan@samaritan-vm (pts/1) (Mon Jan 24 04:14:05 2022

There is an impostor among us
```

10) uptime

uptime gives a one line display of the following information. The current time, how long the system has been running, how many users are currently logged on, and the system load averages for the past 1, 5, and 15 minutes.



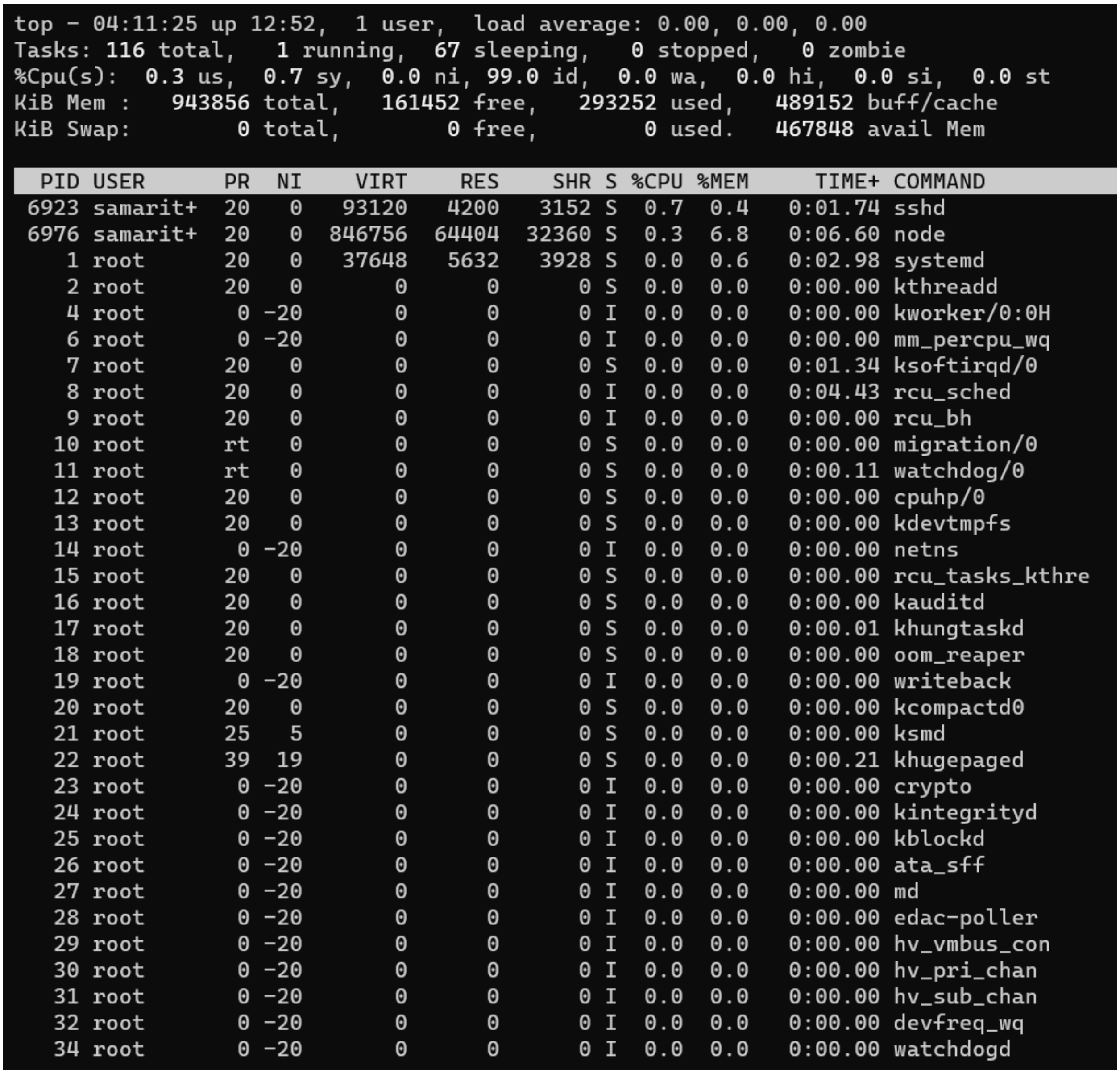
```
samaritan@samaritan-vm:~/computer-networks$ uptime --pretty
up 12 hours, 57 minutes
samaritan@samaritan-vm:~/computer-networks$ uptime --since
2022-01-23 15:18:41
```

12) nslookup

Nslookup is a program to query Internet domain name servers. Nslookup has two modes: interactive and non-interactive. Interactive mode allows the user to query name servers for information about various hosts and domains or to print a list of hosts in a domain. Non-interactive mode is used to print just the name and requested information for a host or domain.

11) top

The top program provides a dynamic real-time view of a running system. It can display system summary information as well as a list of processes or threads currently being managed by the Linux kernel. The types of system summary information shown and the types, order and size of information displayed for processes are all user configurable and that configuration can be made persistent across restarts.



```
top - 04:11:25 up 12:52,  1 user,  load average: 0.00, 0.00, 0.00
Tasks: 116 total,   1 running,  67 sleeping,   0 stopped,   0 zombie
%Cpu(s):  0.3 us,  0.7 sy,  0.0 ni, 99.0 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
KiB Mem :   943856 total,   161452 free,   293252 used,   489152 buff/cache
KiB Swap:        0 total,        0 free,        0 used.   467848 avail Mem

  PID USER      PR  NI    VIRT    RES    SHR S %CPU %MEM     TIME+ COMMAND
 6923 samarit+  20   0   93120   4200   3152 S  0.7  0.4   0:01.74 sshd
 6976 samarit+  20   0  846756  64404  32360 S  0.3  6.8   0:06.60 node
    1 root      20   0   37648   5632   3928 S  0.0  0.6   0:02.98 systemd
    2 root      20   0       0      0      0 S  0.0  0.0   0:00.00 kthreadd
    4 root       0 -20       0      0      0 I  0.0  0.0   0:00.00 kworker/0:0H
    6 root       0 -20       0      0      0 I  0.0  0.0   0:00.00 mm_percpu_wq
    7 root      20   0       0      0      0 S  0.0  0.0   0:01.34 ksoftirqd/0
    8 root      20   0       0      0      0 I  0.0  0.0   0:04.43 rcu_sched
    9 root      20   0       0      0      0 I  0.0  0.0   0:00.00 rcu_bh
   10 root      rt   0       0      0      0 S  0.0  0.0   0:00.00 migration/0
   11 root      rt   0       0      0      0 S  0.0  0.0   0:00.11 watchdog/0
   12 root      20   0       0      0      0 S  0.0  0.0   0:00.00 cpuhp/0
   13 root      20   0       0      0      0 S  0.0  0.0   0:00.00 kdevtmpfs
   14 root       0 -20       0      0      0 I  0.0  0.0   0:00.00 netns
   15 root      20   0       0      0      0 S  0.0  0.0   0:00.00 rcu_tasks_kthre
   16 root      20   0       0      0      0 S  0.0  0.0   0:00.00 kauditd
   17 root      20   0       0      0      0 S  0.0  0.0   0:00.01 khungtaskd
   18 root      20   0       0      0      0 S  0.0  0.0   0:00.00 oom_reaper
   19 root       0 -20       0      0      0 I  0.0  0.0   0:00.00 writeback
   20 root      20   0       0      0      0 S  0.0  0.0   0:00.00 kcompactd0
   21 root      25   5       0      0      0 S  0.0  0.0   0:00.00 ksmd
   22 root      39  19       0      0      0 S  0.0  0.0   0:00.21 khugepaged
   23 root       0 -20       0      0      0 I  0.0  0.0   0:00.00 crypto
   24 root       0 -20       0      0      0 I  0.0  0.0   0:00.00 kintegrityd
   25 root       0 -20       0      0      0 I  0.0  0.0   0:00.00 kblockd
   26 root       0 -20       0      0      0 I  0.0  0.0   0:00.00 ata_sff
   27 root       0 -20       0      0      0 I  0.0  0.0   0:00.00 md
   28 root       0 -20       0      0      0 I  0.0  0.0   0:00.00 edac-poller
   29 root       0 -20       0      0      0 I  0.0  0.0   0:00.00 hv_vmbus_con
   30 root       0 -20       0      0      0 I  0.0  0.0   0:00.00 hv_pri_chan
   31 root       0 -20       0      0      0 I  0.0  0.0   0:00.00 hv_sub_chan
   32 root       0 -20       0      0      0 I  0.0  0.0   0:00.00 devfreq_wq
   34 root       0 -20       0      0      0 I  0.0  0.0   0:00.00 watchdogd
```