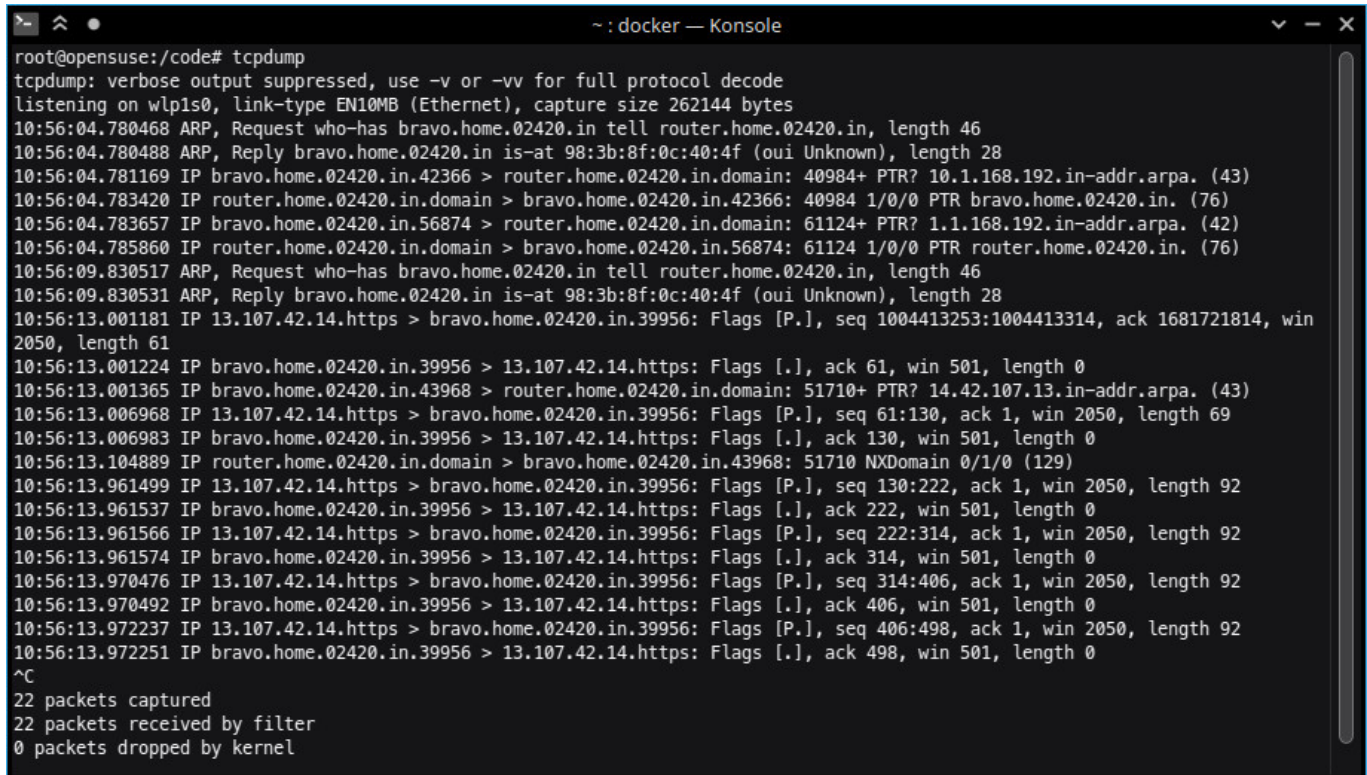


Lab 1: Network Commands

Aryan Tyagi

2019A7PS0136G

1. tcpdump

A screenshot of a terminal window titled '~: docker — Konsole'. The terminal shows the execution of the 'tcpdump' command. The output displays a series of network packets captured on the 'wlp1s0' interface. The packets include ARP requests and replies, and IP traffic from 13.107.42.14 to 13.107.42.14. The output is truncated with '^C' and summary statistics: '22 packets captured', '22 packets received by filter', and '0 packets dropped by kernel'.

```
root@opensuse:/code# tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wlp1s0, link-type EN10MB (Ethernet), capture size 262144 bytes
10:56:04.780468 ARP, Request who-has bravo.home.02420.in tell router.home.02420.in, length 46
10:56:04.780488 ARP, Reply bravo.home.02420.in is-at 98:3b:8f:0c:40:4f (oui Unknown), length 28
10:56:04.781169 IP bravo.home.02420.in.42366 > router.home.02420.in.domain: 40984+ PTR? 10.1.168.192.in-addr.arpa. (43)
10:56:04.783420 IP router.home.02420.in.domain > bravo.home.02420.in.42366: 40984 1/0/0 PTR bravo.home.02420.in. (76)
10:56:04.783657 IP bravo.home.02420.in.56874 > router.home.02420.in.domain: 61124+ PTR? 1.1.168.192.in-addr.arpa. (42)
10:56:04.785860 IP router.home.02420.in.domain > bravo.home.02420.in.56874: 61124 1/0/0 PTR router.home.02420.in. (76)
10:56:09.830517 ARP, Request who-has bravo.home.02420.in tell router.home.02420.in, length 46
10:56:09.830531 ARP, Reply bravo.home.02420.in is-at 98:3b:8f:0c:40:4f (oui Unknown), length 28
10:56:13.001181 IP 13.107.42.14.https > bravo.home.02420.in.39956: Flags [P.], seq 1004413253:1004413314, ack 1681721814, win 2050, length 61
10:56:13.001224 IP bravo.home.02420.in.39956 > 13.107.42.14.https: Flags [.], ack 61, win 501, length 0
10:56:13.001365 IP bravo.home.02420.in.43968 > router.home.02420.in.domain: 51710+ PTR? 14.42.107.13.in-addr.arpa. (43)
10:56:13.006968 IP 13.107.42.14.https > bravo.home.02420.in.39956: Flags [P.], seq 61:130, ack 1, win 2050, length 69
10:56:13.006983 IP bravo.home.02420.in.39956 > 13.107.42.14.https: Flags [.], ack 130, win 501, length 0
10:56:13.104889 IP router.home.02420.in.domain > bravo.home.02420.in.43968: 51710 NXDomain 0/1/0 (129)
10:56:13.961499 IP 13.107.42.14.https > bravo.home.02420.in.39956: Flags [P.], seq 130:222, ack 1, win 2050, length 92
10:56:13.961537 IP bravo.home.02420.in.39956 > 13.107.42.14.https: Flags [.], ack 222, win 501, length 0
10:56:13.961566 IP 13.107.42.14.https > bravo.home.02420.in.39956: Flags [P.], seq 222:314, ack 1, win 2050, length 92
10:56:13.961574 IP bravo.home.02420.in.39956 > 13.107.42.14.https: Flags [.], ack 314, win 501, length 0
10:56:13.970476 IP 13.107.42.14.https > bravo.home.02420.in.39956: Flags [P.], seq 314:406, ack 1, win 2050, length 92
10:56:13.970492 IP bravo.home.02420.in.39956 > 13.107.42.14.https: Flags [.], ack 406, win 501, length 0
10:56:13.972237 IP 13.107.42.14.https > bravo.home.02420.in.39956: Flags [P.], seq 406:498, ack 1, win 2050, length 92
10:56:13.972251 IP bravo.home.02420.in.39956 > 13.107.42.14.https: Flags [.], ack 498, win 501, length 0
^C
22 packets captured
22 packets received by filter
0 packets dropped by kernel
```

tcpdump - dump traffic on a network

tcpdump is a data-network packet analyzer. It reads packets from a network interface card and shows their source/destination addresses, size, protocol etc. It can also be used to intercept unencrypted data sent over HTTP

2. ifconfig

```
root@opensuse:/code# ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255
    inet6 fe80::42:d9ff:fe5:64c3 prefixlen 64 scopeid 0x20<link>
    ether 02:42:d9:f5:64:c3 txqueuelen 0 (Ethernet)
    RX packets 36051 bytes 2130445 (2.1 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 54295 bytes 215074292 (215.0 MB)
    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 4082 bytes 361871 (361.8 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4082 bytes 361871 (361.8 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

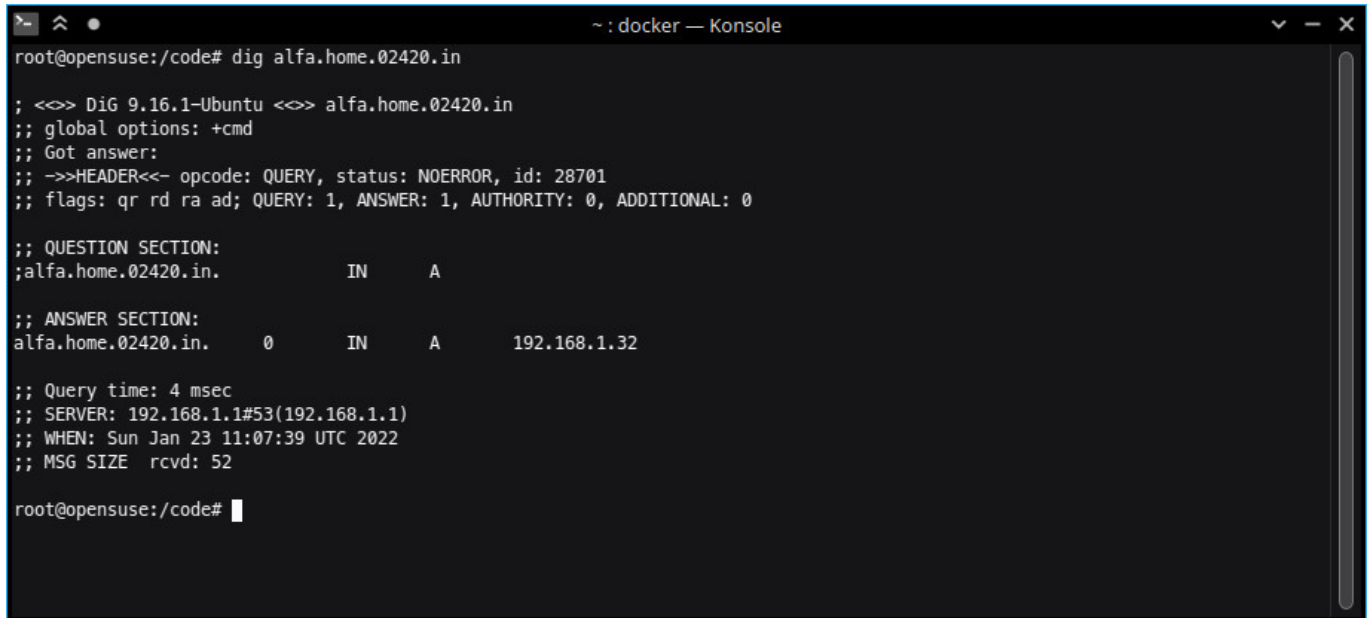
wlp1s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.10 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::559e:abf:2d2:c93f prefixlen 64 scopeid 0x20<link>
    ether 98:3b:8f:0c:40:4f txqueuelen 1000 (Ethernet)
    RX packets 1307967 bytes 1502116290 (1.5 GB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 428558 bytes 232821828 (232.8 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@opensuse:/code#
```

`ifconfig` - configure a network interface

`ifconfig` displays the status of the active network interfaces. It is commonly used to find the local IP address and MAC address of the machine. It can also be used to configure a network interface.

3. dig



```
root@opensuse:/code# dig alfa.home.02420.in

; <<>> DiG 9.16.1-Ubuntu <<>> alfa.home.02420.in
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 28701
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;alfa.home.02420.in.          IN      A

;; ANSWER SECTION:
alfa.home.02420.in.         0       IN      A      192.168.1.32

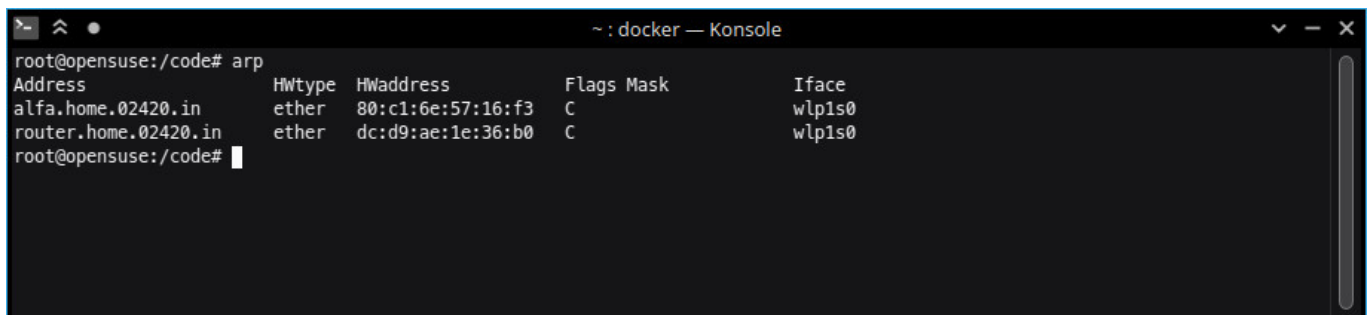
;; Query time: 4 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Sun Jan 23 11:07:39 UTC 2022
;; MSG SIZE rcvd: 52

root@opensuse:/code#
```

dig - DNS lookup utility

dig is a network administration tool for querying the Domain Name System. It displays all DNS records associated with a given domain (A, AAAA, CNAME, MX, etc) and the IP address of the server. It should not be used to test the connection since DNS lookups are often cached.

4. arp



```
root@opensuse:/code# arp
Address          HWtype  HWaddress      Flags Mask    Iface
alfa.home.02420.in ether    80:c1:6e:57:16:f3 C           wlp1s0
router.home.02420.in ether    dc:d9:ae:1e:36:b0 C           wlp1s0
root@opensuse:/code#
```

arp - manipulate the system ARP cache

ARP stands for Address Resolution Protocol, which is used to find the MAC address of device from a given IPv4 Address. arp prints the content of the ARP table. It can also be used to modify the ARP cache.

5. netstat

```
root@opensuse:/code# netstat | head -n 25
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp      0      0 bravo.home.02420.:39970 13.107.42.14:https      ESTABLISHED
tcp      0      0 bravo.home.02420.:53786 lb-140-82-112-26-:https ESTABLISHED
udp      0      0 bravo.home.02420.:34769 router.home.0242:domain ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State      I-Node  Path
unix   2      [ ]         DGRAM      CONNECTED  20245   /var/run/chrony/chronyd.sock
unix   2      [ ]         DGRAM      CONNECTED  29924   /run/user/1000/systemd/notify
unix   4      [ ]         DGRAM      CONNECTED  11422   /run/systemd/notify
unix  21      [ ]         DGRAM      CONNECTED  11432   /run/systemd/journal/dev-log
unix   7      [ ]         DGRAM      CONNECTED  11434   /run/systemd/journal/socket
unix   3      [ ]         SEQPACKET  CONNECTED  181833  @0005c
unix   3      [ ]         SEQPACKET  CONNECTED  181831  @0005b
unix   3      [ ]         SEQPACKET  CONNECTED  31144   @0000a
unix   3      [ ]         SEQPACKET  CONNECTED  169933  @0004f
unix   2      [ ]         DGRAM      CONNECTED  29806   public/postlog
unix   3      [ ]         SEQPACKET  CONNECTED  174307  @00053
unix   2      [ ]         DGRAM      CONNECTED  33114   @00010
unix   3      [ ]         SEQPACKET  CONNECTED  169935  @00050
unix   3      [ ]         SEQPACKET  CONNECTED  174309  @00054
unix   3      [ ]         SEQPACKET  CONNECTED  31142   @00009
unix   3      [ ]         STREAM     CONNECTED  187504
unix   3      [ ]         STREAM     CONNECTED  186492
unix   3      [ ]         STREAM     CONNECTED  170812
root@opensuse:/code#
```

`netstat` - Print network connections, routing tables, interface statistics, masquerade connections, and multicast memberships

`netstat` displays a list of all open ports, the applications servicing those ports and the protocol used.

6. telnet

```
~: docker — Konsole
root@opensuse:/code# telnet telehack.com
Trying 64.139.230...
Connected to telehack.com.
Escape character is '^J'.

Connected to TELEHACK port 40

It is 6:05 am on Sunday, January 23, 2022 in Mountain View, California, USA.
There are 64 local users. There are 26641 hosts on the network.

Type HELP for a detailed command list.
Type NEWUSER to create an account.

May the command line live forever.

Command, one of the following:
2048      ?      a2      ac      advent  aquarium
basic     bf      c8      cal     calc     ching
clear     clock  cowsay  echo    eliza    factor
figlet    finger fnord    geoip   help     hosts
ipaddr    joke   login    mac     md5      newuser
notes     octopus phoon    pig     ping     primes
privacy   qr      rain     rand    rfc      rig
roll      rot13  sleep    starwars traceroute typespeed
units     uptime usenet   users   uumap    uupath
uuplot    weather when     zc      zork     zrun

.
telnet> quit
Connection closed.
root@opensuse:/code#
```

telnet - user interface to the TELNET protocol

telnet command is used to communicate over the TELNET protocol (like browser is used for HTTP). TELNET is used for bidirectional communication between the host and the client. SSH should always be preferred over TELNET since it uses encryption.

7. traceroute

```
root@opensuse:/code# traceroute google.com
traceroute to google.com (142.250.193.238), 30 hops max, 60 byte packets
 1  router.home.02420.in (192.168.1.1)  1.852 ms  2.315 ms  2.756 ms
 2  223.182.79.255 (223.182.79.255)  9.325 ms  9.426 ms  9.559 ms
 3  nsg-corporate-5.30.187.122.airtel.in (122.187.30.5)  20.677 ms  nsg-corporate-9.30.187.122.airtel.in (122.187.30.9)  11.094 ms  nsg-corporate-5.30.187.122.airtel.in (122.187.30.5)  20.320 ms
 4  142.250.161.56 (142.250.161.56)  12.504 ms  142.250.168.34 (142.250.168.34)  13.280 ms  13.568 ms
 5  * * *
 6  172.253.50.152 (172.253.50.152)  13.777 ms  66.249.95.74 (66.249.95.74)  7.166 ms  142.251.54.90 (142.251.54.90)  6.837 ms
 7  108.170.251.106 (108.170.251.106)  7.949 ms  142.251.54.101 (142.251.54.101)  11.316 ms  108.170.251.98 (108.170.251.98)  12.121 ms
 8  dell1s18-in-f14.1e100.net (142.250.193.238)  11.288 ms  74.125.243.97 (74.125.243.97)  12.589 ms  dell1s18-in-f14.1e100.net (142.250.193.238)  11.888 ms
root@opensuse:/code#
```

traceroute - print the route packets trace to network host

traceroute tracks the route packets taken from a client to a given host and displays the (round-trip) transit delays between each network hop. It is similar to ping but also displays intermediate delays. It can be used over a local network to find congested nodes.

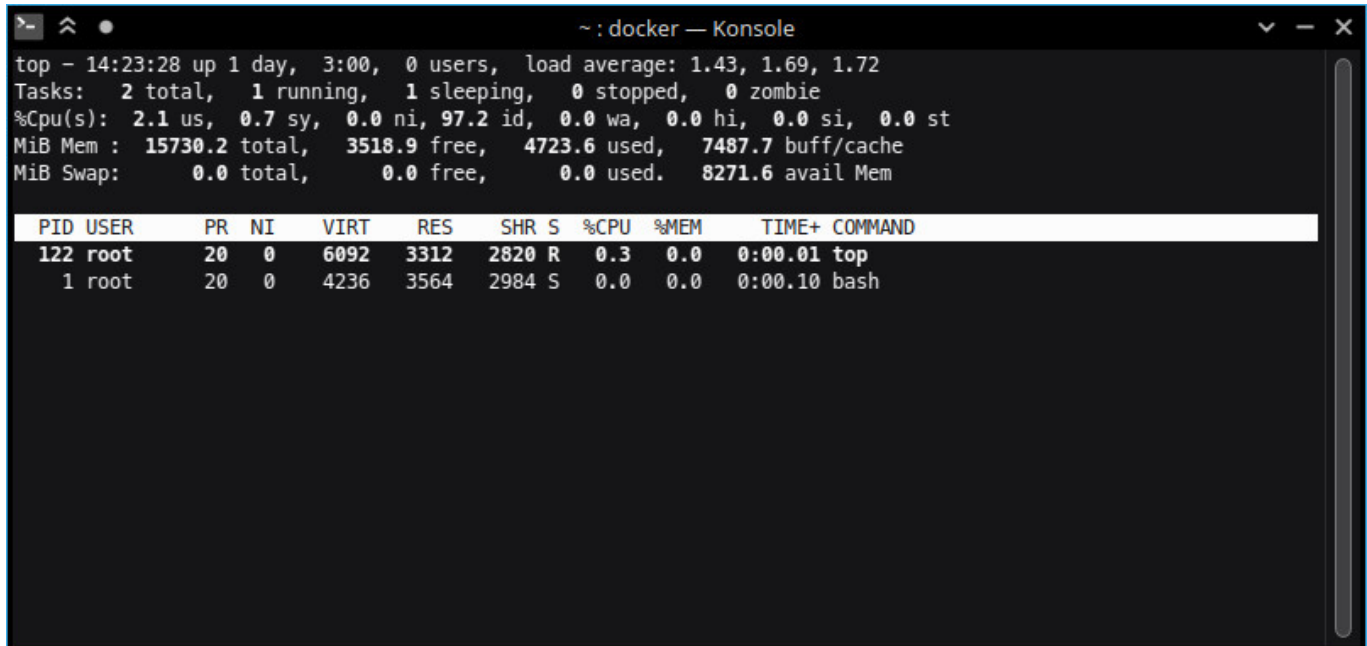
8. ping

```
root@opensuse:/code# ping alfa.home.02420.in
PING alfa.home.02420.in (192.168.1.32) 56(84) bytes of data:
 64 bytes from alfa.home.02420.in (192.168.1.32): icmp_seq=1 ttl=64 time=1.78 ms
 64 bytes from alfa.home.02420.in (192.168.1.32): icmp_seq=2 ttl=64 time=2.77 ms
 64 bytes from alfa.home.02420.in (192.168.1.32): icmp_seq=3 ttl=64 time=1.61 ms
 64 bytes from alfa.home.02420.in (192.168.1.32): icmp_seq=4 ttl=64 time=2.03 ms
 64 bytes from alfa.home.02420.in (192.168.1.32): icmp_seq=5 ttl=64 time=1.84 ms
 64 bytes from alfa.home.02420.in (192.168.1.32): icmp_seq=6 ttl=64 time=1.35 ms
^C
--- alfa.home.02420.in ping statistics ---
 6 packets transmitted, 6 received, 0% packet loss, time 5008ms
 rtt min/avg/max/mdev = 1.352/1.898/2.774/0.444 ms
root@opensuse:/code#
```

ping - send ICMP ECHO_REQUEST to network hosts

ping command is commonly used to check the reachability of a host. It continuously sends fixed sized packets to the host at regular intervals and measured the round-trip time of the when it receives a reply. It also displays the packet loss and min/max/avg rt time.

9. top



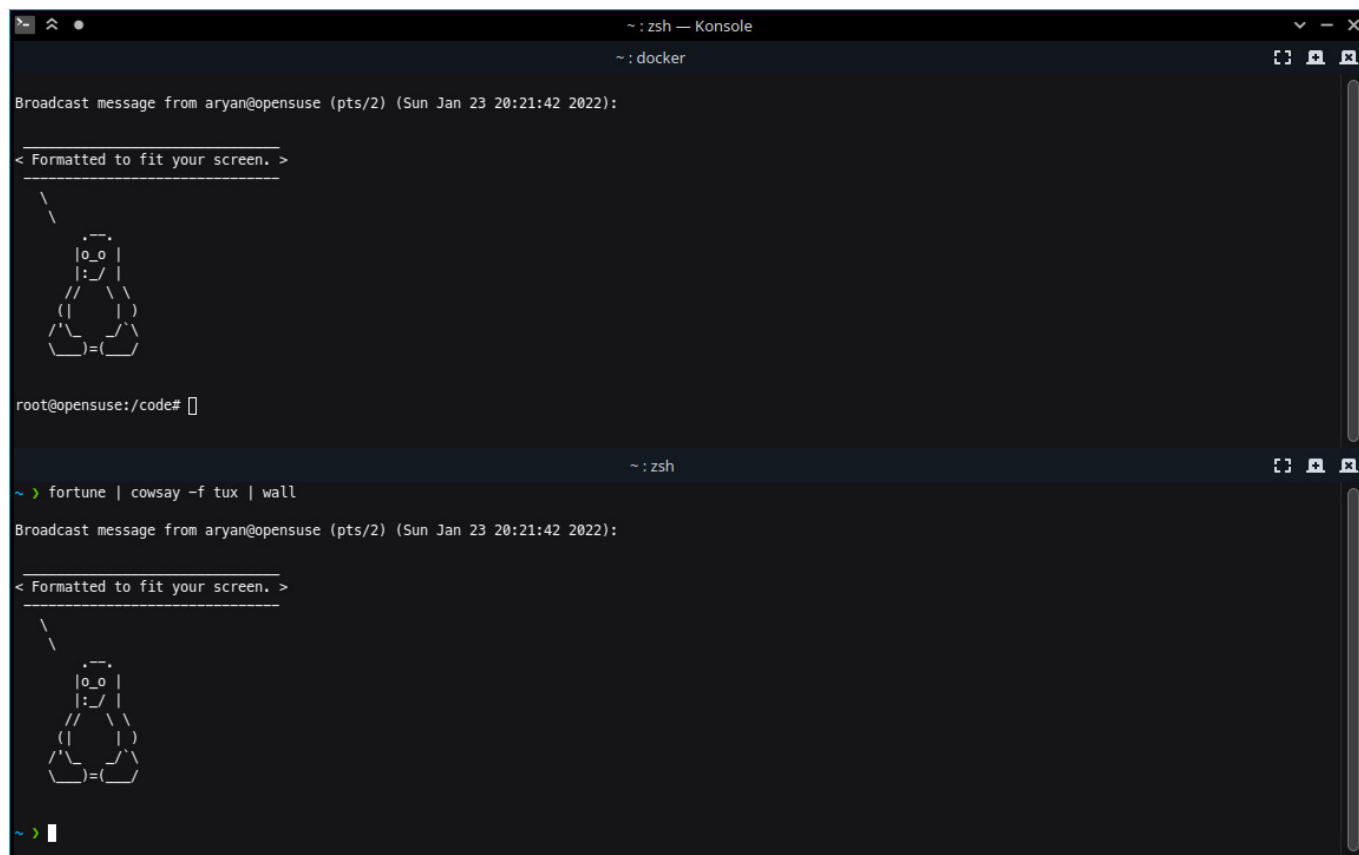
```
top - 14:23:28 up 1 day, 3:00, 0 users, load average: 1.43, 1.69, 1.72
Tasks:  2 total,  1 running,  1 sleeping,  0 stopped,  0 zombie
%Cpu(s):  2.1 us,  0.7 sy,  0.0 ni, 97.2 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
MiB Mem : 15730.2 total,  3518.9 free,  4723.6 used,  7487.7 buff/cache
MiB Swap:   0.0 total,   0.0 free,   0.0 used.  8271.6 avail Mem

  PID USER      PR  NI   VIRT   RES   SHR  S  %CPU  %MEM     TIME+ COMMAND
  122 root        20   0   6092   3312  2820  R   0.3   0.0   0:00.01 top
    1 root        20   0   4236   3564  2984  S   0.0   0.0   0:00.10 bash
```

top - display Linux processes

top displays a dynamic real-time view of a running system. It displays system summary information (CPU, RAM) as well as a list of processes/threads, their types (running/waiting), size, and resource usage.

10. wall



The image shows two terminal windows side-by-side. The top window is titled '~: zsh — Konsole' and shows a broadcast message from 'aryan@opensuse (pts/2) (Sun Jan 23 20:21:42 2022):'. Below the message, it says '< Formatted to fit your screen. >' and displays a ASCII art of a cow. The bottom window is titled '~: zsh' and shows the command 'fortune | cowsay -f tux | wall' being executed. It also shows the same broadcast message and ASCII art cow.

```
~: zsh — Konsole
~: docker

Broadcast message from aryan@opensuse (pts/2) (Sun Jan 23 20:21:42 2022):

< Formatted to fit your screen. >

      /\
     /--\
    |o_o |
    |:~|
   //~~\\
  ( (    )\
  /(\____)\(\
   \_____/=(\

root@opensuse:/code#

~: zsh

~ > fortune | cowsay -f tux | wall

Broadcast message from aryan@opensuse (pts/2) (Sun Jan 23 20:21:42 2022):

< Formatted to fit your screen. >

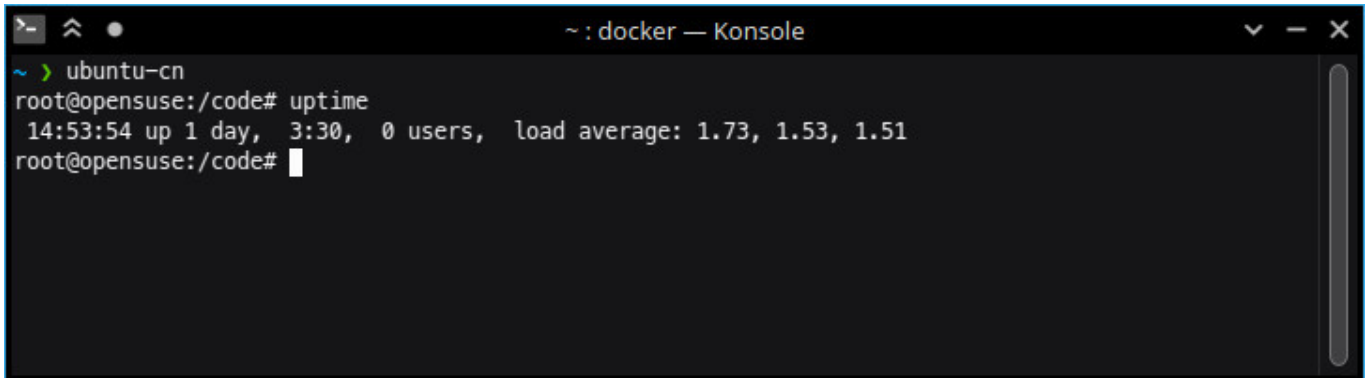
      /\
     /--\
    |o_o |
    |:~|
   //~~\\
  ( (    )\
  /(\____)\(\
   \_____/=(\

~ >
```

wall - write a message to all users

wall displays a message on the terminals of all currently logged in users.

11. uptime

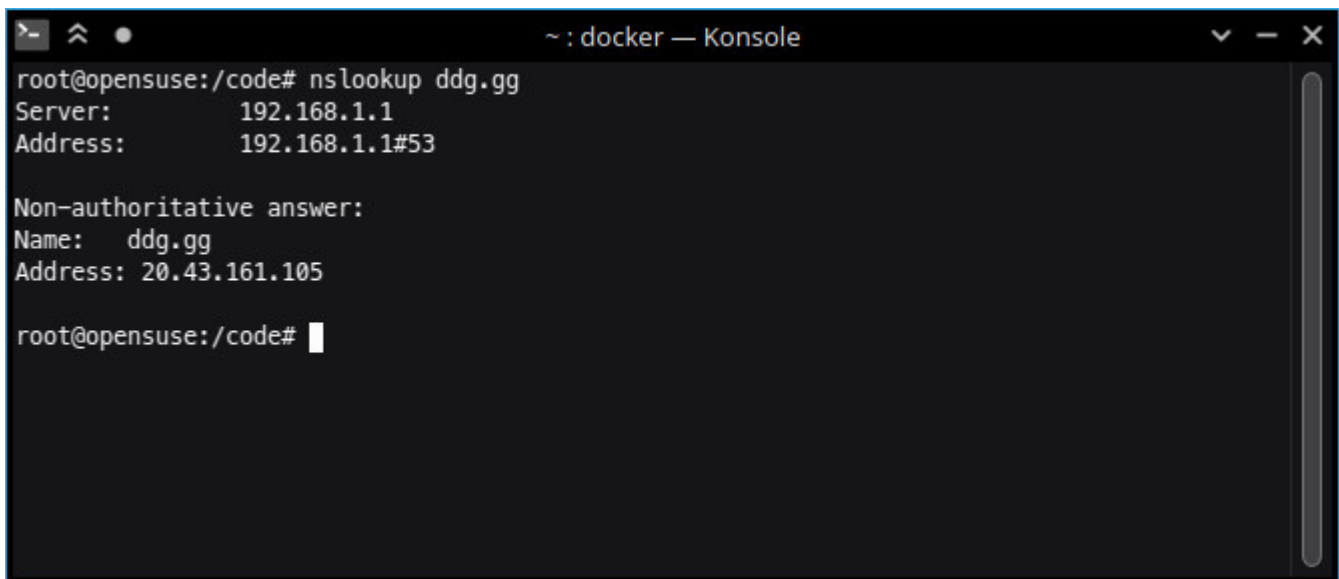
A terminal window titled '~: docker — Konsole' showing the execution of the 'uptime' command. The prompt is 'root@opensuse:/code#'. The output is '14:53:54 up 1 day, 3:30, 0 users, load average: 1.73, 1.53, 1.51'.

```
> ^ ● ~: docker — Konsole ~ > ubuntu-cn root@opensuse:/code# uptime 14:53:54 up 1 day, 3:30, 0 users, load average: 1.73, 1.53, 1.51 root@opensuse:/code#
```

uptime - Tell how long the system has been running.

uptime command displays 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. This information is also the very first line of the top command

12. nslookup

A terminal window titled '~: docker — Konsole' showing the execution of the 'nslookup ddg.gg' command. The prompt is 'root@opensuse:/code#'. The output shows the server and address used for the query, followed by a non-authoritative answer for the domain 'ddg.gg' with IP address '20.43.161.105'.

```
> ^ ● ~: docker — Konsole root@opensuse:/code# nslookup ddg.gg Server: 192.168.1.1 Address: 192.168.1.1#53 Non-authoritative answer: Name: ddg.gg Address: 20.43.161.105 root@opensuse:/code#
```

nslookup - query Internet name servers interactively

nslookup is a program to find the IP address associated with the given domain name. it can also be used to query other DNS records. DNS is split into multiple zones each with its own authoritative servers. DNS is often cached and here we receive the answer from a non-authoritative source.