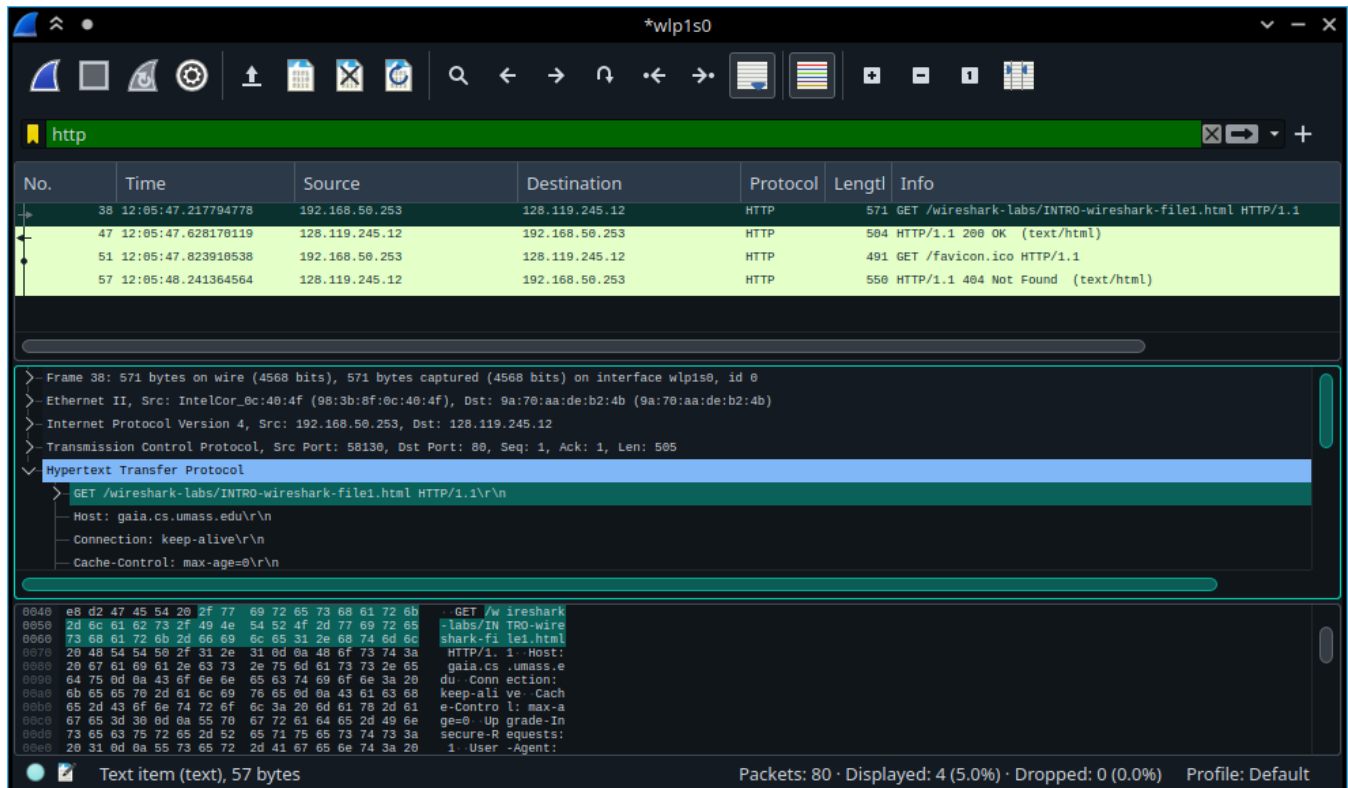


Lab 2: Introduction to Wireshark and Use of Network Commands

Aryan Tyagi

2019A7PS0136G



```
38      12:05:47.217794778      192.168.50.253  128.119.245.12  HTTP      571      GET
/wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
47      12:05:47.628170119      128.119.245.12  192.168.50.253  HTTP      504      HTTP/1.1 200
OK (text/html)
```

1. protocols available in the unfiltered packet-listing window

HTTP, TCP, NTP

2. Delay between HTTP GET and HTTP OK

about 410 ms

3. Internet address of the gaia.cs.umass.edu

gaia.cs.umass.edu: 128.119.245.12

my computer: 192.168.50.253 (only local ip is captured)

4. HTTP messages

No.	Time	Source	Destination	Protocol	Length	Info
1	12:05:47.217794778	192.168.50.253	128.119.245.12	HTTP	571	GET

/wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1

Frame 1: 571 bytes on wire (4568 bits), 571 bytes captured (4568 bits) on interface wlp1s0, id 0

Ethernet II, Src: IntelCor_0c:40:4f (98:3b:8f:0c:40:4f), Dst: 9a:70:aa:de:b2:4b (9a:70:aa:de:b2:4b)

Internet Protocol Version 4, Src: 192.168.50.253, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 58130, Dst Port: 80, Seq: 1, Ack: 1, Len: 505

Hypertext Transfer Protocol

GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n

Host: gaia.cs.umass.edu\r\n

Connection: keep-alive\r\n

Cache-Control: max-age=0\r\n

Upgrade-Insecure-Requests: 1\r\n

User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)

Chrome/96.0.4664.110 Safari/537.36\r\n

Accept:

text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n

Sec-GPC: 1\r\n

Accept-Encoding: gzip, deflate\r\n

Accept-Language: en-US,en;q=0.9\r\n

\r\n

[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]

[HTTP request 1/1]

[Response in frame: 2]

No.	Time	Source	Destination	Protocol	Length	Info
2	12:05:47.628170119	128.119.245.12	192.168.50.253	HTTP	504	

HTTP/1.1 200 OK (text/html)

Frame 2: 504 bytes on wire (4032 bits), 504 bytes captured (4032 bits) on interface wlp1s0, id 0

Ethernet II, Src: 9a:70:aa:de:b2:4b (9a:70:aa:de:b2:4b), Dst: IntelCor_0c:40:4f (98:3b:8f:0c:40:4f)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.50.253

Transmission Control Protocol, Src Port: 80, Dst Port: 58130, Seq: 1, Ack: 506, Len: 438

Hypertext Transfer Protocol

HTTP/1.1 200 OK\r\n

Date: Mon, 31 Jan 2022 06:35:47 GMT\r\n

Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.27 mod_perl/2.0.11

Perl/v5.16.3\r\n

Last-Modified: Mon, 31 Jan 2022 06:35:01 GMT\r\n

ETag: "51-5d6dafbedd427"\r\n

Accept-Ranges: bytes\r\n

Content-Length: 81\r\n

Keep-Alive: timeout=5, max=100\r\n

Connection: Keep-Alive\r\n

Content-Type: text/html; charset=UTF-8\r\n

\r\n

[HTTP response 1/1]

[Time since request: 0.410375341 seconds]

[Request in frame: 1]

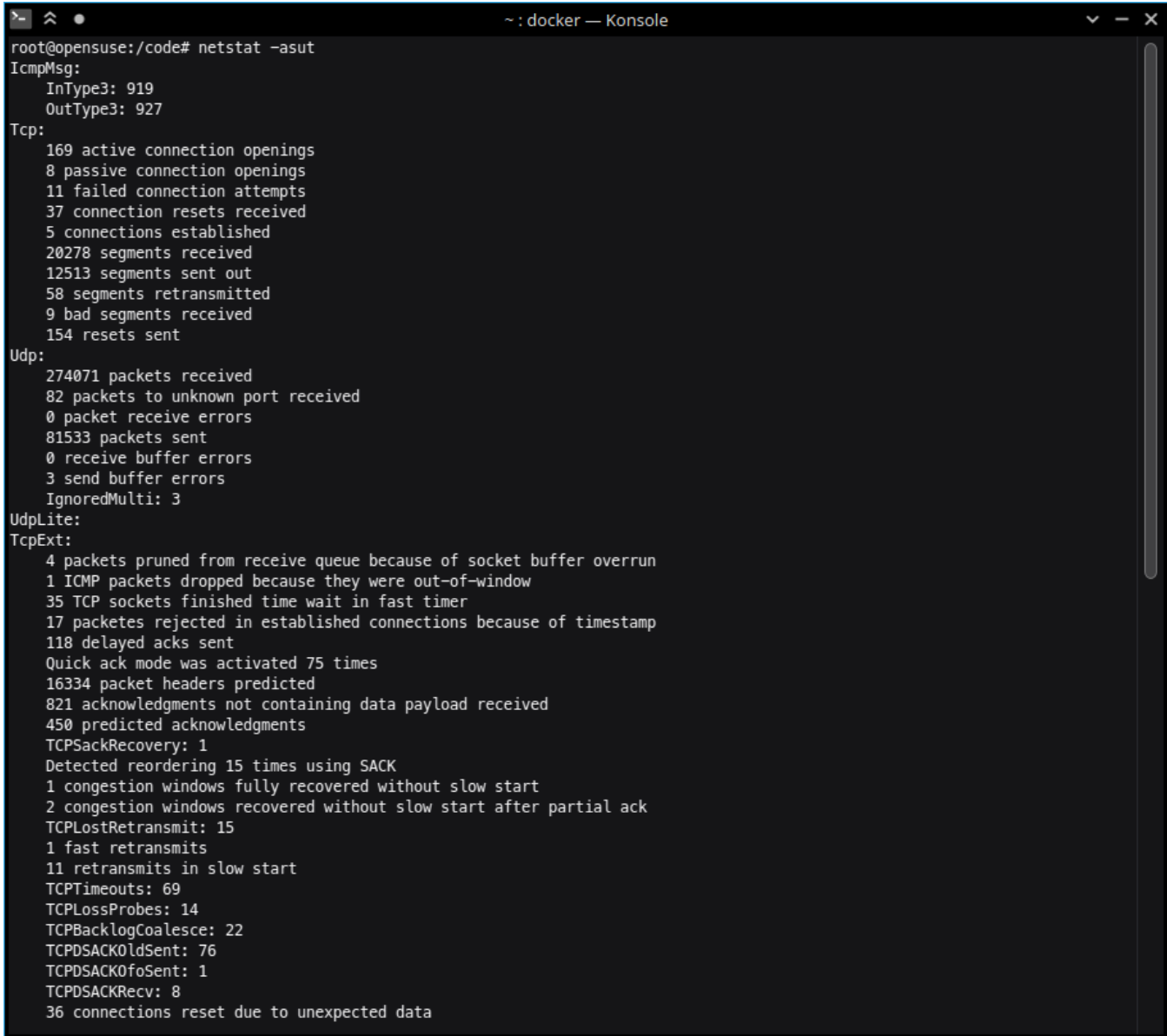
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]

File Data: 81 bytes

Line-based text data: text/html (3 lines)

5. Statistics of TCP and UDP ports on Linux machine

```
netstat -asut
# -a --all           Show both listening and non-listening sockets
# -s --statistics    Display summary statistics for each protocol
# -t --tcp
# -u --udp
```



The screenshot shows a terminal window titled '~: docker — Konsole'. The user is at the prompt 'root@opensuse:/code#'. They have entered the command 'netstat -asut'. The output is as follows:

```
root@opensuse:/code# netstat -asut
IcmpMsg:
  InType3: 919
  OutType3: 927
Tcp:
  169 active connection openings
  8 passive connection openings
  11 failed connection attempts
  37 connection resets received
  5 connections established
  20278 segments received
  12513 segments sent out
  58 segments retransmitted
  9 bad segments received
  154 resets sent
Udp:
  274071 packets received
  82 packets to unknown port received
  0 packet receive errors
  81533 packets sent
  0 receive buffer errors
  3 send buffer errors
  IgnoredMulti: 3
UdpLite:
TcpExt:
  4 packets pruned from receive queue because of socket buffer overrun
  1 ICMP packets dropped because they were out-of-window
  35 TCP sockets finished time wait in fast timer
  17 packetes rejected in established connections because of timestamp
  118 delayed acks sent
  Quick ack mode was activated 75 times
  16334 packet headers predicted
  821 acknowledgments not containing data payload received
  450 predicted acknowledgments
  TCPSackRecovery: 1
  Detected reordering 15 times using SACK
  1 congestion windows fully recovered without slow start
  2 congestion windows recovered without slow start after partial ack
  TCPLostRetransmit: 15
  1 fast retransmits
  11 retransmits in slow start
  TCPTimeouts: 69
  TCPLossProbes: 14
  TCPBacklogCoalesce: 22
  TCPDSACKOldSent: 76
  TCPDSACKOfoSent: 1
  TCPDSACKRecv: 8
  36 connections reset due to unexpected data
```

6. List the listening ports on your machine

```
netstat -s1
# -a --all           List both servers and established connections
# -l --listening     Show only listening sockets
```

```
root@opensuse:/code# netstat -al
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:smtp          0.0.0.0:*               LISTEN
tcp        0      0 localhost:ipp           0.0.0.0:*               LISTEN
tcp        0      0 bravo.home.02420.:47702 whatsapp-cdn-shv--https ESTABLISHED
tcp6       0      0 [::]:1716              [::]:*                  LISTEN
tcp6       0      0 [::]:3000              [::]:*                  LISTEN
tcp6       0      0 localhost:ipp           [::]:*                  LISTEN
tcp6       0      0 localhost:smtp          [::]:*                  LISTEN
udp        0      0 0.0.0.0:37583           0.0.0.0:*               LISTEN
udp        0      0 224.0.0.251:mdns       0.0.0.0:*               LISTEN
udp        0      0 0.0.0.0:mdns           0.0.0.0:*               LISTEN
udp        0      0 0.0.0.0:bootpc         0.0.0.0:*               LISTEN
udp        0      0 0.0.0.0:57612          0.0.0.0:*               LISTEN
udp        0      0 localhost:323           0.0.0.0:*               LISTEN
udp        0      0 bravo.home.02420.:41692 del12s02-in-f14.1e1:443 ESTABLISHED
udp        0      0 0.0.0.0:41854           0.0.0.0:*               LISTEN
udp        0      0 bravo.home.02420.:34400 del11s20-in-f14.1e1:443 ESTABLISHED
udp        0      0 bravo.home.02420.:59736 del12s09-in-f1.1e10:443 ESTABLISHED
udp        0      0 0.0.0.0:35234           0.0.0.0:*               LISTEN
udp6       0      0 [::]:mdns              [::]:*                  LISTEN
udp6       0      0 [::]:40776              [::]:*                  LISTEN
udp6       0      0 [::]:41026              [::]:*                  LISTEN
udp6       0      0 [::]:57512              [::]:*                  LISTEN
udp6       0      0 localhost:323           [::]:*                  LISTEN
udp6       0      0 [::]:50729              [::]:*                  LISTEN
udp6       0      0 [::]:1716               [::]:*                  LISTEN
raw6       0      0 [::]:ipv6-icmp          [::]:*                  LISTEN
7

Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State       I-Node      Path
unix   2      [ ACC ] STREAM    LISTENING   29825       @/tmp/.ICE-unix/1986
unix   2      [ ACC ] STREAM    LISTENING   22542       /run/mcelog/mcelog-client
unix   2      [ ACC ] STREAM    LISTENING   16815       /run/avahi-daemon/socket
unix   2      [ ACC ] STREAM    LISTENING   16817       /run/cups/cups.sock
unix   2      [ ACC ] STREAM    LISTENING   16819       /run/dbus/system_bus_socket
unix   2      [ ACC ] STREAM    LISTENING   16821       /run/pcscd/pcscd.comm
unix   2      [ ]       DGRAM     LISTENING   23281       /run/user/1000/systemd/notify
unix   2      [ ACC ] STREAM    LISTENING   16195       /tmp/sddm-auth9db85346-c55a-4f07-a13a-a72182593f71
unix   2      [ ACC ] STREAM    LISTENING   23284       /run/user/1000/systemd/private
unix   2      [ ACC ] STREAM    LISTENING   26646       /tmp/.X11-unix/X0
unix   2      [ ACC ] STREAM    LISTENING   23289       /run/user/1000/bus
unix   2      [ ACC ] STREAM    LISTENING   27671       /tmp/.PlKHRk/s
unix   2      [ ACC ] STREAM    LISTENING   24343       private/rewrite
unix   2      [ ACC ] STREAM    LISTENING   23291       /run/user/1000/pulse/native
unix   2      [ ACC ] STREAM    LISTENING   23293       /run/user/1000/pipewire-0
unix   4      [ ]       DGRAM     CONNECTED   15364       /run/systemd/notify
unix   2      [ ACC ] STREAM    LISTENING   30722       /tmp/ssh-XXXXXXLtoZ0c/agent.1816
```

7. MX record for www.gmail.com

```
dig gmail.com mx
```

```
root@opensuse:/code# dig gmail.com mx

; <<> DiG 9.16.1-Ubuntu <<> gmail.com mx
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 55421
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;gmail.com.                IN      MX

;; ANSWER SECTION:
gmail.com.                3582    IN      MX      30 alt3.gmail-smtp-in.l.google.com.
gmail.com.                3582    IN      MX      20 alt2.gmail-smtp-in.l.google.com.
gmail.com.                3582    IN      MX      5  gmail-smtp-in.l.google.com.
gmail.com.                3582    IN      MX      40 alt4.gmail-smtp-in.l.google.com.
gmail.com.                3582    IN      MX      10 alt1.gmail-smtp-in.l.google.com.

;; Query time: 8 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Mon Jan 31 05:40:22 UTC 2022
;; MSG SIZE rcvd: 161

root@opensuse:/code#
```

8. Display the all network interfaces on your machine

```
netstat -aie                                Show interfaces that are not up
# -a --all                                  Display a table of all network interfaces.
# -i --interface
# OR
ifconfig -a                                Display all interfaces which are currently available,
# -a                                         even if down
```

```
root@opensuse:/code# ifconfig -a
docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255
    ether 02:42:e1:53:53:96 txqueuelen 0 (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 2303 bytes 17658106 (17.6 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 2303 bytes 17658106 (17.6 MB)
    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 352769 bytes 180250062 (180.2 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 104416 bytes 15617043 (15.6 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@opensuse:/code#
```

9. List of intermediate routers to reach 8.8.8.8 and read latency

```
traceroute 8.8.8.8
```

```
root@opensuse:/code# traceroute 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1 router.home.02420.in (192.168.1.1)  5.762 ms  5.721 ms  5.802 ms
 2 223.182.79.255 (223.182.79.255)  11.233 ms  11.445 ms  11.370 ms
 3 nsg-corporate-5.30.187.122.airtel.in (122.187.30.5)  70.658 ms nsg-corporate-9.30.187.122.airtel.in (122.187.30.9)  70.608 ms  70.554 ms
 4 72.14.243.0 (72.14.243.0)  70.503 ms  70.451 ms  70.402 ms
 5 74.125.243.97 (74.125.243.97)  67.463 ms 74.125.244.193 (74.125.244.193)  70.296 ms *
 6 dns.google (8.8.8.8)  67.312 ms 142.251.52.207 (142.251.52.207)  66.540 ms 64.233.174.71 (64.233.174.71)  8.628 ms
root@opensuse:/code#
```

Each line of the output shows a network hop. The IP address of the routers is listed inside brackets. 3 separate time values are also displayed. These are the round-trip time delays and are used to find consistencies. * represents a timeout.

10. Send 10 Echo requests to 8.8.8.8

```
ping -c 10 8.8.8.8
# -c <count>
```

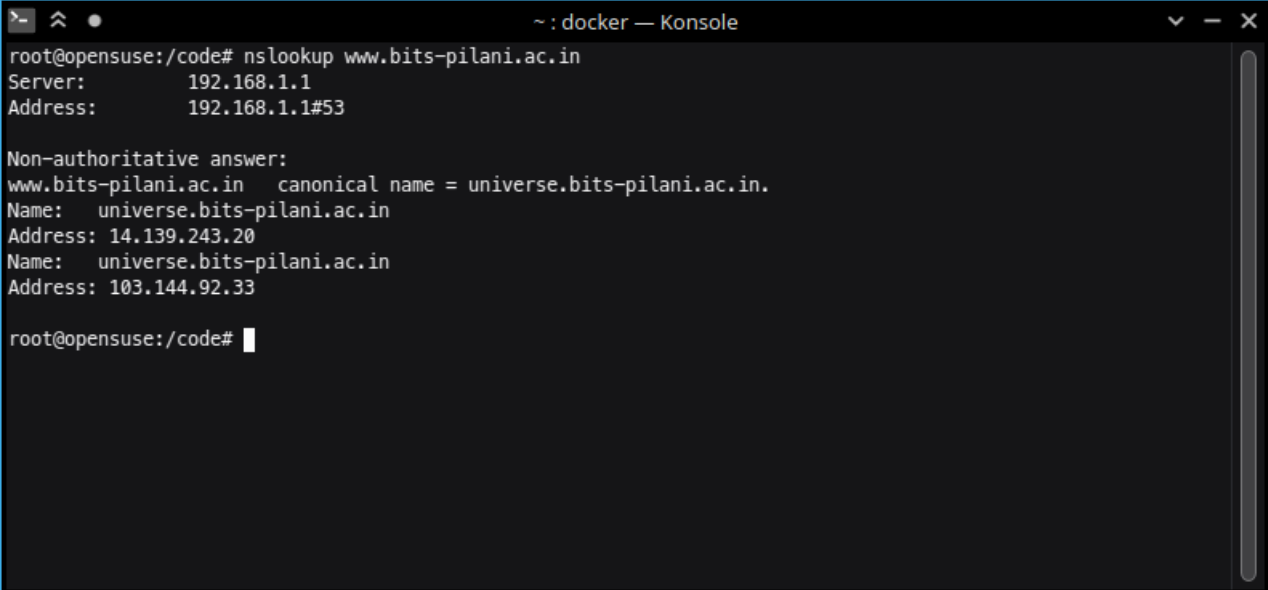
Stop after sending count ECHO_REQUEST packets.

```
root@opensuse:/code# ping -c 10 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=119 time=127 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=119 time=67.4 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=119 time=13.0 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=119 time=7.84 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=119 time=7.76 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=119 time=9.09 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=119 time=8.08 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=119 time=7.99 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=119 time=8.10 ms
64 bytes from 8.8.8.8: icmp_seq=10 ttl=119 time=12.7 ms

--- 8.8.8.8 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9010ms
rtt min/avg/max/mdev = 7.763/26.855/126.561/37.515 ms
root@opensuse:/code#
```

11. Get the IP address of www.bits-pilani.ac.in

```
host www.bits-pilani.ac.in
# OR
nslookup www.bits-pilani.ac.in
```

A terminal window titled '~ : docker — Konsole' showing the output of the 'nslookup www.bits-pilani.ac.in' command. The output displays the server IP (192.168.1.1), the address (192.168.1.1#53), and a non-authoritative answer indicating a canonical name 'universe.bits-pilani.ac.in' with two IP addresses: 14.139.243.20 and 103.144.92.33.

```
root@opensuse:/code# nslookup www.bits-pilani.ac.in
Server:      192.168.1.1
Address:     192.168.1.1#53

Non-authoritative answer:
www.bits-pilani.ac.in canonical name = universe.bits-pilani.ac.in.
Name:   universe.bits-pilani.ac.in
Address: 14.139.243.20
Name:   universe.bits-pilani.ac.in
Address: 103.144.92.33

root@opensuse:/code#
```

The domain `www.bits-pilani.ac.in` is aliased to `universe.bits-pilani.ac.in` which has two different IP addresses `103.144.92.33` and `14.139.243.20`. The browser can choose to connect to any of the IP. This is used for load-balancing and fault-tolerance.