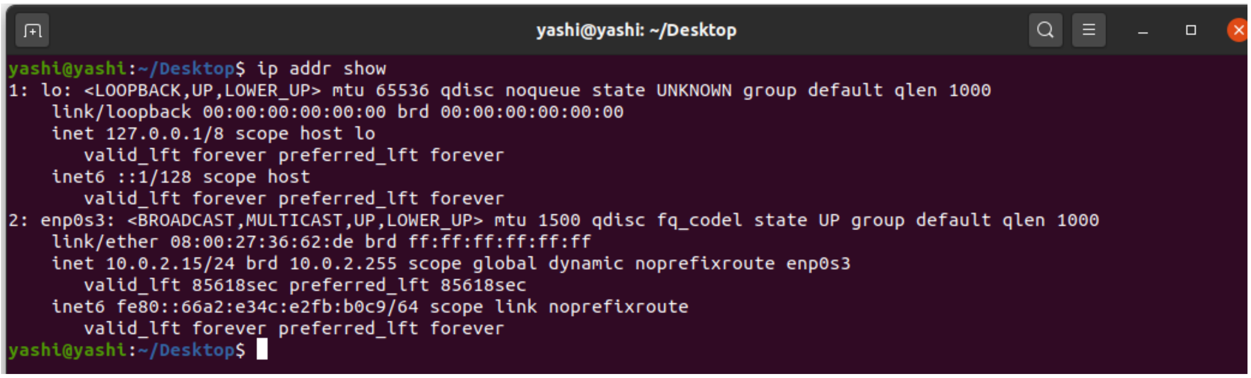
Computer Networks Lab - Week 1

PES1UG19CS592

Yashi Chawla

1. Linux Interface Configuration

1.1 ip addr show

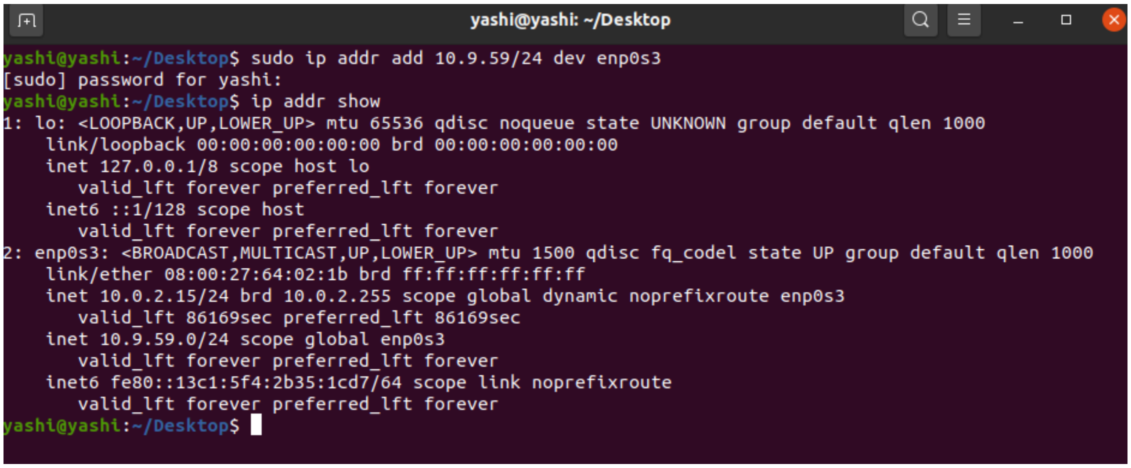


```
yashi@yashi:~/Desktop$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:36:62:de brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
       valid_lft 85618sec preferred_lft 85618sec
    inet6 fe80::66a2:e34c:e2fb:b0c9/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
yashi@yashi:~/Desktop$
```

Interface Name	IPv4/IPv6	MAC address
lo	127.0.0.1/::1	00:00:00:00:00:00
enp0s3	10.0.2.15/fe80::66a2:e34c:e2fb:b0c9	08:00:27:36:62:de

1.2 Assigning an IP

Command used: sudo ip addr add 10.0.9.59/24 dev enp0s3



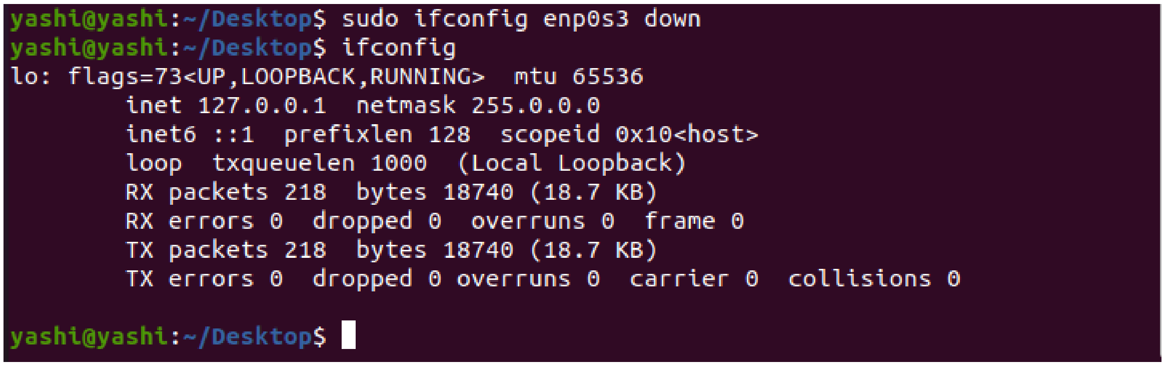
```
yashi@yashi:~/Desktop$ sudo ip addr add 10.9.59/24 dev enp0s3
[sudo] password for yashi:
yashi@yashi:~/Desktop$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:64:02:1b brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
       valid_lft 86169sec preferred_lft 86169sec
    inet 10.9.59.0/24 scope global enp0s3
       valid_lft forever preferred_lft forever
    inet6 fe80::13c1:5f4:2b35:1cd7/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
yashi@yashi:~/Desktop$
```

inet 10.0.9.59/24 scope global enp0s3

1.3 Activating and Deactivating Network Interfaces

1.3.1 Deactivating enp0s3

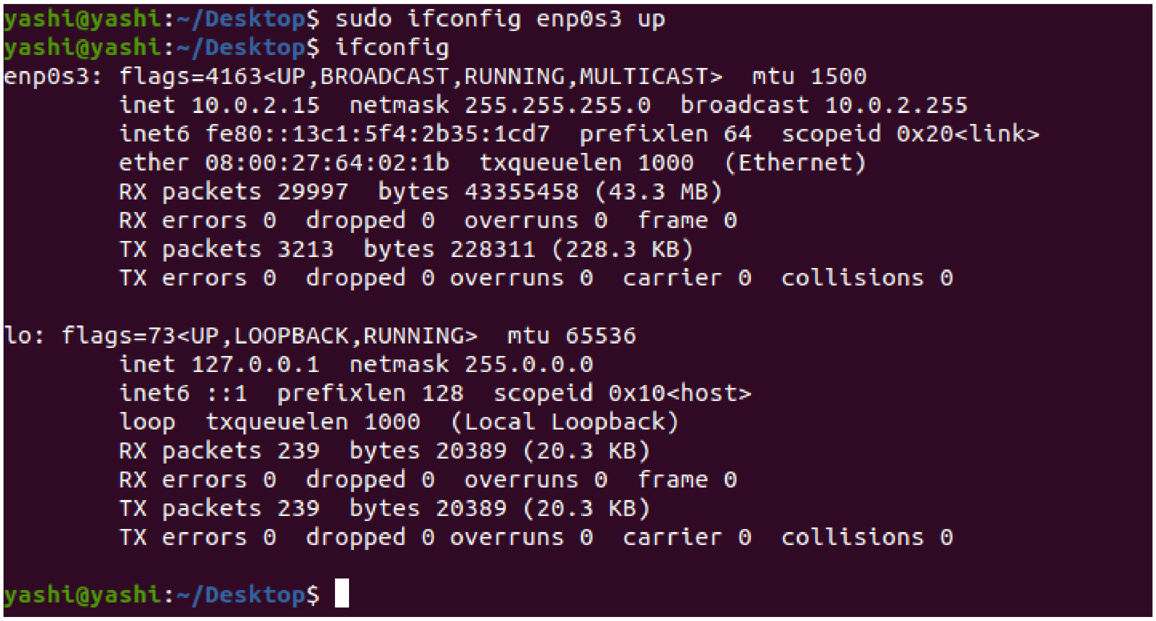
Command used: sudo ifconfig enp0s3 down



```
yashi@yashi:~/Desktop$ sudo ifconfig enp0s3 down
yashi@yashi:~/Desktop$ ifconfig
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 218  bytes 18740 (18.7 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 218  bytes 18740 (18.7 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

yashi@yashi:~/Desktop$ 
```

Only lo is displayed above

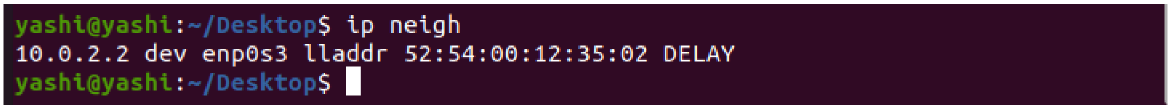
1.3.2 Activating enp0s3



```
yashi@yashi:~/Desktop$ sudo ifconfig enp0s3 up
yashi@yashi:~/Desktop$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::13c1:5f4:2b35:1cd7  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:64:02:1b  txqueuelen 1000  (Ethernet)
        RX packets 29997  bytes 43355458 (43.3 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3213  bytes 228311 (228.3 KB)
        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 239  bytes 20389 (20.3 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 239  bytes 20389 (20.3 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

yashi@yashi:~/Desktop$ 
```

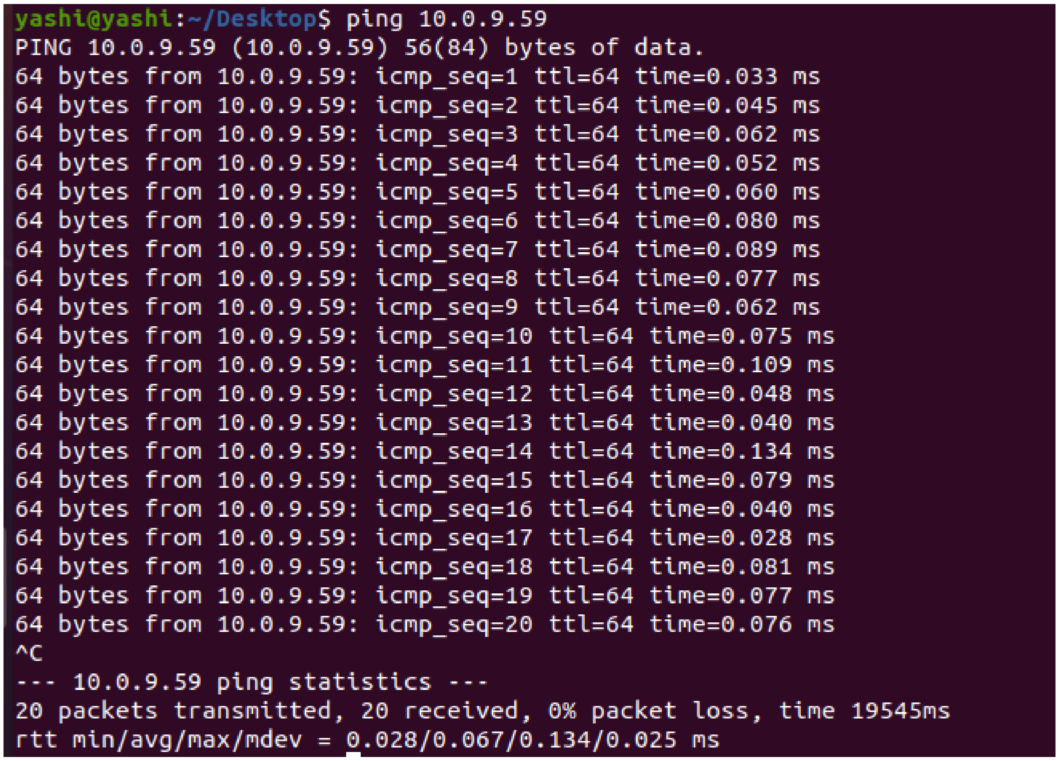
enp0s3 has been activated

1.4 Step4- ip neigh



```
yashi@yashi:~/Desktop$ ip neigh
10.0.2.2 dev enp0s3 lladdr 52:54:00:12:35:02 DELAY
yashi@yashi:~/Desktop$ 
```

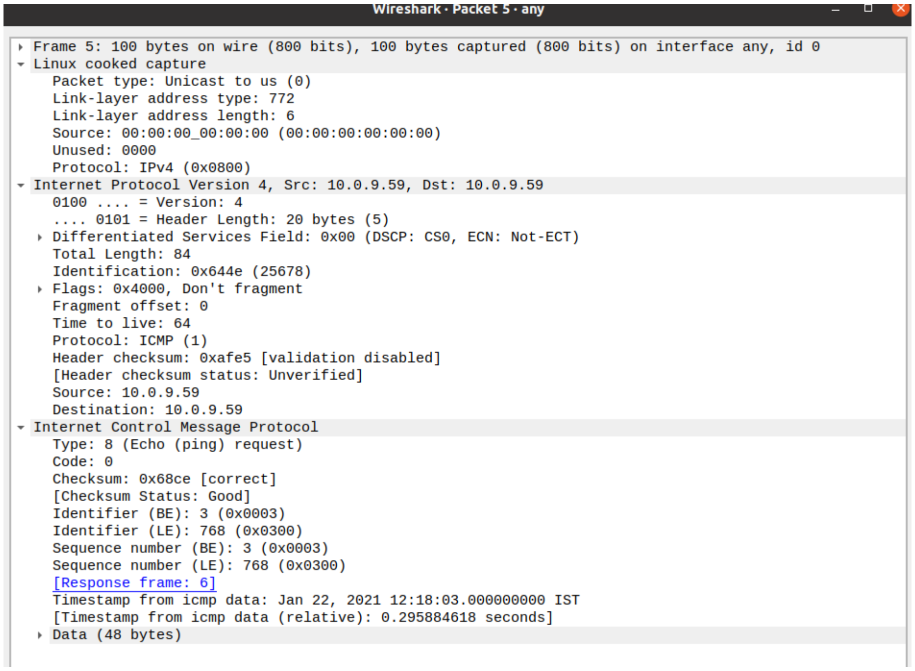
2. Ping PDU (Packet Data Units) Capture



```
yashi@yashi:~/Desktop$ ping 10.0.9.59
PING 10.0.9.59 (10.0.9.59) 56(84) bytes of data.
64 bytes from 10.0.9.59: icmp_seq=1 ttl=64 time=0.033 ms
64 bytes from 10.0.9.59: icmp_seq=2 ttl=64 time=0.045 ms
64 bytes from 10.0.9.59: icmp_seq=3 ttl=64 time=0.062 ms
64 bytes from 10.0.9.59: icmp_seq=4 ttl=64 time=0.052 ms
64 bytes from 10.0.9.59: icmp_seq=5 ttl=64 time=0.060 ms
64 bytes from 10.0.9.59: icmp_seq=6 ttl=64 time=0.080 ms
64 bytes from 10.0.9.59: icmp_seq=7 ttl=64 time=0.089 ms
64 bytes from 10.0.9.59: icmp_seq=8 ttl=64 time=0.077 ms
64 bytes from 10.0.9.59: icmp_seq=9 ttl=64 time=0.062 ms
64 bytes from 10.0.9.59: icmp_seq=10 ttl=64 time=0.075 ms
64 bytes from 10.0.9.59: icmp_seq=11 ttl=64 time=0.109 ms
64 bytes from 10.0.9.59: icmp_seq=12 ttl=64 time=0.048 ms
64 bytes from 10.0.9.59: icmp_seq=13 ttl=64 time=0.040 ms
64 bytes from 10.0.9.59: icmp_seq=14 ttl=64 time=0.134 ms
64 bytes from 10.0.9.59: icmp_seq=15 ttl=64 time=0.079 ms
64 bytes from 10.0.9.59: icmp_seq=16 ttl=64 time=0.040 ms
64 bytes from 10.0.9.59: icmp_seq=17 ttl=64 time=0.028 ms
64 bytes from 10.0.9.59: icmp_seq=18 ttl=64 time=0.081 ms
64 bytes from 10.0.9.59: icmp_seq=19 ttl=64 time=0.077 ms
64 bytes from 10.0.9.59: icmp_seq=20 ttl=64 time=0.076 ms
^C
--- 10.0.9.59 ping statistics ---
20 packets transmitted, 20 received, 0% packet loss, time 19545ms
rtt min/avg/max/mdev = 0.028/0.067/0.134/0.025 ms
```

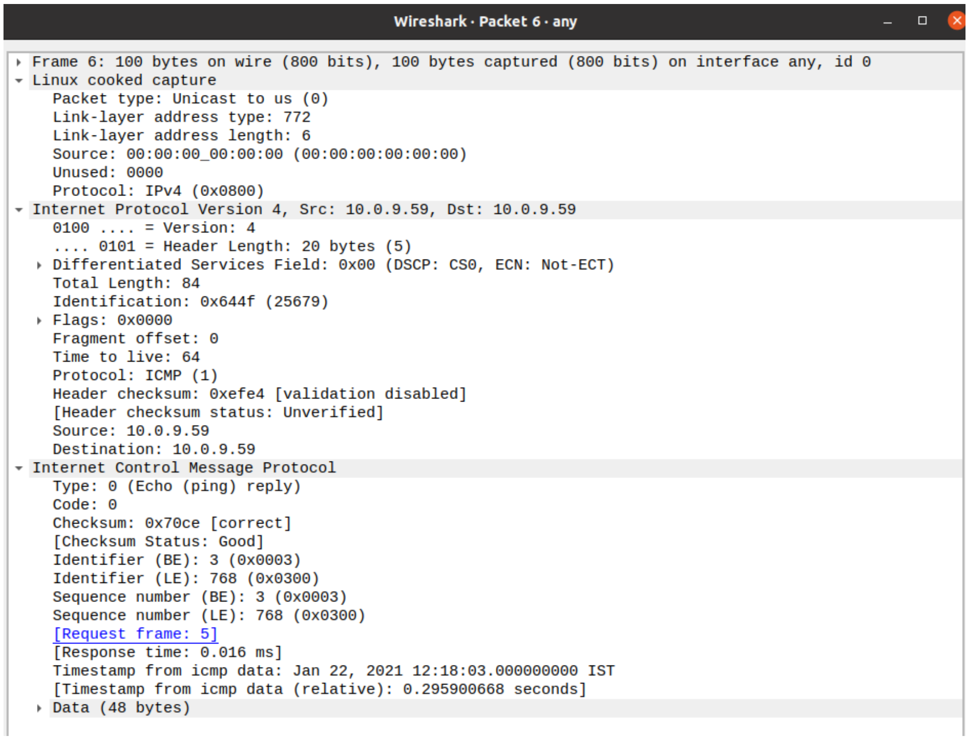
Ping 10.0.9.59

TTL	64
Protocol used by ping	ICMP
Time	Order of 10^{-2} ms



```
▸ Frame 5: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface any, id 0
▾ Linux cooked capture
    Packet type: Unicast to us (0)
    Link-layer address type: 772
    Link-layer address length: 6
    Source: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Unused: 0000
    Protocol: IPv4 (0x0800)
▾ Internet Protocol Version 4, Src: 10.0.9.59, Dst: 10.0.9.59
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x644e (25678)
  ▸ Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 64
    Protocol: ICMP (1)
    Header checksum: 0xafe5 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.0.9.59
    Destination: 10.0.9.59
▾ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x68ce [correct]
    [Checksum Status: Good]
    Identifier (BE): 3 (0x0003)
    Identifier (LE): 768 (0x0300)
    Sequence number (BE): 3 (0x0003)
    Sequence number (LE): 768 (0x0300)
    [Response frame: 6]
    Timestamp from icmp data: Jan 22, 2021 12:18:03.000000000 IST
    [Timestamp from icmp data (relative): 0.295884618 seconds]
  ▸ Data (48 bytes)
```

Request Packet

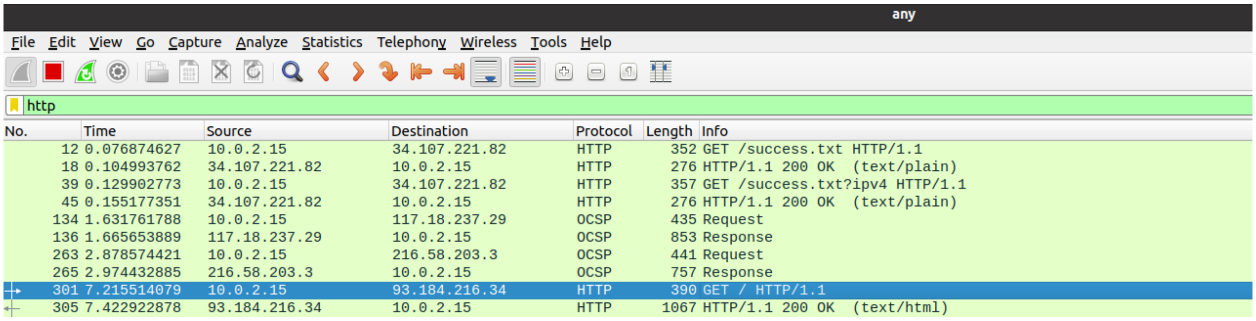


```
▸ Frame 6: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface any, id 0
▾ Linux cooked capture
    Packet type: Unicast to us (0)
    Link-layer address type: 772
    Link-layer address length: 6
    Source: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Unused: 0000
    Protocol: IPv4 (0x0800)
▾ Internet Protocol Version 4, Src: 10.0.9.59, Dst: 10.0.9.59
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x644f (25679)
  ▸ Flags: 0x0000
    Fragment offset: 0
    Time to live: 64
    Protocol: ICMP (1)
    Header checksum: 0xefe4 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.0.9.59
    Destination: 10.0.9.59
▾ Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x70ce [correct]
    [Checksum Status: Good]
    Identifier (BE): 3 (0x0003)
    Identifier (LE): 768 (0x0300)
    Sequence number (BE): 3 (0x0003)
    Sequence number (LE): 768 (0x0300)
    [Request frame: 5]
    [Response time: 0.016 ms]
    Timestamp from icmp data: Jan 22, 2021 12:18:03.000000000 IST
    [Timestamp from icmp data (relative): 0.295900668 seconds]
  ▸ Data (48 bytes)
```

Response Packet

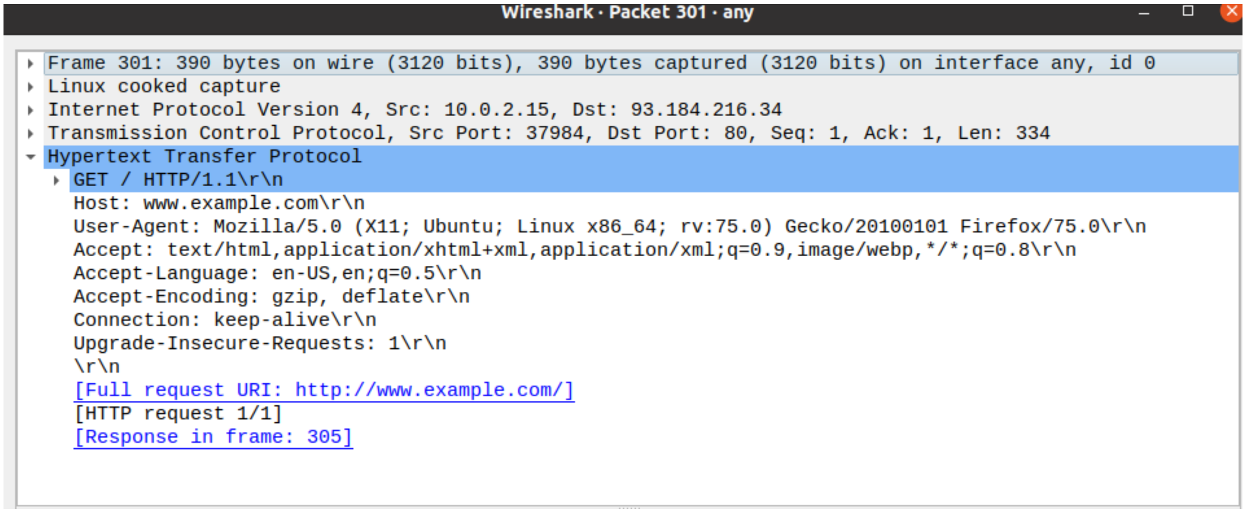
Details	First Echo Request	First Echo Reply
Frame Number	5	6
Source IP address	10.0.9.59	10.0.9.59
Destination IP address	10.0.9.59	10.0.9.59
ICMP Type Value	8	0
ICMP Code Value	0	0
Source Ethernet Address	00:00:00:00:00:00	00:00:00:00:00:00
Destination Ethernet	00:00:00:00:00:00	00:00:00:00:00:00
Internet Protocol Version	IPv4	IPv4
Time To Live(TTL)	64	64

3. HTTP PDU Capture


any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

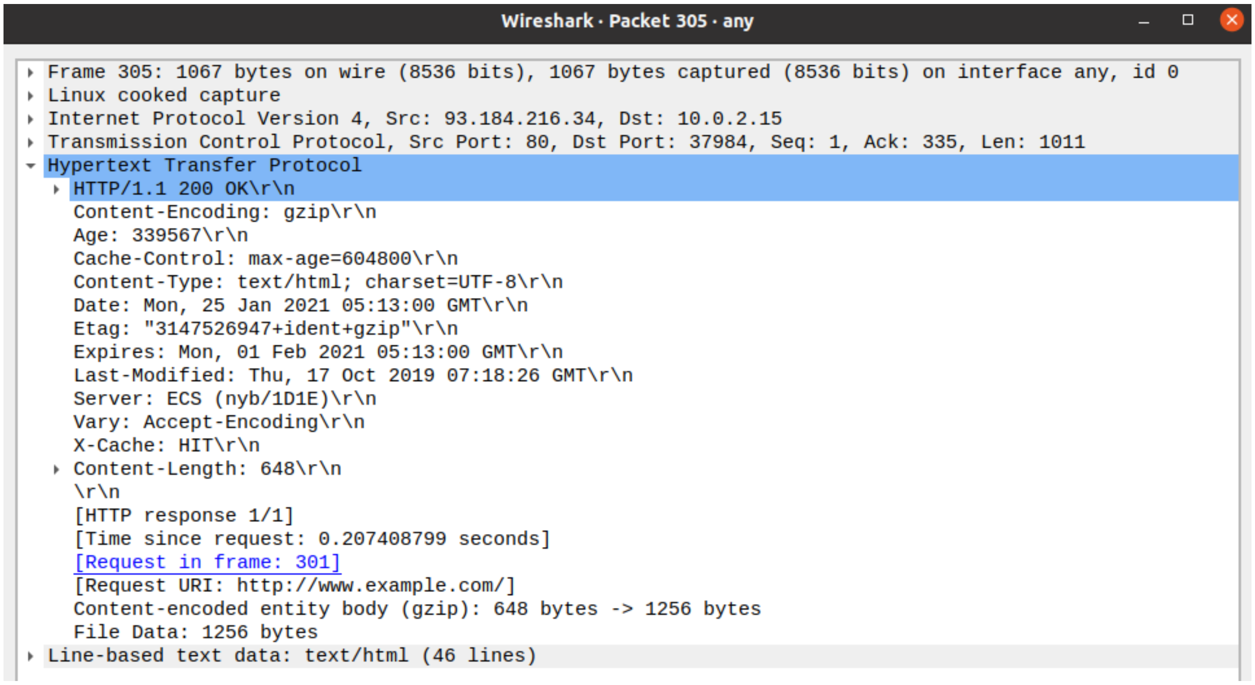
```
http
No.   Time          Source          Destination     Protocol Length Info
   12 0.076874627   10.0.2.15       34.107.221.82   HTTP      352 GET /success.txt HTTP/1.1
   18 0.104993762   34.107.221.82   10.0.2.15       HTTP      276 HTTP/1.1 200 OK  (text/plain)
   39 0.129902773   10.0.2.15       34.107.221.82   HTTP      357 GET /success.txt?ipv4 HTTP/1.1
   45 0.155177351   34.107.221.82   10.0.2.15       HTTP      276 HTTP/1.1 200 OK  (text/plain)
  134 1.631761788   10.0.2.15       117.18.237.29   OCSP      435 Request
  136 1.665653889   117.18.237.29   10.0.2.15       OCSP      853 Response
  263 2.878574421   10.0.2.15       216.58.203.3    OCSP      441 Request
  265 2.974432885   216.58.203.3    10.0.2.15       OCSP      757 Response
  301 7.215514079   10.0.2.15       93.184.216.34   HTTP      390 GET / HTTP/1.1
  305 7.422922878   93.184.216.34   10.0.2.15       HTTP     1067 HTTP/1.1 200 OK  (text/html)
```

3.1 Echo Request and Reply



```
▸ Frame 301: 390 bytes on wire (3120 bits), 390 bytes captured (3120 bits) on interface any, id 0
▸ Linux cooked capture
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 93.184.216.34
▸ Transmission Control Protocol, Src Port: 37984, Dst Port: 80, Seq: 1, Ack: 1, Len: 334
▾ Hypertext Transfer Protocol
  ▸ GET / HTTP/1.1\r\n
    Host: www.example.com\r\n
    User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:75.0) Gecko/20100101 Firefox/75.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    \r\n
    [Full request URI: http://www.example.com/]
    [HTTP request 1/1]
    [Response in frame: 305]
```

Request Packet



```
▸ Frame 305: 1067 bytes on wire (8536 bits), 1067 bytes captured (8536 bits) on interface any, id 0
▸ Linux cooked capture
▸ Internet Protocol Version 4, Src: 93.184.216.34, Dst: 10.0.2.15
▸ Transmission Control Protocol, Src Port: 80, Dst Port: 37984, Seq: 1, Ack: 335, Len: 1011
▾ Hypertext Transfer Protocol
  ▸ HTTP/1.1 200 OK\r\n
    Content-Encoding: gzip\r\n
    Age: 339567\r\n
    Cache-Control: max-age=604800\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    Date: Mon, 25 Jan 2021 05:13:00 GMT\r\n
    Etag: "3147526947+ident+gzip"\r\n
    Expires: Mon, 01 Feb 2021 05:13:00 GMT\r\n
    Last-Modified: Thu, 17 Oct 2019 07:18:26 GMT\r\n
    Server: ECS (nyb/1D1E)\r\n
    Vary: Accept-Encoding\r\n
    X-Cache: HIT\r\n
  ▸ Content-Length: 648\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.207408799 seconds]
    [Request in frame: 301]
    [Request URI: http://www.example.com/]
    Content-encoded entity body (gzip): 648 bytes -> 1256 bytes
    File Data: 1256 bytes
▸ Line-based text data: text/html (46 lines)
```

Response Packet

Details	First Echo Request	First Echo Reply
Frame Number	301	305
Source Port	37984	80
Destination Port	80	37984
Source IP address	10.0.2.15	93.184.216.34
Destination IP address	93.184.216.34	10.0.2.15
Source Ethernet address	08:00:27:64:02:1b	52:54:00:12:35:02
Destination Ethernet address	52:54:00:12:35:02	08:00:27:64:02:1b

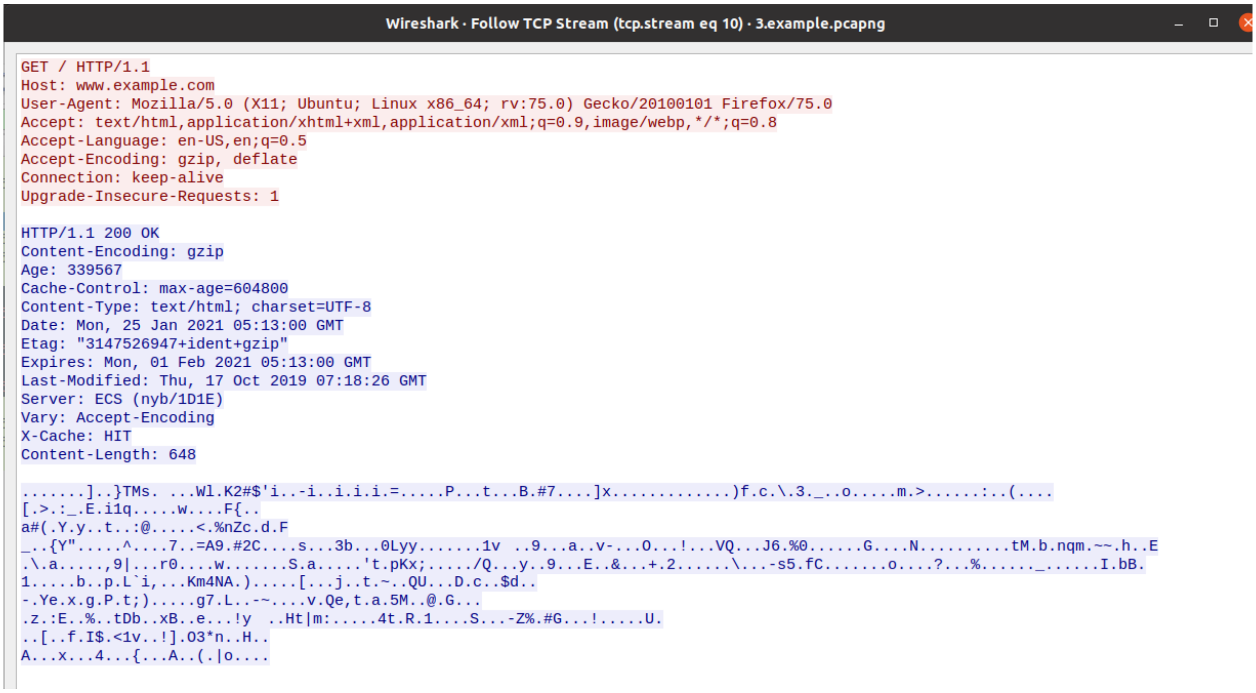
Connection Details

3.2 HTTP Request and Response

HTTP Request		**HTTP Response**	
Get	GET/HTTP/1.1\r/n	**Server**	ECS (nyb/1D1E)
Host	www.example.com	**Content-Type**	Text/html
User-agent	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:75.0) Gecko/20100101	**Date**	Mon, 25 Jan 2021 05:13:00 GMT

	Firefox/75.0		
Accept-language	En-US,en;q=0.5	**Location**	https://www.example.com
Accept-encoding	Gzip,deflate	**Content-Length**	648
Connection	Keep-alive	**Connection**	Keep-alive

3.3 Following TCP Stream

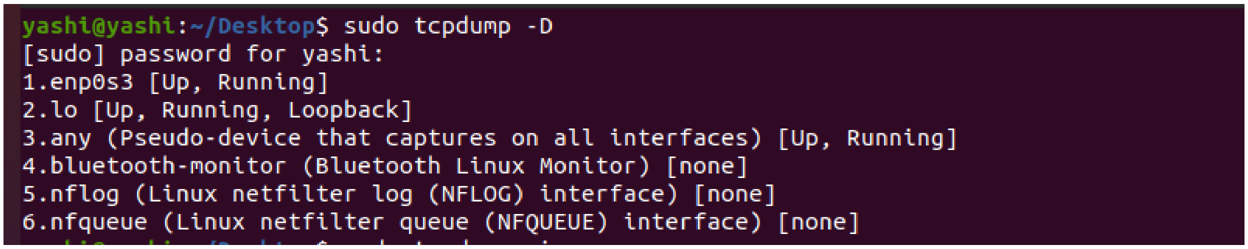


Wireshark · Follow TCP Stream (tcp.stream eq 10) · 3.example.pcapng

```
GET / HTTP/1.1
Host: www.example.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:75.0) Gecko/20100101 Firefox/75.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1

HTTP/1.1 200 OK
Content-Encoding: gzip
Age: 339567
Cache-Control: max-age=604800
Content-Type: text/html; charset=UTF-8
Date: Mon, 25 Jan 2021 05:13:00 GMT
Etag: "3147526947+ident+gzip"
Expires: Mon, 01 Feb 2021 05:13:00 GMT
Last-Modified: Thu, 17 Oct 2019 07:18:26 GMT
Server: ECS (nyb/1D1E)
Vary: Accept-Encoding
X-Cache: HIT
Content-Length: 648

.......]..}TMs. ...Wl.K2#$'i..-i..i.i.i.=.....P...t...B.#7....]x.............)f.c.\.3._..o.....m.>......:..(....
[.>.:_.E.i1q.....w....F{..
a#(.Y.y..t..:@.....<.%nZc.d.F
_..{Y".....^....7..=A9.#2C....s...3b...0Lyy.......1v ..9...a..v-...O...!...VQ...J6.%0......G....N..........tM.b.nqm.~~.h..E
.\.a.....,9|...r0....w.......S.a.....'t.pKx;...../Q...y..9...E..&...+.2......\...-s5.fC.......o....?...%......_......I.bB.
1.....b..p.L`i,...Km4NA.).....[...j..t.~..QU...D.c..$d..
-.Ye.x.g.P.t;).....g7.L..-~....v.Qe,t.a.5M..@.G...
.z.:E..%..tDb..xB..e...!y ..Ht|m:.....4t.R.1....S...-Z%.#G...!.....U.
..[..f.I$.<1v..!].O3*n..H..
A...x...4...{...A..(.|o....
```

4. Capturing Packets with tcpdump

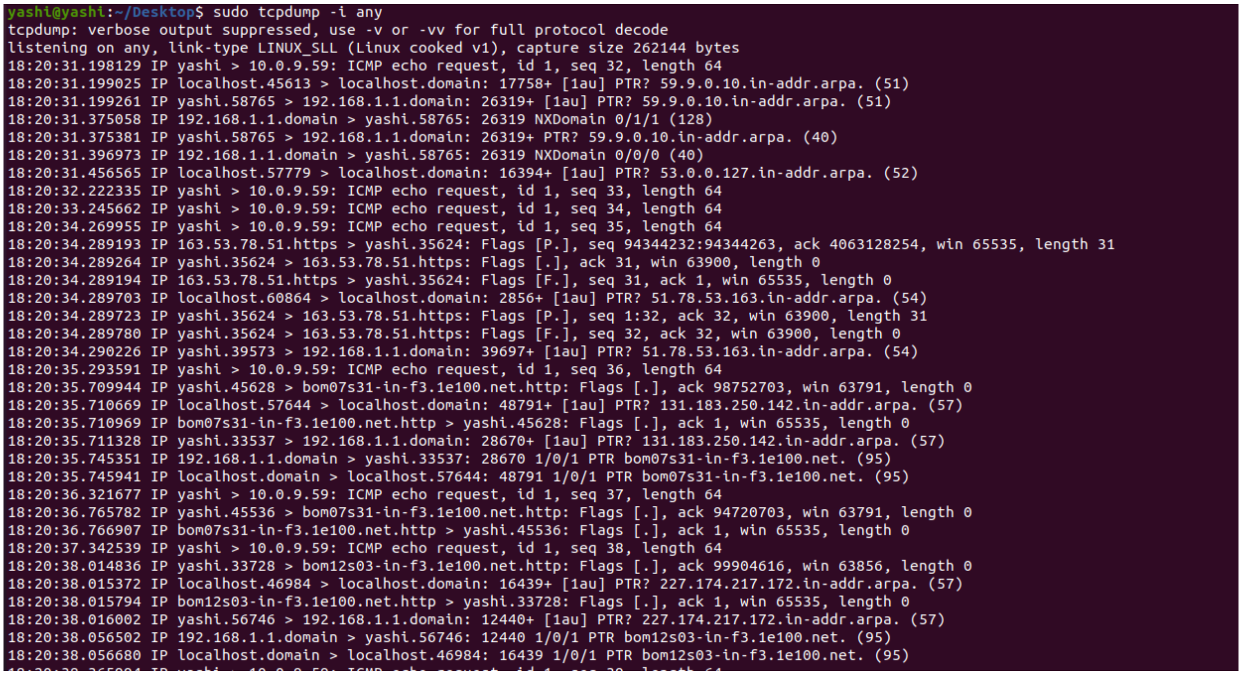
4.1 Viewing Interfaces available for Capture



```
yashi@yashi:~/Desktop$ sudo tcpdump -D
[sudo] password for yashi:
1.enp0s3 [Up, Running]
2.lo [Up, Running, Loopback]
3.any (Pseudo-device that captures on all interfaces) [Up, Running]
4.bluetooth-monitor (Bluetooth Linux Monitor) [none]
5.nflog (Linux netfilter log (NFLOG) interface) [none]
6.nfqueue (Linux netfilter queue (NFQUEUE) interface) [none]
```

tcpdump -D

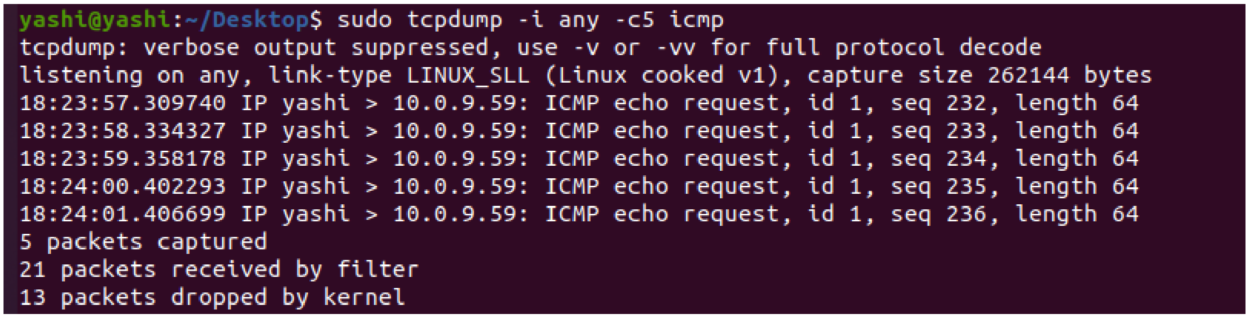
4.2 Capturing all Packets in any Interface



```
yashi@yashi:~/Desktop$ sudo tcpdump -i any
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked v1), capture size 262144 bytes
18:20:31.198129 IP yashi > 10.0.9.59: ICMP echo request, id 1, seq 32, length 64
18:20:31.199025 IP localhost.45613 > localhost.domain: 17758+ [1au] PTR? 59.9.0.10.in-addr.arpa. (51)
18:20:31.199261 IP yashi.58765 > 192.168.1.1.domain: 26319+ [1au] PTR? 59.9.0.10.in-addr.arpa. (51)
18:20:31.375058 IP 192.168.1.1.domain > yashi.58765: 26319 NXDomain 0/1/1 (128)
18:20:31.375381 IP yashi.58765 > 192.168.1.1.domain: 26319+ PTR? 59.9.0.10.in-addr.arpa. (40)
18:20:31.396973 IP 192.168.1.1.domain > yashi.58765: 26319 NXDomain 0/0/0 (40)
18:20:31.456565 IP localhost.57779 > localhost.domain: 16394+ [1au] PTR? 53.0.0.127.in-addr.arpa. (52)
18:20:32.222335 IP yashi > 10.0.9.59: ICMP echo request, id 1, seq 33, length 64
18:20:33.245662 IP yashi > 10.0.9.59: ICMP echo request, id 1, seq 34, length 64
18:20:34.269955 IP yashi > 10.0.9.59: ICMP echo request, id 1, seq 35, length 64
18:20:34.289193 IP 163.53.78.51.https > yashi.35624: Flags [P.], seq 94344232:94344263, ack 4063128254, win 65535, length 31
18:20:34.289264 IP yashi.35624 > 163.53.78.51.https: Flags [.], ack 31, win 63900, length 0
18:20:34.289194 IP 163.53.78.51.https > yashi.35624: Flags [F.], seq 31, ack 1, win 65535, length 0
18:20:34.289703 IP localhost.60864 > localhost.domain: 2856+ [1au] PTR? 51.78.53.163.in-addr.arpa. (54)
18:20:34.289723 IP yashi.35624 > 163.53.78.51.https: Flags [P.], seq 1:32, ack 32, win 63900, length 31
18:20:34.289780 IP yashi.35624 > 163.53.78.51.https: Flags [F.], seq 32, ack 32, win 63900, length 0
18:20:34.290226 IP yashi.39573 > 192.168.1.1.domain: 39697+ [1au] PTR? 51.78.53.163.in-addr.arpa. (54)
18:20:35.293591 IP yashi > 10.0.9.59: ICMP echo request, id 1, seq 36, length 64
18:20:35.709944 IP yashi.45628 > bom07s31-in-f3.1e100.net.http: Flags [.], ack 98752703, win 63791, length 0
18:20:35.710669 IP localhost.57644 > localhost.domain: 48791+ [1au] PTR? 131.183.250.142.in-addr.arpa. (57)
18:20:35.710969 IP bom07s31-in-f3.1e100.net.http > yashi.45628: Flags [.], ack 1, win 65535, length 0
18:20:35.711328 IP yashi.33537 > 192.168.1.1.domain: 28670+ [1au] PTR? 131.183.250.142.in-addr.arpa. (57)
18:20:35.745351 IP 192.168.1.1.domain > yashi.33537: 28670 1/0/1 PTR bom07s31-in-f3.1e100.net. (95)
18:20:35.745941 IP localhost.domain > localhost.57644: 48791 1/0/1 PTR bom07s31-in-f3.1e100.net. (95)
18:20:36.321677 IP yashi > 10.0.9.59: ICMP echo request, id 1, seq 37, length 64
18:20:36.765782 IP yashi.45536 > bom07s31-in-f3.1e100.net.http: Flags [.], ack 94720703, win 63791, length 0
18:20:36.766907 IP bom07s31-in-f3.1e100.net.http > yashi.45536: Flags [.], ack 1, win 65535, length 0
18:20:37.342539 IP yashi > 10.0.9.59: ICMP echo request, id 1, seq 38, length 64
18:20:38.014836 IP yashi.33728 > bom12s03-in-f3.1e100.net.http: Flags [.], ack 99904616, win 63856, length 0
18:20:38.015372 IP localhost.46984 > localhost.domain: 16439+ [1au] PTR? 227.174.217.172.in-addr.arpa. (57)
18:20:38.015794 IP bom12s03-in-f3.1e100.net.http > yashi.33728: Flags [.], ack 1, win 65535, length 0
18:20:38.016002 IP yashi.56746 > 192.168.1.1.domain: 12440+ [1au] PTR? 227.174.217.172.in-addr.arpa. (57)
18:20:38.056502 IP 192.168.1.1.domain > yashi.56746: 12440 1/0/1 PTR bom12s03-in-f3.1e100.net. (95)
18:20:38.056680 IP localhost.domain > localhost.46984: 16439 1/0/1 PTR bom12s03-in-f3.1e100.net. (95)
```

tcpdump -I any

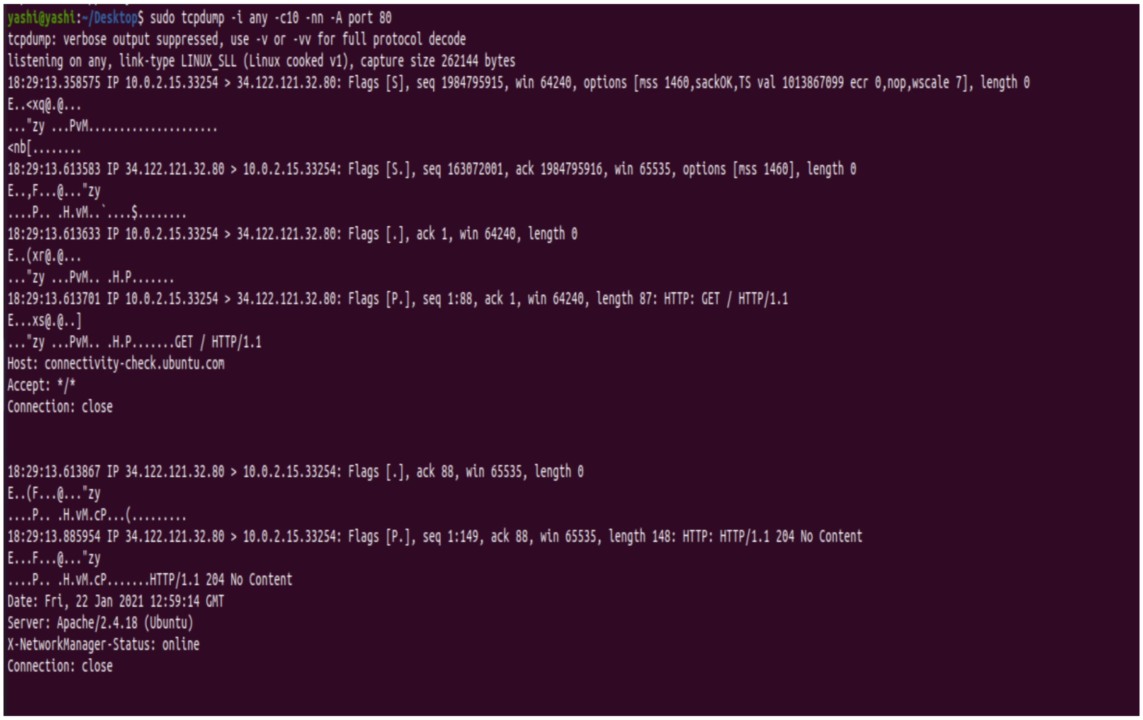
4.3 Filtering Packets based on Protocol



```
yashi@yashi:~/Desktop$ sudo tcpdump -i any -c5 icmp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked v1), capture size 262144 bytes
18:23:57.309740 IP yashi > 10.0.9.59: ICMP echo request, id 1, seq 232, length 64
18:23:58.334327 IP yashi > 10.0.9.59: ICMP echo request, id 1, seq 233, length 64
18:23:59.358178 IP yashi > 10.0.9.59: ICMP echo request, id 1, seq 234, length 64
18:24:00.402293 IP yashi > 10.0.9.59: ICMP echo request, id 1, seq 235, length 64
18:24:01.406699 IP yashi > 10.0.9.59: ICMP echo request, id 1, seq 236, length 64
5 packets captured
21 packets received by filter
13 packets dropped by kernel
```

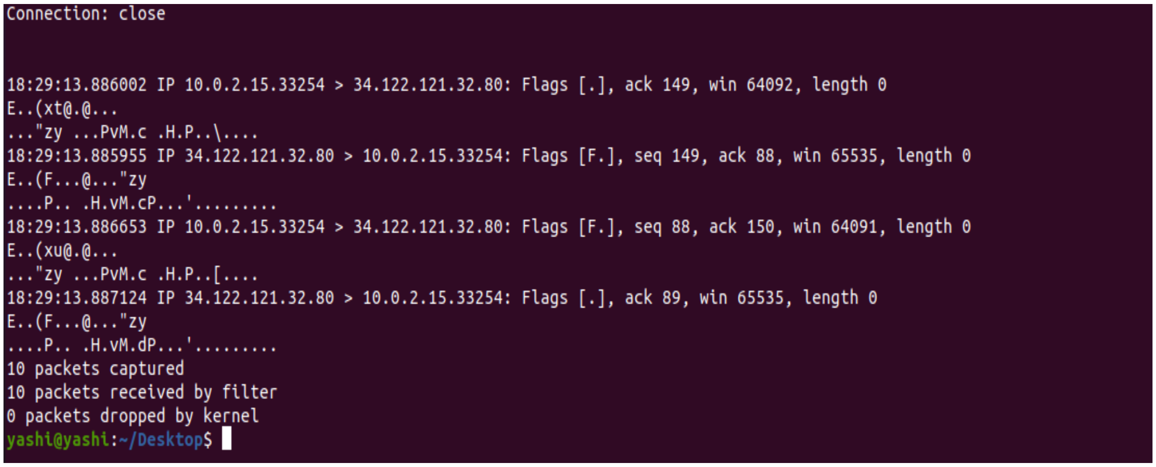
sudo tcpdump -i any -c5 icmp

4.4 Checking Packet Content



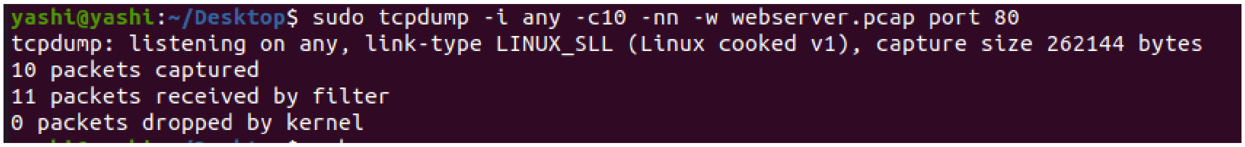
```
yashi@yashi:~/Desktop$ sudo tcpdump -i any -c10 -nn -A port 80
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked v1), capture size 262144 bytes
18:29:13.358575 IP 10.0.2.15.33254 > 34.122.121.32.80: Flags [S], seq 1984795915, win 64240, options [mss 1460,sackOK,TS val 1013867099 ecr 0,nop,wscale 7], length 0
E..<xq@.@...
..."zy ...PvM....................
<nb[........
18:29:13.613583 IP 34.122.121.32.80 > 10.0.2.15.33254: Flags [S.], seq 163072001, ack 1984795916, win 65535, options [mss 1460], length 0
E..,F...@..."zy
....P.. .H.vM..`....$........
18:29:13.613633 IP 10.0.2.15.33254 > 34.122.121.32.80: Flags [.], ack 1, win 64240, length 0
E..(xr@.@...
..."zy ...PvM.. .H.P.......
18:29:13.613701 IP 10.0.2.15.33254 > 34.122.121.32.80: Flags [P.], seq 1:88, ack 1, win 64240, length 87: HTTP: GET / HTTP/1.1
E...xs@.@..]
..."zy ...PvM.. .H.P.......GET / HTTP/1.1
Host: connectivity-check.ubuntu.com
Accept: */*
Connection: close


18:29:13.613867 IP 34.122.121.32.80 > 10.0.2.15.33254: Flags [.], ack 88, win 65535, length 0
E..(F...@..."zy
....P.. .H.vM.cP...(.........
18:29:13.885954 IP 34.122.121.32.80 > 10.0.2.15.33254: Flags [P.], seq 1:149, ack 88, win 65535, length 148: HTTP: HTTP/1.1 204 No Content
E...F...@..."zy
....P.. .H.vM.cP.......HTTP/1.1 204 No Content
Date: Fri, 22 Jan 2021 12:59:14 GMT
Server: Apache/2.4.18 (Ubuntu)
X-NetworkManager-Status: online
Connection: close
```

sudo tcpdump -i any -c10 -nn -A port 80



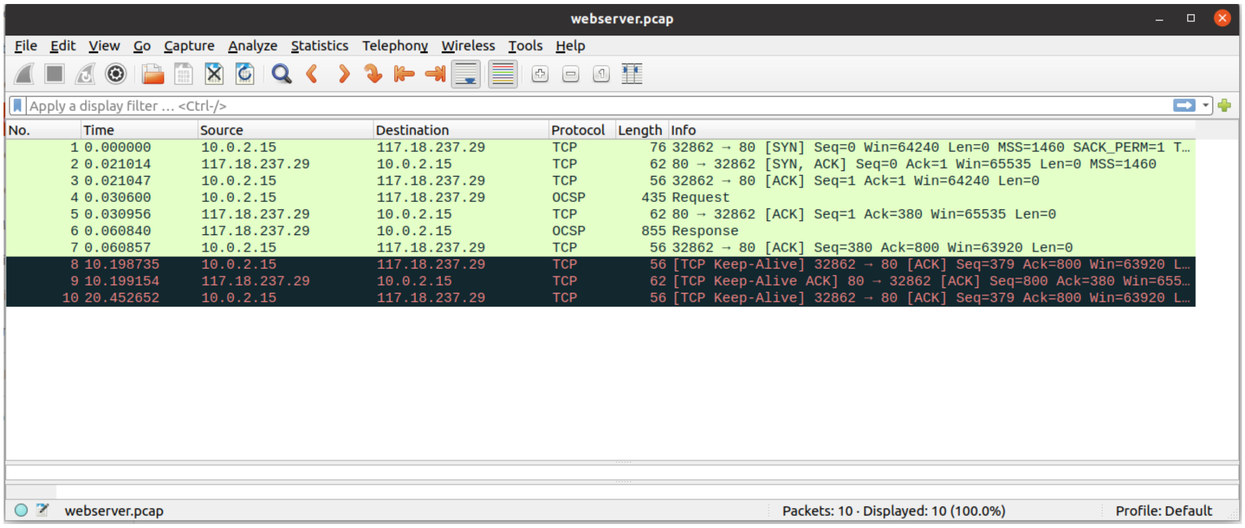
```
Connection: close


18:29:13.886002 IP 10.0.2.15.33254 > 34.122.121.32.80: Flags [.], ack 149, win 64092, length 0
E..(xt@.@...
..."zy ...PvM.c .H.P..\....
18:29:13.885955 IP 34.122.121.32.80 > 10.0.2.15.33254: Flags [F.], seq 149, ack 88, win 65535, length 0
E..(F...@..."zy
....P.. .H.vM.cP...'.........
18:29:13.886653 IP 10.0.2.15.33254 > 34.122.121.32.80: Flags [F.], seq 88, ack 150, win 64091, length 0
E..(xu@.@...
..."zy ...PvM.c .H.P..[....
18:29:13.887124 IP 34.122.121.32.80 > 10.0.2.15.33254: Flags [.], ack 89, win 65535, length 0
E..(F...@..."zy
....P.. .H.vM.dP...'.........
10 packets captured
10 packets received by filter
0 packets dropped by kernel
yashi@yashi:~/Desktop$ 
```

4.5 Saving Packets to a File



```
yashi@yashi:~/Desktop$ sudo tcpdump -i any -c10 -nn -w webserver.pcap port 80
tcpdump: listening on any, link-type LINUX_SLL (Linux cooked v1), capture size 262144 bytes
10 packets captured
11 packets received by filter
0 packets dropped by kernel
```

sudo tcpdump -I any -c10 -nn -w webserver.pcap port 80



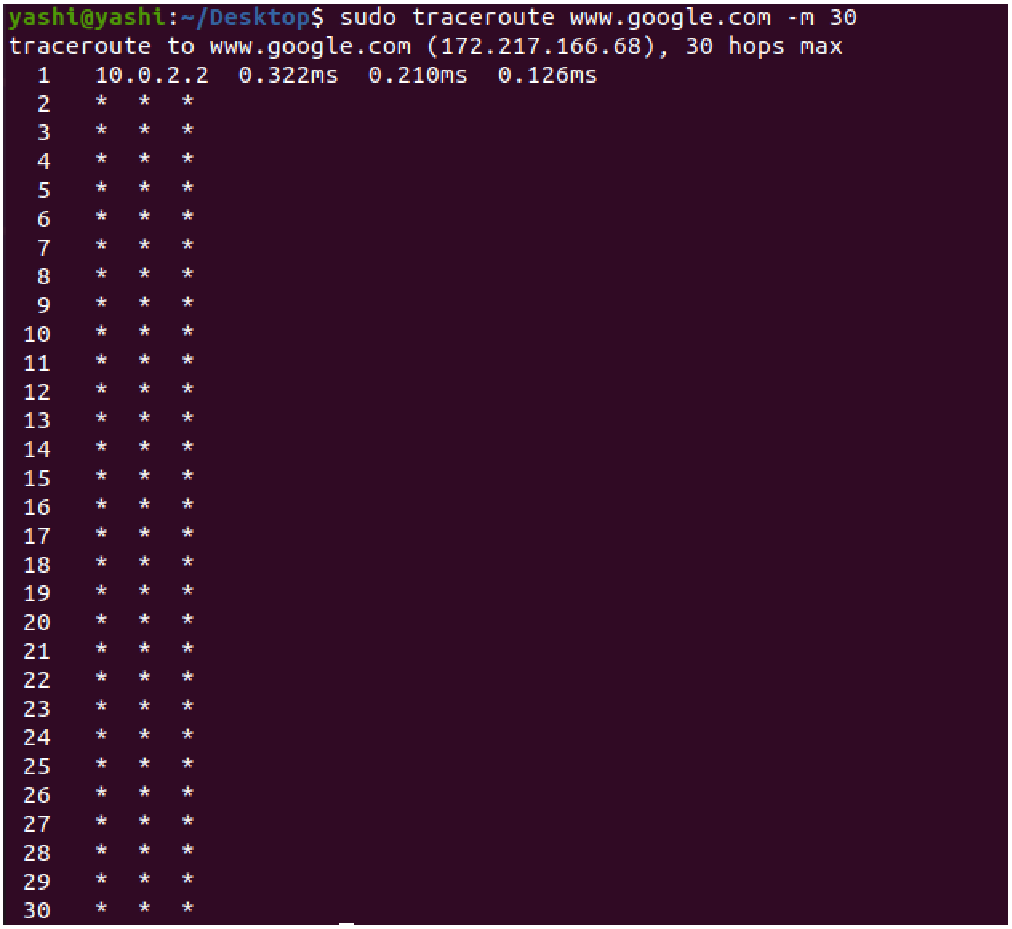
webserver.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
webserver.pcap
Packets: 10 · Displayed: 10 (100.0%)
Profile: Default

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.2.15	117.18.237.29	TCP	76	32862 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T…
2	0.021014	117.18.237.29	10.0.2.15	TCP	62	80 → 32862 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
3	0.021047	10.0.2.15	117.18.237.29	TCP	56	32862 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
4	0.030600	10.0.2.15	117.18.237.29	OCSP	435	Request
5	0.030956	117.18.237.29	10.0.2.15	TCP	62	80 → 32862 [ACK] Seq=1 Ack=380 Win=65535 Len=0
6	0.060840	117.18.237.29	10.0.2.15	OCSP	855	Response
7	0.060857	10.0.2.15	117.18.237.29	TCP	56	32862 → 80 [ACK] Seq=380 Ack=800 Win=63920 Len=0
8	10.198735	10.0.2.15	117.18.237.29	TCP	56	[TCP Keep-Alive] 32862 → 80 [ACK] Seq=379 Ack=800 Win=63920 L…
9	10.199154	117.18.237.29	10.0.2.15	TCP	62	[TCP Keep-Alive ACK] 80 → 32862 [ACK] Seq=800 Ack=380 Win=655…
10	20.452652	10.0.2.15	117.18.237.29	TCP	56	[TCP Keep-Alive] 32862 → 80 [ACK] Seq=379 Ack=800 Win=63920 L…

Webserver.pcap

5. Perform traceroute checks

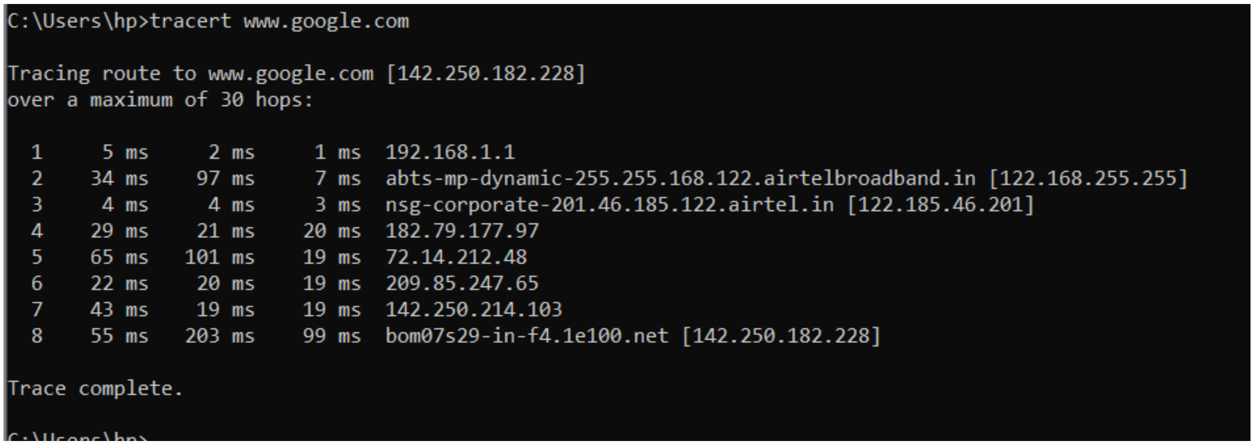
5.1 Running traceroute



```
yashi@yashi:~/Desktop$ sudo traceroute www.google.com -m 30
traceroute to www.google.com (172.217.166.68), 30 hops max
  1   10.0.2.2  0.322ms  0.210ms  0.126ms
  2   *  *  *
  3   *  *  *
  4   *  *  *
  5   *  *  *
  6   *  *  *
  7   *  *  *
  8   *  *  *
  9   *  *  *
 10   *  *  *
 11   *  *  *
 12   *  *  *
 13   *  *  *
 14   *  *  *
 15   *  *  *
 16   *  *  *
 17   *  *  *
 18   *  *  *
 19   *  *  *
 20   *  *  *
 21   *  *  *
 22   *  *  *
 23   *  *  *
 24   *  *  *
 25   *  *  *
 26   *  *  *
 27   *  *  *
 28   *  *  *
 29   *  *  *
 30   *  *  *
```

sudo traceroute www.google.com

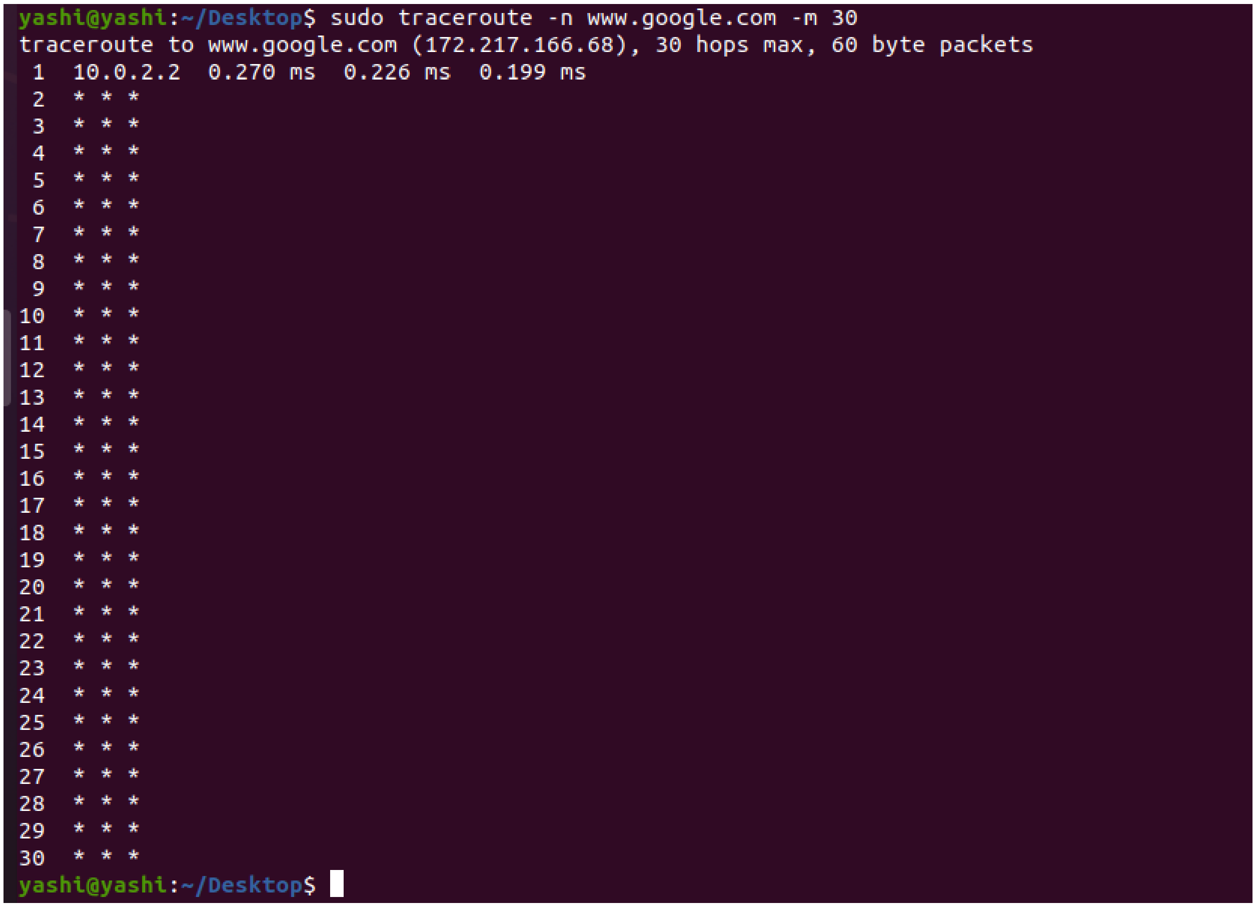
Running traceroute on Windows using tracert



```
C:\Users\hp>tracert www.google.com

Tracing route to www.google.com [142.250.182.228]
over a maximum of 30 hops:

  1     5 ms     2 ms     1 ms  192.168.1.1
  2    34 ms    97 ms     7 ms  abts-mp-dynamic-255.255.168.122.airtelbroadband.in [122.168.255.255]
  3     4 ms     4 ms     3 ms  nsg-corporate-201.46.185.122.airtel.in [122.185.46.201]
  4    29 ms    21 ms    20 ms  182.79.177.97
  5    65 ms   101 ms    19 ms  72.14.212.48
  6    22 ms    20 ms    19 ms  209.85.247.65
  7    43 ms    19 ms    19 ms  142.250.214.103
  8    55 ms   203 ms    99 ms  bom07s29-in-f4.1e100.net [142.250.182.228]

Trace complete.

C:\Users\hp>
```

tracert www.google.com

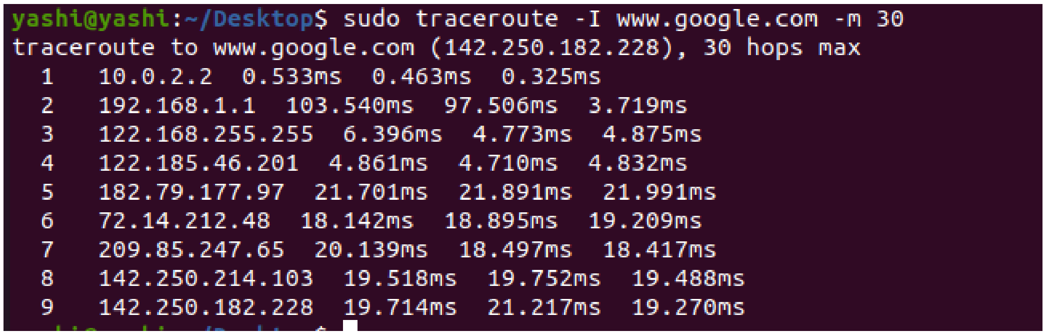
5.2 Disabling mapping of IP addresses with host names



```
yashi@yashi:~/Desktop$ sudo traceroute -n www.google.com -m 30
traceroute to www.google.com (172.217.166.68), 30 hops max, 60 byte packets
 1  10.0.2.2  0.270 ms  0.226 ms  0.199 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
yashi@yashi:~/Desktop$
```

sudo traceruote -n www.google.com

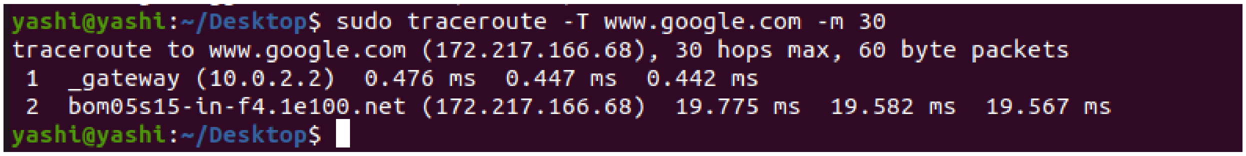
5.3 traceroute with ICMP Protocol



```
yashi@yashi:~/Desktop$ sudo traceroute -I www.google.com -m 30
traceroute to www.google.com (142.250.182.228), 30 hops max
  1   10.0.2.2  0.533ms  0.463ms  0.325ms
  2   192.168.1.1  103.540ms  97.506ms  3.719ms
  3   122.168.255.255  6.396ms  4.773ms  4.875ms
  4   122.185.46.201  4.861ms  4.710ms  4.832ms
  5   182.79.177.97  21.701ms  21.891ms  21.991ms
  6   72.14.212.48  18.142ms  18.895ms  19.209ms
  7   209.85.247.65  20.139ms  18.497ms  18.417ms
  8   142.250.214.103  19.518ms  19.752ms  19.488ms
  9   142.250.182.228  19.714ms  21.217ms  19.270ms
```

sudo traceroute -I www.google.com

5.4 Testing TCP connection with traceroute

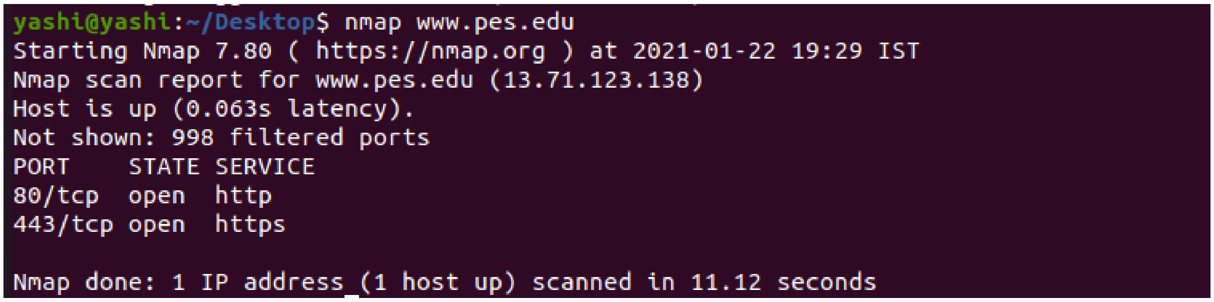


```
yashi@yashi:~/Desktop$ sudo traceroute -T www.google.com -m 30
traceroute to www.google.com (172.217.166.68), 30 hops max, 60 byte packets
 1  _gateway (10.0.2.2)  0.476 ms  0.447 ms  0.442 ms
 2  bom05s15-in-f4.1e100.net (172.217.166.68)  19.775 ms  19.582 ms  19.567 ms
yashi@yashi:~/Desktop$ 
```

sudo traceroute -T www.google.com

6. Exploring a network with nmap

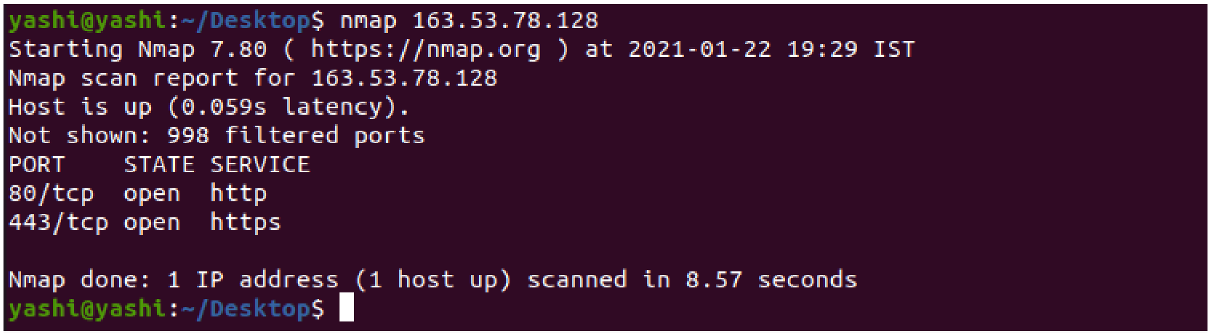
6.1 Scanning Host with Hostname



```
yashi@yashi:~/Desktop$ nmap www.pes.edu
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-22 19:29 IST
Nmap scan report for www.pes.edu (13.71.123.138)
Host is up (0.063s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 11.12 seconds
```

nmap www.pes.edu

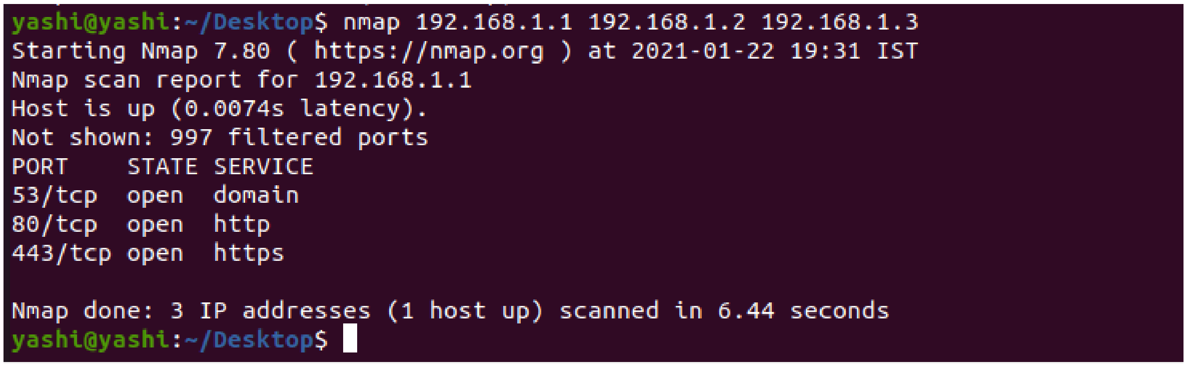
6.2 Scanning Host with IP address



```
yashi@yashi:~/Desktop$ nmap 163.53.78.128
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-22 19:29 IST
Nmap scan report for 163.53.78.128
Host is up (0.059s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 8.57 seconds
yashi@yashi:~/Desktop$ 
```

nmap 163.53.78.128

6.3 Scanning Multiple IP addresses or Subnet (IPv4)

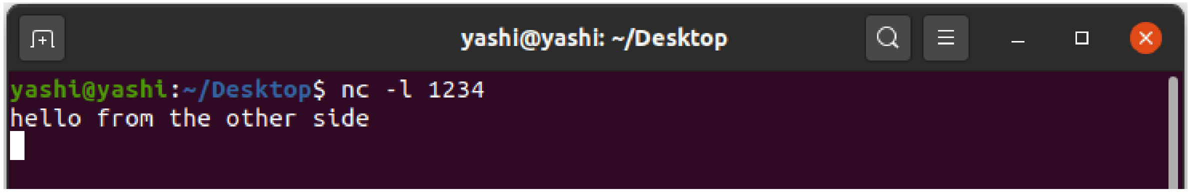


```
yashi@yashi:~/Desktop$ nmap 192.168.1.1 192.168.1.2 192.168.1.3
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-22 19:31 IST
Nmap scan report for 192.168.1.1
Host is up (0.0074s latency).
Not shown: 997 filtered ports
PORT    STATE SERVICE
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https

Nmap done: 3 IP addresses (1 host up) scanned in 6.44 seconds
yashi@yashi:~/Desktop$ 
```

nmap 192.168.1.1 192.168.1.2 192.168.1.3

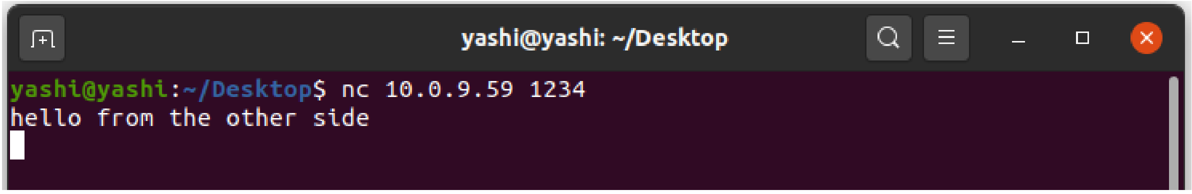
7.a. Netcat as Chat Tool

a) Intra system communication



```
yashi@yashi:~/Desktop$ nc -l 1234
hello from the other side
```

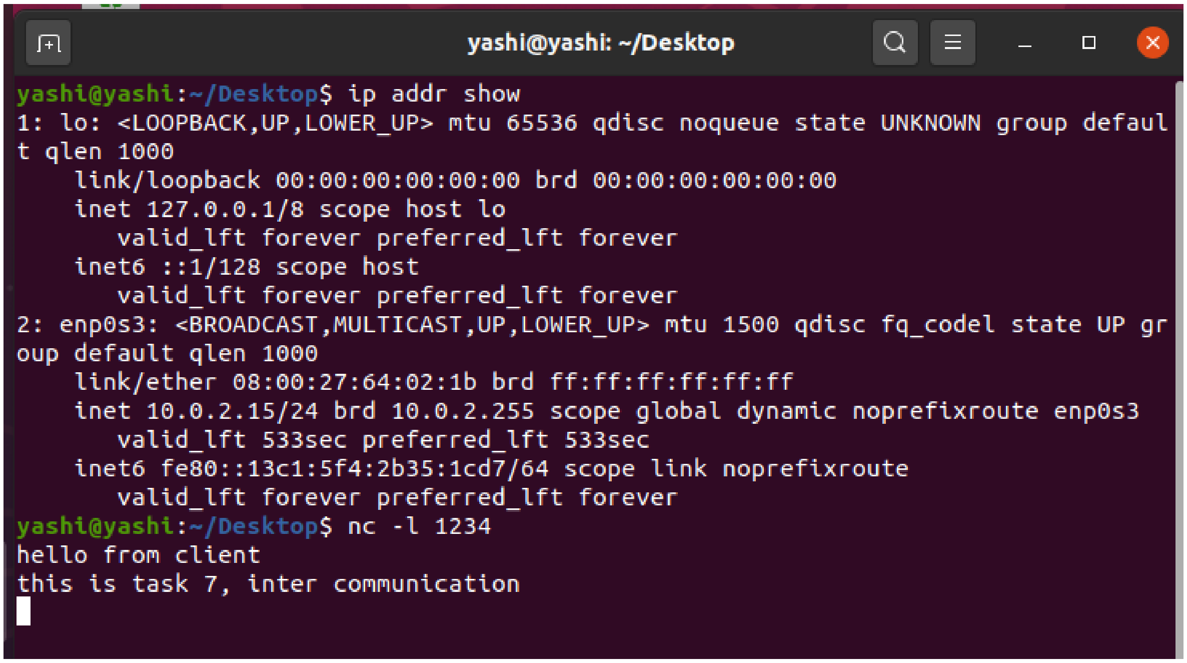
Server side



```
yashi@yashi:~/Desktop$ nc 10.0.9.59 1234
hello from the other side
```

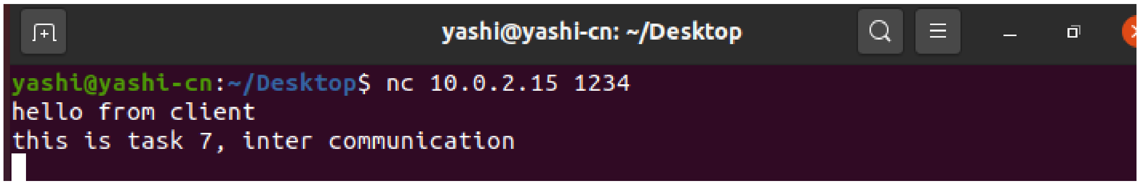
Client side

b) Inter system communication



```
yashi@yashi:~/Desktop$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t 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: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gr
oup default qlen 1000
    link/ether 08:00:27:64:02:1b brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
       valid_lft 533sec preferred_lft 533sec
    inet6 fe80::13c1:5f4:2b35:1cd7/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
yashi@yashi:~/Desktop$ nc -l 1234
hello from client
this is task 7, inter communication
```

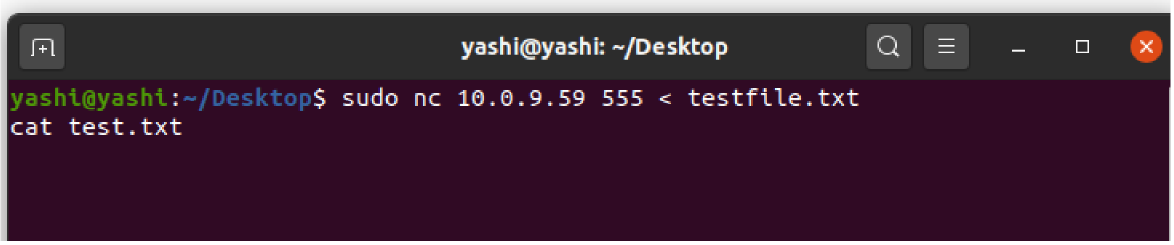
Server side



```
yashi@yashi-cn:~/Desktop$ nc 10.0.2.15 1234
hello from client
this is task 7, inter communication
```

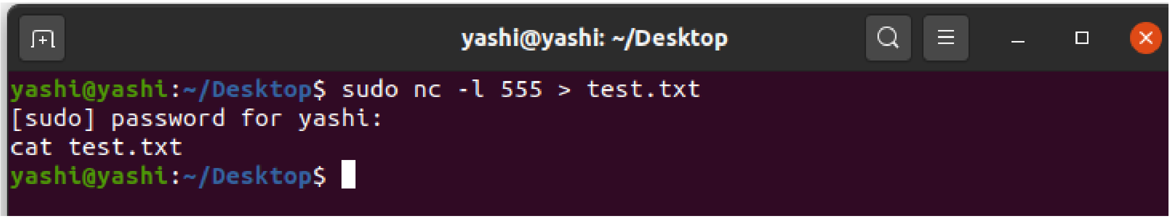
Client side

7.b. Use netcat to transfer files



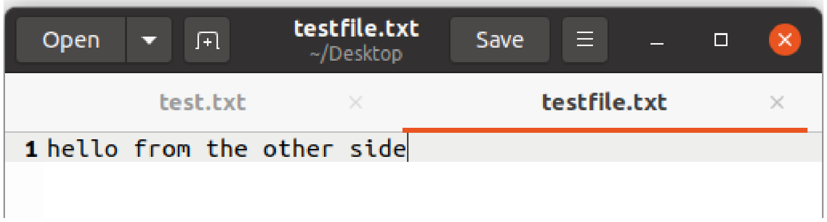
```
yashi@yashi:~/Desktop$ sudo nc 10.0.9.59 555 < testfile.txt
cat test.txt
```

client side

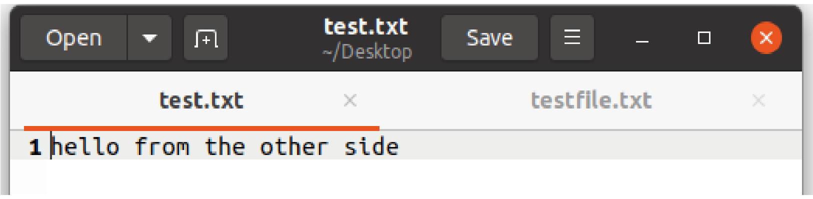


```
yashi@yashi:~/Desktop$ sudo nc -l 555 > test.txt
[sudo] password for yashi:
cat test.txt
yashi@yashi:~/Desktop$ 
```

server side

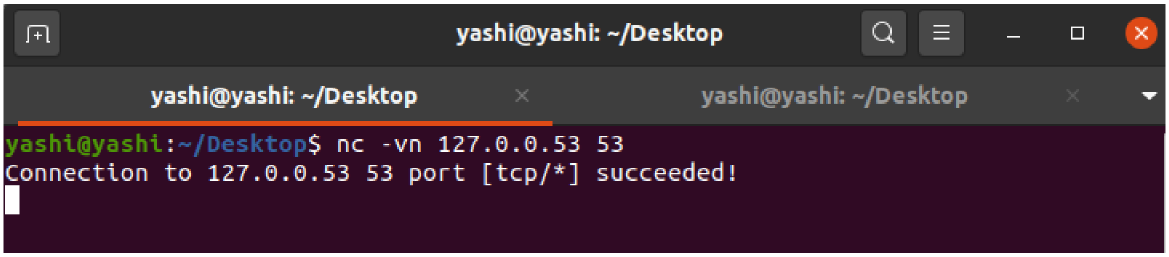


```
1 hello from the other side
```



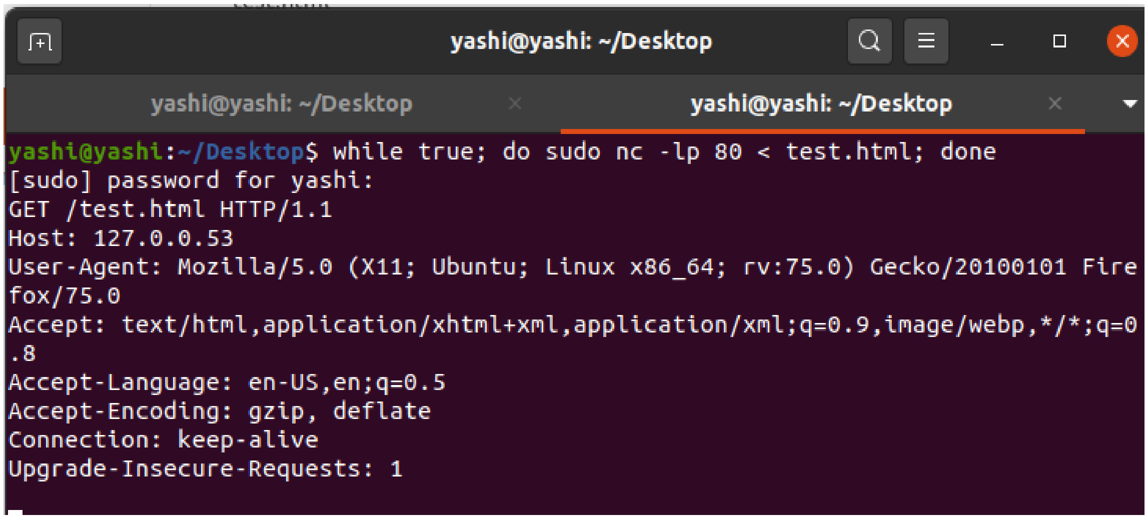
```
1 hello from the other side
```

7.c. other commands



```
yashi@yashi:~/Desktop$ nc -vn 127.0.0.53 53
Connection to 127.0.0.53 53 port [tcp/*] succeeded!
```

Test and connect a remote host



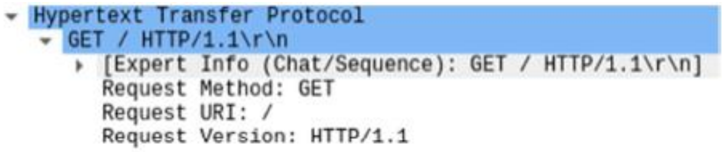
```
yashi@yashi:~/Desktop$ while true; do sudo nc -lp 80 < test.html; done
[sudo] password for yashi:
GET /test.html HTTP/1.1
Host: 127.0.0.53
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:75.0) Gecko/20100101 Fire
fox/75.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0
.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
```

Details obtained

Questions

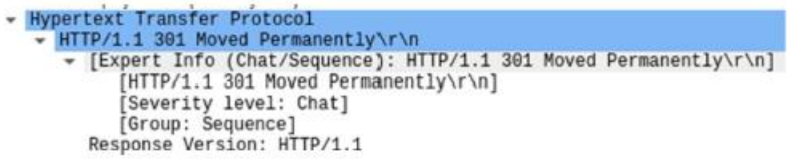
1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server?

Answer- The Firefox browser used in running HTTP v1.1, and this can be seen in the request header which contains the method (GET) followed by the HTTP version. Similarly, the HTTP version of web server is v1.1 and can be seen in the header of the HTTP response sent back to browser.



```
▾ Hypertext Transfer Protocol
  ▾ GET / HTTP/1.1\r\n
    ▸ [Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /
      Request Version: HTTP/1.1
```

Request



```
▾ Hypertext Transfer Protocol
  ▾ HTTP/1.1 301 Moved Permanently\r\n
    ▾ [Expert Info (Chat/Sequence): HTTP/1.1 301 Moved Permanently\r\n]
        [HTTP/1.1 301 Moved Permanently\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Response Version: HTTP/1.1
```

Response

2. When was the HTML file that you are retrieving last modified at the server?

Answer – We can find the last modified time of the HTML file at the server by observing the Last-Modified field of the HTTP response object. The Last-Modified field stores a timestamp of the last modification time.

3. How to tell ping to exit after a specified number of ECHO_REQUEST packets?

Answer- Ping continues to send ICMP packages until it receives an interrupt signal. To specify the number of ECHO_REQUEST packages after which ping will exit, we can use the -c option followed by the number of packages.

ping -c 10 www.pes.edu

4. How will you identify remote host apps and OS?

Answer-

1. We can obtain the remote host app and OS of the server by observing the Server files of the HTTP response object. The server field stores the remote host app or the server on which it is hosted and the OS too.

2. We can use nmap to find the OS too. It will scan the network to find information about the remote host apps and OS.

```
nmap -O -v www.flipkart.com
```