COMPUTER NETWORKS LABORATORY
WEEK #1

NAME : SIRI S
SEMESTER : 4
SECTION : H
SRN : PES1UG19CS485

Task 1:

Linux Interface Configuration (ifconfig / IP command)

IP Address Table:

Interface Name	IP address (IPv4/IPv6)	MAC address
lo0	127.0.0.1/8	00:00:00:00:00:00
en5	fe80::aede:48ff:fe00:1122/64	ac:de:48:00:11:22
en0	192.168.0.100/24	38:f9:d3:c0:fb:14

STEP 1: To display status of all active network interfaces.

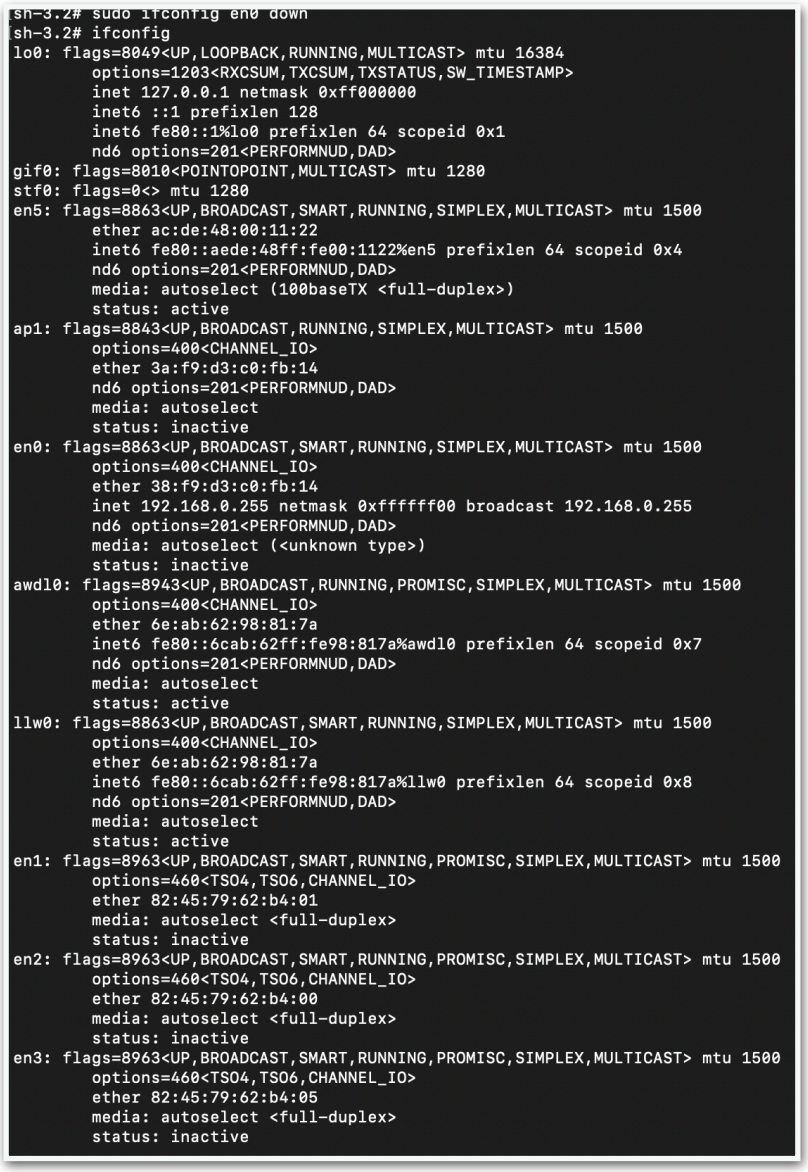
```
sh-3.2# ip addr show
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
        inet 127.0.0.1/8 lo0
        inet6 ::1/128
        inet6 fe80::1/64 scopeid 0x1
en5: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        ether ac:de:48:00:11:22
        inet6 fe80::aede:48ff:fe00:1122/64 scopeid 0x4
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        ether 38:f9:d3:c0:fb:14
        inet6 fe80::1012:38c9:1a86:ab3c/64 secured scopeid 0x6
        inet 192.168.0.100/24 brd 192.168.0.255 en0
awdl0: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
        ether 6e:ab:62:98:81:7a
        inet6 fe80::6cab:62ff:fe98:817a/64 scopeid 0x7
llw0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        ether 6e:ab:62:98:81:7a
        inet6 fe80::6cab:62ff:fe98:817a/64 scopeid 0x8
utun0: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1380
        inet6 fe80::4635:63c5:54f9:e7fc/64 scopeid 0xe
utun1: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 2000
        inet6 fe80::4f1e:8e38:d8be:855d/64 scopeid 0xf
```

STEP 2: To assign an IP address to an interface.

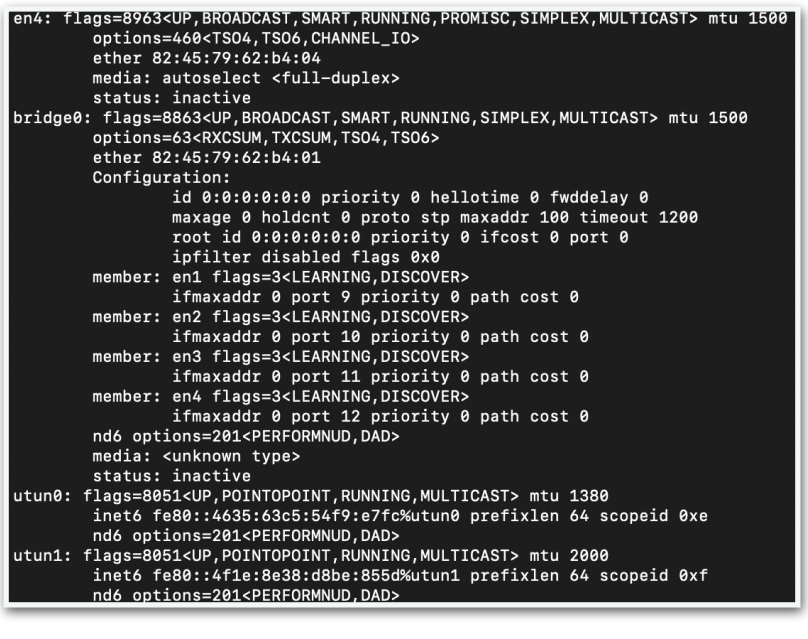
```
sh-3.2# sudo ip addr add 192.168.0.100/24 dev en0
Executing: /usr/bin/sudo /sbin/ifconfig en0 add 192.168.0.100/24

sh-3.2# ip addr show
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
        inet 127.0.0.1/8 lo0
        inet6 ::1/128
        inet6 fe80::1/64 scopeid 0x1
en5: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        ether ac:de:48:00:11:22
        inet6 fe80::aede:48ff:fe00:1122/64 scopeid 0x4
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        ether 38:f9:d3:c0:fb:14
        inet 192.168.0.255/24 brd 192.168.0.255 en0
        inet6 fe80::1012:38c9:1a86:ab3c/64 secured scopeid 0x6
        inet 192.168.0.100/24 brd 192.168.0.255 en0
awdl0: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
        ether 6e:ab:62:98:81:7a
        inet6 fe80::6cab:62ff:fe98:817a/64 scopeid 0x7
llw0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        ether 6e:ab:62:98:81:7a
        inet6 fe80::6cab:62ff:fe98:817a/64 scopeid 0x8
utun0: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1380
        inet6 fe80::4635:63c5:54f9:e7fc/64 scopeid 0xe
utun1: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 2000
        inet6 fe80::4f1e:8e38:d8be:855d/64 scopeid 0xf
```

STEP 3: To activate / deactivate a network interface.

en0 down :



```
sh-3.2# sudo ifconfig en0 down
sh-3.2# ifconfig
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
        options=1203<RXCSUM,TXCSUM,TXSTATUS,SW_TIMESTAMP>
        inet 127.0.0.1 netmask 0xff000000
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
        nd6 options=201<PERFORMNUD,DAD>
gif0: flags=8010<POINTOPOINT,MULTICAST> mtu 1280
stf0: flags=0<> mtu 1280
en5: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        ether ac:de:48:00:11:22
        inet6 fe80::aede:48ff:fe00:1122%en5 prefixlen 64 scopeid 0x4
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect (100baseTX <full-duplex>)
        status: active
ap1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=400<CHANNEL_IO>
        ether 3a:f9:d3:c0:fb:14
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect
        status: inactive
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=400<CHANNEL_IO>
        ether 38:f9:d3:c0:fb:14
        inet 192.168.0.255 netmask 0xffffff00 broadcast 192.168.0.255
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect (<unknown type>)
        status: inactive
awdl0: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
        options=400<CHANNEL_IO>
        ether 6e:ab:62:98:81:7a
        inet6 fe80::6cab:62ff:fe98:817a%awdl0 prefixlen 64 scopeid 0x7
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect
        status: active
llw0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=400<CHANNEL_IO>
        ether 6e:ab:62:98:81:7a
        inet6 fe80::6cab:62ff:fe98:817a%llw0 prefixlen 64 scopeid 0x8
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect
        status: active
en1: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
        options=460<TSO4,TSO6,CHANNEL_IO>
        ether 82:45:79:62:b4:01
        media: autoselect <full-duplex>
        status: inactive
en2: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
        options=460<TSO4,TSO6,CHANNEL_IO>
        ether 82:45:79:62:b4:00
        media: autoselect <full-duplex>
        status: inactive
en3: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
        options=460<TSO4,TSO6,CHANNEL_IO>
        ether 82:45:79:62:b4:05
        media: autoselect <full-duplex>
        status: inactive
```



```
en4: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
        options=460<TSO4,TSO6,CHANNEL_IO>
        ether 82:45:79:62:b4:04
        media: autoselect <full-duplex>
        status: inactive
bridge0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=63<RXCSUM,TXCSUM,TSO4,TSO6>
        ether 82:45:79:62:b4:01
        Configuration:
                id 0:0:0:0:0:0 priority 0 hellotime 0 fwddelay 0
                maxage 0 holdcnt 0 proto stp maxaddr 100 timeout 1200
                root id 0:0:0:0:0:0 priority 0 ifcost 0 port 0
                ipfilter disabled flags 0x0
        member: en1 flags=3<LEARNING,DISCOVER>
                ifmaxaddr 0 port 9 priority 0 path cost 0
        member: en2 flags=3<LEARNING,DISCOVER>
                ifmaxaddr 0 port 10 priority 0 path cost 0
        member: en3 flags=3<LEARNING,DISCOVER>
                ifmaxaddr 0 port 11 priority 0 path cost 0
        member: en4 flags=3<LEARNING,DISCOVER>
                ifmaxaddr 0 port 12 priority 0 path cost 0
        nd6 options=201<PERFORMNUD,DAD>
        media: <unknown type>
        status: inactive
utun0: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1380
        inet6 fe80::4635:63c5:54f9:e7fc%utun0 prefixlen 64 scopeid 0xe
        nd6 options=201<PERFORMNUD,DAD>
utun1: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 2000
        inet6 fe80::4f1e:8e38:d8be:855d%utun1 prefixlen 64 scopeid 0xf
        nd6 options=201<PERFORMNUD,DAD>
```

en0 up:

```
sh-3.2# sudo ifconfig en0 up
sh-3.2# ifconfig
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
        options=1203<RXCSUM,TXCSUM,TXSTATUS,SW_TIMESTAMP>
        inet 127.0.0.1 netmask 0xff000000
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
        nd6 options=201<PERFORMNUD,DAD>
gif0: flags=8010<POINTOPOINT,MULTICAST> mtu 1280
stf0: flags=0<> mtu 1280
en5: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        ether ac:de:48:00:11:22
        inet6 fe80::aede:48ff:fe00:1122%en5 prefixlen 64 scopeid 0x4
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect (100baseTX <full-duplex>)
        status: active
ap1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=400<CHANNEL_IO>
        ether 3a:f9:d3:c0:fb:14
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect
        status: inactive
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=400<CHANNEL_IO>
        ether 38:f9:d3:c0:fb:14
        inet 192.168.0.255 netmask 0xffffff00 broadcast 192.168.0.255
        inet6 fe80::1012:38c9:1a86:ab3c%en0 prefixlen 64 secured scopeid 0x6
        inet 192.168.0.100 netmask 0xffffff00 broadcast 192.168.0.255
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect
        status: active
awdl0: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
        options=400<CHANNEL_IO>
        ether 6e:ab:62:98:81:7a
        inet6 fe80::6cab:62ff:fe98:817a%awdl0 prefixlen 64 scopeid 0x7
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect
        status: active
llw0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=400<CHANNEL_IO>
        ether 6e:ab:62:98:81:7a
        inet6 fe80::6cab:62ff:fe98:817a%llw0 prefixlen 64 scopeid 0x8
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect
        status: active
en1: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
        options=460<TSO4,TSO6,CHANNEL_IO>
        ether 82:45:79:62:b4:01
        media: autoselect <full-duplex>
        status: inactive
en2: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
        options=460<TSO4,TSO6,CHANNEL_IO>
        ether 82:45:79:62:b4:00
        media: autoselect <full-duplex>
        status: inactive
en3: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
        options=460<TSO4,TSO6,CHANNEL_IO>
        ether 82:45:79:62:b4:05
        media: autoselect <full-duplex>
        status: inactive
```

```
en4: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
        options=460<TSO4,TSO6,CHANNEL_IO>
        ether 82:45:79:62:b4:04
        media: autoselect <full-duplex>
        status: inactive
bridge0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=63<RXCSUM,TXCSUM,TSO4,TSO6>
        ether 82:45:79:62:b4:01
        Configuration:
                id 0:0:0:0:0:0 priority 0 hellotime 0 fwddelay 0
                maxage 0 holdcnt 0 proto stp maxaddr 100 timeout 1200
                root id 0:0:0:0:0:0 priority 0 ifcost 0 port 0
                ipfilter disabled flags 0x0
        member: en1 flags=3<LEARNING,DISCOVER>
                ifmaxaddr 0 port 9 priority 0 path cost 0
        member: en2 flags=3<LEARNING,DISCOVER>
                ifmaxaddr 0 port 10 priority 0 path cost 0
        member: en3 flags=3<LEARNING,DISCOVER>
                ifmaxaddr 0 port 11 priority 0 path cost 0
        member: en4 flags=3<LEARNING,DISCOVER>
                ifmaxaddr 0 port 12 priority 0 path cost 0
        nd6 options=201<PERFORMNUD,DAD>
        media: <unknown type>
        status: inactive
utun0: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1380
        inet6 fe80::4635:63c5:54f9:e7fc%utun0 prefixlen 64 scopeid 0xe
        nd6 options=201<PERFORMNUD,DAD>
utun1: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 2000
        inet6 fe80::4f1e:8e38:d8be:855d%utun1 prefixlen 64 scopeid 0xf
        nd6 options=201<PERFORMNUD,DAD>
```

Step 4: To show the current neighbour table in kernel

```
sh-3.2# ip neigh
fe80::1 dev lo0 lladdr (incomplete) REACHABLE
fe80::aede:48ff:fe00:1122 dev en5 lladdr ac:de:48:0:11:22 REACHABLE
fe80::aede:48ff:fe33:4455 dev en5 lladdr ac:de:48:33:44:55 REACHABLE
fe80::1012:38c9:1a86:ab3c dev en0 lladdr 38:f9:d3:c0:fb:14 REACHABLE
fe80::da07:b6ff:feec:7500 dev en0 lladdr d8:7:b6:ec:75:0 STALE
fe80::6cab:62ff:fe98:817a dev awdl0 lladdr 6e:ab:62:98:81:7a REACHABLE
fe80::6cab:62ff:fe98:817a dev llw0 lladdr 6e:ab:62:98:81:7a REACHABLE
fe80::4635:63c5:54f9:e7fc dev utun0 lladdr (incomplete) REACHABLE
fe80::4f1e:8e38:d8be:855d dev utun1 lladdr (incomplete) REACHABLE
192.168.0.1 dev en0 lladdr d8:7:b6:ec:75:0 REACHABLE
224.0.0.251 dev en0 lladdr 1:0:5e:0:0:fb REACHABLE
239.255.255.250 dev en0 lladdr 1:0:5e:7f:ff:fa REACHABLE
```

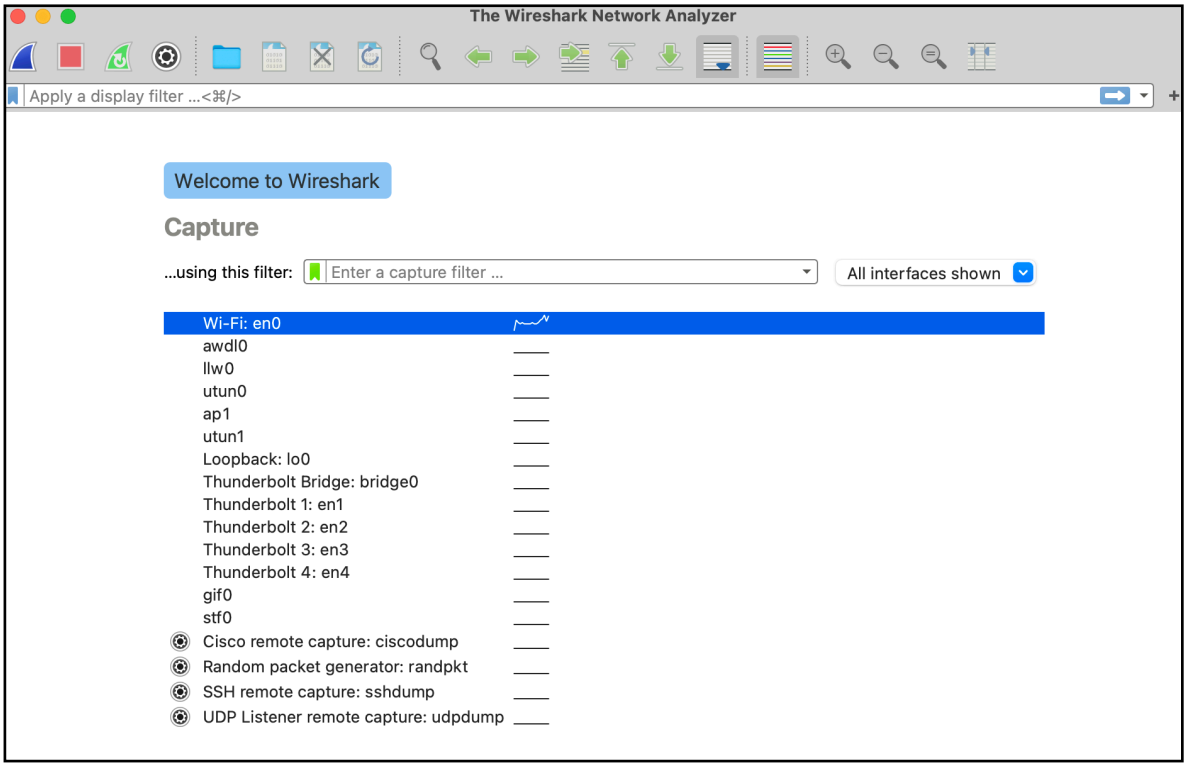
Task 2 :

Ping PDU (Packet Data Units or Packets) Capture

Step 1: Assign an IP address to the system (Host).

```
sh-3.2# sudo ifconfig lo0 192.168.0.100 netmask 255.255.255.0
```

Step 2: Launch Wireshark

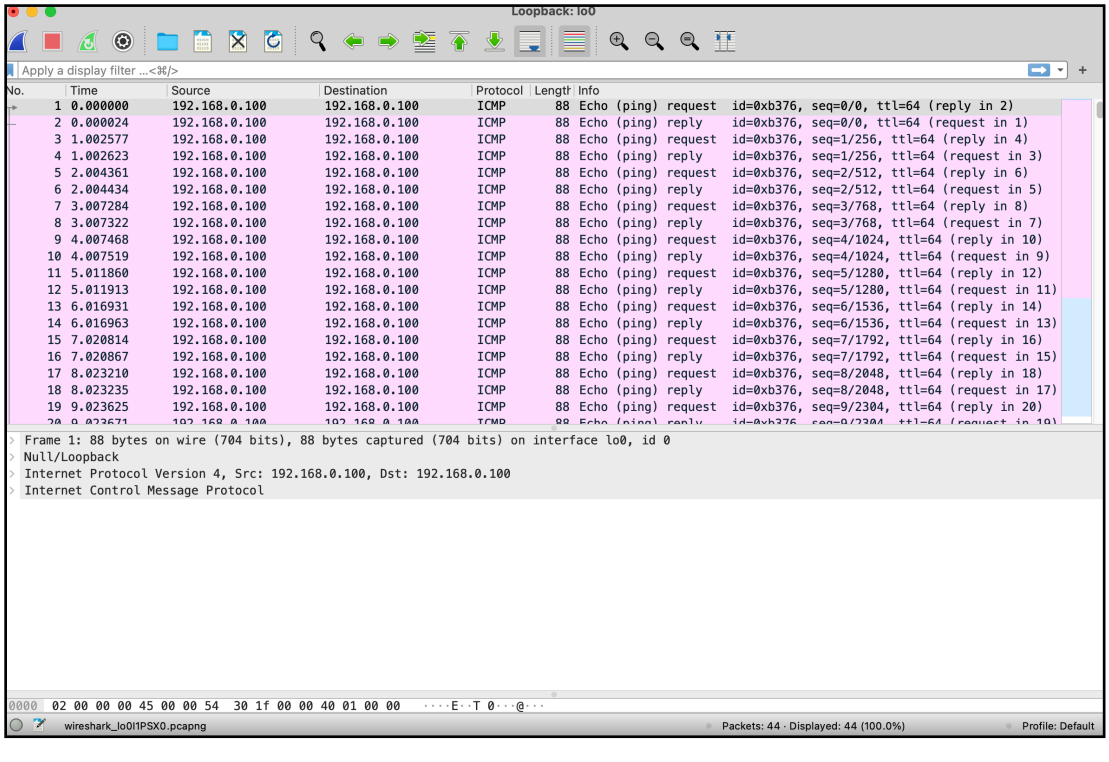


Step 3: Pinging

```
sh-3.2# sudo ifconfig lo0 192.168.0.100 netmask 255.255.255.0
sh-3.2# ping 192.168.0.100
PING 192.168.0.100 (192.168.0.100): 56 data bytes
64 bytes from 192.168.0.100: icmp_seq=0 ttl=64 time=0.053 ms
64 bytes from 192.168.0.100: icmp_seq=1 ttl=64 time=0.125 ms
64 bytes from 192.168.0.100: icmp_seq=2 ttl=64 time=0.137 ms
64 bytes from 192.168.0.100: icmp_seq=3 ttl=64 time=0.121 ms
64 bytes from 192.168.0.100: icmp_seq=4 ttl=64 time=0.088 ms
64 bytes from 192.168.0.100: icmp_seq=5 ttl=64 time=0.124 ms
64 bytes from 192.168.0.100: icmp_seq=6 ttl=64 time=0.076 ms
64 bytes from 192.168.0.100: icmp_seq=7 ttl=64 time=0.122 ms
64 bytes from 192.168.0.100: icmp_seq=8 ttl=64 time=0.061 ms
64 bytes from 192.168.0.100: icmp_seq=9 ttl=64 time=0.101 ms
64 bytes from 192.168.0.100: icmp_seq=10 ttl=64 time=0.105 ms
64 bytes from 192.168.0.100: icmp_seq=11 ttl=64 time=0.118 ms
64 bytes from 192.168.0.100: icmp_seq=12 ttl=64 time=0.078 ms
64 bytes from 192.168.0.100: icmp_seq=13 ttl=64 time=0.103 ms
^C
--- 192.168.0.100 ping statistics ---
14 packets transmitted, 14 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.053/0.101/0.137/0.025 ms
```

Step4: Analysis

- TTL - 64
- Protocol used by ping - ICMP
- Time - 0.101ms on average



First Echo Request from Wireshark:

```
Frame 1: 88 bytes on wire (704 bits), 88 bytes captured (704 bits) on interface lo0, id 0
  > Interface id: 0 (lo0)
    Encapsulation type: NULL/Loopback (15)
    Arrival Time: Jan 23, 2021 23:04:52.100384000 IST
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1611423292.100384000 seconds
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]
    Frame Number: 1
    Frame Length: 88 bytes (704 bits)
    Capture Length: 88 bytes (704 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: null:ip:icmp:data]
    [Coloring Rule Name: ICMP]
    [Coloring Rule String: icmp || icmpv6]
Null/Loopback
    Family: IP (2)
Internet Protocol Version 4, Src: 192.168.0.100, Dst: 192.168.0.100
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x301f (12319)
  > Flags: 0x00
    Fragment Offset: 0
    Time to Live: 64
    Protocol: ICMP (1)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.0.100
    Destination Address: 192.168.0.100
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x1335 [correct]
    [Checksum Status: Good]
    Identifier (BE): 45942 (0xb376)
    Identifier (LE): 30387 (0x76b3)
    Sequence Number (BE): 0 (0x0000)
    Sequence Number (LE): 0 (0x0000)
    [Response frame: 2]
```

First Echo Response from Wireshark:

```
Frame 2: 88 bytes on wire (704 bits), 88 bytes captured (704 bits) on interface lo0, id 0
  > Interface id: 0 (lo0)
    Encapsulation type: NULL/Loopback (15)
    Arrival Time: Jan 23, 2021 23:04:52.100408000 IST
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1611423292.100408000 seconds
    [Time delta from previous captured frame: 0.000024000 seconds]
    [Time delta from previous displayed frame: 0.000024000 seconds]
    [Time since reference or first frame: 0.000024000 seconds]
    Frame Number: 2
    Frame Length: 88 bytes (704 bits)
    Capture Length: 88 bytes (704 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: null:ip:icmp:data]
    [Coloring Rule Name: ICMP]
    [Coloring Rule String: icmp || icmpv6]
Null/Loopback
    Family: IP (2)
Internet Protocol Version 4, Src: 192.168.0.100, Dst: 192.168.0.100
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x0a58 (2648)
  > Flags: 0x00
    Fragment Offset: 0
    Time to Live: 64
    Protocol: ICMP (1)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.0.100
    Destination Address: 192.168.0.100
Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x1b35 [correct]
    [Checksum Status: Good]
    Identifier (BE): 45942 (0xb376)
    Identifier (LE): 30387 (0x76b3)
    Sequence Number (BE): 0 (0x0000)
    Sequence Number (LE): 0 (0x0000)
    [Request frame: 1]
```

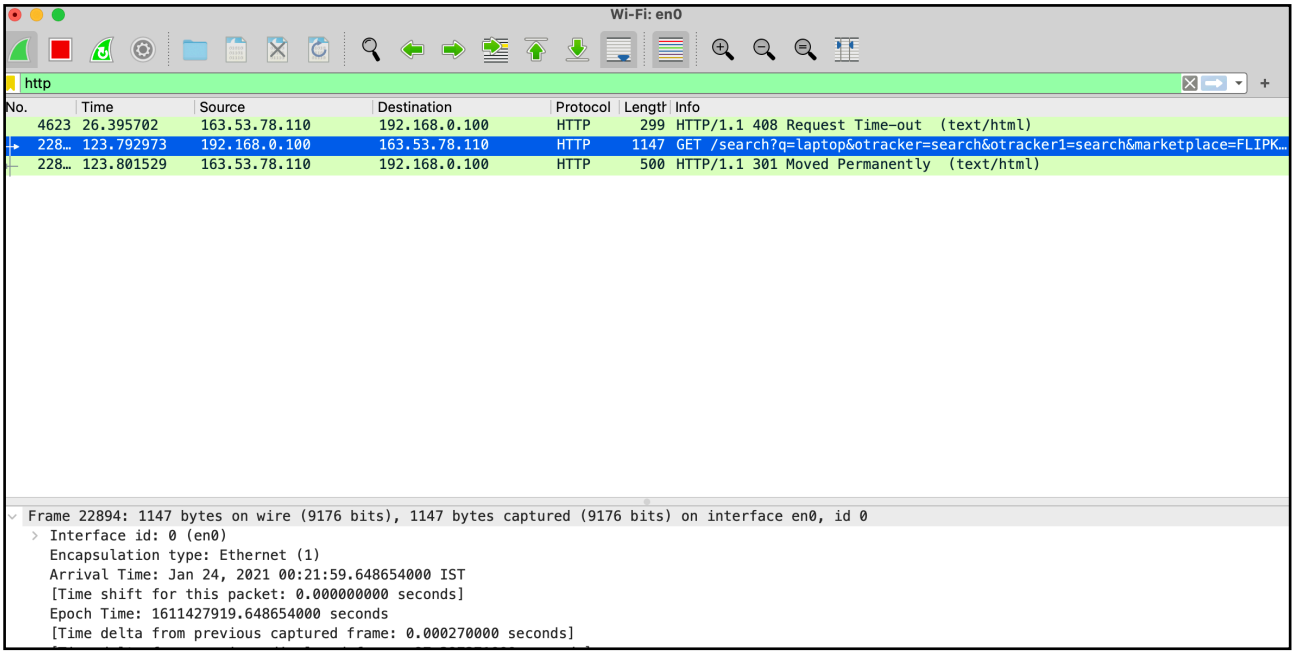
Observation:

Details	First Echo Request	First Echo Reply
Frame Number	1	2
Source IP address	192.168.0.100	192.168.0.100
Destination IP address	192.168.0.100	192.168.0.100
ICMP Type Value	8	0
ICMP Code Value	0	0
Source Ethernet Address	38:f9:d3:c0:fb:14	38:f9:d3:c0:fb:14
Destination Ethernet Address	38:f9:d3:c0:fb:14	38:f9:d3:c0:fb:14
Internet Protocol Version	ICMP	ICMP
Time To Live (TTL) Value	64	64

Task 3:

HTTP PDU Capture (Using Wireshark's Filter feature)

Step 1: Launch Wireshark. On the Filter toolbar, type-in 'http'



Step 2: Opened Safari browser, and browsed www.flipkart.com

First Echo Request to http://www.flipkart.com

```
> Frame 22894: 1147 bytes on wire (9176 bits), 1147 bytes captured (9176 bits) on interface en0, id 0
> Ethernet II, Src: Apple_c0:fb:14 (38:f9:d3:c0:fb:14), Dst: Tp-LinkT_ec:75:00 (d8:07:b6:ec:75:00)
> Internet Protocol Version 4, Src: 192.168.0.100, Dst: 163.53.78.110
v Transmission Control Protocol, Src Port: 55228, Dst Port: 80, Seq: 1, Ack: 1, Len: 1081
    Source Port: 55228
    Destination Port: 80
    [Stream index: 64]
    [TCP Segment Len: 1081]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 135137345
    [Next Sequence Number: 1082    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 1519254977
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x018 (PSH, ACK)
    Window: 2063
    [Calculated window size: 132032]
    [Window size scaling factor: 64]
    Checksum: 0x6a8e [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  > [SEQ/ACK analysis]
  > [Timestamps]
    TCP payload (1081 bytes)
v Hypertext Transfer Protocol
  > GET /search?q=laptop&otracker=search&otracker1=search&marketplace=FLIPKART&as-show=on&as=off HTTP/1.1\r\n
    Host: www.flipkart.com\r\n
    Connection: keep-alive\r\n
    DNT: 1\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 11_1_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.96 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
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-IN,en-GB;q=0.9,en-US;q=0.8,en;q=0.7\r\n
  > [truncated]Cookie: SN=VIB27FEEBDC7D34791B382735E6B9EF22D.TOK9750813038804B1A9387C0079221695F.1611427832.LO; AMCVS_17EB401053DAF4840A490D4C%40AdobeOrg=1; AMCV_17EB401053DAF4
    \r\n
    [Full request URI: http://www.flipkart.com/search?q=laptop&otracker=search&otracker1=search&marketplace=FLIPKART&as-show=on&as=off]
    [HTTP request 1/1]
    [Response in frame: 22895]
```

First Echo Response to http://www.flipkart.com

```
> Frame 22895: 500 bytes on wire (4000 bits), 500 bytes captured (4000 bits) on interface en0, id 0
> Ethernet II, Src: Tp-LinkT_ec:75:00 (d8:07:b6:ec:75:00), Dst: Apple_c0:fb:14 (38:f9:d3:c0:fb:14)
> Internet Protocol Version 4, Src: 163.53.78.110, Dst: 192.168.0.100
v Transmission Control Protocol, Src Port: 80, Dst Port: 55228, Seq: 1, Ack: 1082, Len: 434
    Source Port: 80
    Destination Port: 55228
    [Stream index: 64]
    [TCP Segment Len: 434]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 1519254977
    [Next Sequence Number: 435    (relative sequence number)]
    Acknowledgment Number: 1082    (relative ack number)
    Acknowledgment number (raw): 135138426
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x018 (PSH, ACK)
    Window: 60
    [Calculated window size: 30720]
    [Window size scaling factor: 512]
    Checksum: 0x0175 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  > [SEQ/ACK analysis]
  > [Timestamps]
    TCP payload (434 bytes)
v Hypertext Transfer Protocol
  > HTTP/1.1 301 Moved Permanently\r\n
    Server: nginx\r\n
    Date: Sat, 23 Jan 2021 18:51:59 GMT\r\n
    Content-Type: text/html\r\n
  > Content-Length: 178\r\n
    Location: https://www.flipkart.com/search?q=laptop&otracker=search&otracker1=search&marketplace=FLIPKART&as-show=on&as=off\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.008556000 seconds]
    [Request in frame: 22894]
    [Request URI: http://www.flipkart.com/search?q=laptop&otracker=search&otracker1=search&marketplace=FLIPKART&as-show=on&as=off]
    File Data: 178 bytes
> Line-based text data: text/html (7 lines)
```

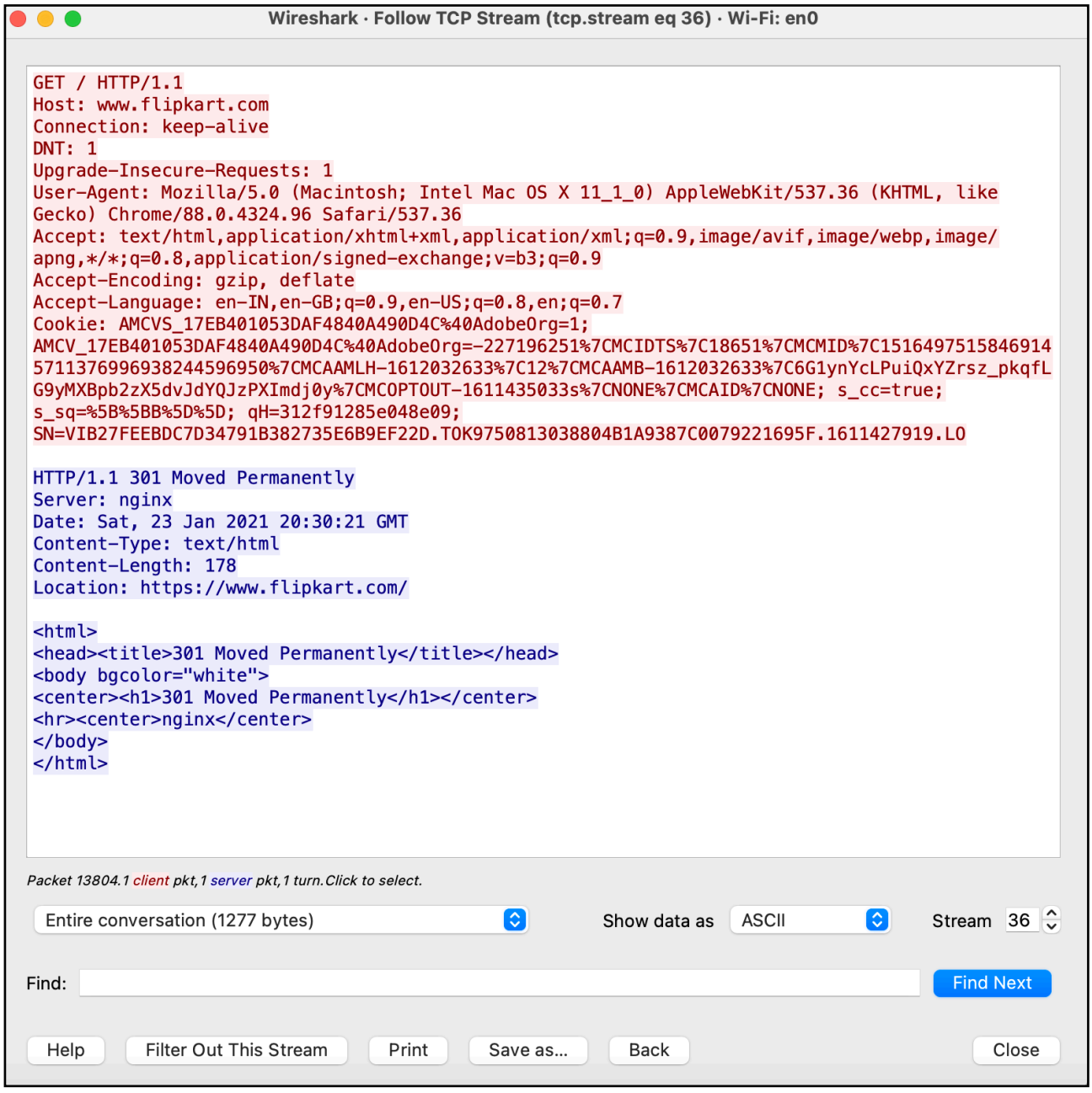
Step 3: Analyse the first (interaction of host to the web server) and second frame (response of server to the client). By analysing the filtered frames, complete the table below:

Details	First Echo Request	First Echo Reply
Frame Number	22894	22895
Source Port	55228	80
Destination Port	80	55228
Source IP address	192.168.0.100	163.53.78.110
Destination IP address	163.53.78.110	192.168.0.100
Source Ethernet Address	38:f9:d3:c0:fb:14	d8:07:b6:ec:75:00
Destination Ethernet Address	d8:07:b6:ec:75:00	38:f9:d3:c0:fb:14

Step 4: Analyse the HTTP request and response and complete the table below.

HTTP Request		HTTP Response	
Get	/HTTP/1.1\r\n	**Server**	nginx\r\n
Host	www.flipkart.com	**Content-Type**	text/html\r\n
User-Agent	Mozilla/5.0 (Macintosh; Intel Mac OS X 11_1_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.96 Safari/537.36\r\n	**Date**	Sat, 23 Jan 2021 18:51:59 GMT\r\n
Accept-Language	en-IN,en-GB;q=0.9,en-US;q=0.8,en;q=0.7\r\n	**Location**	http://www.flipkart.com/
Accept-Encoding	gzip, deflate\r\n	**Content-Length**	178\r\n
Connection	keep-alive	**Connection**	keep-alive

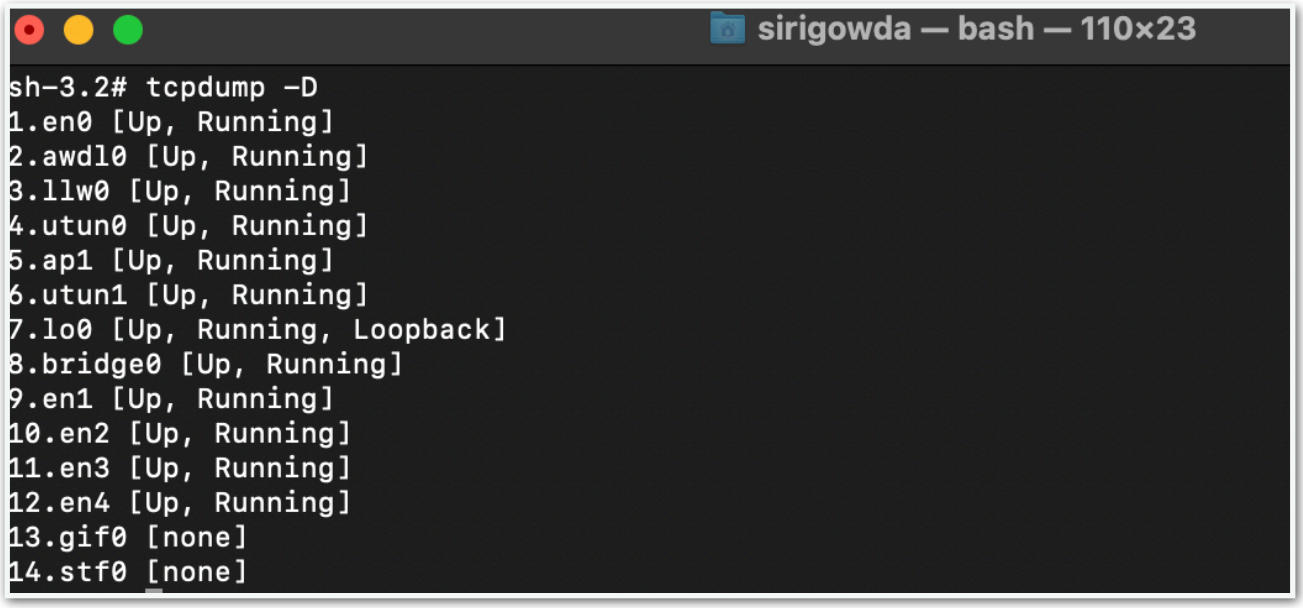
Using Wireshark's Follow TCP Stream



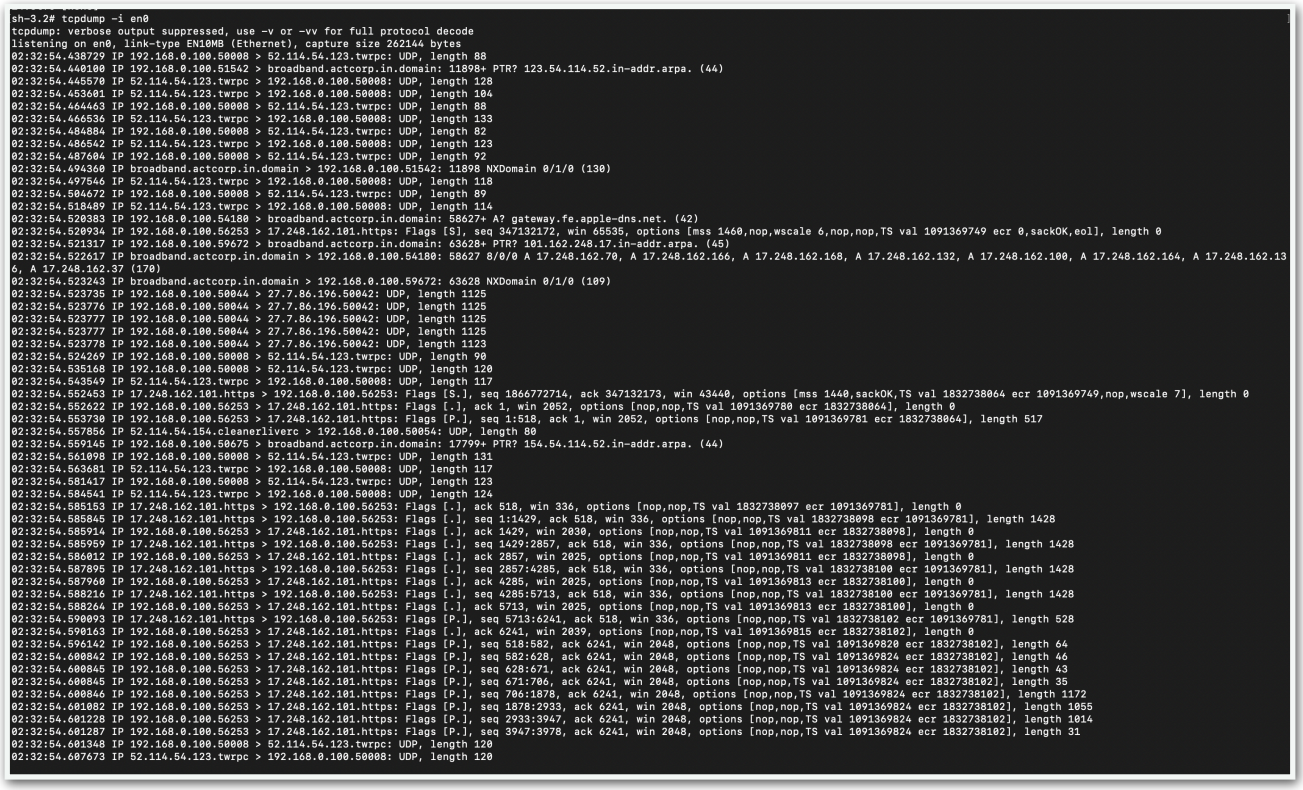
Task 4:

Capturing packets with tcpdump

Step 1: On running tcpdump -D in shell:



Step 2: Performing some pinging operation, while capturing packets and running www.google.com



Observation

Step 3: Understanding the output format.

[Time request made] IP [source]>[Destination] : [protocol type], id [id], seq [seq], length[length]

Step 4: To filter packets based on protocol, specifying the protocol in the command line. Here, we're filtering UDP packets.

```
sh-3.2# sudo tcpdump -i en0 -c5 udp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on en0, link-type EN10MB (Ethernet), capture size 262144 bytes
16:08:33.756945 IP 192.168.0.100.64556 > 239.255.255.250.ssdp: UDP, length 174
16:08:34.758073 IP 192.168.0.100.64556 > 239.255.255.250.ssdp: UDP, length 174
16:08:35.759176 IP 192.168.0.100.64556 > 239.255.255.250.ssdp: UDP, length 174
16:08:38.134991 IP 192.168.0.100.64623 > maa03s31-in-f14.1e100.net.https: UDP, length 1345
16:08:38.135035 IP 192.168.0.100.64623 > maa03s31-in-f14.1e100.net.https: UDP, length 121
5 packets captured
12 packets received by filter
0 packets dropped by kernel
```

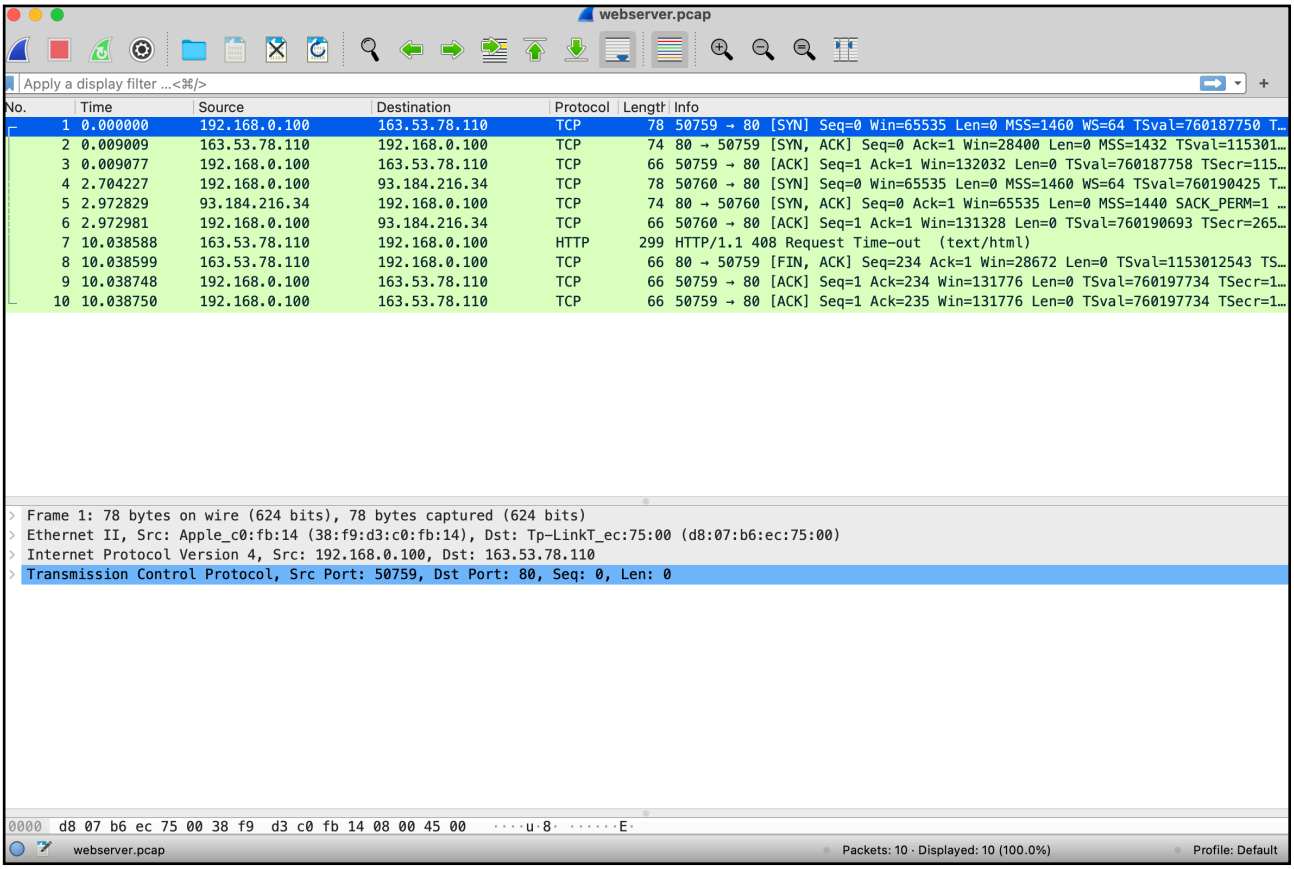
Step 5: Check the packet content. For example, inspect the HTTP content of a web request

```
sh-3.2# sudo tcpdump -i en0 -c10 -nn -A port 80
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on en0, link-type EN10MB (Ethernet), capture size 262144 bytes
16:15:03.157917 IP 192.168.0.100.50290 > 93.184.216.34.80: Flags [S], seq 1456324385, win 65535, options [mss 1460,nop,wscale 6,nop,nop,TS val 756846939 ecr 0,sackOK,eol], length 0
E..@..@.@.C....d]..".r.PV..!.....................
-..[........
16:15:03.377977 IP 93.184.216.34.80 > 192.168.0.100.50290: Flags [S.], seq 3555293196, ack 1456324386, win 65535, options [mss 1440,sackOK,TS val 2375542693 ecr 756846939,nop,wscale 9], length 0
E .<VS..3.:b]..".."...d.P.r..x.V..".............
....-..[...
16:15:03.378127 IP 192.168.0.100.50290 > 93.184.216.34.80: Flags [.], ack 1, win 2052, options [nop,nop,TS val 756847153 ecr 2375542693], length 0
E..4..@.@.C....d]..".r.PV.."..x.....
-..1....
16:15:03.378645 IP 192.168.0.100.50290 > 93.184.216.34.80: Flags [P.], seq 1:471, ack 1, win 2052, options [nop,nop,TS val 756847153 ecr 2375542693], length 470: HTTP: GET / HTTP/1.1
E..
..@.@.B....d]..".r.PV.."..x......Y.....
-..1....GET / HTTP/1.1
Host: www.example.com
Connection: keep-alive
DNT: 1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 11_1_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.96 Safari/537.36
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
Accept-Encoding: gzip, deflate
Accept-Language: en-IN,en-GB;q=0.9,en-US;q=0.8,en;q=0.7


16:15:03.598630 IP 93.184.216.34.80 > 192.168.0.100.50290: Flags [.], ack 471, win 131, options [nop,nop,TS val 2375542914 ecr 756847153], length 0
E .4Va..3.:\]..".."...d.P.r..x.V.......!k.....
....-..1
16:15:03.599027 IP 93.184.216.34.80 > 192.168.0.100.50290: Flags [P.], seq 1:1023, ack 471, win 131, options [nop,nop,TS val 2375542914 ecr 756847153], length 1022: HTTP: HTTP/1.1 200 OK
E .2Vb..3.6]]..".."...d.P.r..x.V.............
....-..1HTTP/1.1 200 OK
Content-Encoding: gzip
Accept-Ranges: bytes
Age: 351302
Cache-Control: max-age=604800
Content-Type: text/html; charset=UTF-8
Date: Sun, 24 Jan 2021 10:45:03 GMT
Etag: "3147526947"
Expires: Sun, 31 Jan 2021 10:45:03 GMT
Last-Modified: Thu, 17 Oct 2019 07:18:26 GMT
Server: ECS (dcb/7F17)
Vary: Accept-Encoding
X-Cache: HIT
Content-Length: 648
```

```
2 packets captured
28 packets received by filter
0 packets dropped by kernel
```

Step 6: To save packets to a file instead of displaying them on screen, use the option -w:

- Opening webserver.pcap from wireshark



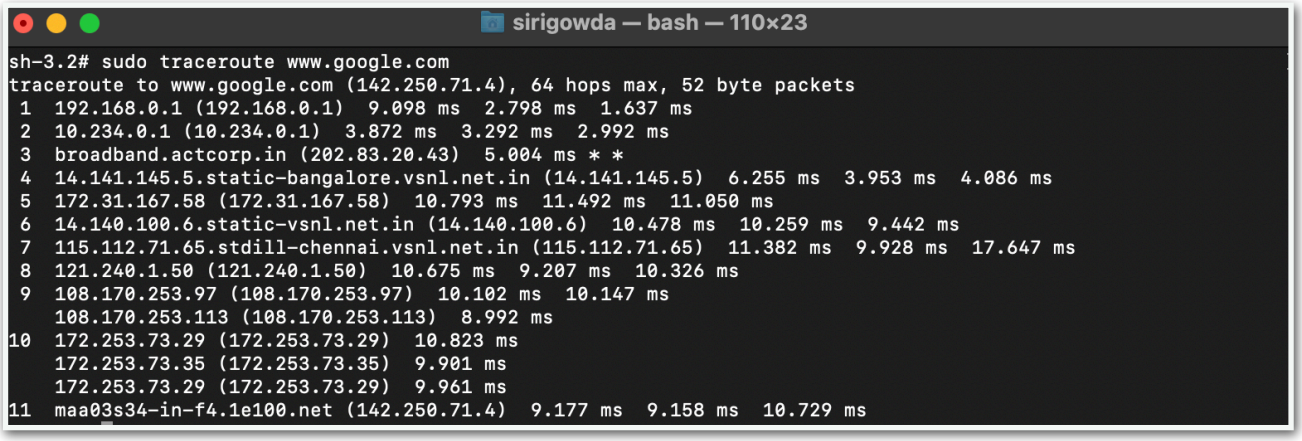
- Command in the terminal:

```
sh-3.2# sudo tcpdump -i en0 -c10 -nn -w webserver.pcap port 80
tcpdump: listening on en0, link-type EN10MB (Ethernet), capture size 262144 bytes
10 packets captured
2543 packets received by filter
0 packets dropped by kernel
```

Task 5:

Perform Traceroute checks

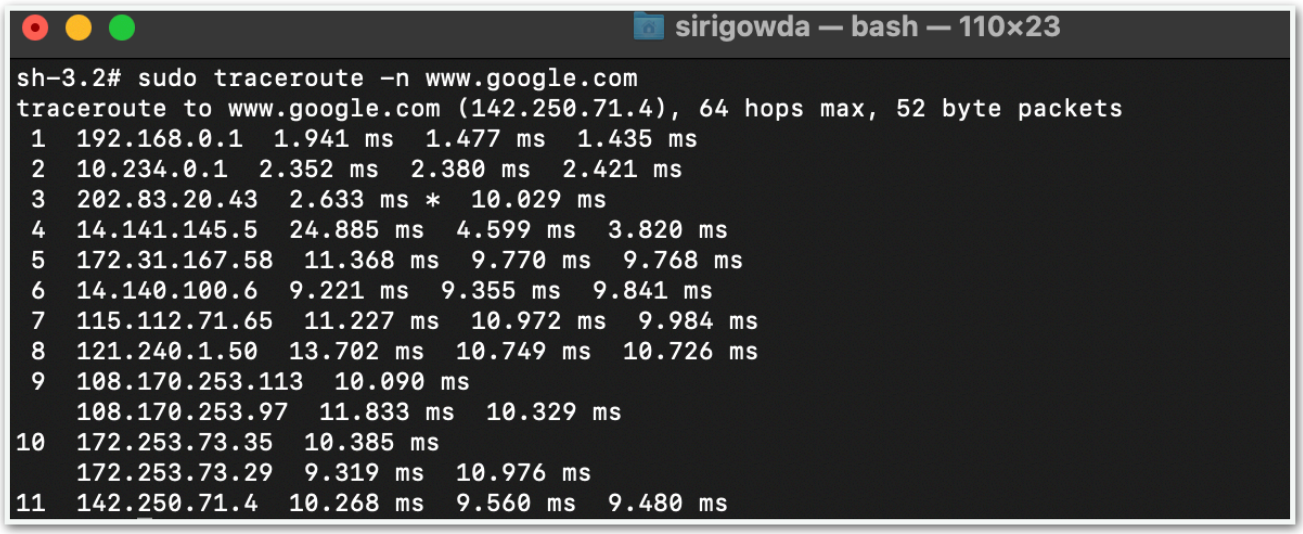
Step 1: Tracing the route to www.google.com



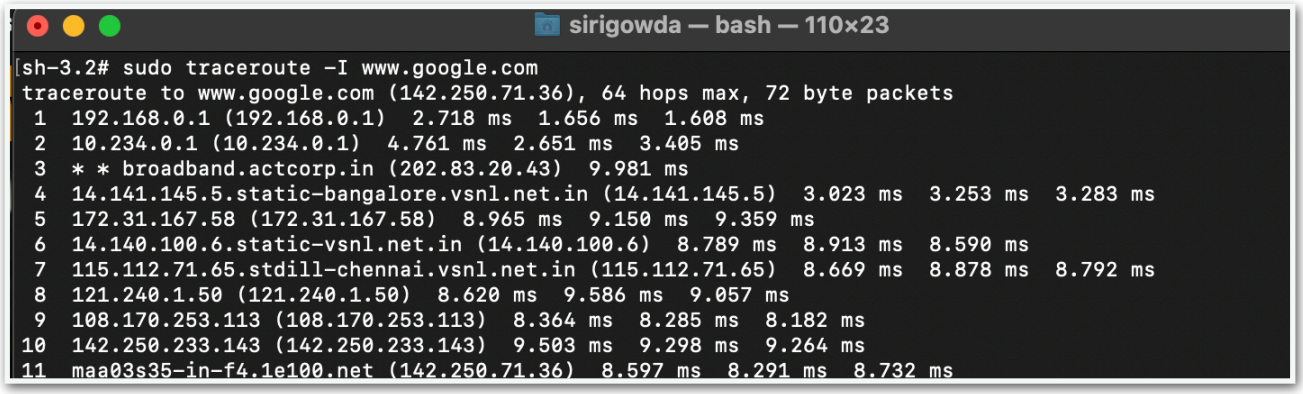
Step 2: Analysis of the destination address of google.com and no. of hops

- The maximum number of hops : 64
- The number hops www.google.com took: 11
- The destination address of www.google.com : 142.250.71.4
- The size of packets : 52 bytes

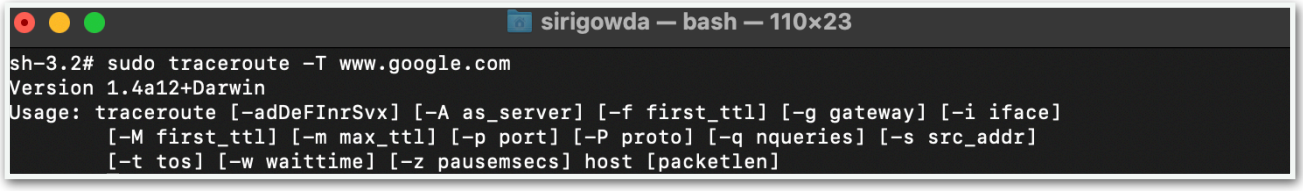
Step 3: To speed up the process we can disable the mapping of IP addresses with hostnames



Step 4: For traceroute to use ICMP.



Step 5: To test the TCP connection to a website, we can use the -T option instead of the default ICMP packets.



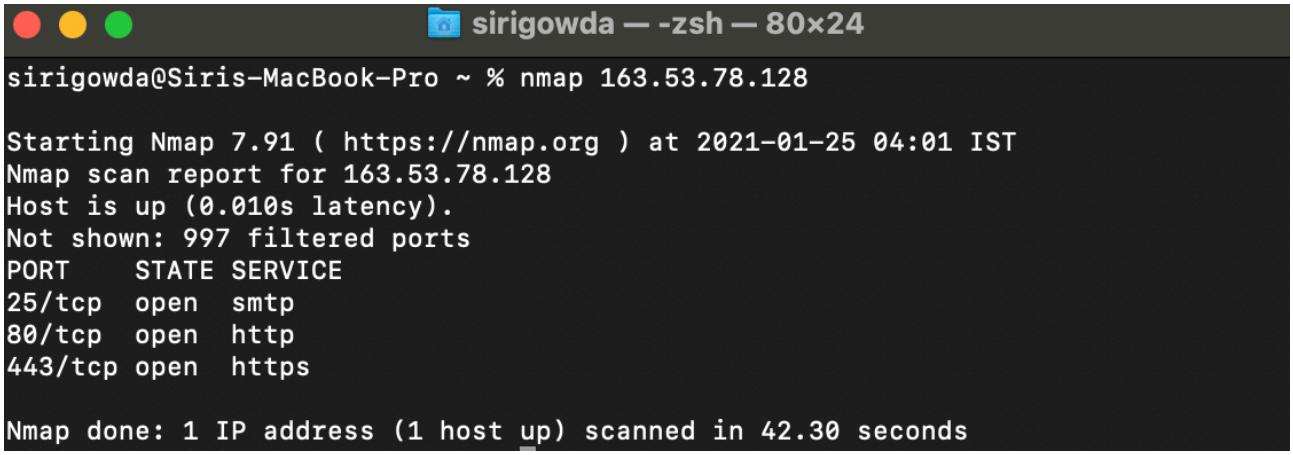
Task 6:

Explore an entire network for information (Nmap)

Step 1: Scanning a host to get various details about the host like name, port etc

```
sirigowda@Siris-MacBook-Pro ~ % nmap www.pes.edu
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-25 03:58 IST
Nmap scan report for www.pes.edu (13.71.123.138)
Host is up (0.013s latency).
Not shown: 997 filtered ports
PORT    STATE SERVICE
25/tcp  open  smtp
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 42.92 seconds
```

Step 2: Alternatively, using an IP address to scan.



Step 3: Scanning multiple IP address or subnet (IPv4)

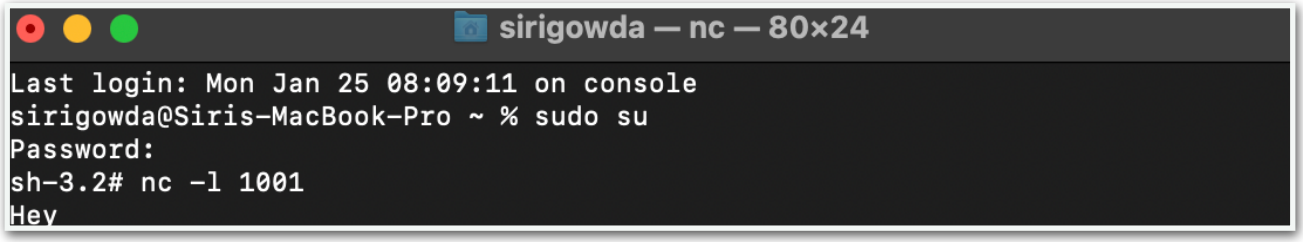
Task 7a

Netcat as Chat tool

a) Intra system communication (Using 2 terminals in the same system)

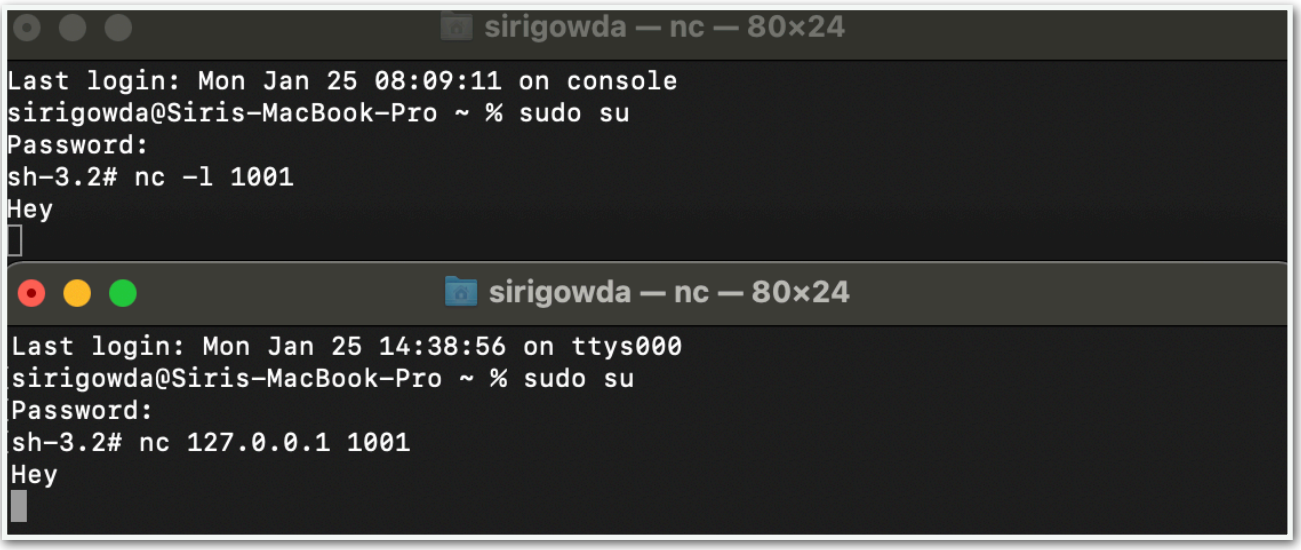
Step 1: Opening a terminal that acts as a server

Step 2: Setting up a server (It will go to listening mood)



Step 3: Opening another terminal that acts as a client

Server and Client

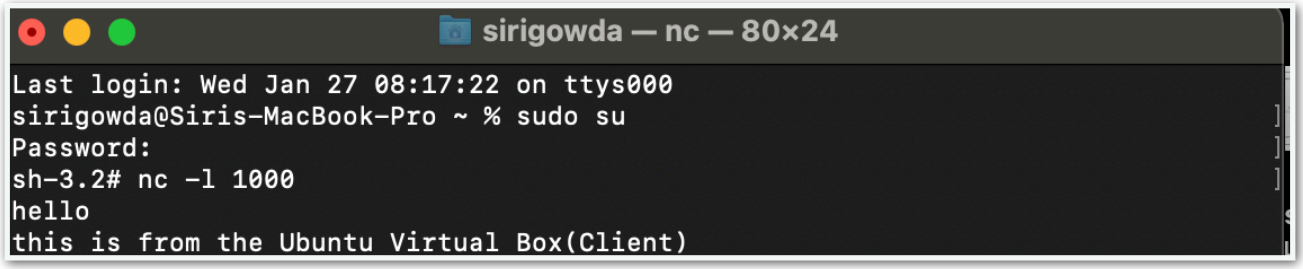


The string "hey" in the client terminal infers the connection between the server and client.

b) Inter System Communication

In this case, Server is macOS and client is Ubuntu Virtual Box.

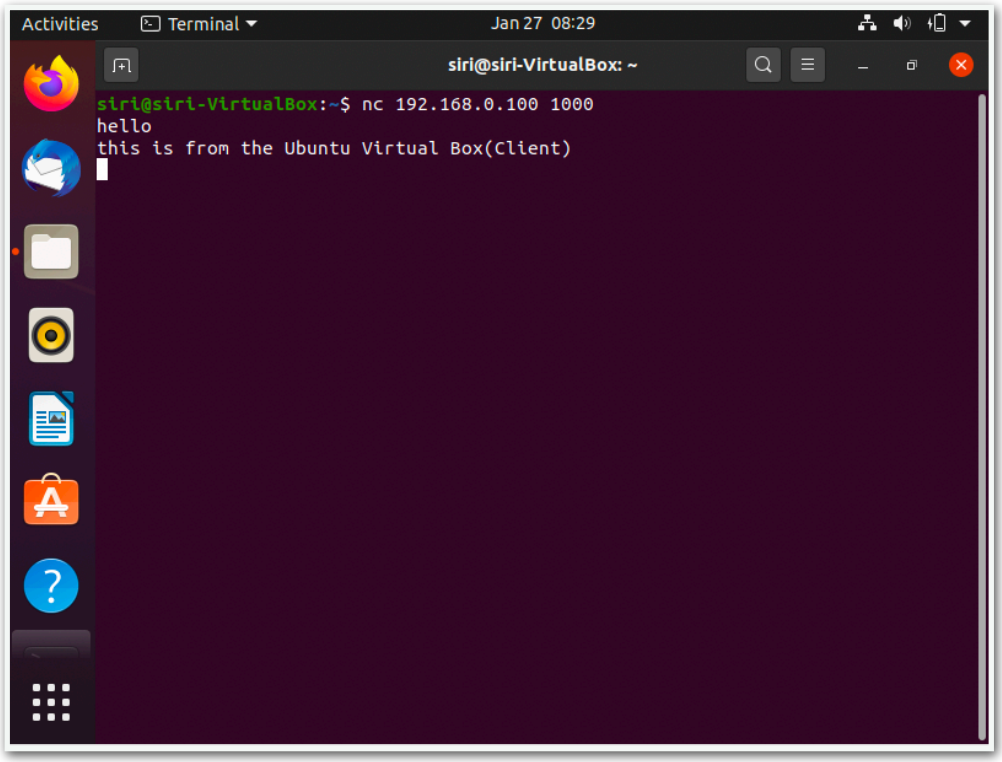
Setting Up a server on macOS:



Setting up a client on Ubuntu and sending 2 Messages:

-hello

-This is from the Ubuntu Virtual Box(client)

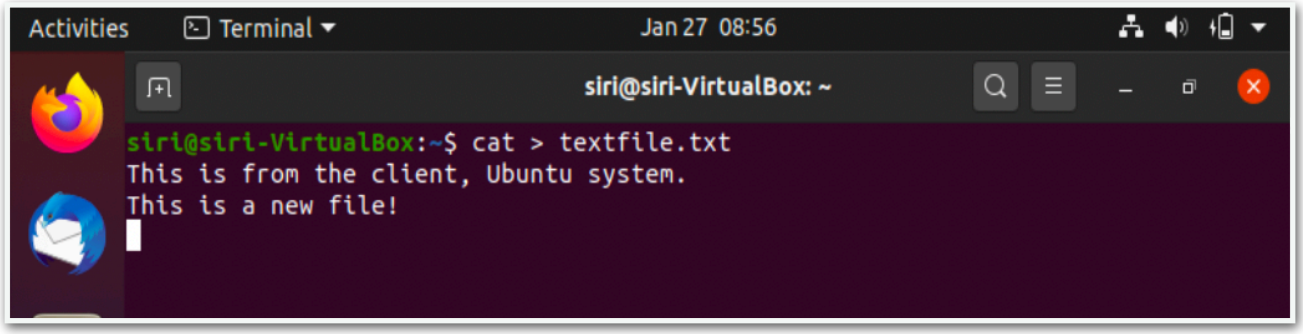


This shows that whatever is typed in the Client, comes in the server. Therefore, a connection has been established.

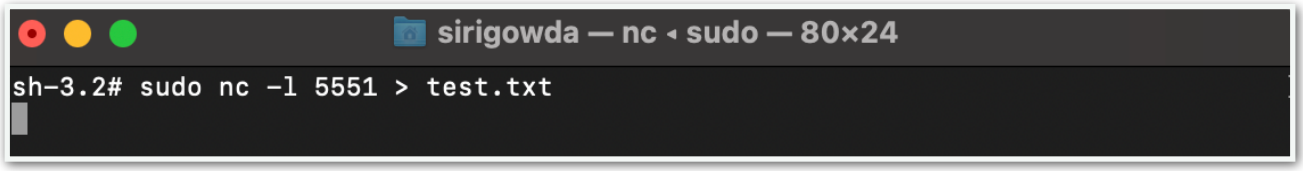
Task 7b :

Use Netcat to Transfer Files

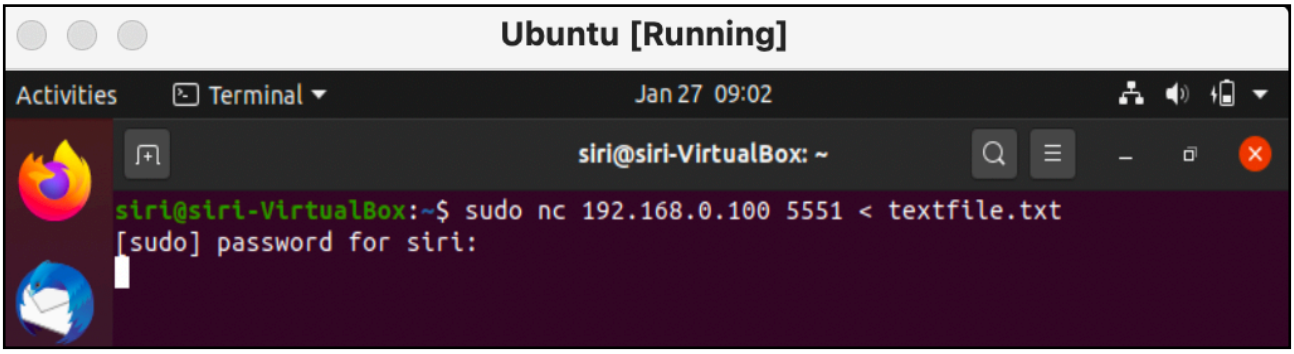
A file called textile.txt is created on the client side with the following content.



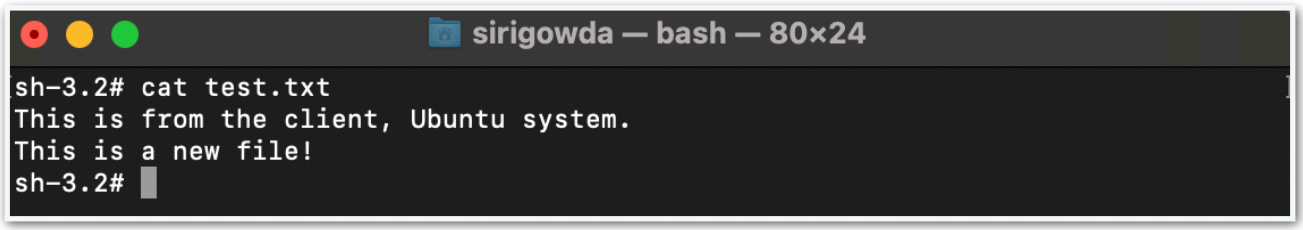
Running: "sudo nc -l 5551 > test.txt" on server.



Running : "sudo nc 192.168.56.1 5551 < textfile.txt" on Client.



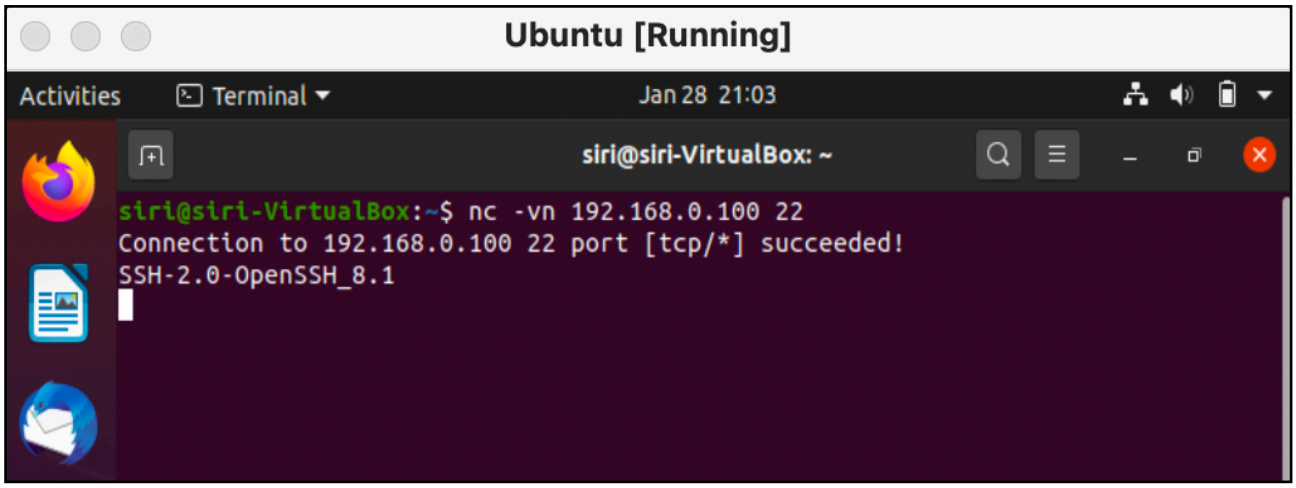
Then running cat test.txt in the server gives the following output:



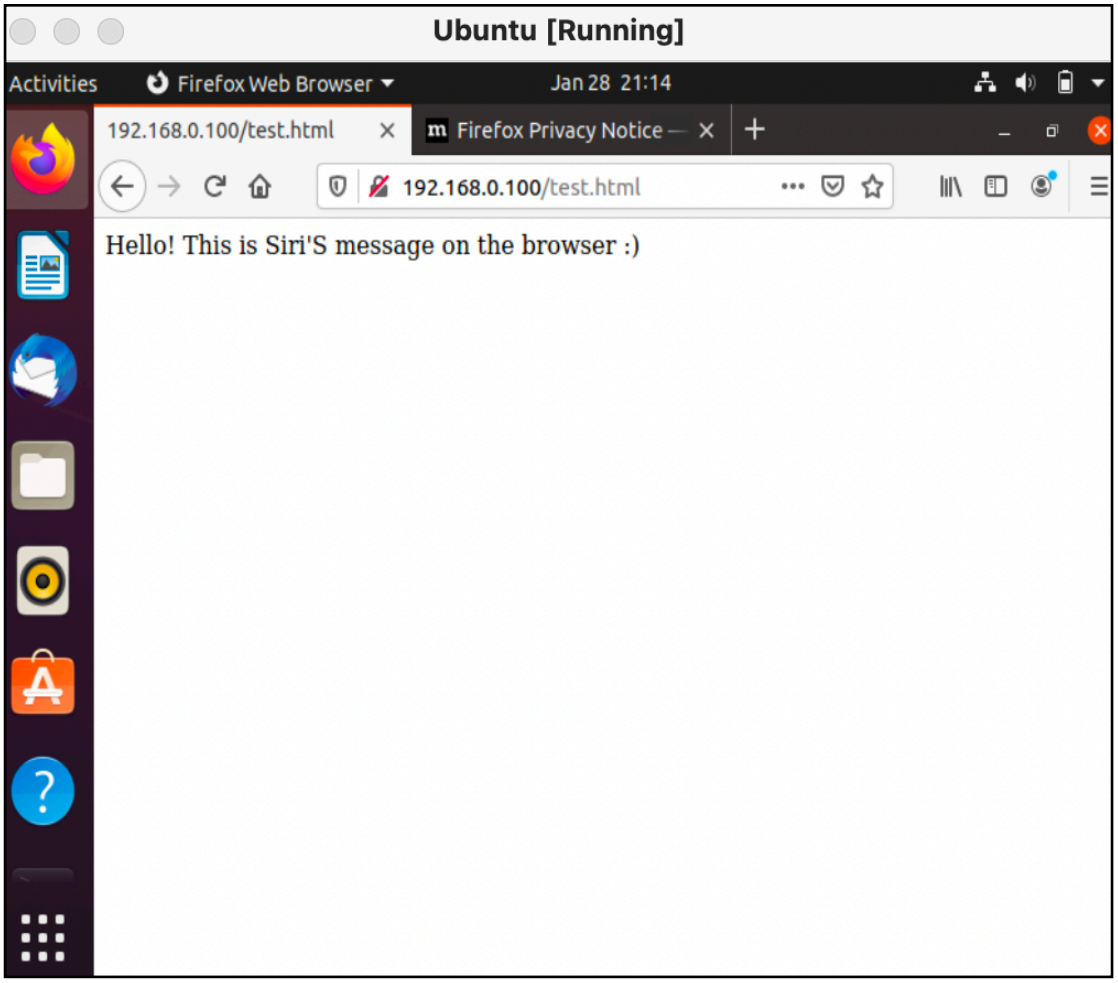
Task 7c :

Other Commands

Step 1: Testing if a particular TCP port of a remote host is open.



Step 2: Running a web server with a static web page.



Step 3: Observing the details on the terminal

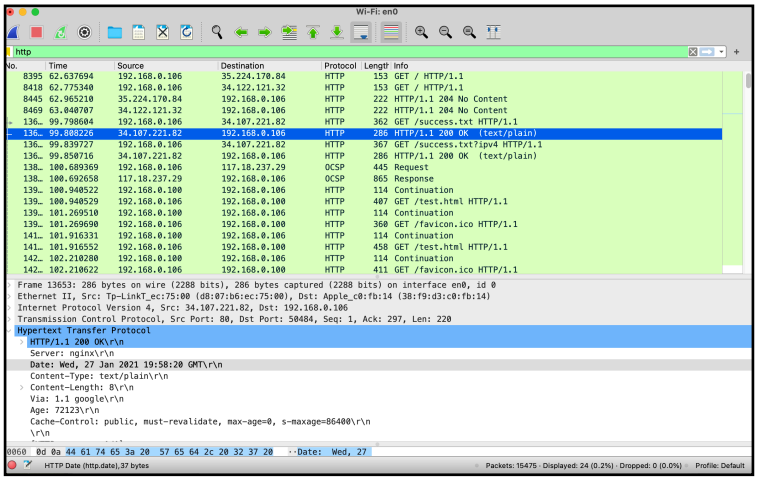
```
sirigowda — nc ◂ sudo — 98×32
Last login: Thu Jan 28 08:26:57 on console
sh-3.2# cat test.html
Hello! This is Siri'S message on the browser :)
sh-3.2# while true; do sudo nc -l 80 < test.html; done
GET /test.html HTTP/1.1
Host: 192.168.0.100
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:84.0) Gecko/20100101 Firefox/84.0
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

GET /favicon.ico HTTP/1.1
Host: 192.168.0.100
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:84.0) Gecko/20100101 Firefox/84.0
Accept: image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://192.168.0.100/test.html
```

Questions on above observations:

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

My browser is running HTTP version 1.1 and the HTTP version of the server is 1.1

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



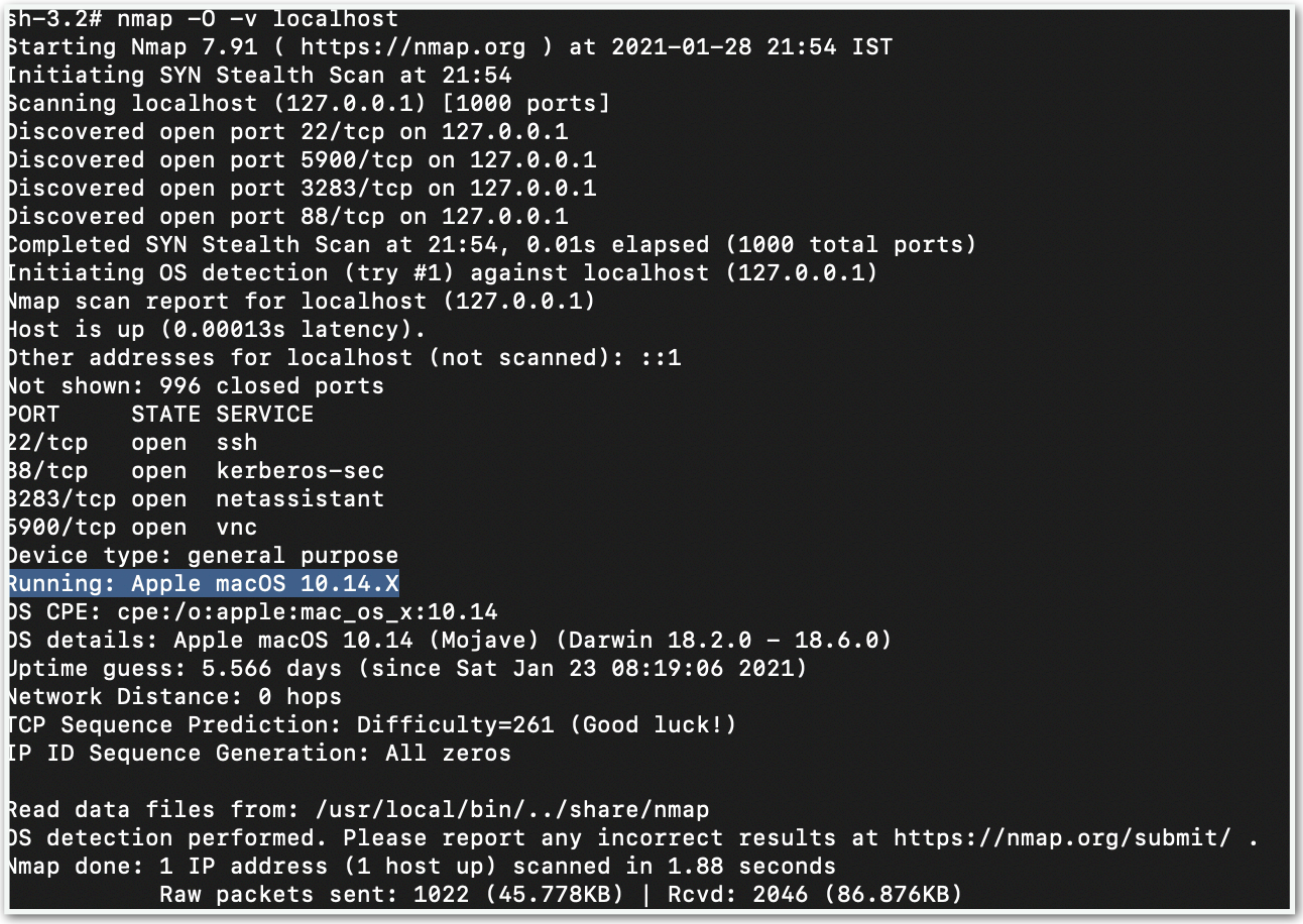
Last modified at: Wed, 27 Jan 2021 19:58:20 GMT\r\n

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

We can specify the number of ECHO_REQUEST packets with the help of the command: ping -c 3 <Website URL>

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

We can identify the remote host OS using the command: nmap -O -v localhost



— —