

# **COMPUTER NETWORKS LABORATORY**

## **WEEK #1**

NAME : SIRI S  
SEMESTER : 4  
SECTION : H  
SRN : PESIUGI9CS485

### **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 brd 127.0.0.1 scopeid 0x1
        ether 00:00:00:00:00:00
        brd 00:00:00:00:00:00
        inet6 fe80::1/128 brd fe80::ff:fe00:1 scopeid 0x1
            ether 00:00:00:00:00:00
            brd fe80::ff:fe00:1
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 brd fe80::ff:fe00:1122 scopeid 0x4
        ether ac:de:48:00:11:22
        brd fe80::ff:fe00:1122
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 brd fe80::ff:fe00:1012:38c9:1a86:ab3c secured scopeid 0x6
        ether 38:f9:d3:c0:fb:14
        brd fe80::ff:fe00:1012:38c9:1a86:ab3c
        inet 192.168.0.100/24 brd 192.168.0.255 scopeid 0x1
            ether 38:f9:d3:c0:fb:14
            brd 192.168.0.255
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 brd fe80::ff:fe00:6cab:62ff:fe98:817a scopeid 0x7
        ether 6e:ab:62:98:81:7a
        brd fe80::ff:fe00:6cab:62ff:fe98:817a
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 brd fe80::ff:fe00:6cab:62ff:fe98:817a scopeid 0x8
        ether 6e:ab:62:98:81:7a
        brd fe80::ff:fe00:6cab:62ff:fe98:817a
utun0: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1380
    ether 4635:63c5:54f9:e7fc/64 brd 4635:63c5:54f9:e7fc scopeid 0xe
        ether 4635:63c5:54f9:e7fc
        brd 4635:63c5:54f9:e7fc
utun1: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 2000
    ether 4f1e:8e38:d8be:855d/64 brd 4f1e:8e38:d8be:855d scopeid 0xf
        ether 4f1e:8e38:d8be:855d
        brd 4f1e:8e38:d8be:855d]
```

## **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 brd 127.0.0.1 scopeid 0x1
        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 0xffff0000
        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::aebe:4bff%en5 prefixlen 64 scopeid 0x4
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect (100baseTX <full-duplex>)
            status: active
api1: 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 0xffffffff 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%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%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<TS04,TS06,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<TS04,TS06,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<TS04,TS06,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<TS04,TS06,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,TS04,TS06>
    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:8e38:08be:855d%utun1 prefixlen 64 scopeid 0xf
        nd6 options=201<PERFORMNUD,DAD>
```

en0 up:

```
sn-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 0xffff00000
    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%en5 prefixlen 64 scopeid 0x4
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect (100baseTX <full-duplex>)
        status: active
api1: 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 0xffffffff broadcast 192.168.0.255
    inet6 fe80::1012:38c9:1a86:ab3c%en0 prefixlen 64 secured scopeid 0x6
    inet 192.168.0.100 netmask 0xffffffff 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<TS04, TS06, 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<TS04, TS06, 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<TS04, TS06, 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<TS04, TS06, 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,TS04,TS06>
    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]
```

---

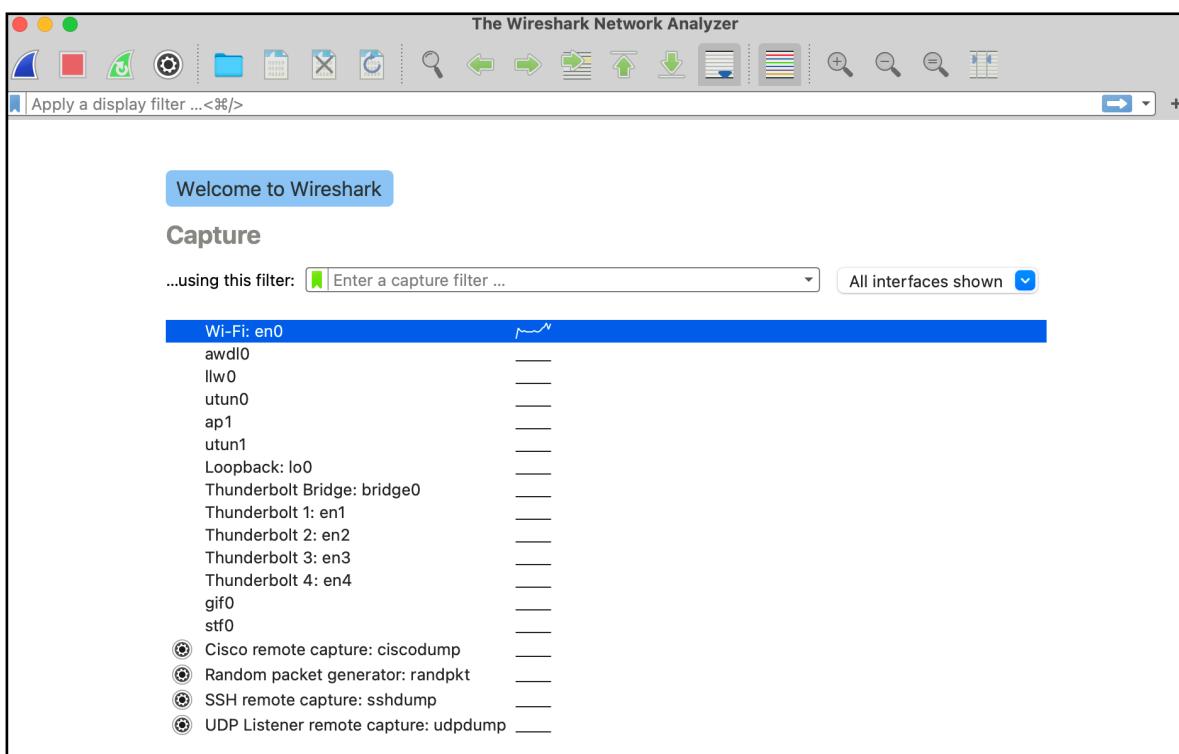
## **Task 2:**

### **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

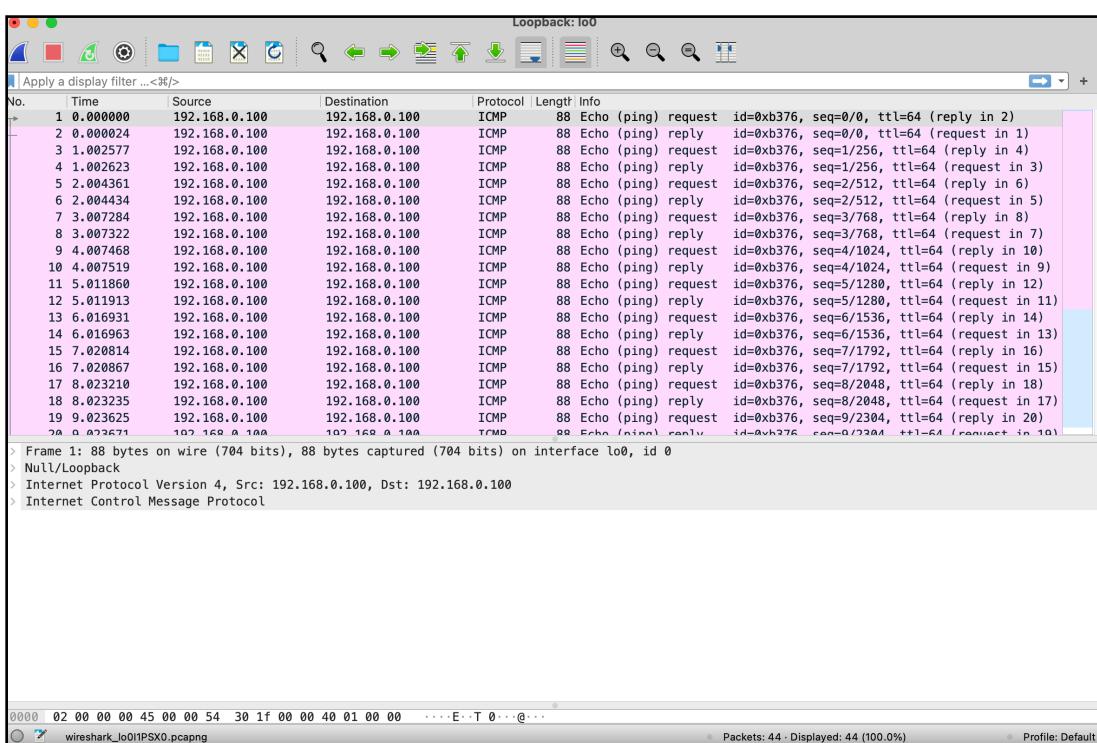


## Step 3: Pinging

```
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:

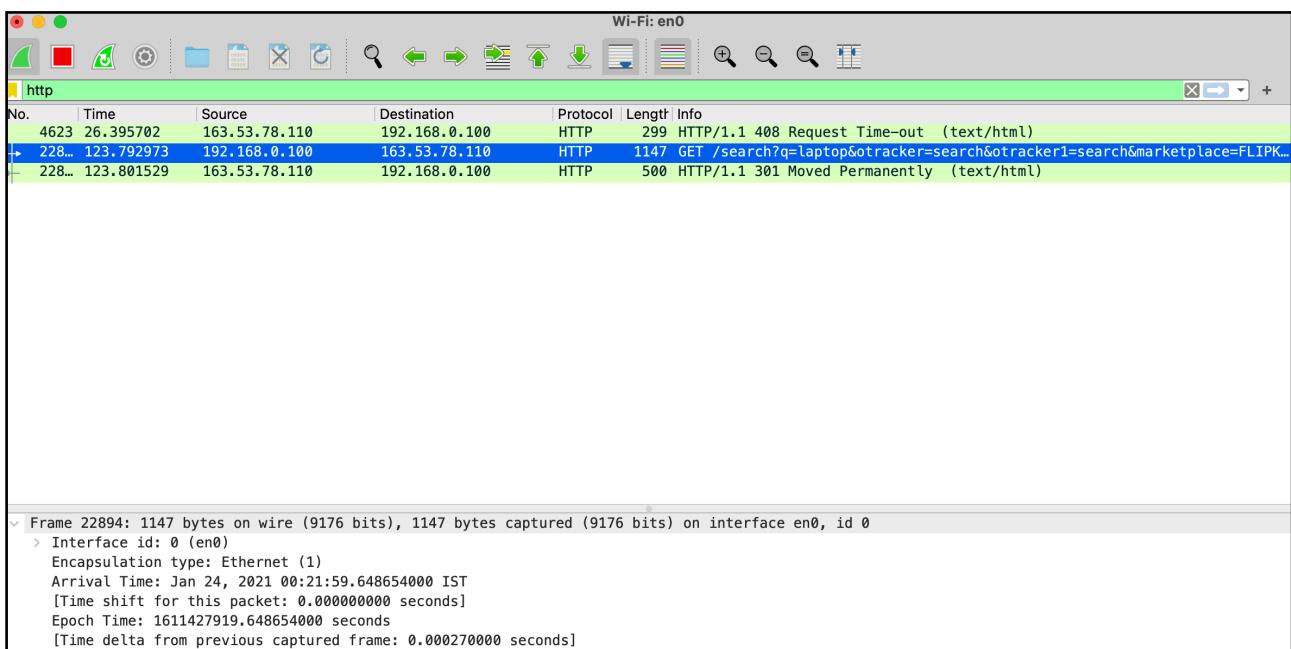
| Details                             | First Echo Request | First Echo Reply  |
|-------------------------------------|--------------------|-------------------|
| <b>Frame Number</b>                 | 1                  | 2                 |
| <b>Source IP address</b>            | 192.168.0.100      | 192.168.0.100     |
| <b>Destination IP address</b>       | 192.168.0.100      | 192.168.0.100     |
| <b>ICMP Type Value</b>              | 8                  | 0                 |
| <b>ICMP Code Value</b>              | 0                  | 0                 |
| <b>Source Ethernet Address</b>      | 38:f9:d3:c0:fb:14  | 38:f9:d3:c0:fb:14 |
| <b>Destination Ethernet Address</b> | 38:f9:d3:c0:fb:14  | 38:f9:d3:c0:fb:14 |
| <b>Internet Protocol Version</b>    | ICMP               | ICMP              |
| <b>Time To Live (TTL) Value</b>     | 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](http://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_0: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
> 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)
> 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.L0; 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]
[Request in frame: 22894]
[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_0:fb:14 (38:f9:d3:c0:fb:14)
> Internet Protocol Version 4, Src: 163.53.78.110, Dst: 192.168.0.100
> 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)
> 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  |
|-------------------------------------|--------------------|-------------------|
| <b>Frame Number</b>                 | 22894              | 22895             |
| <b>Source Port</b>                  | 55228              | 80                |
| <b>Destination Port</b>             | 80                 | 55228             |
| <b>Source IP address</b>            | 192.168.0.100      | 163.53.78.110     |
| <b>Destination IP address</b>       | 163.53.78.110      | 192.168.0.100     |
| <b>Source Ethernet Address</b>      | 38:f9:d3:c0:fb:14  | d8:07:b6:ec:75:00 |
| <b>Destination Ethernet Address</b> | 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.

| <u>HTTP Request</u>    |   | <u>HTTP Response</u>  |                                   |
|------------------------|---|-----------------------|-----------------------------------|
| <b>Get</b>             | /HTTP/1.1\r\n   | <b>Server</b>         | nginx\r\n                         |
| <b>Host</b>            | <u>www.flipkart.com</u>   | <b>Content-Type</b>   | text/html\r\n                     |
| <b>User-Agent</b>      | 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 | <b>Date</b>           | Sat, 23 Jan 2021 18:51:59 GMT\r\n |
| <b>Accept-Language</b> | en-IN,en-GB;q=0.9,en-US;q=0.8,en;q=0.7\r\n  | <b>Location</b>       | http://www.flipkart.com/          |
| <b>Accept-Encoding</b> | gzip, deflate\r\n   | <b>Content-Length</b> | 178\r\n                           |
| <b>Connection</b>      | keep-alive  | <b>Connection</b>     | keep-alive                        |

## Using Wireshark's Follow TCP Stream

The screenshot shows the Wireshark interface with the title "Wireshark · Follow TCP Stream (tcp.stream eq 36) · Wi-Fi: en0". The main pane displays the content of a TCP stream, specifically a GET request to www.flipkart.com. The request includes various headers such as Host, Connection, DNT, Upgrade-Insecure-Requests, User-Agent, Accept, Accept-Encoding, Accept-Language, and Cookie. The response is an HTTP/1.1 301 Moved Permanently status code, with the Location header pointing to https://www.flipkart.com. The response body contains an HTML page with a single line of text: "301 Moved Permanently". Below the main pane, there is a message: "Packet 13804.1 client pkt, 1 server pkt, 1 turn. Click to select." At the bottom, there are several buttons: "Entire conversation (1277 bytes)", "Show data as ASCII", "Stream 36", "Find", "Help", "Filter Out This Stream", "Print", "Save as...", "Back", and "Close".

```
GET / HTTP/1.1
Host: www.flipkart.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
Cookie: AMCVS_17EB401053DAF4840A490D4C%40AdobeOrg=1;
AMCV_17EB401053DAF4840A490D4C%40AdobeOrg=-227196251%7CMCIDTS%7C18651%7CMCMID%7C1516497515846914
5711376996938244596950%7CMCAMLH-1612032633%7C12%7CMCAAMB-1612032633%7C6G1ynYcLPuiQxYZrsz_pkqfL
G9yMXBpb2zX5dvJdYQJzPXImdj0y%7CMCOPTOUT-1611435033s%7CNONE%7CMCAID%7CNONE; s_cc=true;
s_sq=%5B%5BB%5D%5D; qH=312f91285e048e09;
SN=VIB27FEEBDC7D34791B382735E6B9EF22D.T0K9750813038804B1A9387C0079221695F.1611427919.L0

HTTP/1.1 301 Moved Permanently
Server: nginx
Date: Sat, 23 Jan 2021 20:30:21 GMT
Content-Type: text/html
Content-Length: 178
Location: https://www.flipkart.com/

<html>
<head><title>301 Moved Permanently</title></head>
<body bgcolor="white">
<center><h1>301 Moved Permanently</h1></center>
<hr><center>nginx</center>
</body>
</html>

Packet 13804.1 client pkt, 1 server pkt, 1 turn. Click to select.
```

Entire conversation (1277 bytes) Show data as ASCII Stream 36 Find

Help Filter Out This Stream Print Save as... Back Close

# Task 4:

# Capturing packets with tcpdump

**Step 1:** On running tcpdump -D in shell:

```
sh-3.2# tcpdump -D
1.en0 [Up, Running]
2.awdl0 [Up, Running]
3.llw0 [Up, Running]
4.utun0 [Up, Running]
5.ap1 [Up, Running]
6.utun1 [Up, Running]
7.lo0 [Up, Running, Loopback]
8.bridge0 [Up, Running]
9.en1 [Up, Running]
10.en2 [Up, Running]
11.en3 [Up, Running]
12.en4 [Up, Running]
13.gif0 [none]
14.stf0 [none]
```

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

```
sh-3.2# tcpdump -i en0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on en0, link-type EN10MBASET (Ethernet), max link size: 65536 bytes
[...]
02:32:54.440198 IP 192.168.0.100.50008 > 52.114.54.123.twpco: UDP, length 88
02:32:54.445578 IP 52.114.54.123.twpco > 192.168.0.100.50008: UDP, length 128
02:32:54.453601 IP 52.114.54.123.twpco > 192.168.0.100.50008: UDP, length 104
02:32:54.464463 IP 192.168.0.100.50008 > 52.114.54.123.twpco: UDP, length 88
02:32:54.466529 IP 52.114.54.123.twpco > 192.168.0.100.50008: UDP, length 133
02:32:54.484884 IP 192.168.0.100.50008 > 52.114.54.123.twpco: UDP, length 82
02:32:54.486104 IP 52.114.54.123.twpco > 192.168.0.100.50008: UDP, length 123
02:32:54.486104 IP 192.168.0.100.50008 > 52.114.54.123.twpco: UDP, length 72
02:32:54.494308 IP broadcast.acctcp.in.domain > 192.168.0.100.51521: 11898 NXDomain 0/1/0 (138)
02:32:54.497566 IP 52.114.54.123.twpco > 192.168.0.100.50008: UDP, length 118
02:32:54.504672 IP 192.168.0.100.50008 > 52.114.54.123.twpco: UDP, length 89
02:32:54.518489 IP 52.114.54.123.twpco > 192.168.0.100.50008: UDP, length 114
02:32:54.520838 IP 192.168.0.100.54188 broadcast.acctcp.in.domain 58627? A gateway.fe.apple-dns.net. (42)
02:32:54.520939 IP 192.168.0.100.56253 > 17.248.162.101.https: Flags [S], seq 347132173, win 65535, options [mss 1440,nop,wscale 6,nop,nop,TS val 1091369749 ecr 0,sackOK,eol], length 0
02:32:54.521072 IP 192.168.0.100.56252 > broadcast.acctcp.in.domain 63628? PTR? 191.162.248.17.in-addr.arpa. (45)
02:32:54.521072 IP broadcast.acctcp.in.domain > 192.168.0.100.54186: 65627 8/8 A 17.248.162.100, A 17.248.162.168, A 17.248.162.132, A 17.248.162.100, A 17.248.162.164, A 17.248.162.133
02:32:54.523243 IP broadcast.acctcp.in.domain > 192.168.0.100.59572: 63628 NXDomain 0/1/0 (109)
02:32:54.523735 IP 192.168.0.100.50044 > 27.7.86.196.50042: UDP, length 1125
02:32:54.523776 IP 192.168.0.100.50044 > 27.7.86.196.50042: UDP, length 1125
02:32:54.523777 IP 192.168.0.100.50044 > 27.7.86.196.50042: UDP, length 1125
02:32:54.523777 IP 192.168.0.100.50044 > 27.7.86.196.50042: UDP, length 1125
02:32:54.523778 IP 192.168.0.100.50044 > 27.7.86.196.50042: UDP, length 1123
02:32:54.524004 IP 192.168.0.100.50008 > 52.114.54.123.twpco: UDP, length 90
02:32:54.525108 IP 192.168.0.100.50008 > 52.114.54.123.twpco: UDP, length 128
02:32:54.534549 IP 52.114.54.123.twpco > 192.168.0.100.50008: UDP, length 117
02:32:54.552453 IP 17.248.162.101.https: 192.168.0.100.56253: Flags [S], seq 1866772714, ack 347132173, win 43440, options [mss 1440,sackOK,TS val 1832738064 ecr 1091369749,nop,wscale 7], length 0
02:32:54.552622 IP 192.168.0.100.56253 > 17.248.162.101.https: Flags [S], ack 1, win 2802, options [nop,nop,TS val 1091369780 ecr 1832738064], length 0
02:32:54.553738 IP 192.168.0.100.56253 > 17.248.162.101.https: Flags [P..], seq 1:518, ack 1, win 2802, options [nop,nop,TS val 1091369781 ecr 1832738064], length 517
02:32:54.557858 IP 52.114.54.154.cleanneriver > 192.168.0.100.50054: UDP, length 80
02:32:54.559145 IP 192.168.0.100.56257 broadcast.acctcp.in.domain 17799? PTR? 154.54.114.52.in-addr.arpa. (44)
02:32:54.563004 IP 192.168.0.100.50008 > 52.114.54.123.twpco: UDP, length 94
02:32:54.563661 IP 50.149.162.122.twpco > 192.168.0.100.50008: UDP, length 117
02:32:54.581417 IP 192.168.0.100.50008 > 52.114.54.123.twpco: UDP, length 223
02:32:54.584541 IP 52.114.54.123.twpco > 192.168.0.100.50008: UDP, length 124
02:32:54.585158 IP 17.248.162.101.https: 192.168.0.100.56253: Flags [S], ack 518, win 336, options [nop,nop,TS val 1832738097 ecr 1091369781], length 0
02:32:54.585845 IP 17.248.162.101.https: 192.168.0.100.56253: Flags [S], seq 11429, ack 518, win 336, options [nop,nop,TS val 1832738098 ecr 1091369781], length 1428
02:32:54.585914 IP 192.168.0.100.56253 > 17.248.162.101.https: Flags [S..], seq 1429, win 2030, options [nop,nop,TS val 1091369811 ecr 1832738098], length 0
02:32:54.585989 IP 17.248.162.101.https: 192.168.0.100.56253: Flags [S..], seq 1429/2857, ack 518, win 336, options [nop,nop,TS val 1832738098 ecr 1091369781], length 1428
02:32:54.586012 IP 192.168.0.100.56253 > 17.248.162.101.https: Flags [S..], ack 2857, win 2025, options [nop,nop,TS val 1091369811 ecr 1832738098], length 0
02:32:54.586012 IP 192.168.0.100.56253 > 17.248.162.101.https: Flags [S..], seq 1429/2857, ack 518, win 336, options [nop,nop,TS val 1832738098 ecr 1091369781], length 1428
02:32:54.587948 IP 192.168.0.100.56253 > 17.248.162.101.https: Flags [S..], ack 4285, win 2025, options [nop,nop,TS val 1091349813 ecr 1832738108], length 0
02:32:54.588216 IP 17.248.162.101.https: 192.168.0.100.56253: Flags [S..], seq 4285/5733, ack 518, win 336, options [nop,nop,TS val 1832738108 ecr 1091369781], length 1428
02:32:54.588244 IP 192.168.0.100.56253 > 17.248.162.101.https: Flags [S..], seq 4285/5733, ack 518, win 336, options [nop,nop,TS val 1091349813 ecr 1832738108], length 0
02:32:54.590993 IP 17.248.162.101.https: 192.168.0.100.56253: Flags [P..], seq 51713/6241, ack 518, win 336, options [nop,nop,TS val 1832738102 ecr 1091369781], length 528
02:32:54.591612 IP 192.168.0.100.56253 > 17.248.162.101.https: Flags [P..], seq 51713/6241, ack 2039, options [nop,nop,TS val 1091369815 ecr 1832738102], length 0
02:32:54.591612 IP 192.168.0.100.56253 > 17.248.162.101.https: Flags [P..], seq 518/582, ack 6241, win 2048, options [nop,nop,TS val 1091369820 ecr 1832738102], length 64
02:32:54.608842 IP 192.168.0.100.56253 > 17.248.162.101.https: Flags [P..], seq 518/582, ack 6241, win 2048, options [nop,nop,TS val 1091369824 ecr 1832738102], length 46
02:32:54.619478 IP 192.168.0.100.56253 > 17.248.162.101.https: Flags [P..], seq 623/582, ack 6241, win 2048, options [nop,nop,TS val 1091369824 ecr 1832738102], length 43
02:32:54.620045 IP 192.168.0.100.56253 > 17.248.162.101.https: Flags [P..], seq 623/582, ack 6241, win 2048, options [nop,nop,TS val 1091369824 ecr 1832738102], length 35
02:32:54.639984 IP 192.168.0.100.56253 > 17.248.162.101.https: Flags [P..], seq 768/1787, ack 6241, win 2048, options [nop,nop,TS val 1091369824 ecr 1832738102], length 1172
02:32:54.641082 IP 192.168.0.100.56253 > 17.248.162.101.https: Flags [P..], seq 1878/2939, ack 6241, win 2048, options [nop,nop,TS val 1091369824 ecr 1832738102], length 1055
02:32:54.641228 IP 192.168.0.100.56253 > 17.248.162.101.https: Flags [P..], seq 2933/3947, ack 6241, win 2048, options [nop,nop,TS val 1091369824 ecr 1832738102], length 1014
02:32:54.651287 IP 192.168.0.100.56253 > 17.248.162.101.https: Flags [P..], seq 3947/3978, ack 6241, win 2048, options [nop,nop,TS val 1091369824 ecr 1832738102], length 31
02:32:54.687673 IP 52.114.54.123.twpco > 192.168.0.100.50008: UDP, length 120
```

## 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
```

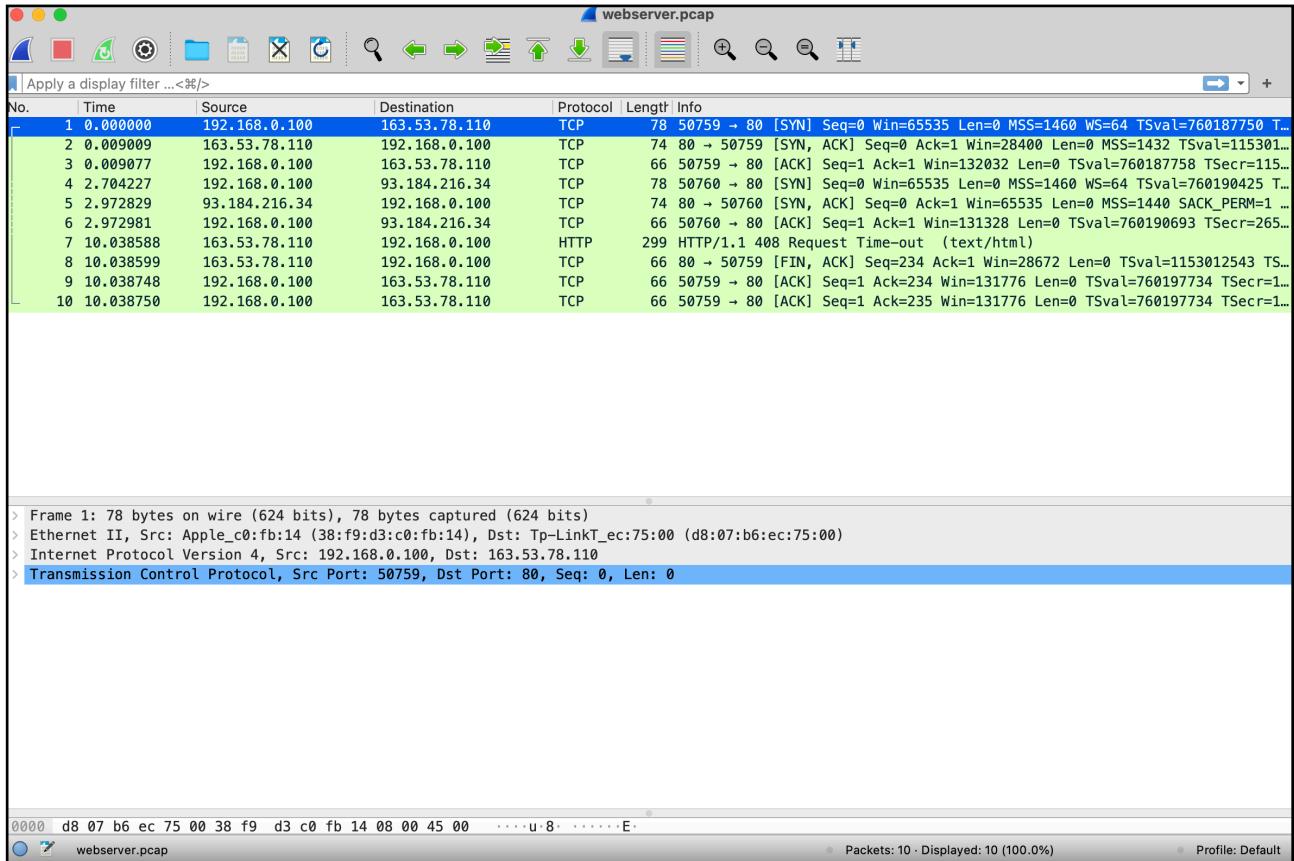
### **Step 5:** Check the packet content. For example, inspect the HTTP content of a web request

```
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
16:15:03.379717 IP 192.168.0.100.50298 > 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..@.0.C....d].".r.PV.!. .....
16:15:03.379777 IP 93.184.216.34.80 > 192.168.0.100.50298: Flags [S.], seq 3555293196, ack 1456324386, win 65535, options [mss 1440,sackOK,TS val 2375542693 ecr 756846939,nop,wscale 9], length 0
E..<S..3.:b!..".d.P.r..x.V.".....
.....[...
16:15:03.378127 IP 192.168.0.100.50298 > 93.184.216.34.80: Flags [.], ack 1, win 2052, options [nop,nop,TS val 756847153 ecr 2375542693], length 0
E..4..@.0.C....d].".r.PV.."x.....".
16:15:03.378648 IP 192.168.0.100.50298 > 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..
..@.0.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-US;q=0.9,en;q=0.8,en;q=0.7
16:15:03.598430 IP 93.184.216.34.80 > 192.168.0.100.50298: Flags [.], ack 471, win 131, options [nop,nop,TS val 2375542914 ecr 756847153], length 0
E..4Va..3.:`]..".d.P.r..x.V."....!
.....1
16:15:03.599027 IP 93.184.216.34.80 > 192.168.0.100.50298: 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.".....
.....HTTP/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 (dcbb/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



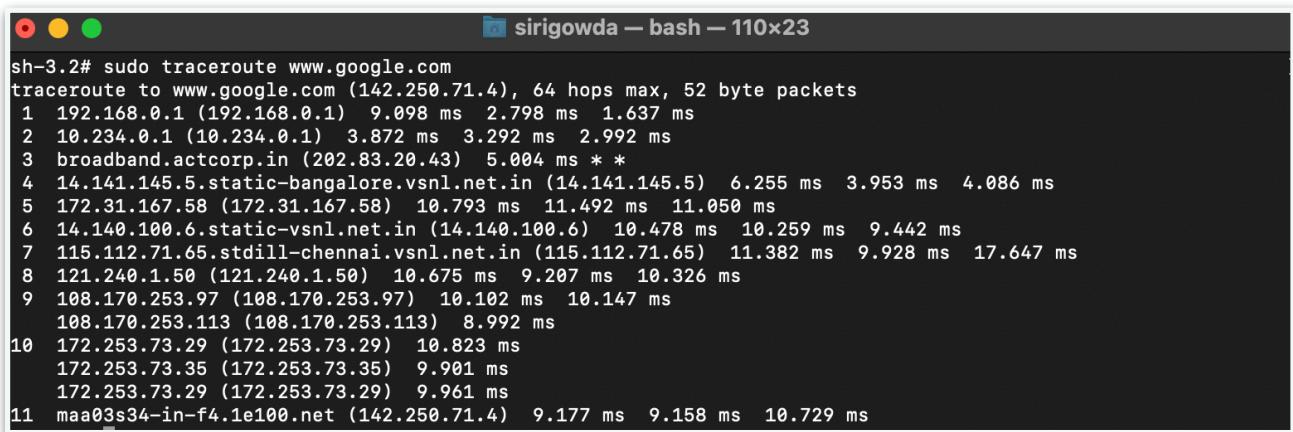
- Command in the terminal:

```
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](http://www.google.com)



```
sirigowda — bash — 110x23
sh-3.2# sudo traceroute www.google.com
traceroute to www.google.com (142.250.71.4), 64 hops max, 52 byte packets
 1  192.168.0.1 (192.168.0.1)  9.098 ms  2.798 ms  1.637 ms
 2  10.234.0.1 (10.234.0.1)  3.872 ms  3.292 ms  2.992 ms
 3  broadband.actcorp.in (202.83.20.43)  5.004 ms * *
 4  14.141.145.5.static-bangalore.vsnl.net.in (14.141.145.5)  6.255 ms  3.953 ms  4.086 ms
 5  172.31.167.58 (172.31.167.58)  10.793 ms  11.492 ms  11.050 ms
 6  14.140.100.6.static-vsnl.net.in (14.140.100.6)  10.478 ms  10.259 ms  9.442 ms
 7  115.112.71.65.stdill-chennai.vsnl.net.in (115.112.71.65)  11.382 ms  9.928 ms  17.647 ms
 8  121.240.1.50 (121.240.1.50)  10.675 ms  9.207 ms  10.326 ms
 9  108.170.253.97 (108.170.253.97)  10.102 ms  10.147 ms
   108.170.253.113 (108.170.253.113)  8.992 ms
10  172.253.73.29 (172.253.73.29)  10.823 ms
   172.253.73.35 (172.253.73.35)  9.901 ms
   172.253.73.29 (172.253.73.29)  9.961 ms
11  maa03s34-in-f4.1e100.net (142.250.71.4)  9.177 ms  9.158 ms  10.729 ms
```

### 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

```
sh-3.2# sudo traceroute -n www.google.com
traceroute to www.google.com (142.250.71.4), 64 hops max, 52 byte packets
 1  192.168.0.1  1.941 ms  1.477 ms  1.435 ms
 2  10.234.0.1  2.352 ms  2.380 ms  2.421 ms
 3  202.83.20.43  2.633 ms * 10.029 ms
 4  14.141.145.5  24.885 ms  4.599 ms  3.820 ms
 5  172.31.167.58  11.368 ms  9.770 ms  9.768 ms
 6  14.140.100.6  9.221 ms  9.355 ms  9.841 ms
 7  115.112.71.65  11.227 ms  10.972 ms  9.984 ms
 8  121.240.1.50  13.702 ms  10.749 ms  10.726 ms
 9  108.170.253.113  10.090 ms
   108.170.253.97  11.833 ms  10.329 ms
10  172.253.73.35  10.385 ms
   172.253.73.29  9.319 ms  10.976 ms
11  142.250.71.4  10.268 ms  9.560 ms  9.480 ms
```

**Step 4:** For traceroute to use ICMP.

```
sh-3.2# sudo traceroute -I www.google.com
traceroute to www.google.com (142.250.71.36), 64 hops max, 72 byte packets
 1  192.168.0.1 (192.168.0.1)  2.718 ms  1.656 ms  1.608 ms
 2  10.234.0.1 (10.234.0.1)  4.761 ms  2.651 ms  3.405 ms
 3  * * broadband.actcorp.in (202.83.20.43)  9.981 ms
 4  14.141.145.5.static-bangalore.vsnl.net.in (14.141.145.5)  3.023 ms  3.253 ms  3.283 ms
 5  172.31.167.58 (172.31.167.58)  8.965 ms  9.150 ms  9.359 ms
 6  14.140.100.6.static-vsnl.net.in (14.140.100.6)  8.789 ms  8.913 ms  8.590 ms
 7  115.112.71.65.stdill-chennai.vsnl.net.in (115.112.71.65)  8.669 ms  8.878 ms  8.792 ms
 8  121.240.1.50 (121.240.1.50)  8.620 ms  9.586 ms  9.057 ms
 9  108.170.253.113 (108.170.253.113)  8.364 ms  8.285 ms  8.182 ms
10  142.250.233.143 (142.250.233.143)  9.503 ms  9.298 ms  9.264 ms
11  maa03s35-in-f4.1e100.net (142.250.71.36)  8.597 ms  8.291 ms  8.732 ms
```

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

```
sh-3.2# sudo traceroute -T www.google.com
Version 1.4a12+Darwin
Usage: traceroute [-adDefInrSvx] [-A as_server] [-f first_ttl] [-g gateway] [-i iface]
                  [-M first_ttl] [-m max_ttl] [-p port] [-P proto] [-q nqueries] [-s src_addr]
                  [-t tos] [-w waittime] [-z pausesecs] host [packetlen]
```

# 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.

```
● ● ● sirigowda — -zsh — 80x24
sirigowda@Siris-MacBook-Pro ~ % nmap 163.53.78.128
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-25 04:01 IST
Nmap scan report for 163.53.78.128
Host is up (0.010s 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 42.30 seconds
```

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

```
● ● ● sirigowda — bash — 80x24
sh-3.2# nmap 192.168.1.1 192.168.1.2 192.168.1.3
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-25 04:06 IST
Nmap done: 3 IP addresses (0 hosts up) scanned in 5.12 seconds
```

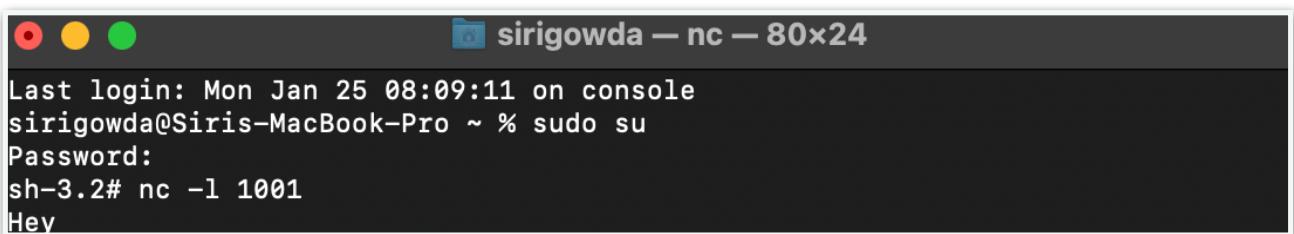
# Task 7a

## 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

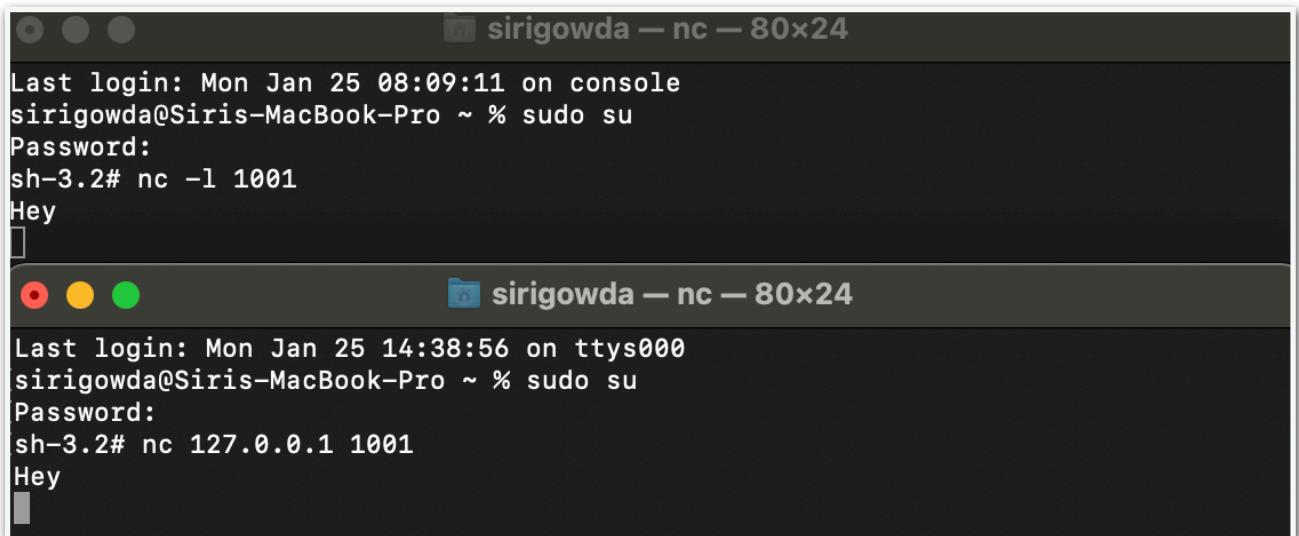
**Step 2:** Setting up a server (It will go to listening mood)



A screenshot of a Mac OS X terminal window titled "sirigowda — nc — 80x24". The window shows the following text:  
Last login: Mon Jan 25 08:09:11 on console  
sirigowda@Siris-MacBook-Pro ~ % sudo su  
Password:  
sh-3.2# nc -l 1001  
Hey

**Step 3:** Opening another terminal that acts as a client

### Server and Client



Two screenshots of Mac OS X terminal windows. The top window is titled "sirigowda — nc — 80x24" and shows the server setup:  
Last login: Mon Jan 25 08:09:11 on console  
sirigowda@Siris-MacBook-Pro ~ % sudo su  
Password:  
sh-3.2# nc -l 1001  
Hey

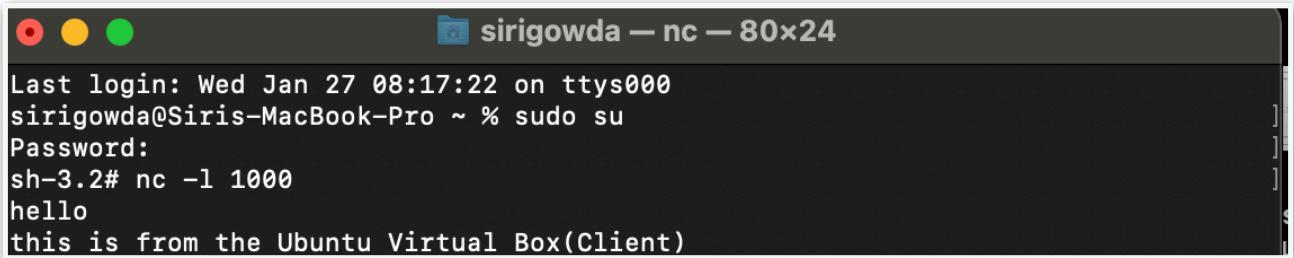
The bottom window is also titled "sirigowda — nc — 80x24" and shows the client connection:  
Last login: Mon Jan 25 14:38:56 on ttys000  
sirigowda@Siris-MacBook-Pro ~ % sudo su  
Password:  
sh-3.2# nc 127.0.0.1 1001  
Hey

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:

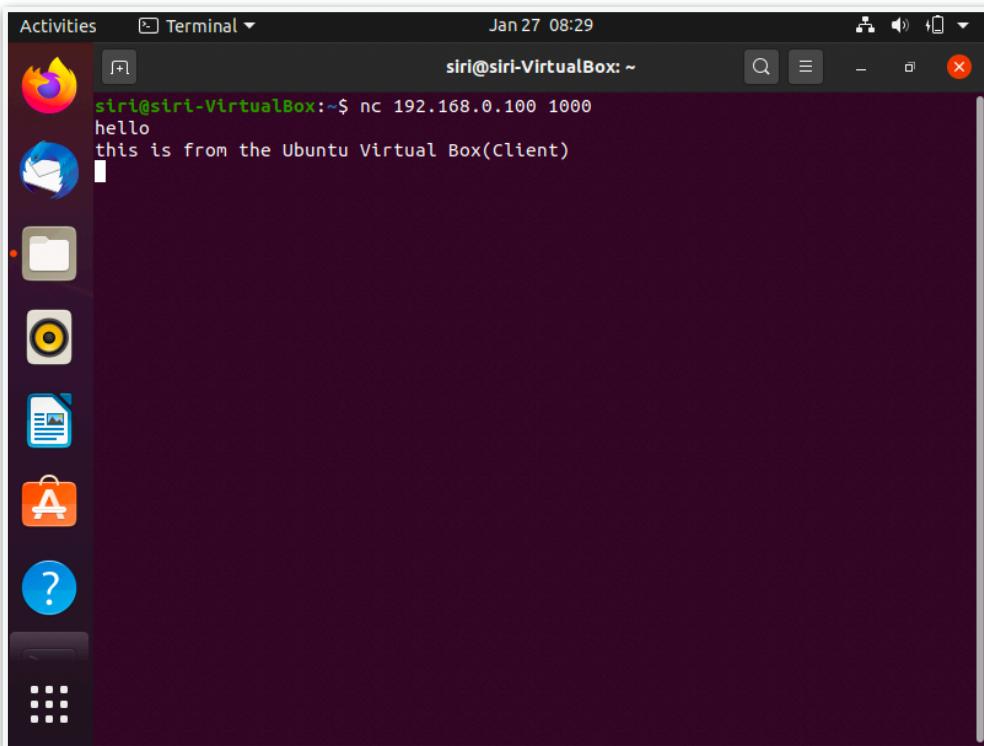


A screenshot of a macOS Terminal window titled "sirigowda — nc — 80x24". The window shows the following text:  
Last login: Wed Jan 27 08:17:22 on ttys000  
sirigowda@Siris-MacBook-Pro ~ % sudo su  
Password:  
sh-3.2# nc -l 1000  
hello  
this is from the Ubuntu Virtual Box(Client)

Setting up a client on Ubuntu and sending 2 Messages:

-hello

-This is from the Ubuntu Virtual Box(client)



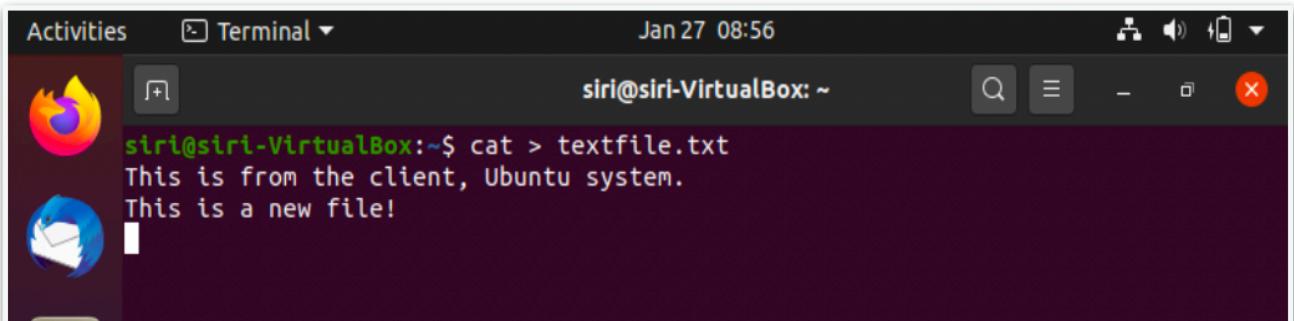
A screenshot of an Ubuntu terminal window titled "Terminal". The window shows the following text:  
Activities Terminal ▾ Jan 27 08:29 siri@siri-VirtualBox: ~  
siri@siri-VirtualBox:~\$ nc 192.168.0.100 1000  
hello  
this is from the Ubuntu Virtual Box(Client)

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

# Task 7b :

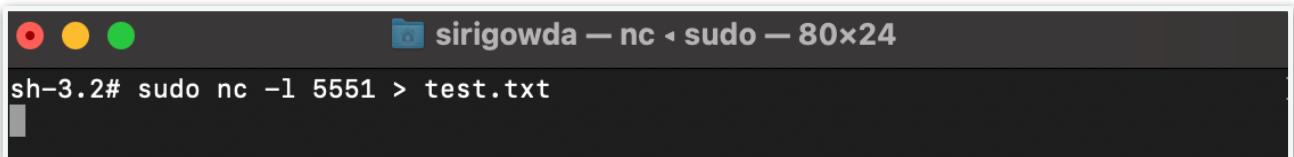
## Use Netcat to Transfer Files

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



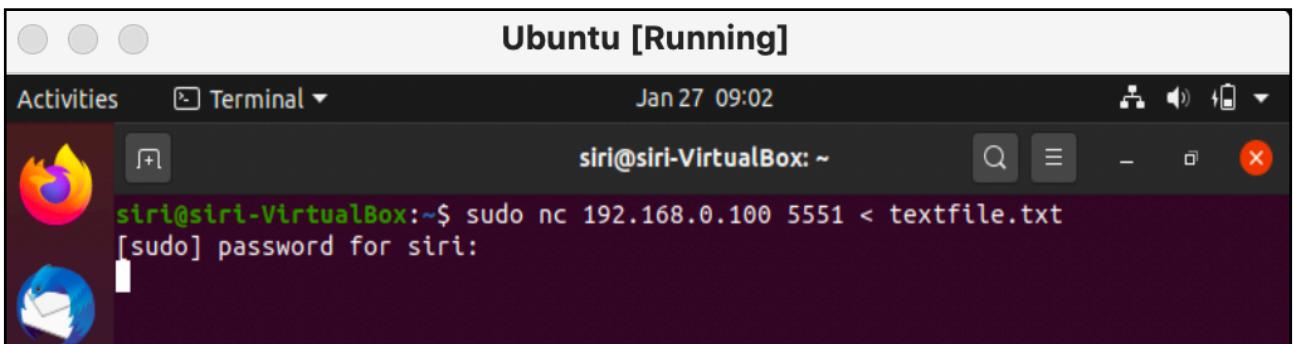
```
siri@siri-VirtualBox:~$ cat > textile.txt
This is from the client, Ubuntu system.
This is a new file!
```

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



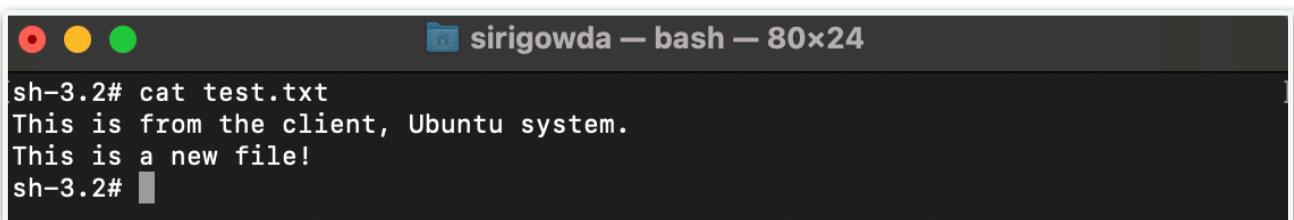
```
sh-3.2# sudo nc -l 5551 > test.txt
```

Running : “sudo nc 192.168.56.1 5551 < textile.txt” on Client.



```
siri@siri-VirtualBox:~$ sudo nc 192.168.0.100 5551 < textile.txt
[sudo] password for siri:
```

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

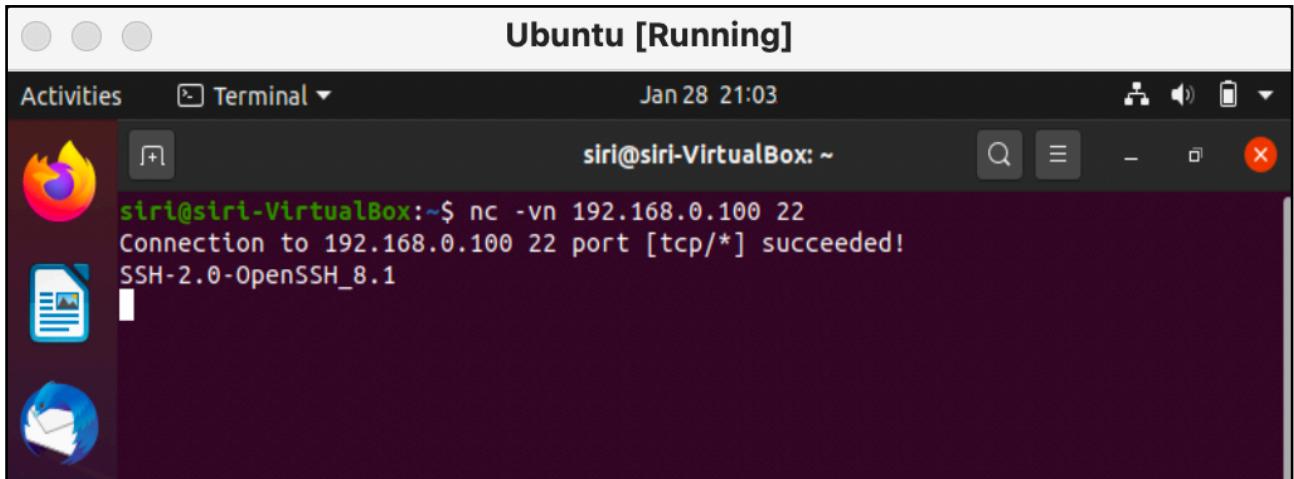


```
sh-3.2# cat test.txt
This is from the client, Ubuntu system.
This is a new file!
sh-3.2#
```

# Task 7c :

## Other Commands

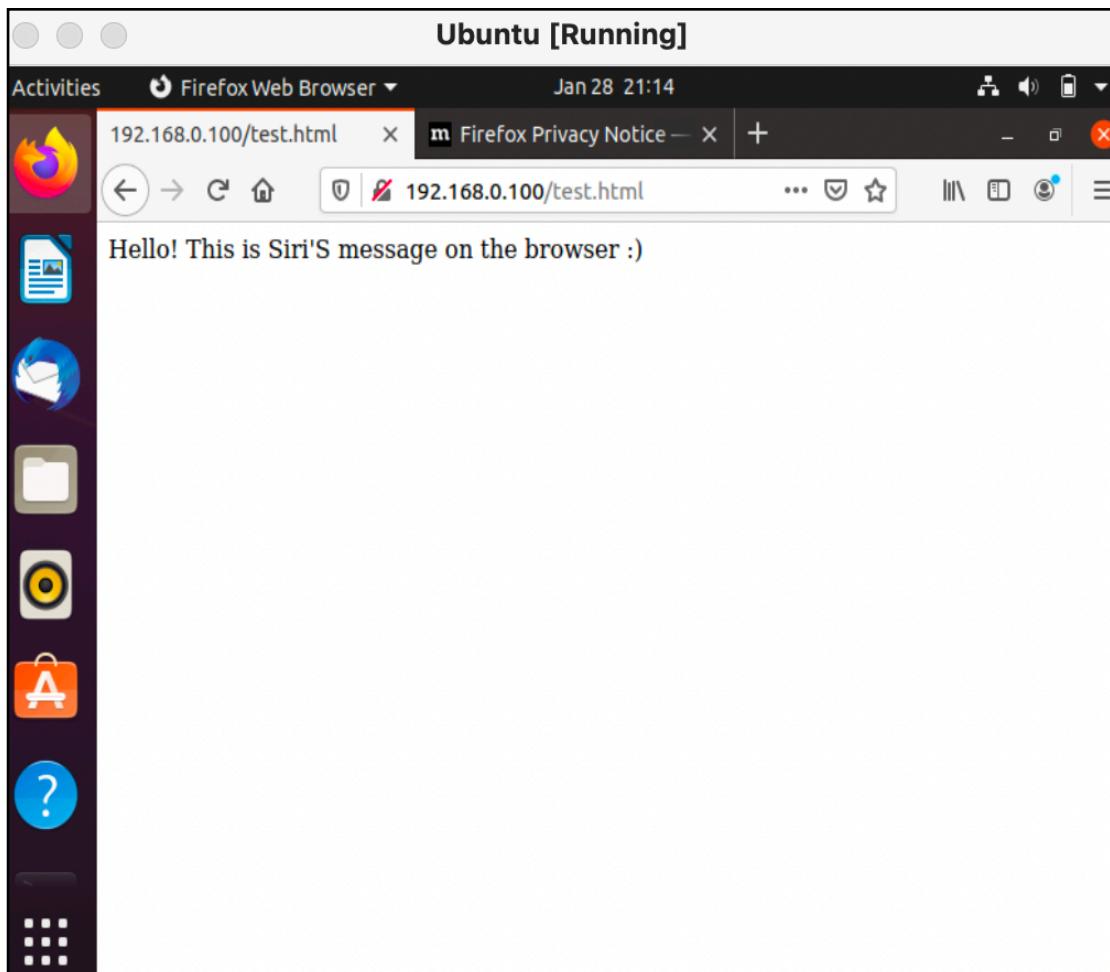
**Step 1:** Testing if a particular TCP port of a remote host is open.



A screenshot of a terminal window titled "Ubuntu [Running]". The window shows the command "nc -vn 192.168.0.100 22" being run, followed by the output: "Connection to 192.168.0.100 22 port [tcp/\*] succeeded! SSH-2.0-OpenSSH\_8.1". The terminal interface includes a dock on the left with icons for Dash, Home, Activities, and a terminal icon.

```
siri@siri-VirtualBox:~$ nc -vn 192.168.0.100 22
Connection to 192.168.0.100 22 port [tcp/*] succeeded!
SSH-2.0-OpenSSH_8.1
```

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



## Step 3: Observing the details on the terminal

```
sirigowda — nc -s sudo — 98x32
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

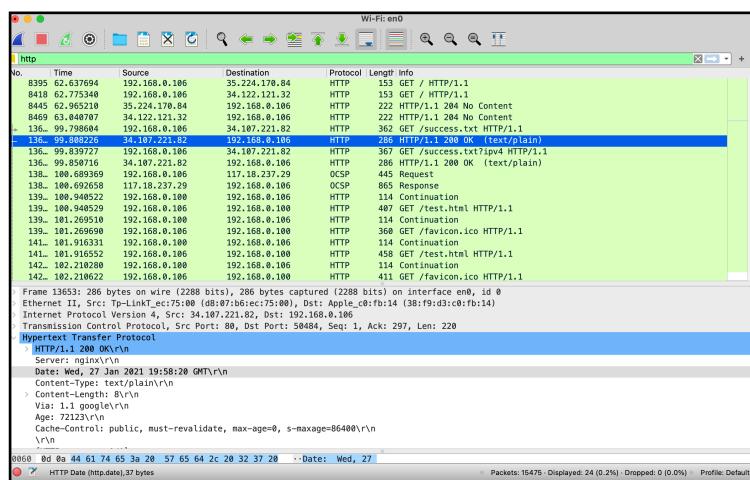
GET /favicon.ico HTTP/1.1
Host: 192.168.0.100
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:84.0) Gecko/20100101 Firefox/84.0
Accept: image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://192.168.0.100/test.html
```

## 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

```
sh-3.2# nmap -O -v localhost
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-28 21:54 IST
Initiating SYN Stealth Scan at 21:54
Scanning localhost (127.0.0.1) [1000 ports]
Discovered open port 22/tcp on 127.0.0.1
Discovered open port 5900/tcp on 127.0.0.1
Discovered open port 3283/tcp on 127.0.0.1
Discovered open port 88/tcp on 127.0.0.1
Completed SYN Stealth Scan at 21:54, 0.01s elapsed (1000 total ports)
Initiating OS detection (try #1) against localhost (127.0.0.1)
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00013s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 996 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
38/tcp    open  kerberos-sec
3283/tcp  open  netassistant
5900/tcp  open  vnc
Device type: general purpose
Running: Apple macOS 10.14.X
OS CPE: cpe:/o:apple:mac_os_x:10.14
OS details: Apple macOS 10.14 (Mojave) (Darwin 18.2.0 - 18.6.0)
Uptime guess: 5.566 days (since Sat Jan 23 08:19:06 2021)
Network Distance: 0 hops
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: All zeros

Read data files from: /usr/local/bin/../share/nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.88 seconds
    Raw packets sent: 1022 (45.778KB) | Rcvd: 2046 (86.876KB)
```

---