

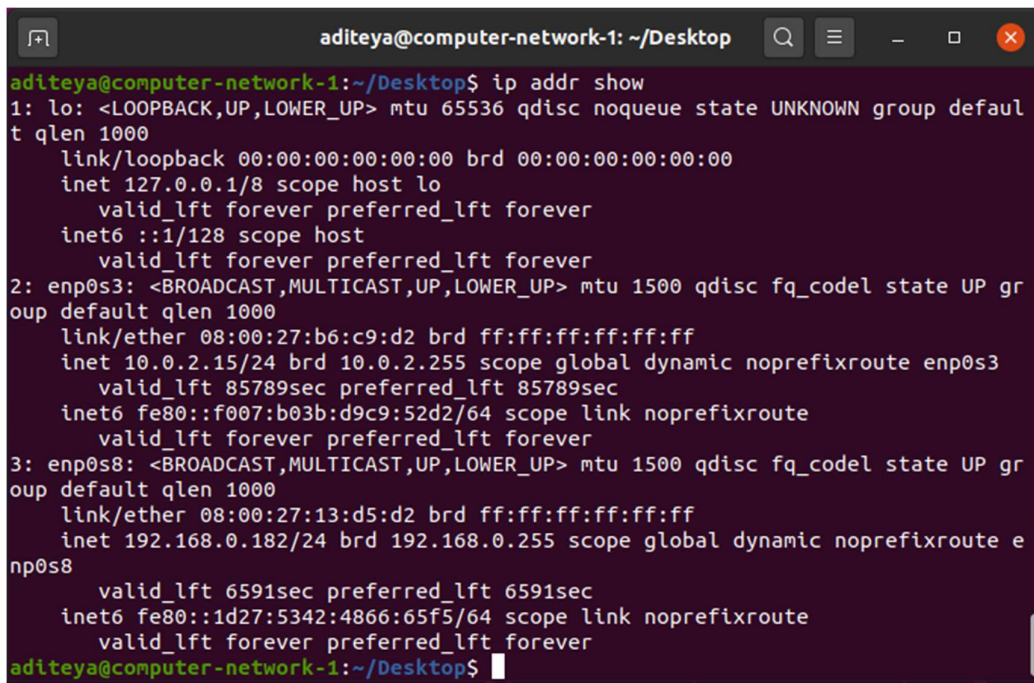
# Computer Networks Lab - Week 1

PES1201800366

Aditeya Baral

## 1. Linux Interface Configuration

### 1.1 `ip addr show`



```
aditeya@computer-network-1: ~/Desktop
aditeya@computer-network-1:~/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:b6:c9:d2 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 85789sec preferred_lft 85789sec
    inet6 fe80::f007:b03b:d9c9:52d2/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:13:d5:d2 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.182/24 brd 192.168.0.255 scope global dynamic noprefixroute enp0s8
        valid_lft 6591sec preferred_lft 6591sec
    inet6 fe80::1d27:5342:4866:65f5/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
aditeya@computer-network-1:~/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::f007:b03b:d9c9:52d2	08:00:27:b6:c9:d2
enp0s8	192.168.0.182/fe80::1d27:5342:4866:65f5	08:00:27:13:d5:d2

### 1.2 Assigning an IP

Command used: `sudo ip addr add 10.0.4.26/24 dev enp0s3`

```
aditeya@computer-network-1: ~/Desktop
aditeya@computer-network-1:~/Desktop$ sudo ip addr add 10.0.4.26/24 dev enp0s3
aditeya@computer-network-1:~/Desktop$ ip addr
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:b6:c9:d2 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 85298sec preferred_lft 85298sec
    inet 10.0.4.26/24 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::f007:b03b:d9c9:52d2/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:13:d5:d2 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.182/24 brd 192.168.0.255 scope global dynamic noprefixroute enp0s8
        valid_lft 6100sec preferred_lft 6100sec
```

inet 10.0.4.26/24 scope global enp0s3

## 1.3 Activating and Deactivating Network Interfaces

### 1.3.1 Deactivating enp0s3

Command used: `sudo ifconfig enp0s3 down`

```
aditeya@computer-network-1: ~/Desktop
aditeya@computer-network-1:~/Desktop$ sudo ifconfig enp0s3 down
aditeya@computer-network-1:~/Desktop$ ifconfig
enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.0.182 netmask 255.255.255.0 broadcast 192.168.0.255
    inet6 fe80::1d27:5342:4866:65f5 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:13:d5:d2 txqueuelen 1000 (Ethernet)
    RX packets 2142 bytes 283227 (283.2 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1632 bytes 170219 (170.2 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 1530 bytes 170571 (170.5 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1530 bytes 170571 (170.5 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Only enp0s8 and lo are displayed above

### 1.3.2 Activating enp0s3

```
aditeya@computer-network-1: ~/Desktop
aditeya@computer-network-1:~/Desktop$ sudo ifconfig enp0s3 up
aditeya@computer-network-1:~/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::f007:b03b:d9c9:52d2 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:b6:c9:d2 txqueuelen 1000 (Ethernet)
    RX packets 7551 bytes 6847290 (6.8 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 3584 bytes 508079 (508.0 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.0.182 netmask 255.255.255.0 broadcast 192.168.0.255
    inet6 fe80::1d27:5342:4866:65f5 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:13:d5:d2 txqueuelen 1000 (Ethernet)
    RX packets 2169 bytes 286012 (286.0 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1664 bytes 173944 (173.9 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 1543 bytes 172040 (172.0 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1543 bytes 172040 (172.0 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

enp0s3 has been reactivated

#### 1.4 Step 4 – ip neigh

```
aditeya@computer-network-1: ~/Desktop
aditeya@computer-network-1:~/Desktop$ ip neigh
192.168.0.1 dev enp0s8 lladdr 1c:3b:f3:b3:e2:54 REACHABLE
10.0.2.2 dev enp0s3 lladdr 52:54:00:12:35:02 REACHABLE
aditeya@computer-network-1:~/Desktop$
```

## 2. Ping PDU (Packet Data Units) Capture

```
aditeya@computer-network-1: ~/Desktop
aditeya@computer-network-1: ~/Desktop$ ping 10.0.4.26
64 bytes from 10.0.4.26: icmp_seq=55 ttl=64 time=0.107 ms
64 bytes from 10.0.4.26: icmp_seq=56 ttl=64 time=0.050 ms
64 bytes from 10.0.4.26: icmp_seq=57 ttl=64 time=0.050 ms
64 bytes from 10.0.4.26: icmp_seq=58 ttl=64 time=0.036 ms
64 bytes from 10.0.4.26: icmp_seq=59 ttl=64 time=0.051 ms
64 bytes from 10.0.4.26: icmp_seq=60 ttl=64 time=0.060 ms
64 bytes from 10.0.4.26: icmp_seq=61 ttl=64 time=0.050 ms
64 bytes from 10.0.4.26: icmp_seq=62 ttl=64 time=0.115 ms
64 bytes from 10.0.4.26: icmp_seq=63 ttl=64 time=0.037 ms
64 bytes from 10.0.4.26: icmp_seq=64 ttl=64 time=0.049 ms
64 bytes from 10.0.4.26: icmp_seq=65 ttl=64 time=0.093 ms
64 bytes from 10.0.4.26: icmp_seq=66 ttl=64 time=0.062 ms
64 bytes from 10.0.4.26: icmp_seq=67 ttl=64 time=0.049 ms
64 bytes from 10.0.4.26: icmp_seq=68 ttl=64 time=0.107 ms
```

ping 10.0.4.26

<b>TTL</b>	64
<b>Protocol used by ping</b>	ICMP
<b>Time</b>	Order of $10^{-2}$ ms

```

Wireshark · Packet 19 · any
└─▶ Frame 19: 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: 10.0.4.26, Dst: 10.0.4.26
        0100 .... = Version: 4
        .... 0101 = Header Length: 20 bytes (5)
        └─ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
            Total Length: 84
            Identification: 0xf3bf (62399)
        └─ Flags: 0x4000, Don't fragment
            Fragment offset: 0
            Time to live: 64
            Protocol: ICMP (1)
            Header checksum: 0x2ab6 [validation disabled]
            [Header checksum status: Unverified]
            Source: 10.0.4.26
            Destination: 10.0.4.26
    └─ Internet Control Message Protocol
        Type: 8 (Echo (ping) request)
        Code: 0
        Checksum: 0xb381 [correct]
        [Checksum Status: Good]
        Identifier (BE): 1 (0x0001)
        Identifier (LE): 256 (0x0100)
        Sequence number (BE): 1 (0x0001)
        Sequence number (LE): 256 (0x0100)
        [Response frame: 20]
        Timestamp from icmp data: Sep  4, 2020 23:00:57.000000000 IST
        [Timestamp from icmp data (relative): 0.512114265 seconds]
    └─ Data (48 bytes)
  
```

Request Packet

```

Wireshark · Packet 20 · any
└─▶ Frame 20: 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: 10.0.4.26, Dst: 10.0.4.26
        0100 .... = Version: 4
        .... 0101 = Header Length: 20 bytes (5)
        └─ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
            Total Length: 84
            Identification: 0xf3c0 (62400)
        └─ Flags: 0x0000
            Fragment offset: 0
            Time to live: 64
            Protocol: ICMP (1)
            Header checksum: 0x6ab5 [validation disabled]
            [Header checksum status: Unverified]
            Source: 10.0.4.26
            Destination: 10.0.4.26
    └─ Internet Control Message Protocol
        Type: 0 (Echo (ping) reply)
        Code: 0
        Checksum: 0xbb81 [correct]
        [Checksum Status: Good]
        Identifier (BE): 1 (0x0001)
        Identifier (LE): 256 (0x0100)
        Sequence number (BE): 1 (0x0001)
        Sequence number (LE): 256 (0x0100)
        [Request frame: 19]
        [Response time: 0.012 ms]
        Timestamp from icmp data: Sep  4, 2020 23:00:57.000000000 IST
        [Timestamp from icmp data (relative): 0.512125874 seconds]
    └─ Data (48 bytes)
  
```

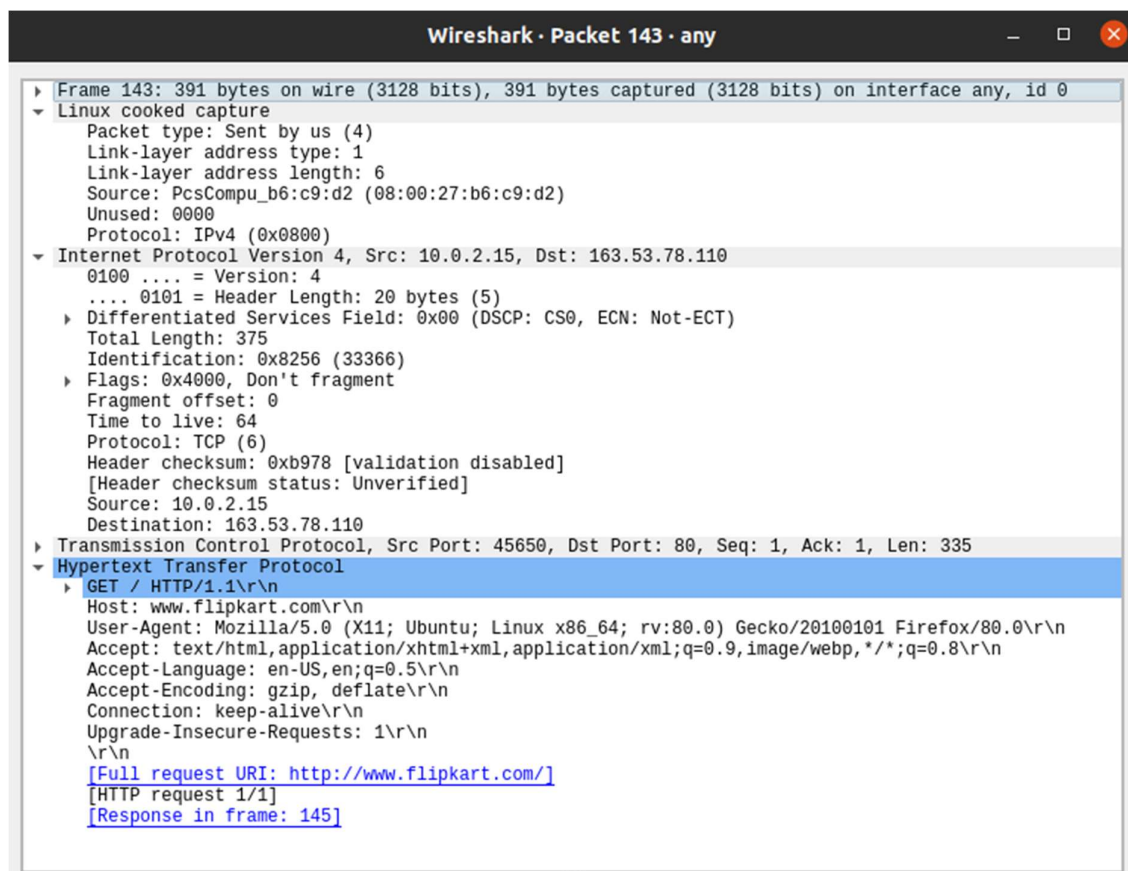
Response Packet



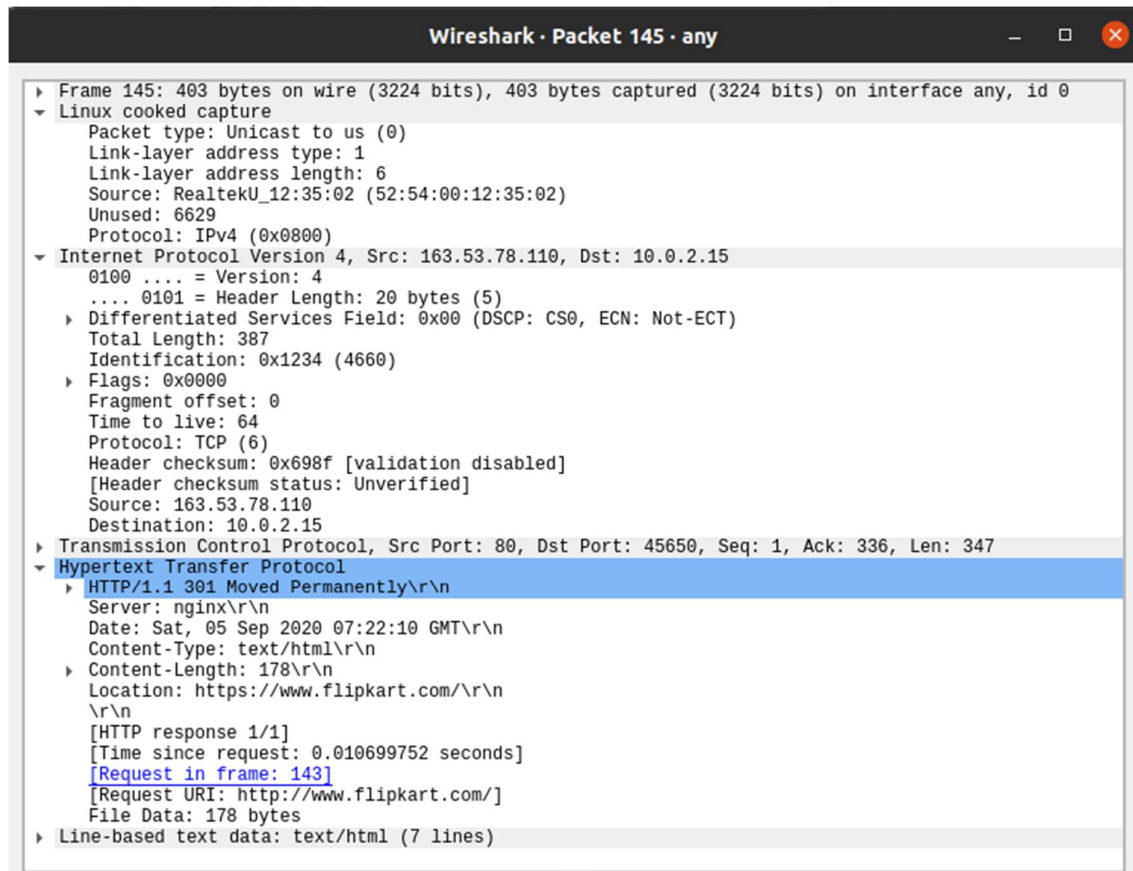
Details	First Echo Request	First Echo Reply
Frame Number	19	20
Source IP address	10.0.4.26	10.0.4.26
Destination IP address	10.0.4.26	10.0.4.26
ICMP Type Value	8	0
ICMP Code Value	0	0
Source Ethernet Address	00:00:00:00:00:00	00:00:00:00:00:00
Destination Ethernet	00:00:00:00:00:00	00:00:00:00:00:00
Internet Protocol Version	IPv4	IPv4
Time To Live (TTL)	64	64

### 3. HTTP PDU Capture

#### 3.1 Echo Request and Reply



Request Packet



Response Packet

Details	First Echo Request	First Echo Reply
Frame Number	143	145
Source Port	45650	80
Destination Port	80	45650
Source IP Address	10.0.2.15	163.53.78.110
Destination IP Address	163.53.78.110	10.0.2.15
Source Ethernet Address	08:00:27:b6:c9:d2	52:54:00:12:35:02
Destination Ethernet Address	52:54:00:12:35:02	08:00:27:b6:c9:d2

Connection Details

### 3.2 HTTP Request and Response

HTTP Request		HTTP Response	
<b>Get</b>	GET / HTTP/1.1\r\n	<b>Server</b>	nginx
<b>Host</b>	www.flipkart.com	<b>Content-Type</b>	text/html
<b>User-Agent</b>	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0) Gecko/20100101 Firefox/80.0	<b>Date</b>	Sat, 05 Sep 2020 07:22:10 GMT
<b>Accept-Language</b>	en-US,en;q=0.5	<b>Location</b>	https://www.flipkart.com/
<b>Accept-Encoding</b>	gzip, deflate	<b>Content-Length</b>	178
<b>Connection</b>	keep-alive	<b>Connection</b>	keep-alive

### 3.3 Following TCP Stream

The screenshot shows the Wireshark interface with the title bar "Wireshark · Follow TCP Stream (tcp.stream eq 12) · any". The main pane displays the raw data of the selected packet, which is an HTTP 301 response. The data is color-coded: red for the client request and blue for the server response. The response status is "HTTP/1.1 301 Moved Permanently". The body of the response is an HTML document with a title "301 Moved Permanently" and a message "301 Moved Permanently" displayed in the center.

```

GET / HTTP/1.1
Host: www.flipkart.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0) Gecko/20100101 Firefox/80.0
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/1.1 301 Moved Permanently
Server: nginx
Date: Sat, 05 Sep 2020 07:22:10 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>

```

1 client pkt, 1 server pkt, 1 turn.

## 4. Capturing Packets with `tcpdump`

### 4.1 Viewing Interfaces available for Capture

```
aditeya@computer-network-1: ~/Desktop$ sudo tcpdump -D
1.enp0s3 [Up, Running]
2.enp0s8 [Up, Running]
3.lo [Up, Running, Loopback]
4.any (Pseudo-device that captures on all interfaces) [Up, Running]
5.bluetooth-monitor (Bluetooth Linux Monitor) [none]
6.nflog (Linux netfilter log (NFLOG) interface) [none]
7.nfqueue (Linux netfilter queue (NFQUEUE) interface) [none]
aditeya@computer-network-1: ~/Desktop$
```

`tcpdump -D`

### 4.2 Capturing all Packets in any Interface

```
aditeya@computer-network-1: ~/Desktop$ tcpdump -i any
00:23:04.317212 IP computer-network-1 > computer-network-1: ICMP echo reply, id 3, seq 32, length 64
00:23:04.930592 IP computer-network-1 > 224.0.0.251: igmp v2 report 224.0.0.251
00:23:05.214929 IP computer-network-1.50802 > maa05s12-in-f3.1e100.net.http: Flags [.], ack 590592703, win 63791, length 0
00:23:05.215341 IP maa05s12-in-f3.1e100.net.http > computer-network-1.50802: Flags [.], ack 1, win 65535, length 0
00:23:05.342439 IP computer-network-1 > computer-network-1: ICMP echo request, id 3, seq 33, length 64
00:23:05.342450 IP computer-network-1 > computer-network-1: ICMP echo reply, id 3, seq 33, length 64
00:23:06.377561 IP computer-network-1 > computer-network-1: ICMP echo request, id 3, seq 34, length 64
00:23:06.377577 IP computer-network-1 > computer-network-1: ICMP echo reply, id 3, seq 34, length 64
00:23:07.397728 IP computer-network-1 > computer-network-1: ICMP echo request, id 3, seq 35, length 64
00:23:07.397743 IP computer-network-1 > computer-network-1: ICMP echo reply, id 3, seq 35, length 64
00:23:08.422962 IP computer-network-1 > computer-network-1: ICMP echo request, id 3, seq 36, length 64
00:23:08.422981 IP computer-network-1 > computer-network-1: ICMP echo reply, id 3, seq 36, length 64
```

`tcpdump -i any`



### 4.3 Filtering Packets based on Protocol

```
aditeya@computer-network-1: ~/Desktop
aditeya@computer-network-1: ~/Desk... x aditeya@computer-network-1: ~/Desk... x
aditeya@computer-network-1:~/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
00:23:43.232476 IP computer-network-1 > computer-network-1: ICMP echo request, id 3, seq 70, length 64
00:23:43.232496 IP computer-network-1 > computer-network-1: ICMP echo reply, id 3, seq 70, length 64
00:23:44.253907 IP computer-network-1 > computer-network-1: ICMP echo request, id 3, seq 71, length 64
00:23:44.253923 IP computer-network-1 > computer-network-1: ICMP echo reply, id 3, seq 71, length 64
00:23:45.276631 IP computer-network-1 > computer-network-1: ICMP echo request, id 3, seq 72, length 64
5 packets captured
12 packets received by filter
0 packets dropped by kernel
aditeya@computer-network-1:~/Desktop$
```

`sudo tcpdump -i any -c5 icmp`

### 4.4 Checking Packet Content

```
aditeya@computer-network-1: ~/Desktop
aditeya@computer-network-1: ~/Desk... x aditeya@computer-network-1: ~/Desk... x
aditeya@computer-network-1:~/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
00:26:28.548169 IP 192.168.0.182.34630 > 35.224.99.156.80: Flags [S], seq 3018992784, win 64240, options [mss 1460,sackOK,TS val 763909104 ecr 0,nop,wscale 7], length 0
E..<..@..7....#..C..F.P.,.....I .....
..S.....
00:26:28.794963 IP 35.224.99.156.80 > 192.168.0.182.34630: Flags [S.], seq 758257839, ack 3018992785, win 28160, options [mss 1420,sackOK,TS val 209086629 ecr 763909104,nop,wscale 7], length 0
E..<..@.4....#..C.....P.F-2.,...n.....
..vh.-.S.....oQ
00:26:28.795019 IP 192.168.0.182.34630 > 35.224.99.156.80: Flags [.], ack 1, win 502, options [nop,nop,TS val 763909351 ecr 209086629], length 0
E..4..@..>....#..C..F.P.,-2.....I.....
..T..vh.
00:26:28.795524 IP 192.168.0.182.34630 > 35.224.99.156.80: Flags [P.], seq 1:88, ack 1, win 502, options [nop,nop,TS val 763909351 ecr 209086629], length 87: HTTP: GET / HTTP/1.1
E.....@.....#..C..F.P.,-2.....IX.....
..T..vh.GET / HTTP/1.1
Host: connectivity-check.ubuntu.com
Accept: */*
```

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

```
aditeya@computer-network-1: ~/Desktop
Accept: /*
Connection: close

00:26:29.023025 IP 35.224.99.156.80 > 192.168.0.182.34630: Flags [.], ack 88, win 225, options [nop,nop,TS val 209086910 ecr 763909351], length 0
E..4..@.4.KE#.C.....P.F-2.....
.....
.vi.-.T.vX
00:26:29.023069 IP 35.224.99.156.80 > 192.168.0.182.34630: Flags [P.], seq 1:149, ack 88, win 225, options [nop,nop,TS val 209086911 ecr 763909351], length 148:
HTTP: HTTP/1.1 204 No Content
E....@.4.J.#.C.....P.F-2.....M.....
.vi.-.T.HTTP/1.1 204 No Content
Date: Fri, 04 Sep 2020 18:56:28 GMT
Server: Apache/2.4.18 (Ubuntu)
X-NetworkManager-Status: online
Connection: close

00:26:29.023081 IP 192.168.0.182.34630 > 35.224.99.156.80: Flags [.], ack 149, win 501, options [nop,nop,TS val 763909579 ecr 209086911], length 0
E..4..@.@.<....#.C..F.P.,.-2.D....I.....
..U..vi.
00:26:29.023195 IP 192.168.0.182.34630 > 35.224.99.156.80: Flags [F.], seq 88, a
```

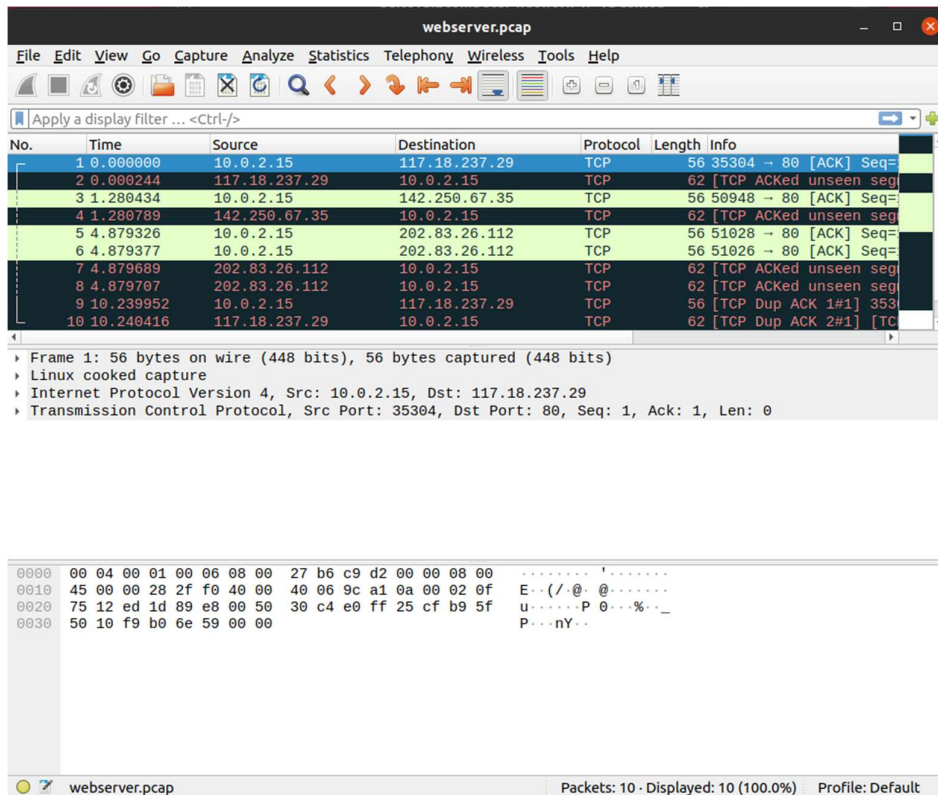
```
aditeya@computer-network-1: ~/Desktop
Server: Apache/2.4.18 (Ubuntu)
X-NetworkManager-Status: online
Connection: close

00:26:29.023081 IP 192.168.0.182.34630 > 35.224.99.156.80: Flags [.], ack 149, win 501, options [nop,nop,TS val 763909579 ecr 209086911], length 0
E..4..@.@.<....#.C..F.P.,.-2.D....I.....
..U..vi.
00:26:29.023195 IP 192.168.0.182.34630 > 35.224.99.156.80: Flags [F.], seq 88, ack 149, win 501, options [nop,nop,TS val 763909579 ecr 209086911], length 0
E..4..@.@.;...#.C..F.P.,.-2.D....I.....
..U..vi.
00:26:29.032005 IP 35.224.99.156.80 > 192.168.0.182.34630: Flags [F.], seq 149, ack 88, win 225, options [nop,nop,TS val 209086911 ecr 763909351], length 0
E..4..@.4.KC#.C.....P.F-2.D.,.....t....
.vi.-.T...
00:26:29.032005 IP 192.168.0.182.34630 > 35.224.99.156.80: Flags [.], ack 150, win 501, options [nop,nop,TS val 763909588 ecr 209086911], length 0
E..4..@.@.:...#.C..F.P.,.-2.E....I.....
..U..vi.
10 packets captured
10 packets received by filter
0 packets dropped by kernel
aditeya@computer-network-1:~/Desktop$
```

## 4.5 Saving Packets to a File

```
aditeya@computer-network-1: ~/Desktop
aditeya@computer-network-1:~/Desktop$ sudo tcpdump -i any -c10 -nn -w webserver.pcap port 80
pcap port 80
tcpdump: listening on any, link-type LINUX_SLL (Linux cooked v1), capture size 262144 bytes
10 packets captured
10 packets received by filter
0 packets dropped by kernel
aditeya@computer-network-1:~/Desktop$
```

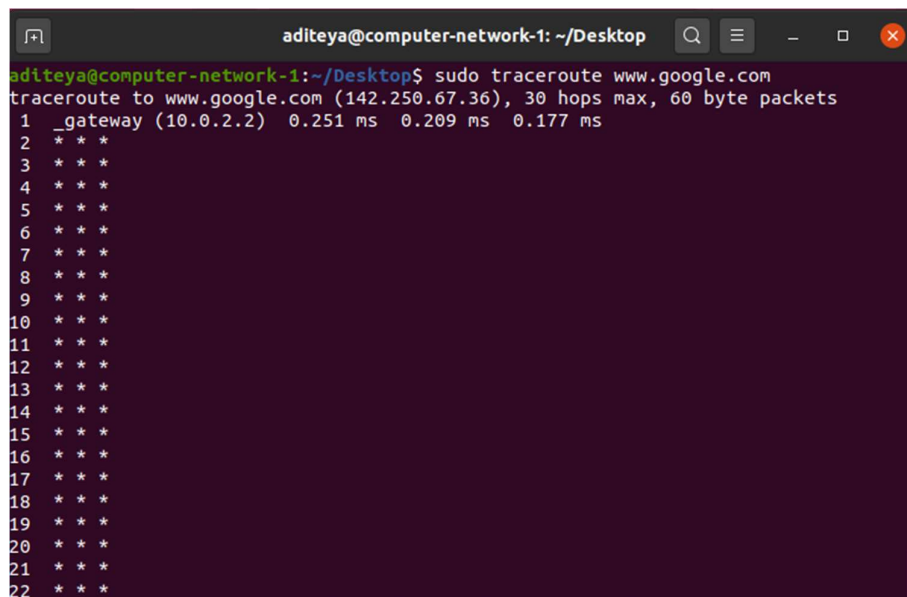
`sudo tcpdump -i any -c10 -nn -w webserver.pcap port 80`



webserver.pcap

## 5. Perform **traceroute** Checks

### 5.1 Running **traceroute**



sudo **traceroute** [www.google.com](http://www.google.com)

```
aditeya@computer-network-1: ~/Desktop
8 * * *
9 * * *
10 * * *
11 * * *
12 * * *
13 * * *
14 * * *
15 * * *
16 * * *
17 * * *
18 * * *
19 * * *
20 * * *
21 * * *
22 * * *
23 * * *
24 * * *
25 * * *
26 * * *
27 * * *
28 * * *
29 * * *
30 * * *
aditeya@computer-network-1:~/Desktop$
```

Running traceroute on Windows using `tracert`

```
Command Prompt
C:\Users\Aditeya\Desktop>tracert www.google.com

Tracing route to www.google.com [142.250.67.36]
over a maximum of 30 hops:

  0  6 ms   3 ms   4 ms  192.168.0.1
  1  40 ms   3 ms  21 ms  10.240.0.1
  2  5 ms    4 ms  24 ms  14.142.183.201.static-Bangalore.vsnl.net.in [14.142.183.201]
  3  11 ms   12 ms  11 ms  172.31.167.54
  4  10 ms   9 ms  13 ms  14.140.100.6.static-vsnl.net.in [14.140.100.6]
  5  10 ms  13 ms  10 ms  115.112.71.65.STDILL-Chennai.vsnl.net.in [115.112.71.65]
  6  10 ms  10 ms  11 ms  121.240.1.50
  7  11 ms   9 ms  16 ms  74.125.242.129
  8  10 ms   9 ms  11 ms  142.250.228.83
  9  9 ms    13 ms 12 ms  maa05s12-in-f4.1e100.net [142.250.67.36]

Trace complete.

C:\Users\Aditeya\Desktop>
```

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

## 5.2 Disabling mapping of IP addresses with hostnames



```
aditeya@computer-network-1: ~/Desktop
aditeya@computer-network-1:~/Desktop$ sudo traceroute -n www.google.com
traceroute to www.google.com (142.250.67.36), 30 hops max, 60 byte packets
 1  10.0.2.2  0.310 ms  0.292 ms  0.276 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
```

`sudo traceroute -n www.google.com`

### 5.3 traceroute with ICMP Protocol

```
aditeya@computer-network-1: ~/Desktop
aditeya@computer-network-1:~/Desktop$ sudo traceroute -I www.google.com
[sudo] password for aditeya:
traceroute to www.google.com (142.250.67.36), 30 hops max, 60 byte packets
 1  _gateway (10.0.2.2)  0.394 ms  0.389 ms  0.384 ms
 2  _gateway (192.168.0.1)  2.662 ms  3.919 ms  4.282 ms
 3  10.240.0.1 (10.240.0.1)  4.282 ms  5.881 ms  6.199 ms
 4  14.142.183.201.static-Bangalore.vsnl.net.in (14.142.183.201)  7.372 ms  7.72
8 ms  7.725 ms
 5  172.31.167.54 (172.31.167.54)  12.076 ms  12.585 ms  12.579 ms
 6  14.140.100.6.static-vsnl.net.in (14.140.100.6)  12.266 ms  10.414 ms  11.433
ms
 7  115.112.71.65.STDILL-Chennai.vsnl.net.in (115.112.71.65)  14.023 ms  10.228
ms  11.095 ms
 8  121.240.1.50 (121.240.1.50)  11.422 ms  11.420 ms  11.694 ms
 9  74.125.242.145 (74.125.242.145)  10.414 ms  10.735 ms  10.733 ms
10  142.250.228.81 (142.250.228.81)  10.728 ms  10.197 ms  10.480 ms
11  maa05s12-in-f4.1e100.net (142.250.67.36)  10.819 ms  11.111 ms  11.109 ms
aditeya@computer-network-1:~/Desktop$
```

`sudo traceroute -I www.google.com`

### 5.4 Testing TCP Connection with traceroute

```
aditeya@computer-network-1: ~/Desktop
aditeya@computer-network-1:~/Desktop$ sudo traceroute -T www.google.com
[sudo] password for aditeya:
traceroute to www.google.com (142.250.67.36), 30 hops max, 60 byte packets
 1 _gateway (10.0.2.2)  0.337 ms  0.337 ms  0.329 ms
 2 maa05s12-in-f4.1e100.net (142.250.67.36)  19.221 ms  19.202 ms  25.603 ms
aditeya@computer-network-1:~/Desktop$
```

`sudo traceroute -T www.google.com`

## 6. Exploring a network with nmap

### 6.1 Scanning Host with Hostname

```
aditeya@computer-network-1: ~/Desktop
aditeya@computer-network-1:~/Desktop$ nmap www.pes.edu
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-05 00:41 IST
Nmap scan report for www.pes.edu (13.71.123.138)
Host is up (0.036s 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 4.88 seconds
aditeya@computer-network-1:~/Desktop$
```

`nmap www.pes.edu`

### 6.2 Scanning Host with IP Address

```
aditeya@computer-network-1: ~/Desktop
aditeya@computer-network-1:~/Desktop$ nmap 163.53.78.128
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-05 00:41 IST
Nmap scan report for 163.53.78.128
Host is up (0.031s 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 11.09 seconds
aditeya@computer-network-1:~/Desktop$
```

`nmap 163.53.78.128`

### 6.3 Scanning Multiple IP Addresses or Subnet (IPv4)

```
aditeya@computer-network-1: ~/Desktop
aditeya@computer-network-1:~/Desktop$ nmap 192.168.1.1 192.168.1.2 192.168.1.3
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-05 00:42 IST
Nmap done: 3 IP addresses (0 hosts up) scanned in 3.09 seconds
aditeya@computer-network-1:~/Desktop$
```

`nmap 192.168.1.1 192.168.1.2 192.168.1.3`

## 7. 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 is 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 the web server is v1.1 and can be seen in the header of the HTTP response sent back to the 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. Example:

```

▼ Hypertext Transfer Protocol
  ▶ HTTP/1.1 200 OK\r\n
    Date: Sat, 05 Sep 2020 08:20:03 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.9 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Sat, 21 Aug 2004 14:21:11 GMT\r\n

```

### 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** –

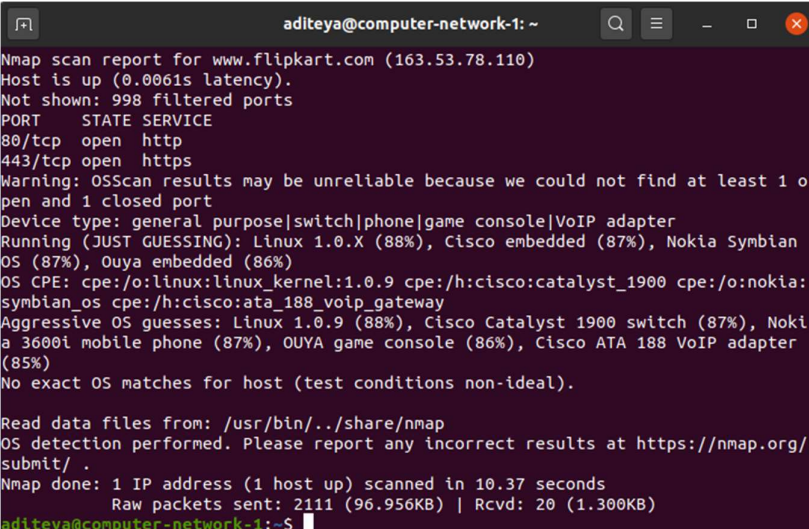
1. We can obtain the remote host app and OS of the server by observing the **Server** files of the HTTP response object. The Server field stores the remote host app or server on which it is hosted and the OS too. Example:

```

▼ Hypertext Transfer Protocol
  ▶ HTTP/1.1 200 OK\r\n
    Date: Sat, 05 Sep 2020 08:20:03 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.9 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Sat, 21 Aug 2004 14:21:11 GMT\r\n

```

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.



```

aditeya@computer-network-1: ~
Nmap scan report for www.flipkart.com (163.53.78.110)
Host is up (0.0061s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|switch|phone|game console|VoIP adapter
Running (JUST GUESSING): Linux 1.0.X (88%), Cisco embedded (87%), Nokia Symbian OS (87%), Ouya embedded (86%)
OS CPE: cpe:/o:linux:linux_kernel:1.0.9 cpe:/h:cisco:catalyst_1900 cpe:/o:nokia:symbian_os cpe:/h:cisco:ata_188_voip_gateway
Aggressive OS guesses: Linux 1.0.9 (88%), Cisco Catalyst 1900 switch (87%), Nokia 3600i mobile phone (87%), OUYA game console (86%), Cisco ATA 188 VoIP adapter (85%)
No exact OS matches for host (test conditions non-ideal).

Read data files from: /usr/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 10.37 seconds
Raw packets sent: 2111 (96.956KB) | Rcvd: 20 (1.300KB)
aditeya@computer-network-1:~$

```

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