

PES1201800410, sec G, rollno 24 , Prashanth A R

Task 1: Linux Interface Configuration(ifconfig / IP command)

Step 1:

ip address table

Interface name	Ip address	Mac address
eth0	(not in use so not assigned)	08:97:98:9c:90:19
mpqemubr0	10.225.240.1	52:54:00:76:85:8c
wlan0	192.168.43.149	D2:F8:8C:FA:7F:5F

```
Applications Places System Terminal Fri Sep 4, 8:55 AM
File Edit View Search Help
eth0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
      ether 08:97:98:9c:90:19 txqueuelen 1000 (Ethernet)
      RX packets 0 bytes 0 (0.0 B)   RX errors 0 dropped 0 overruns 0 frame 0
      TX packets 0 bytes 0 (0.0 B)   TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
      inet 127.0.0.1 netmask 255.0.0.0
      inet6 ::1 prefixlen 128 scopeid 0x10<host>
          loop txqueuelen 1000 (Local Loopback)
          RX packets 11/I bytes 324355 (316.7 KiB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 11/I bytes 324355 (316.7 KiB)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

Interface Configuration(ifconfig / IP command)

Interface name      Ip address      Mac address
mpqemubr0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
      inet 10.225.240.1 netmask 255.255.255.0 broadcast 10.225.240.255
      ether 52:54:00:76:85:8c txqueuelen 1000 (Ethernet)
      RX packets 0 bytes 0 (0.0 B)      10.225.240.1      52:54:00:76:85:8c
      RX errors 0 dropped 0 overruns 0 frame 0
      TX packets 0 bytes 0 (0.0 B)      192.168.43.149      D2:F8:8C:FA:7F:5F
      TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 192.168.43.149 netmask 255.255.255.0 broadcast 192.168.43.255
      inet6 fe80::2e43:d3c9:6c92:f1d prefixlen 64 scopeid 0x20<link>
      inet6 2402:3a80:ccaa:8a56:6819:5a98:186b:c97 prefixlen 64 scopeid 0x0<global>
      ether 14:6:d8:15:5e:4b txqueuelen 1000 (Ethernet)
      RX packets 221723 bytes 113837679 (108.5 MiB)
      RX errors 0 dropped 0 overruns 0 frame 0
      TX packets 29733 bytes 7101827 (6.7 MiB)
      TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(base) [prashanth@parrot:~] 1 characters Default Style English (India) 100% C3 0.00 0.00 3.60%
☰ Menu Pr00TTJTHaoI DcA.pptx Parrot Terminal PES1201800410.odt - L Parrot Terminal
```

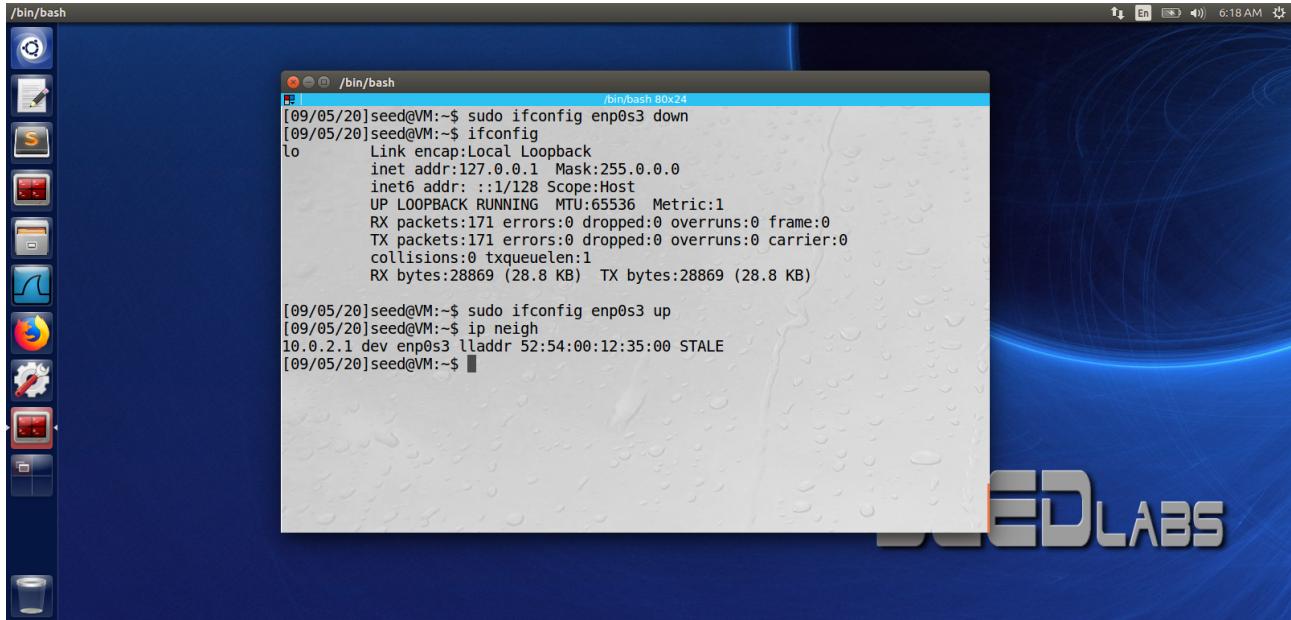
step 2:

```
/bin/bash
[09/05/20]seed@VM:~$ sudo ifconfig enp0s3 10.0.7.24 netmask 255.255.255.0
[09/05/20]seed@VM:~$ ifconfig
enp0s3      Link encap:Ethernet HWaddr 08:00:27:64:ce:db
            inet addr:10.0.7.24 Bcast:10.0.7.255 Mask:255.255.255.0
            inet6 addr: fe80::3518:5f3a:ea76:7828/64 Scope:Link
              UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
              RX packets:92 errors:0 dropped:0 overruns:0 frame:0
              TX packets:176 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 txqueuelen:1000
              RX bytes:56838 (56.8 KB) TX bytes:19529 (19.5 KB)

lo          Link encap:Local Loopback
            inet addr:127.0.0.1 Mask:255.0.0.0
            inet6 addr: ::1/128 Scope:Host
              UP LOOPBACK RUNNING MTU:65536 Metric:1
              RX packets:120 errors:0 dropped:0 overruns:0 frame:0
              TX packets:120 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 txqueuelen:1
              RX bytes:24653 (24.6 KB) TX bytes:24653 (24.6 KB)

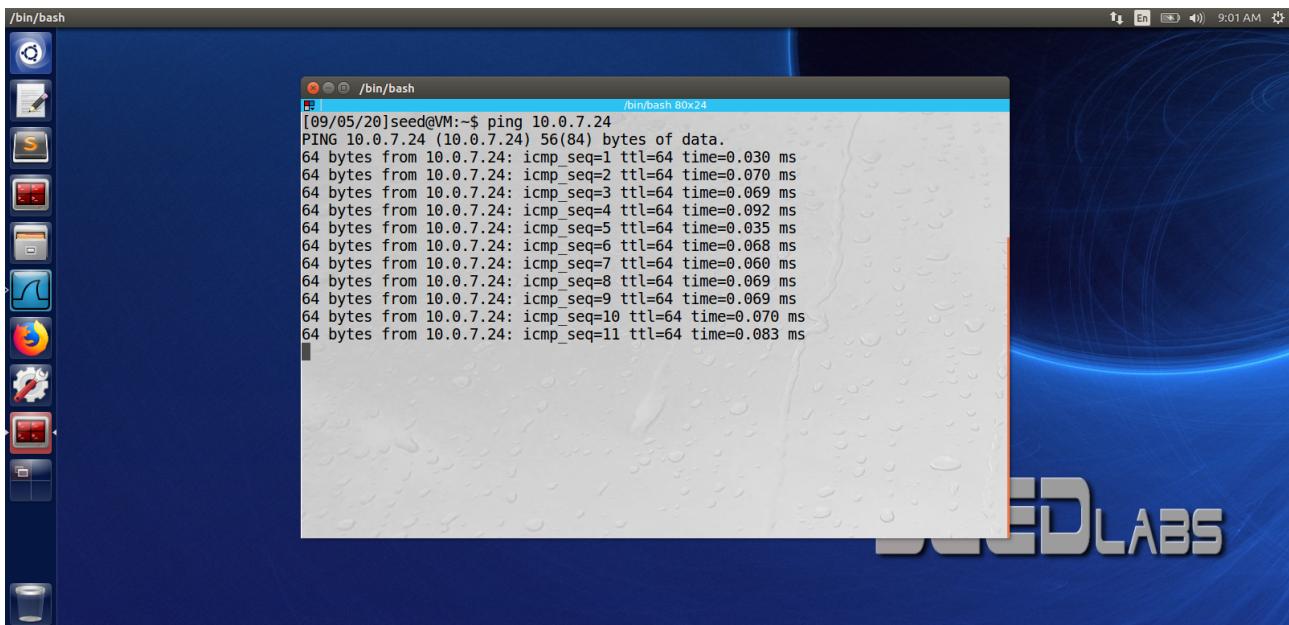
[09/05/20]seed@VM:~$
```

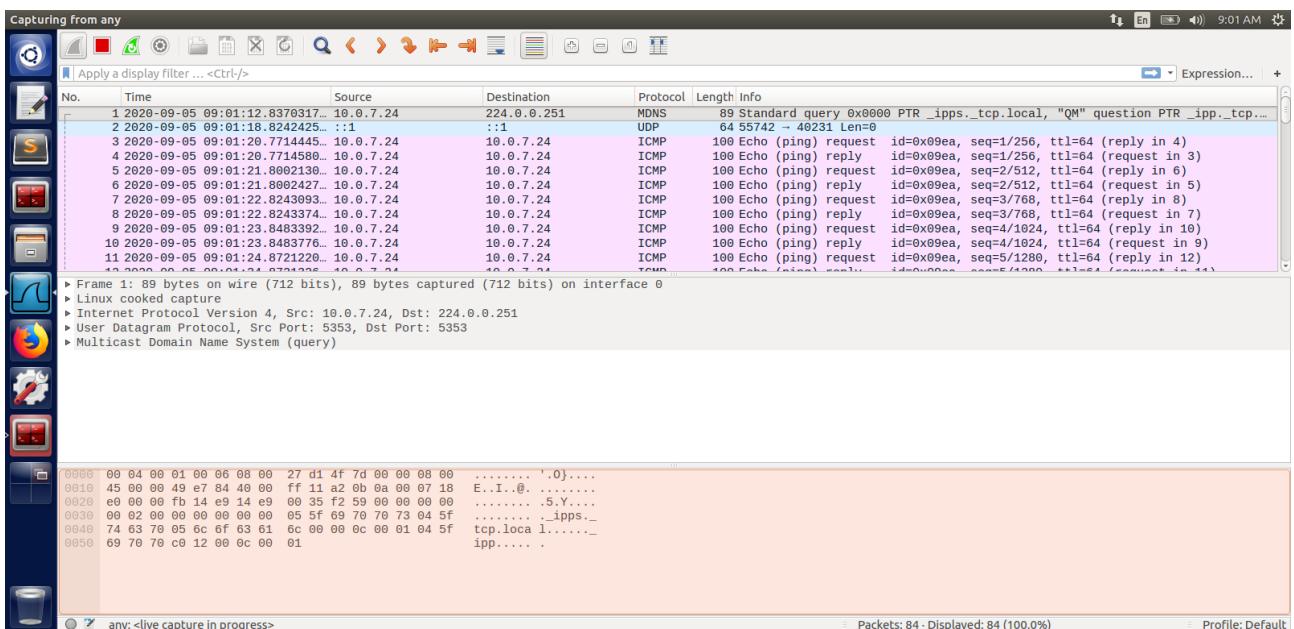
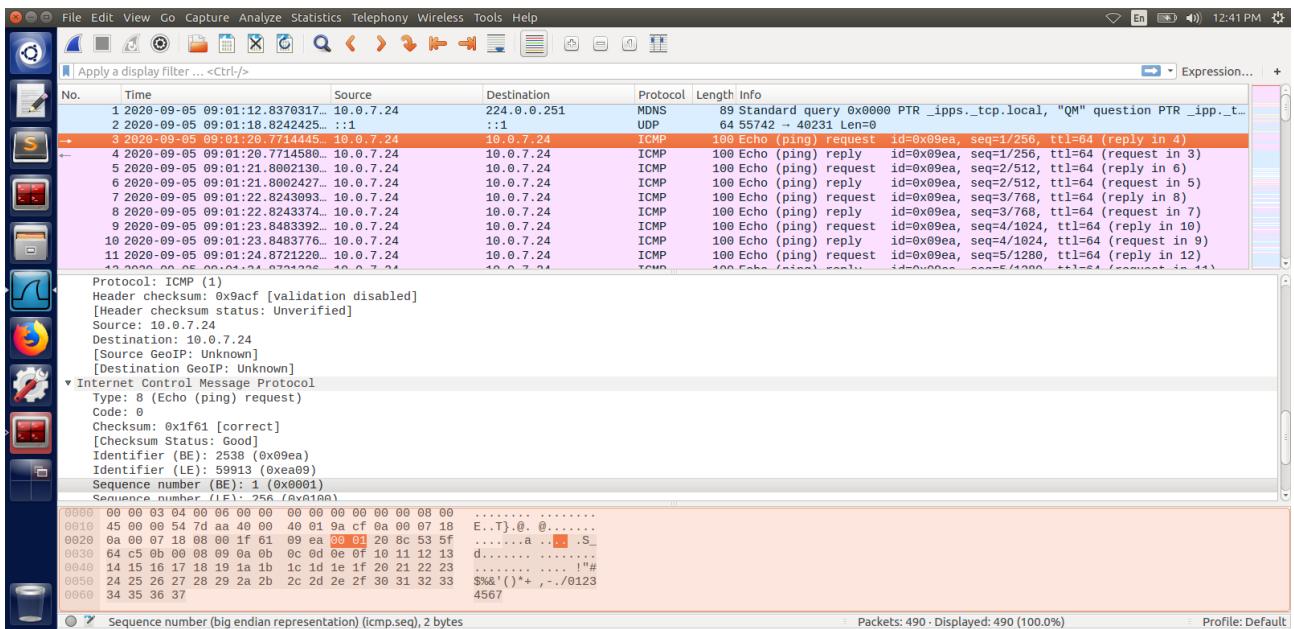
step 3 + step 4



Task 2 :Ping PDU (Packet Data Unitsor Packets) Capture

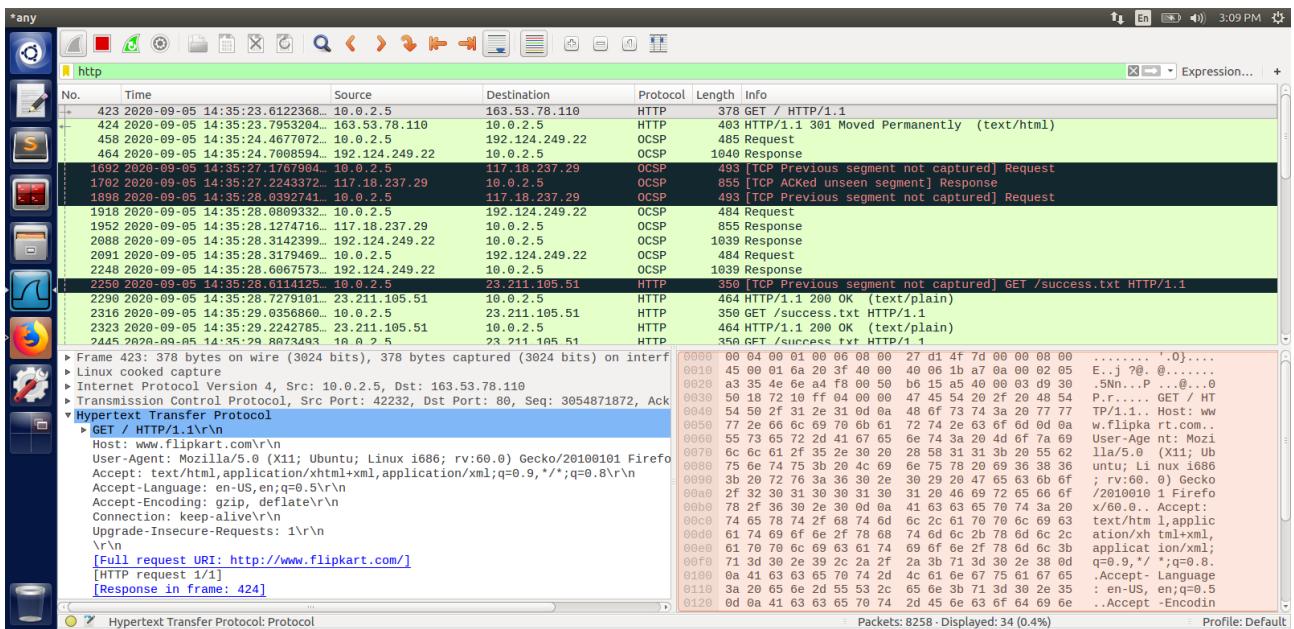
Details	First Echo Request	First Echo Reply
Frame number	3	4
Source IP address	10.0.7.24	10.0.7.24
Destination IP address	10.0.7.24	10.0.7.24
ICMP Type Value	8	0
ICMP Code Value	0	0
Source Ethernet Address	00:00:00:00:00:00	00:00:00:00:00:00
Destination Ethernet Address	00:00:00:00:00:00	00:00:00:00:00:00
Internet Protocol Version	4	4
Time To Live (TTL) Value	64	64





Task 3 :HTTP PDU Capture

Details	First Echo Request	First Echo Reply
Frame number	423	424
Source port	42232	80
Destination port	80	42232
Source IP address	10.0.2.5	163.53.78.110
Destination IP address	163.53.78.110	10.0.2.5
Source Ethernet Address	08:00:27:d1:4f:7d	52:54:00:12:35:00
Destination Ethernet Address	nan	nan



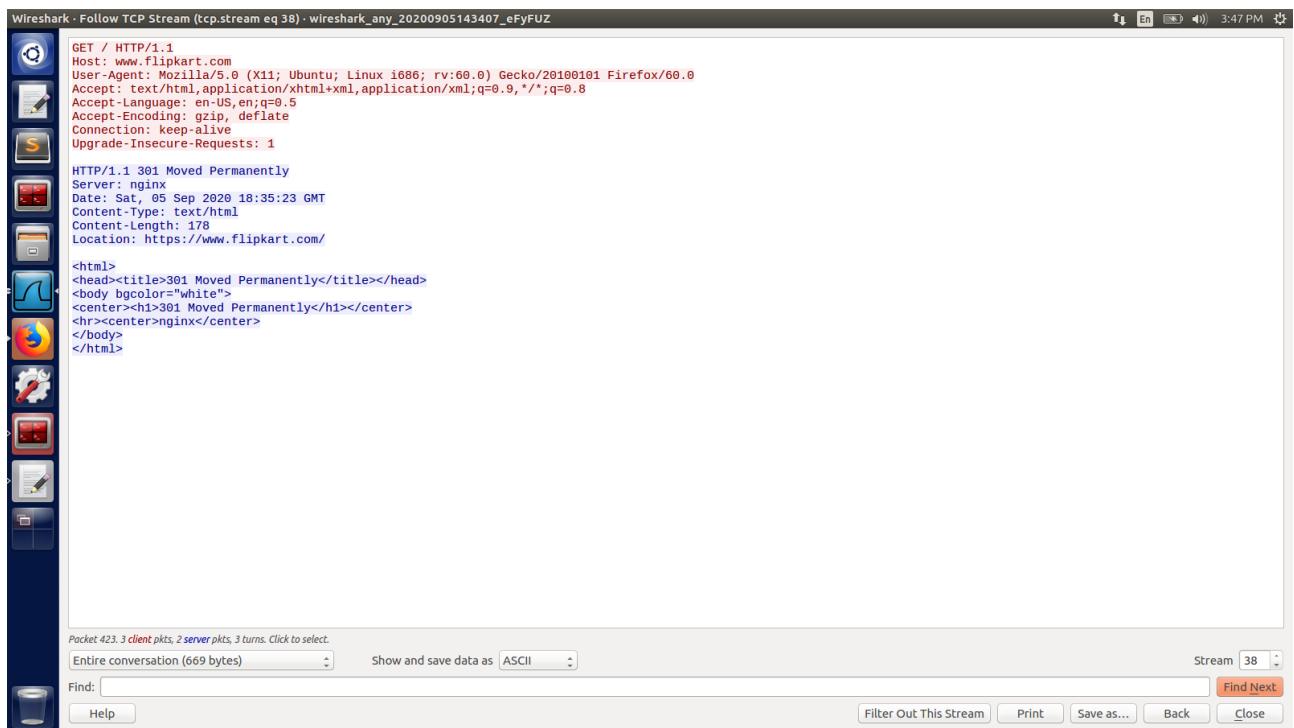
HTTP Request

Get
 Host: www.flipkart.com
 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:60.0) Gecko/20100101 Firefox/60.0
 Accept-Language: en-US,en;q=0.5
 Accept-Encoding: gzip, deflate
 Connection: keep-alive
 Upgrade-Insecure-Requests: 1
[\[Full request URI: http://www.flipkart.com/\]](http://www.flipkart.com/)
[\[HTTP request 1/1\]](#)
[\[Response in frame: 424\]](#)

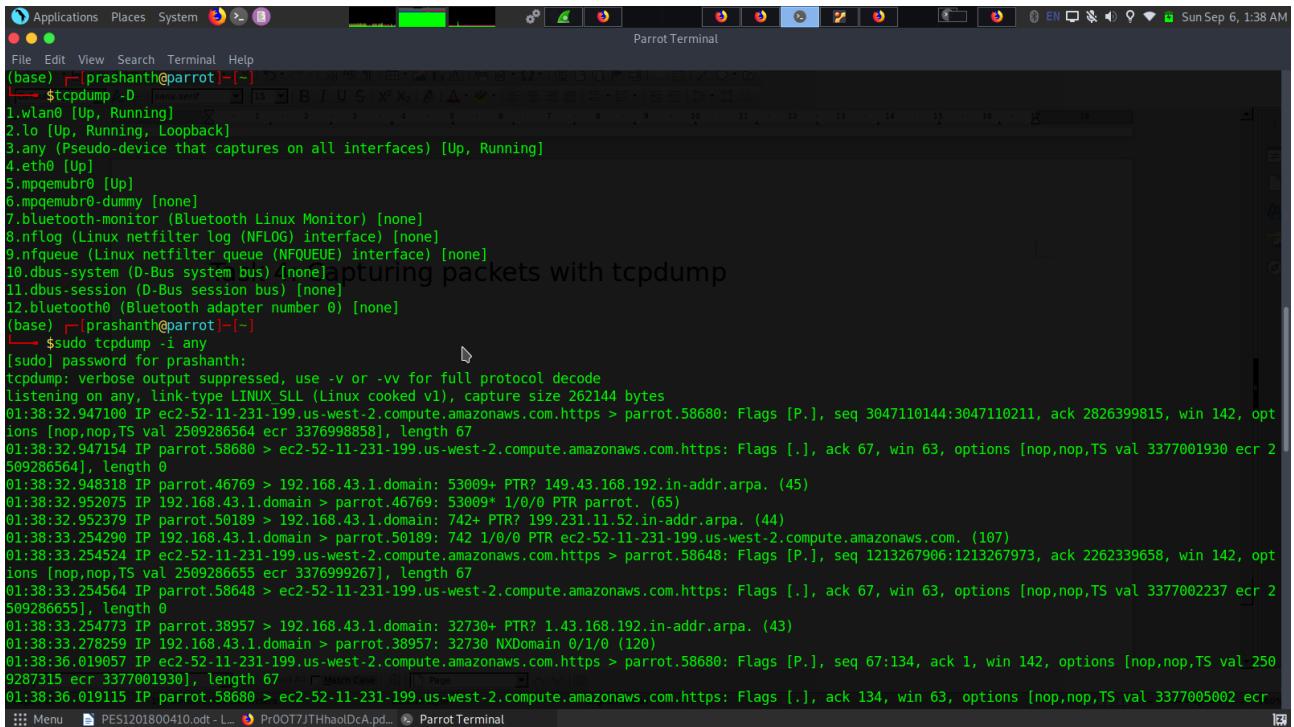
HTTP Response

Server: nginx
 Content-Type: text/html
 Date: Sat, 05 Sep 2020 18:35:23 GMT
 Location: https://www.flipkart.com/
 Content-Length: 178
 Connection: nan

Using Wireshark's Follow TCP Stream



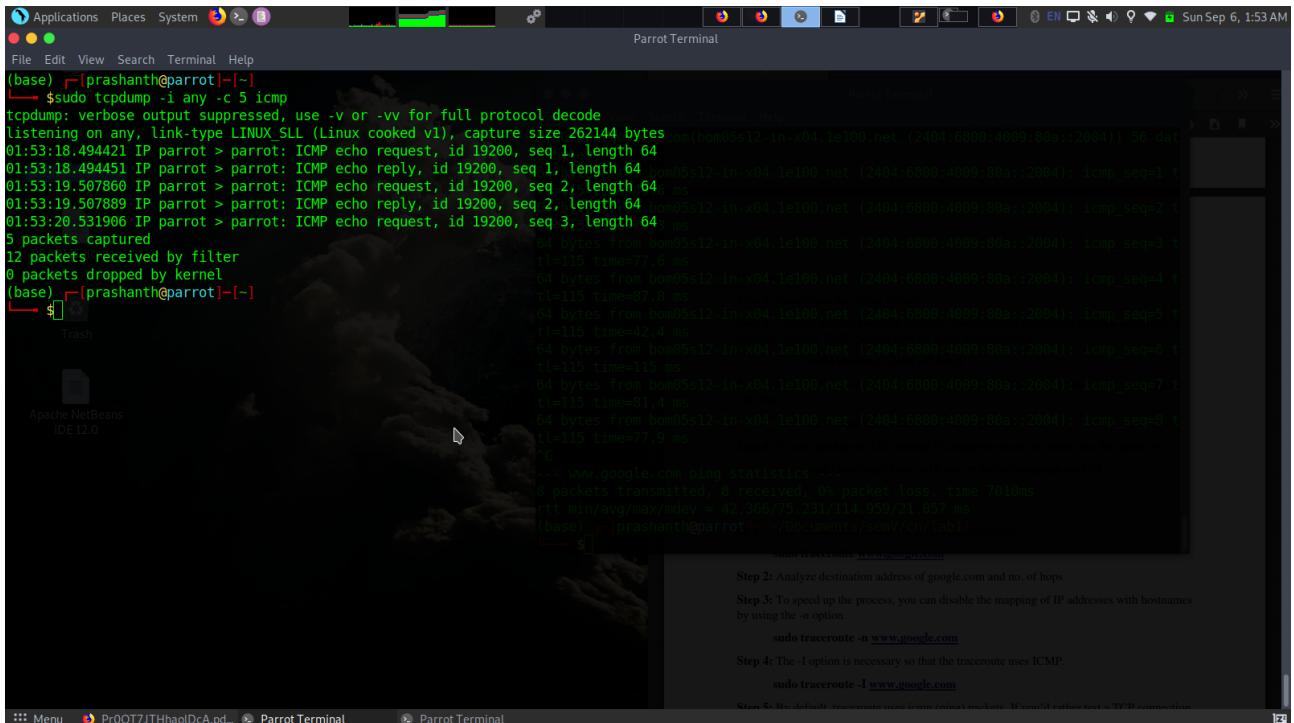
Task 4: Capturing packets with tcpdump



```
(base) [prashanth@parrot] ~
└─$ tcpdump -D
1.wlan0 [Up, Running]
2.lo [Up, Running, Loopback]
3.any (Pseudo-device that captures on all interfaces) [Up, Running]
4.eth0 [Up]
5.mpqemubr0 [Up]
6.mpqemubr0-dummy [none]
7.bluetooth-monitor (Bluetooth Linux Monitor) [none]
8.nflog (Linux netfilter log (NFLOG) interface) [none]
9.nfqueue (Linux netfilter queue (NFQUEUE) interface) [none]
10 dbus-system (D-Bus system bus) [none]
11 dbus-session (D-Bus session bus) [none]
12 bluetooth0 (Bluetooth adapter number 0) [none]
(base) [prashanth@parrot] ~
└─$ sudo tcpdump -i any
[sudo] password for prashanth:
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
01:38:32.947100 IP ec2-52-11-231-199.us-west-2.compute.amazonaws.com.https > parrot.58680: Flags [P.], seq 3047110144:3047110211, ack 2826399815, win 142, options [nop,nop,TS val 2509286564 ecr 3376998858], length 67
01:38:32.947154 IP parrot.58680 > ec2-52-11-231-199.us-west-2.compute.amazonaws.com.https: Flags [.], ack 67, win 63, options [nop,nop,TS val 3377001930 ecr 2509286564], length 0
01:38:32.948318 IP parrot.46769 > 192.168.43.1.domain: 53009+ PTR? 19.43.168.192.in-addr.arpa. (45)
01:38:32.952075 IP 192.168.43.1.domain > parrot.46769: 53009+ 1/0/0 PTR parrot. (65)
01:38:32.952379 IP parrot.50189 > 192.168.43.1.domain: 742+ PTR? 199.231.11.52.in-addr.arpa. (44)
01:38:33.254290 IP 192.168.43.1.domain > parrot.50189: 742 1/0/0 PTR ec2-52-11-231-199.us-west-2.compute.amazonaws.com. (107)
01:38:33.254524 IP ec2-52-11-231-199.us-west-2.compute.amazonaws.com.https > parrot.58648: Flags [P.], seq 1213267906:1213267973, ack 2262339658, win 142, options [nop,nop,TS val 2509286655 ecr 3376999267], length 67
01:38:33.254564 IP parrot.58648 > ec2-52-11-231-199.us-west-2.compute.amazonaws.com.https: Flags [.], ack 67, win 63, options [nop,nop,TS val 3377002237 ecr 2509286655], length 0
01:38:33.254773 IP parrot.38957 > 192.168.43.1.domain: 32730+ PTR? 1.43.168.192.in-addr.arpa. (43)
01:38:33.278259 IP 192.168.43.1.domain > parrot.38957: 32730 NXDomain 0/1/0 (120)
01:38:36.019057 IP ec2-52-11-231-199.us-west-2.compute.amazonaws.com.https > parrot.58680: Flags [P.], seq 67:134, ack 1, win 142, options [nop,nop,TS val 2509287315 ecr 3377001930], length 67
01:38:36.019115 IP parrot.58680 > ec2-52-11-231-199.us-west-2.compute.amazonaws.com.https: Flags [.], ack 134, win 63, options [nop,nop,TS val 3377005002 ecr 2509287315]
::: Menu PES1201800410.odt - L_ PrOOT7JTHaoIDcA.pd... Parrot Terminal
```

format:

timestamp , ipv4 or ipv6 , src ip.port > dst ip.port , tcp flags and respective infomations



```
(base) [prashanth@parrot] ~
└─$ sudo tcpdump -i any -c 5 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
01:53:18.494421 IP parrot > parrot: ICMP echo request, id 19200, seq 1, length 64
01:53:18.494451 IP parrot > parrot: ICMP echo reply, id 19200, seq 1, length 64
01:53:19.507860 IP parrot > parrot: ICMP echo request, id 19200, seq 2, length 64
01:53:19.507889 IP parrot > parrot: ICMP echo reply, id 19200, seq 2, length 64
01:53:20.531906 IP parrot > parrot: ICMP echo request, id 19200, seq 3, length 64
5 packets captured
12 packets received by filter
0 packets dropped by kernel
(base) [prashanth@parrot] ~
└─$ 
Apache NetBeans
IDE 12.0
www.doodle.com ping statistics ...
8 packets transmitted, 8 received, 0% packet loss, time 7010ms
rtt min/avg/max/mdev = 42.366/75.231/114.959/21.057 ms
(base) [prashanth@parrot] ~ /Documents/seminar/cntroute/
```

File Edit View Search Terminal Help

```
$ sudo tcpdump -i any -c 10 -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
01:55:10.679237 IP 192.168.43.149.49142 > 162.6.217.119.80: Flags [S], seq 1038243093, win 64240, options [mss 1460,sackOK,TS val 1040529399 ecr 0,nop,wscale 10], length 0
E..<....@.0....+.w...P.....g.....>.....
01:55:10.929894 IP 192.168.43.149.49144 > 162.6.217.119.80: Flags [S], seq 4071420659, win 64240, options [mss 1460,sackOK,TS val 1040529649 ecr 0,nop,wscale 10], length 0
E..<0 ..@.0....+.w...P.....g.....>.....
01:55:11.042891 IP 162.6.217.119.80 > 192.168.43.149.49142: Flags [S.], seq 2462099445, ack 1038243094, win 8192, options [mss 1370,nop,wscale 8,sackOK,TS val 188784251 ecr 1040529399], length 0
E..<h0.p....w...+..P.....=U.....Z.....>.....
01:55:11.042993 IP 192.168.43.149.49142 > 162.6.217.119.80: Flags [.], ack 1, win 63, options [nop,nop,TS val 1040529763 ecr 188784251], length 0
E..<..5....+.w...P.....?g.....>.....
01:55:11.043408 IP 192.168.43.149.49142 > 162.6.217.119.80: Flags [P.], seq 1:332, ack 1, win 63, options [nop,nop,TS val 1040529763 ecr 188784251], length 33
1: HTTP: GET /HTTP/1.1
E....@.0....+.w...P.....?i.....>.....
9c.0.(GET /HTTP/1.1
Host: redcross.org
User-Agent: Mozilla/5.0 (X11; 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
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1

01:55:11.332121 IP 162.6.217.119.80 > 192.168.43.149.49142: Flags [P.], seq 1:366, ack 332, win 259, options [nop,nop,TS val 188784290 ecr 1040529763], length 365: HTTP: HTTP/1.1 301 Moved Permanently

```

File Edit View Search Terminal Help

Parrot Terminal

File Edit View Search Terminal Help

```
(base) [prashanth@parrot](-/Documents/semV/cn/lab1]
└─$ sudo tcpdump -i any -c 10 -nn -w webserver.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
(base) [prashanth@parrot](-/Documents/semV/cn/lab1]
└─$ cat webserver.pcap
00:00:05 zDD00^E4p@000+0hxIf00P0U;()00-0?0B
00:00:05 (0D0000E4y@0 /hxIf00+0P00)00-0U;00
00:00:05 _README.license
00:00:05 000005 000005 E4.0@0(00+000,00P=0V^000c0?g0
>00
00:00:05 _ZDD00^E4h@p:000,00+0P0000c=0Va0-0
00:00:05 <0D0000E4h@p:T00,00+0P0000c=0Va0-0
00:00:05 >00:00:05 _ZDD00^E4q@000+0hxIf00P0U;))00-0?0B
00:00:05 _ZDD00^E4z@06^.hxIf00+0P00)00-0U;00Dm
00:00:05 JtDD00^E4@@0506+0hxIf00P0U;+)00070B
00:00:05 (base) [prashanth@parrot](-/Documents/semV/cn/lab1]
└─$ ls
1.png ifconfig.png T2_2.png tcpdump_icmp.png
2.png PES1201800410.odt T2_ping.png tcpdump_port80.png
3.png T2_1.png tcpdump1.png 'Updated_Week 1 - Learn and Understand Network Tools.pdf'
(base) [prashanth@parrot](-/Documents/semV/cn/lab1]
└─$ 
```

File Edit View Search Terminal Help

Parrot Terminal

Task 5: Perform Traceroute checks

The screenshot shows a Parrot OS desktop environment. On the left, a terminal window titled 'Parrot Terminal' displays the output of several traceroute commands. One command shows a route to www.google.com through various IP addresses with varying latencies. Another command uses the -I option to show ICMP-based tracerouting. On the right, a web browser window is open to a local file 'index.html' which contains instructions for network analysis, including steps for packet capture and Nmap scanning.

```
(base) [prashanth@parrot](-/Documents/semV/cn/lab1)
└─$ traceroute www.google.com
traceroute to www.google.com (216.58.203.4), 30 hops max, 60 byte packets
1 192.168.43.1 (192.168.43.1) 1.371 ms 1.889 ms 2.042 ms
2 * * *
3 * * *
4 * * *
5 * * *
6 * * *
7 * * *
8 * * * license
9 * * *
10 * * *
11 * * *
12 * * *
13 * * *
14 hkg12s09-in-f4.1e100.net (216.58.203.4) 179.206 ms * 179.596 ms
(base) [prashanth@parrot](-/Documents/semV/cn/lab1)
└─$ traceroute -n www.google.com
traceroute to www.google.com (216.58.203.4), 30 hops max, 60 byte packets
1 192.168.43.1 1.606 ms 2.009 ms 1.953 ms
2 * * *
3 * * *
4 * * *
5 * * *
6 * * *
7 * * *
8 * * *
9 * * *
10 * * *
11 * * *
12 * * *
13 * * *
14 216.58.203.4 57.163 ms * *
(base) [prashanth@parrot](-/Documents/semV/cn/lab1)
└─$
```

Step 4: To filter packets based on protocol, specifying the protocol in the command line. For example, capture ICMP packets only by using this command:
sudo tcpdump -i any -c10 -nn -A port 80

Step 5: Check the packet content. For example, inspect the HTTP content of a web request like this:
sudo tcpdump -i any -c10 -nn -w webserver.pcap port 80

Task 5: Perform Traceroute checks

Step 1: Run the traceroute using the following command.
sudo traceroute www.google.com

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

Step 3: To speed up the process, you can disable the mapping of IP addresses with hostnames by using the -n option
sudo traceroute -n www.google.com

Step 4: The -I option is necessary so that the traceroute uses ICMP.
sudo traceroute -I www.google.com

Step 5: By default, traceroute uses icmp (ping) packets. If you'd rather test a TCP connection to gather data more relevant to web server, you can use the -T flag.
sudo traceroute -T www.google.com

Task 6: Explore an entire network for information (Nmap)

Step 1: You can scan a host using its host name or IP address, for instance.
nmap www.pcs.edu

Step 2: Alternatively, use an IP address to scan.
nmap 163.53.78.128

The screenshot shows a Parrot OS desktop environment. On the left, a terminal window titled 'Parrot Terminal' displays the output of several traceroute commands, similar to the previous screenshot but with different results due to the different host. On the right, a web browser window is open to a local file 'index.html' which contains instructions for network analysis, including steps for packet capture and Nmap scanning.

```
(base) [prashanth@parrot](-/Documents/semV/cn/lab1)
└─$ sudo traceroute -I www.google.com
traceroute to www.google.com (216.58.203.4), 30 hops max, 60 byte packets
1 192.168.43.1 (192.168.43.1) 1.308 ms 1.243 ms 1.675 ms
2 * * *
3 10.166.52.254 (10.166.52.254) 31.478 ms 31.457 ms 31.434 ms
4 10.166.32.9 (10.166.32.9) 32.629 ms 32.610 ms 32.595 ms
5 * * *
6 * * *
7 * * *
8 * * * license
9 * * *
10 * * *
11 * * *
12 * * *
13 * * *
14 hkg12s09-in-f4.1e100.net (216.58.203.4) 34.649 ms 36.434 ms 31.844 ms
(base) [prashanth@parrot](-/Documents/semV/cn/lab1)
└─$ sudo traceroute -T www.google.com
traceroute to www.google.com (216.58.203.4), 30 hops max, 60 byte packets
1 192.168.43.1 (192.168.43.1) 3.883 ms 3.802 ms 3.765 ms
2 * * *
3 * * *
4 * * *
5 * * *
6 * * *
7 * * *
8 * * *
9 * * *
10 * * *
11 * * *
12 * * *
13 * * * hkg12s09-in-f4.1e100.net (216.58.203.4) 53.979 ms
(base) [prashanth@parrot](-/Documents/semV/cn/lab1)
└─$
```

Step 4: To filter packets based on protocol, specifying the protocol in the command line. For example, capture ICMP packets only by using this command:
sudo tcpdump -i any -c10 -nn -A port 80

Step 5: Check the packet content. For example, inspect the HTTP content of a web request like this:
sudo tcpdump -i any -c10 -nn -w webserver.pcap port 80

Task 5: Perform Traceroute checks

Step 1: Run the traceroute using the following command.
sudo traceroute www.google.com

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

Step 3: To speed up the process, you can disable the mapping of IP addresses with hostnames by using the -n option
sudo traceroute -n www.google.com

Step 4: The -I option is necessary so that the traceroute uses ICMP.
sudo traceroute -I www.google.com

Step 5: By default, traceroute uses icmp (ping) packets. If you'd rather test a TCP connection to gather data more relevant to web server, you can use the -T flag.
sudo traceroute -T www.google.com

Task 6: Explore an entire network for information (Nmap)

Step 1: You can scan a host using its host name or IP address, for instance.
nmap www.pcs.edu

Step 2: Alternatively, use an IP address to scan.
nmap 163.53.78.128

Task 6: Explore an entire network for information (Nmap)

The screenshot shows a Parrot OS desktop environment. In the foreground, a terminal window titled "Parrot Terminal" is open, displaying Nmap scan results for "www.pes.edu". The output shows the host is up with 998 filtered ports, and ports 80/tcp and 443/tcp are open. The command used was \$nmap www.pes.edu.

In the background, a web browser window is open to "https://www.google.com". A tooltip from a help guide is visible, explaining the use of the -I option for ICMP traceroute.

```
(base) [prashanth@parrot]~/Documents/semV/cn/lab1]$ nmap www.pes.edu
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-06 02:01 IST
Nmap scan report for www.pes.edu (13.71.123.138)
Host is up (0.025s latency).
Other addresses for www.pes.edu (not scanned): fd00:0:b:33::d47:7b8a
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 3.96 seconds
(base) [prashanth@parrot]~/Documents/semV/cn/lab1]$ nmap 163.53.78.128
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-06 02:01 IST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 0.08 seconds
(base) [prashanth@parrot]~/Documents/semV/cn/lab1]$ nmap 163.53.78.128 -Pn
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-06 02:01 IST
Nmap scan report for 163.53.78.128
Host is up (0.055s 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 9.25 seconds
(base) [prashanth@parrot]~/Documents/semV/cn/lab1]$
```

The screenshot shows a Parrot OS desktop environment. In the foreground, a terminal window titled "Parrot Terminal" is open, displaying Nmap scan results for "parrot" (192.168.43.149). The host is up with 999 closed ports, and port 22/tcp is open. The command used was \$nmap 192.168.43.149.

In the background, a web browser window is open to "https://www.google.com". A tooltip from a help guide is visible, explaining the use of the -I option for ICMP traceroute.

```
(base) [prashanth@parrot]~/Documents/semV/cn/lab1]$ nmap 192.168.43.149
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-06 02:03 IST
Nmap scan report for parrot (192.168.43.149)
Host is up (0.000072s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap scan report for 192.168.43.1
Host is up (0.0024s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
53/tcp    open  domain

Nmap done: 3 IP addresses (2 hosts up) scanned in 2.56 seconds
(base) [prashanth@parrot]~/Documents/semV/cn/lab1]$
```

Questions on above observations:

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

Ans: HTTP 1.1

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

Ans:

Tue, 26 May 2020 22:22:26 GMT --this is from the website i visited

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

Ans: By using -c flag

eg \$ping -c 5 www.google.com

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

Ans: By using -O Os-detection in nmap

-A to give details about the apps running on the host at a particular port (there are many different options -A is just one way to go)

eg \$nmap www.pes.edu -O -A