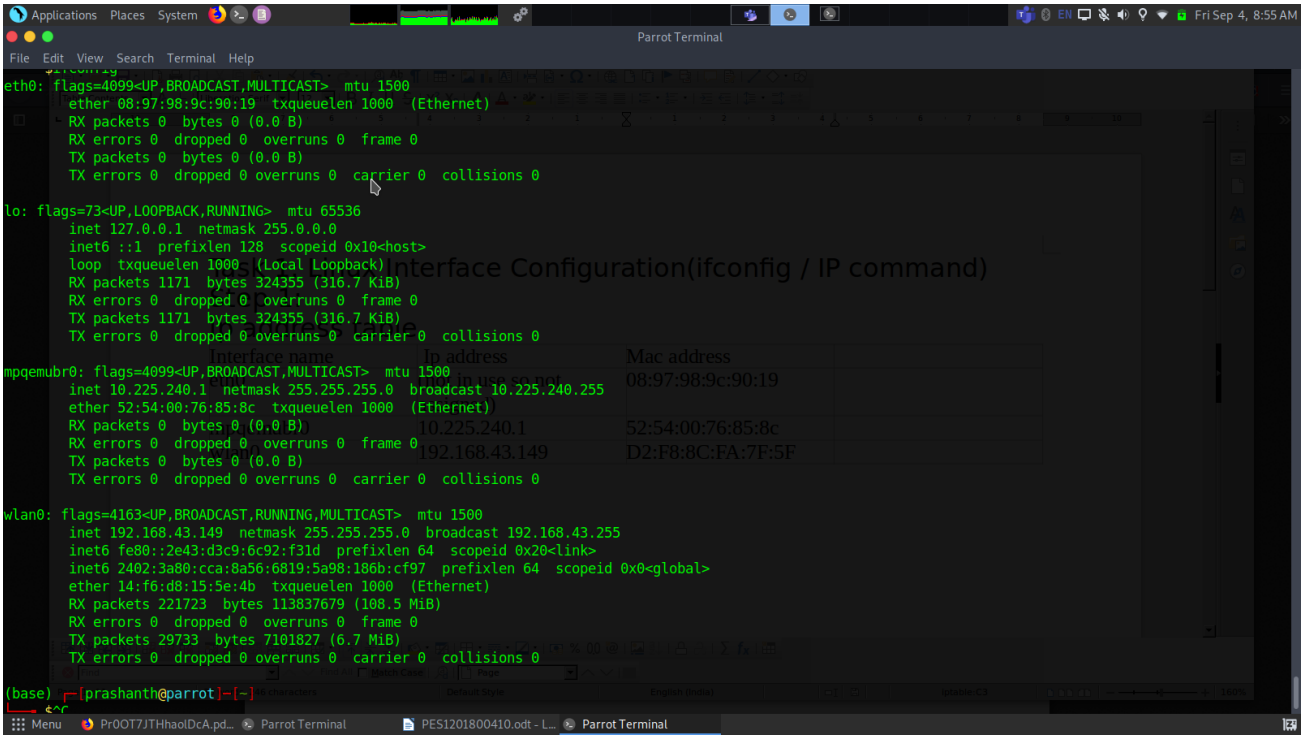
PES1201800410, sec G, rollno 24 , Prashanth A R

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

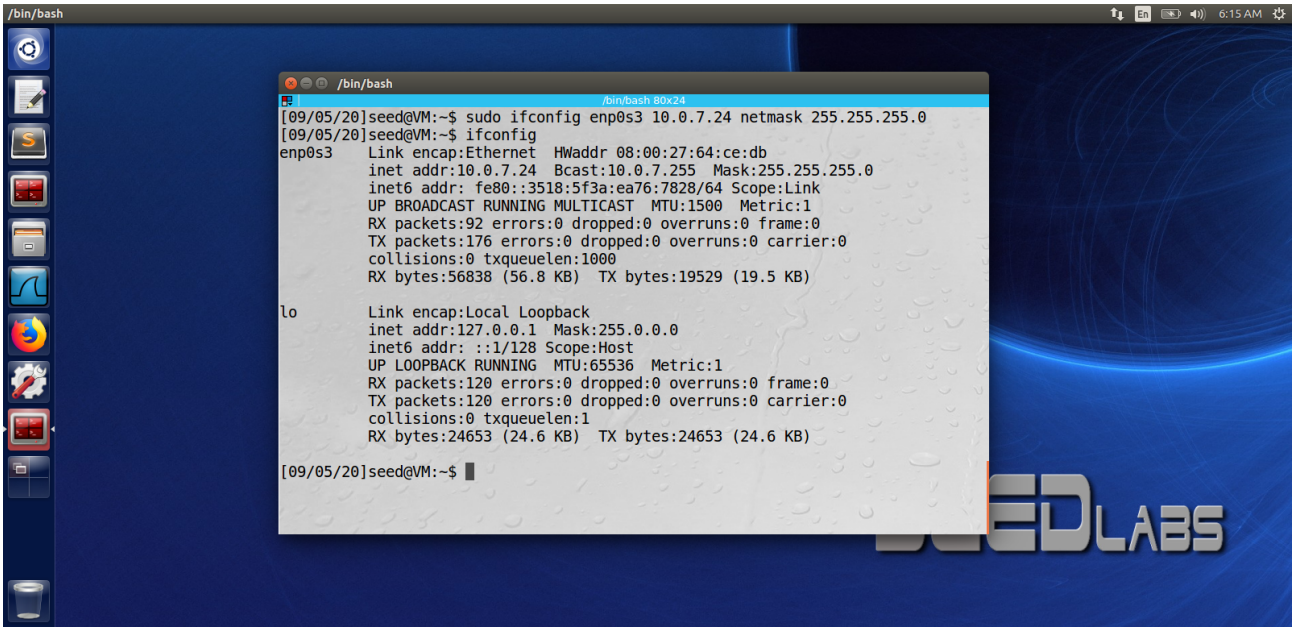
Step 1:

ip address table

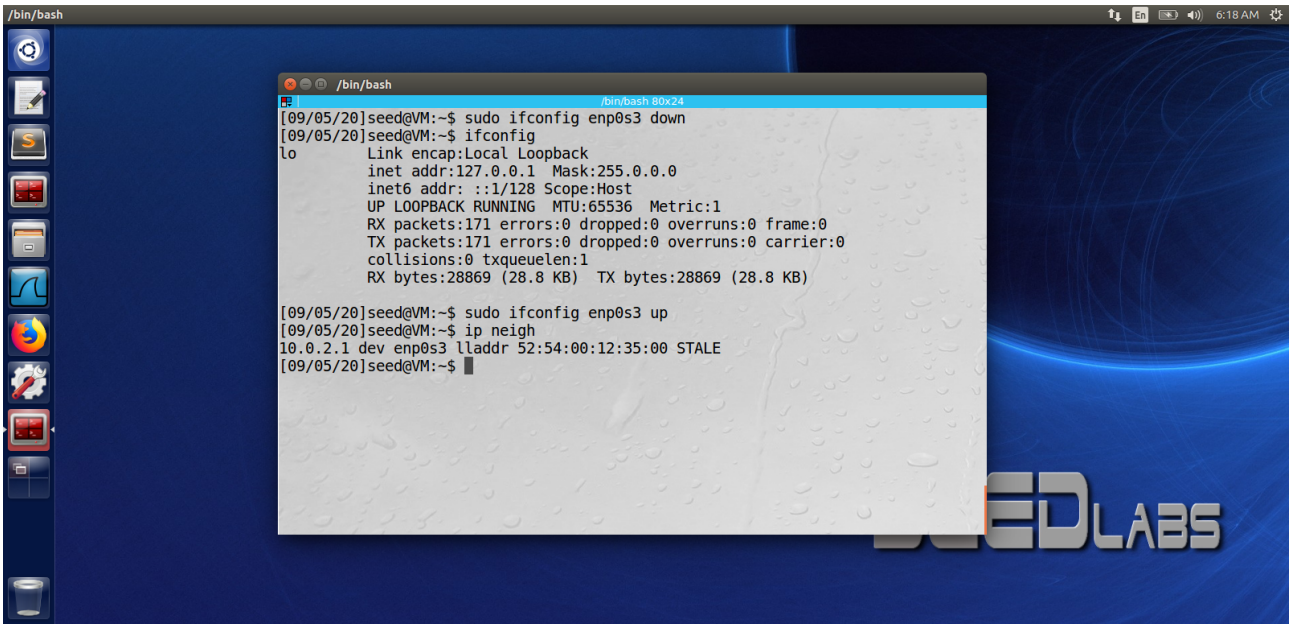
Interface name	Ip address	Mac address
eth0	(not in use so not assigned)	08:97:98:9c:90:19
mpqemubr0	10.225.240.1	52:54:00:76:85:8c
wlan0	192.168.43.149	D2:F8:8C:FA:7F:5F



step 2:

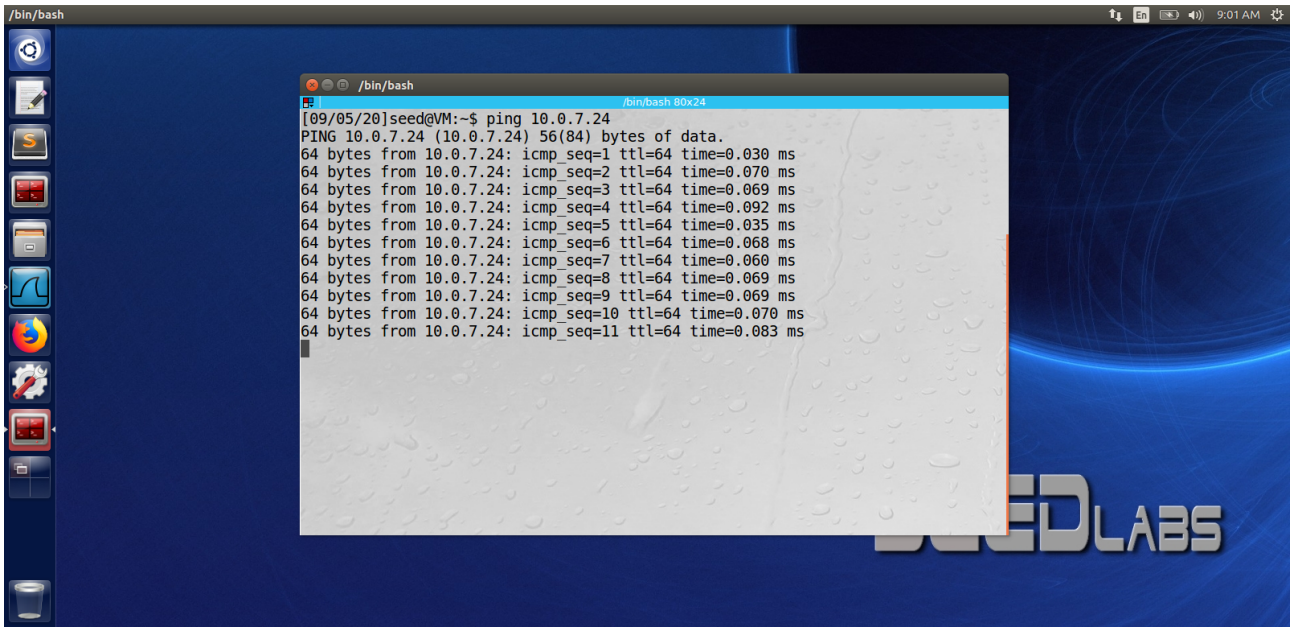


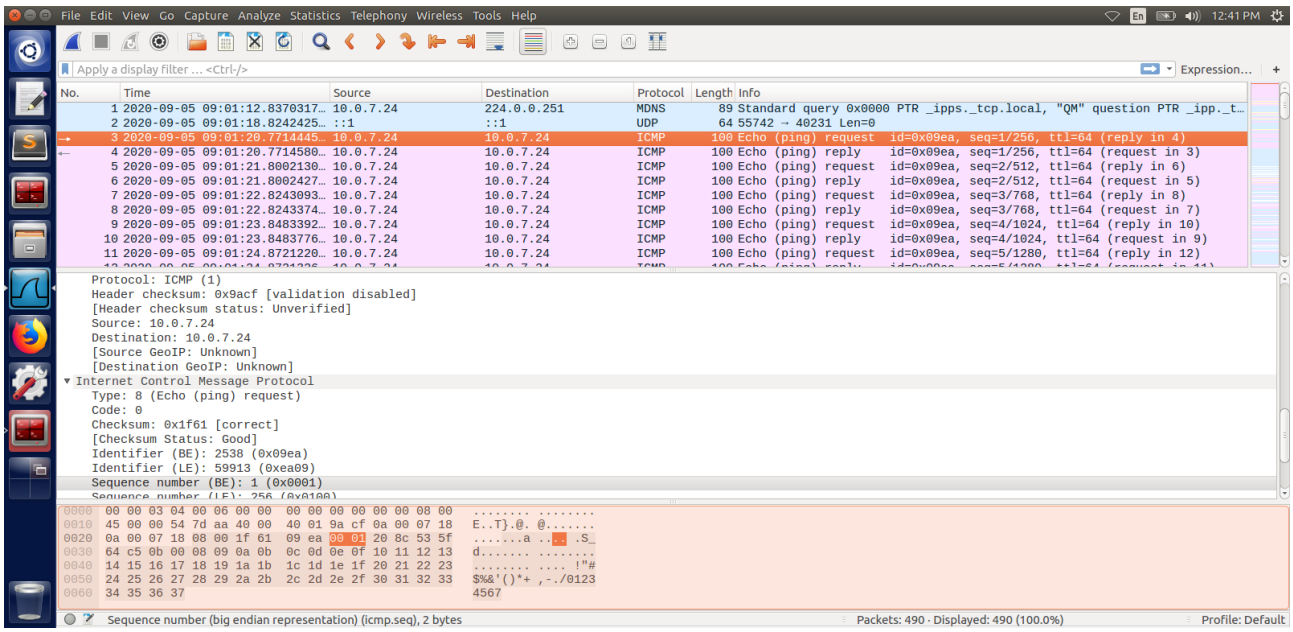
step 3 + step 4

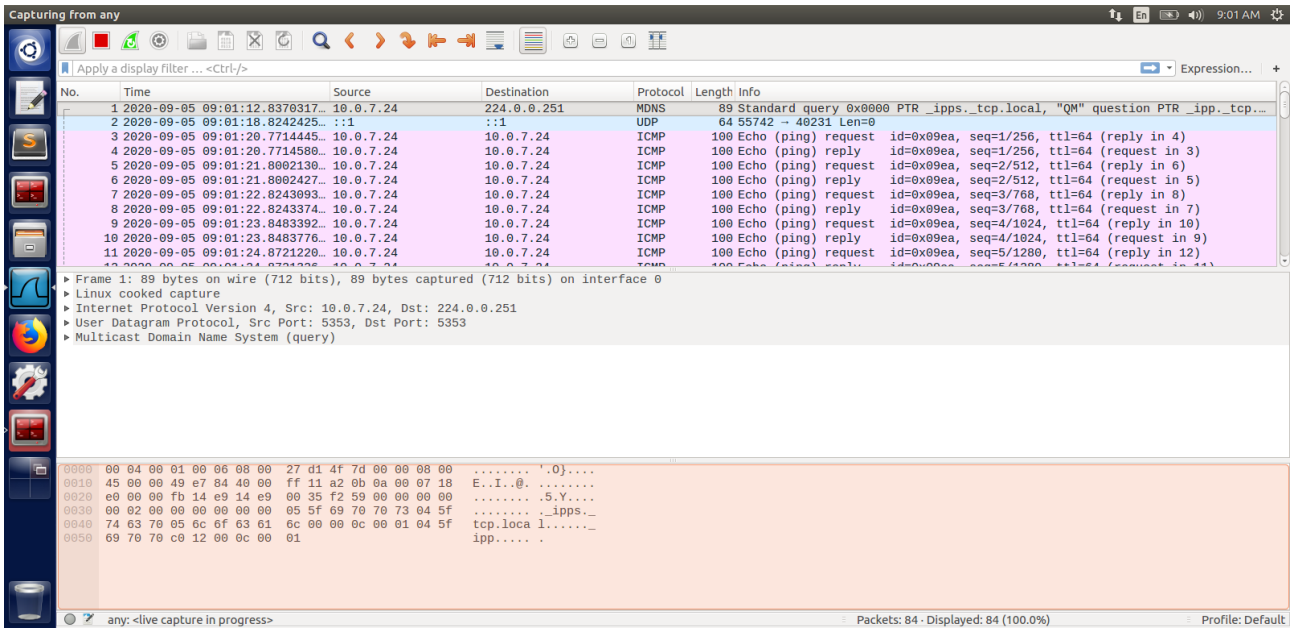

/bin/bash
6:18 AM
/bin/bash
/bin/bash 80x24
[09/05/20]seed@VM:~$ sudo ifconfig enp0s3 down
[09/05/20]seed@VM:~$ ifconfig
lo   Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:65536 Metric:1
          RX packets:171 errors:0 dropped:0 overruns:0 frame:0
          TX packets:171 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:28869 (28.8 KB) TX bytes:28869 (28.8 KB)
[09/05/20]seed@VM:~$ sudo ifconfig enp0s3 up
[09/05/20]seed@VM:~$ ip neigh
10.0.2.1 dev enp0s3 lladdr 52:54:00:12:35:00 STALE
[09/05/20]seed@VM:~$
SEEDLABS

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 Addres	00:00:00:00:00:00	00:00:00:00:00:00
Internet Protocol Version	4	4
Time To Live (TTL) Value	64	64

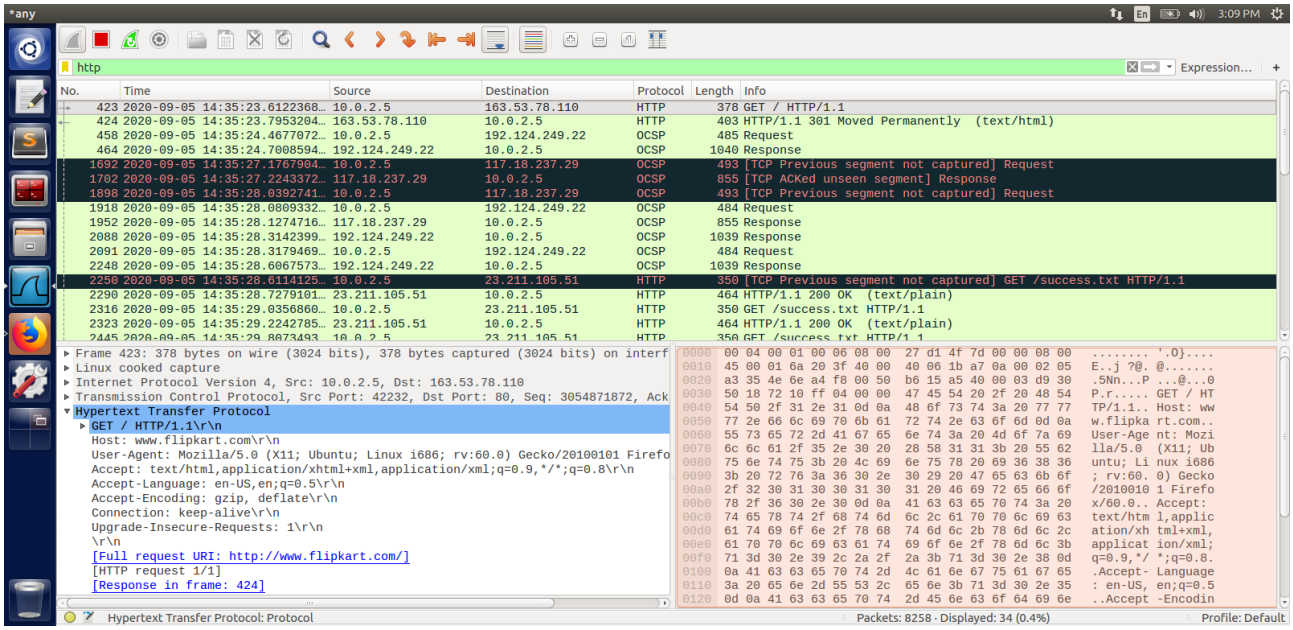



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
12:41 PM
Apply a display filter … <Ctrl-/>
Expression…
No. Time Source Destination Protocol Length Info
1 2020-09-05 09:01:12.8370317… 10.0.7.24 224.0.0.251 MDNS 89 Standard query 0x0000 PTR _ipps._tcp.local, "QM" question PTR _ipp._t…
2 2020-09-05 09:01:18.8242425… ::1 ::1 UDP 64 55742 → 40231 Len=0
3 2020-09-05 09:01:20.7714445… 10.0.7.24 10.0.7.24 ICMP 100 Echo (ping) request id=0x09ea, seq=1/256, ttl=64 (reply in 4)
4 2020-09-05 09:01:20.7714580… 10.0.7.24 10.0.7.24 ICMP 100 Echo (ping) reply id=0x09ea, seq=1/256, ttl=64 (request in 3)
5 2020-09-05 09:01:21.8002130… 10.0.7.24 10.0.7.24 ICMP 100 Echo (ping) request id=0x09ea, seq=2/512, ttl=64 (reply in 6)
6 2020-09-05 09:01:21.8002427… 10.0.7.24 10.0.7.24 ICMP 100 Echo (ping) reply id=0x09ea, seq=2/512, ttl=64 (request in 5)
7 2020-09-05 09:01:22.8243093… 10.0.7.24 10.0.7.24 ICMP 100 Echo (ping) request id=0x09ea, seq=3/768, ttl=64 (reply in 8)
8 2020-09-05 09:01:22.8243374… 10.0.7.24 10.0.7.24 ICMP 100 Echo (ping) reply id=0x09ea, seq=3/768, ttl=64 (request in 7)
9 2020-09-05 09:01:23.8483392… 10.0.7.24 10.0.7.24 ICMP 100 Echo (ping) request id=0x09ea, seq=4/1024, ttl=64 (reply in 10)
10 2020-09-05 09:01:23.8483776… 10.0.7.24 10.0.7.24 ICMP 100 Echo (ping) reply id=0x09ea, seq=4/1024, ttl=64 (request in 9)
11 2020-09-05 09:01:24.8721220… 10.0.7.24 10.0.7.24 ICMP 100 Echo (ping) request id=0x09ea, seq=5/1280, ttl=64 (reply in 12)
Protocol: ICMP (1)
Header checksum: 0x9acf [validation disabled]
[Header checksum status: Unverified]
Source: 10.0.7.24
Destination: 10.0.7.24
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0x1f61 [correct]
[Checksum Status: Good]
Identifier (BE): 2538 (0x09ea)
Identifier (LE): 59913 (0xea09)
Sequence number (BE): 1 (0x0001)
0000 00 00 03 04 00 06 00 00 00 00 00 00 08 00 ....
0010 45 00 00 54 7d aa 40 00 40 01 9a cf 0a 00 07 18 E..T}.@. @.......
0020 0a 00 07 18 08 00 1f 61 09 ea 00 01 20 8c 53 5f ....a .... .S_
0030 64 c5 0b 00 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 d....... ....
0040 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 .... !"#
0050 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 $%&'()*+ ,-./0123
0060 34 35 36 37 4567
Sequence number (big endian representation) (icmp.seq), 2 bytes
Packets: 490 · Displayed: 490 (100.0%)
Profile: Default


Capturing from any
9:01 AM
Apply a display filter … <Ctrl-/>
Expression…
No. Time Source Destination Protocol Length Info
1 2020-09-05 09:01:12.8370317… 10.0.7.24 224.0.0.251 MDNS 89 Standard query 0x0000 PTR _ipps._tcp.local, "QM" question PTR _ipp._tcp.…
2 2020-09-05 09:01:18.8242425… ::1 ::1 UDP 64 55742 → 40231 Len=0
3 2020-09-05 09:01:20.7714445… 10.0.7.24 10.0.7.24 ICMP 100 Echo (ping) request id=0x09ea, seq=1/256, ttl=64 (reply in 4)
4 2020-09-05 09:01:20.7714580… 10.0.7.24 10.0.7.24 ICMP 100 Echo (ping) reply id=0x09ea, seq=1/256, ttl=64 (request in 3)
5 2020-09-05 09:01:21.8002130… 10.0.7.24 10.0.7.24 ICMP 100 Echo (ping) request id=0x09ea, seq=2/512, ttl=64 (reply in 6)
6 2020-09-05 09:01:21.8002427… 10.0.7.24 10.0.7.24 ICMP 100 Echo (ping) reply id=0x09ea, seq=2/512, ttl=64 (request in 5)
7 2020-09-05 09:01:22.8243093… 10.0.7.24 10.0.7.24 ICMP 100 Echo (ping) request id=0x09ea, seq=3/768, ttl=64 (reply in 8)
8 2020-09-05 09:01:22.8243374… 10.0.7.24 10.0.7.24 ICMP 100 Echo (ping) reply id=0x09ea, seq=3/768, ttl=64 (request in 7)
9 2020-09-05 09:01:23.8483392… 10.0.7.24 10.0.7.24 ICMP 100 Echo (ping) request id=0x09ea, seq=4/1024, ttl=64 (reply in 10)
10 2020-09-05 09:01:23.8483776… 10.0.7.24 10.0.7.24 ICMP 100 Echo (ping) reply id=0x09ea, seq=4/1024, ttl=64 (request in 9)
11 2020-09-05 09:01:24.8721220… 10.0.7.24 10.0.7.24 ICMP 100 Echo (ping) request id=0x09ea, seq=5/1280, ttl=64 (reply in 12)
Frame 1: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface 0
Linux cooked capture
Internet Protocol Version 4, Src: 10.0.7.24, Dst: 224.0.0.251
User Datagram Protocol, Src Port: 5353, Dst Port: 5353
Multicast Domain Name System (query)
0000 00 04 00 01 00 06 08 00 27 d1 4f 7d 00 00 08 00 .... '.O}....
0010 45 00 00 49 e7 84 40 00 ff 11 a2 0b 0a 00 07 18 E..I..@. ....
0020 e0 00 00 fb 14 e9 14 e9 00 35 f2 59 00 00 00 00 .... .5.Y....
0030 00 02 00 00 00 00 00 00 05 5f 69 70 70 73 04 5f .... ._ipps._
0040 74 63 70 05 6c 6f 63 61 6c 00 00 0c 00 01 04 5f tcp.loca l......_
0050 69 70 70 c0 12 00 0c 00 01 ipp..... .
any: <live capture in progress>
Packets: 84 · Displayed: 84 (100.0%)
Profile: Default

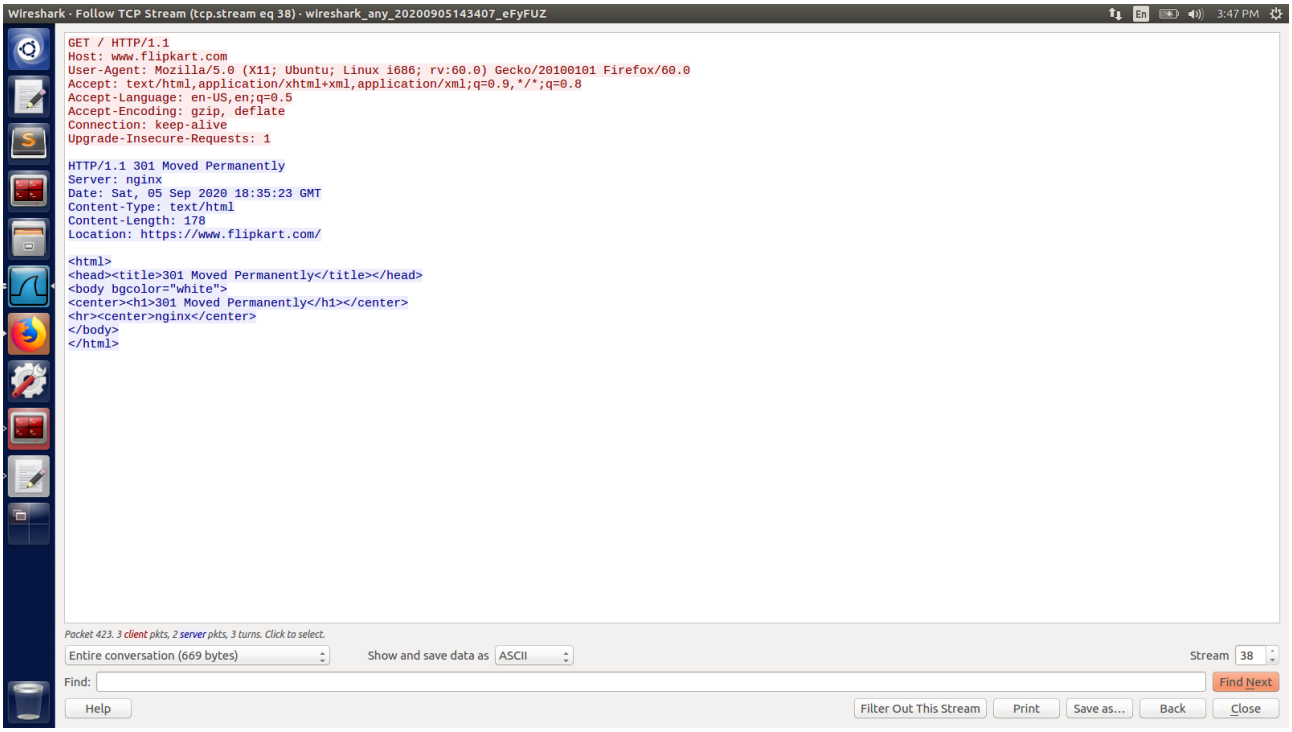
Task 3 :HTTP PDU Capture

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 Addres	nan	nan

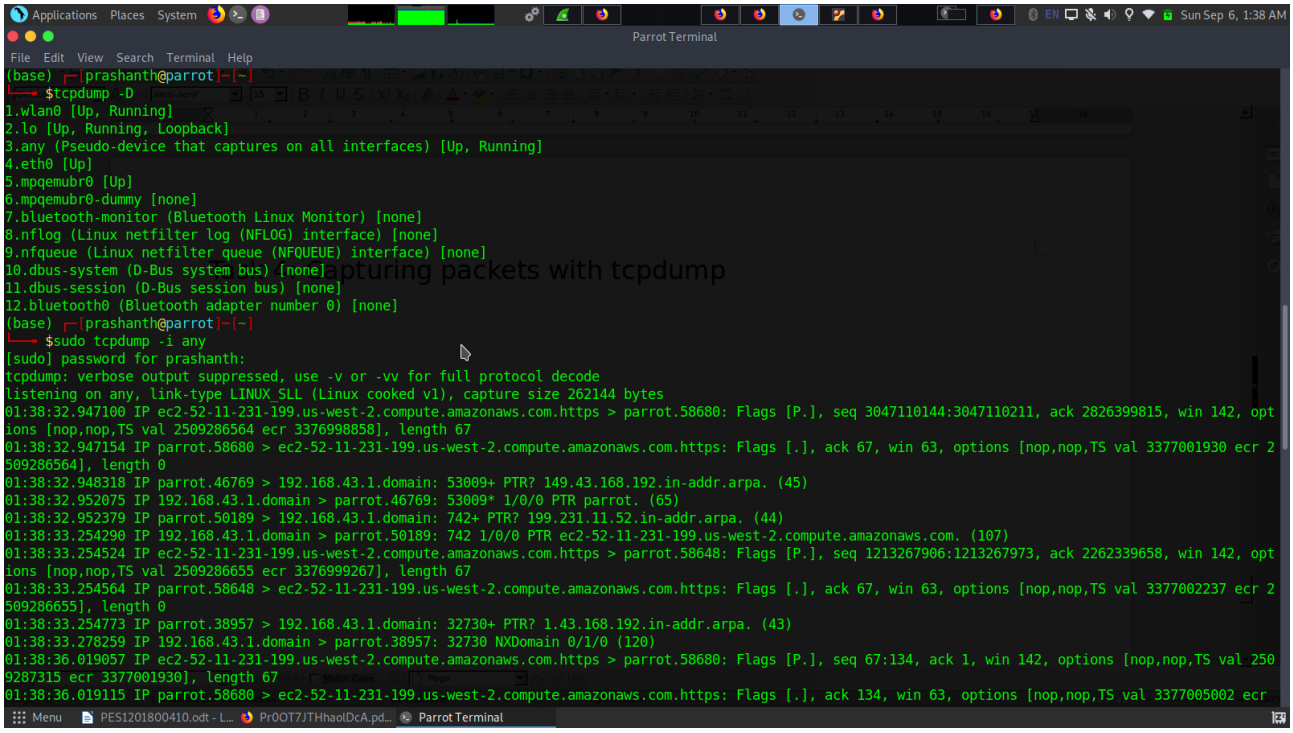


HTTP Request		HTTP Response	
Get	HTTP/1.1	Server	nginx
Host	Www.flipkart.com	Content-Type	text/html
User-Agent	Mozilla/5.0(X11; Ubuntu; Linux i686; rv:60.0) Genko/20100101 Firefox/60.0	Date	Sat, 05 Sep 2020 18:35:23 GMT
Accept-Language	en-US,en;q=0.5	Location	https:// www.flipkart.com/
Accept-Encoding	gzip, deflate	Content-Length	178
Connection	keep-alive	Connection	nan

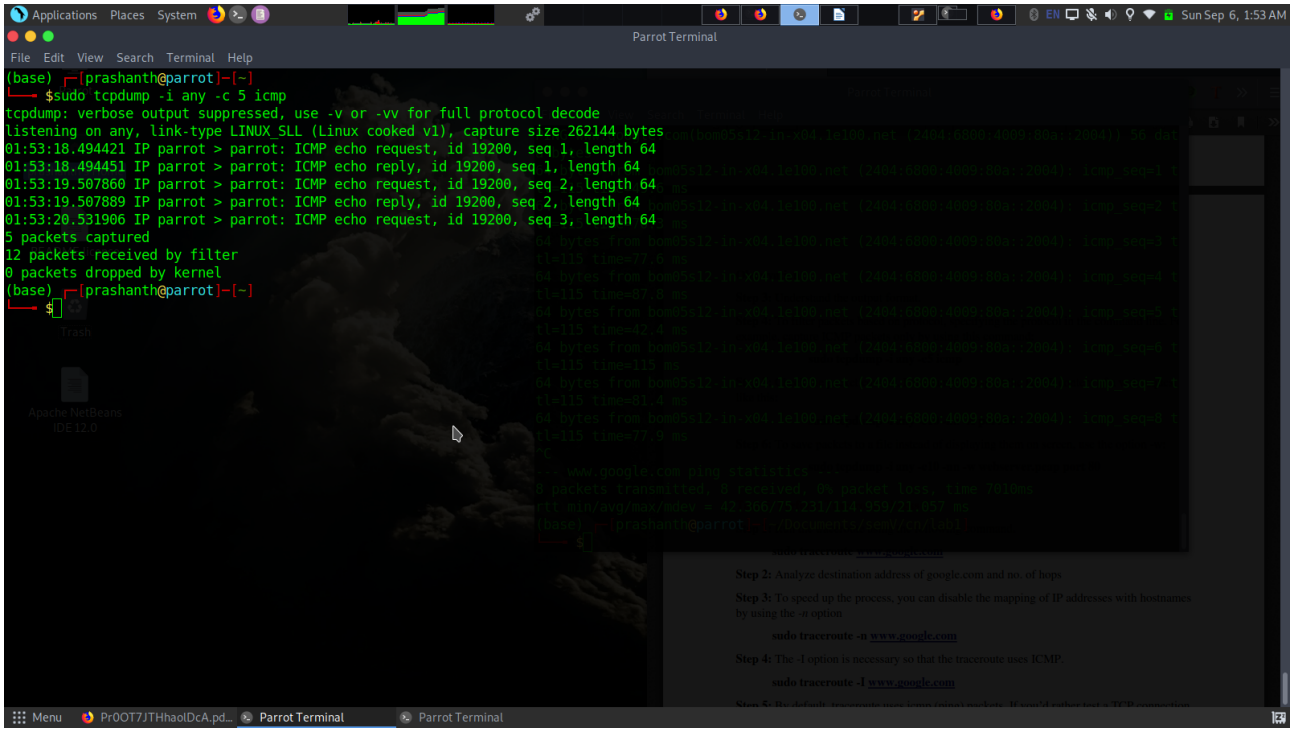
Using Wireshark’s Follow TCP Stream

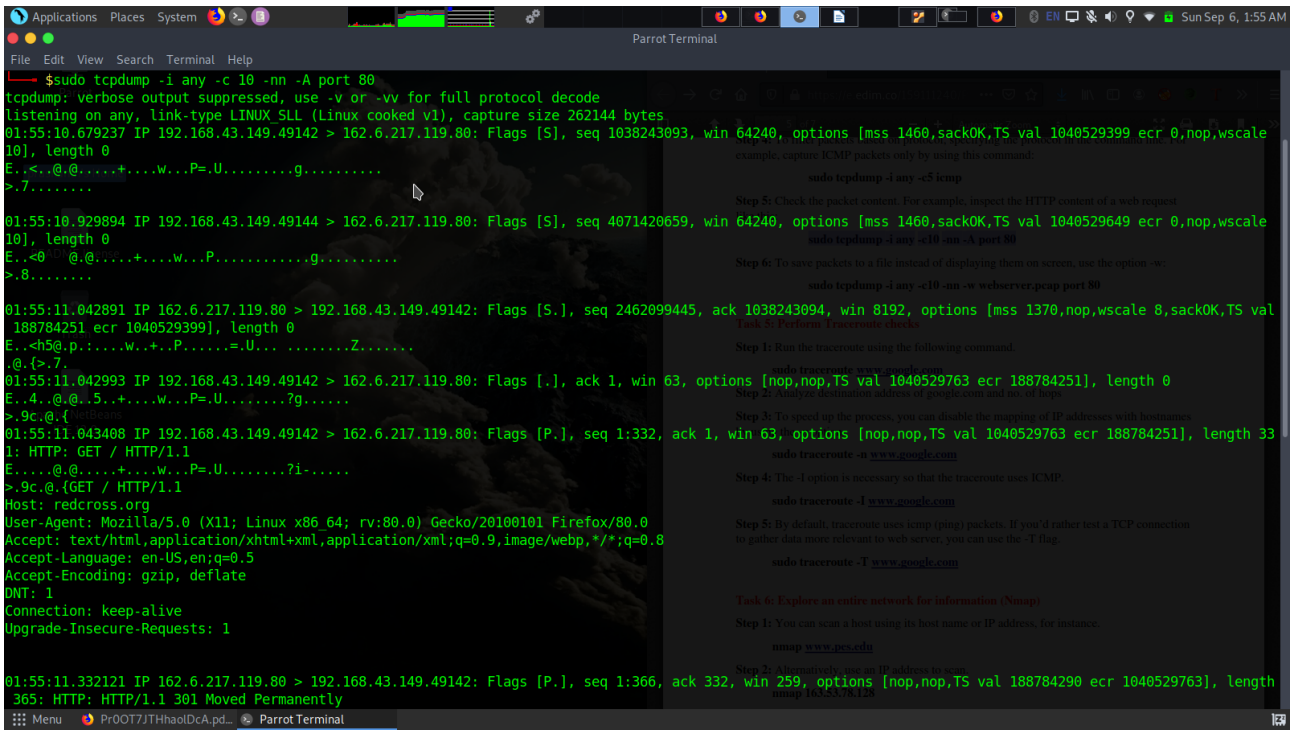


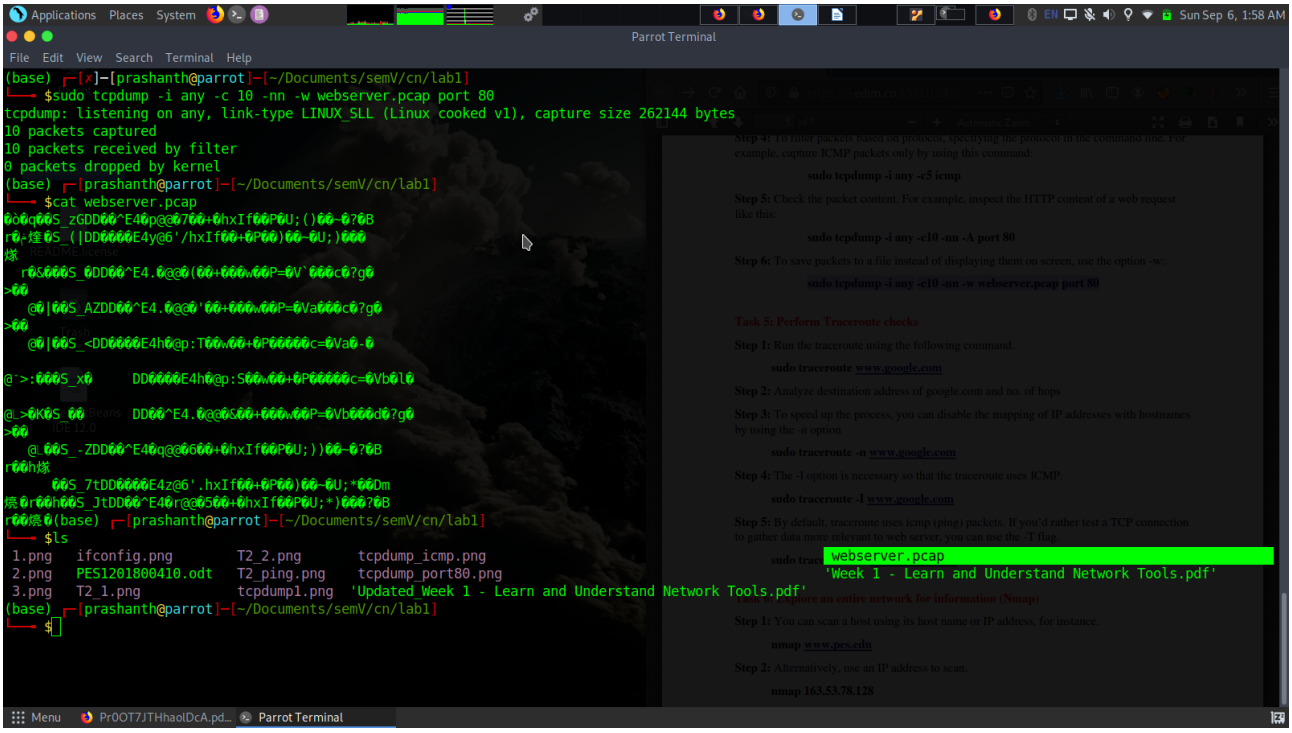
Task 4: Capturing packets with tcpdump



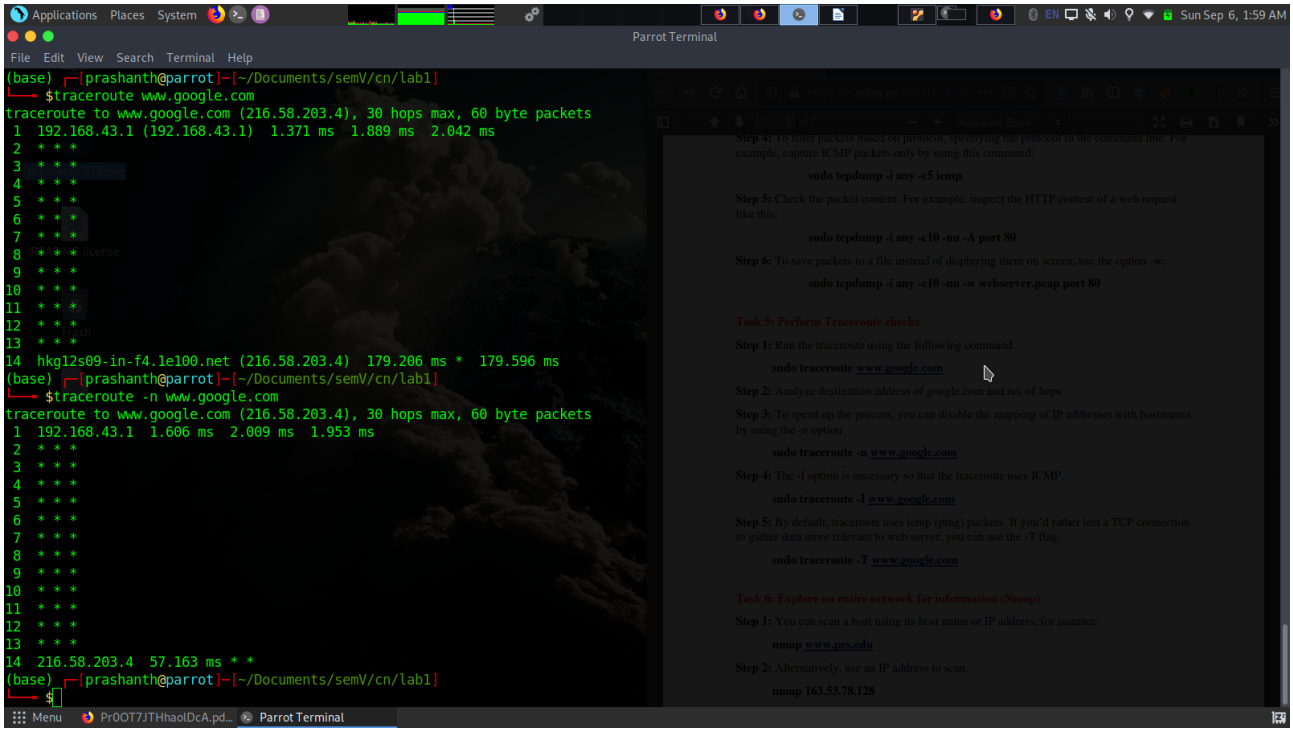
format:
timestamp , ipv4 or ipv6 , src ip.port > dst ip.port , tcp flags and respective infomations

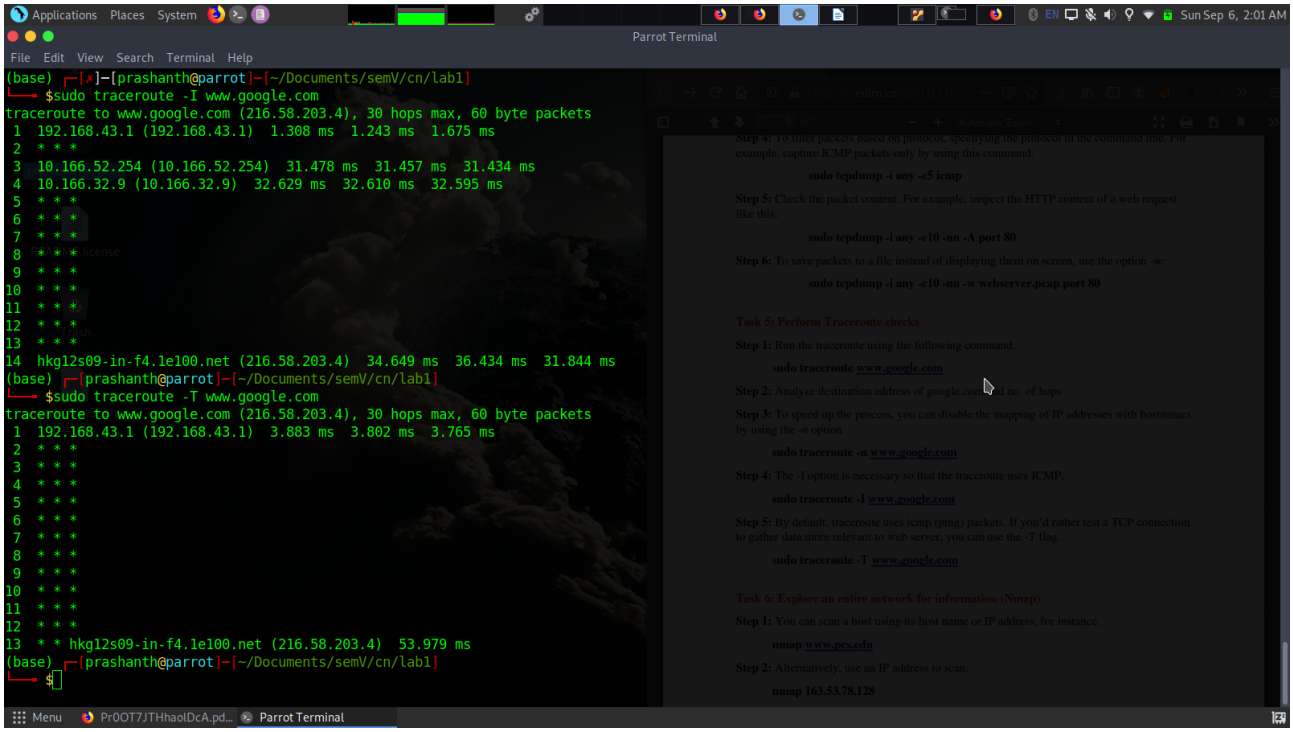



Applications Places System
Sun Sep 6, 1:55 AM
Parrot Terminal
File Edit View Search Terminal Help
$sudo tcpdump -i any -c 10 -nn -A port 80
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked v1), capture size 262144 bytes
01:55:10.679237 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..<..@.@.....+....w...P=.U.........g.........
>.7........
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 @.@.....+....w...P.............g.........
>.8........
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..<h5@.p.:....w..+..P......=.U... ....Z.......
.@.{>.7.
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..4..@.@..5..+....w...P=.U........?g......
>.9c.@.{
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 331: HTTP: GET / HTTP/1.1
E.....@.@.....+....w...P=.U........?i-.....
>.9c.@.{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
Menu
Parrot Terminal

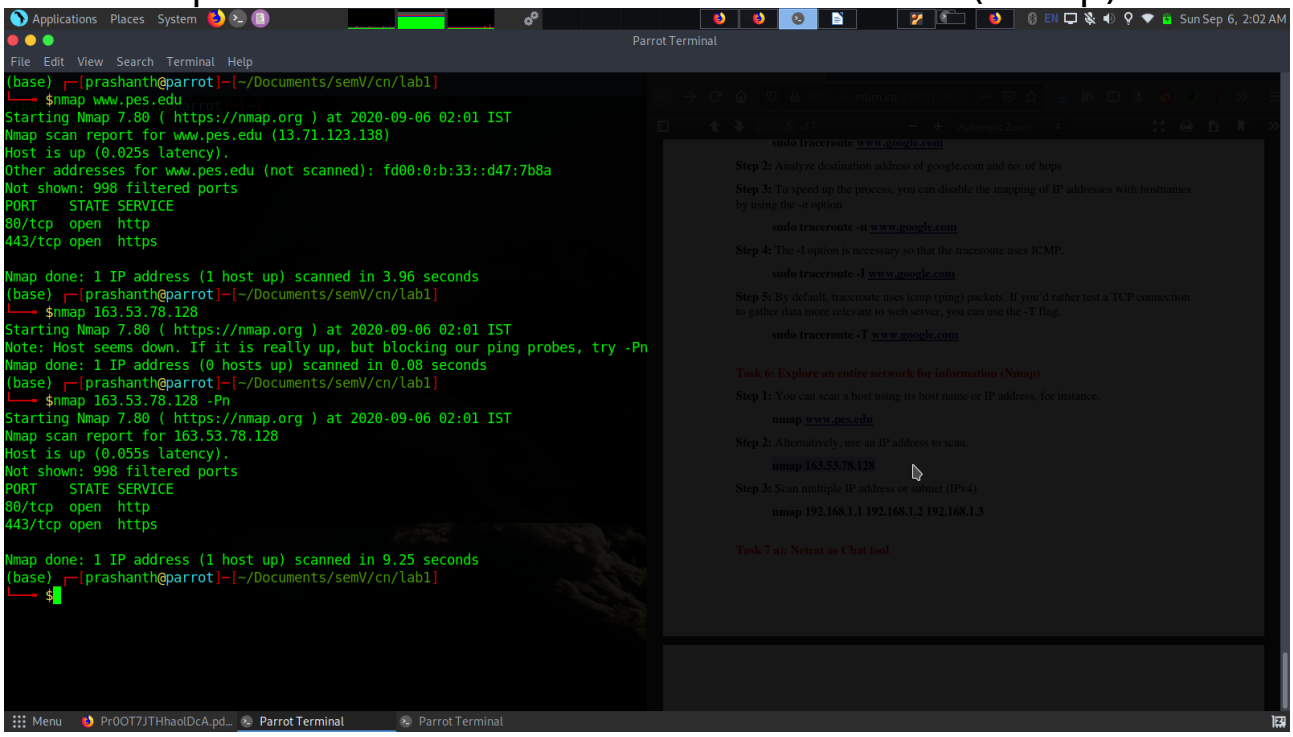

Applications Places System
Sun Sep 6, 1:58 AM
Parrot Terminal
File Edit View Search Terminal Help
(base) [prashanth@parrot]-[~/Documents/semV/cn/lab1]
$sudo tcpdump -i any -c 10 -nn -w webserver.pcap port 80
tcpdump: listening on any, link-type LINUX_SLL (Linux cooked v1), capture size 262144 bytes
10 packets captured
10 packets received by filter
0 packets dropped by kernel
(base) [prashanth@parrot]-[~/Documents/semV/cn/lab1]
$cat webserver.pcap
(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'
webserver.pcap
'Week 1 - Learn and Understand Network Tools.pdf'
(base) [prashanth@parrot]-[~/Documents/semV/cn/lab1]
Menu
Parrot Terminal

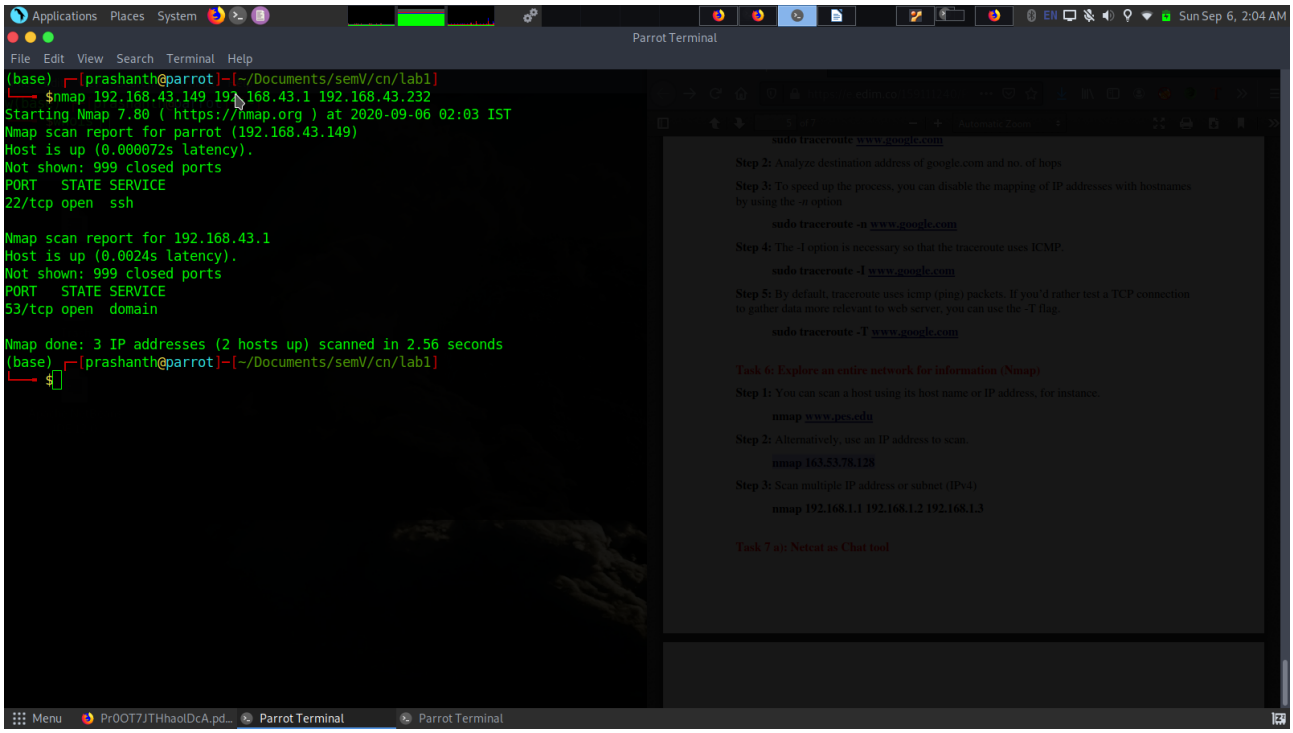
Task 5: Perform Traceroute checks





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





Questionson 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 ofECHO_REQUESTpackets?
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 perticular port (there are many different options -A is just one way to go)
eg $nmap www.pes.edu -O -A