Name: Khushei Meghana Meda

SRN: PES1201800416

Week number: 1

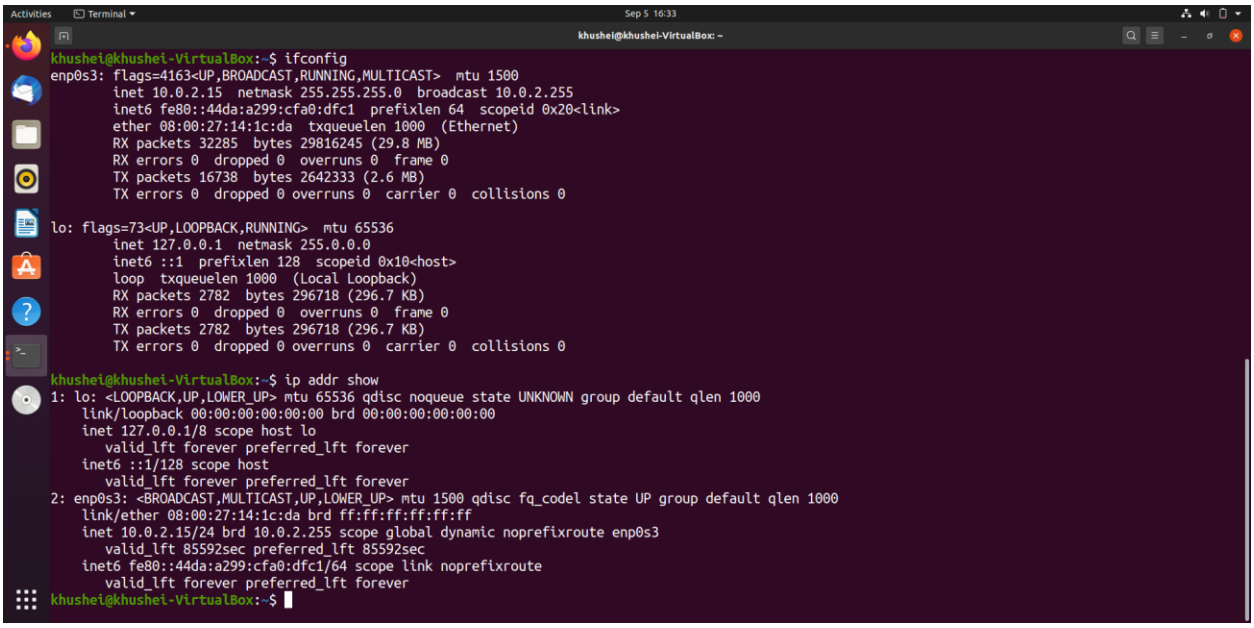
Name of experiment: Learn and Understand Network Tools

Date: 05-09-2020

Objectives of the experiment: Study and understand the basic networking tools - Wireshark, Tcpdump, Ping, Traceroute.

Task1: **Linux Interface Configuration (ifconfig / IP command)**

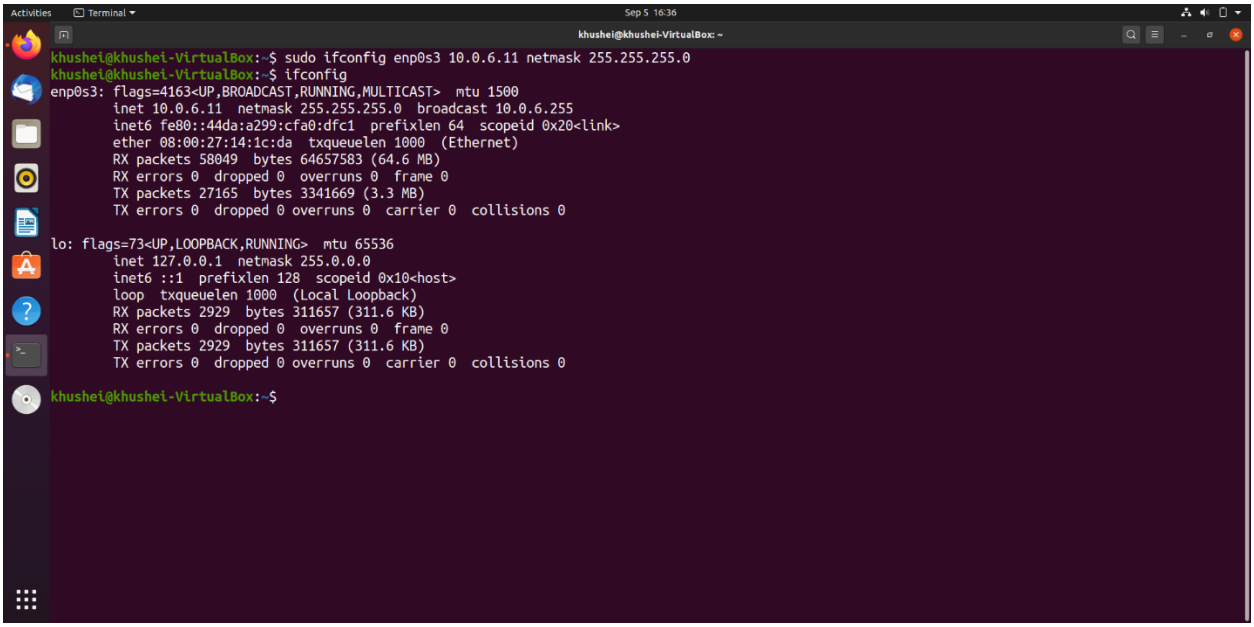
Step 1: To display status of all active network interfaces



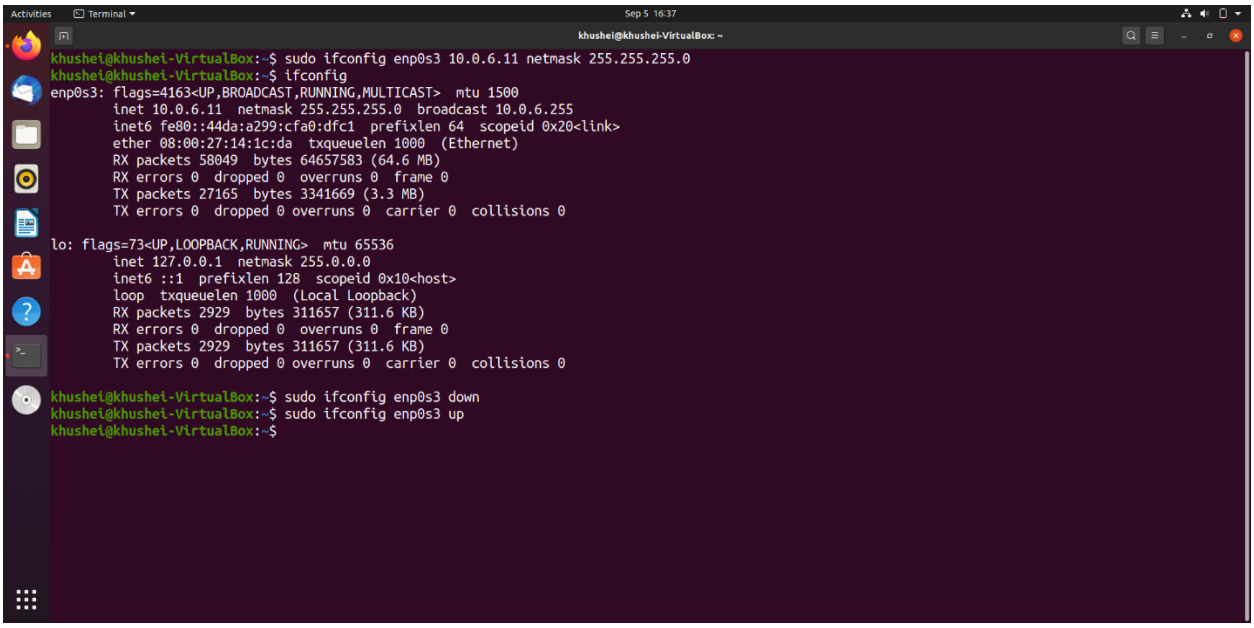
Interface Name	IP Address	MAC Address
lo	127.0.0.1	00:00:00:00:00:00
enp0s3	fe80::44da:a299:cfa0:dfc1	08:00:27:14:1c:da

Step 2: To assign an IP address to an interface, use the following command

Ifconfig is executed again to verify the changes have taken effect.

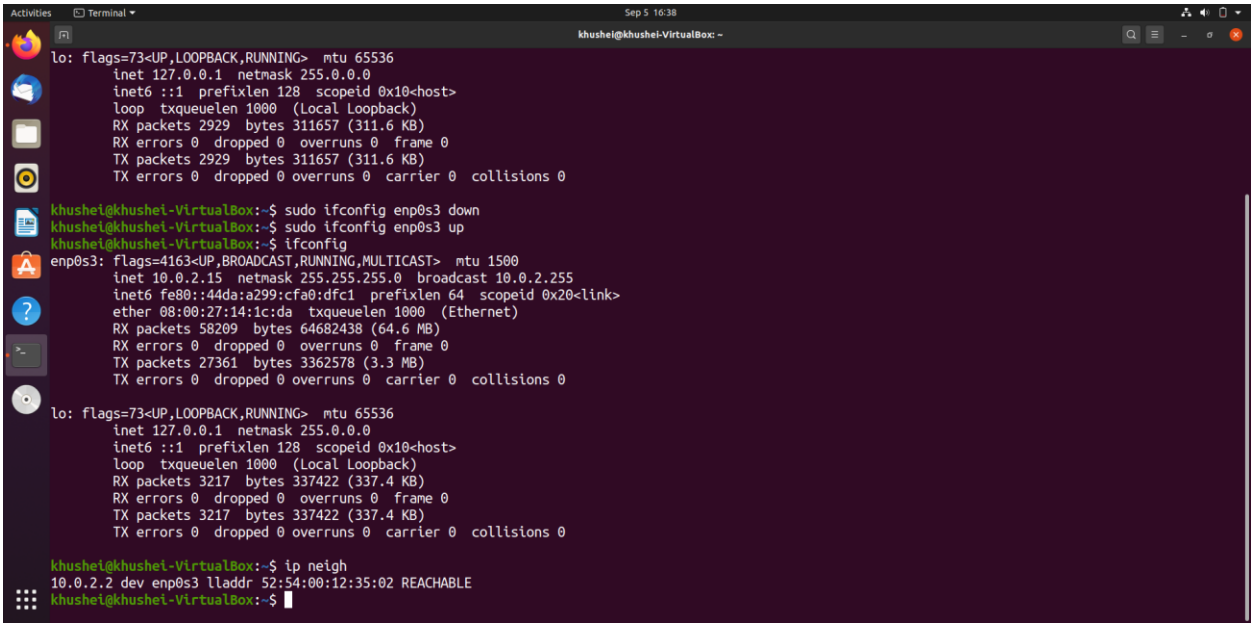


Step 3: To activate / deactivate a network interface, type.



Step 4: To show the current neighbor table in kernel, type

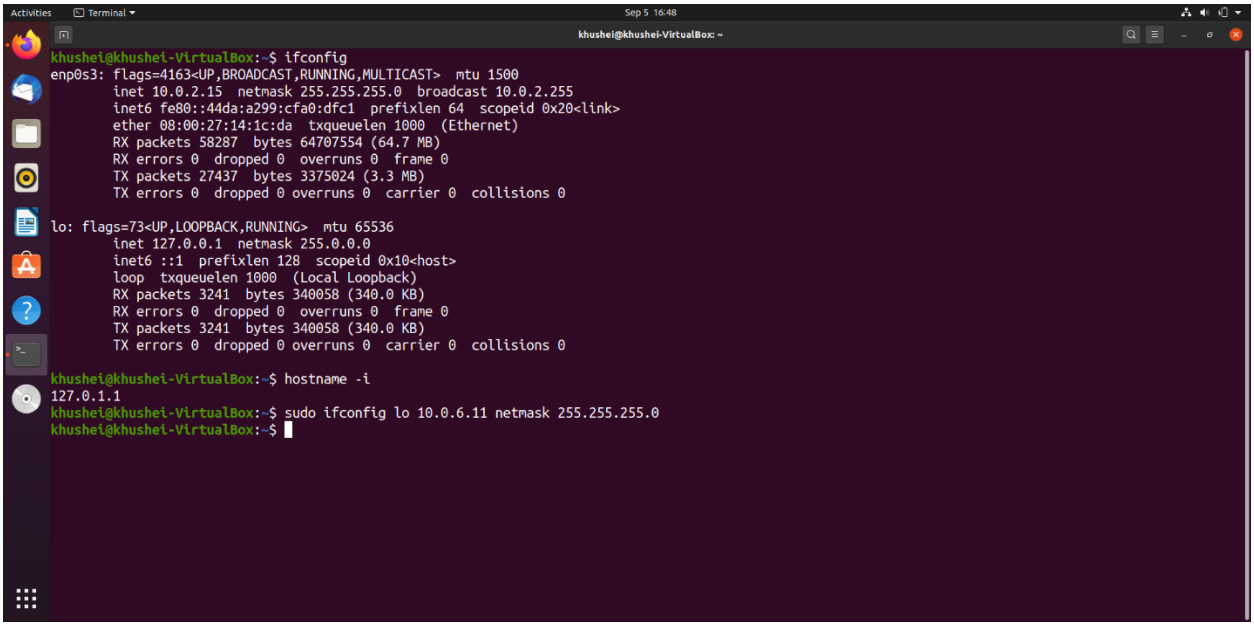
Before executing ip neigh, we execute ifconfig and see that it the IP address has gone back to the original 10.0.2.15 from 10.0.6.11 for enp0s3 interface. I have left it as it is so that ip neigh shows me the current neighbor table while I am connected to the internet. If the IP address were set manually through GUI in step 3, it would have persisted as 10.0.6.11 and in that case we would not get any output for ip neigh as it would not be connected to the internet.


Activities
Terminal
Sep 5 16:38
khushei@khushei-VirtualBox: ~
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 2929 bytes 311657 (311.6 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 2929 bytes 311657 (311.6 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
khushei@khushei-VirtualBox:~$ sudo ifconfig enp0s3 down
khushei@khushei-VirtualBox:~$ sudo ifconfig enp0s3 up
khushei@khushei-VirtualBox:~$ 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::44da:a299:cfa0:dfc1 prefixlen 64 scopeid 0x20<link>
ether 08:00:27:14:1c:da txqueuelen 1000 (Ethernet)
RX packets 58209 bytes 64682438 (64.6 MB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 27361 bytes 3362578 (3.3 MB)
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 3217 bytes 337422 (337.4 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 3217 bytes 337422 (337.4 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
khushei@khushei-VirtualBox:~$ ip neigh
10.0.2.2 dev enp0s3 lladdr 52:54:00:12:35:02 REACHABLE
khushei@khushei-VirtualBox:~$

Task 2: **Ping PDU (Packet Data Units or Packets) Capture**

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

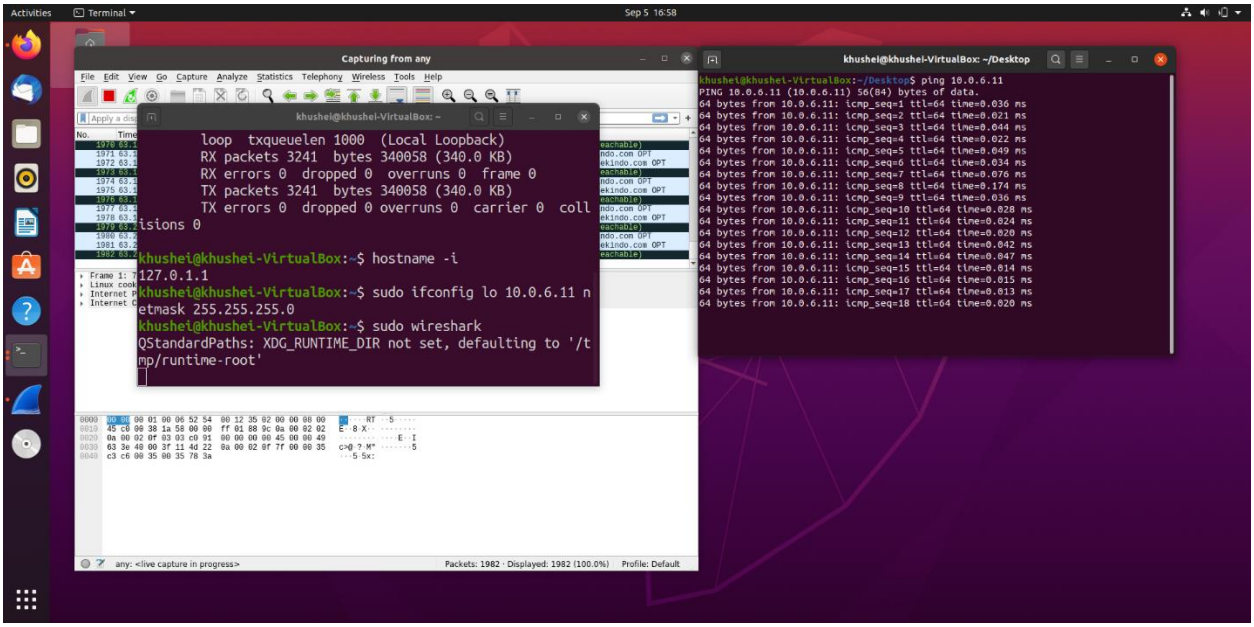
We start by checking the current ip address of the host by executing hostname -i command and find it to be 127.0.1.1. So I now change it to 10.0.6.11



Step 2: Launch Wireshark and select ‘any’ interface

Step 3: In terminal, type **ping 10.0.your_section.your_sno**

Launch wireshark with superuser privileges to find the ‘any’ interface option



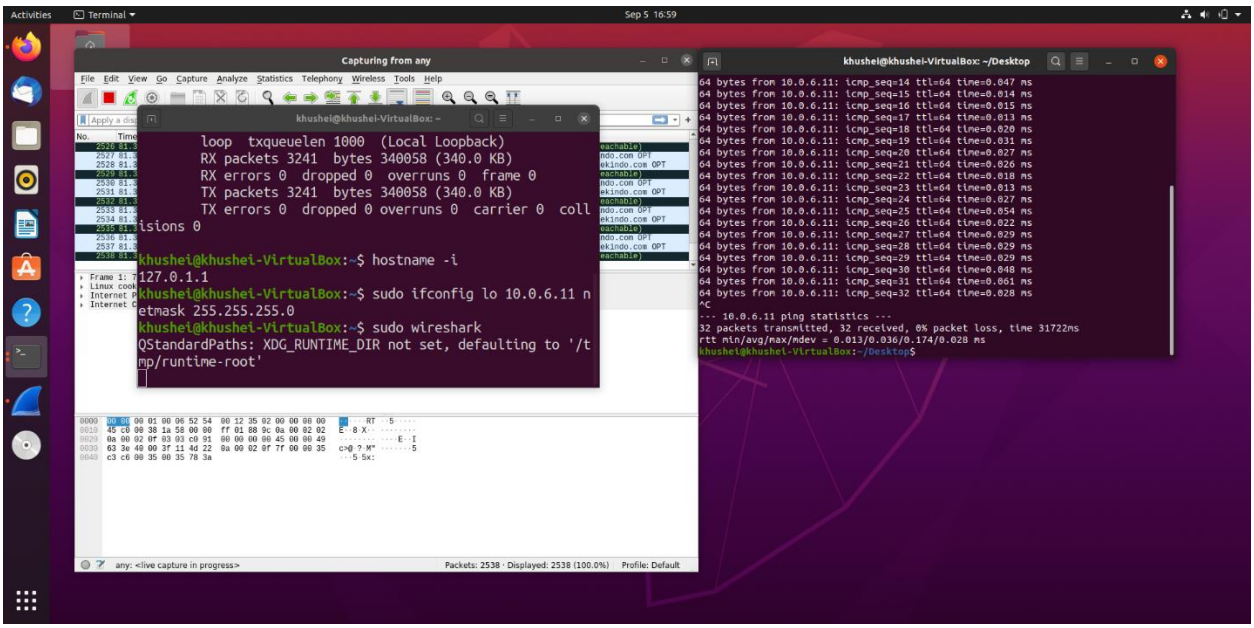
Step 4: Analyze the following in Terminal
• TTL • Protocol used by ping • Time

Observations:

TTL: 64

Protocol: ICMP

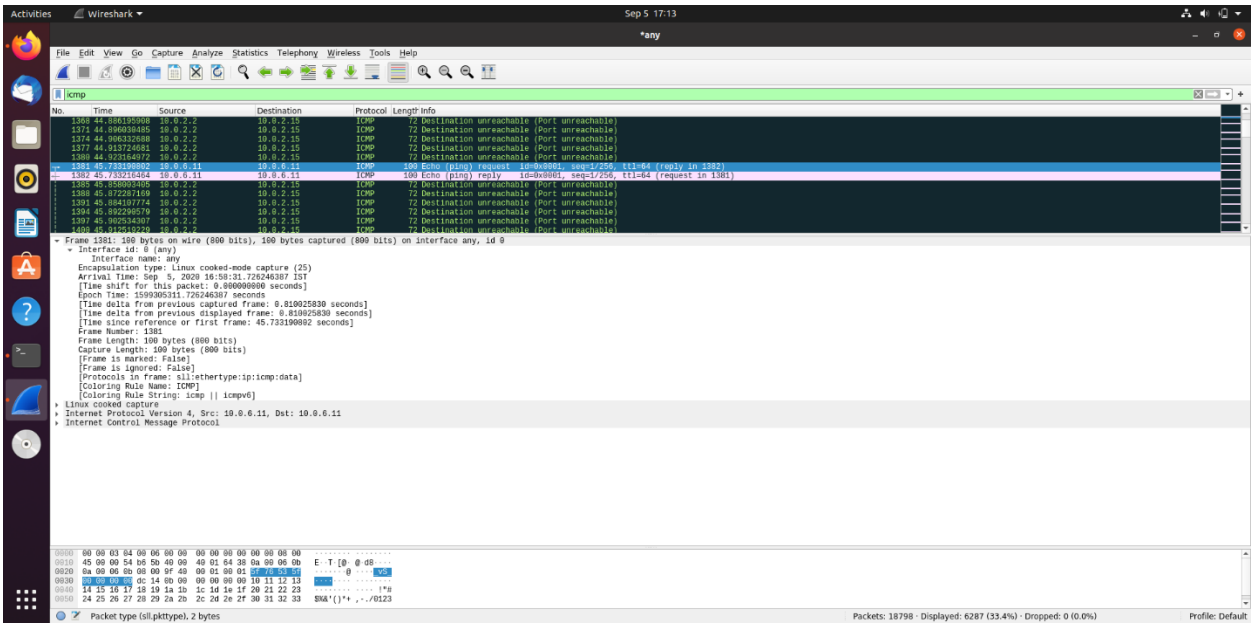
Time for transmission and reception of 32 packets: 31722 ms

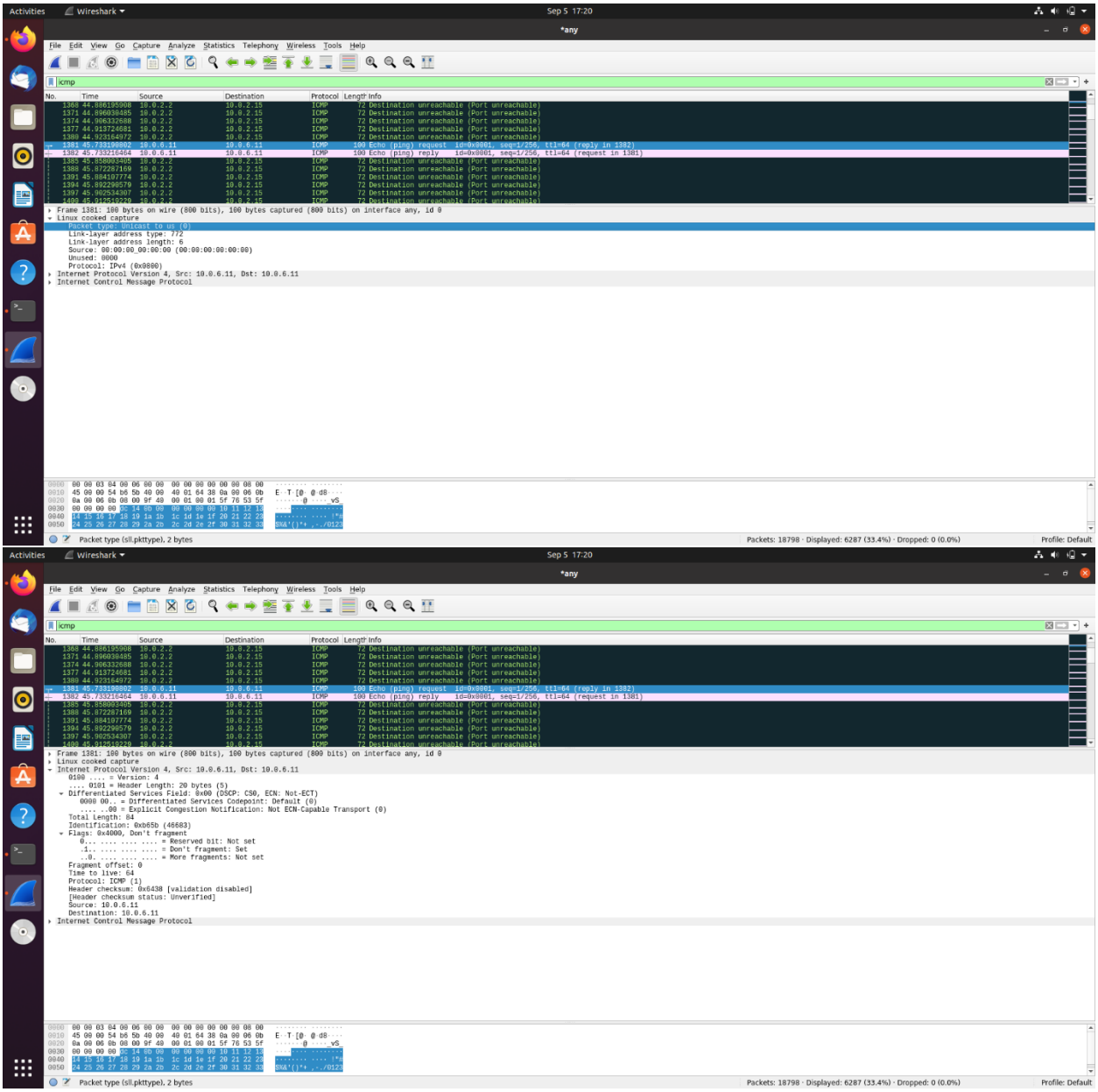


Step 5: Analyze the following in Wireshark

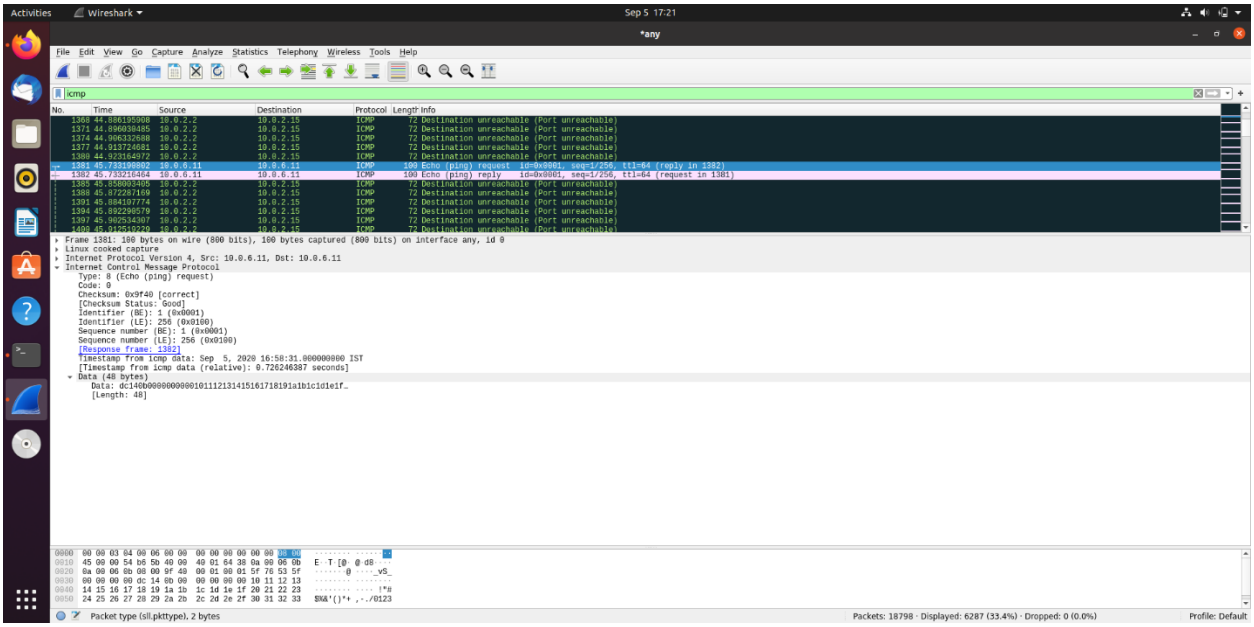
	First Echo Request	First Echo Reply
Frame Number	1381	1382
Source IP address	10.0.6.11	10.0.6.11
Destination IP address	10.0.6.11	10.0.6.11
ICMP Type Value	8	0
ICMP Code Value	0	0
Source Ethernet Address	00:00:00_00:00:00	00:00:00_00:00:00
Destination Ethernet Address	00:00:00_00:00:00	00:00:00_00:00:00
Internet Protocol Version	4	4
Time To Live (TTL) Value	64	64

First echo request (all the information has been expanded in the following screenshots):

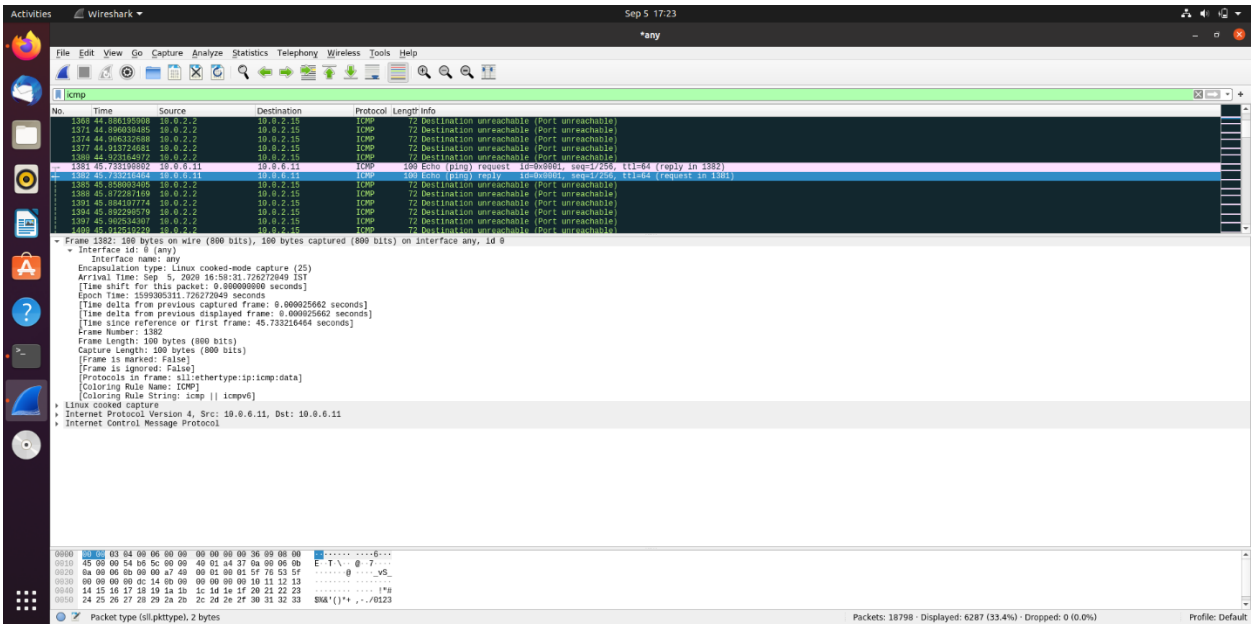


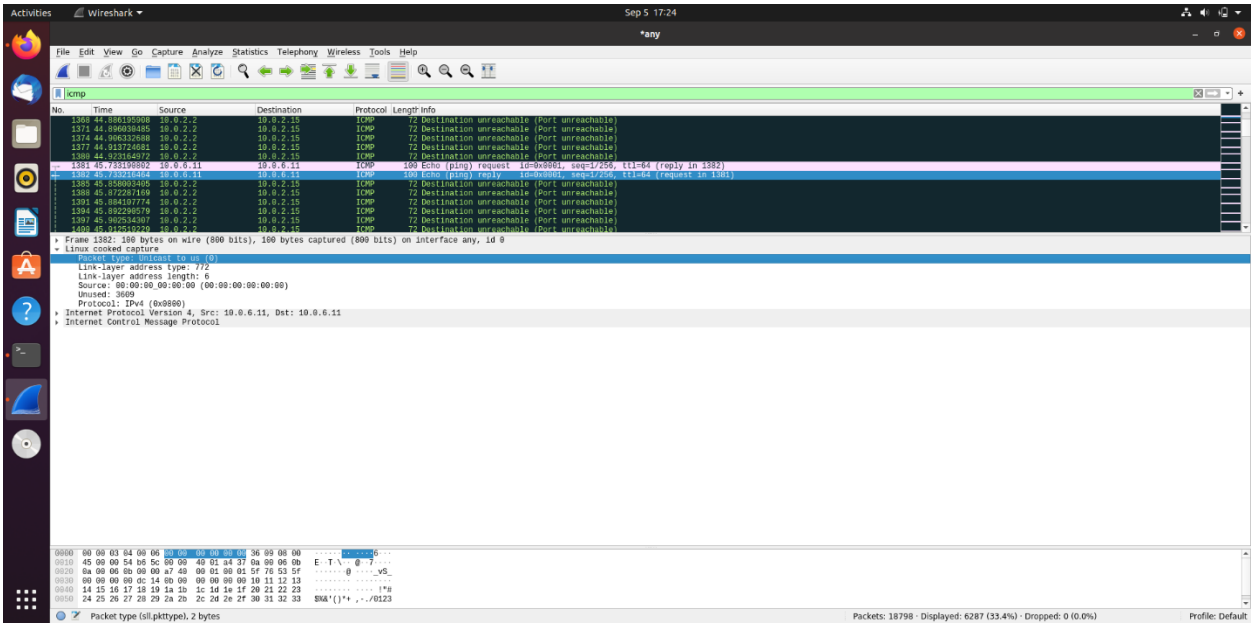

Activities
Wireshark
Sep 5 17:20
*any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
No. Time Source Destination Protocol Length Info
1368 44.886195908 10.0.2.2 10.0.2.15 ICMP 72 Destination unreachable (Port unreachable)
1371 44.896030485 10.0.2.2 10.0.2.15 ICMP 72 Destination unreachable (Port unreachable)
1374 44.906332688 10.0.2.2 10.0.2.15 ICMP 72 Destination unreachable (Port unreachable)
1377 44.913724681 10.0.2.2 10.0.2.15 ICMP 72 Destination unreachable (Port unreachable)
1380 44.923164972 10.0.2.2 10.0.2.15 ICMP 72 Destination unreachable (Port unreachable)
1381 45.733190802 10.0.6.11 10.0.6.11 ICMP 100 Echo (ping) request id=0x0001, seq=1/256, ttl=64 (reply in 1382)
1382 45.733216464 10.0.6.11 10.0.6.11 ICMP 100 Echo (ping) reply id=0x0001, seq=1/256, ttl=64 (request in 1381)
1385 45.858093465 10.0.2.2 10.0.2.15 ICMP 72 Destination unreachable (Port unreachable)
1388 45.872287169 10.0.2.2 10.0.2.15 ICMP 72 Destination unreachable (Port unreachable)
1391 45.884197774 10.0.2.2 10.0.2.15 ICMP 72 Destination unreachable (Port unreachable)
1394 45.892290579 10.0.2.2 10.0.2.15 ICMP 72 Destination unreachable (Port unreachable)
1397 45.902534307 10.0.2.2 10.0.2.15 ICMP 72 Destination unreachable (Port unreachable)
1400 45.913554220 10.0.2.2 10.0.2.15 ICMP 72 Destination unreachable (Port unreachable)
Frame 1381: 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: 10.0.6.11, Dst: 10.0.6.11
Internet Control Message Protocol
Packet type (sll.pkttype), 2 bytes
Packets: 18798 · Displayed: 6287 (33.4%) · Dropped: 0 (0.0%)
Profile: Default

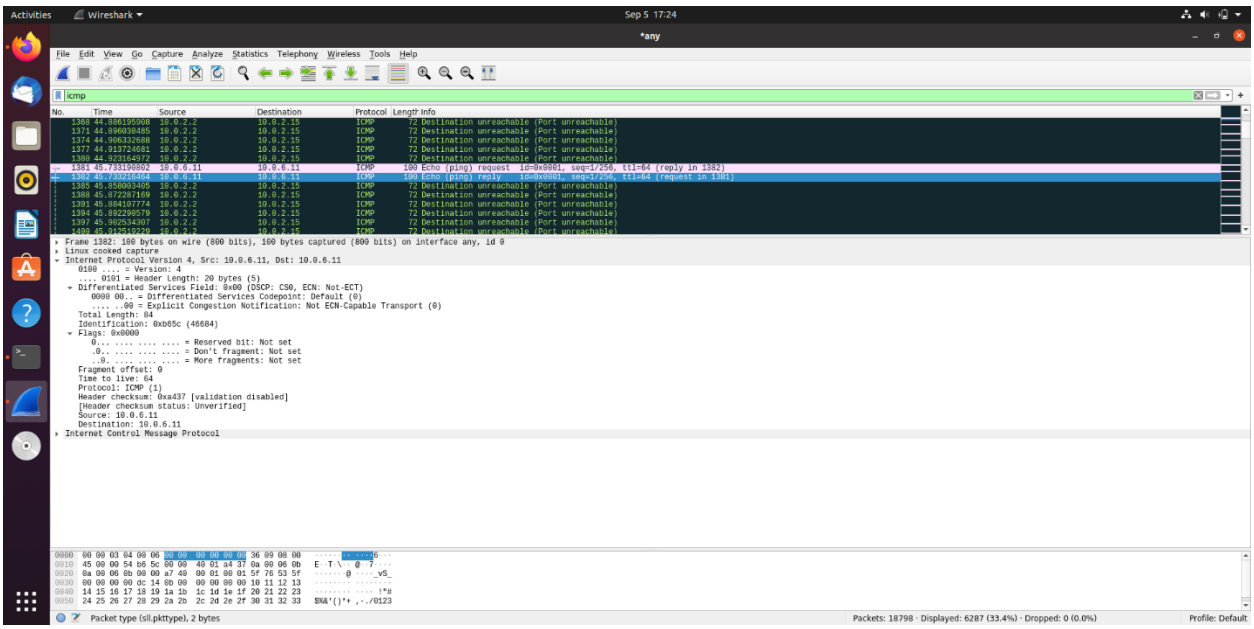
Activities
Wireshark
Sep 5 17:20
*any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
No. Time Source Destination Protocol Length Info
1368 44.886195908 10.0.2.2 10.0.2.15 ICMP 72 Destination unreachable (Port unreachable)
1371 44.896030485 10.0.2.2 10.0.2.15 ICMP 72 Destination unreachable (Port unreachable)
1374 44.906332688 10.0.2.2 10.0.2.15 ICMP 72 Destination unreachable (Port unreachable)
1377 44.913724681 10.0.2.2 10.0.2.15 ICMP 72 Destination unreachable (Port unreachable)
1380 44.923164972 10.0.2.2 10.0.2.15 ICMP 72 Destination unreachable (Port unreachable)
1381 45.733190802 10.0.6.11 10.0.6.11 ICMP 100 Echo (ping) request id=0x0001, seq=1/256, ttl=64 (reply in 1382)
1382 45.733216464 10.0.6.11 10.0.6.11 ICMP 100 Echo (ping) reply id=0x0001, seq=1/256, ttl=64 (request in 1381)
1385 45.858093465 10.0.2.2 10.0.2.15 ICMP 72 Destination unreachable (Port unreachable)
1388 45.872287169 10.0.2.2 10.0.2.15 ICMP 72 Destination unreachable (Port unreachable)
1391 45.884197774 10.0.2.2 10.0.2.15 ICMP 72 Destination unreachable (Port unreachable)
1394 45.892290579 10.0.2.2 10.0.2.15 ICMP 72 Destination unreachable (Port unreachable)
1397 45.902534307 10.0.2.2 10.0.2.15 ICMP 72 Destination unreachable (Port unreachable)
1400 45.913554220 10.0.2.2 10.0.2.15 ICMP 72 Destination unreachable (Port unreachable)
Frame 1381: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface any, id 0
Linux cooked capture
Internet Protocol Version 4, Src: 10.0.6.11, Dst: 10.0.6.11
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 84
Identification: 0xb65b (46683)
Flags: 0x4000, Don't fragment
0... .... = Reserved bit: Not set
.1.. .... = Don't fragment: Set
..0. .... = More fragments: Not set
Fragment offset: 0
Time to live: 64
Protocol: ICMP (1)
Header checksum: 0x6438 [validation disabled]
[Header checksum status: Unverified]
Source: 10.0.6.11
Destination: 10.0.6.11
Internet Control Message Protocol
Packet type (sll.pkttype), 2 bytes
Packets: 18798 · Displayed: 6287 (33.4%) · Dropped: 0 (0.0%)
Profile: Default

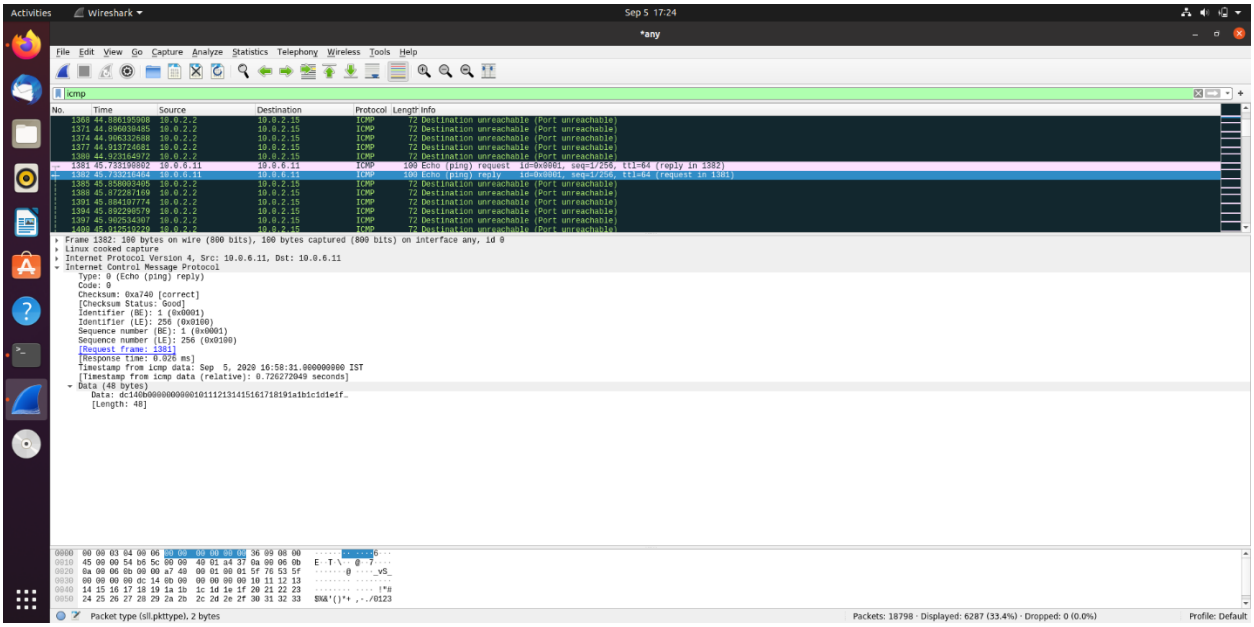


First echo response (all the information has been expanded in the following screenshots):




Activities
Wireshark
Sep 5 17:24
*any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
No. Time Source Destination Protocol Length Info
1368 44.886195908 10.0.2.2 10.0.2.15 ICMP 72 Destination unreachable (Port unreachable)
1371 44.896030485 10.0.2.2 10.0.2.15 ICMP 72 Destination unreachable (Port unreachable)
1374 44.906332688 10.0.2.2 10.0.2.15 ICMP 72 Destination unreachable (Port unreachable)
1377 44.913724681 10.0.2.2 10.0.2.15 ICMP 72 Destination unreachable (Port unreachable)
1380 44.923164972 10.0.2.2 10.0.2.15 ICMP 72 Destination unreachable (Port unreachable)
1381 45.733190002 10.0.6.11 10.0.6.11 ICMP 100 Echo (ping) request id=0x0001, seq=1/256, ttl=64 (reply in 1382)
1382 45.733215464 10.0.6.11 10.0.6.11 ICMP 100 Echo (ping) reply id=0x0001, seq=1/256, ttl=64 (request in 1381)
1385 45.858003405 10.0.2.2 10.0.2.15 ICMP 72 Destination unreachable (Port unreachable)
1388 45.872267169 10.0.2.2 10.0.2.15 ICMP 72 Destination unreachable (Port unreachable)
1391 45.884107774 10.0.2.2 10.0.2.15 ICMP 72 Destination unreachable (Port unreachable)
1394 45.892290579 10.0.2.2 10.0.2.15 ICMP 72 Destination unreachable (Port unreachable)
1397 45.902534307 10.0.2.2 10.0.2.15 ICMP 72 Destination unreachable (Port unreachable)
1400 45.912510229 10.0.2.2 10.0.2.15 ICMP 72 Destination unreachable (Port unreachable)
Frame 1382: 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: 3609
Protocol: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.0.6.11, Dst: 10.0.6.11
Internet Control Message Protocol
0000 00 00 03 04 00 06 00 00 00 00 00 00 36 09 08 00 ····· ····· 6···
0010 45 00 00 54 b6 5c 00 00 40 01 a4 37 0a 00 06 0b E··T·\·· @··7····
0020 0a 00 06 0b 00 00 a7 48 00 01 00 01 5f 76 53 5f ····· H ····_vS_
0030 00 00 00 00 dc 14 0b 00 00 00 00 00 10 11 12 13 ····· ····· ·····
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
Packet type (sll.pkttype), 2 bytes
Packets: 18798 · Displayed: 6287 (33.4%) · Dropped: 0 (0.0%)
Profile: Default

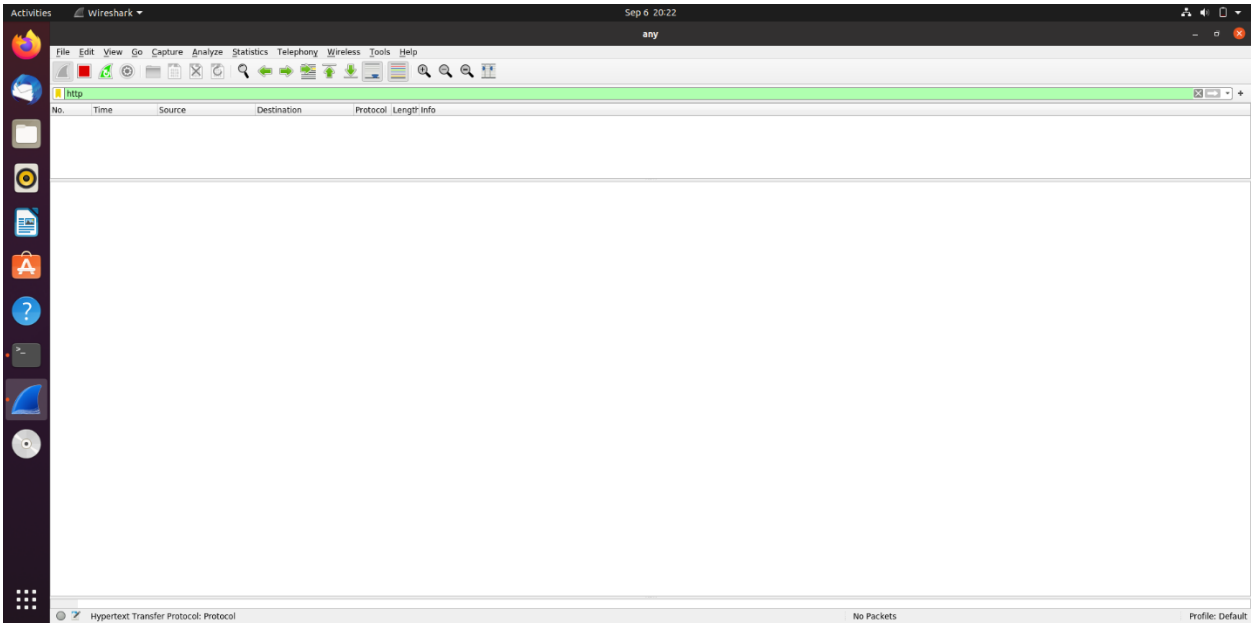

Activities
Wireshark
Sep 5 17:24
*any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
No. Time Source Destination Protocol Length Info
1368 44.886195908 10.0.2.2 10.0.2.15 ICMP 72 Destination unreachable (Port unreachable)
1371 44.896030485 10.0.2.2 10.0.2.15 ICMP 72 Destination unreachable (Port unreachable)
1374 44.906332688 10.0.2.2 10.0.2.15 ICMP 72 Destination unreachable (Port unreachable)
1377 44.913724681 10.0.2.2 10.0.2.15 ICMP 72 Destination unreachable (Port unreachable)
1380 44.923164972 10.0.2.2 10.0.2.15 ICMP 72 Destination unreachable (Port unreachable)
1381 45.733190002 10.0.6.11 10.0.6.11 ICMP 100 Echo (ping) request id=0x0001, seq=1/256, ttl=64 (reply in 1382)
1382 45.733215464 10.0.6.11 10.0.6.11 ICMP 100 Echo (ping) reply id=0x0001, seq=1/256, ttl=64 (request in 1381)
1385 45.858003405 10.0.2.2 10.0.2.15 ICMP 72 Destination unreachable (Port unreachable)
1388 45.872267169 10.0.2.2 10.0.2.15 ICMP 72 Destination unreachable (Port unreachable)
1391 45.884107774 10.0.2.2 10.0.2.15 ICMP 72 Destination unreachable (Port unreachable)
1394 45.892290579 10.0.2.2 10.0.2.15 ICMP 72 Destination unreachable (Port unreachable)
1397 45.902534307 10.0.2.2 10.0.2.15 ICMP 72 Destination unreachable (Port unreachable)
1400 45.912510229 10.0.2.2 10.0.2.15 ICMP 72 Destination unreachable (Port unreachable)
Frame 1382: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface any, id 0
Linux cooked capture
Internet Protocol Version 4, Src: 10.0.6.11, Dst: 10.0.6.11
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 84
Identification: 0xb65c (46684)
Flags: 0x0000
0... .... = Reserved bit: Not set
.0.. .... = Don't fragment: Not set
..0. .... = More fragments: Not set
Fragment offset: 0
Time to live: 64
Protocol: ICMP (1)
Header checksum: 0xa437 [validation disabled]
[Header checksum status: Unverified]
Source: 10.0.6.11
Destination: 10.0.6.11
Internet Control Message Protocol
0000 00 00 03 04 00 06 00 00 00 00 00 00 36 09 08 00 ····· ····· 6···
0010 45 00 00 54 b6 5c 00 00 40 01 a4 37 0a 00 06 0b E··T·\·· @··7····
0020 0a 00 06 0b 00 00 a7 48 00 01 00 01 5f 76 53 5f ····· H ····_vS_
0030 00 00 00 00 dc 14 0b 00 00 00 00 00 10 11 12 13 ····· ····· ·····
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
Packet type (sll.pkttype), 2 bytes
Packets: 18798 · Displayed: 6287 (33.4%) · Dropped: 0 (0.0%)
Profile: Default


Activities
Wireshark
Sep 5 17:24
*any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
No. Time Source Destination Protocol Length Info
1368 44.896195908 10.0.2.2 10.0.2.15 ICMP 72 Destination unreachable (Port unreachable)
1371 44.896030485 10.0.2.2 10.0.2.15 ICMP 72 Destination unreachable (Port unreachable)
1374 44.906332688 10.0.2.2 10.0.2.15 ICMP 72 Destination unreachable (Port unreachable)
1377 44.913724681 10.0.2.2 10.0.2.15 ICMP 72 Destination unreachable (Port unreachable)
1380 44.923164972 10.0.2.2 10.0.2.15 ICMP 72 Destination unreachable (Port unreachable)
1381 45.733190002 10.0.6.11 10.0.6.11 ICMP 100 Echo (ping) request id=0x0001, seq=1/256, ttl=64 (reply in 1382)
1382 45.733218161 10.0.6.11 10.0.6.11 ICMP 100 Echo (ping) reply id=0x0001, seq=1/256, ttl=64 (request in 1381)
1385 45.858003405 10.0.2.2 10.0.2.15 ICMP 72 Destination unreachable (Port unreachable)
1388 45.872287169 10.0.2.2 10.0.2.15 ICMP 72 Destination unreachable (Port unreachable)
1391 45.884107774 10.0.2.2 10.0.2.15 ICMP 72 Destination unreachable (Port unreachable)
1394 45.892290579 10.0.2.2 10.0.2.15 ICMP 72 Destination unreachable (Port unreachable)
1397 45.902534307 10.0.2.2 10.0.2.15 ICMP 72 Destination unreachable (Port unreachable)
1400 45.910554220 10.0.2.2 10.0.2.15 ICMP 72 Destination unreachable (Port unreachable)
Frame 1382: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface any, id 0
Linux cooked capture
Internet Protocol Version 4, Src: 10.0.6.11, Dst: 10.0.6.11
Internet Control Message Protocol
Type: 0 (Echo (ping) reply)
Code: 0
Checksum: 0xa740 [correct]
[Checksum Status: Good]
Identifier (BE): 1 (0x0001)
Identifier (LE): 256 (0x0100)
Sequence number (BE): 1 (0x0001)
Sequence number (LE): 256 (0x0100)
[Request frame: 1381]
[Response time: 0.028 ms]
[Timestamp from icmp data: Sep 5, 2020 16:58:31.000000000 IST]
[Timestamp from icmp data (relative): 0.726272049 seconds]
Data (48 bytes)
Data: dc140b0000000000101112131415161718191a1b1c1d1e1f…
[Length: 48]
0000 00 00 03 04 00 06 00 00 00 00 00 00 36 09 08 00 ····· ····· ····6···
0010 45 00 00 54 b6 5c 00 00 40 01 a4 37 0a 00 06 0b E··T·\·· @··7····
0020 0a 00 06 0b 00 00 a7 40 00 01 00 01 5f 76 53 5f ····· ····@ ····_vS_
0030 00 00 00 00 dc 14 0b 00 00 00 00 00 10 11 12 13 ····· ····· ····· ····
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
Packet type (sll.pkttype), 2 bytes
Packets: 18798 · Displayed: 6287 (33.4%) · Dropped: 0 (0.0%)
Profile: Default

Task 3: HTTP PDU Capture

Using Wireshark's Filter feature

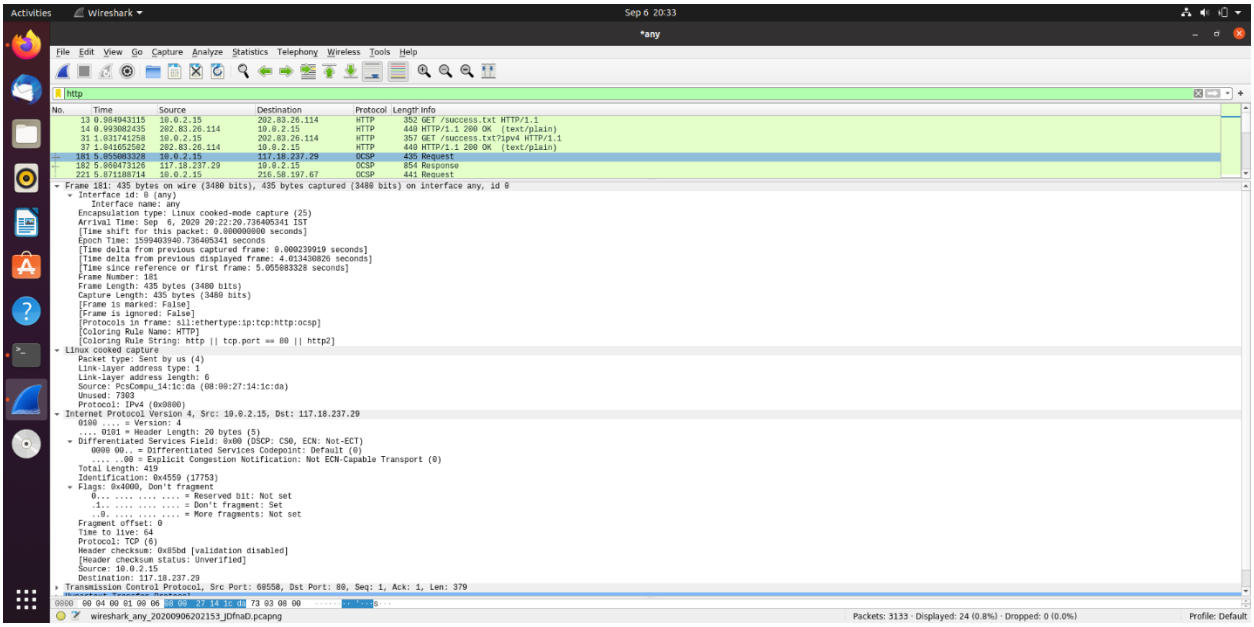
Step 1: Launch Wireshark and select 'any' interface. On the Filter toolbar, type-in 'http' and press enter

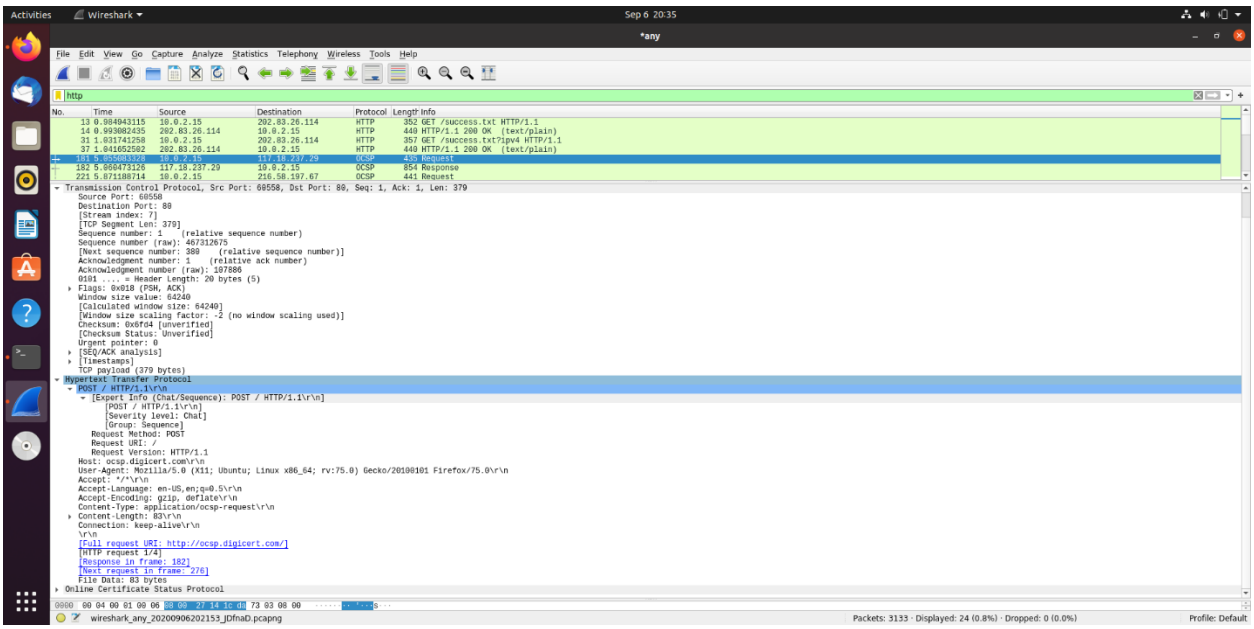


Step 2: Open Firefox browser, and browse www.nyu.edu

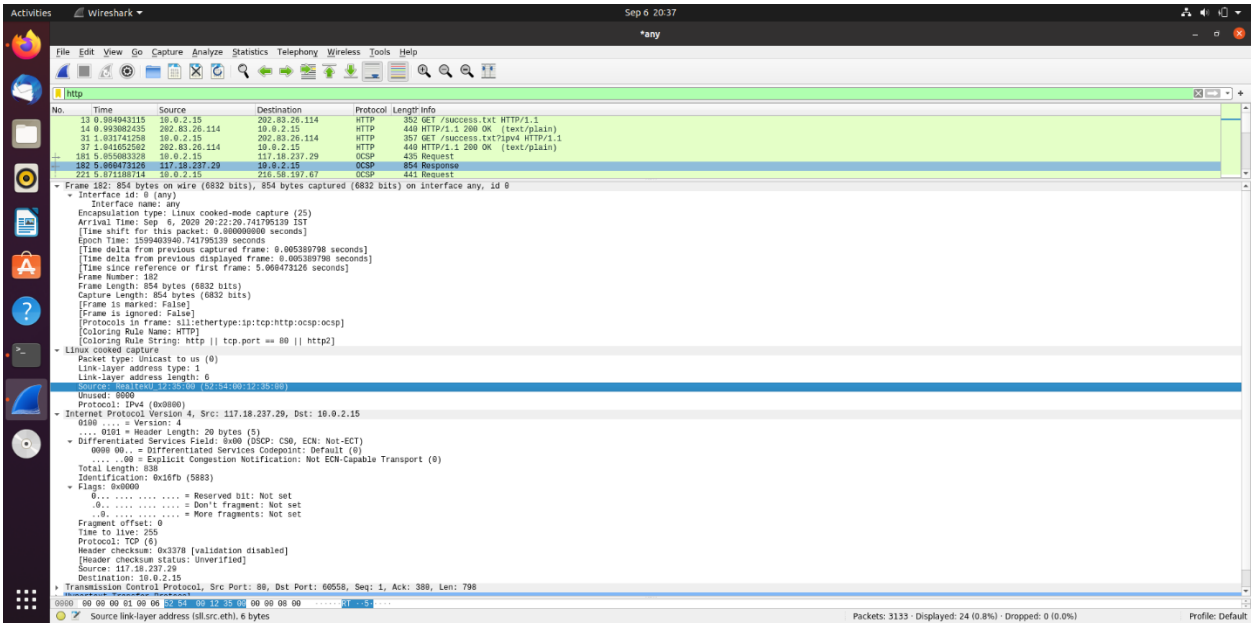
Details	First Echo Request	First Echo Reply
Frame Number	181	182
Source Port	60558	80
Destination Port	80	60558
Source IP address	10.0.2.15	117.18.237.29
Destination IP address	117.18.237.29	10.0.2.15
Source Ethernet Address	08:00:27:14:1c:da	52:54:00:12:35:00
Destination Ethernet Address	52:54:00:12:35:00	08:00:27:14:1c:da

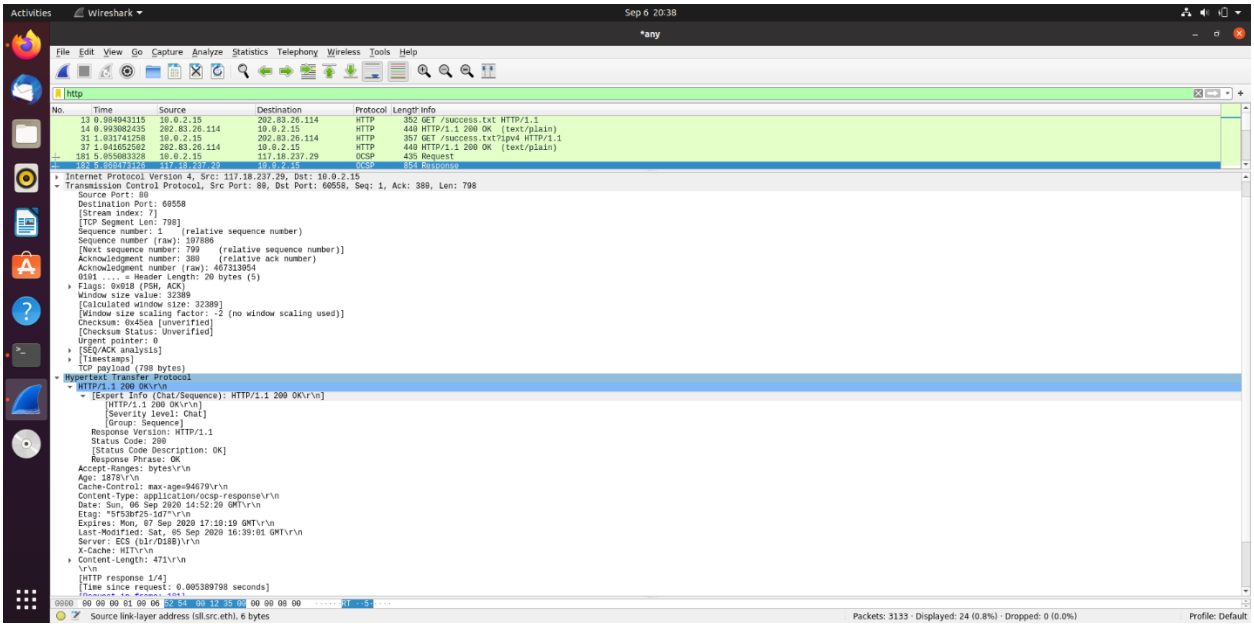
First echo request (the required information has been expanded in the following screenshots):





First echo response (the required information has been expanded in the following screenshots):



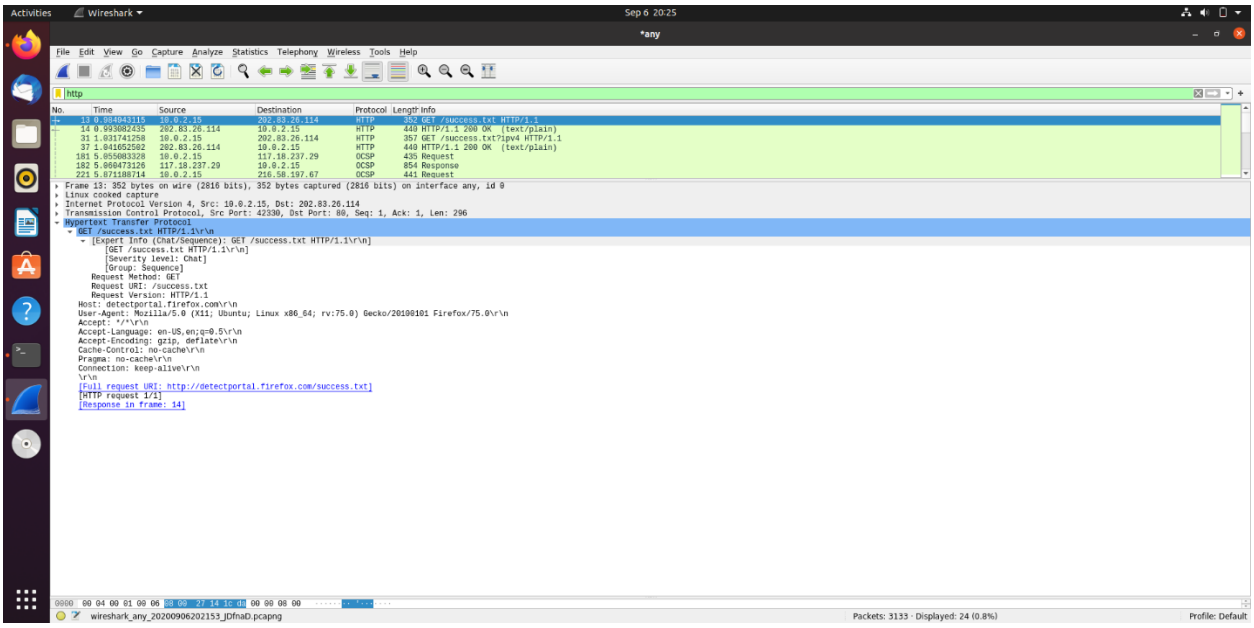


Step 4: Analyze the HTTP request and response and complete the table below.

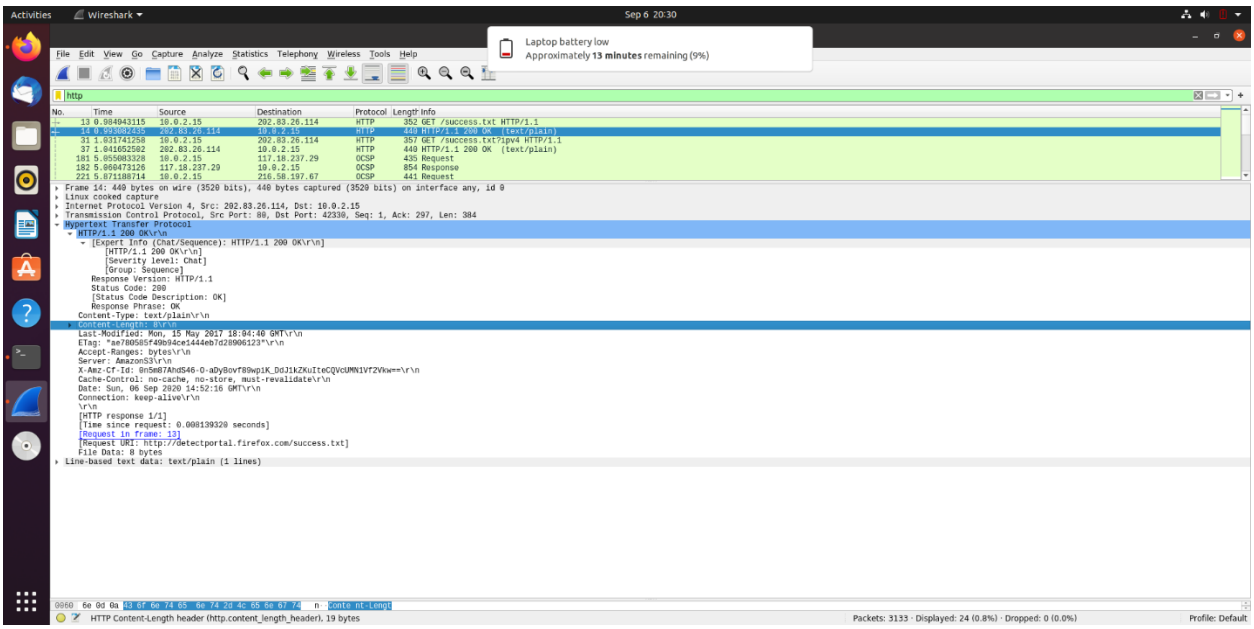
HTTP Request		**HTTP Response**	
Get	GET /success.txt HTTP/1.1\r\n	Server	AmazonS3
Host	detectportal.firefox.com\r\n	Content-Type	text/plain
User-Agent	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:75.0) Gecko/20100101 Firefox/75.0	Date	Sun, 06 Sep 2020 14:52:16 GMT

Accept-Language	en-US,en;q=0.5	Location	*N/A*
Accept-Encoding	gzip, deflate	Content-Length	8\r\n
Connection	keep-alive\r\n	Connection	keep-alive\r\n

HTTP request:



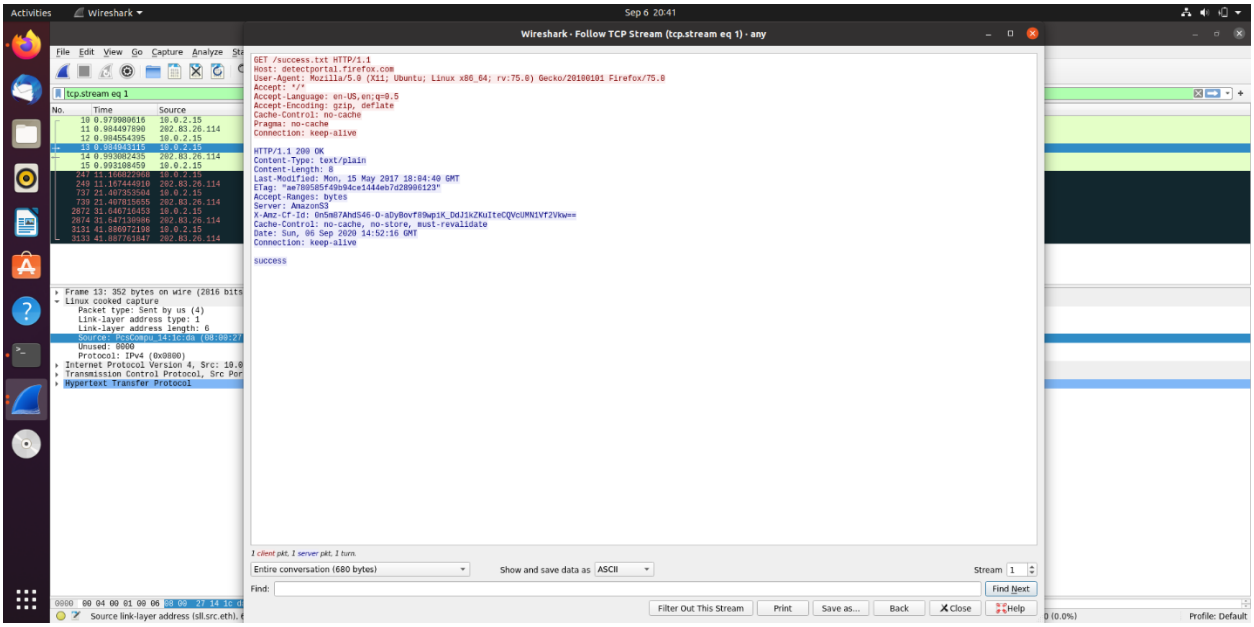
HTTP response (all the information has been expanded in the following screenshots):



Using Wireshark's Follow TCP Stream

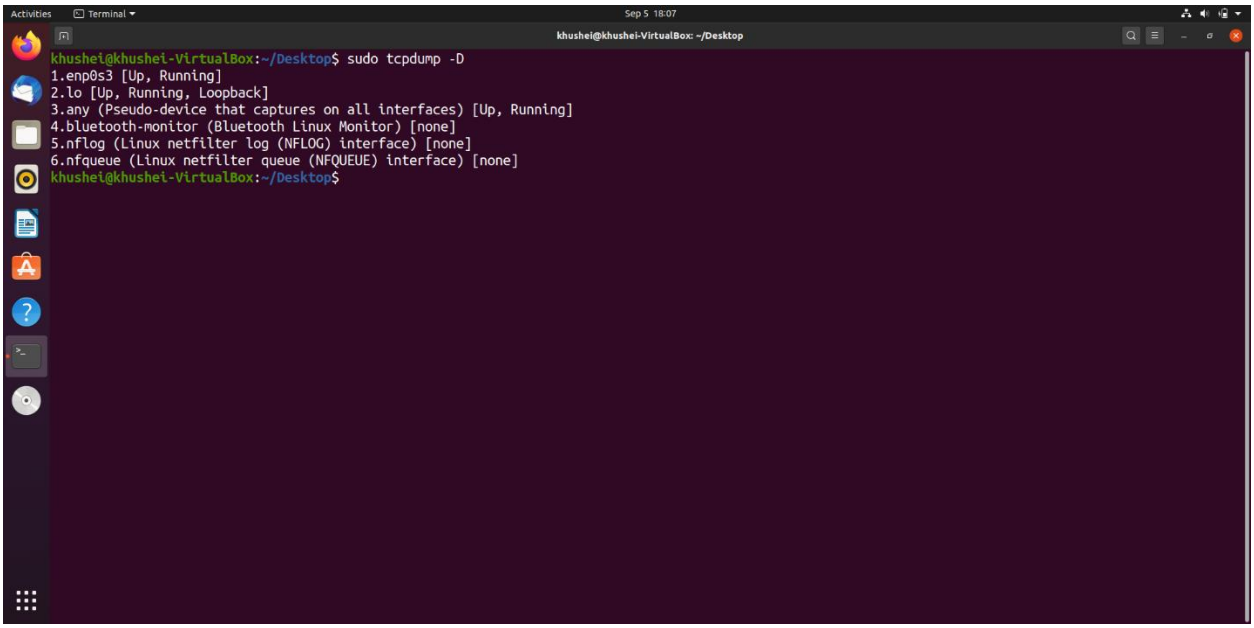
Step 1: Make sure the filter is blank. Right-click any packet inside the Packet List Pane, then select 'Follow TCP Stream'. For demo purpose, a packet containing the HTTP GET request "GET / HTTP / 1.1" can be selected.

Step 2: Upon following a TCP stream, screenshot the whole window.

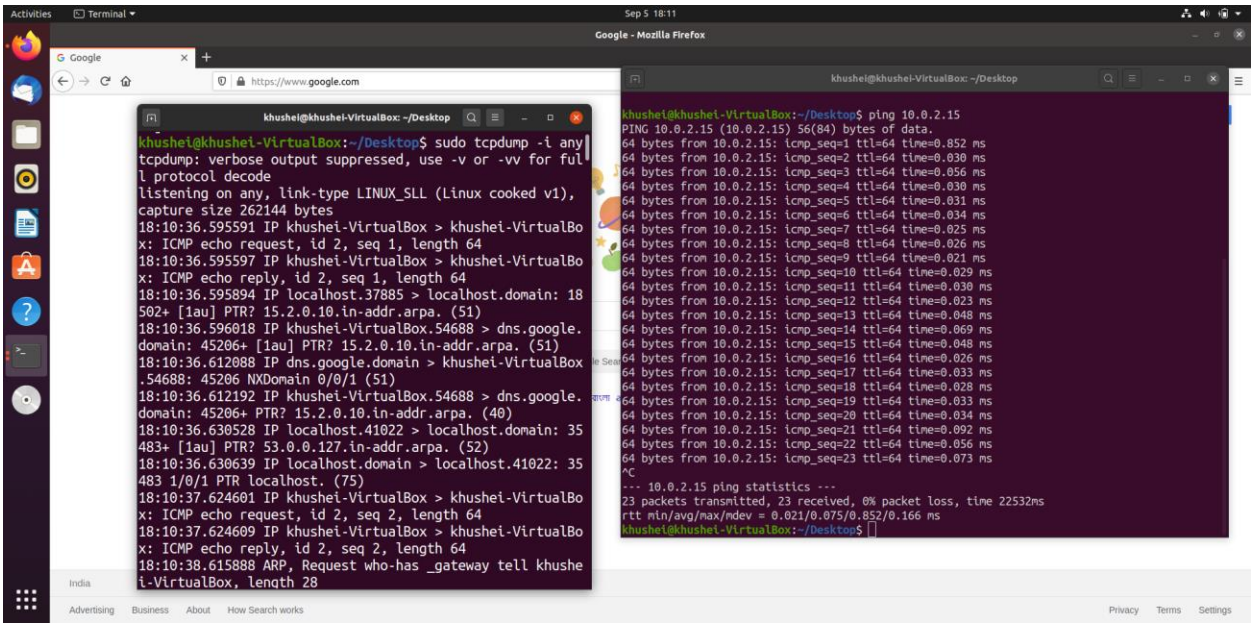


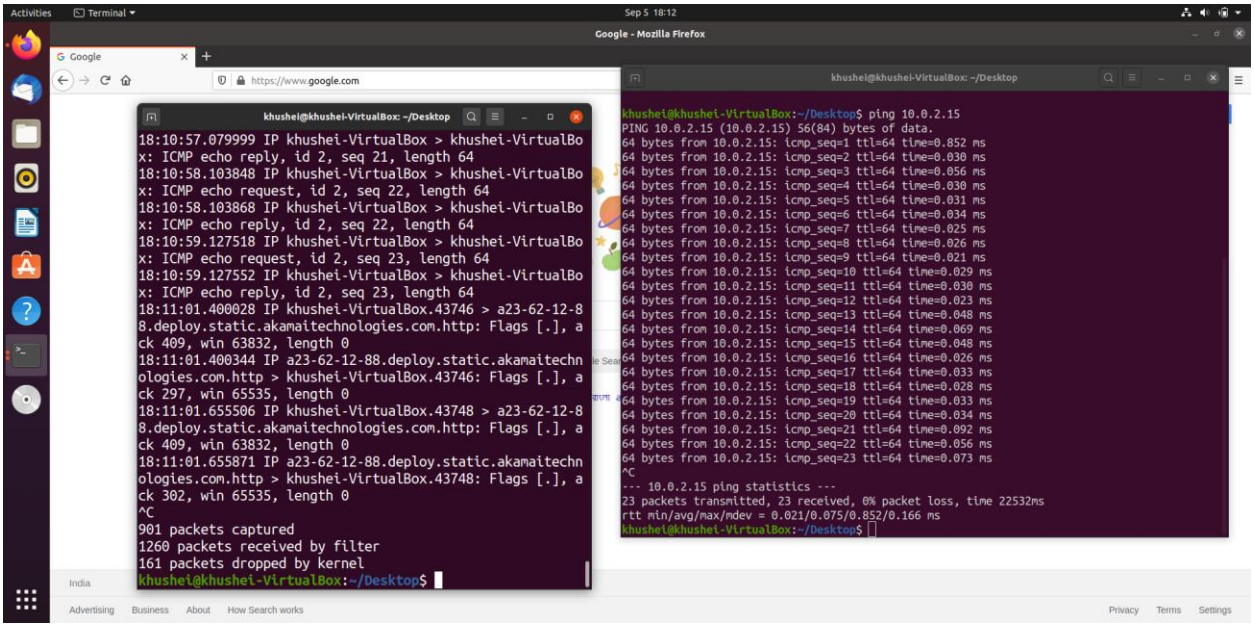
Task 4: Capturing packets with tcpdump

Step 1: Use the command **tcpdump -D** to see which interfaces are available for capture.



Step 2: Capture all packets in any interface by running this command

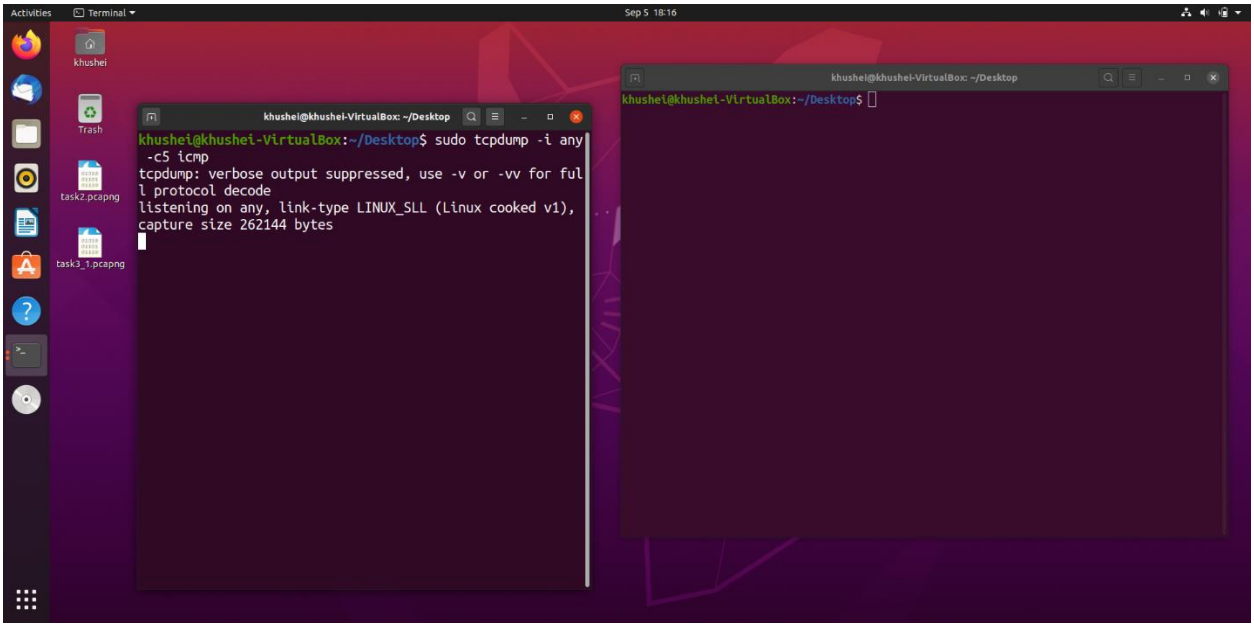


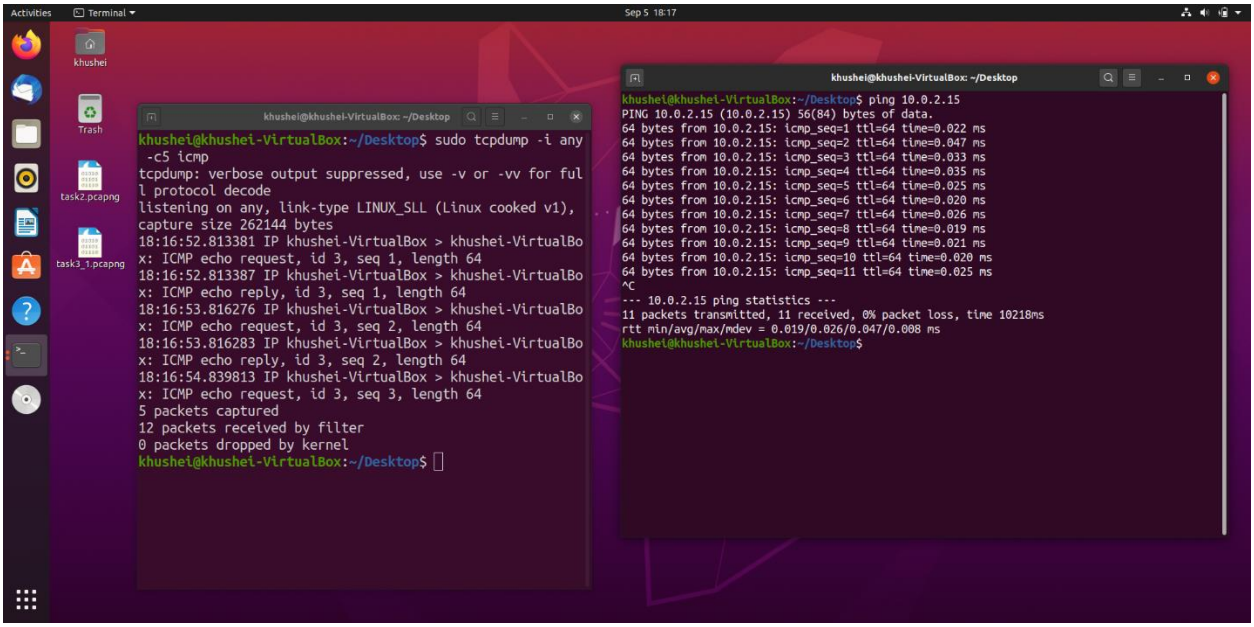


Step 3: Understand the output format.

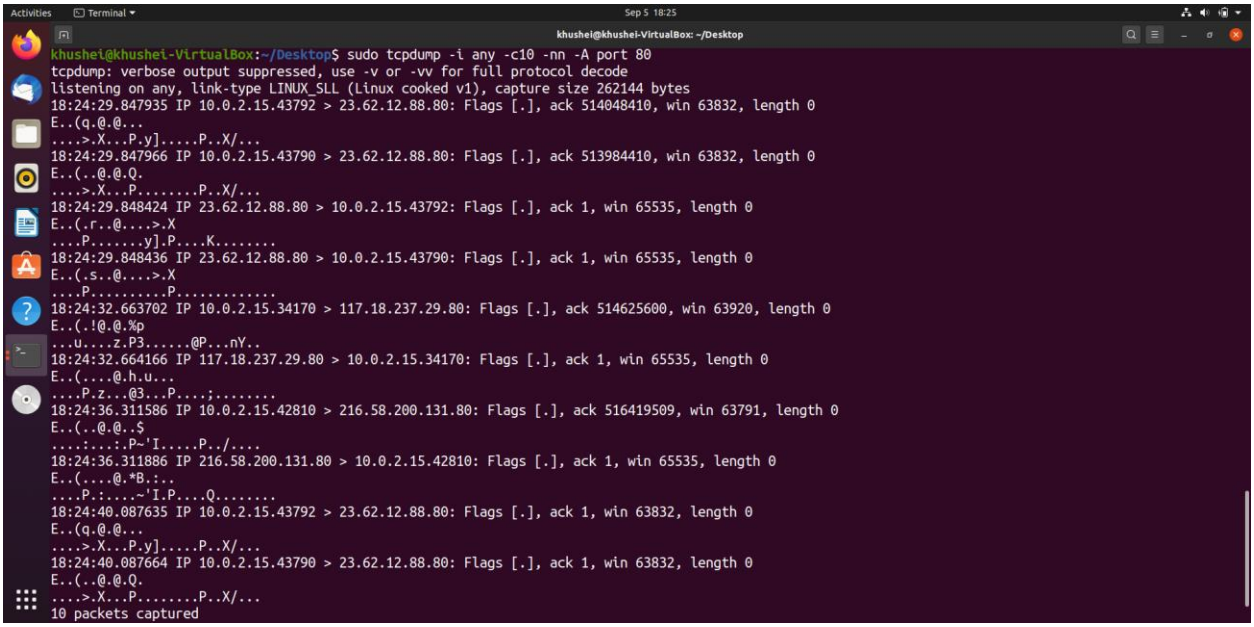
Each line begins with a timestamp. That is followed by the network layer protocol IP. Then we get the source IP and port, a '>' symbol and then the destination IP and port. After this we get a flag indicating the type of interchange. Then there is an acknowledgement number representing the byte to be sent or received. Following this is win and a number that represents the size available in the receiving buffer. After this finally is the packet length.

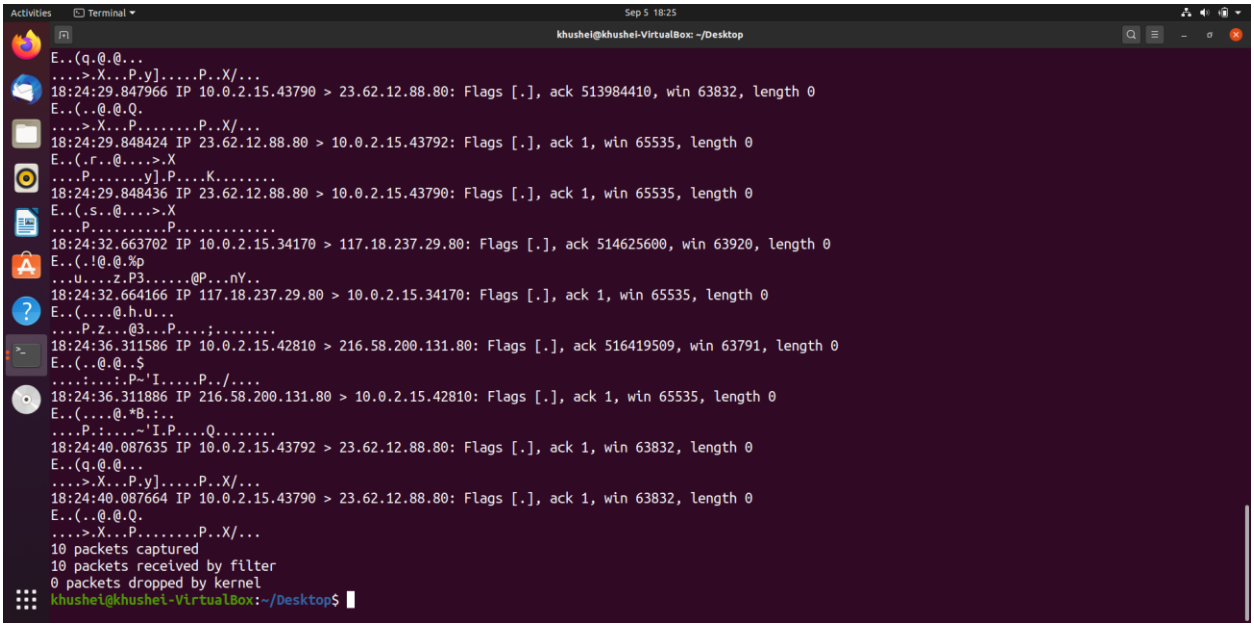
Step 4: To filter packets based on protocol, specifying the protocol in the command line. For example, capture ICMP packets only by using this command:



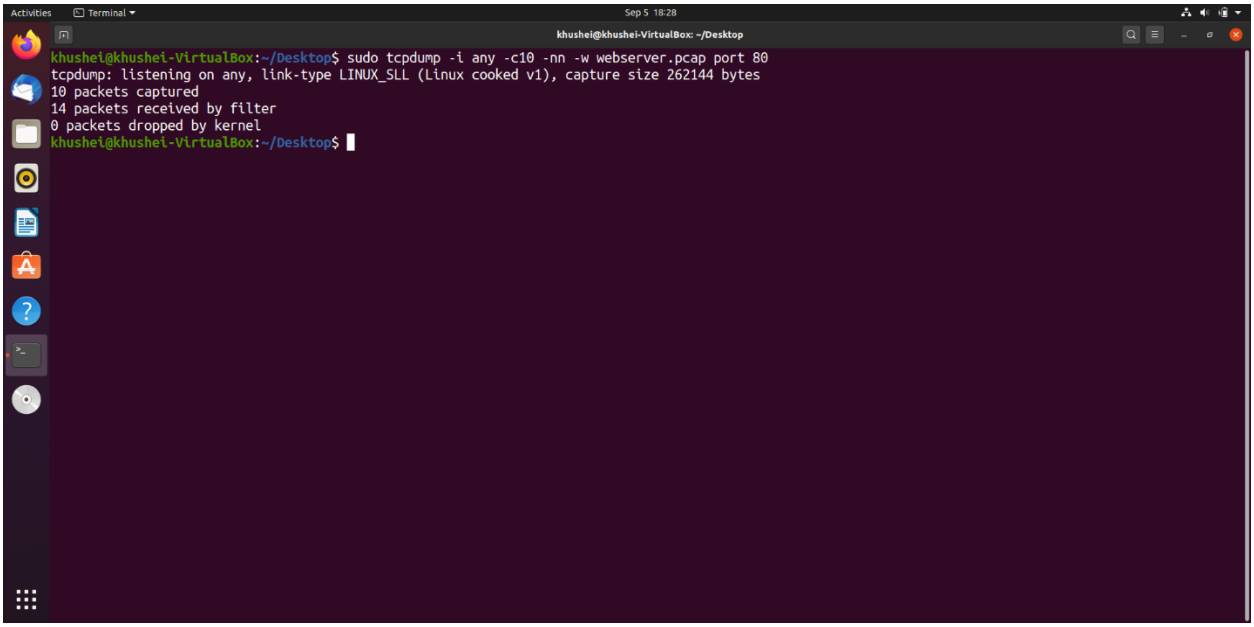


Step 5: Check the packet content. For example, inspect the HTTP content of a web request:

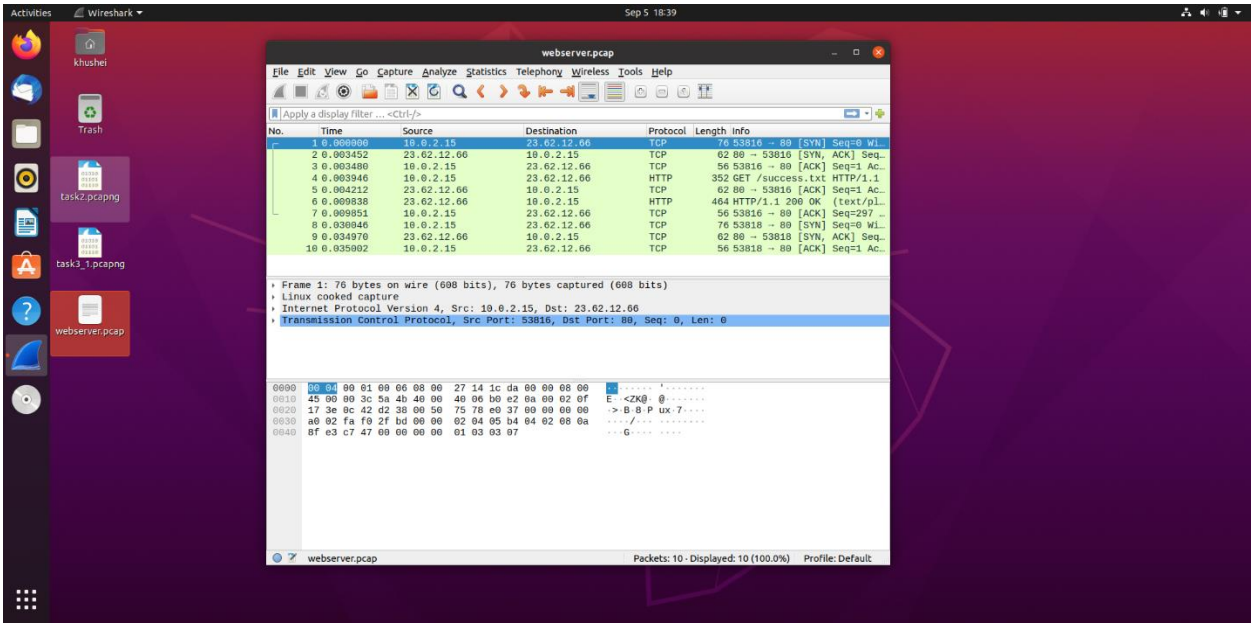




Step 6: To save packets to a file instead of displaying them on screen, use the option -w:



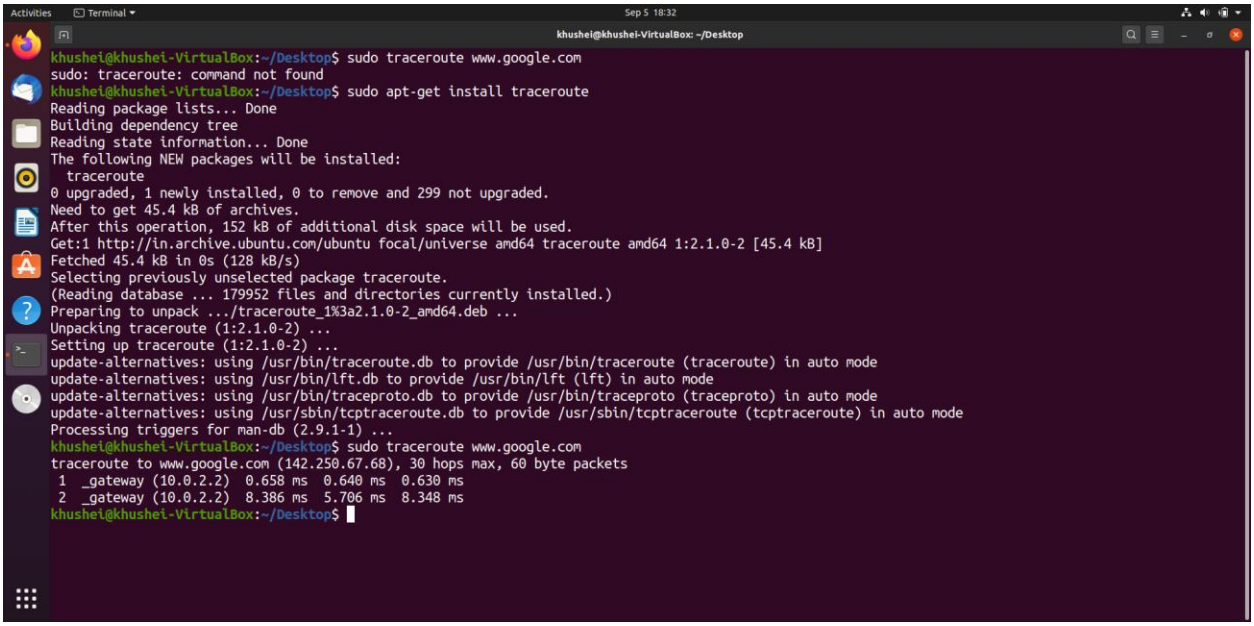
The wireshark file-



Task 5: Perform Traceroute checks

Step 1: Run the traceroute using the following command.

Traceroute was not installed in my Ubuntu VM, so I installed it with sudo apt-get install traceroute and then executed the given command.



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

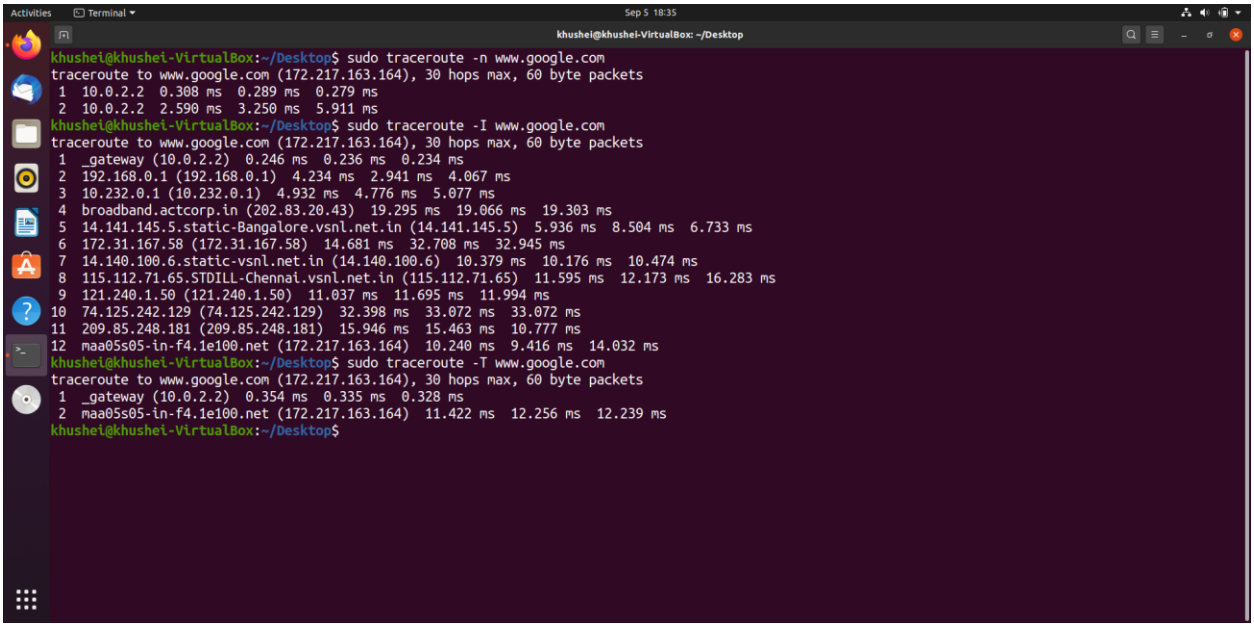
Observation: Destination IP address is 142.250.67.68 and number of hops are 2

Step 3: To speed up the process, you can disable the mapping of IP addresses with hostnames by using the *-n* option

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

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.

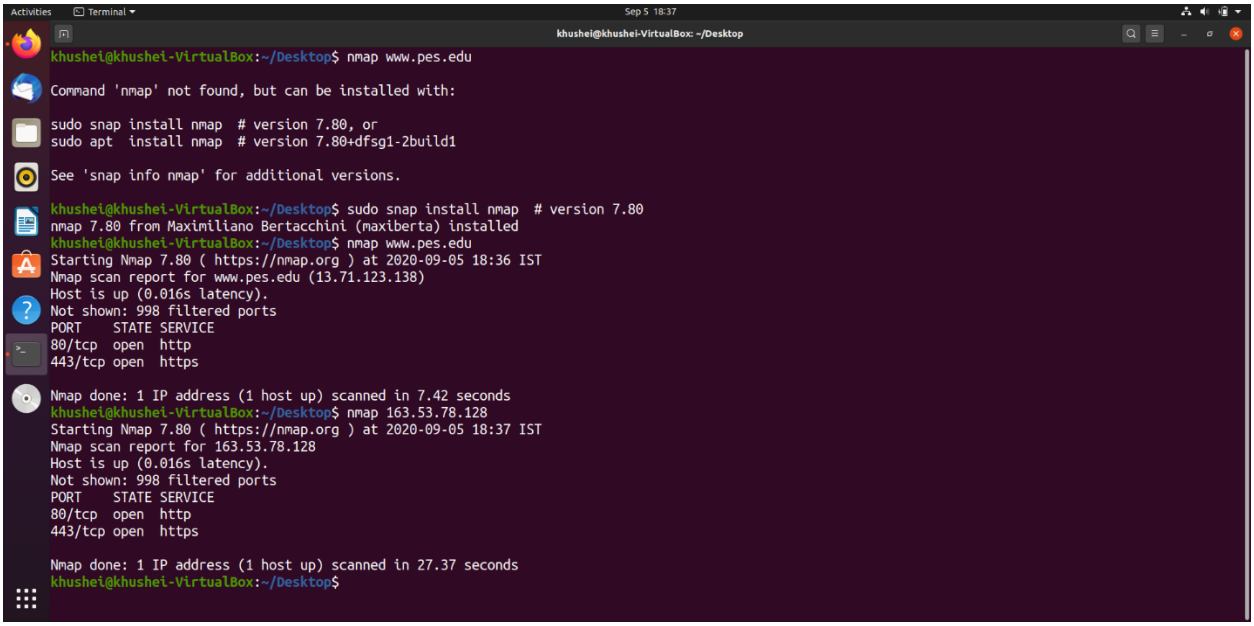
(Step 3,4,5 are all shown in the below screenshot)


Activities
Terminal
Sep 5 18:35
khushei@khushei-VirtualBox: ~/Desktop
khushei@khushei-VirtualBox:~/Desktop$ sudo traceroute -n www.google.com
traceroute to www.google.com (172.217.163.164), 30 hops max, 60 byte packets
1 10.0.2.2 0.308 ms 0.289 ms 0.279 ms
2 10.0.2.2 2.590 ms 3.250 ms 5.911 ms
khushei@khushei-VirtualBox:~/Desktop$ sudo traceroute -I www.google.com
traceroute to www.google.com (172.217.163.164), 30 hops max, 60 byte packets
1 _gateway (10.0.2.2) 0.246 ms 0.236 ms 0.234 ms
2 192.168.0.1 (192.168.0.1) 4.234 ms 2.941 ms 4.067 ms
3 10.232.0.1 (10.232.0.1) 4.932 ms 4.776 ms 5.077 ms
4 broadband.actcorp.in (202.83.20.43) 19.295 ms 19.066 ms 19.303 ms
5 14.141.145.5.static-Bangalore.vsnl.net.in (14.141.145.5) 5.936 ms 8.504 ms 6.733 ms
6 172.31.167.58 (172.31.167.58) 14.681 ms 32.708 ms 32.945 ms
7 14.140.100.6.static-vsnl.net.in (14.140.100.6) 10.379 ms 10.176 ms 10.474 ms
8 115.112.71.65.STDILL-Chennai.vsnl.net.in (115.112.71.65) 11.595 ms 12.173 ms 16.283 ms
9 121.240.1.50 (121.240.1.50) 11.037 ms 11.695 ms 11.994 ms
10 74.125.242.129 (74.125.242.129) 32.398 ms 33.072 ms 33.072 ms
11 209.85.248.181 (209.85.248.181) 15.946 ms 15.463 ms 10.777 ms
12 maa05s05-in-f4.1e100.net (172.217.163.164) 10.240 ms 9.416 ms 14.032 ms
khushei@khushei-VirtualBox:~/Desktop$ sudo traceroute -T www.google.com
traceroute to www.google.com (172.217.163.164), 30 hops max, 60 byte packets
1 _gateway (10.0.2.2) 0.354 ms 0.335 ms 0.328 ms
2 maa05s05-in-f4.1e100.net (172.217.163.164) 11.422 ms 12.256 ms 12.239 ms
khushei@khushei-VirtualBox:~/Desktop$

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

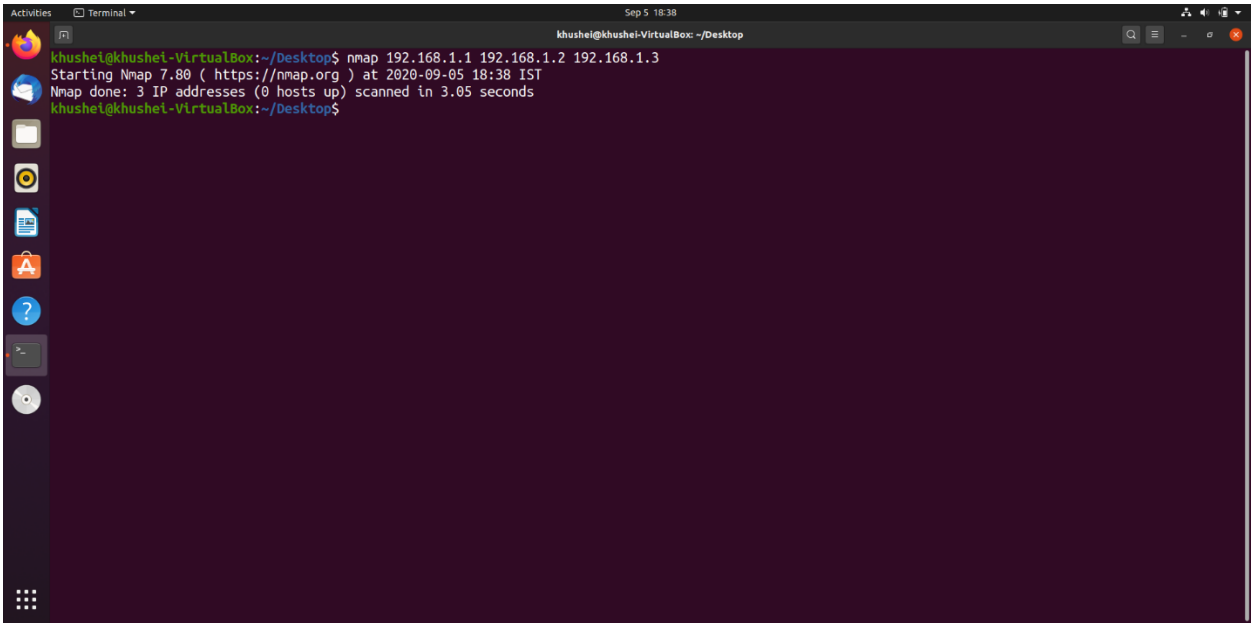
Step 1: You can scan a host using its host name or IP address, for instance.

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



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

The output shows 0 hosts up because neither of these three IP addresses are up and running in our network.


Activities
Terminal
Sep 5 18:38
khushei@khushei-VirtualBox: ~/Desktop
khushei@khushei-VirtualBox:~/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 18:38 IST
Nmap done: 3 IP addresses (0 hosts up) scanned in 3.05 seconds
khushei@khushei-VirtualBox:~/Desktop$

Questions on above observations:

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

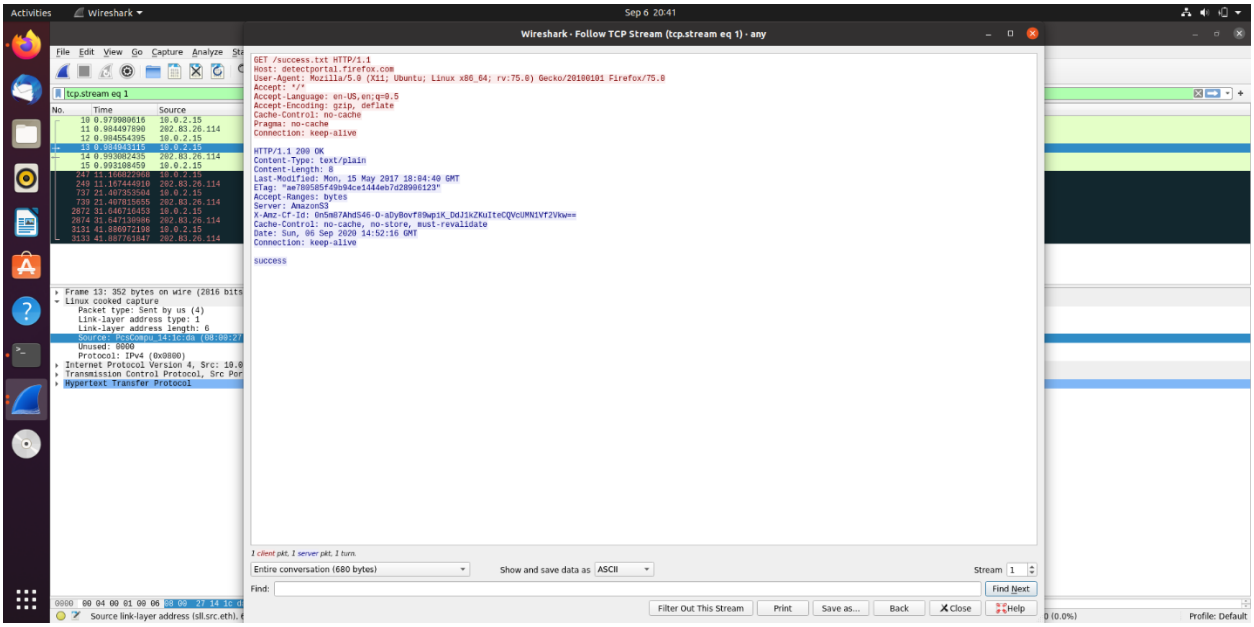
Browser: HTTP version 1.1

Server: HTTP version 1.1

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

In task 3, we had followed TCP stream for the packet containing “GET / HTTP / 1.1”.

In that screenshot, we can see the Last-Modified field. It is Mon, 15 May 2017 18:04:40 GMT in my case.



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

By using the -c flag with ping command.

ping -c <number_of_packets> <hostname>

4) How will you identify remote host apps and OS?
This can be done using nmap:

1) nmap -O -v localhost
2) nmap -O -v server.ip.address