COMPUTER NETWORKS LAB – WEEK1

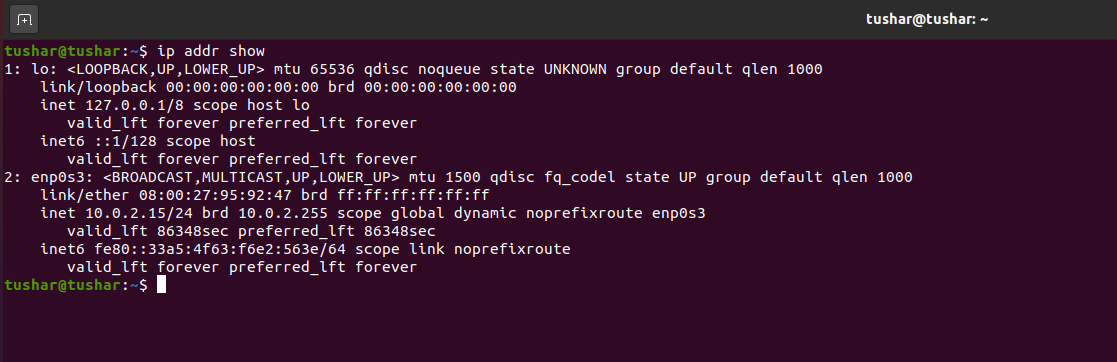
Name: TUSHAR Y S

SRN: PES1UG19CS545

**Task 1: Linux Interface Configuration**

1.1 To display status of all active network interfaces.

Command- ip addr show



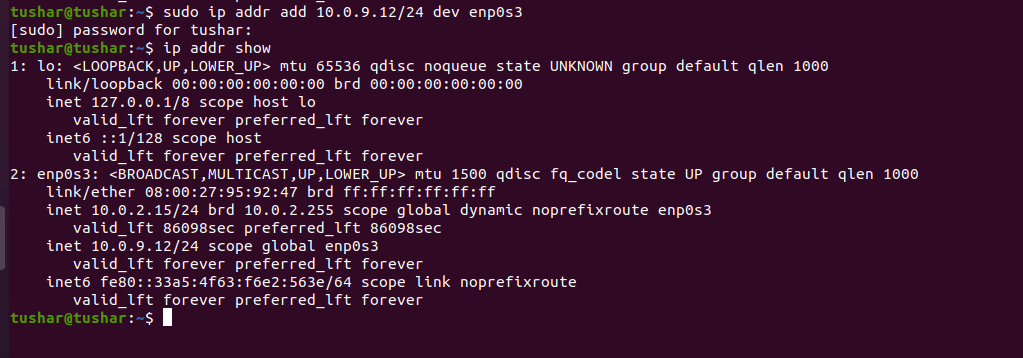
Ip address table:

|  |  |  |
| --- | --- | --- |
| Interface Name | IP address(IPv4/IPv6) | MAC address |
| lo | 127.0.0.1/::1 | 00:00:00:00:00:00 |
| enp0s3 | 10.0.2.15/fe80::33a5:4f63:f6e2:563e | 08:00:27:95:92:47 |

1.2 Assigning an IP address to an interface.

Command- sudo ip addr add 10.0.9.12/24 dev enp0s3

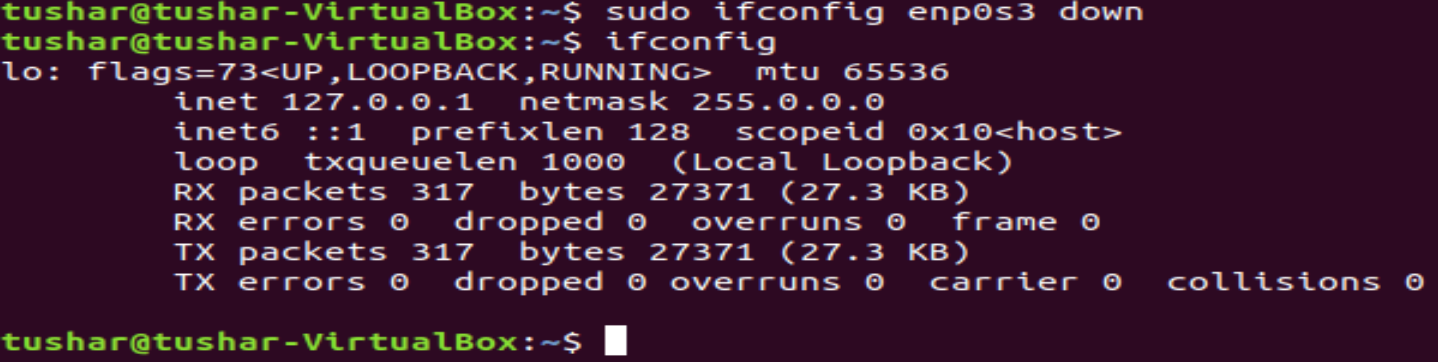
(Section I – 9, Roll No.:12)



1.3 To activate and deactivate a network interface.

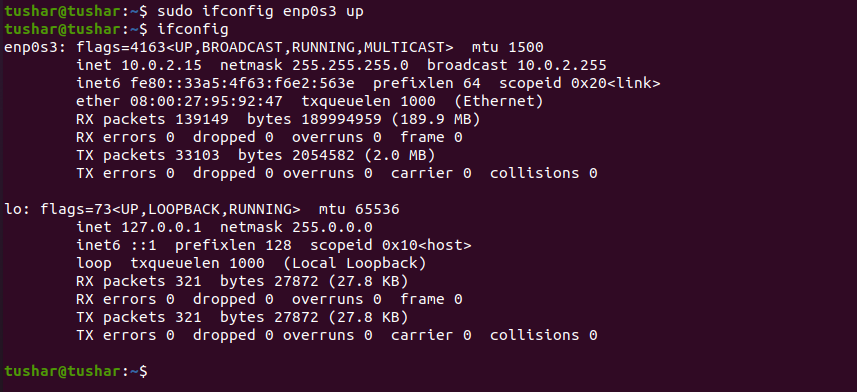
1.3.1 Deactivating an interface(enp0s3)

Command- sudo ifconfig enp0s3 down



1.3.2 Activating an interface(enp0s3)

Command- sudo ifconfig enp0s3 up



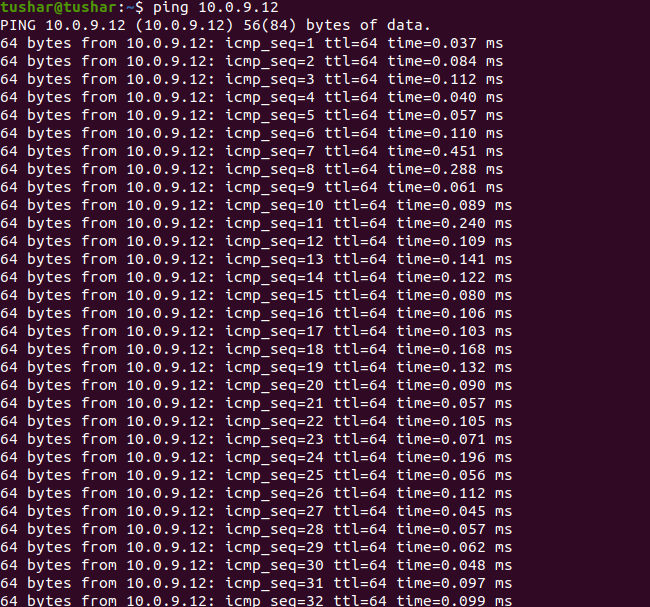
1.4 To show the current neighbor table in kernel.

Command- ip neigh



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

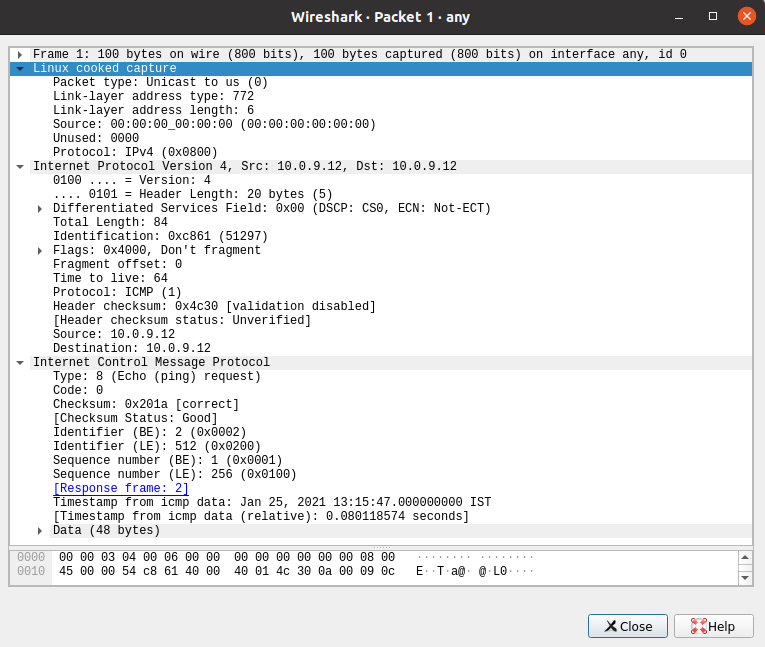
Command- ping 10.0.9.12



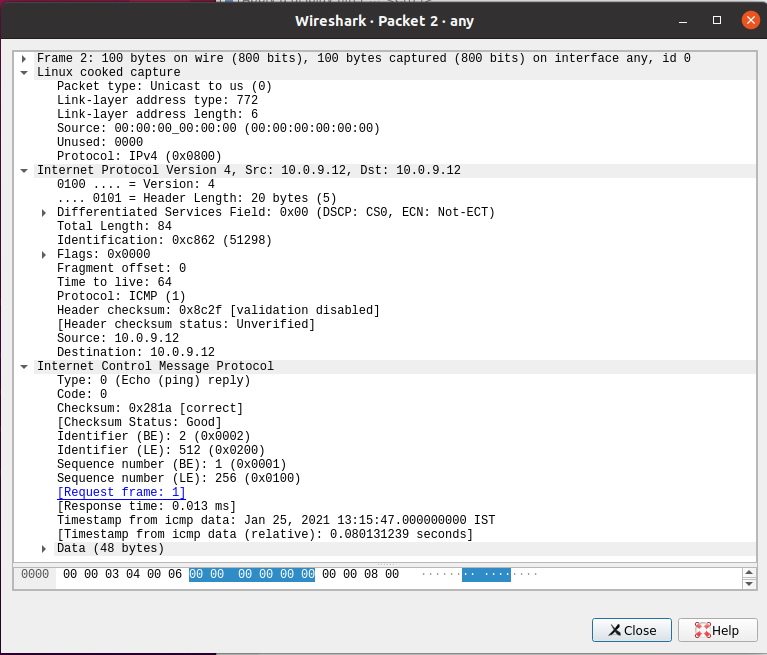
Observation:

|  |  |
| --- | --- |
| TTL | 64 |
| Protocol used by ping | ICMP |
| Time | In the order of 10-2 ms |

Echo Request Packet:



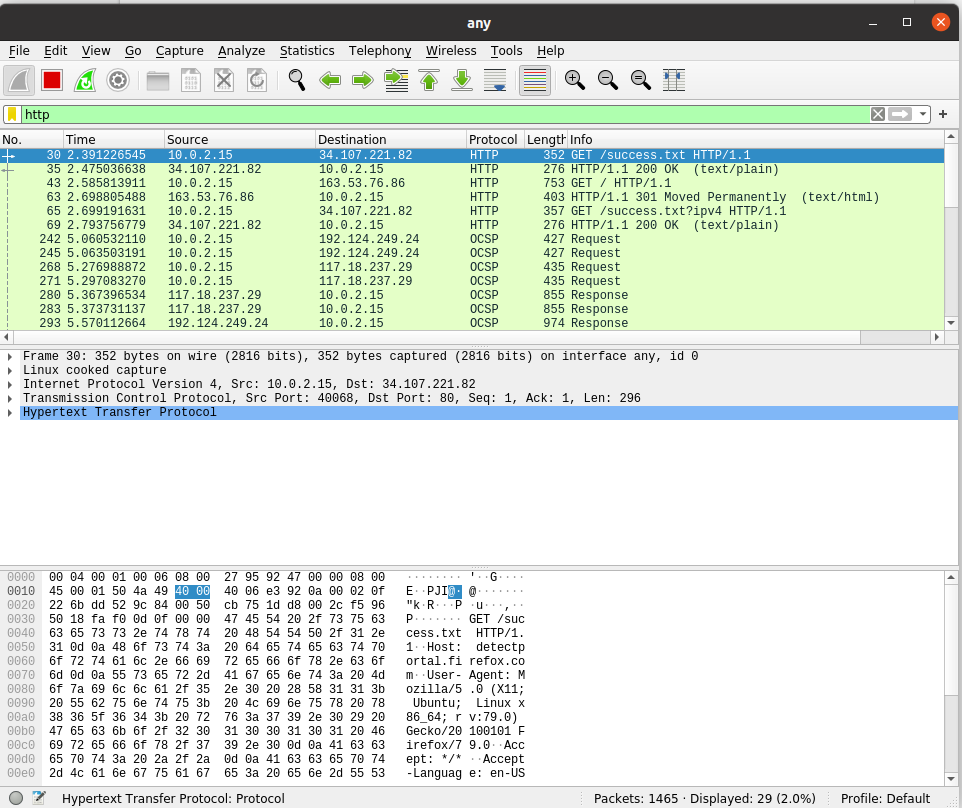
Echo Response Packet:



|  |  |  |
| --- | --- | --- |
| **Details** | **First Echo Request** | **First Echo Reply** |
| Frame Number | 1 | 2 |
| Source IP address | 10.0.9.12 | 10.0.9.12 |
| Destination IP address | 10.0.9.12 | 10.0.9.12 |
| 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 | IPv4 | IPv4 |
| Time To Live (TTL) Value | 64 | 64 |

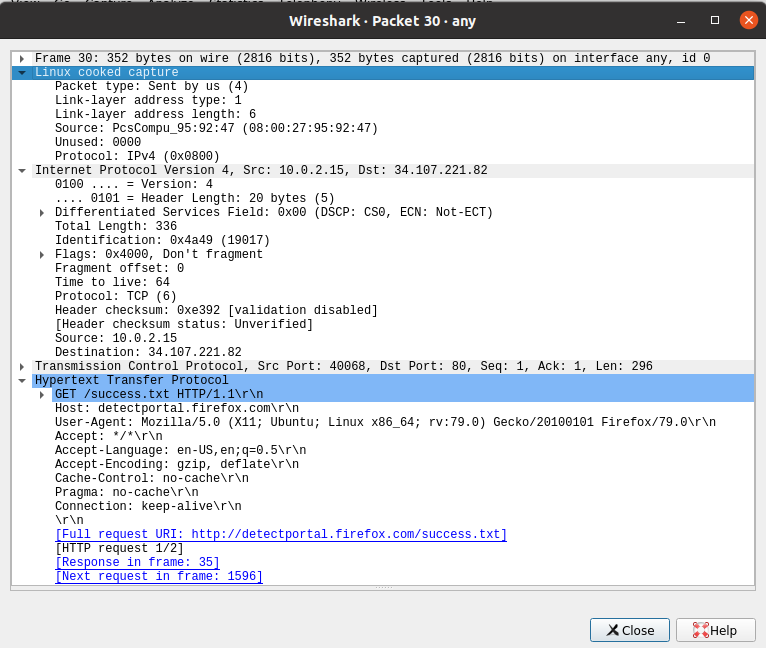
**Task 3: HTTP PDU Capture**

3.1 Upon browsing [www.flipkart.com](http://www.flipkart.com), and selecting ‘http’ in wireshark’s filter toolbar:



3.2 Echo Request and Reply:

3.2.1 Echo Request Packet:



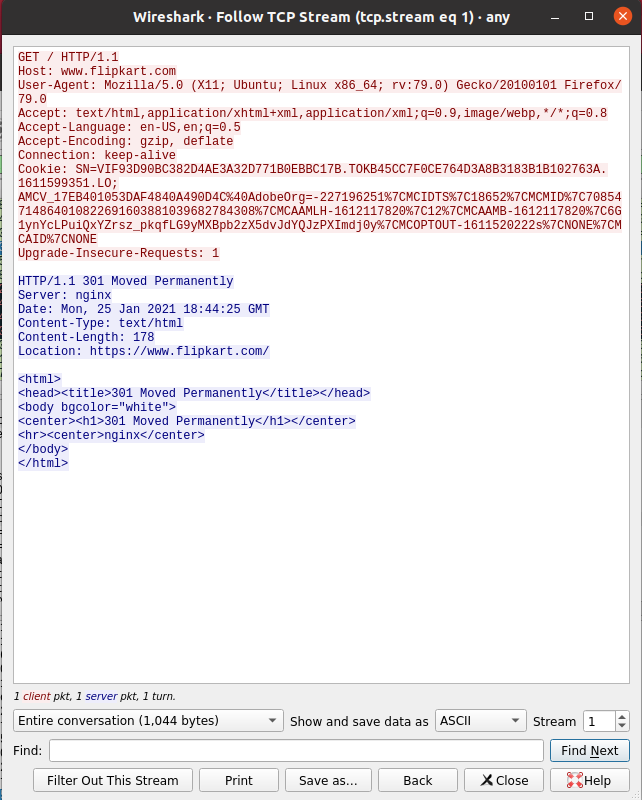
3.2.2 Echo Response Packet:



3.2.3

|  |  |  |
| --- | --- | --- |
| **Details** | **First Echo Request** | **First Echo Reply** |
| Frame Number | 30 | 35 |
| Source Port | 40068 | 80 |
| Destination Port | 80 | 40068 |
| Source IP Address | 10.0.2.15 | 34.107.221.82 |
| Destination IP Address | 34.107.221.82 | 10.0.2.15 |
| Source Ethernet Address | 08:00:27:95:92:47 | 52:54:00:12:35:00 |
| Destination Ethernet Address | 52:54:00:12:35:00 | 08:00:27:95:92:47 |

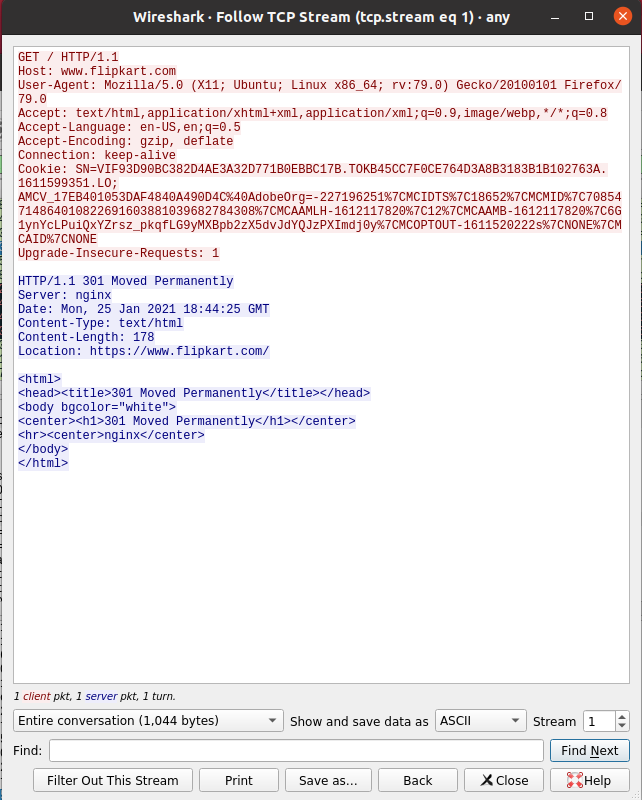
Wireshark’s follow TCP Stream:



3.3 HTTP Request and Response:

|  |  |  |  |
| --- | --- | --- | --- |
| HTTP Request | | HTTP Response | |
| Get | GET/HTTP/1.1\r\n | Server | nginx |
| Host | [www.flipkart.com](http://www.flipkart.com) | Content-Type | Text/plain\r\n |
| User-Agent | Mozilla/5.0 (X11; Ubuntu;Linux x86\_64;rv:79.0) Gecko/20100101 Firefox/79.0\r\n | Date | Mon, 25 Jan 2021 10:28:51 GMT\r\n |
| Accept-Language | en-US,en;q=0.5\r\n | Location | https://www.flipkart.com/ |
| Accept-Encoding | gzip,deflate\r\n | Content-Length | 178 |
| Connection | keep-alive\r\n | Connection | Keep-alive |

3.4 Wireshark’s follow TCP Stream:



**Task 4- Capturing packets with tcpdump**

4.1 Interfaces available for Capture:

Command- sudo tcpdump -D



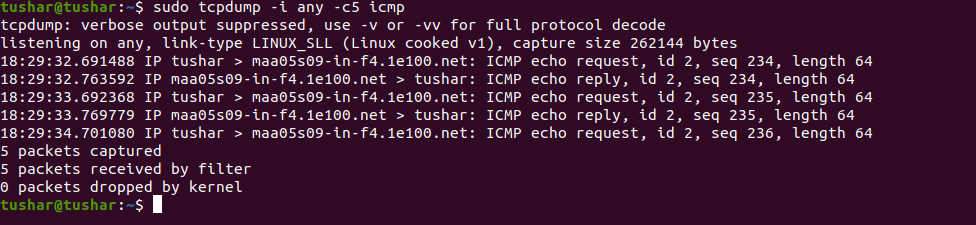
4.2 Capturing all packets in any interface:

Command- sudo tcpdump -i any



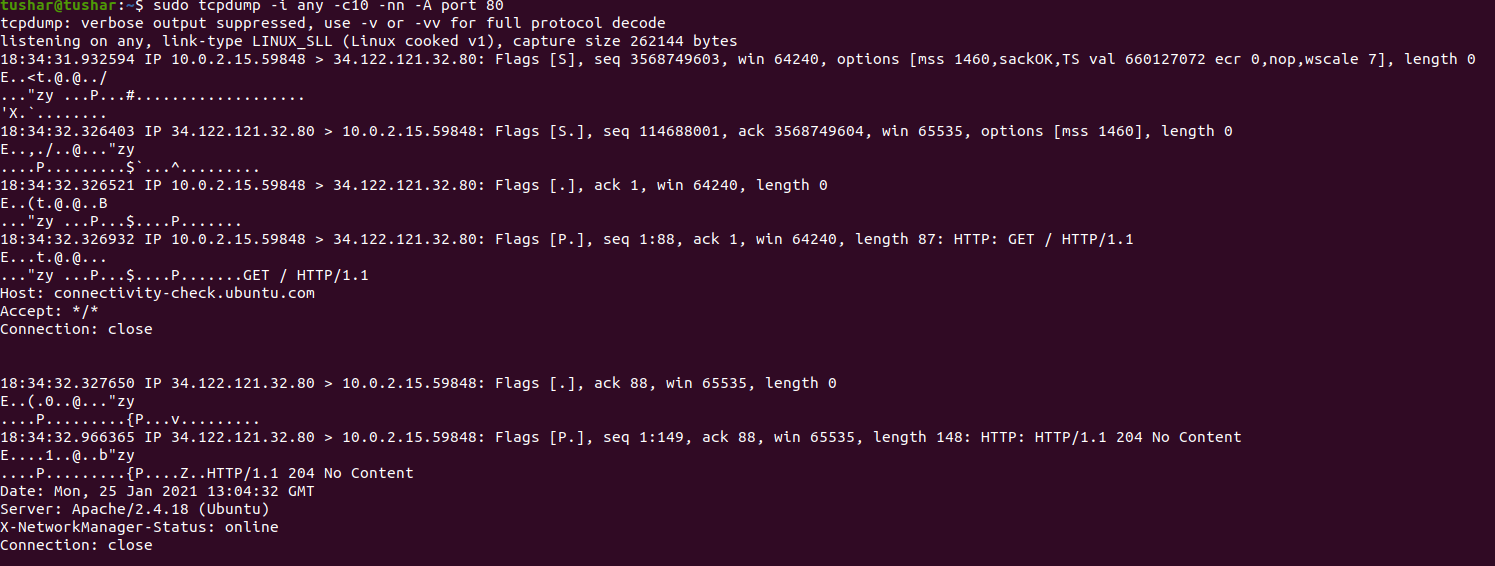
4.3 To filter packets based on protocol(ex:icmp):

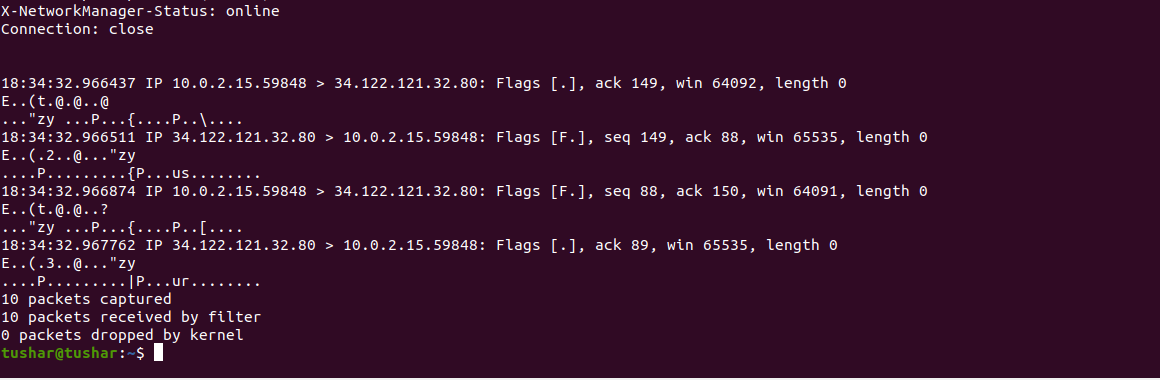
Command- sudo tcpdump -i any -c5 icmp



4.4 To check the packet content:

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



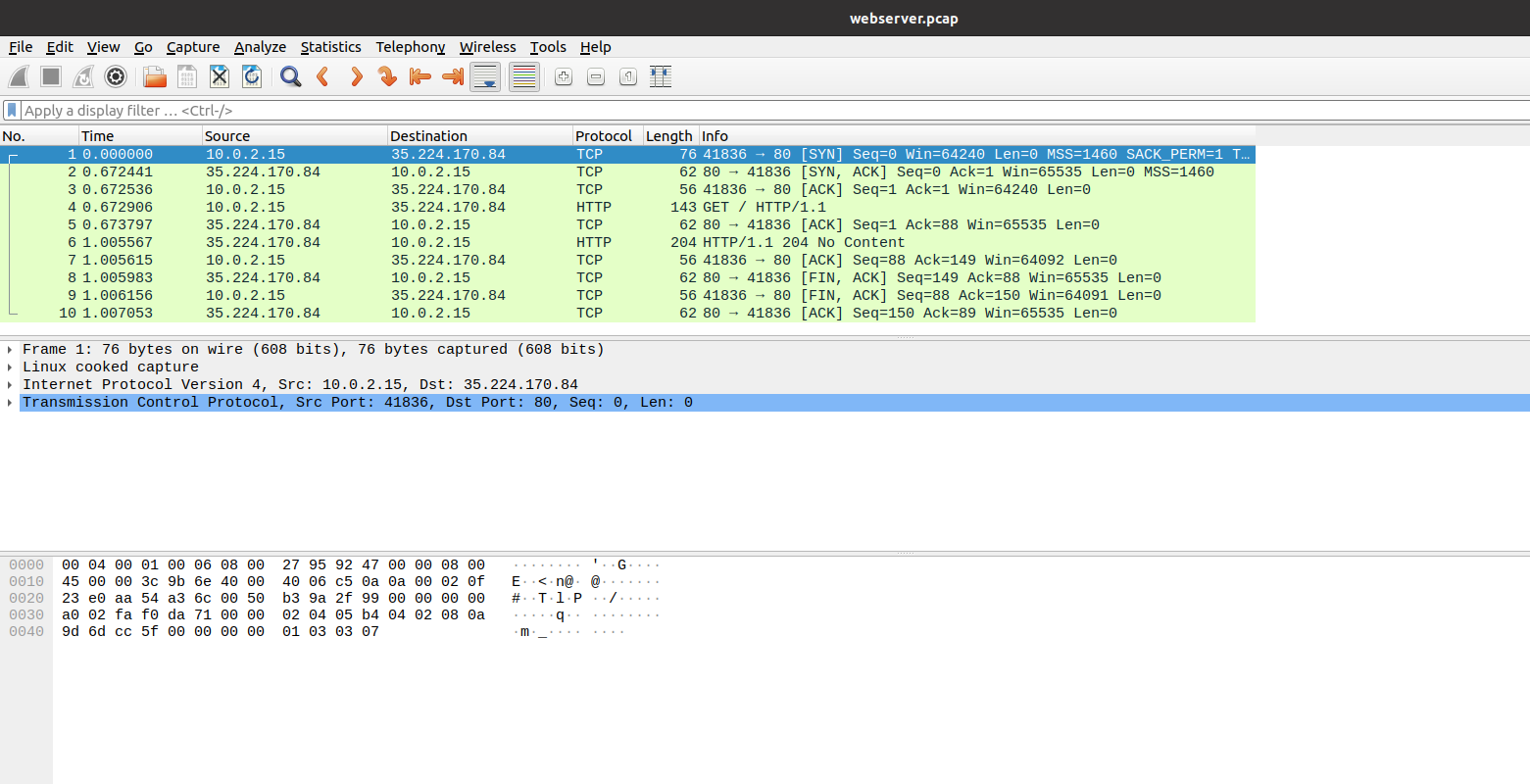


4.5 To save packets to a file:

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



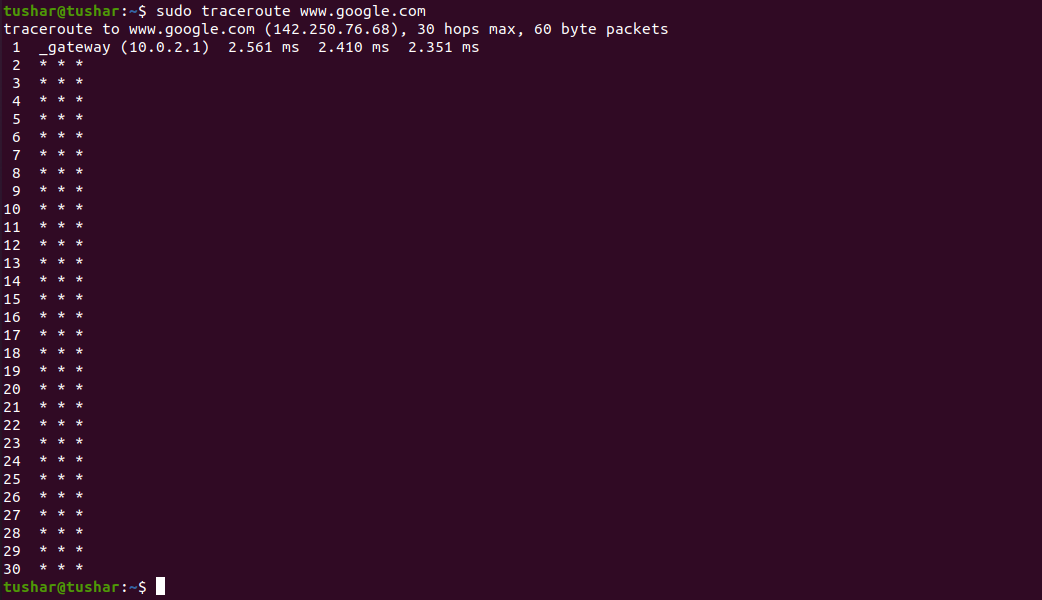
webserver.pcap file:



**Task 5- Perform Traceroute Checks**

5.1 Running the traceroute:

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

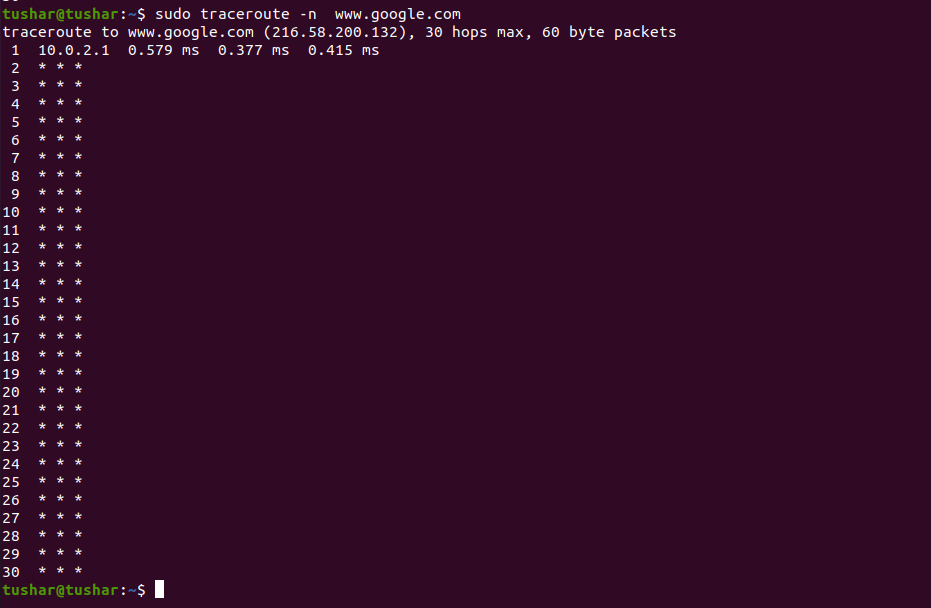


Destination address of google.com – 142.250.76.68

No. of hops – 30 max hops

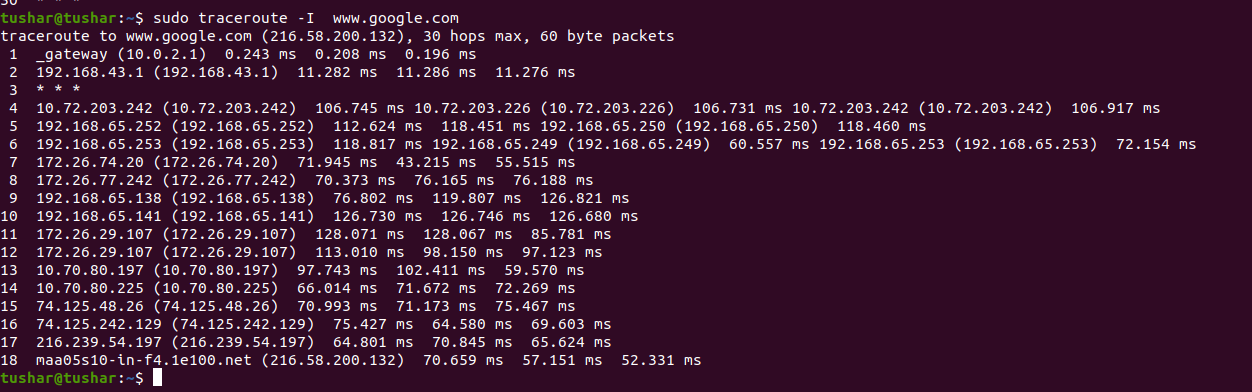
5.2 Disabling the mapping of ip addresses with host names:

Command- sudo traceroute -n [www.google.com](http://www.google.com)



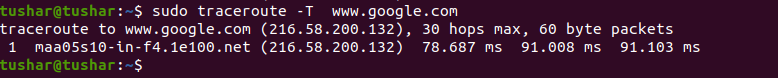
5.3 Using -I option so that traceroute uses ICMP protocol:

Command- sudo traceroute -I [www.google.com](http://www.google.com)



5.4 To test a TCP connection to gather data more relevant to web server:

Command- sudo traceroute -T [www.google.com](http://www.google.com)



**Task 6- Explore an entire network for information (Nmap)**

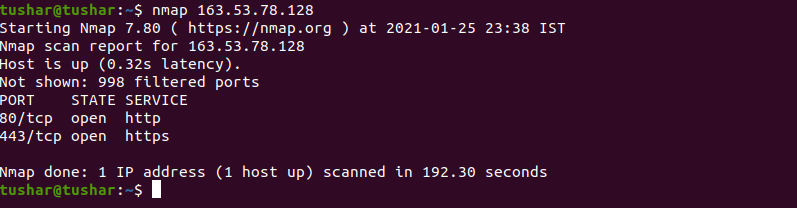
6.1 To scan a host using its hostname:

Command- nmap [www.pes.edu](http://www.pes.edu)



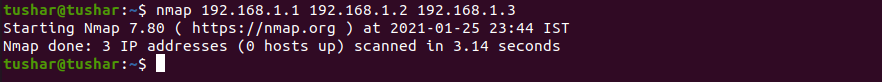
6.2 To scan a host using its IP address:

Command- nmap 163.53.78.128



6.3 Scanning multiple IP address or subnet (IPv4):

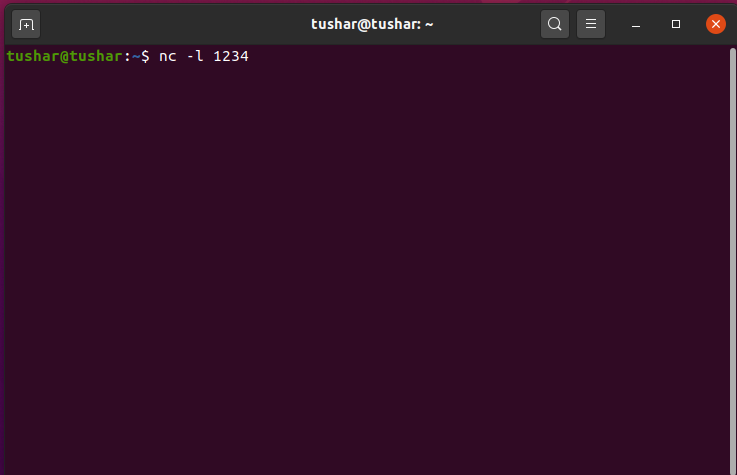
Command- nmap 192.168.1.1 192.168.1.2 192.168.1.3



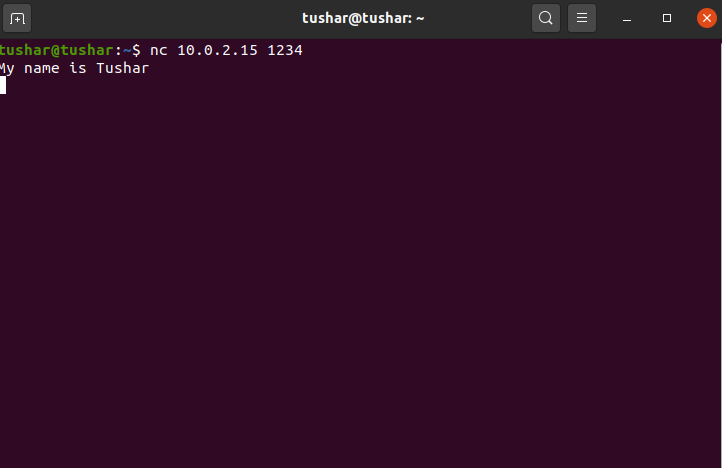
**Task 7 a)- Netcat as Chat tool**

7a.1 Intra system communication:

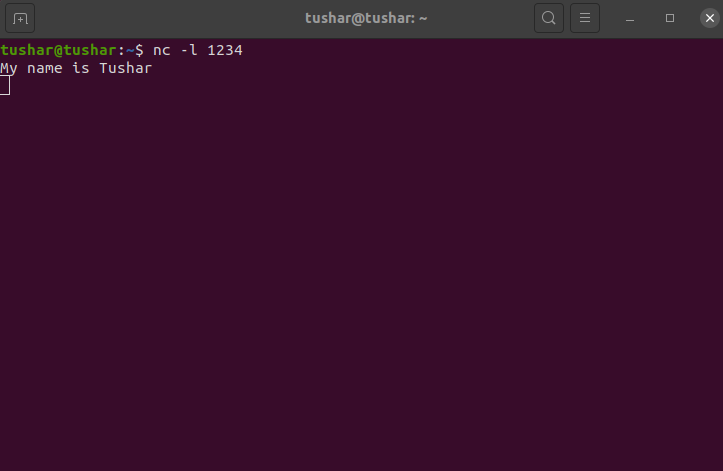
Command on server’s terminal: nc -l 1234



Command on Client’s terminal: nc 10.0.2.15 1234



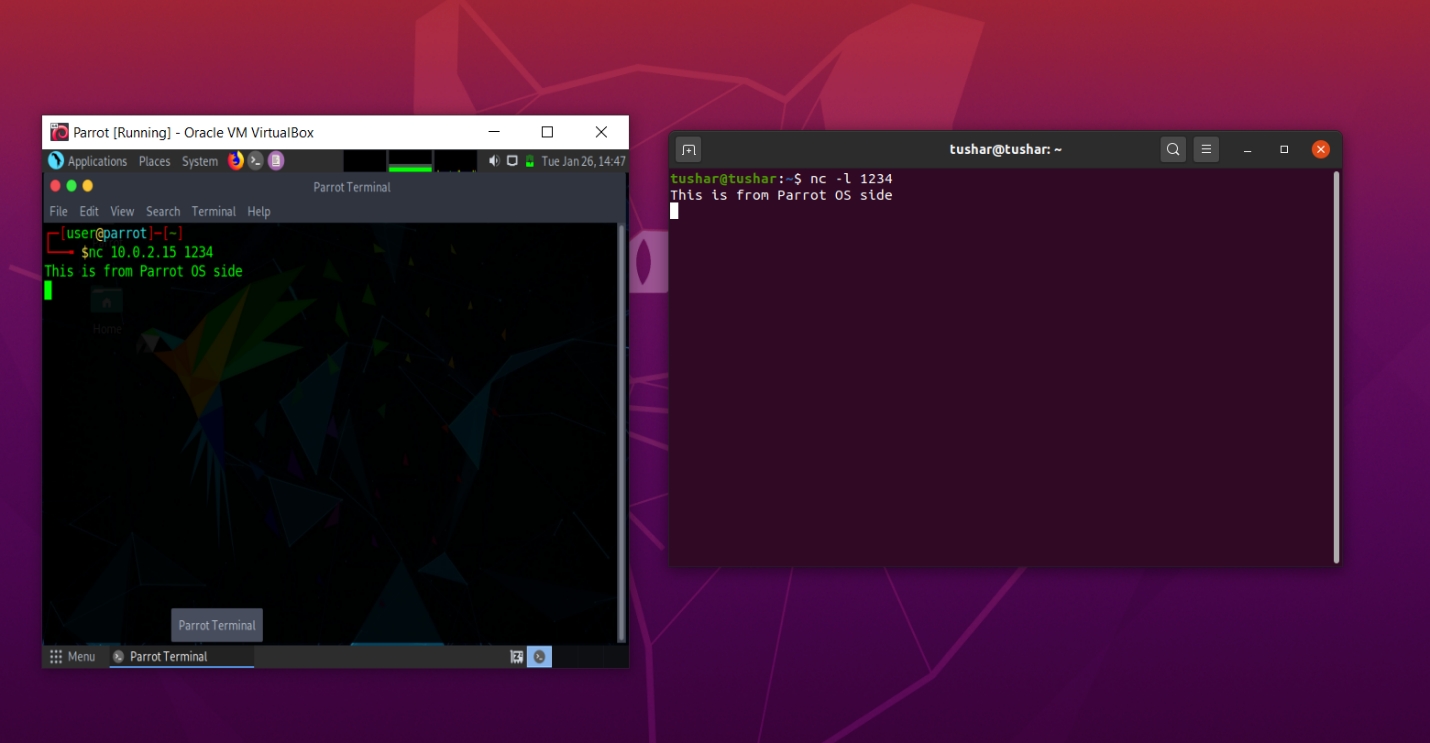
Whatever is typed on client’s terminal is appearing on server side.



7a.2 Inter system communication:

Command on server’s terminal (ubuntu): nc -l 1234

Command on clients’s terminal (parrot): nc 10.0.2.15 1234

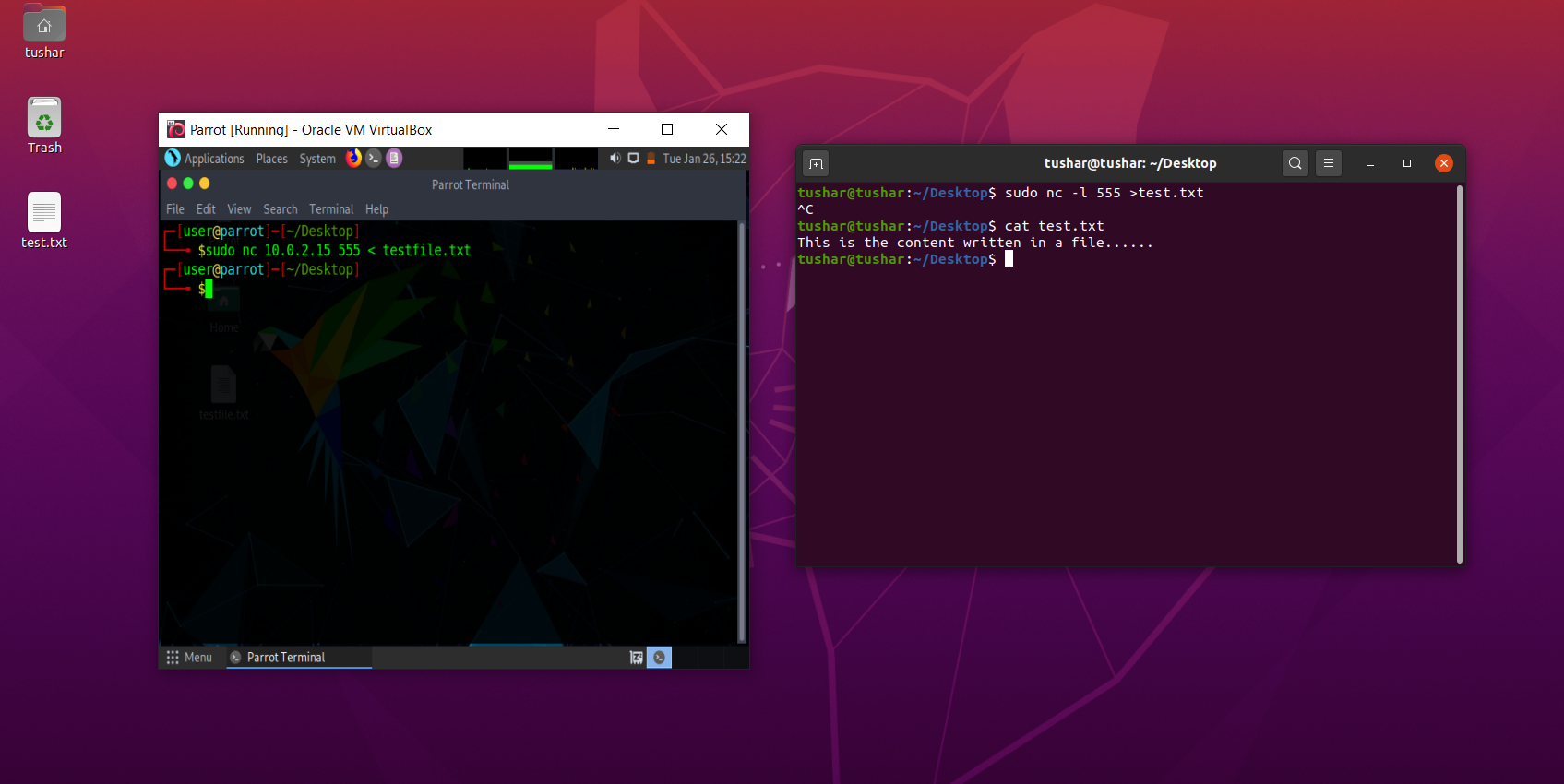
****

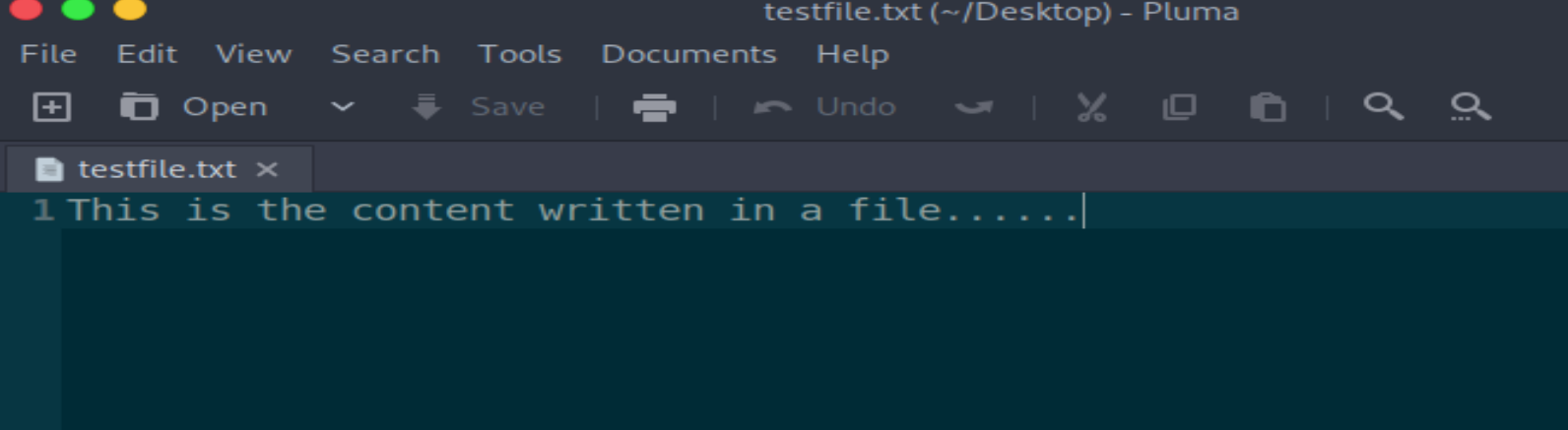
**Task 7 b)- Using Netcat to transfer files**

Command on server side (ubuntu): sudo nc -l 555 > test.txt

Command on client side (parrot): sudo nc 10.0.2.15 555 < testfile.txt

Command on server side to verfify file transfer: cat test.txt

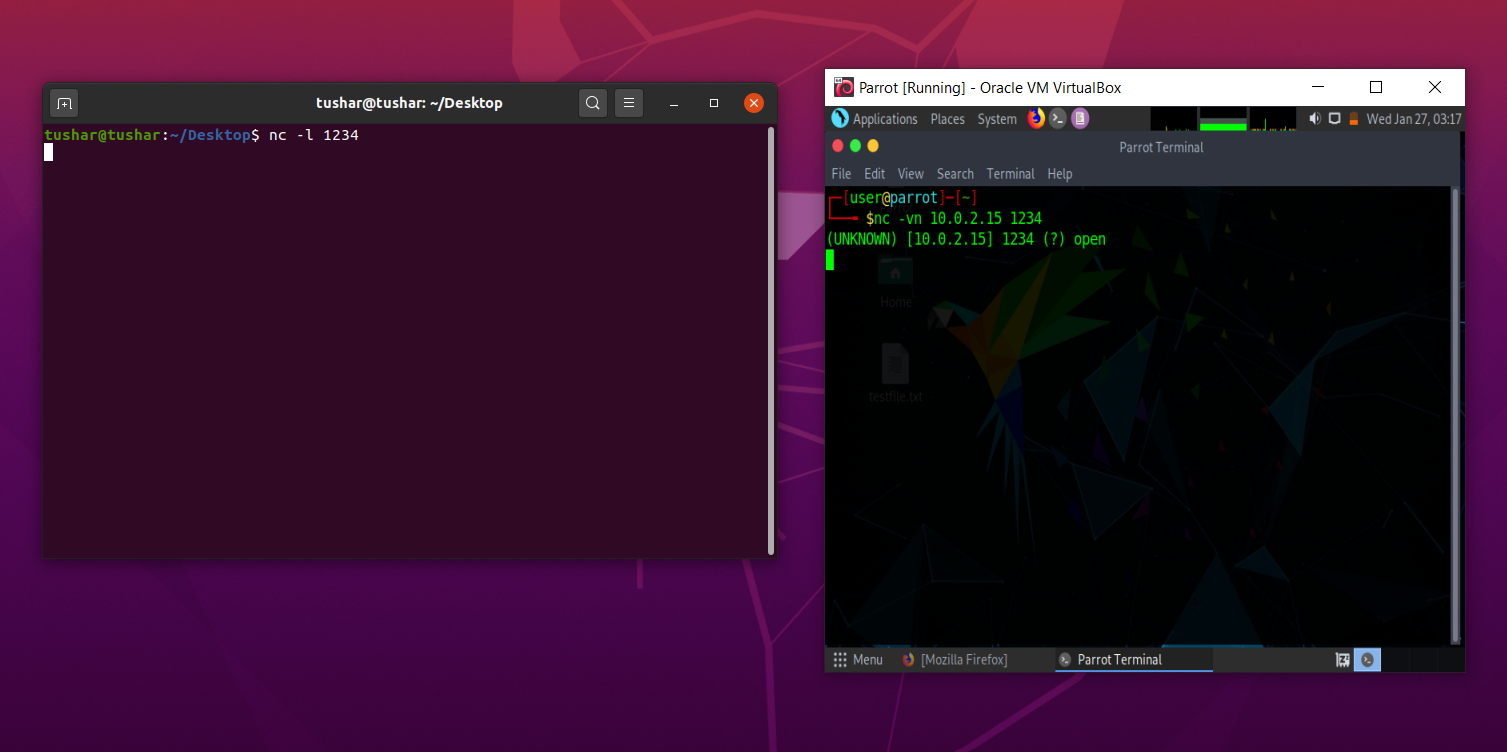




**Task 7 c)- Other commands**

7.1 To check if a particular TCP port of a remote host is open:

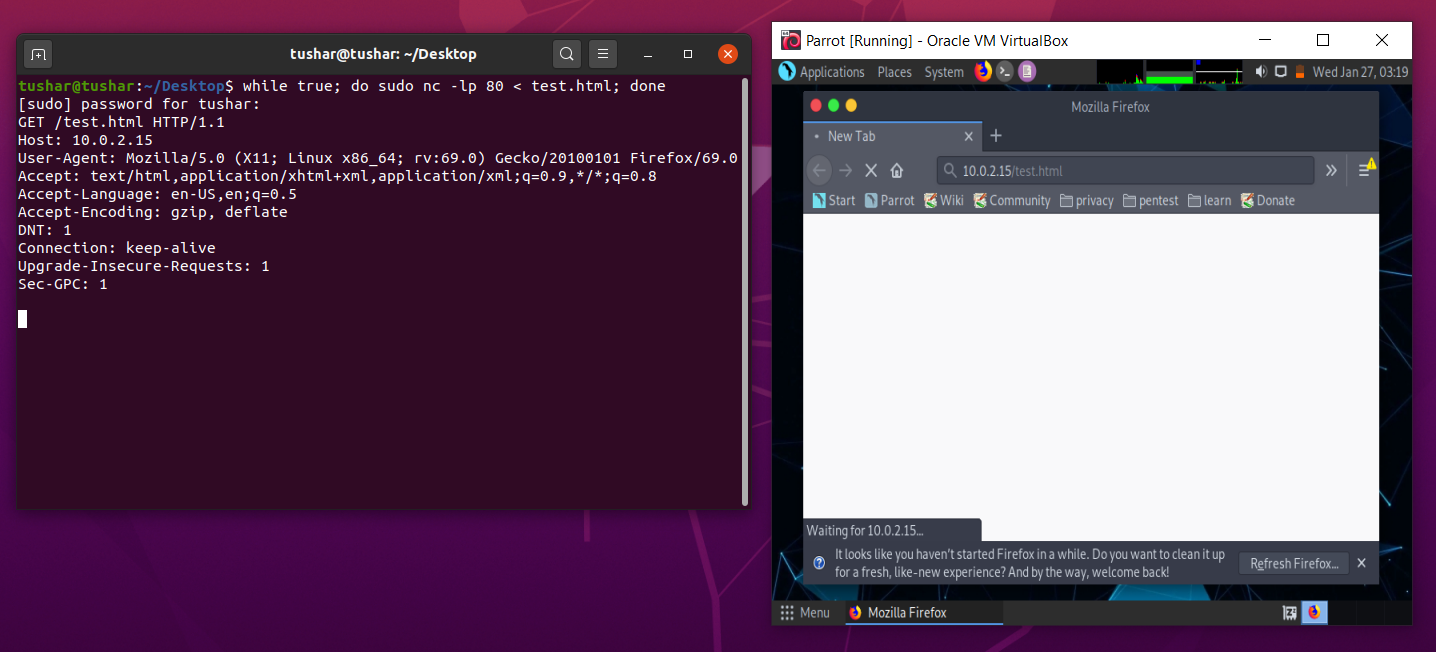
Command: nc -vn 10.0.2.15 1234



7.2 To start a web server that serves test.html on port 80:

Command on local host: while true; do sudo nc -lp 80 < test.html; done

After opening <http://10.0.2.15/test.html> from another host to access test.html:

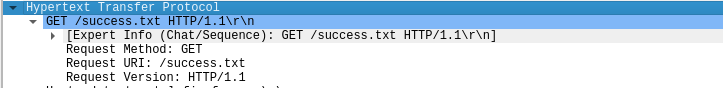


**Questions:**

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

Ans: My browser(Firefox) is running HTTP version 1.1.The request header contains the information of this version.

The server is also of HTTP version 1.1 and can be seen in the header of HTTP response.





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

Ans: It can be seen in the response packet as shown below:



3) How to tell ping to exit after a specified number of ECHO\_REQUEST packets?

Ans: It can be done by using following command:

ping -c 15 [www.google.com](http://www.google.com)

Here no. of ECHO\_REQUEST packets is 15.

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

Ans: The server field in the HTTP response object stores the remote host app or server on which it is hosted.

Alternatively it can be found using the following command:

nmap -O -v [www.flipkart.com](http://www.flipkart.com)