Laboratory

**Question1: Browse google.com and capture HTTP packets using Wireshark**

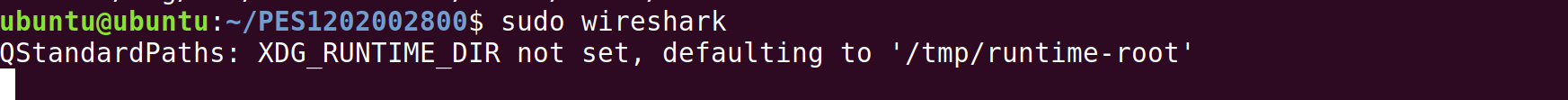
**observation:** Analyze HTTP request and HTTP response and write in your observation

|  |  |
| --- | --- |
| **GET** |  |
| **HOST** |  |
| **USER-AGENT** |  |
| **ACCEPT-LANGUAGE** |  |
| **CACHE-CONTROL** |  |
| **PRAGMA** |  |
| **CONNECTION** |  |

Solution:

step 1: open terminal (CTRL-ALT-T)

sudo Wireshark

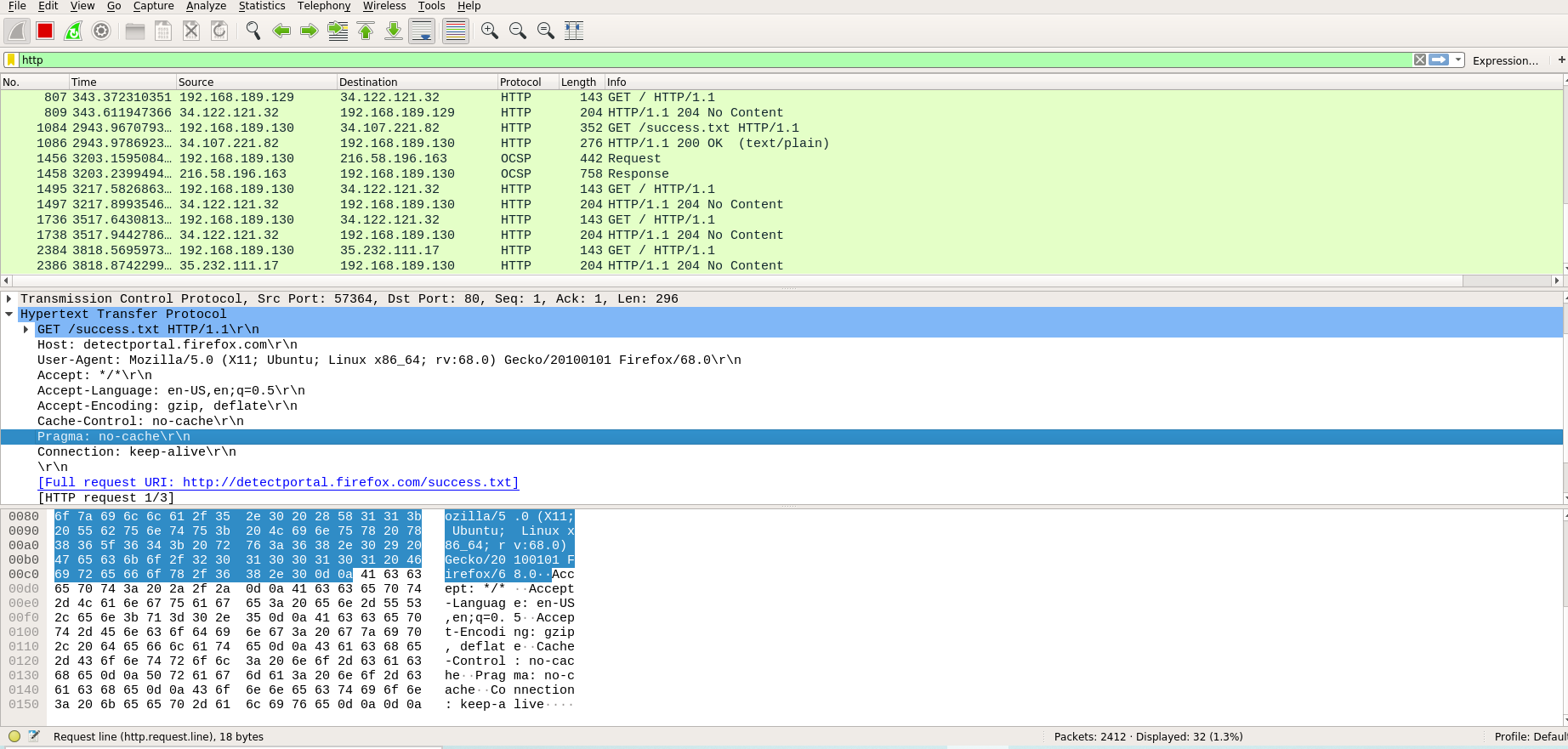


step 2: select any interfaces step 3: set filter as HTTP

step 4 : open Firefox Mozilla browser only [www.google.com](http://www.google.com/)

step 5: switch to Wireshark

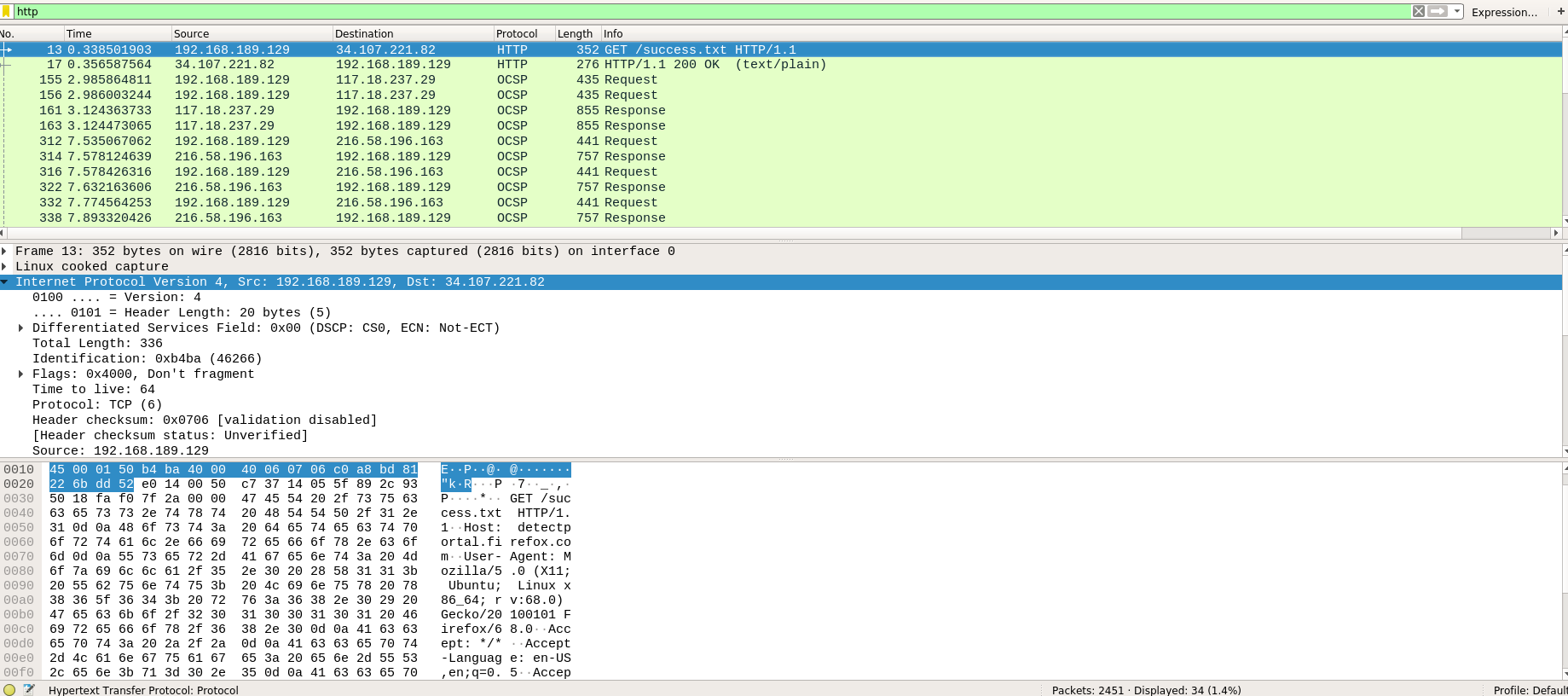
step 6: now you can see http packets .click on http packet and analyse the following

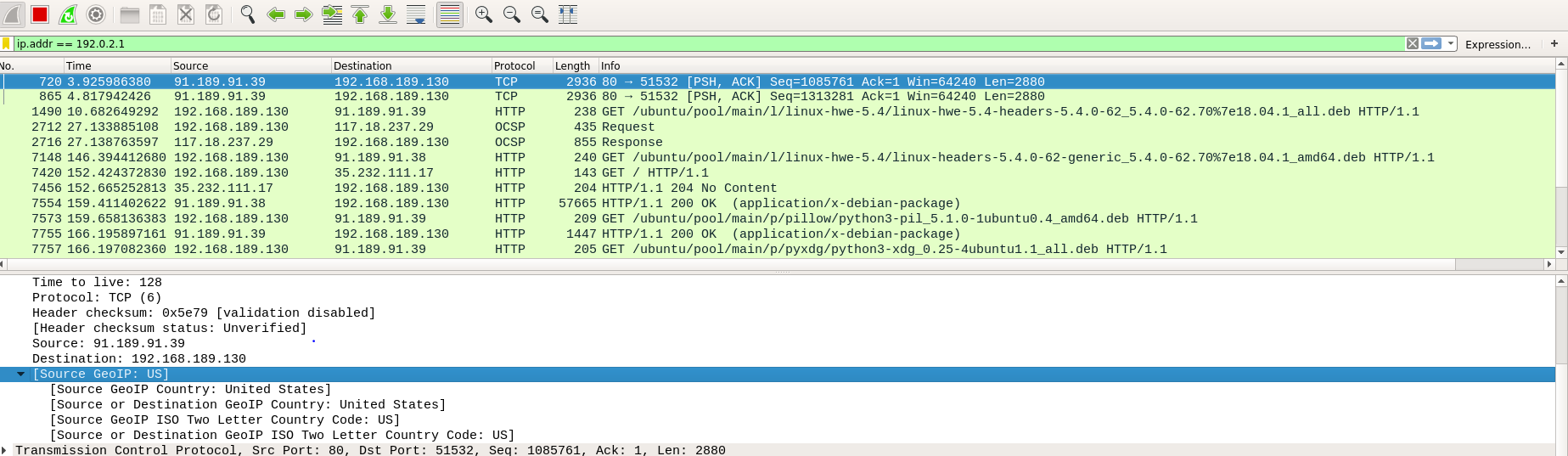


1. **HTTP packet header**

|  |  |
| --- | --- |
| **GET** | GET /success.txt HTTP/1.1\r\n |
| **HOST** | detectportal.firefox.com\r\n |
| **USER-AGENT** | Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:68.0) Gecko/20100101 Firefox/68.0\r\n |
| **ACCEPT-LANGUAGE** | en-US,en;q=0.5\r\n |
| **CACHE-CONTROL** | no-cache\r\n |
| **PRAGMA** | no-cache\r\n |
| **CONNECTION** | keep-alive\r\n |

1. **IPV4 packet**





|  |  |
| --- | --- |
| **VERSION** | 4 |
| **SOURCE IP ADDRESS** | 192.168.189.130 |
| **DESTINATION IP ADDRESS** | 34.107.221.82 |
| **SOURCE GEO IP** | United States |
| **DESTINATION GEO IP** | United States |

Question2: Assign ip address to the system(HOST) and test the connection.

NOTE: ip address of your system must be 10.0.0.your-usn.

for eg: your usn is 001 then your system ip address is 10.0.0.1

Observation: Analyse the icmp packets captured in the wireshark and tcpdump.

Solution:

step 1: sudo ip addr show

analyze and note the following :

interface available and its names



ip address table:

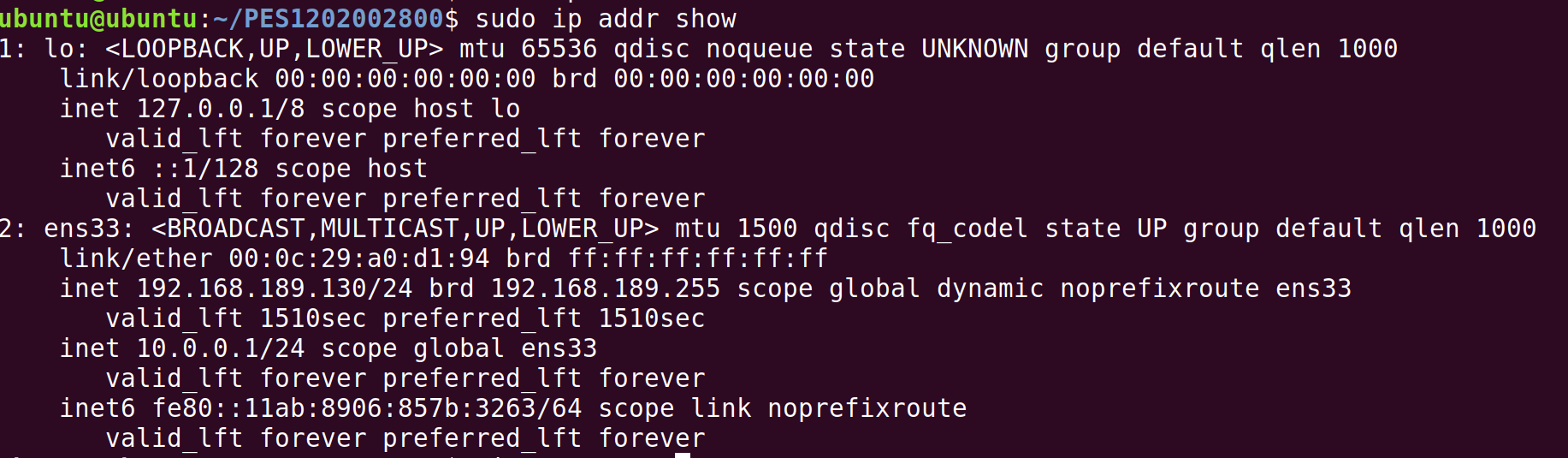
|  |  |  |
| --- | --- | --- |
| Interface name | Ip address | Mac address |
| lo | 127.0.0.1 | 00:00:00:00:00:00 | 00:00:00:00:00:00 |
| ens33 | 192.168.189.130 | 00:0c:29:a0:d1:94 |
|  |  |  |
|  |  |  |

Step 2: sudo ip addr add 10.0.0.your-usn/24 dev interface-name

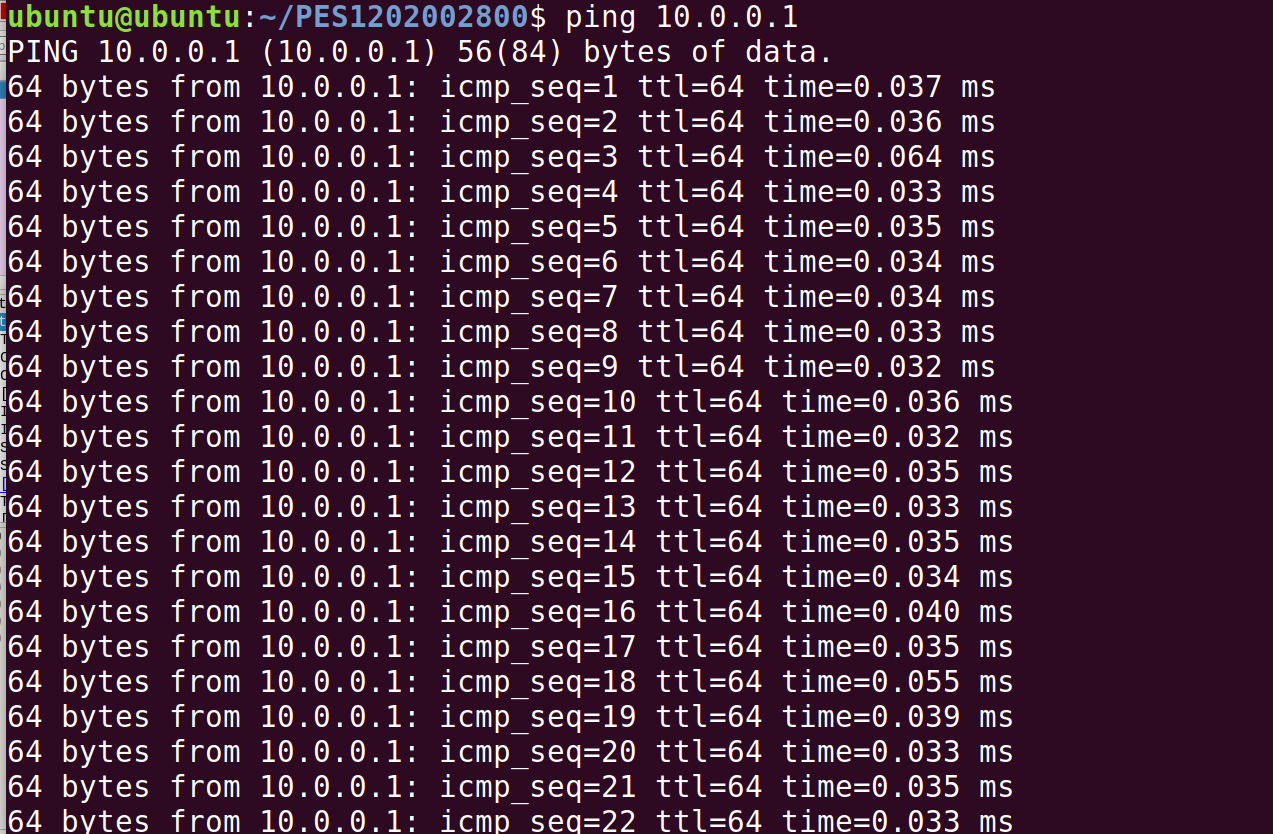
Interface: ens33



step 3: sudo ip addr



Step 4: ping 10.0.0.your-usn



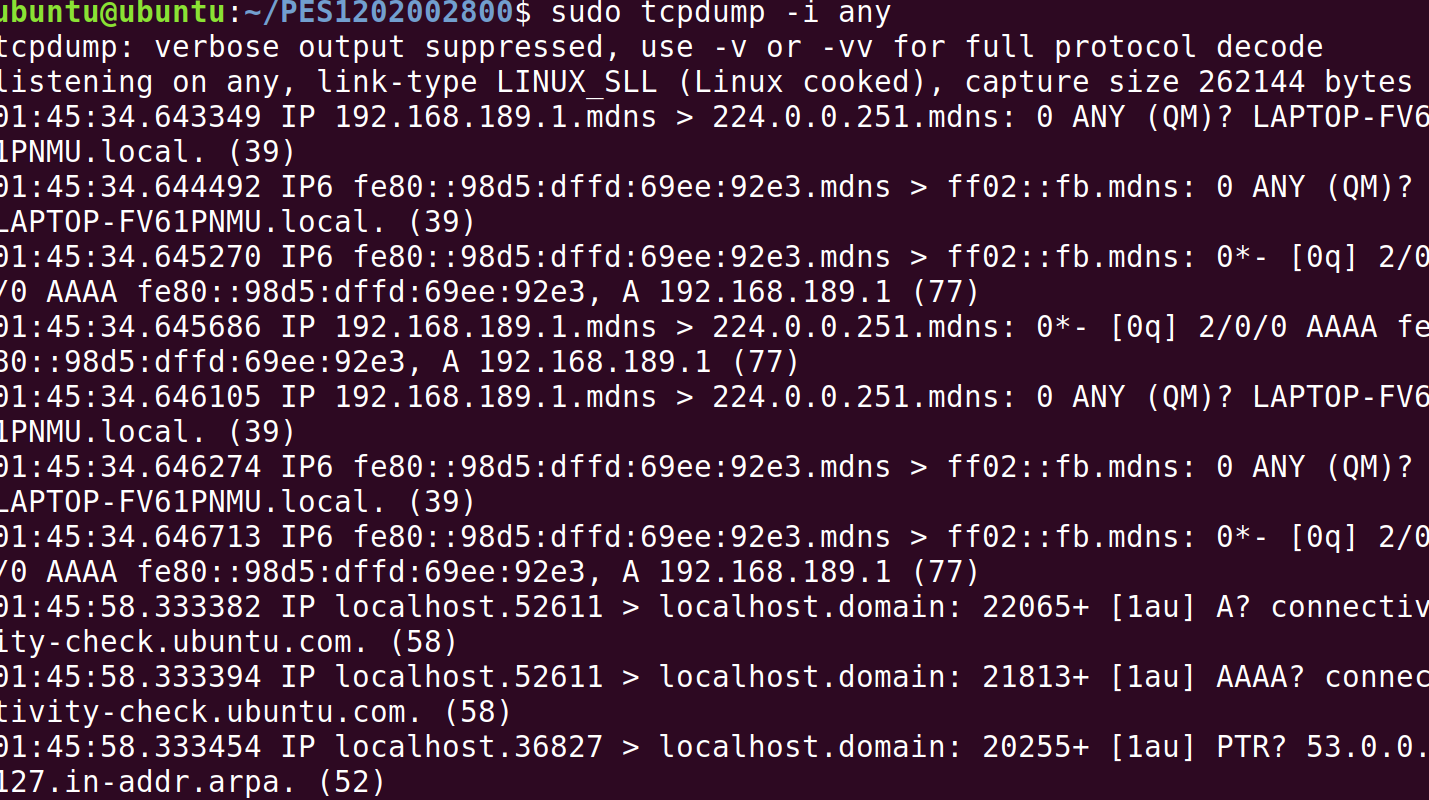
Step 5: Analyze packet and its attributes 1)TTL 2) PROTOCOL 3) TIME



step 6: sudo tcpdump -i any



This program allows you to dump the traffic on a network. tcpdump is able to examine IPv4, ICMPv4, IPv6, ICMPv6, UDP, TCP, SNMP, AFS BGP, RIP, PIM, DVMRP, IGMP, SMB, OSPF, NFS and many other packet types.  
  
It can be used to print out the headers of packets on a network interface, filter packets that match a certain expression. You can use this tool to track down network problems, to detect attacks or to monitor network activities.



Question3: Establish client and server communication

**I) Intra system communication(Using 2 terminals in the same system) step 1:** open terminal (Ctrl-Alt-T)

In Terminal1:**(Act as a SERVER)**

**step 2:** nc -l portno

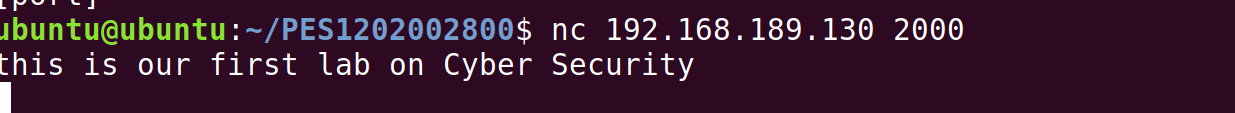


NOTE: give any number i.e., 2000 and same number you need to give in the terminal 2

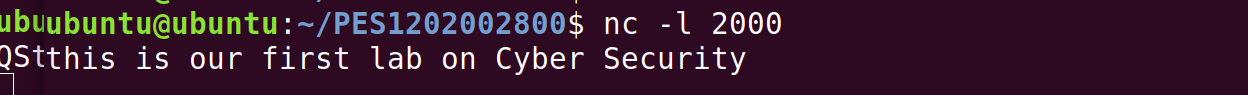
**step 3:** open terminal (Ctrl-Alt-T) In Terminal 2:**(Act as a CLIENT)**

**step 4:** nc <your-system-ip-address> portno

Note:portno should be common in both the terminals for eg., here also 2000



**step 5:** type anything in client will appear in server



**II)Inter system communication(Using 2 systems) step 1:** open terminal (Ctrl-Alt-T)

In System1:**(Act as a SERVER) step 2:** nc -l portno

NOTE: give any number i.e., 2000 and same number you need to give in the terminal 2

**step 3:** open terminal (Ctrl-Alt-T) In system 2:**(Act as a CLIENT)**

**step 4:** nc <server-ip-address> portno

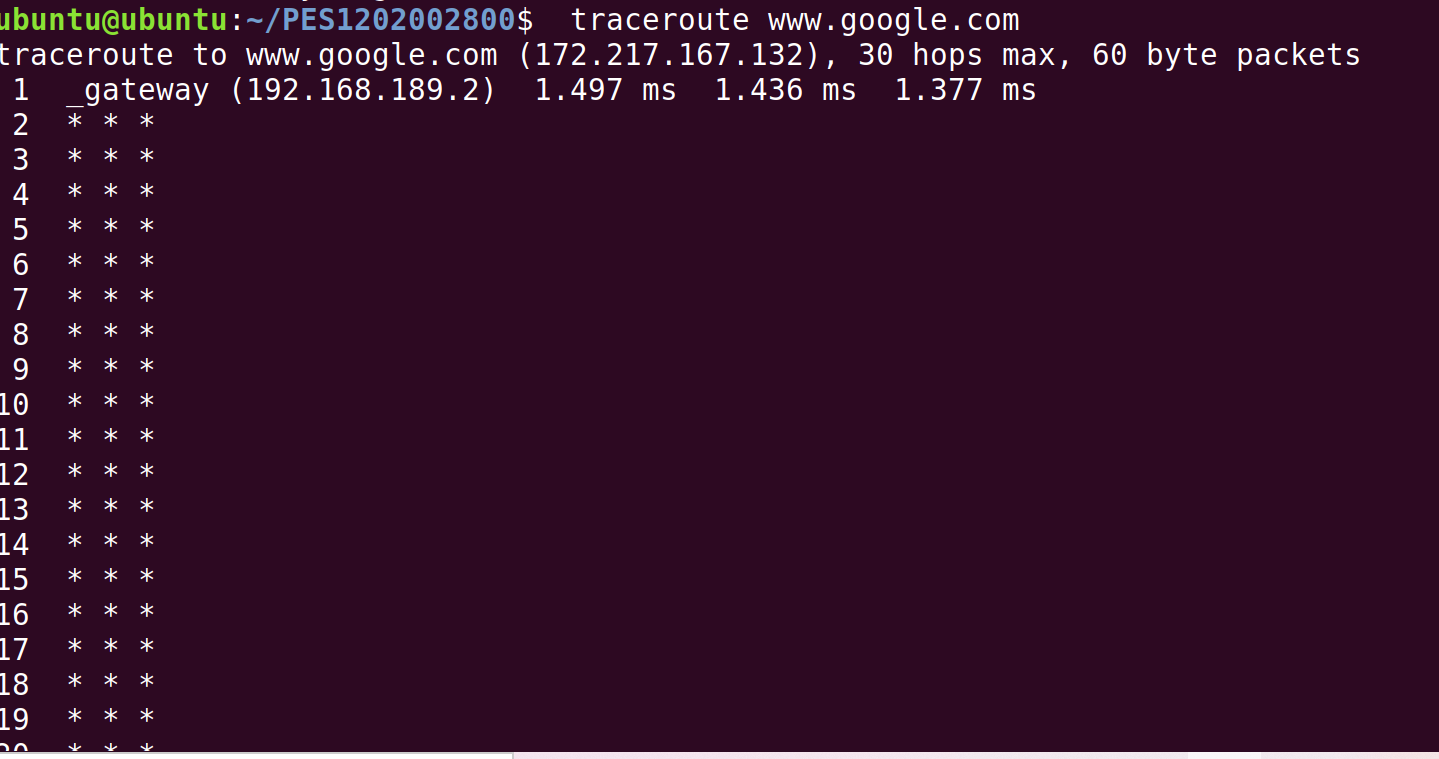
Note:portno should be common in both the terminals for eg., here also 2000

**step 5:** type anything in client will appear in the server terminal

Question4: Use traceroute to google server and and analyse the output

Step 1: traceroute google.com

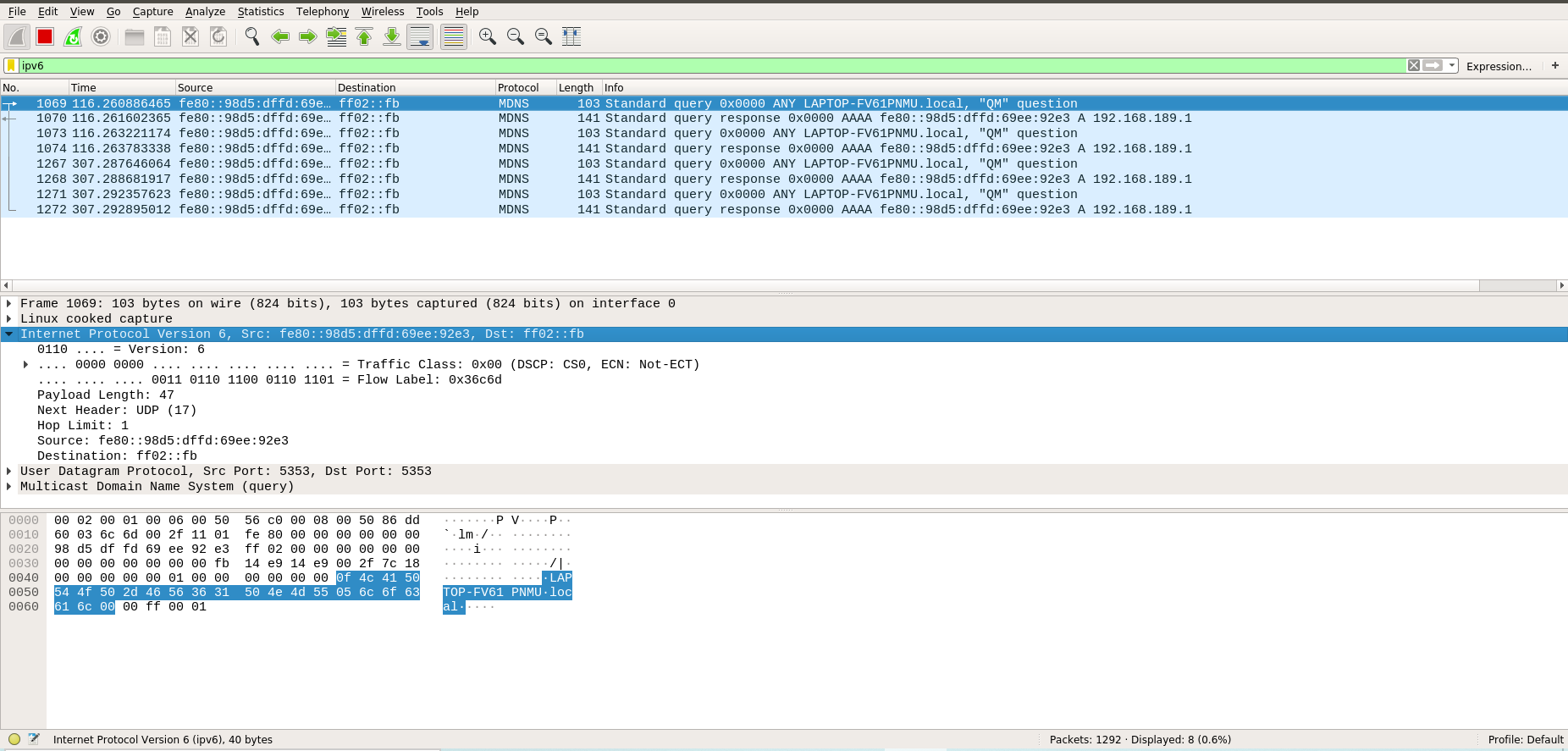
Step 2: analyze destination address of google.com and no of hops



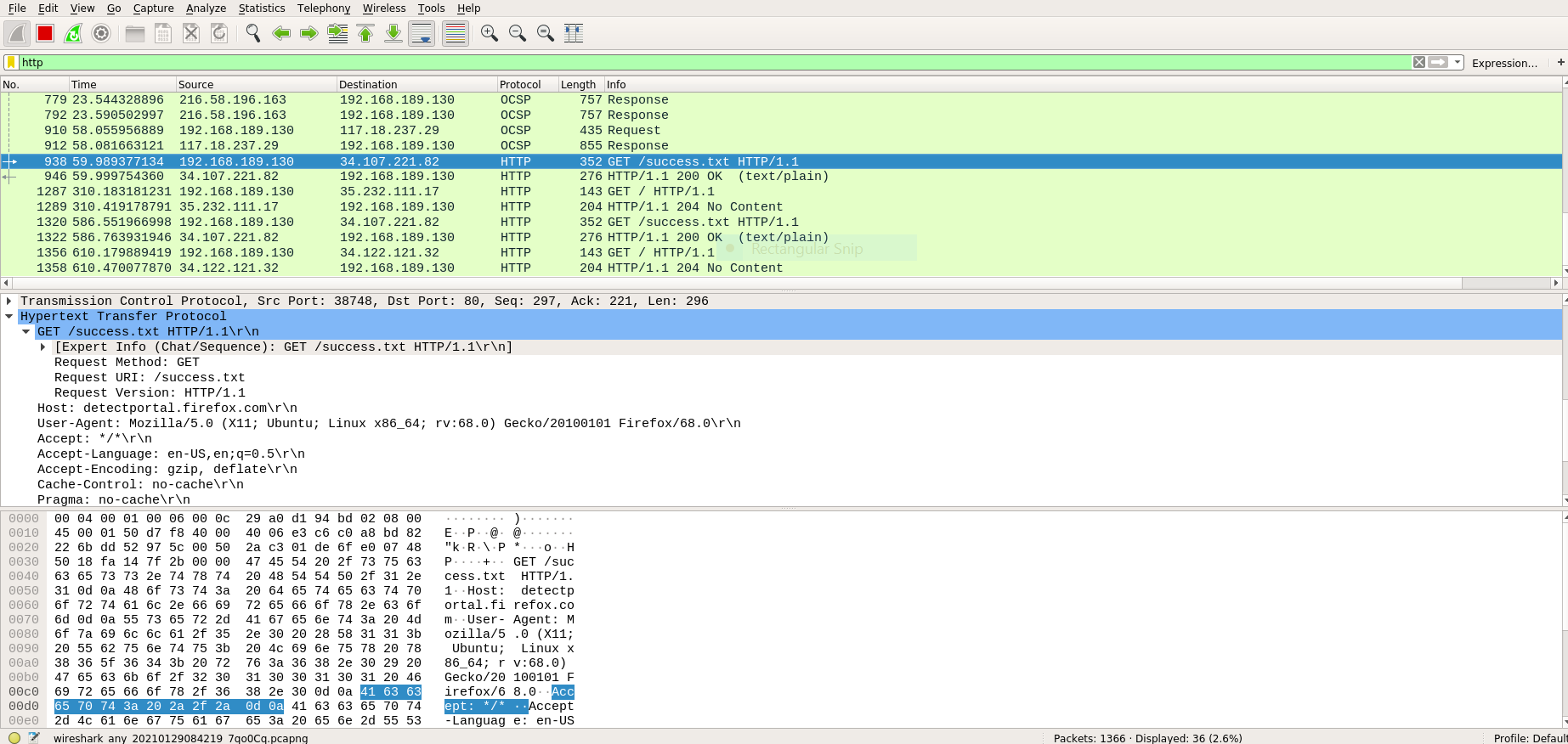
|  |  |
| --- | --- |
| Destination Address | 172.217.167.132 |
| No. of hops | 30 |

Exercise:

**1.capture ipv6 packets and analyze the following**

**ipv6 packet header** 

**HTTP packet header**

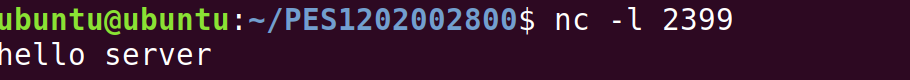


**ipv6 packet header**

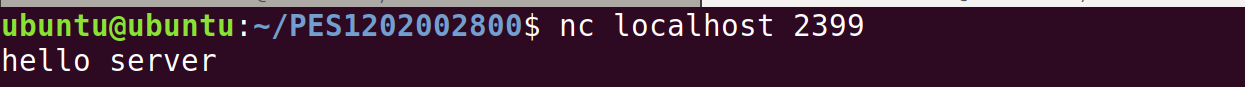
|  |  |
| --- | --- |
| **IPV6** |  |
| **VERSION** | 6 |
| **SOURCE IP ADDRESS** | fe80:98d5:dffd:69ee:92e3 |
| **DESTINATION IP ADDRESS** | ff02::fb |
| **SOURCE GEO IP** | - |
| **DESTINATION GEO IP** | - |
| **HTTP** |  |
| **GET** | /success.txt HTTP/1.1\r\n |
| **HOST** | detectportal.firefox.com\r\n |
| **USER-AGENT** | Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:68.0) Gecko/20100101 Firefox/68.0\r\n |
| **ACCEPT-LANGUAGE** | en-US,en;q=0.5\r\n |
| **CACHE-CONTROL** | no-cache\r\n |
| **PRAGMA** | no-cache\r\n |
| **CONNECTION** | keep-alive\r\n |

1. **can you add more than 1 ip address of same network to same interface?? yes 3.can you add more than 1 ip address to different network same interface?? yes 4.using client server communication ,send data using TCP**

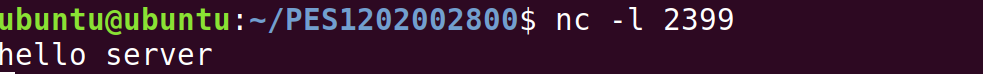
**Server:**



**Client:**

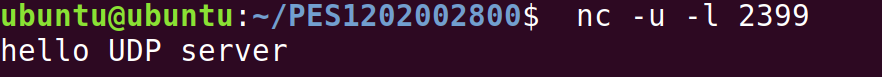


**Server:**

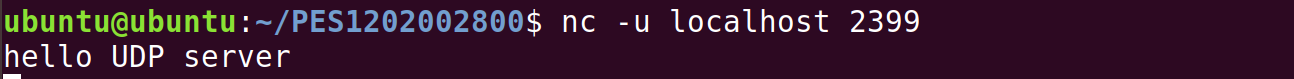


5.using client server communication ,send data using UDP

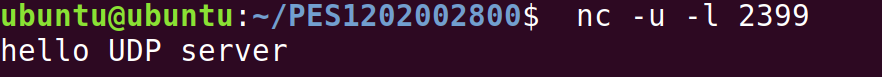
Server:



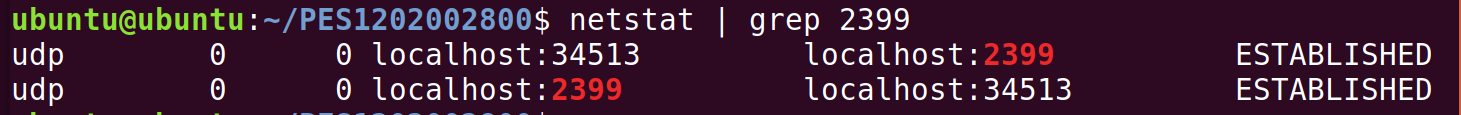
Client:



Server:



To verify communication:



**Week #1**

**Study and understand the basic networking tools - Wireshark, Tcpdump, Ping, Traceroute and Netcat.**

|  |
| --- |
| **Learn and Understand Network Tools**   1. **Wireshark**    * Perform and analyze Ping PDU capture    * Examine HTTP packet capture    * Analyze HTTP packet capture using filter 2. **Netcat**     * Establish communication between client and server    * Transfer files 3. **Tcpdump**    * Capture packets 4. **Ping**    * Test the connectivity between 2 systems 5. **Traceroute**    * Perform traceroute checks 6. **Nmap**     * Explore an entire network |

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

**Step 1:** To display status of all active network interfaces.

**ifconfig** (or) **ip addr show**



Analyze and fill the following table:

**ip address table:**

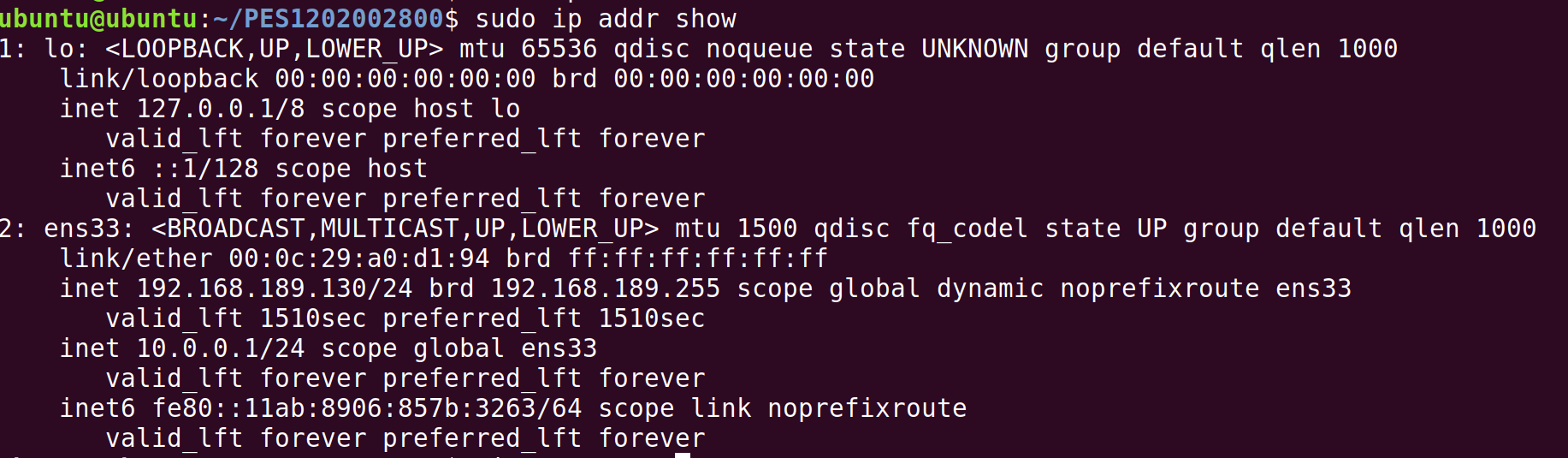
|  |  |  |  |
| --- | --- | --- | --- |
| **Interface name** | **IP address (IPv4 / IPv6)** | **MAC address** |  |
| lo | 127.0.0.1 | 00:00:00:00:00:00 |  |
| Ens33 | 192.168.189.130 | 00:0c:29:a0:d1:94 |  |

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

**sudo ifconfig interface\_name 10.0.0.your\_usn netmask 255.255.255.0**

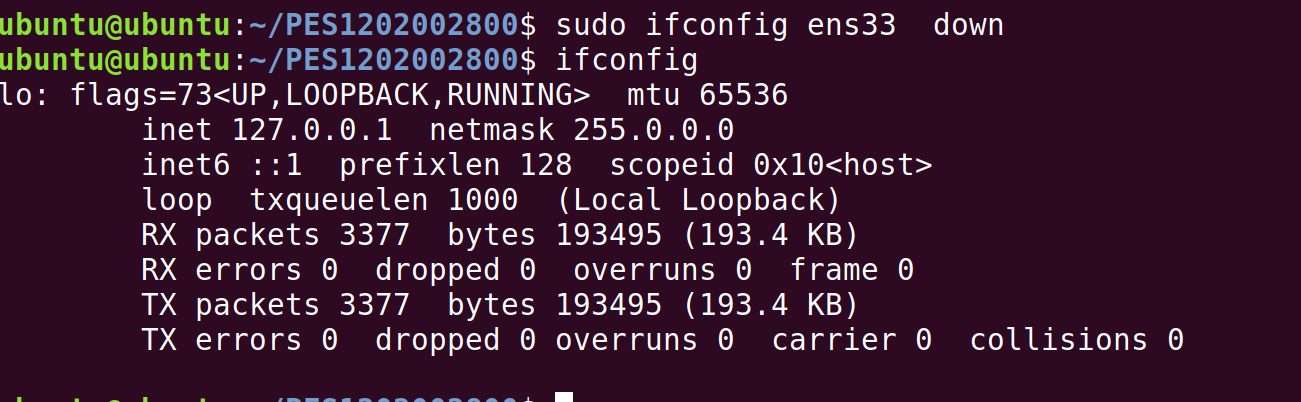
(or) **sudo ip addr add 10.0.0.your\_usn/24 dev interface\_name**



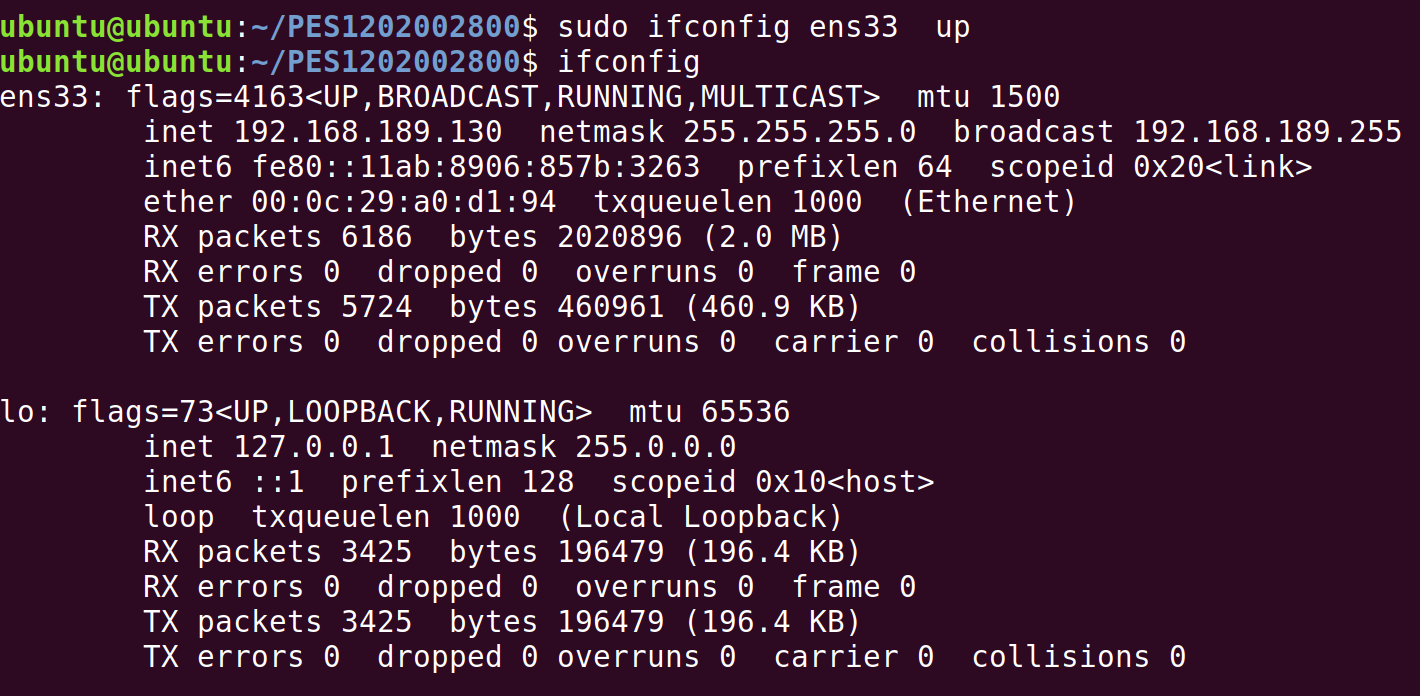


**Step 3:** To activate / deactivate a network interface, type.

**sudo ifconfig down ens33**

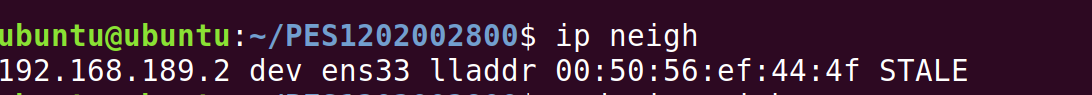


**sudo ifconfig up ens33**



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

**ip neigh**

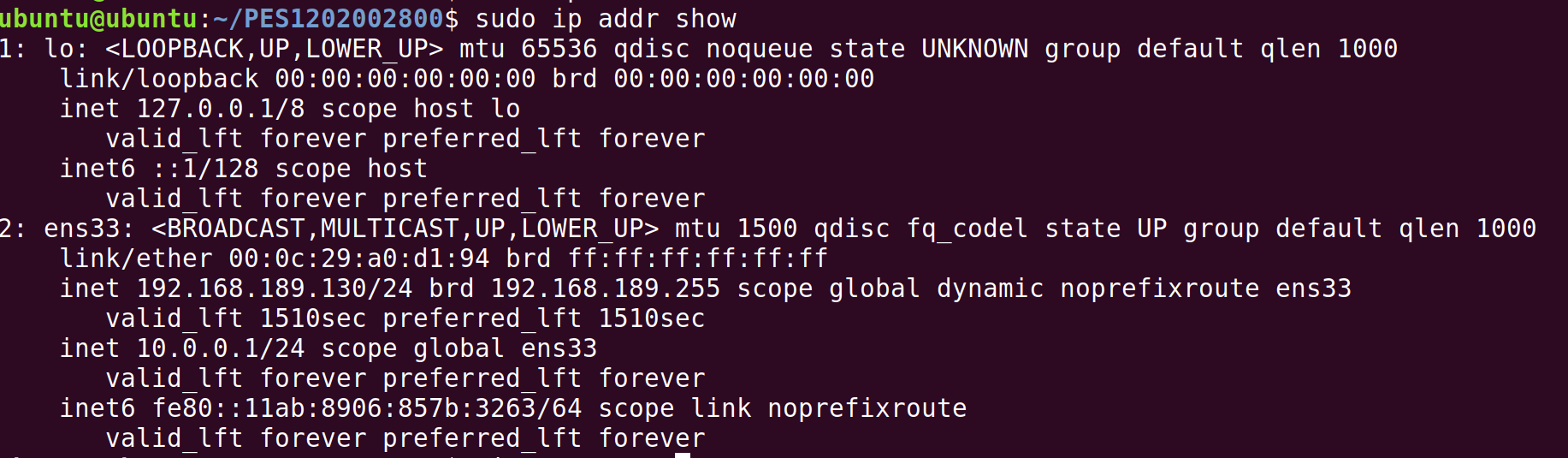


# Task 2: Ping PDU (Packet Data Units or Packets) Capture

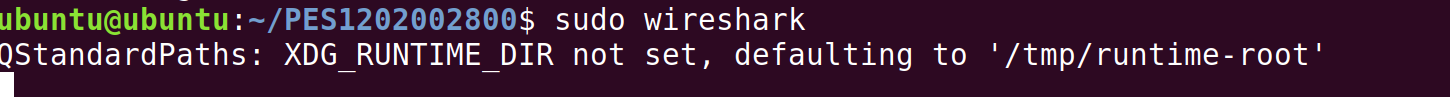
**Step 1:** Assign an IP address to the system (Host).

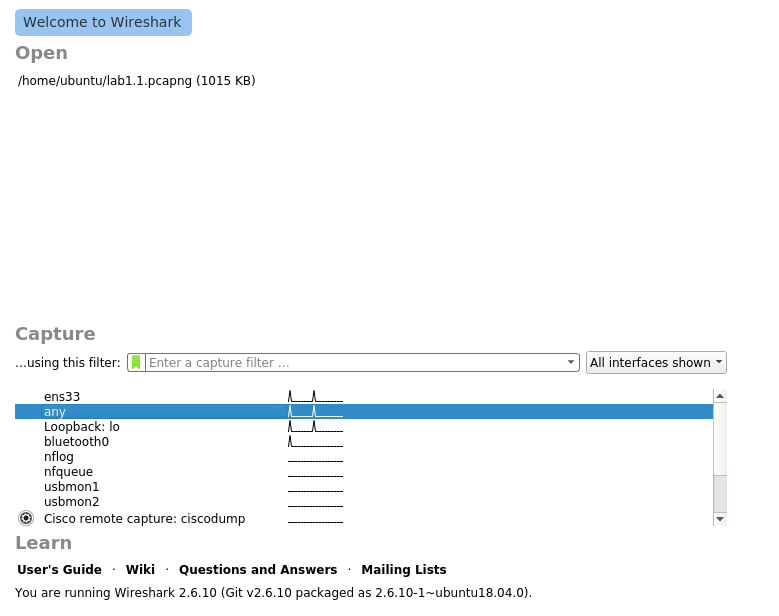


Note: IP address of your system should be 10.0.0.your\_usn. (e.g. if your usn is 001, then your system IP address is 10.0.0.1

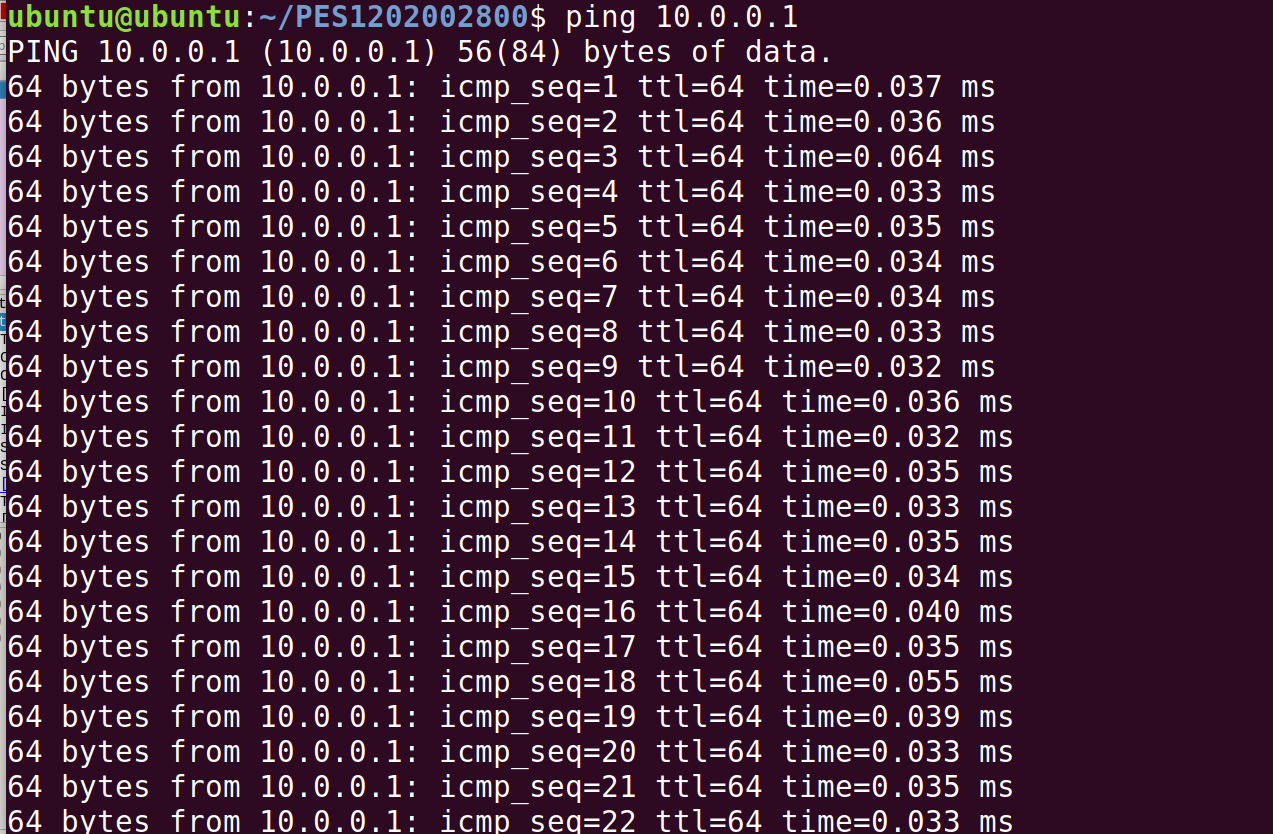


**Step 2:** Launch Wireshark and select ‘any’ interface





**Step 3:** In terminal, type **ping 10.0.0.your\_usn**

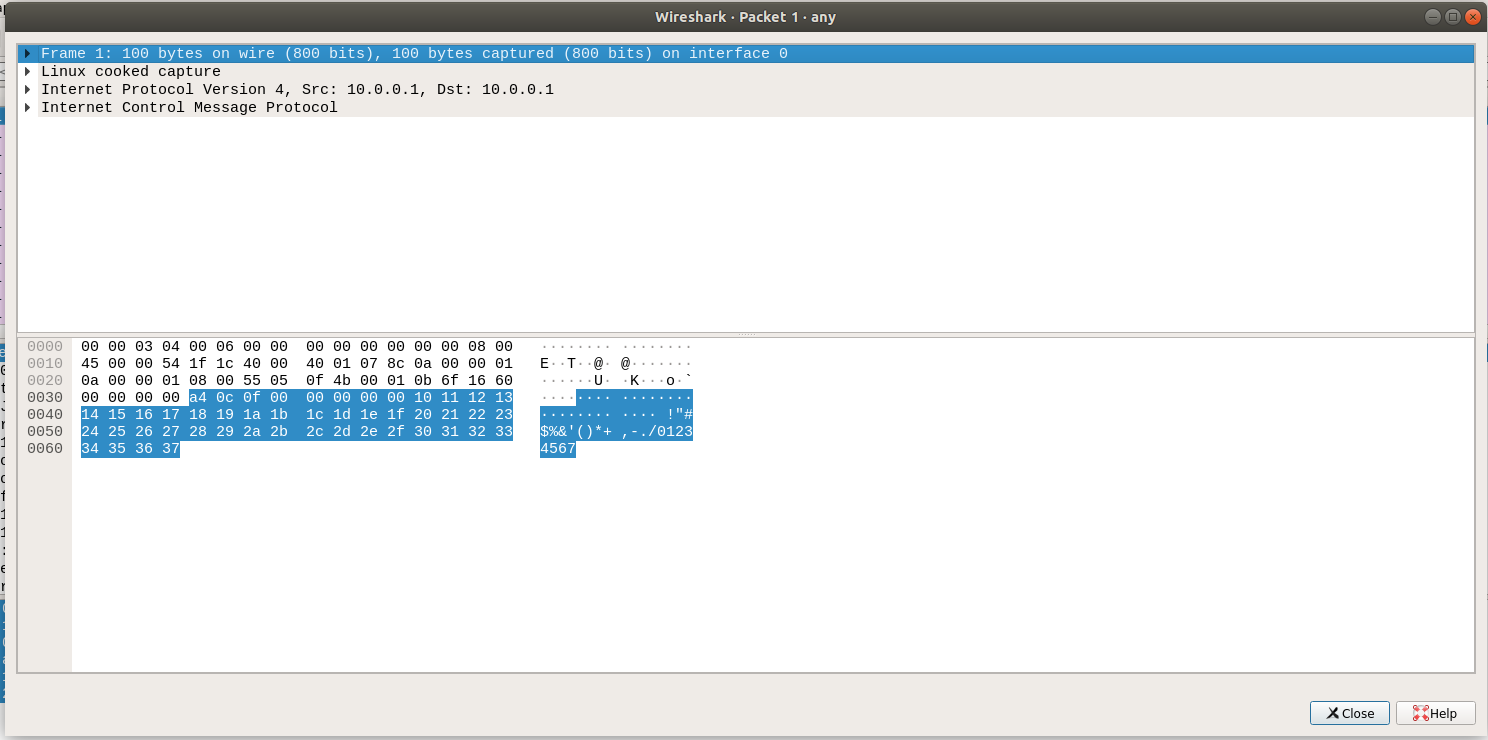


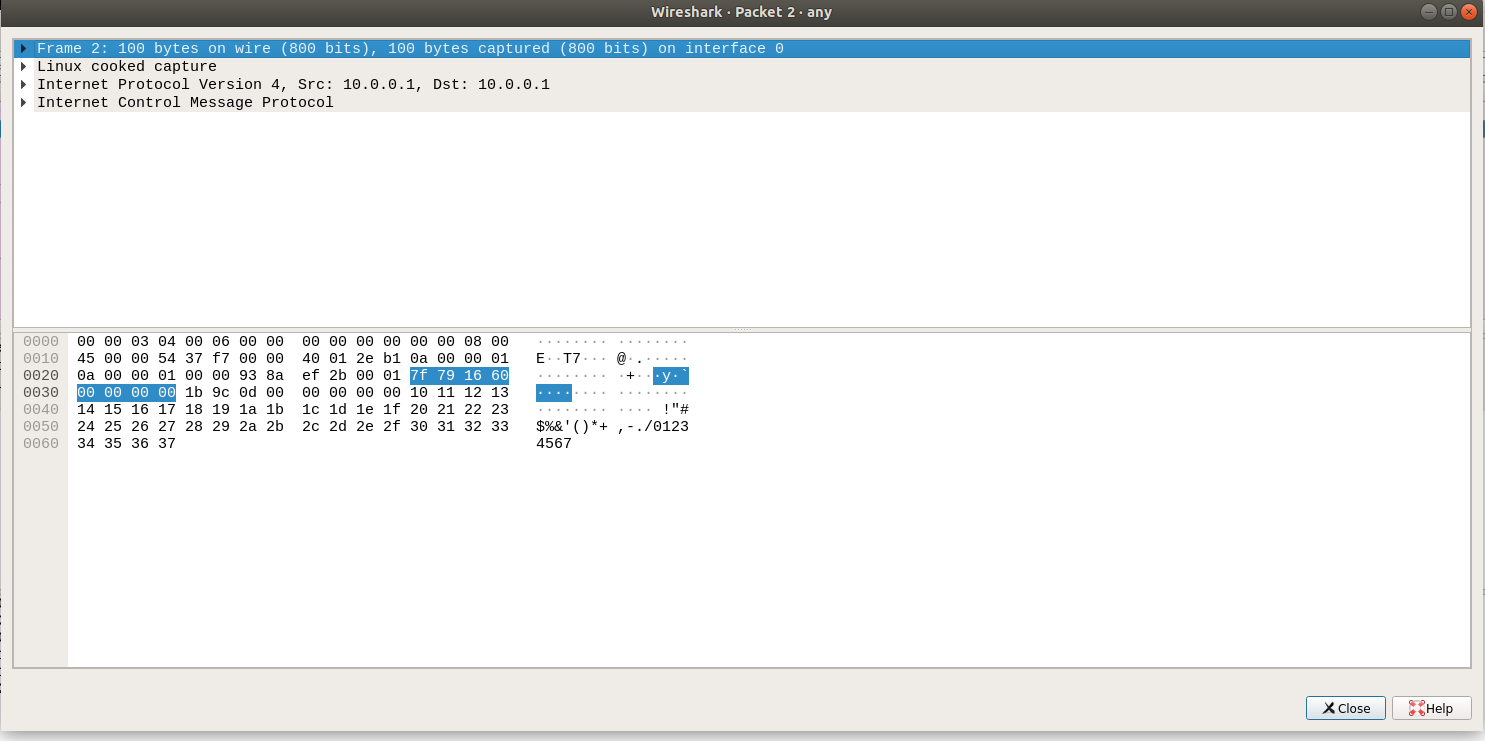
## 

## Observations to be made

**Step 4:** Analyze the following in Terminal

* TTL 🡪64
* Protocol used by ping 🡪ICMP
* Time 🡪2





**Step 5:** Analyze the following in Wireshark

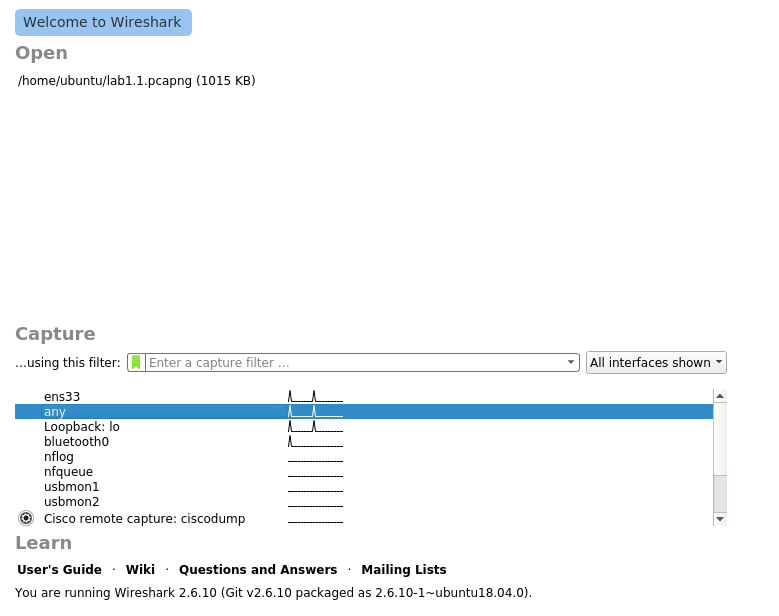
On Packet List Pane, select the first echo packet on the list. On Packet Details Pane, click on each of the four “+” to expand the information. Analyze the frames with the first echo request and echo reply and complete the table below.

|  |  |  |
| --- | --- | --- |
| **Details** | **First Echo Request** | **First Echo Reply** |
| Frame Number | 1 | 2 |
| Source IP address | 10.0.0.1 | 10.0.0.1 |
| Destination IP address | 10.0.0.1 | 10.0.0.1 |
| ICMP Type Value | 8 | 0 |
| ICMP Code Value | 0 | 0 |
| Source Ethernet Address | - | - |
| Destination Ethernet Address | - | - |
| Internet Protocol Version | 4 | 4 |
| Time To Live (TTL) Value | 64 | 64 |

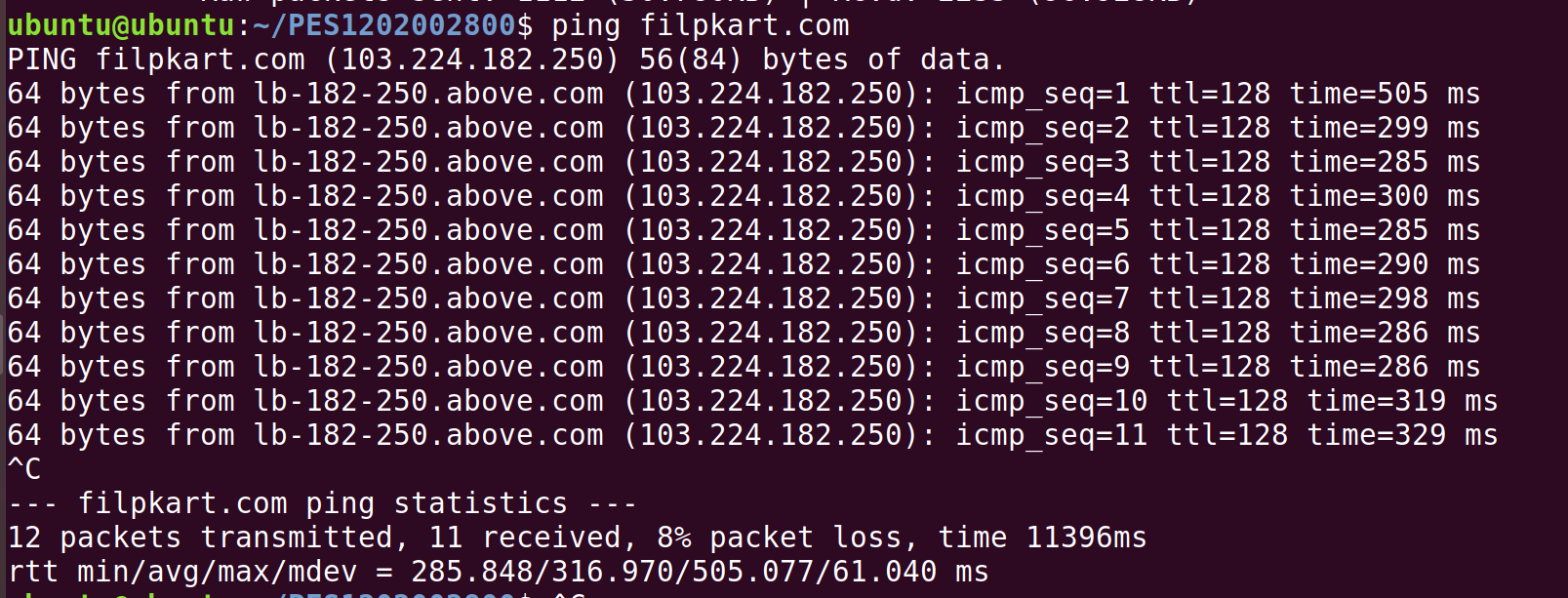
# Task 3: HTTP PDU Capture

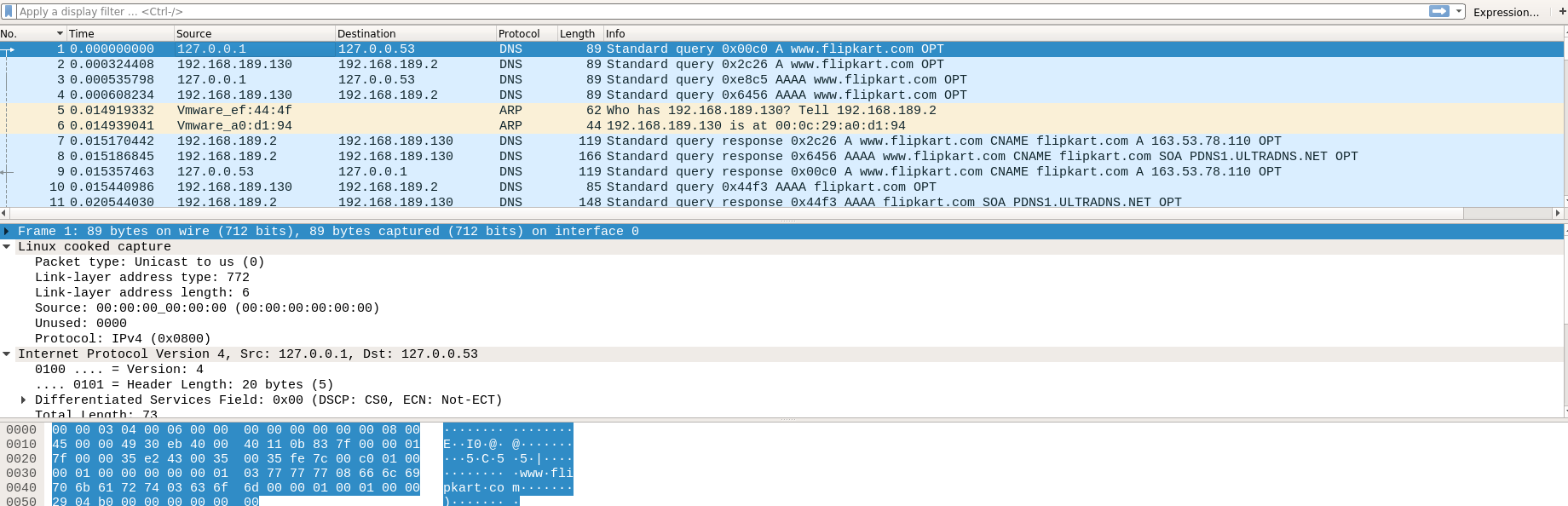
**Using Wireshark’s Filter feature**

**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.flipkart.com](http://www.flipkart.com/)





## Observations to be made

**Step 3:** Analyze the first (interaction of host to the web server) and second frame (response of server to the client). By analyzing the filtered frames, complete the table below:

|  |  |  |
| --- | --- | --- |
| **Details** | **First Echo Request** | **First Echo Reply** |
| Frame Number | 1 | 9 |
| Source Port | 57927 | 57927 |
| Destination Port | 53 | 53 |
| Source IP address | 127.0.0.1 | 127.0.053 |
| Destination IP address | 127.0.0.53 | 127.0.0.1 |
| Source Ethernet Address | - | - |
| Destination Ethernet Address | - | - |

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

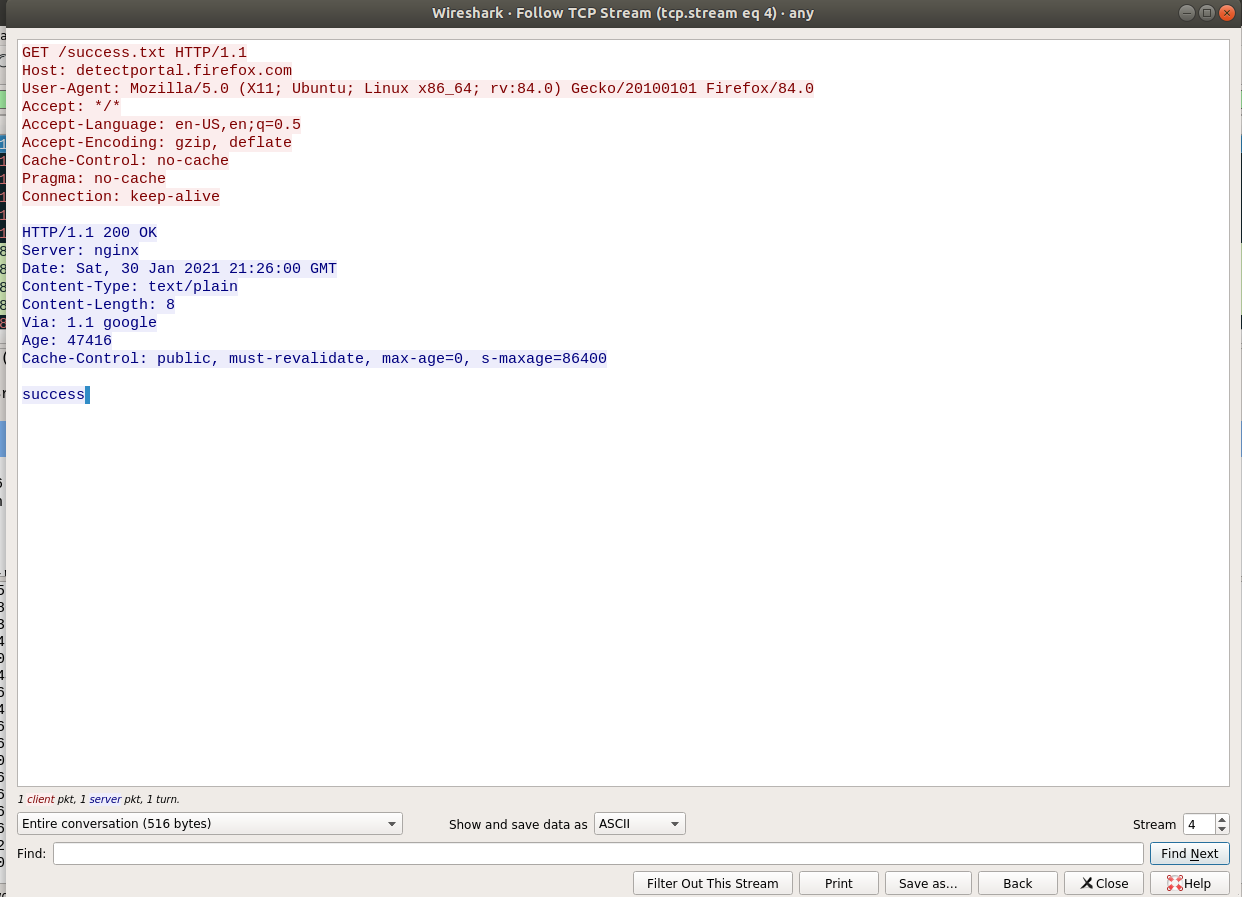
|  |  |  |  |
| --- | --- | --- | --- |
| **HTTP Request** |  | **HTTP Response** |  |
| Get | /success.txt HTTP/1.1 | Server | nginx |
| Host | detectportal.firefox.com | Content-Type | text/plain |
| User-Agent | Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:84.0) Gecko/20100101 Firefox/84.0 | Date | Sat, 30 Jan 2021 21:26:00 GMT |
| Accept-Language | en-US,en;q=0.5 | Location | - |
| Accept-Encoding | gzip, deflate | Content-Length | 8 |
| Connection | keep-alive | Connection | - |

**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.

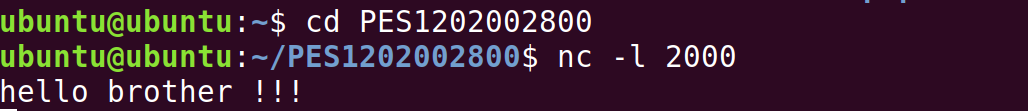


# Task 4 a): Netcat as Chat tool

1. **Intra system communication (Using 2 terminals in the same system)**

**Step 1:** Open a terminal (Ctrl+Alt+T). This will actas a Server.

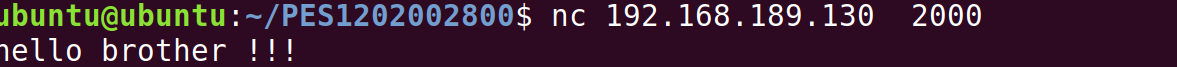
**Step 2:** Type **nc -l any\_portnum** (For eg., nc -l 1234)



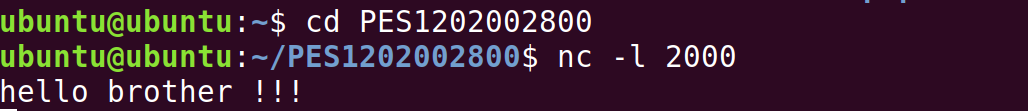
Note: It will goto listening mode

**Step 3:** Open another terminal and this will act as a client.

**Step 4:** Type nc <your-system-ip-address> portnum



Note: portnum should be common in both the terminals (for eg., nc 10.0.2.8 1234) **Step 5:** Type anything in client will appear in server



## b) Inter system communication (Using 2 systems)

Setup a simple switched network of 2 PCs with one acting as Web server. Assign IP addresses for both PCs. Set the capture option as described above.

**Step 1:** Open terminal on Server machine (Machine 1).

## Step 2: Type nc -l any\_portnum

**Step 3:** Open terminal on the Client machine (Machine 2)

**Step 4:** Typenc <server-ip-address> portnum

**Step 5:** Type anything in client will appear in the server terminal

# Task 4 b): Use Netcat to Transfer Files

The netcat utility can also be used to transfer files.

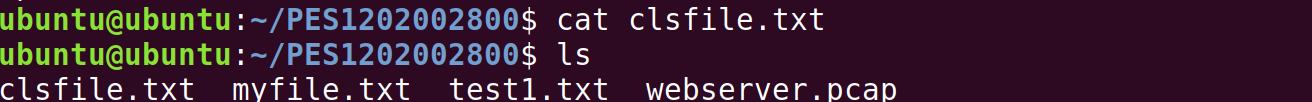
Server:



Client:

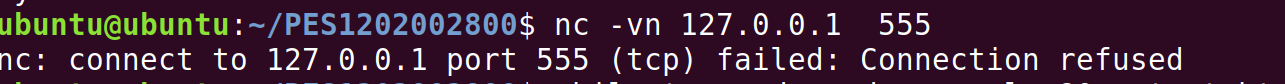


Server:



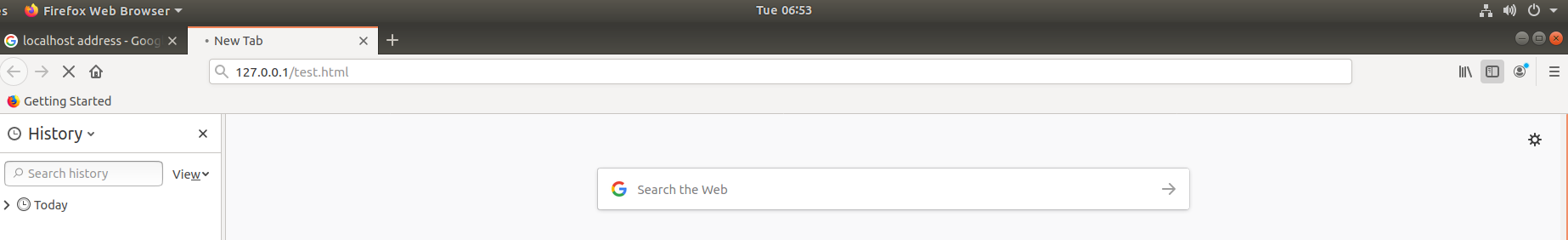
# Task 4 c): Other Commands

1. To test if a particular TCP port of a remote host is open.



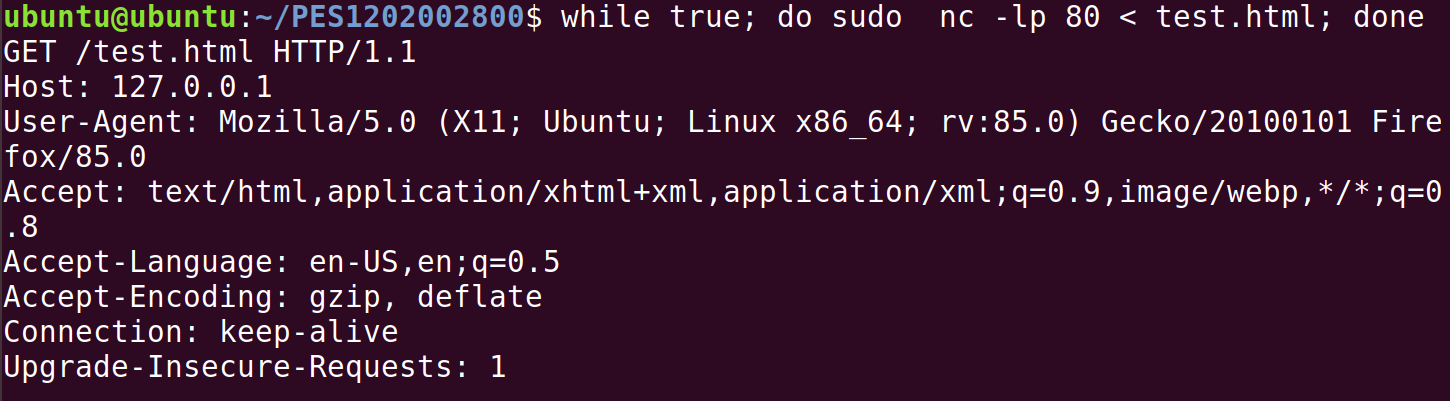
1. Run a web server with a static web page.

**Step 1:** Run the command below on local host (e.g. 10.0.2.8) to start a web server that serves test.html on port 80. **while true; do sudo nc -lp 80 < test.html; done**



**Step 2:** Now open **http://10.0.2.8/test.html** from another host to access it.

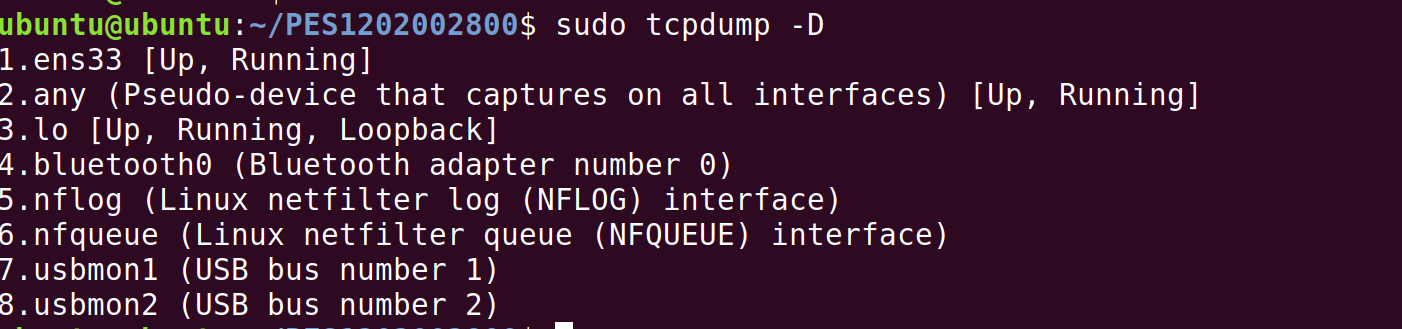
**Step 3:** Observe the details on the terminal



# Task 5: Capturing packets with tcpdump

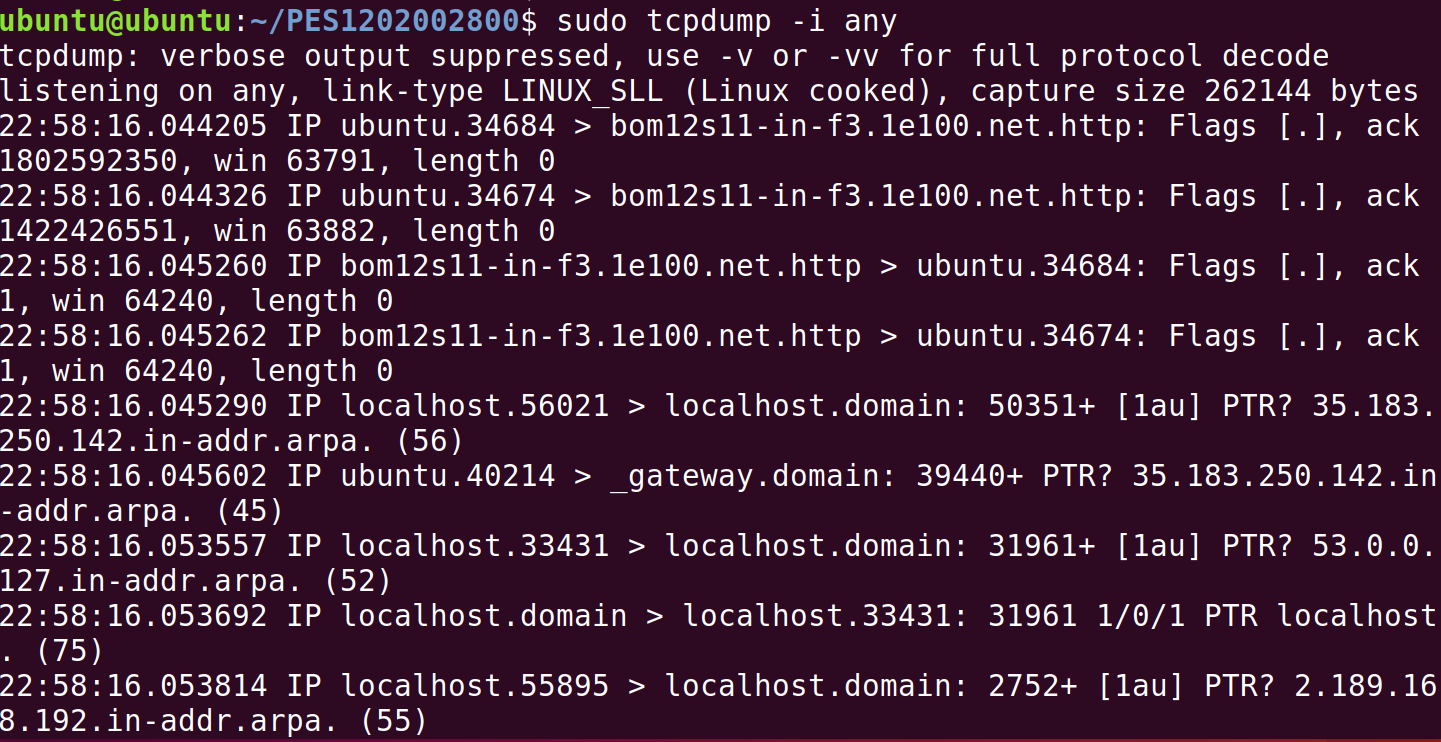
**Step 1:** Use the command **tcpdump -D** to see which interfaces are available for capture.

**sudo tcpdump -D**



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

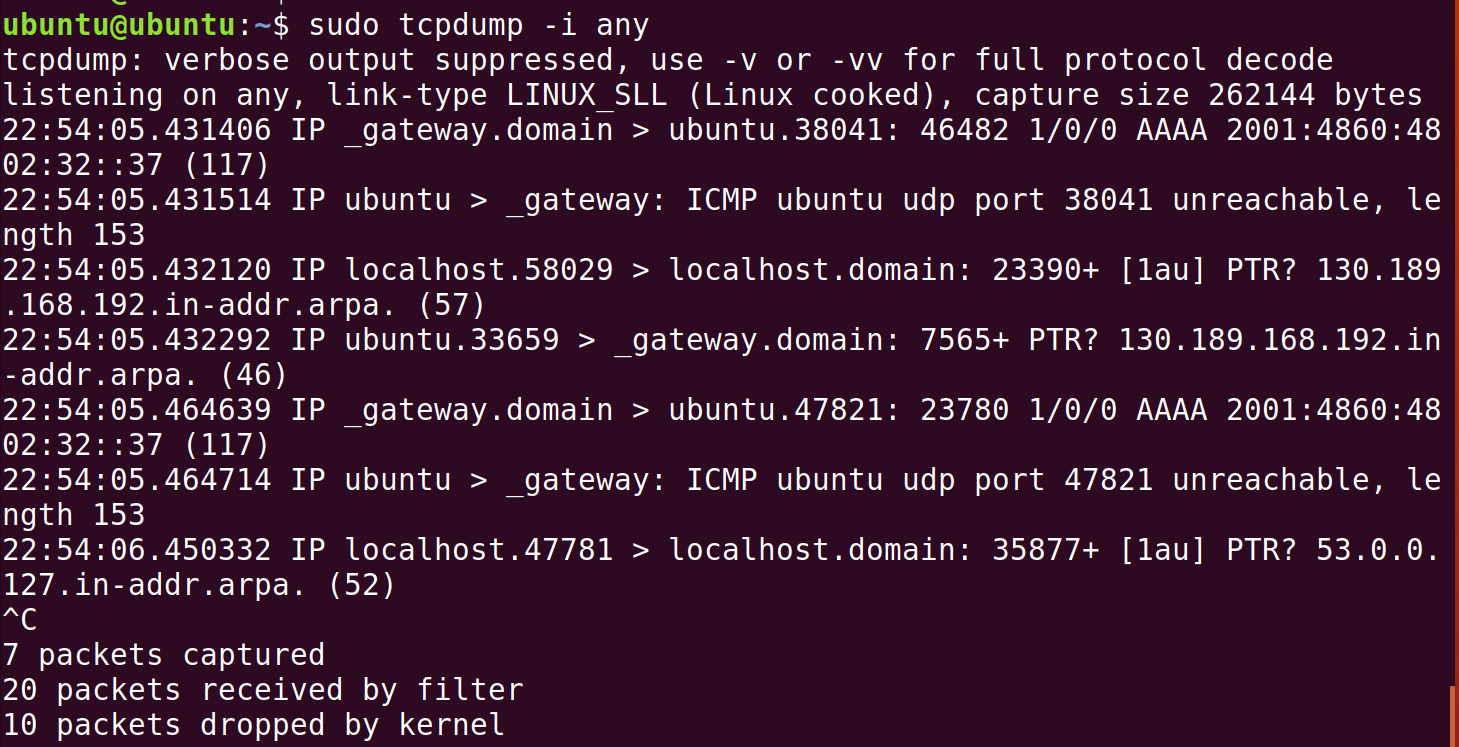
## sudo tcpdump -i any



Note: Perform some pinging operation while giving above command. Also type [www.google.com](http://www.google.com/) in browser.

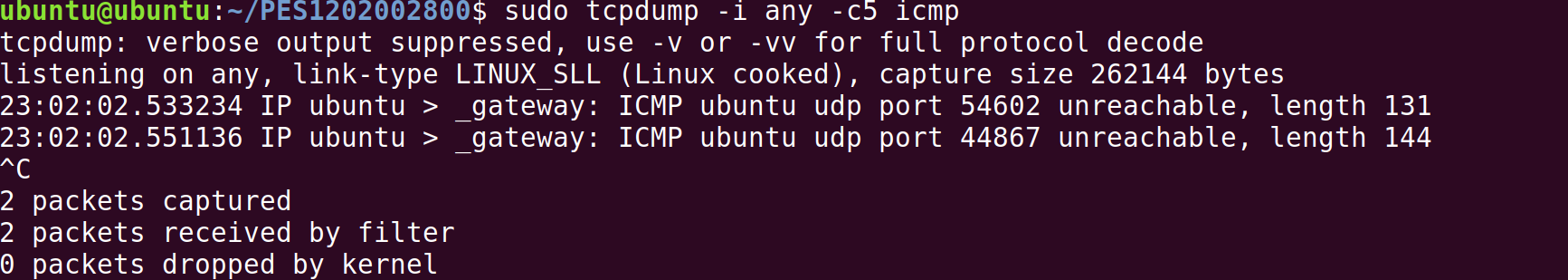
## Observation

**Step 3:** Understand the output format.



**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 -c5 icmp

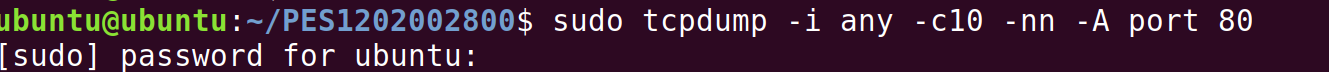


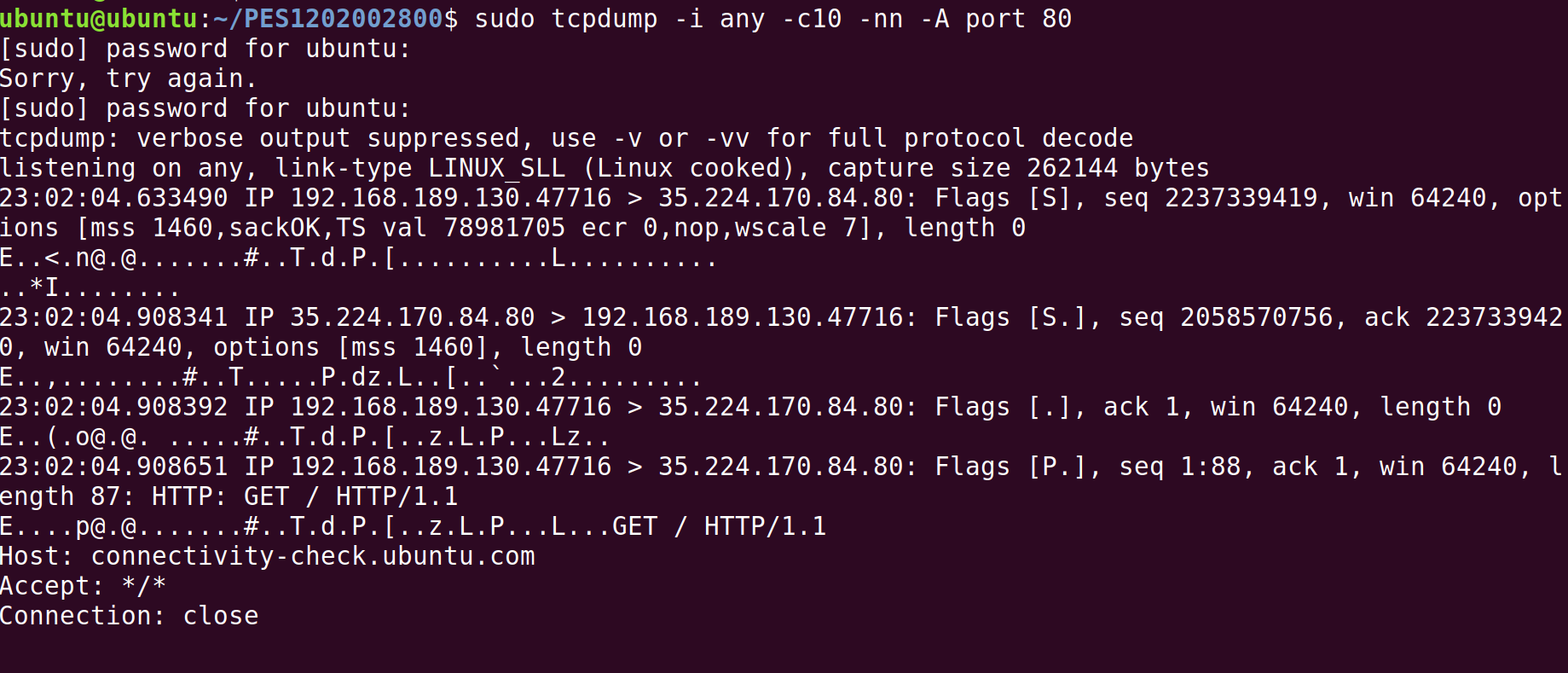
**Step 5:** Check the packet content. For example, inspect the HTTP content of a web request like this:

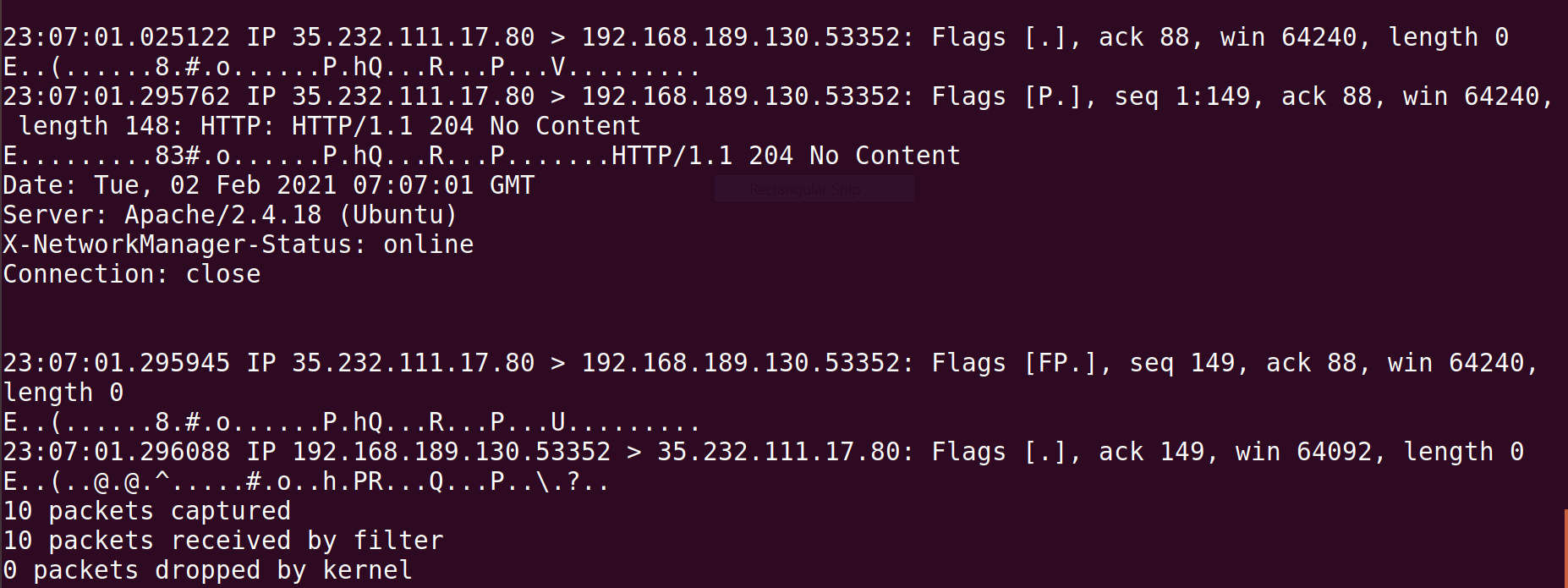
## sudo tcpdump -i any -c10 -nn -A port 80

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

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



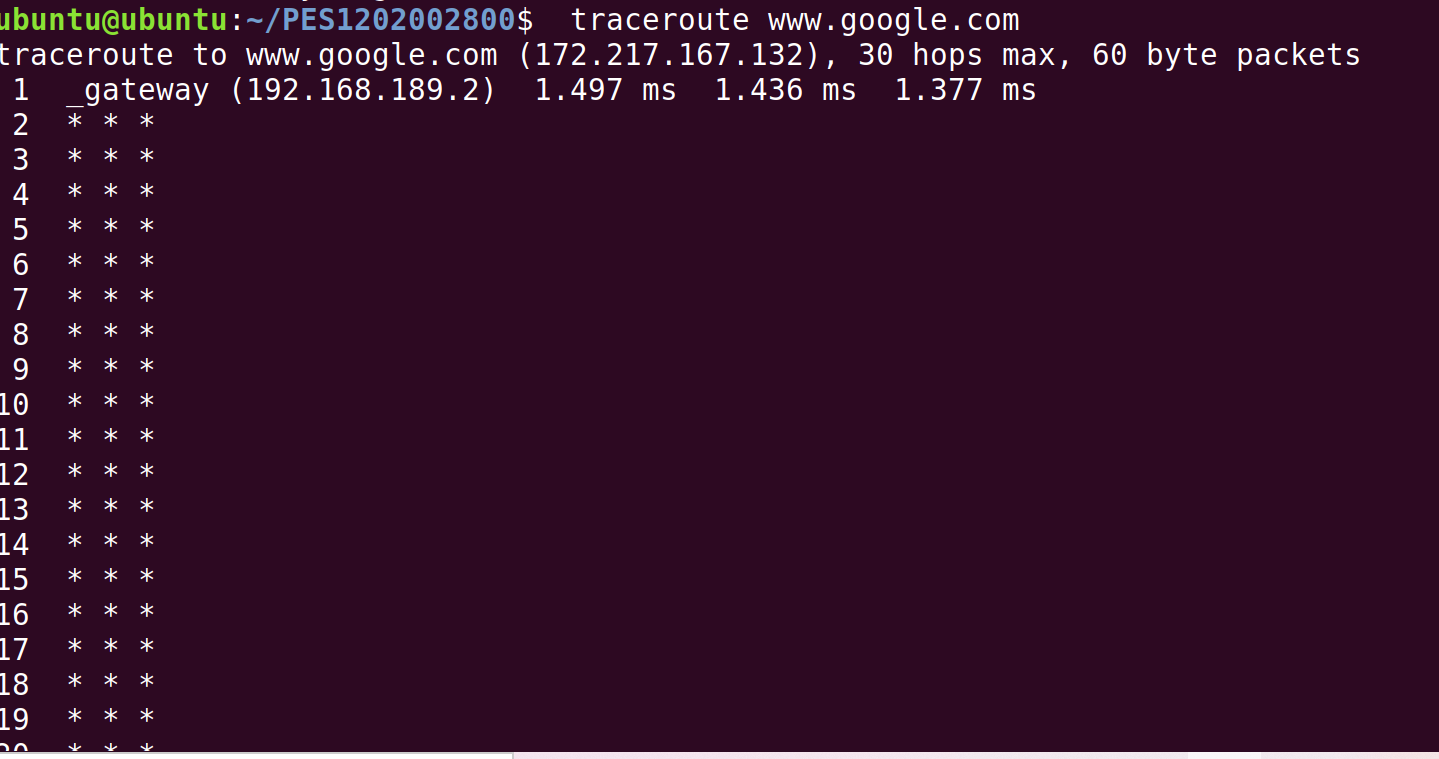




# Task 6: Perform Traceroute checks

**Step 1:** Run the traceroute using the following command.

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



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

* Destination address:172.217.26.196
* No. of hopes:30

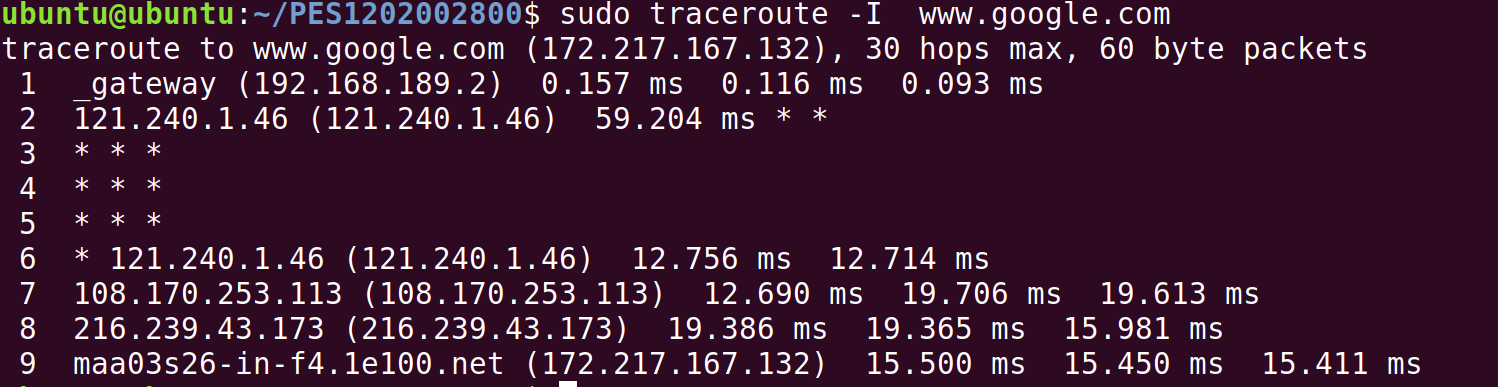
**Step 3:** To speed up the process, you can disable the mapping of IP addresses with hostnames by using the *-n* option

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



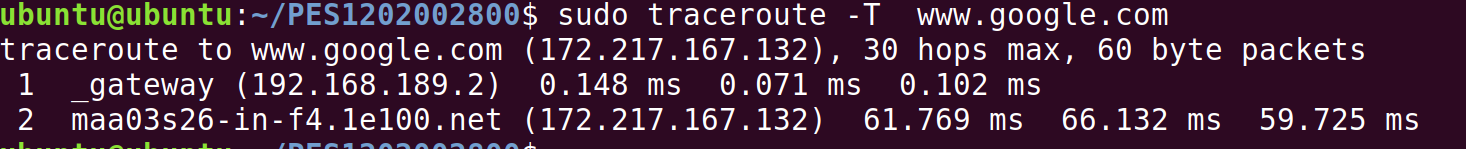
**Step 4:** The -I option is necessary so that the traceroute uses [ICMP.](https://en.wikipedia.org/wiki/Internet_Control_Message_Protocol)

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



# Task 7: 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.pes.edu**](http://www.pes.edu/)

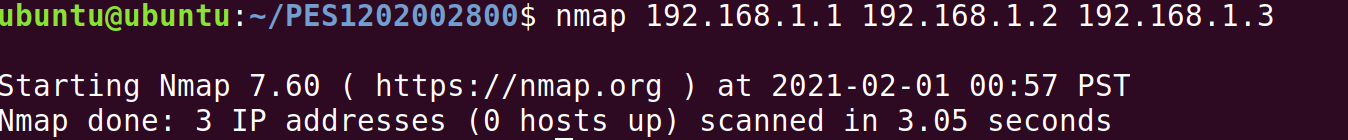


**Step 2:** Alternatively, use an IP address to scan.

## nmap 163.53.78.128

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

**nmap 192.168.1.1 192.168.1.2 192.168.1.3**

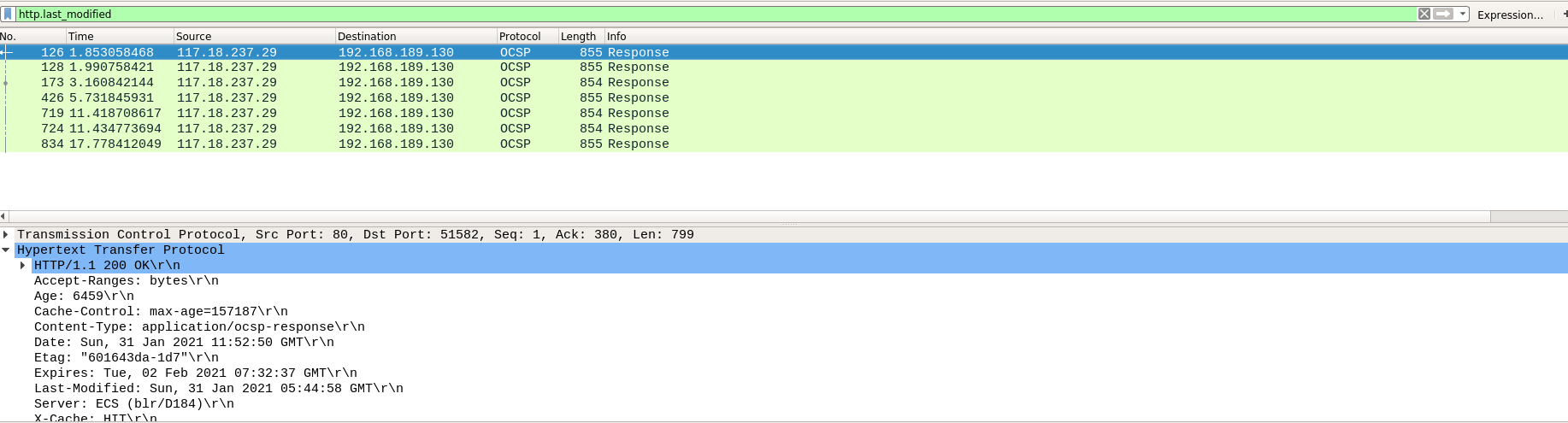


**Questions on above observations:**

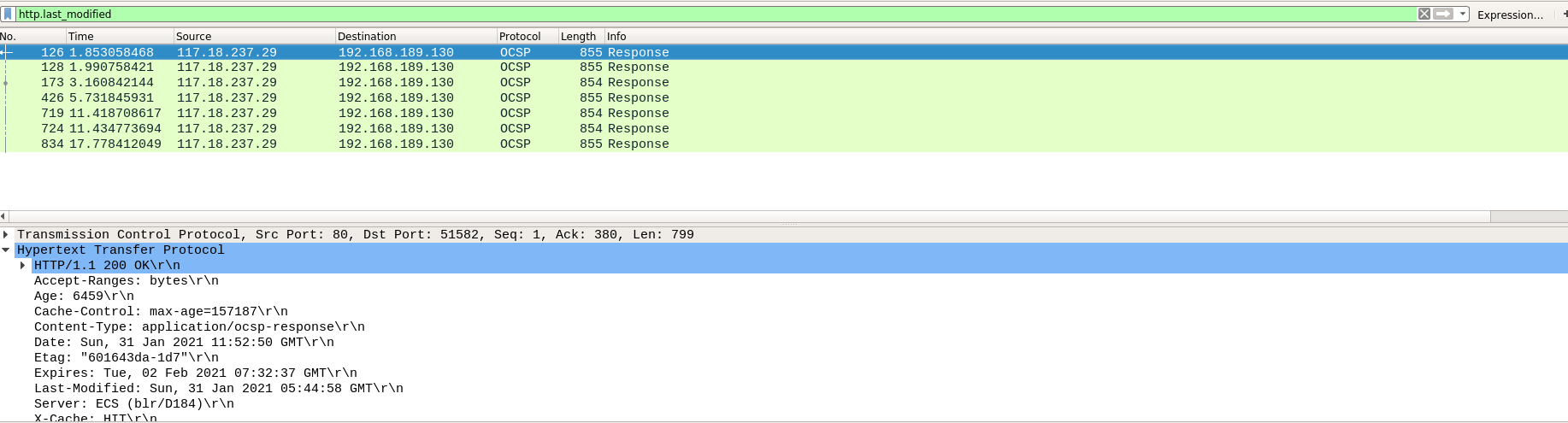
1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server?

My browser is running on http version 1.1

The server also running on http version 1.1

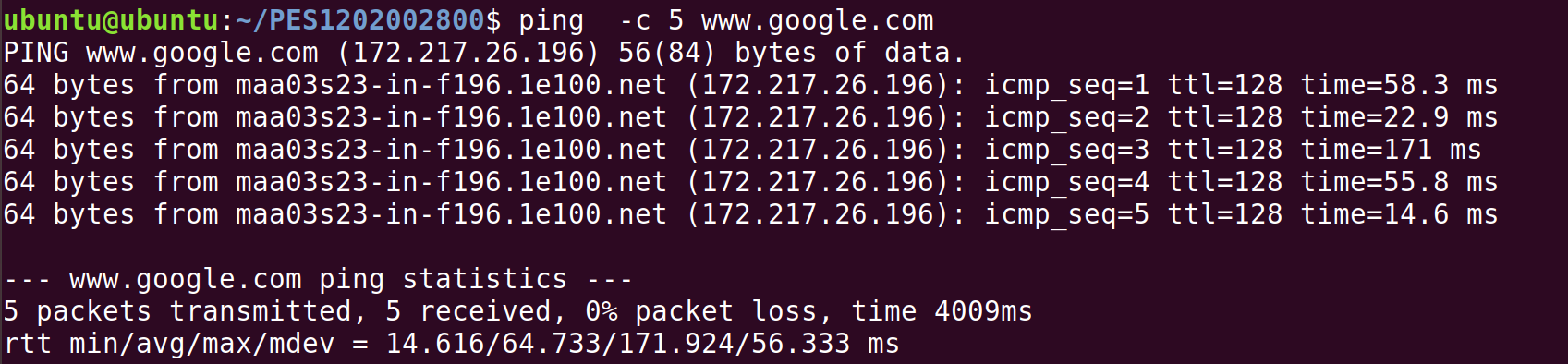


1. When was the HTML file that you are retrieving last modified at the server?



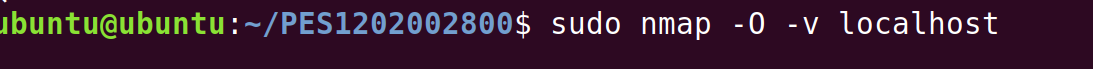
1. How to tell ping to exit after a specified number of ECHO\_REQUEST packets?

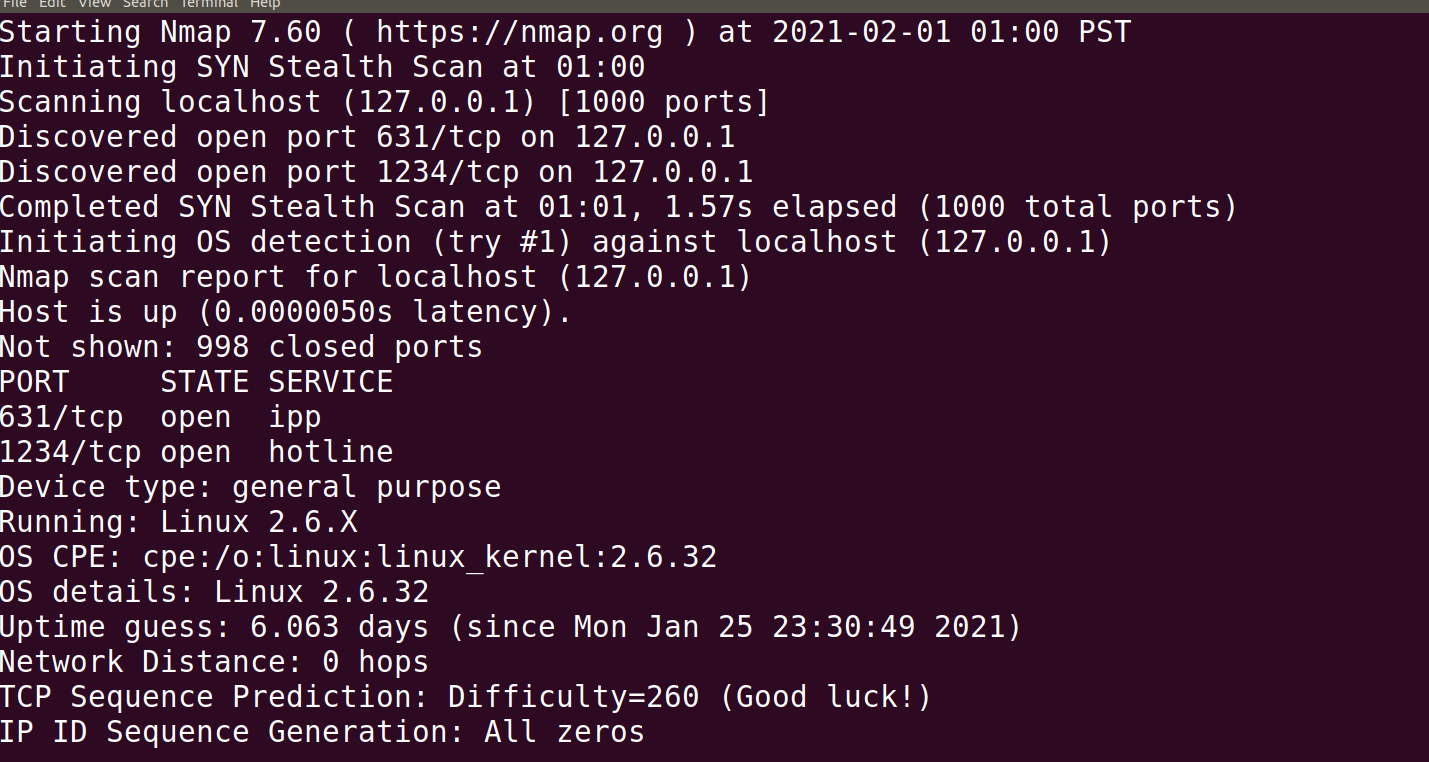
ping -c 5 www.google.com



1. How will you identify remote host apps and OS?

**Sudo nmap – O -v localhost**





**Exercises:**

1) Capture and Analyze IPv4 / IPv6 packets

## IPv4 / IPv6 packet header

|  |  |
| --- | --- |
| GET |  |
| HOST |  |
| USER-AGENT |  |
| ACCEPT-LANGUAGE |  |
| CACHE-CONTROL |  |
| PRAGMA |  |
| CONNECTION |  |

1. Explore various other network configuration, troubleshooting and debugging tools such as Route, Netstat, etc.

**ifconfig**:  initialize an interface, assign **ip addresses** to interface and **enable**or **disable**interface on demand.

**Ping:** **ping** command is the best way to test connectivity between **two nodes**. ping use**ICMP (Internet Control Message Protocol)** to communicate to other devices.

**Traceroute**: it’s a network troubleshooting utility which shows number of hops taken to reach destination also determine packets traveling path.

**Netstat**: this command displays the network status and protocol statistics, also used to display the status of TCP and UDP endpoints in table format, routing table information, and interface information.

**Route: this** command also shows and manipulate **ip** routing table.

**Natcat**: this command is used for reading and writing to network connections using TCP or UDP.

**IMPORTANT INSTRUCTIONS:**

* Perform **sudo apt-get update** before installing any tool or utility.
* Install any tool or utility using the command **sudo apt-get install name\_of\_the\_tool** • Take screenshots whenever necessary (paste in a .doc / .docx) and upload in Edmodo
* Write down the observations in your observation notebook.