Week #1

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

**Learn and Understand Network Tools**

**Wireshark**

Perform and analyze Ping PDU capture

Examine HTTP packet capture

Analyze HTTP packet capture using filter

**Tcpdump**



**3. Ping**



Capture packets

Test the connectivity between 2 systems

**Traceroute**

Perform traceroute checks

**Nmap**

Explore an entire network

**IMPORTANT INSTRUCTIONS:**

* This manual is written for Ubuntu Linux OS only. You can also execute these experiments on VirtualBox or VMWare platform.
* For few tasks, you may need to create 2 VMs for experimental setup.
* 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 wherever necessary and upload it to Edmodo as a single PDF file. (Refer general guidelines for submission requirements).
* To define an IP address for your machine (e.g., Section – ‘a’ & Serial number is 1, then your IP address should be 10.0.1.1. Section – ‘h’ & & Serial number is 23, then your IP address should be 10.0.8.23) – applicable only for relevant tasks (which doesn’t requires internet connectivity to execute the tasks).

**Task 1: Linux Interface Configuration (ifconfig / IP command) Step 1:** To display status of all active network interfaces.

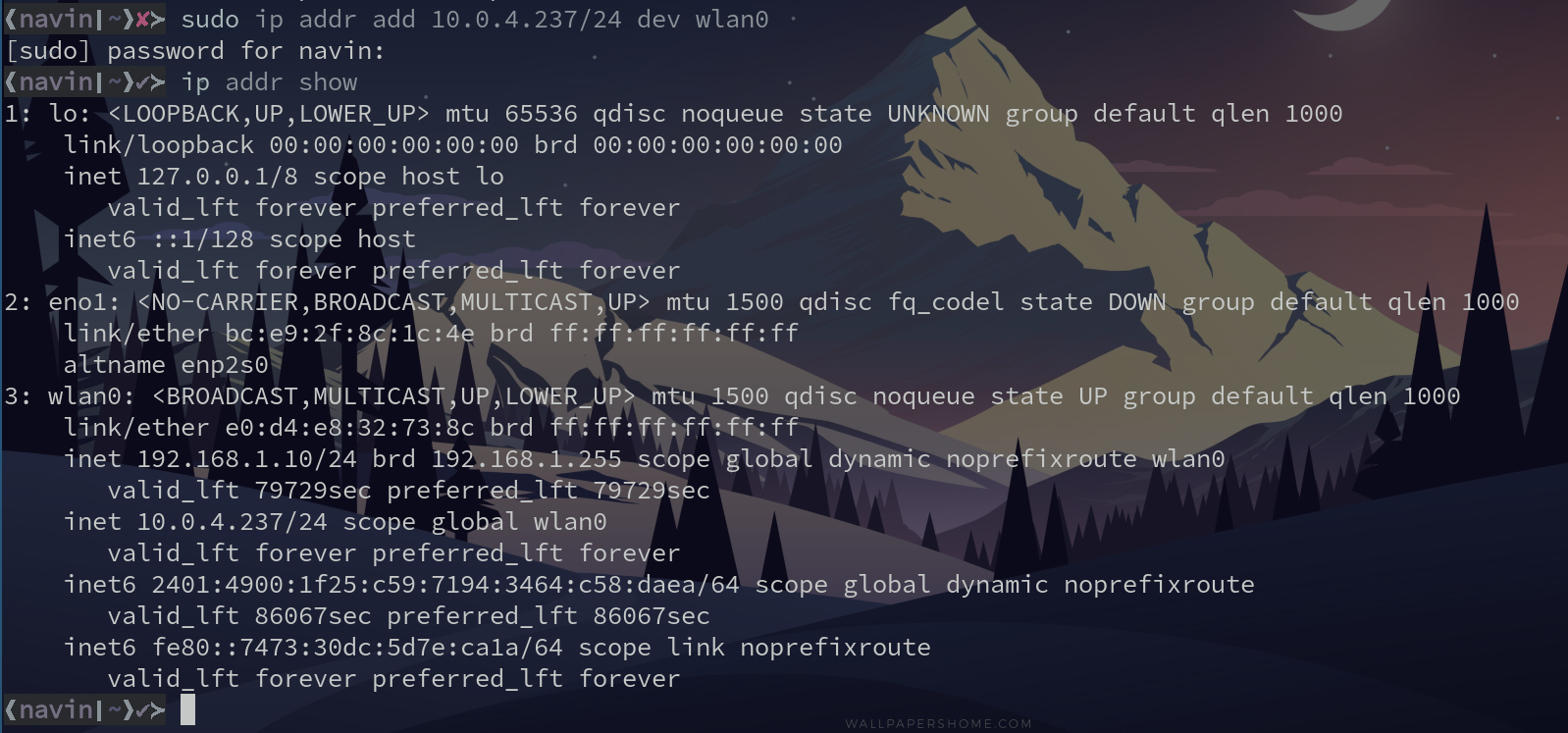
# 

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 | Loop back device |
| Eno1 [enp2s0] | - | bc:e9:2f:8c:1c:4e | Ethernet, disconnected |
| Wlan0 | 192.168.1.10 | e0:d4:e8:32:73:8c | Wireless LAN |

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

****

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

# sudo ifconfig interface\_name down sudo ifconfig interface\_name up

# 

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

# ip neigh

# 

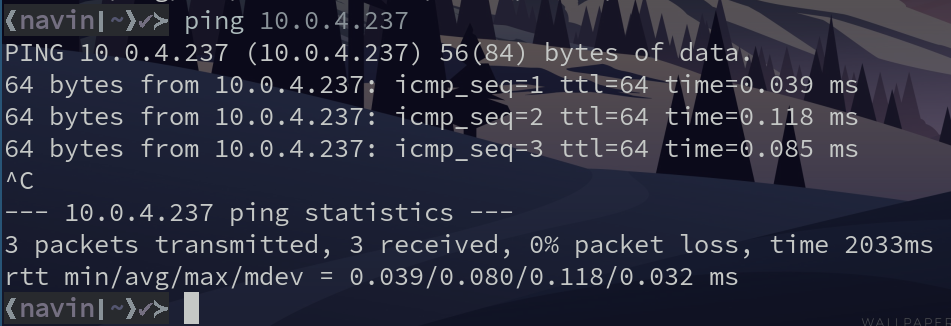
**Task 2: Ping PDU (Packet Data Units or Packets) Capture Step 1:** Assign an IP address to the system (Host).

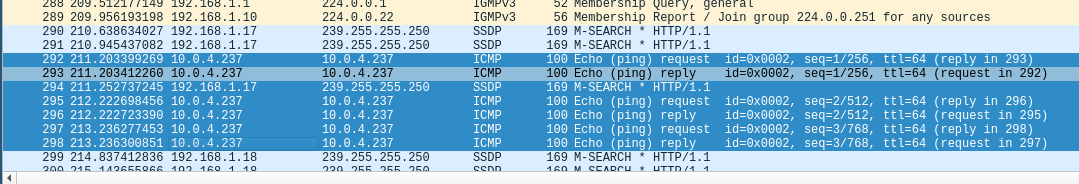
Note: IP address of your system should be 10.0.your\_section.your\_sno.

Done in previous tasks, hence pinging the same machine causes a loopback, this can be seen with indiffrentiating ip add in the table.Can also be seen with the mac address of device used.

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

**Step 3:** In terminal, type **ping 10.0.your\_section.your\_sno**





# Observations to be made

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

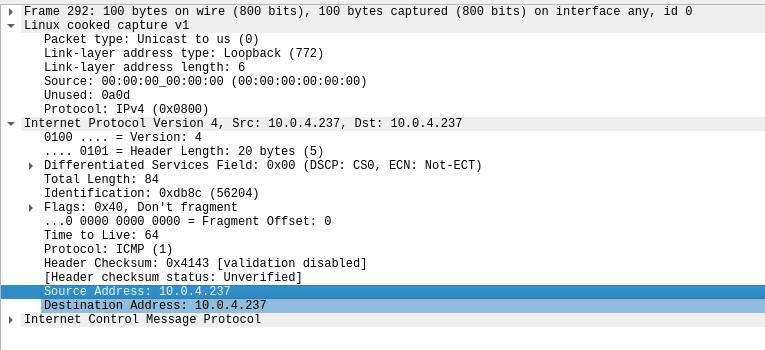
* TTL : 64
* Protocol used by ping : ICMP : Internet Control Message Protocol
* Time : ~2000ms , observed from ping command

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

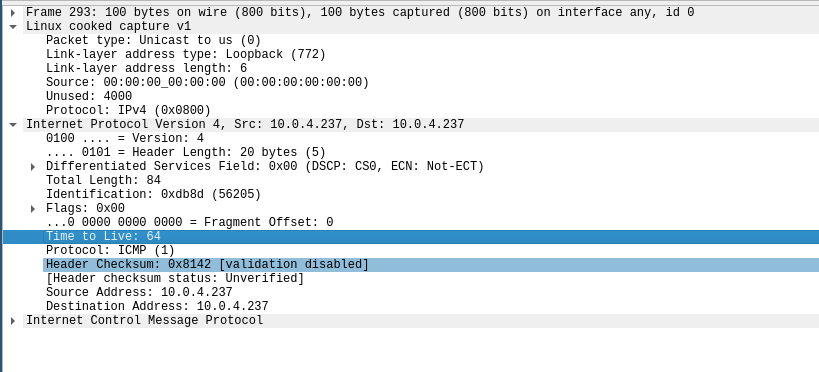
On Packet List Pane, select the first echo packet on the list. On Packet Details Pane, click on each of the four “+” to expand the information. Analyze the frames with the first echo request and echo reply and complete the table below.

|  |  |  |
| --- | --- | --- |
| **Details** | **First Echo Request** | **First Echo Reply** |
| Frame Number | 292 | 293 |
| Source IP address | 10.0.4.237 | 10.0.4.237 |
| Destination IP address | 10.0.4.237 | 10.0.4.237 |
| 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 ping request :



First Ping response :



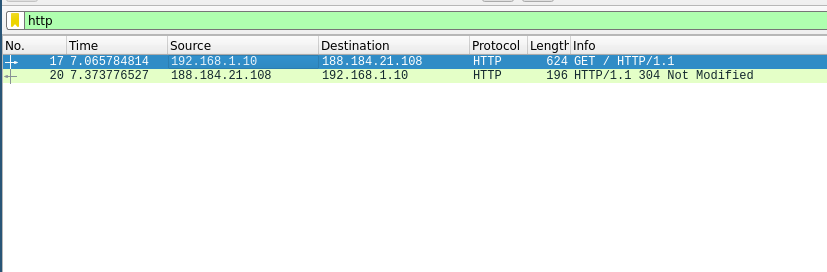
# Task 3: HTTP PDU Capture Using Wireshark’s Filter feature

**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

[www.flipkart.com](http://www.flipkart.com/)does not do http requests and hence wireshark can not analyze them, thus I would be doing my analysis using :

http://info.cern.ch/

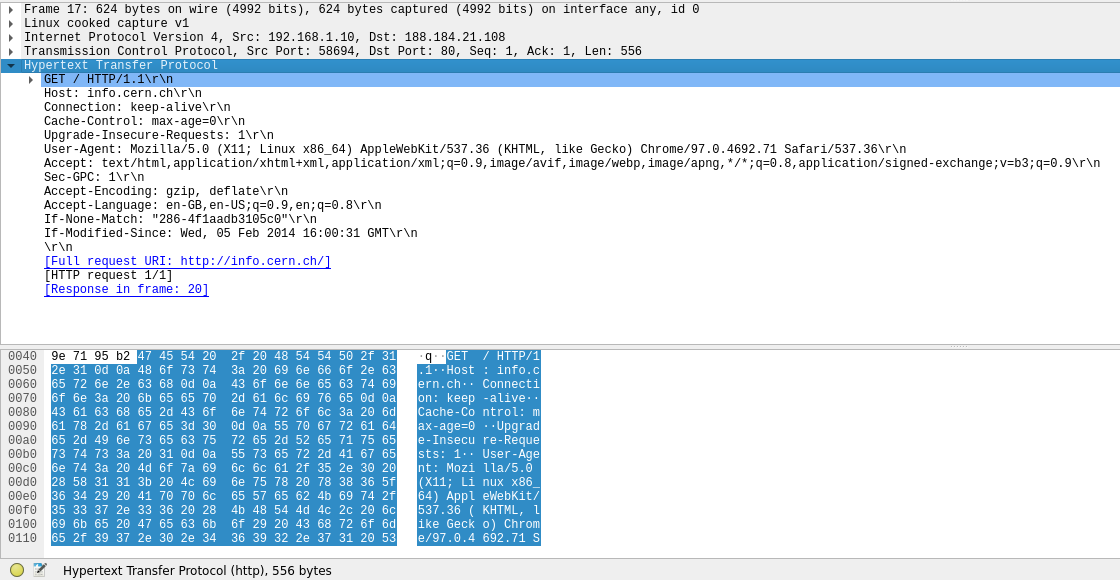


# Observations to be made

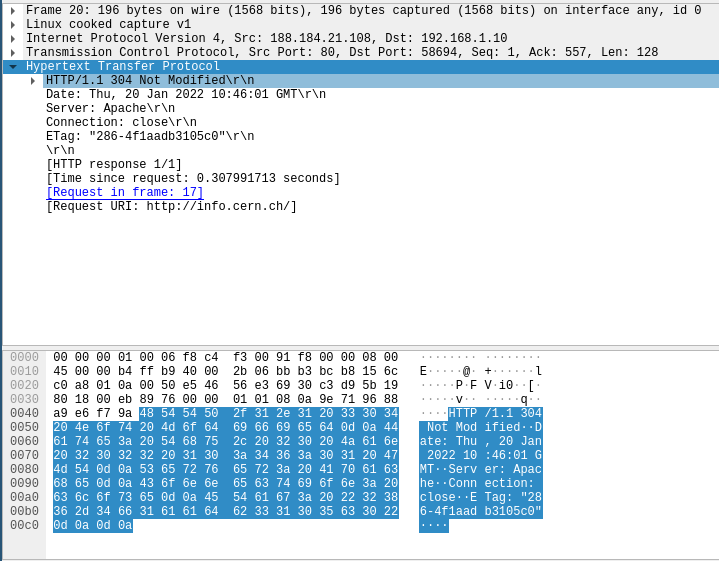
**Step 3:** Analyze the first (interaction of host to the web server) and second frame (response of server to the client). By analyzing the filtered frames, complete the table below:

|  |  |  |
| --- | --- | --- |
| **Details** | **First Echo Request** | **First Echo Reply** |
| Frame Number | 17 | 20 |
| Source Port | 58694 | 80 |
| Destination Port | 80 | 58964 |
| Source IP address | 192.168.1.10 | 188.184.21.108 |
| Destination IP address | 188.184.21.108 | 192.148.1.10 |
| Source Ethernet Address | e0:d4:e8:32:73:8c | f8:c4:f3:00:91:f8 |
| Destination Ethernet Address | f8:c4:f3:00:91:f8 | e0:d4:e8:32:73:8c |

HTTP First request :



HTTP First response :



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

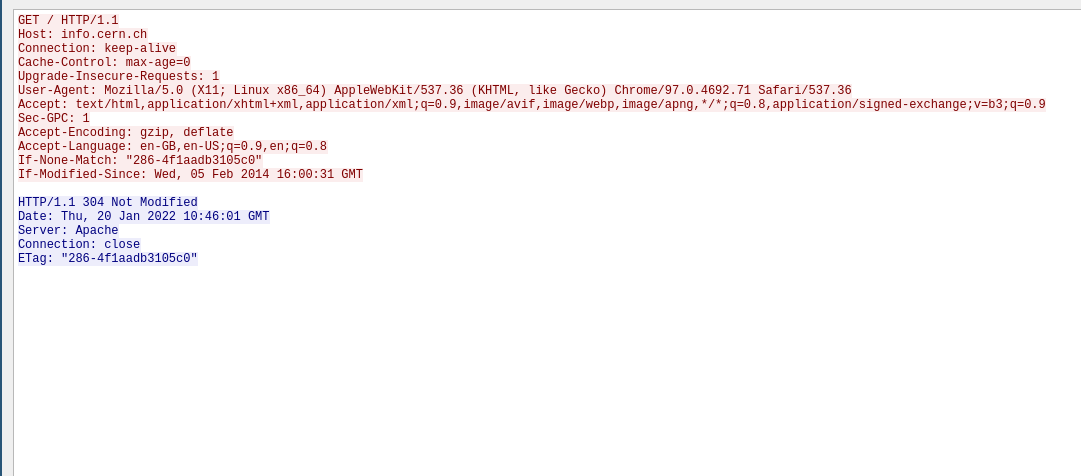
|  |  |  |  |
| --- | --- | --- | --- |
| **HTTP Request** |  | **HTTP Response** |  |
| Get | GET / HTTP/1.1\r\n | Server | Apache |
| Host | info.cern.ch | Content-Type | text/plain |
| User-Agent | Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36 | Date | Thu, 20 Jan 2022 12:09:16 GMT |
| Accept-Language | en-GB,en-US;q=0.9,en;q=0.8 | Location |  |
| Accept-Encoding | gzip, deflate | Content-Length | 25 |
| Connection | keep-alive | Connection | close |

# 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.

Enntire conversation :



Sadly this connection did not yield any TCP connections to follow.

# Task 4: Capturing packets with tcpdump

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

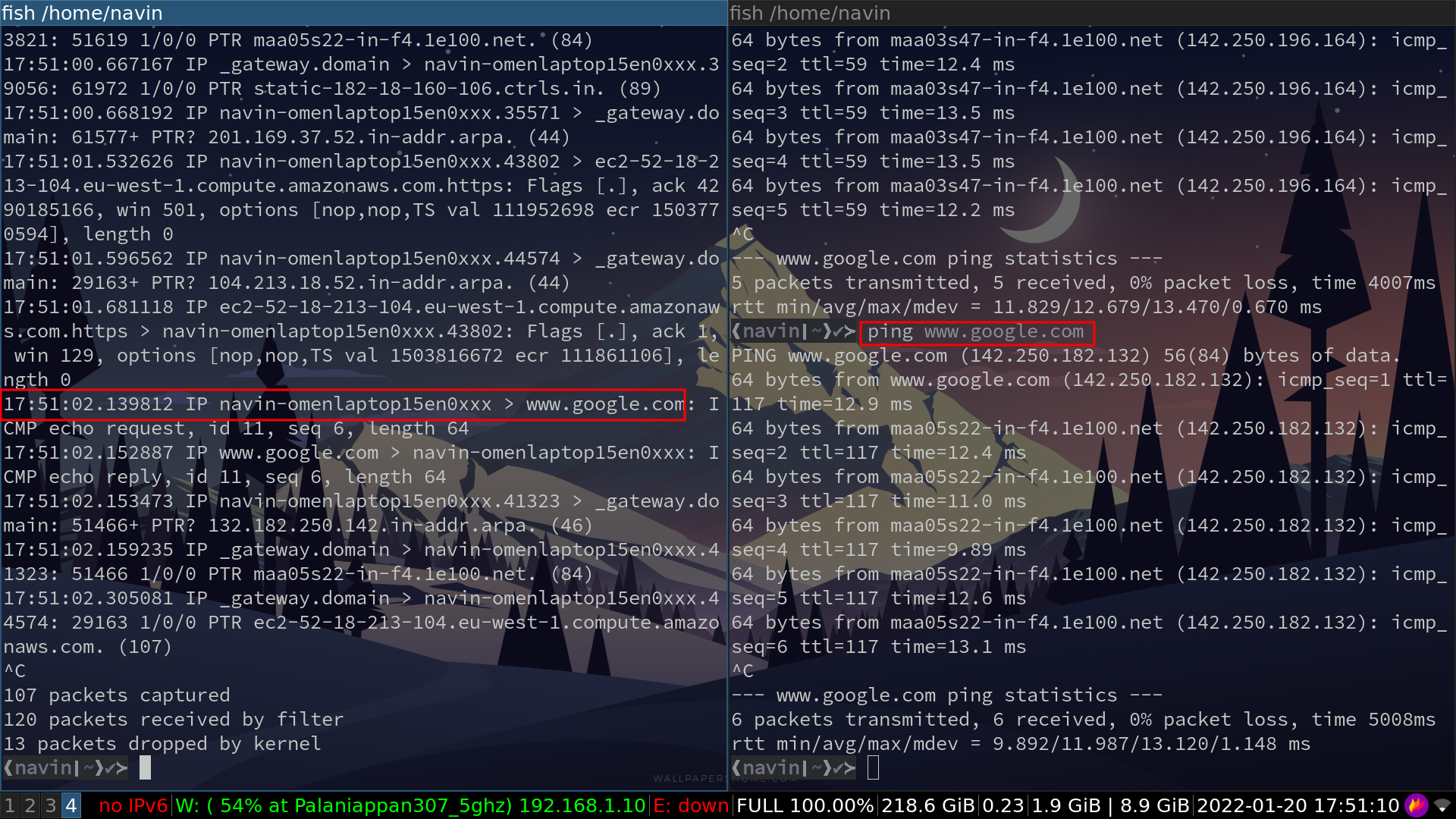
# sudo tcpdump -D

# 

**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.



**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

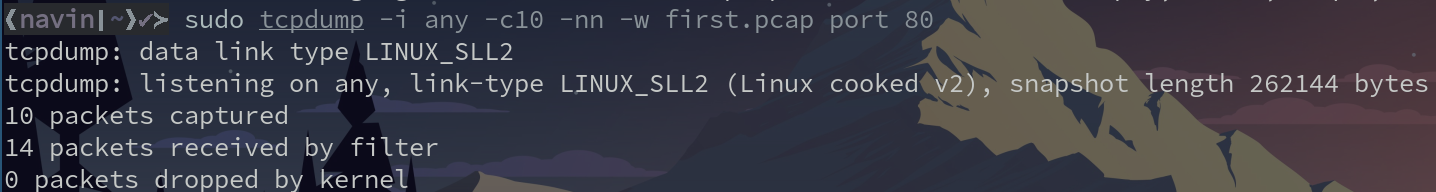
**Step 6:** To save packets to a file instead of displaying them on screen, use the option -w:

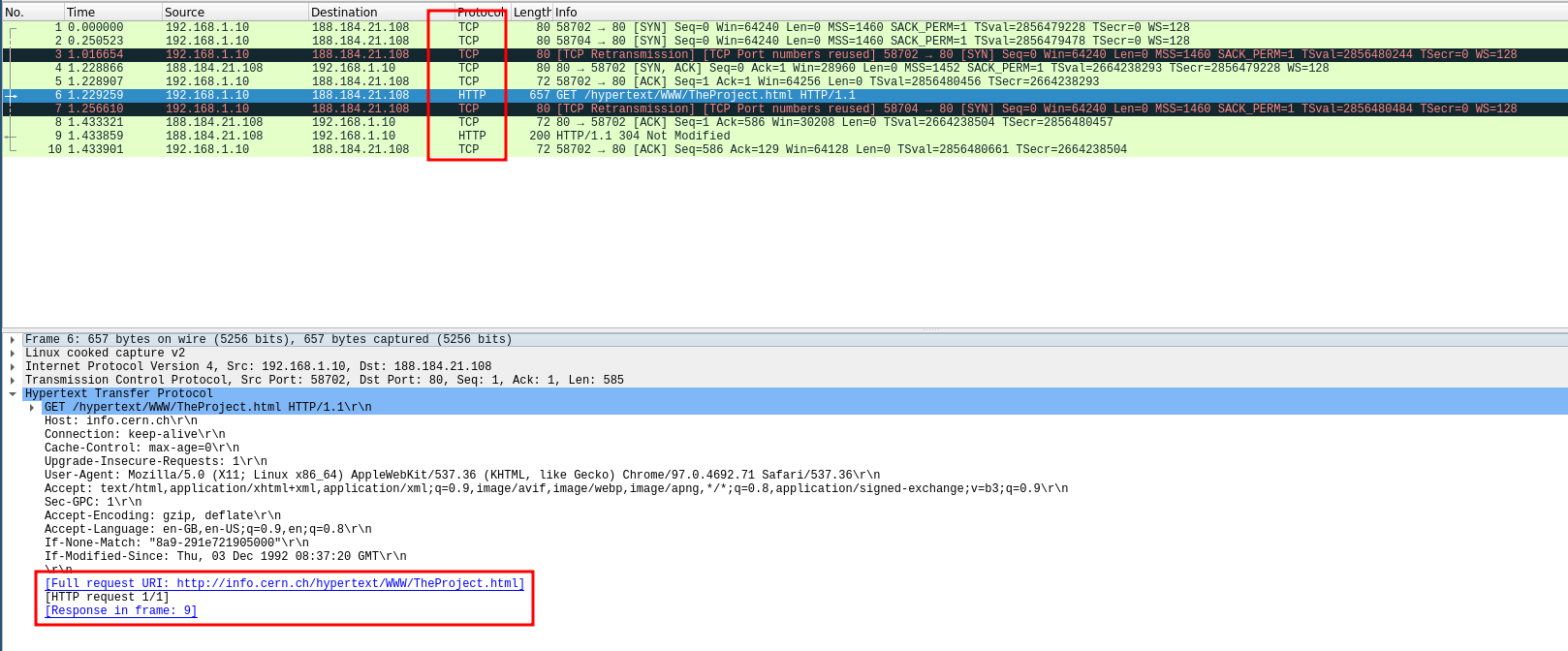
# sudo tcpdump -i any -c10 -nn -w webserver.pcap port 80

# PING TO IN BROWSER : http://info.cern.ch/hypertext/WWW/TheProject.html

# A ping command was not used as filter command was for HTTP and not ICMP

# 

****

**Opening the above file in wireshark :**

**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

Destication : 142.250.182.132

Number of hops : 8

**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](https://en.wikipedia.org/wiki/Internet_Control_Message_Protocol).

# 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.

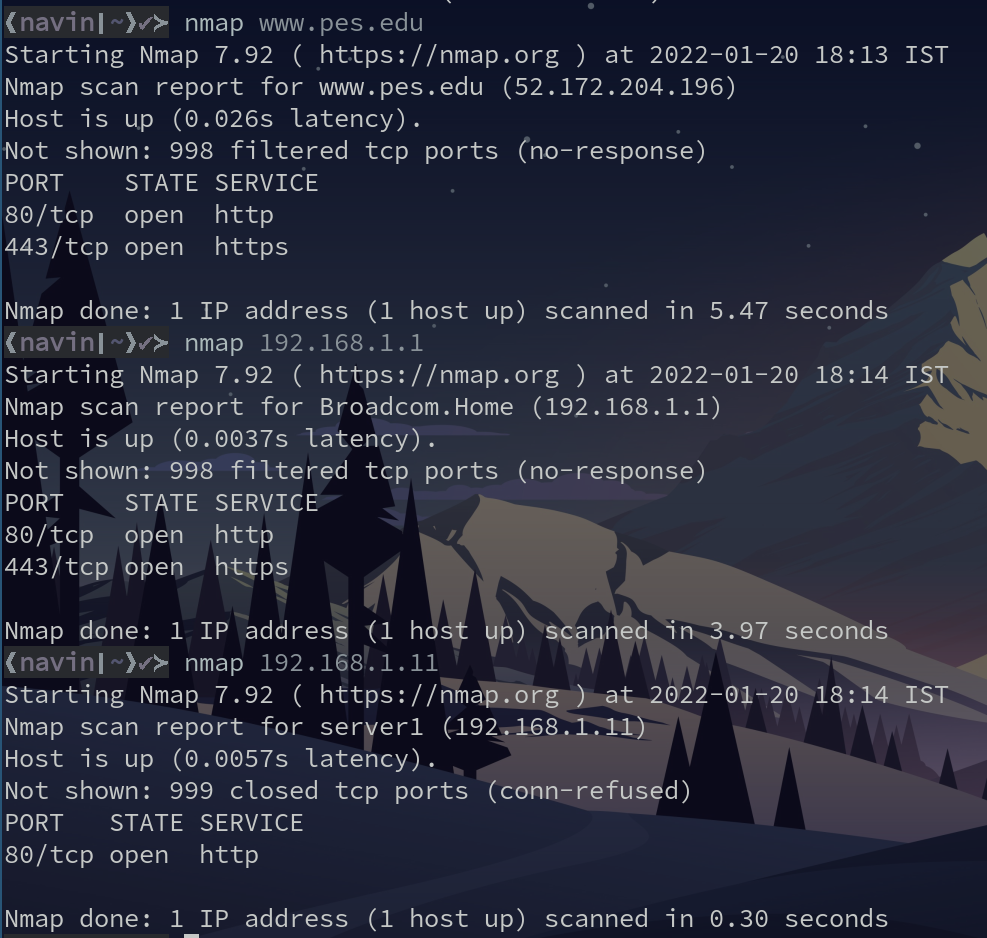
# nmap [www.pes.edu](http://www.pes.edu/)

**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?
2. When was the HTML file that you are retrieving last modified at the server?
3. How to tell ping to exit after a specified number of ECHO\_REQUEST packets?
4. How will you identify remote host apps and OS?