Week #1

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

**Learn and Understand Network Tools**

1. **Wireshark**
   * Perform and analyze Ping PDU capture
   * Examine HTTP packet capture
   * Analyze HTTP packet capture using filter
2. **Tcpdump**



**3. Ping**



Capture packets

Test the connectivity between 2 systems

1. **Traceroute**
   * Perform traceroute checks
2. **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).

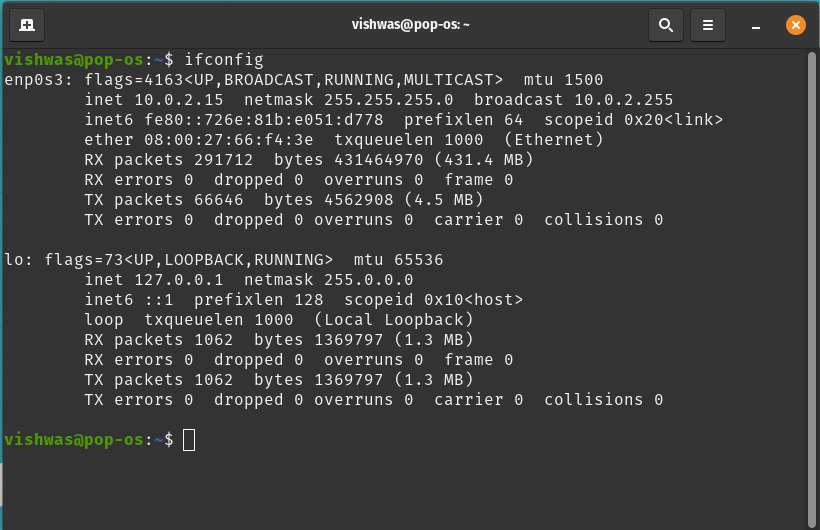
**Task 1: Linux Interface Configuration (ifconfig / IP command) Step 1:** To display status of all active network interfaces.

# ifconfig (or) ip addr show

Analyze and fill the following table:

# ip address table:

|  |  |  |  |
| --- | --- | --- | --- |
| **Interface name** | **IP address (IPv4 / IPv6)** | **MAC address** |  |
| enp0s3 | 10.0.2.15 | 08:00:27:66:f4:3e |  |
| lo | 127.0.0.1 | - |  |
|  |  |  |  |

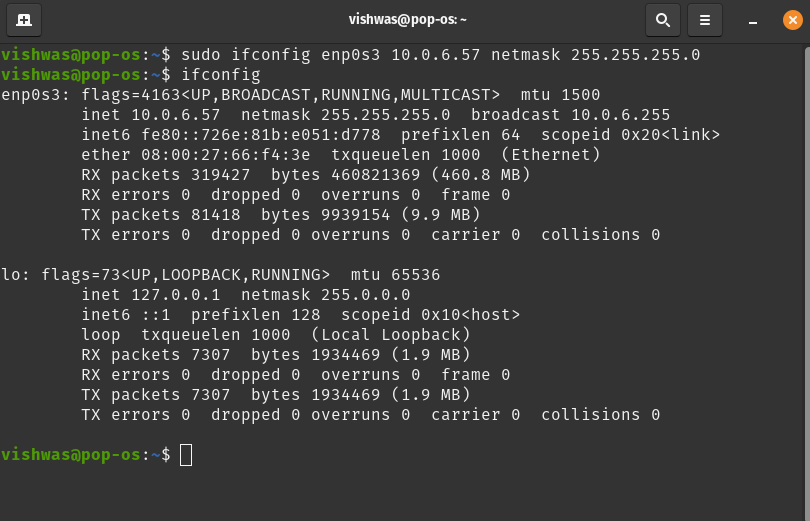


**The hardware address and the IP address is mentioned,when ifconfig is typed in the terminal.**

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

# sudo ifconfig interface\_name 10.0.your\_section.your\_sno netmask 255.255.255.0 (or)

**sudo ip addr add 10.0.your\_section.your\_sno /24 dev interface\_name**



**10.0.6.57 is assigned as the IP address to the interface.**

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

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

# 

# The configured interface is set to up and running if it isn’t.

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

# ip neigh

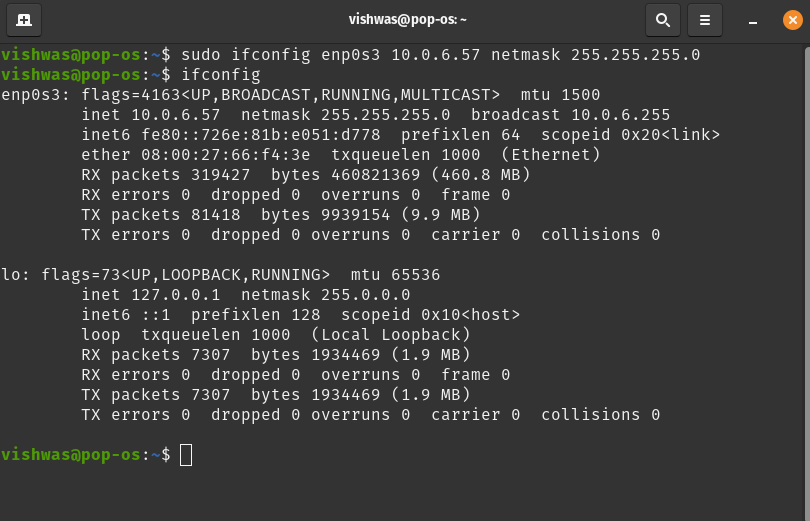
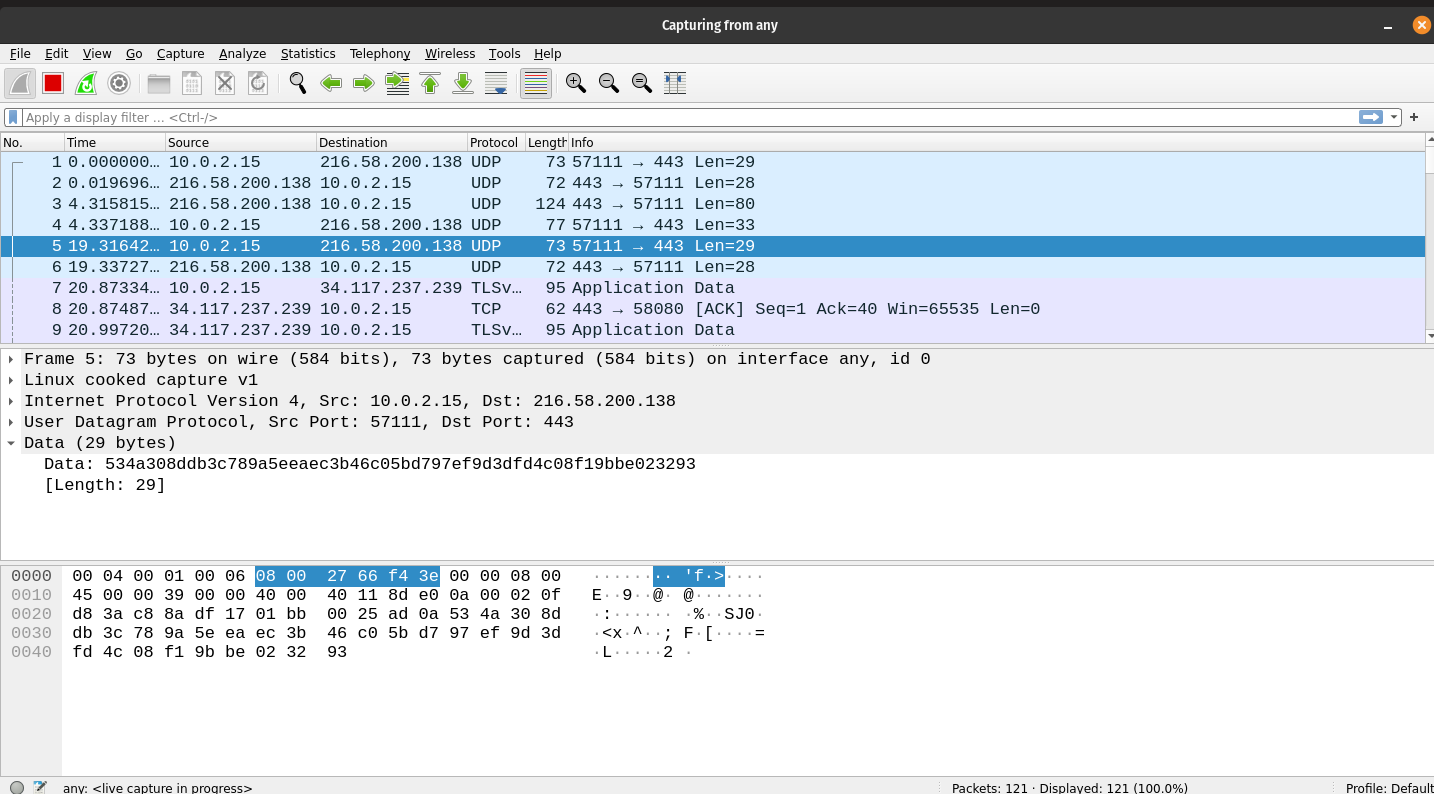
# 

# The neighbor table is shown in the output.

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

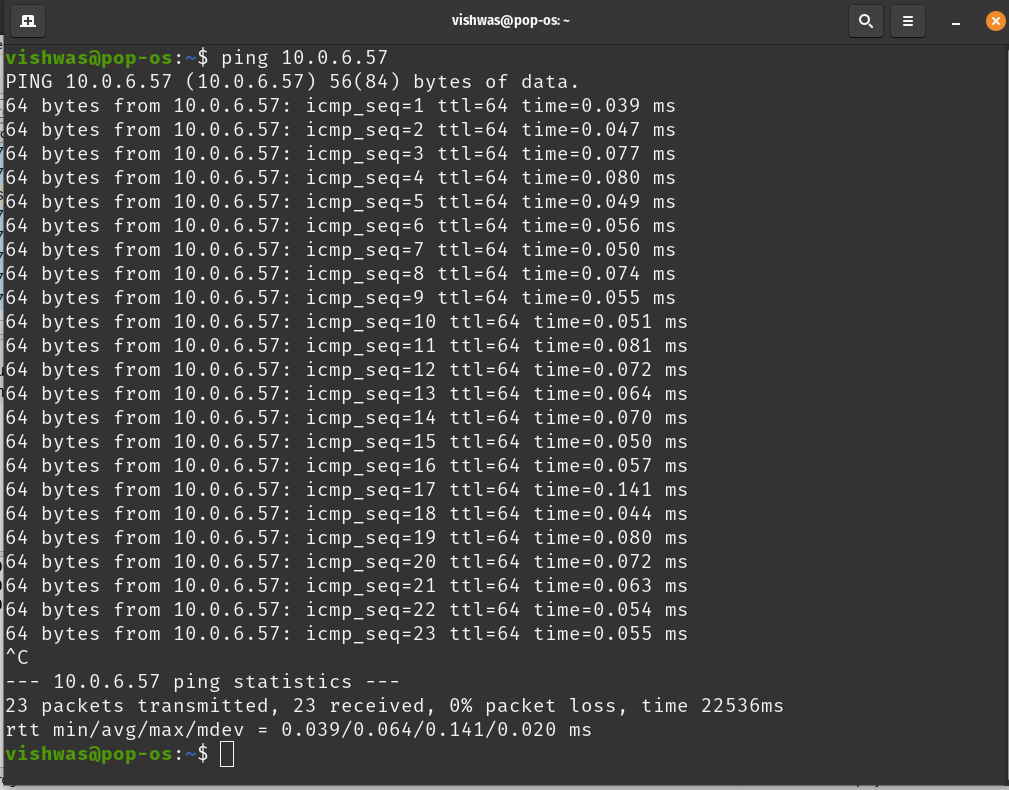
Note: IP address of your system should be 10.0.your\_section.your\_sno.

The IP address is set to 10.0.6.57.

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

Wireshark on launch and opened into “any”.

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



# Observations to be made

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

* TTL
* Protocol used by ping
* Time

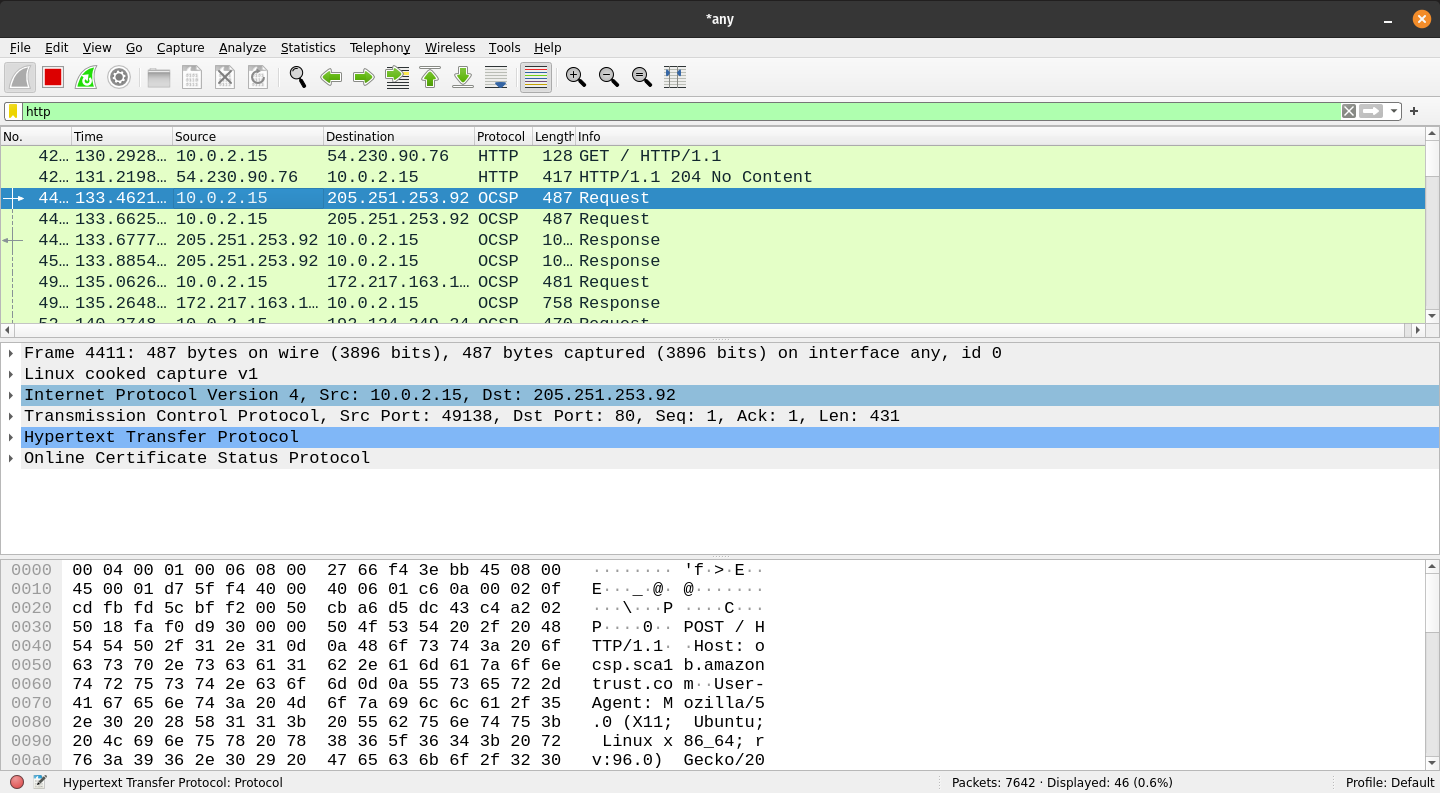
**Step 5:** Analyze the following in Wireshark

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.

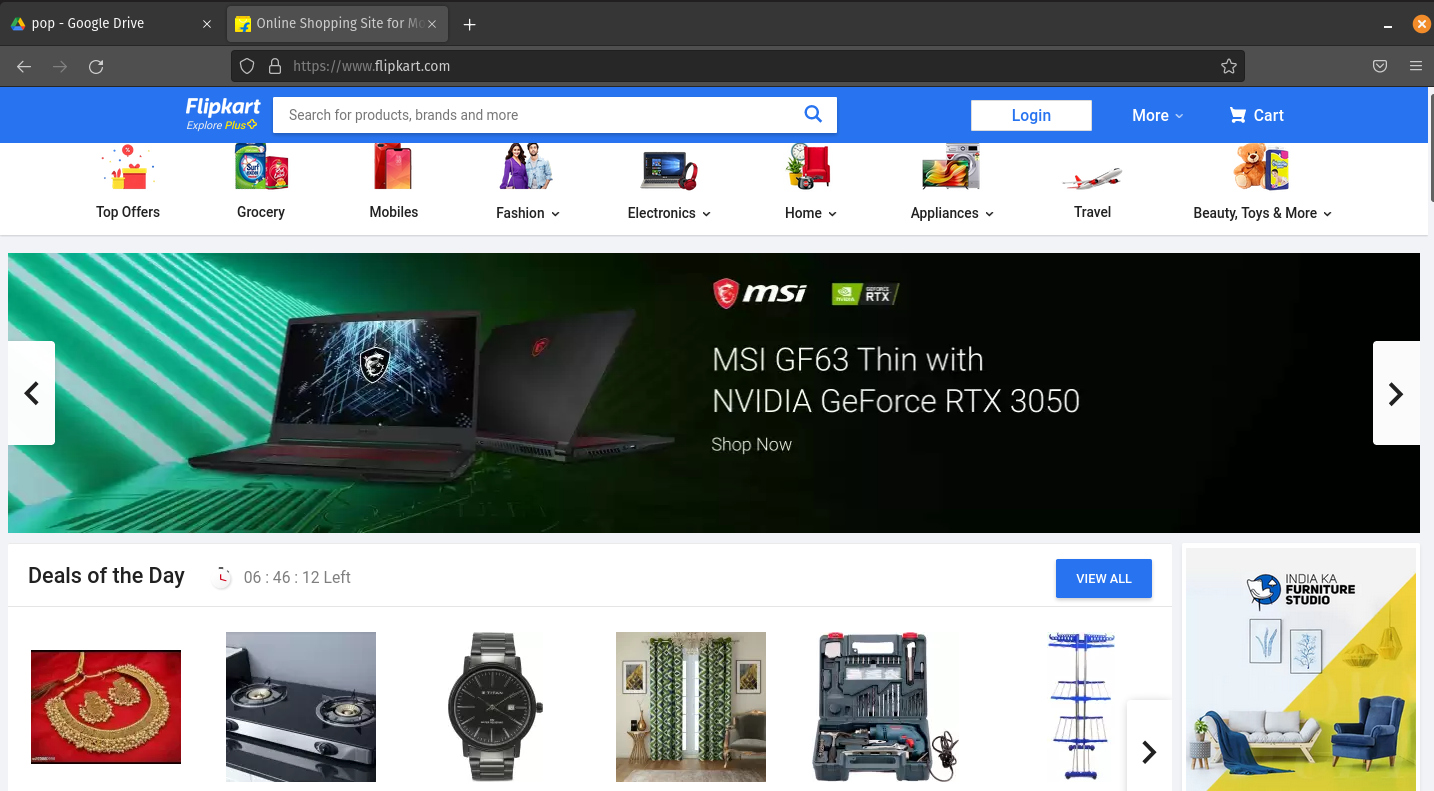
|  |  |  |
| --- | --- | --- |
| **Details** | **First Echo Request** | **First Echo Reply** |
| Frame Number | 207 | 208 |
| Source IP address | 10.0.6.57 | 10.0.6.57 |
| Destination IP address | 10.0.6.57 | 10.0.6.57 |
| ICMP Type Value | 8 | 0 |
| ICMP Code Value | 0 | 0 |
| Source Ethernet Address | 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(reply in 208) | 64(request in 207) |

# 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 | 4411 | 4470 |
| Source Port | 49138 | 80 |
| Destination Port | 80 | 49138 |
| Source IP address | 10.0.2.15 | 205.251.253.92 |
| Destination IP address | 205.251.253.92 | 10.0.2.15 |
| Source Ethernet Address | 08:00:27:66:f4:3e | 52:54:00:12:35:02 |
| Destination Ethernet Address | 52:54:00:12:35:02 | 08:00:27:66:f4:3e |

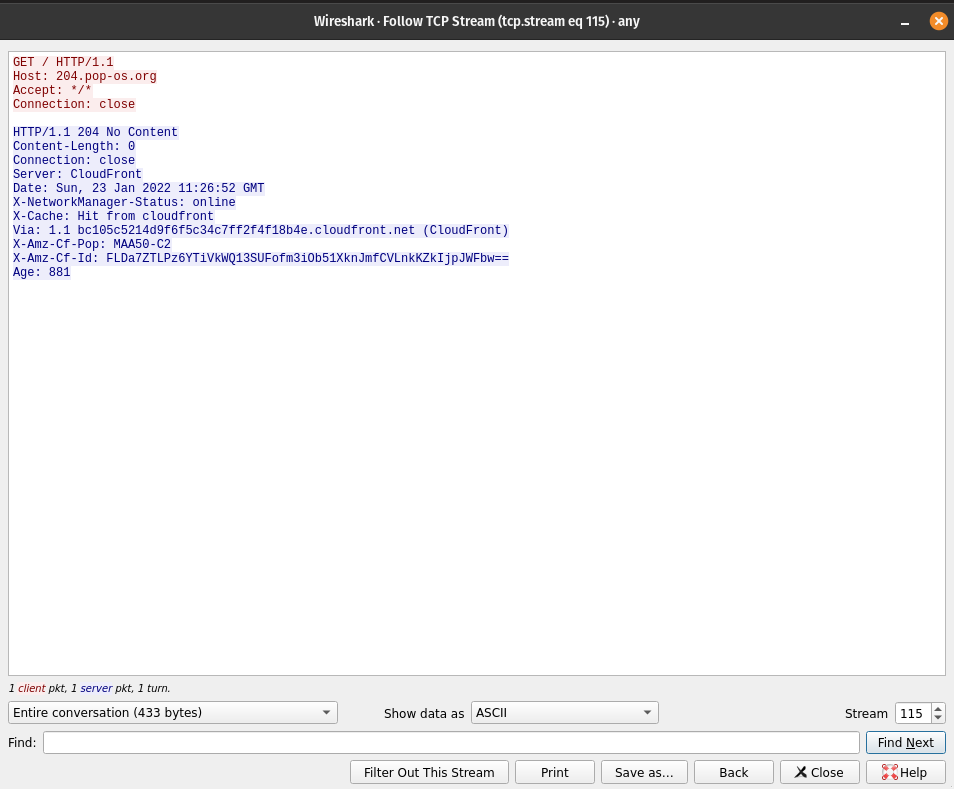
**Step 4:** Analyze the HTTP request and response and complete the table below.

|  |  |  |  |
| --- | --- | --- | --- |
| **HTTP Request** |  | **HTTP Response** |  |
| Get | /HTTP/1.1 | Server | ECS (oxr/8323) |
| Host | Ocsp.sca1b.amazontrust.com | Content-Type | Application/ocsp-request |
| User-Agent | Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:96.0) Gecko/20100101 Firefox/96.0 | Date | Sun,23 Jan 2022 11:41:36 GMT |
| Accept-Language | En-US,en;q=0.5 | Location | <NOT SPECIFIED> |
| Accept-Encoding | Qzip, deflate | Content-Length | 471 |
| Connection | Keep-alive | Connection | Keep-alive |

# 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.

# 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.

**The above command is used to capture all the packets from all the interfaces. ICMP, UDP and TCP are the main packets that are visible in the above screenshot. The timestamp followed by the link level headers, then by ARP/RARP packets if any, Then by IPv4 packets if any, followed by TCP packets. The sequence numbers and the length finish defining the outputs.**

**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 5: 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

**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 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/)

# 

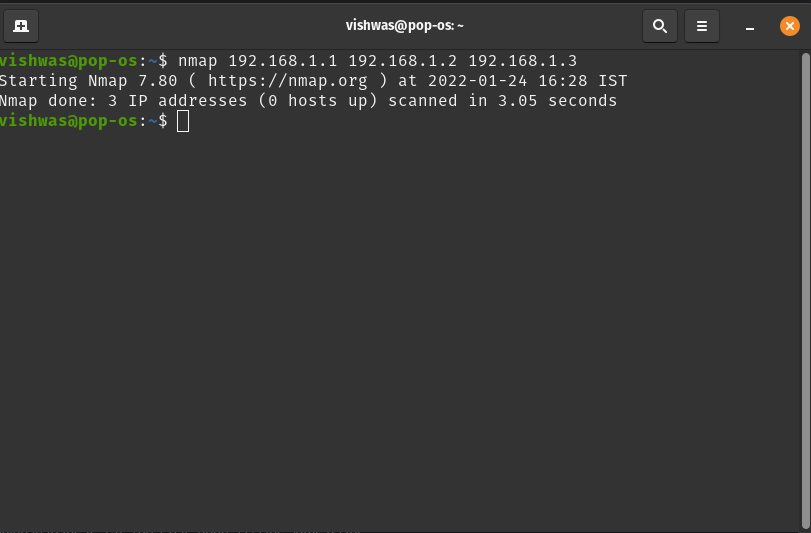
**Step 2:** Alternatively, use an IP address to scan.

# 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?

Ans**: 1.1. The version of the server is 1.1 as well.**

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

Ans: **Sun,23 Jan 2022 11:41:36 GMT**

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

Ans: **$ ping -c <number of packets> <url>**

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

Ans: **Simply scan the entire subnet.**

**Eg: $ nmap -sP 10.0.4.\***