**ST. FRANCIS INSTITUTE OF TECHNOLOGY**

**DEPARTMENT OF INFORMATION TECHNOLOGY**

**SECURITY LAB**

**Experiment – 9: Simulate DOS attack using Hping and Wireshark.**

**Aim:** To simulate DOS attack using Hping3 and observe with Wireshark.

**Objective:** After performing the experiment, the students will be able to analyze DOS attack and its effect on the network using Hping3 and Wireshark.

**Lab objective mapped:** L502.6: Students should be able to Apply network security basics, analyze different attacks on networks and evaluate the performance of firewalls and security protocols, such as SSL, IPSEC, and PGP, and authentication mechanisms to design secure applications.

**Prerequisite:** Basic knowledge of network security.

**Requirements:** kali Linux OR Unix/Linux, Hping3, Wireshark

**Pre-Experiment Theory:**

Denial-of-service (DoS) attack is an attempt to make a machine or network resource unavailable to its intended users, such as to temporarily or indefinitely interrupt or suspend services. A distributed denial-of-service (DDoS) is where the attack source is more than one, often thousands of, unique IP addresses.

A DoS attack tries to make a web resource unavailable to its users by flooding the target URL with more requests than the server can handle. That means during the attack period, regular traffic on the website will be either slowed down or completely interrupted.

A DDoS attack is typically generated using thousands (potentially hundreds of thousands) of unsuspecting zombie machines. The machines used in such attacks are collectively known as “botnets” and will have previously been infected with malicious software, so they can be remotely controlled by the attacker. According to research, tens of millions of computers are likely to be infected with botnet programs worldwide.

Cybercriminals use DoS attacks to extort money from companies that rely on their websites being accessible. But there have also been examples of legitimate businesses having paid underground elements of the Internet to help them cripple rival websites. In addition, cybercriminals combine DoS attacks and phishing to target online bank customers. They use a DoS attack to take down the bank's website and then send out phishing e-mails to direct customers to a fake emergency site instead.

**Implementation:**

1. Install Hping3 and Wireshark on Ubuntu machine. Alternatively, you can use kali Linux machine.
2. Flood the victim with TCP/ICMP/UDP packet using Hping3 (-- flood option). Use following commands in the ‘Terminal’ window,
   1. hping3 –h

Observe all the options hping3 offers. Take screenshot (SS).

* 1. Simultaneously open Wireshark. Start sniffing the appropriate network. Then use following command in the ‘Terminal’ window.

sudo hping3 *(suitable IP Address)*

Observe the DoS attack using Wireshark. Take SS of the terminal and Wireshark window. Terminate hping3 using ‘ctrl c’ and stop sniffing through Wireshark.

Use following commands one by one and observe the DoS attacks using Wireshark. For each command take SS of the terminal and Wireshark window.

* 1. sudo hping3 *(suitable IP Address)* -1
  2. sudo hping3 *(suitable IP Address)* -1 --fast
  3. sudo hping3 *(suitable IP Address)* -1 --faster
  4. sudo hping3 -c 10000 -d 120 -S - w 64 -p 21 --flood --rand-source www.hping3testsite.com or *(suitable IP Address)*

**O bservations & Output:**

1. Attach all the screenshots (SS) in sequence.
2. Under each hping command SS, explain the command with all the options used with it.
3. Under each Wireshark window SS write your own observations.

**Post Experimental Exercise:** *(to be handwritten on journal sheets)*

1. Briefly explain DDOS Attack?
2. Discuss Buffer overflow attack in detail.

**Conclusion:**

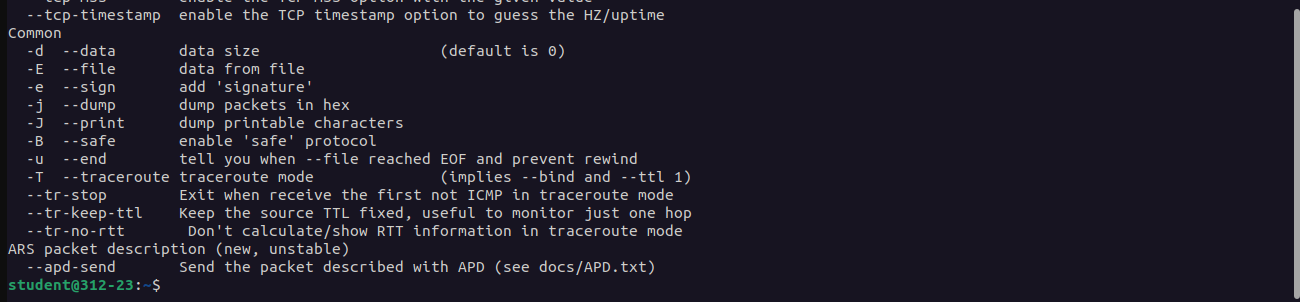
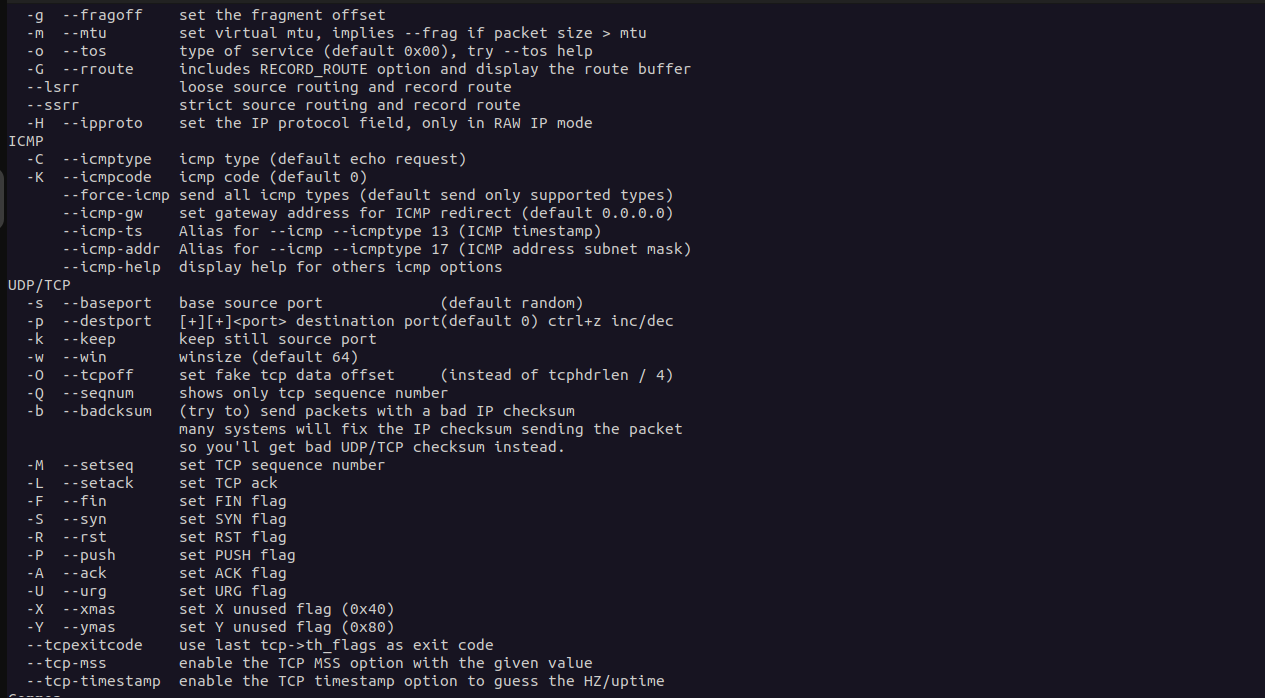
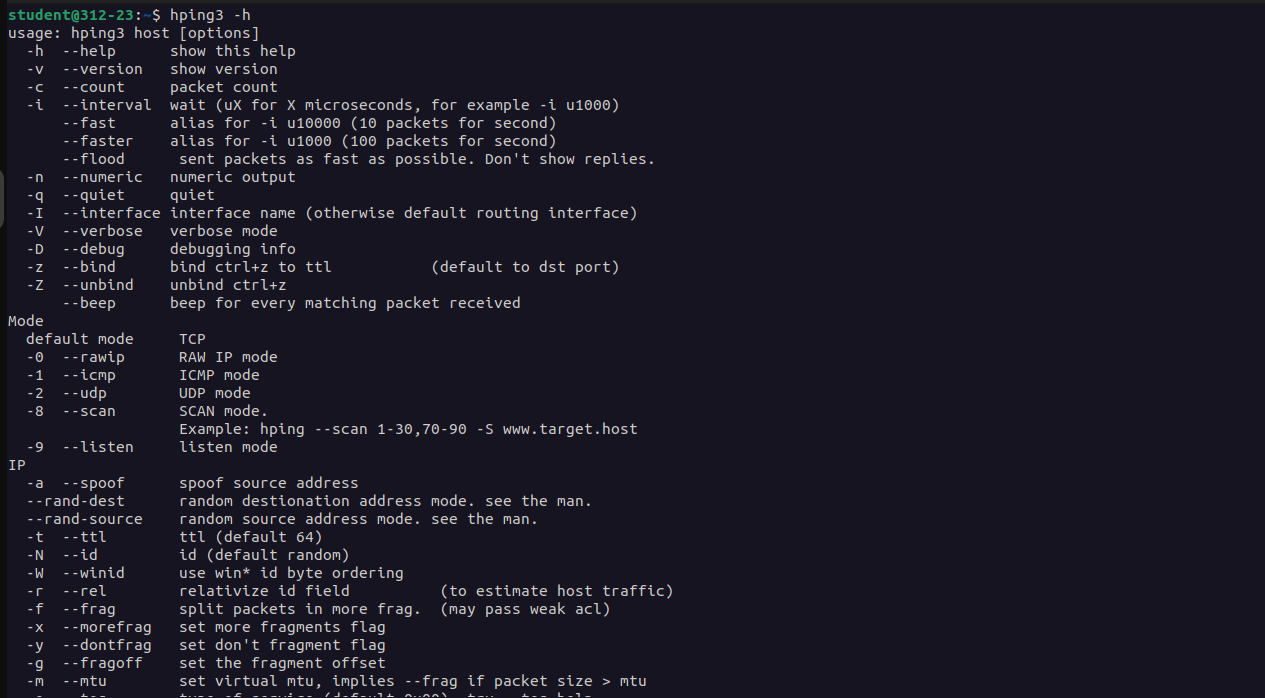
In this experiment DoS attack is simulated using Hping3 and resource exhaustion was monitored using Wireshark. We conclude that DOS is a simple attack technique to deny accessibility to services. It consists of overloading the target with oversized packets, or a big quantity of them. But it does not compromise the information or privacy of the target. It is not a penetrative attack and only aims to prevent access to the target.

**References:**

1. “Denial-of-service Attack – DoS using hping3 with spoofed IP in Kali Linux”, <https://www.blackmoreops.com/2015/04/21/denial-of-service-attack-dos-using-hping3-with-spoofed-ip-in-kali-linux/>
2. “Lecture 45: Denial of Service Attack”, <https://youtu.be/2VmQ3Zb4I2I>
3. “DOS Flood With hping3”, <https://linuxhint.com/hping3/>
4. “15+ hping3 command examples in Linux [Cheat Sheet]”, <https://www.golinuxcloud.com/hping3-command-in-linux/>
5. <http://www.vulnweb.com/>
6. [www.hping3testsite.com](http://www.hping3testsite.com)

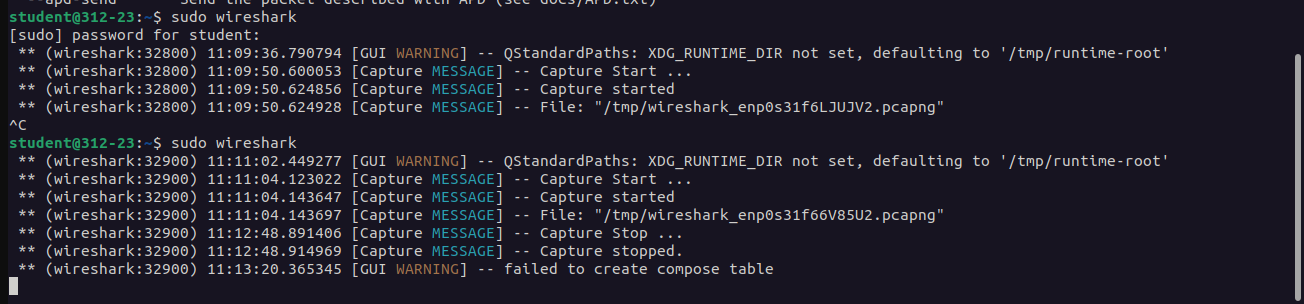
**Observations &Output:**

1. HELP COMMAND : *hping3 -h*

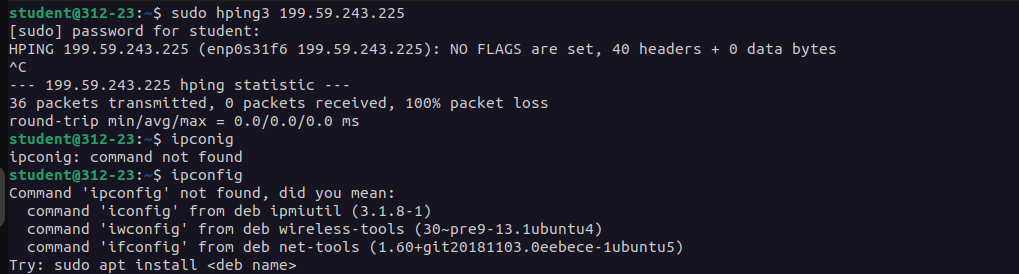


Using the help command we see the manual of hping3 where details of various extensions to the command are given with their information. It displays a summary of its usage, showing that the tool is used to send custom network packets to a target host with various options. It supports various protocols like TCP, UDP, and ICMP, and can perform tasks like port scanning, traceroutes, and network performance testing.

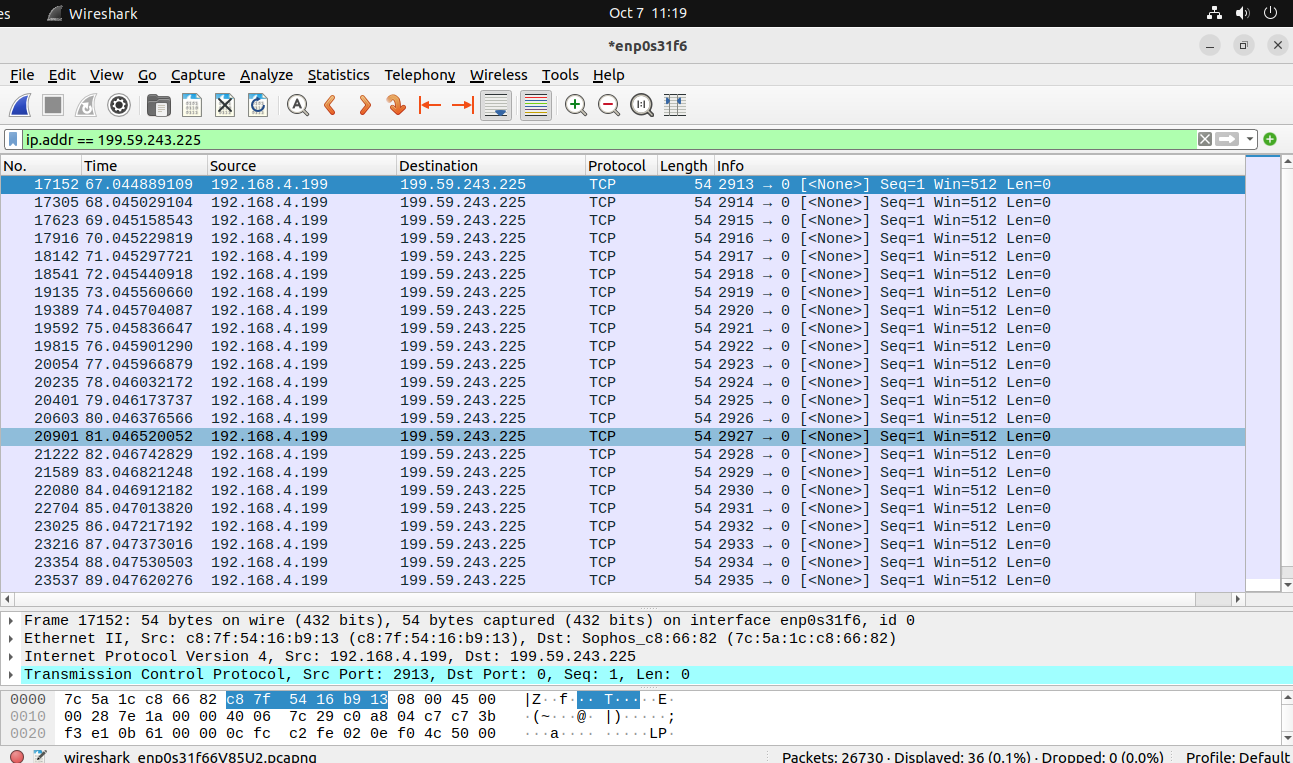
**b. DoS attack using Wireshark: *sudo hping3 199.59.243.***



The wireshark command is used to open the wireshark window where we will sniff the packets that are sent and start capturing them. We open the current network in use and start sniffing.

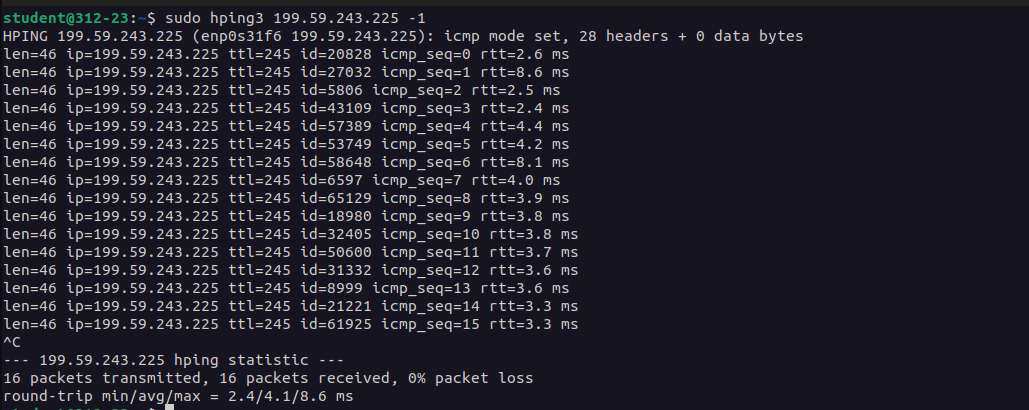


Using this command we send custom network packets to a specified target IP address. We see that 30 packets have been transmitted. This tool is helpful for network administrators and security analysts to assess network behavior.



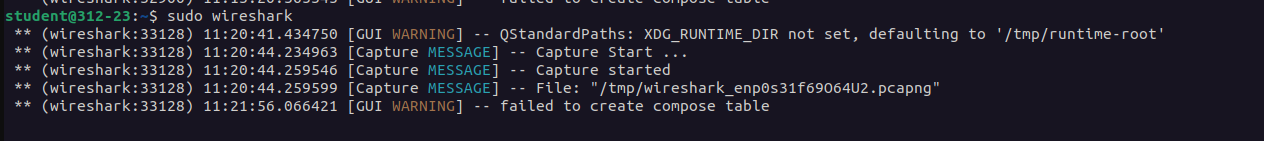
We see using the ip.addr filter that the packets have been sent to the destination we mentioned in the hping command. We see the protocol and some additional information. This is a distributed denial of service attack. The target becomes overloaded, causing service disruption or failure to respond.

**c. sudo hping3 (suitable IP Address) -1**

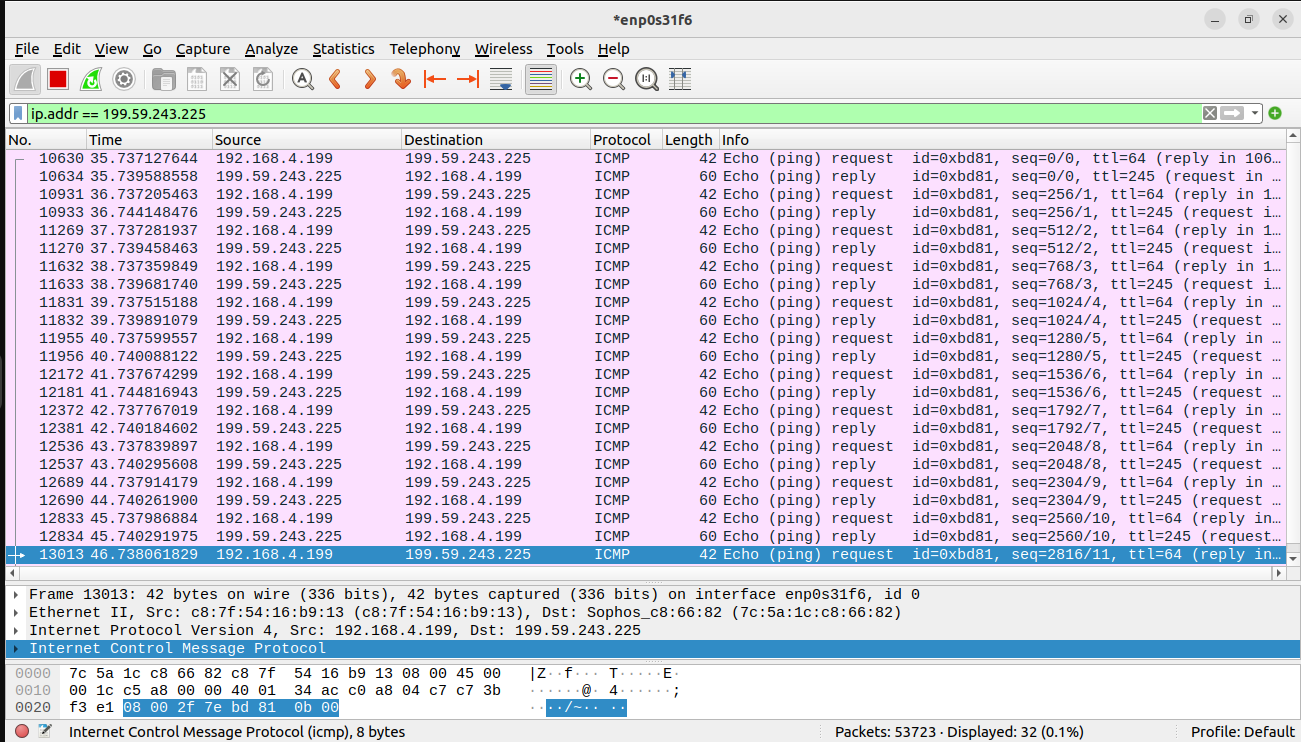


This command is used to send ICMP Echo Requests, which are commonly referred to as ping packets.

The -1 flag instructs hping3 to send these ICMP packets to the specified IP address.his type of operation is typically used for network diagnostics to test the availability of a host.

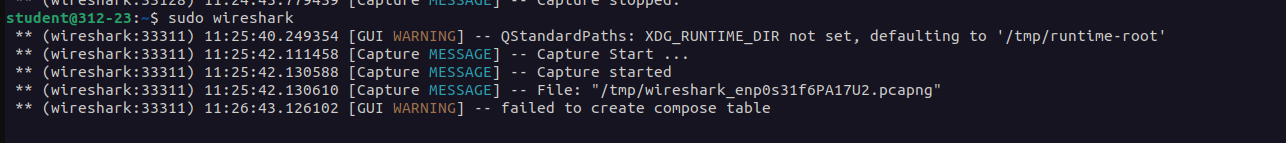


This is used to open the wireshark window and start sniffing the icmp packets that are sent.

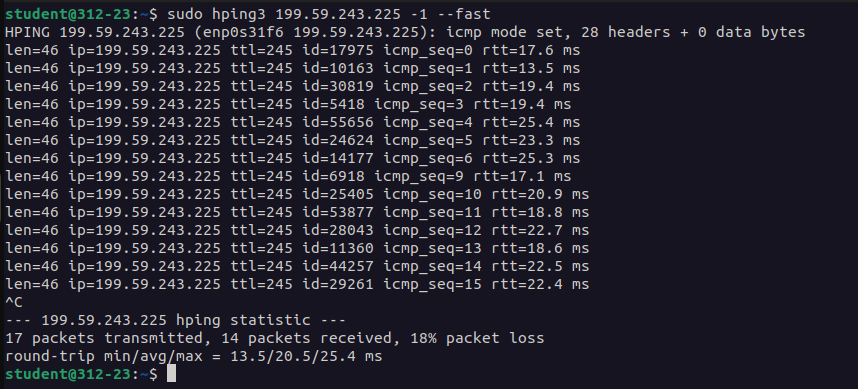


On the wireshark window, we see these packets and the network performance. We can monitor response times, packet loss, or any delays, which help in determining the status and performance of the target host and the network connection.

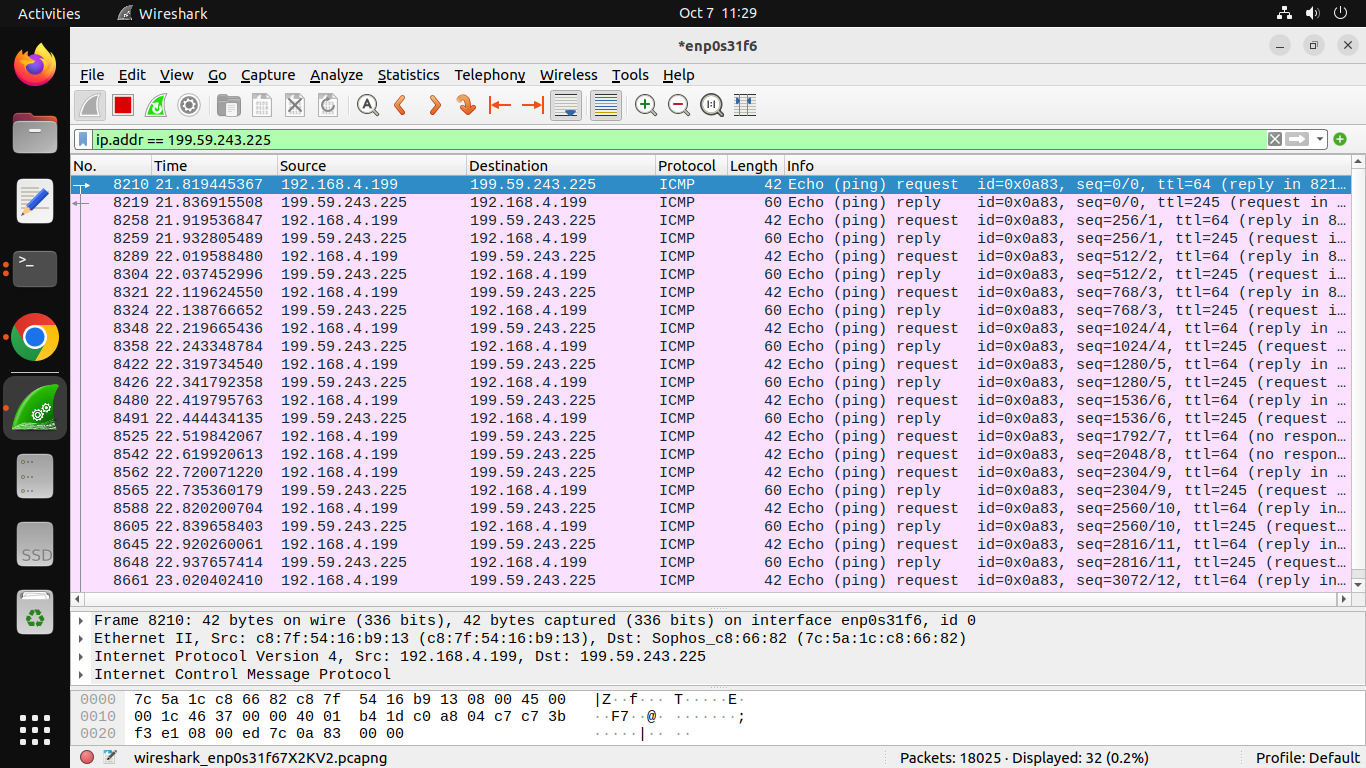
**d. sudo hping3 (suitable IP Address) -1 --fast**



This is used to open the wireshark window and start sniffing the packets that are sent.

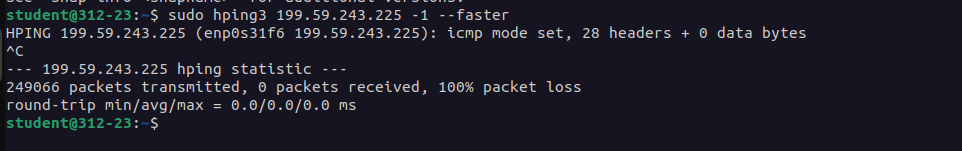


This sends ICMP Echo Requests (ping packets) to the target IP address at a much higher rate than usual. This allows us to perform high-frequency pings, which can help test network latency or packet loss.

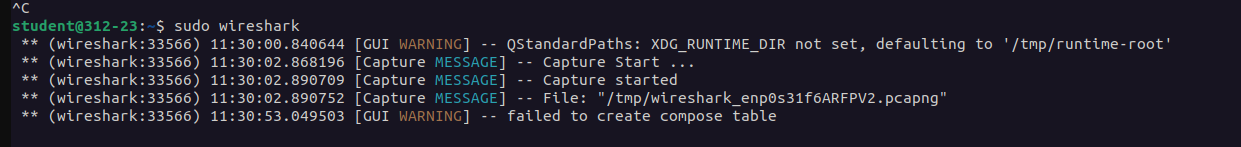


On the wireshark window, we see these packets and the network performance. We can can monitor response times, packet loss, or any delays, which help in determining the status and performance of the target host and the network connection.

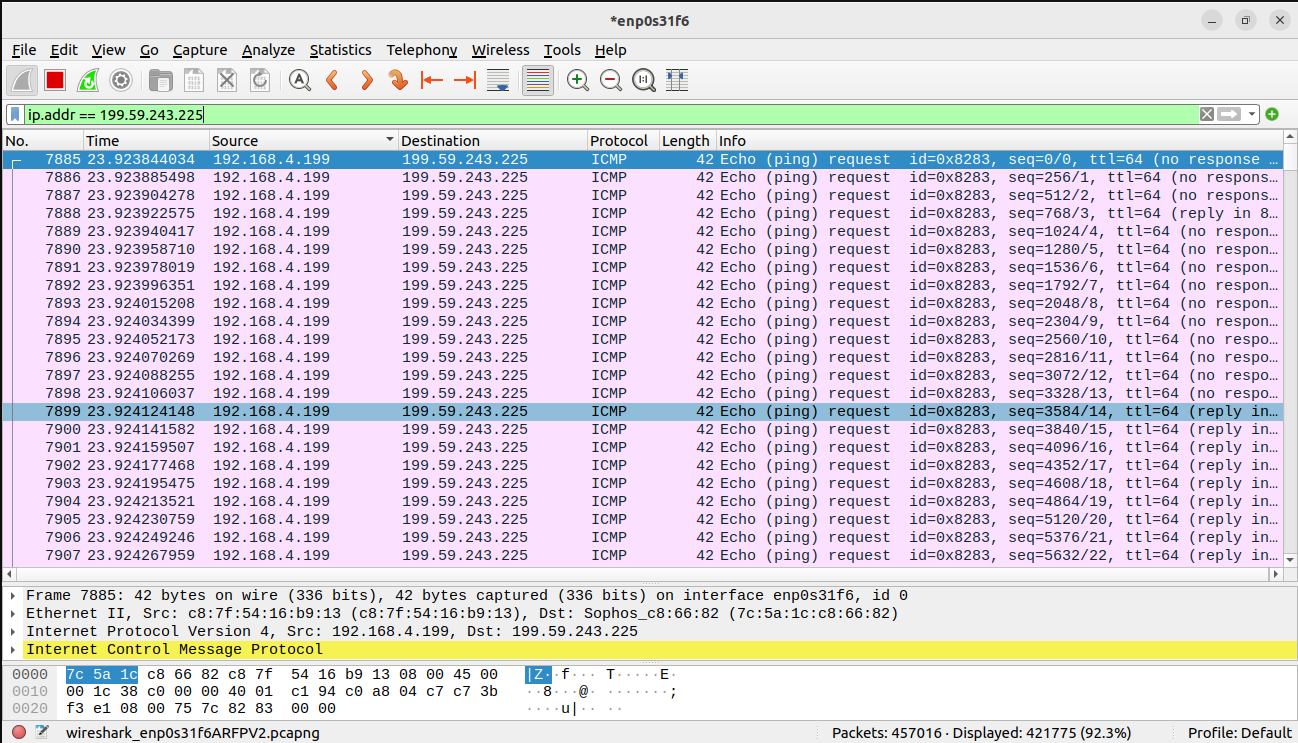
**e. sudo hping3 (suitable IP Address) -1 --faster**



THis sends ICMP Echo Requests (ping packets) to the target IP address at an even higher rate than the --fast option. The --faster option further increases the packet sending speed, typically sending packets at a rate of 100 packets per second. This creates an even more intense load on the network and the target system.



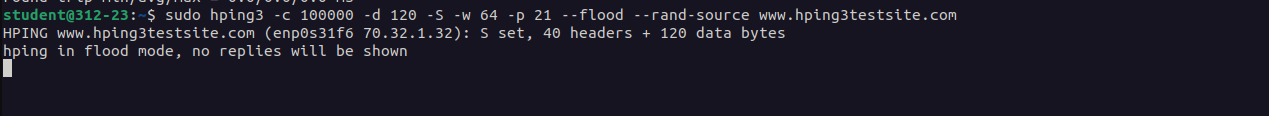
This is used to open the wireshark window and start sniffing the packets that are sent.



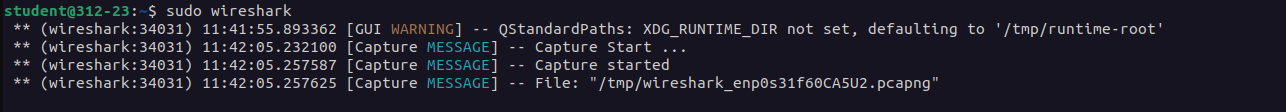
On the wireshark window, we see these packets and the network performance. We can monitor response times, packet loss, or any delays, which help in determining the status and performance of the target host and the network connection.

**f. sudo hping3 -c 10000 -d 120 -S -w 64 -p 21 --flood --rand-source**

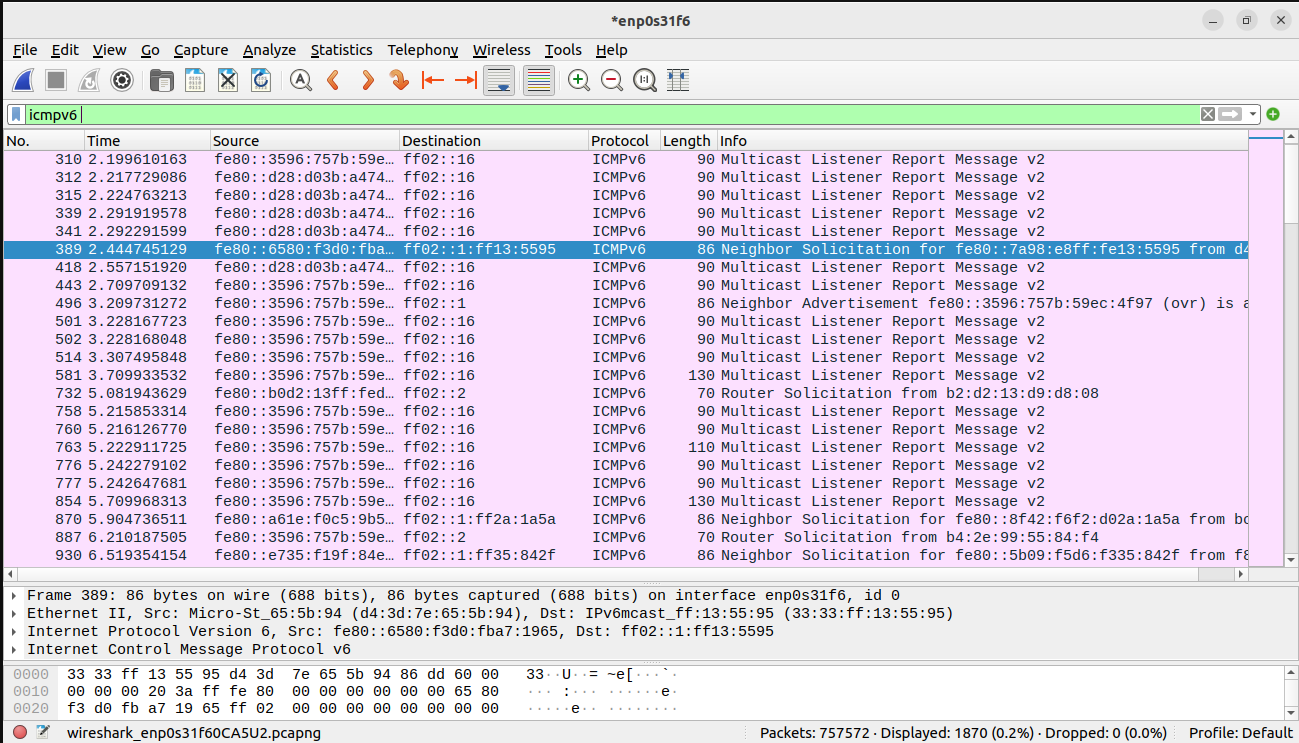
**www.hping3testsite.com or (suitable IP Address)**



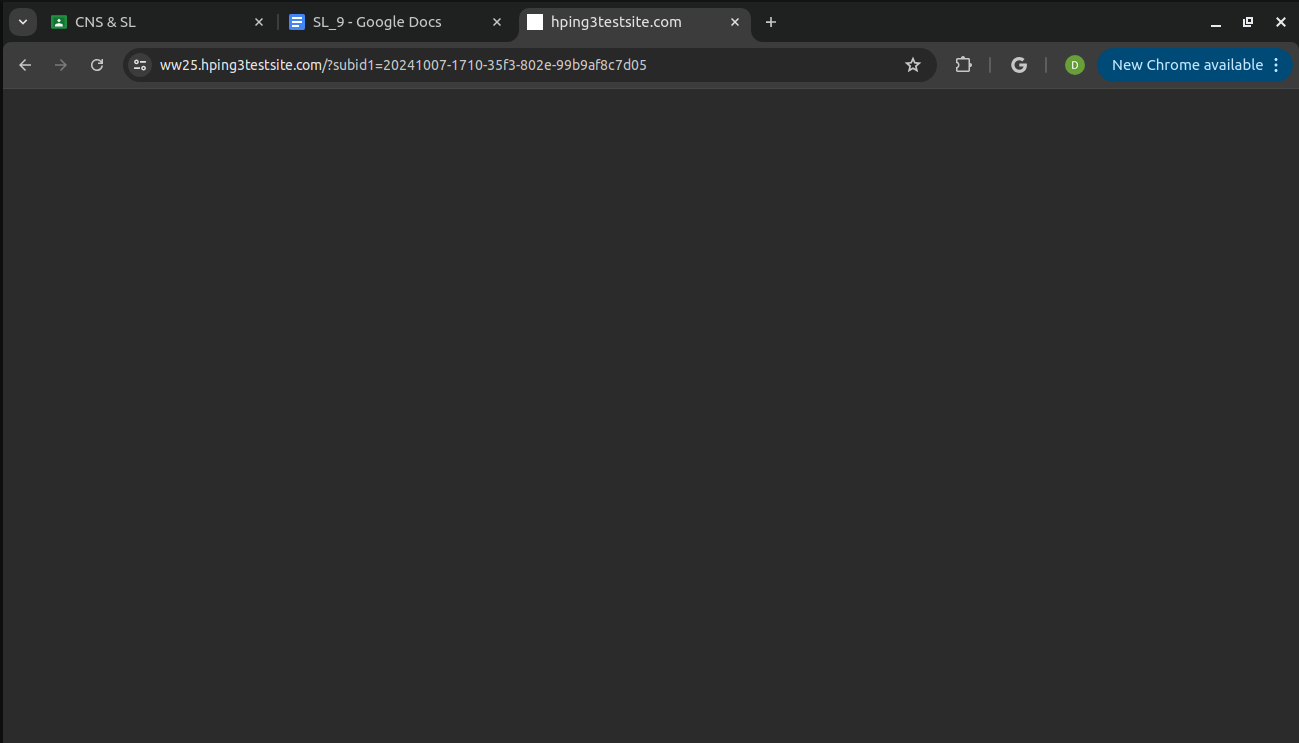
The command uses hping3 to send 10,000 SYN packets to port 21 (commonly used for FTP) on the specified domain or IP address, with a data size of 120 bytes and a window size of 64, simulating a flood attack by randomizing the source IP addresses. command.



This is used to open the wireshark window and start sniffing the packets that are sent.



Here we can see the ICMPv6 packets flooding in Wireshark, it typically means that the target is either responding to the SYN packets with ICMPv6 replies or that there is a misconfiguration causing

excessive ICMPv6 traffic. 

This flooding can saturate the network bandwidth, making it difficult for legitimate traffic to reach the target. The use of hping3 to flood a target with SYN packets can lead to overwhelming the network and server, causing it to crash or become unreachable, especially if there’s accompanying ICMPv6 flooding.