TABLE OF CONTENTS

FOOT PRINTING AND RECONNAISSANCE

- ***Foot printing:***
  - It means gathering information about a target system that can be executed to perform cyber-attack.
  - Foot printing sometimes it's also called Reconnaissance.
  - For this method hackers might use different methods or different tools.
  - This is simple method for hackers to know the information about the system and devices or network.
  - Types of Footprints:
    - ***Active Foot printing:*** It means performing foot printing by getting indirect touch with target machine.
    - ***Passive Foot printing:*** It means collecting information about a system located at remote distance from the attacker.
  - These are information gathered from foot printing:
    - Operating System from target machine.
    - IP address.
    - Firewall
    - Network Map
    - Security configurations of the target machine
    - Email ID
    - Password
    - Server Configuration
    - URL's (Uniform Resource Locator)
    - VPN (Virtual Private Network)
  - From different resources we do foot printing
    - Search Engine
    - Website
    - Social Engineering
    - DNS
    - Email Tracking
    - Social media
  - Advantages of Foot printing:
    - It allows hackers to gather the basic security configurations of target machine.
    - It is best method of vulnerabilities.
    - By using this hacker identify as to which attacker is handier to hack the target system.

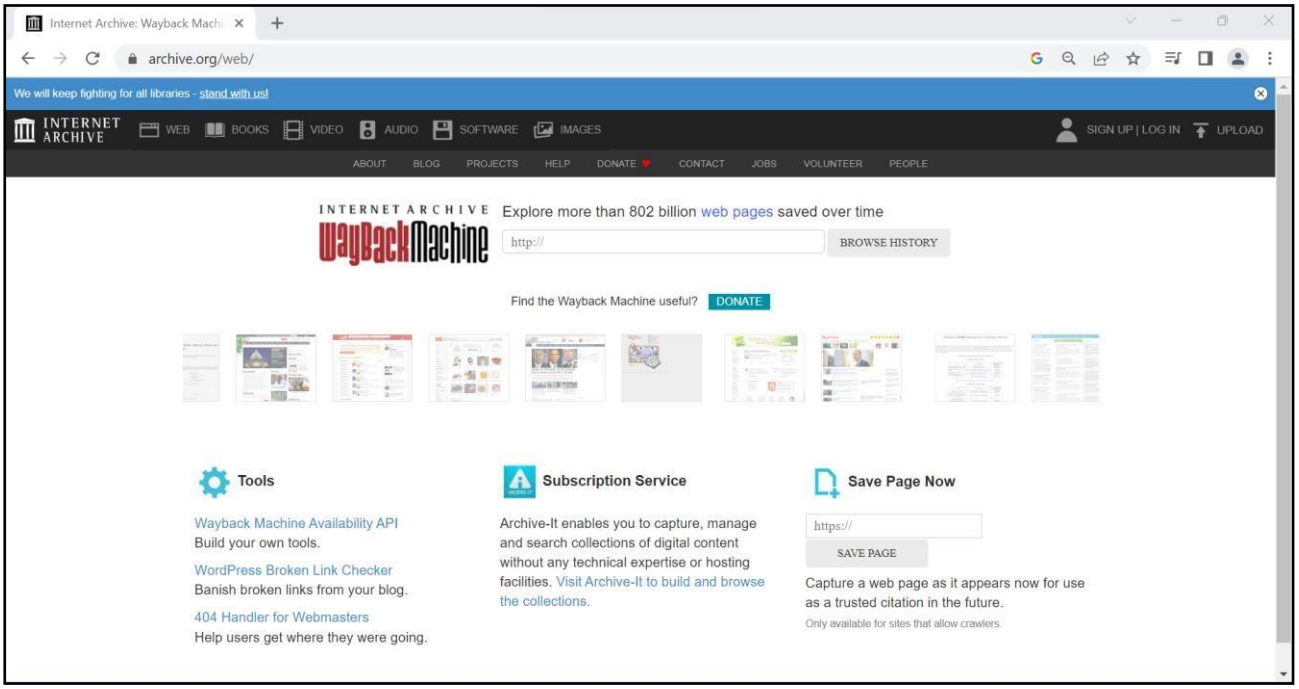
Practical work: Performing Foot printing for website

- ***Website foot printing:*** It is a technique which is used to extract the details related to website.

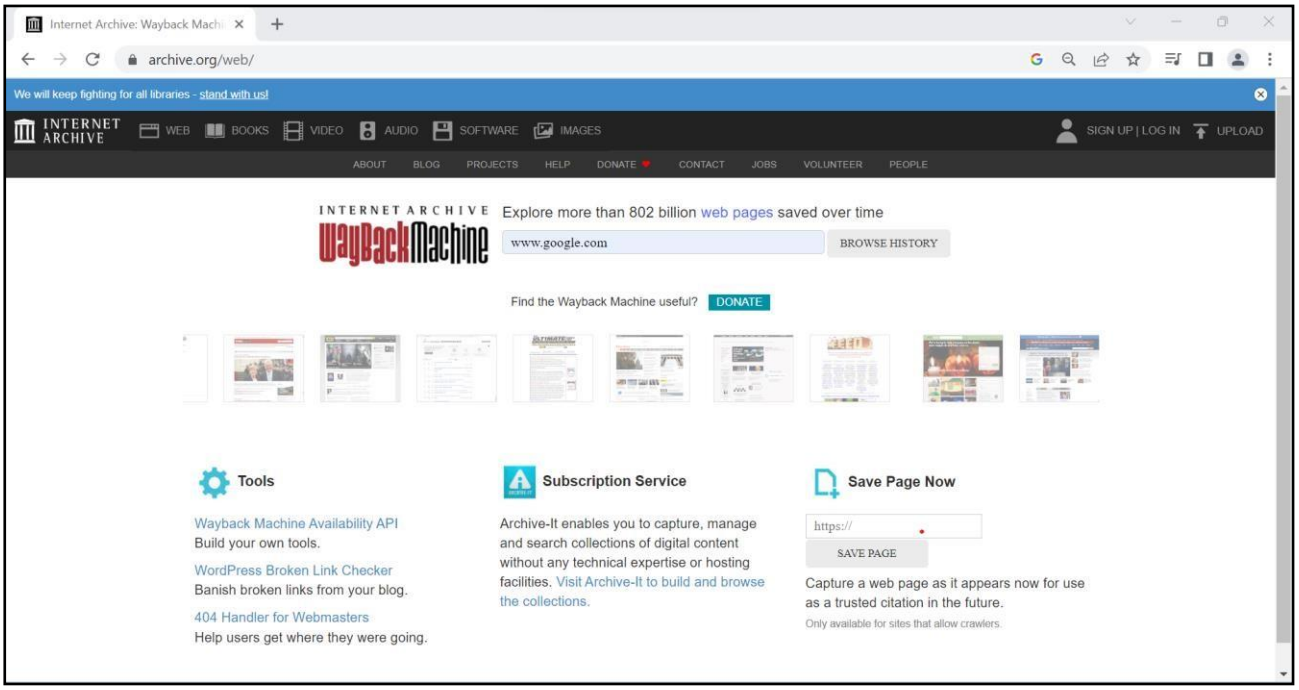
1. Using 'Internet Archive' (WayBackMachine) to perform foot printing.

    - When hacker or any user wants details of archived website or history of website, they can use https://archive.org/
    - 'archive.org' is the online tool which allows us to archived version of website.
    - It refers to the older version of the website which is existed a time before and changed one.
    - 'archive.org' is the website that collect all snapshots of all the websites at all the regular interval of the time.

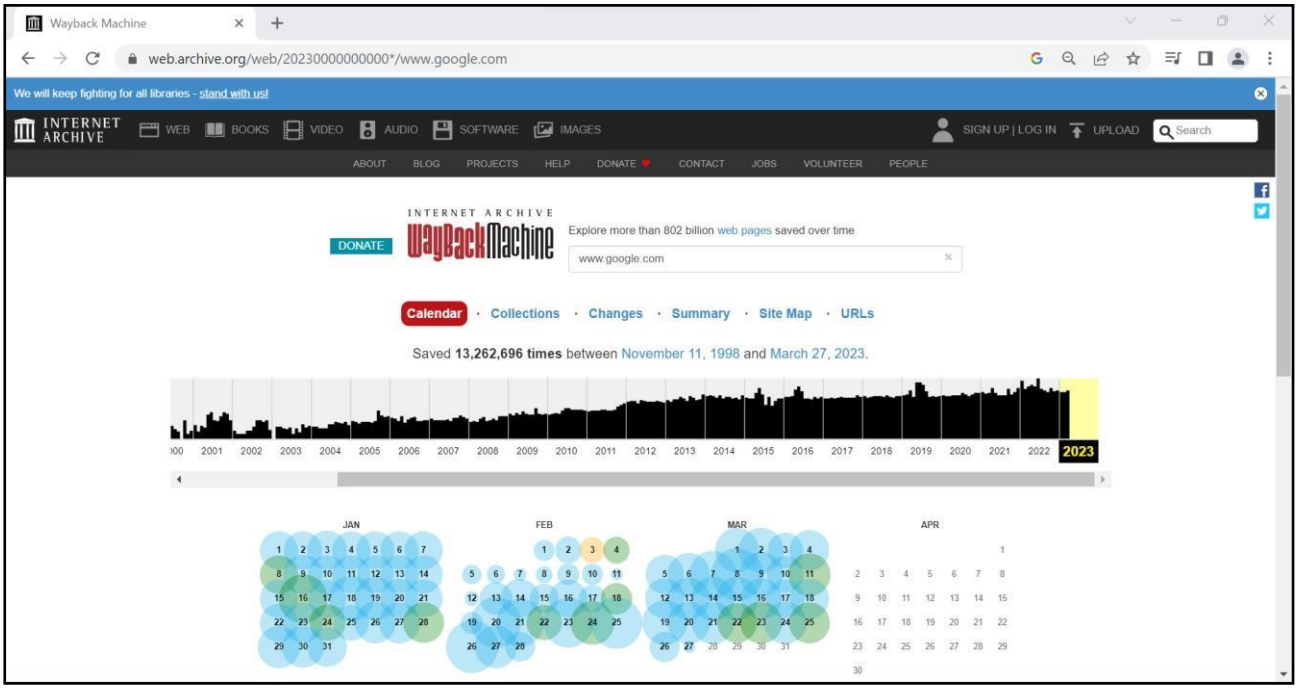
Step 1: Search for 'archive.org' on internet.



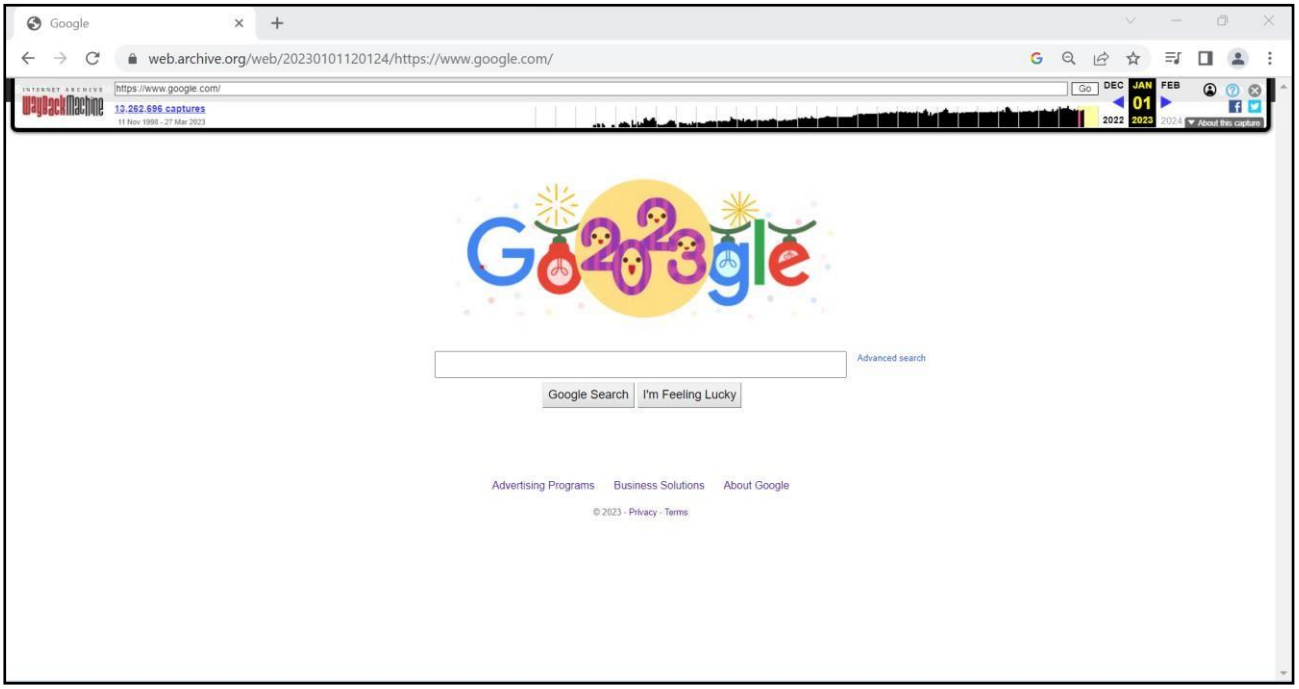
Step 2: Enter the 'URL' or 'Domain Name' to be searched. Here we are getting information regarding 'www.google.com'.



Step 3: After hitting the 'search button' it shows the calendar representing the snapshots data. Hover or select any date and then select the time to get the view of that website at the selected date and time. Here we are searching for '1st January 2023'.



Step 4: Following screen shows the website of google on 1st of January 2023.



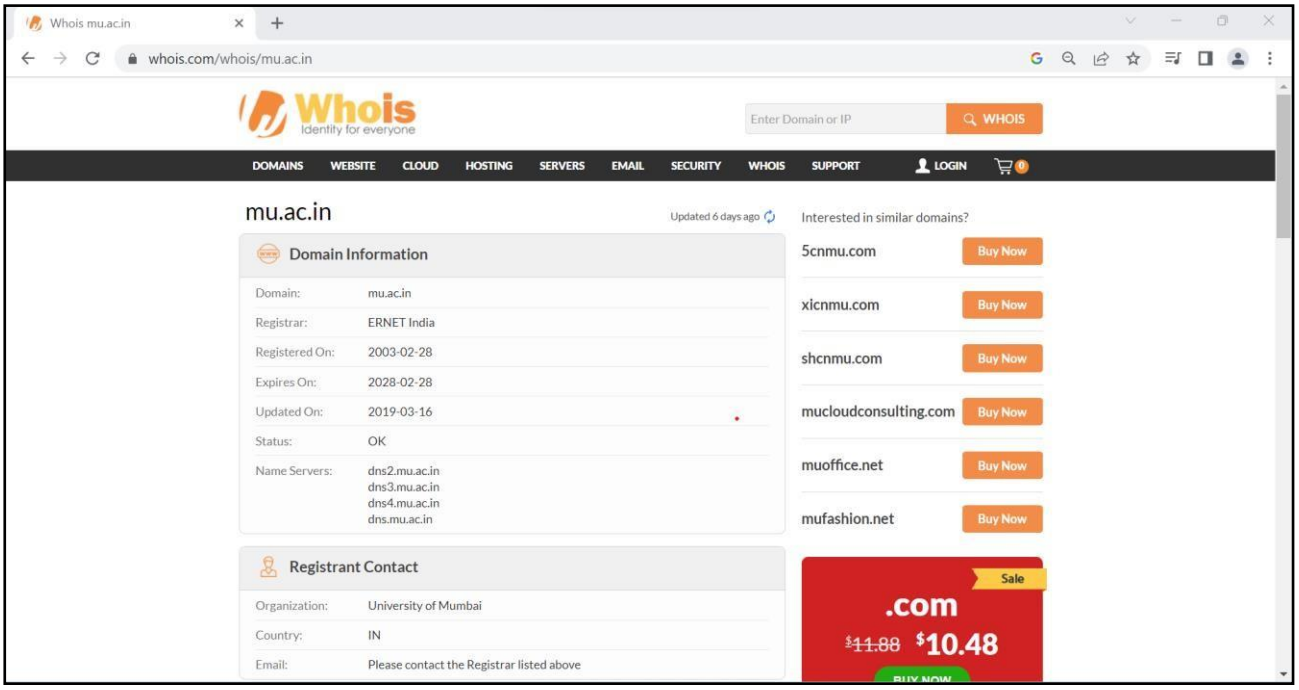
2. Using 'Whois.com' to perform foot printing (To Fetch DNS Information).

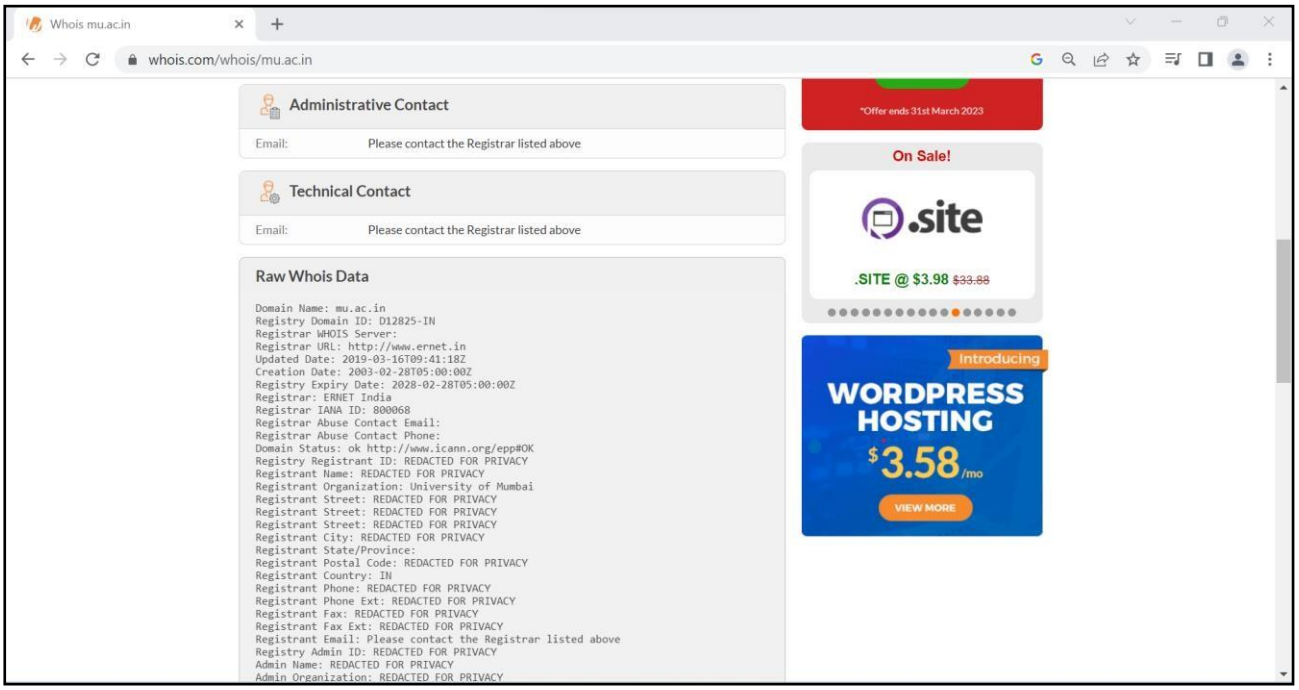
- DNS means Domain Name System. It is a system which allows us to convert Computer IP address into human readable domain name.
- A 'Whois' domain lookup allows you to trace the ownership and tenure of a domain name.
- The 'Whois' database contains details such as the registration date of the domain name, when it expires, ownership and contact information, nameserver information of the domain, the registrar via which the domain was purchased, etc.

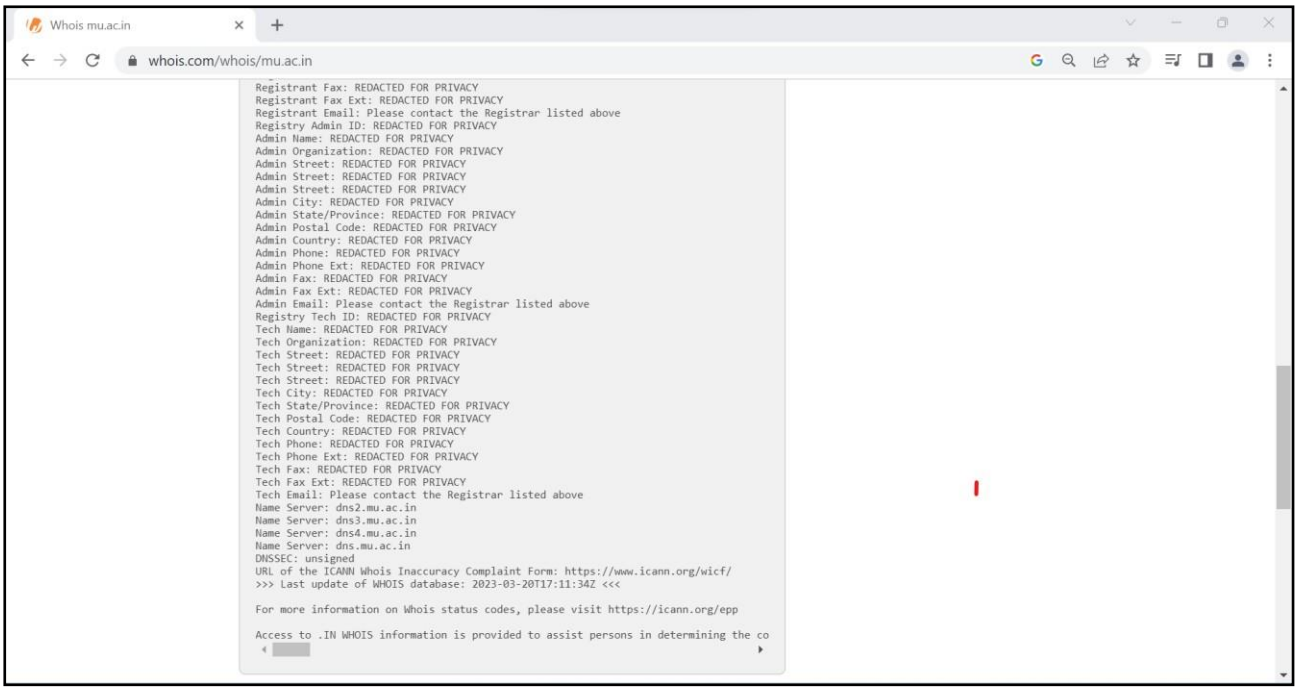
Step 1: Search for 'https://www.whois.com/' on the internet. The following page will appear.

Step 2: Search for the desired domain name for which you need the information. Here we are using 'mu.ac.in'.

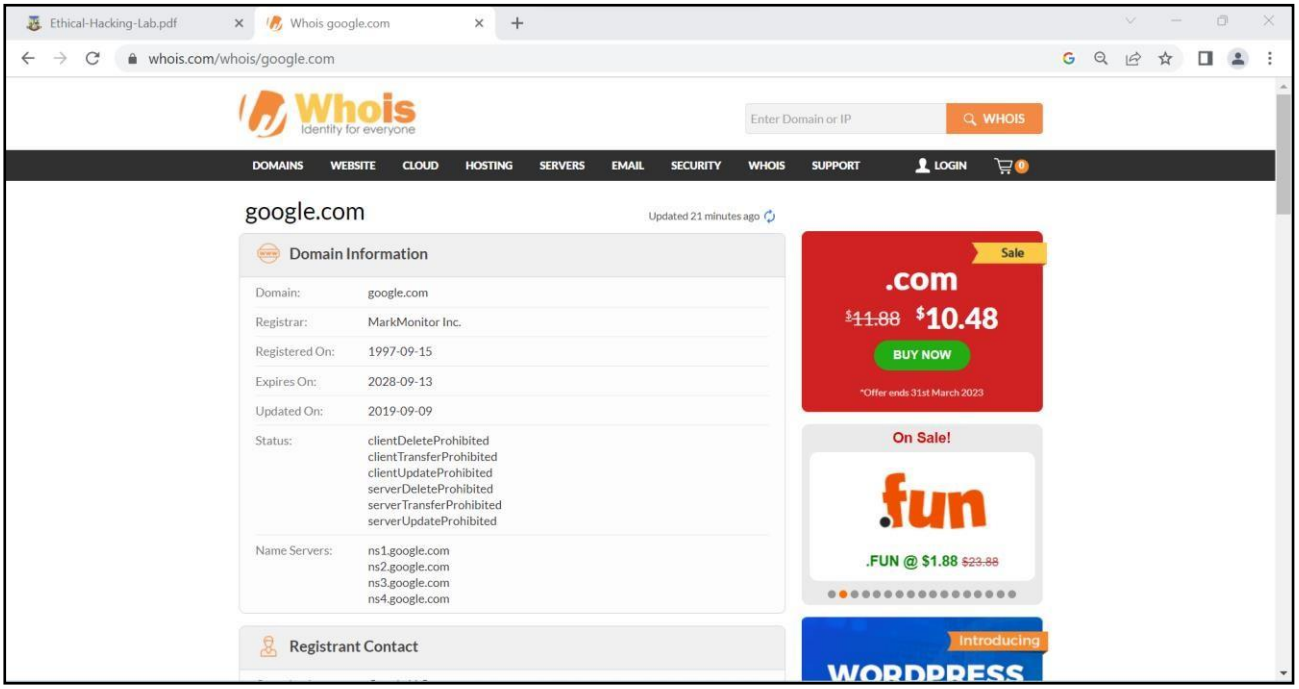
Step 3: It displays all the details for the domain name 'mu.ac.in'. Here it's showing the "Domain Information" and "Registrant Contact" and some other details.

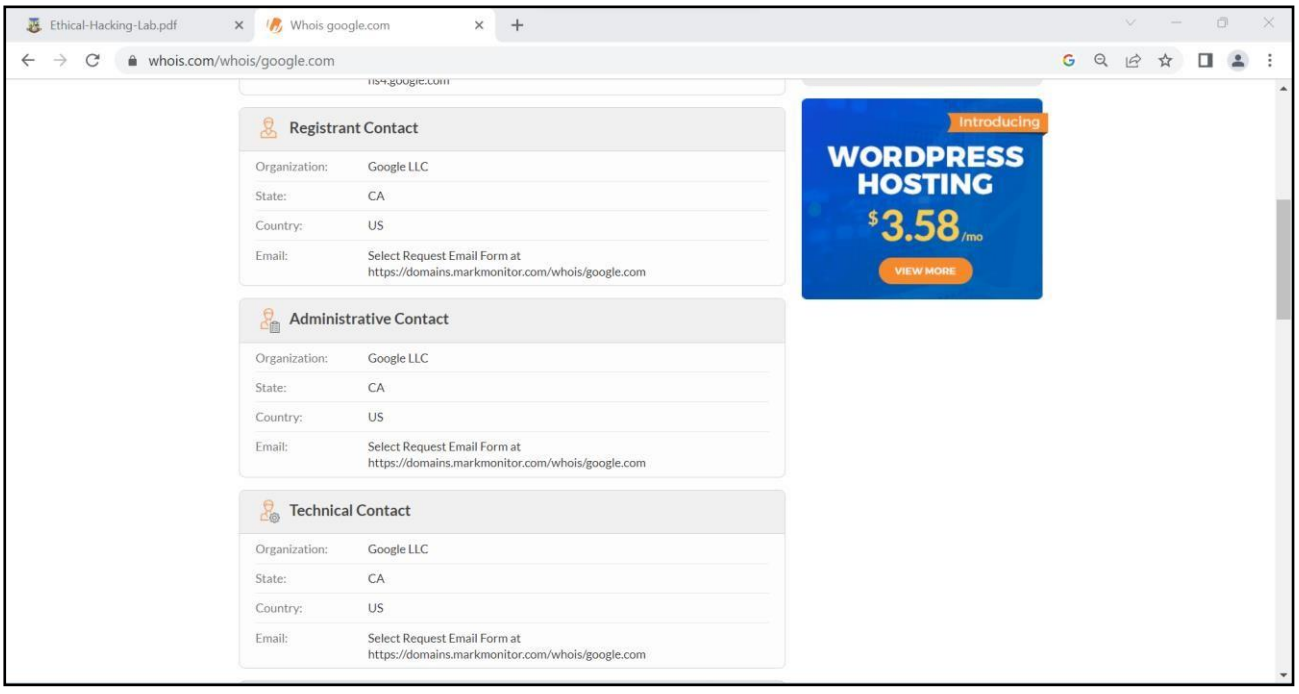



Whois mu.ac.in
whois.com/whois/mu.ac.in
Administrative Contact
Email: Please contact the Registrar listed above
Technical Contact
Email: Please contact the Registrar listed above
Raw Whois Data
Domain Name: mu.ac.in
Registry Domain ID: D12825-IN
Registrar WHOIS Server:
Registrar URL: http://www.ernet.in
Updated Date: 2019-03-16T09:41:18Z
Creation Date: 2003-02-28T05:00:00Z
Registry Expiry Date: 2028-02-28T05:00:00Z
Registrar: ERNET India
Registrar IANA ID: 800068
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Domain Status: ok http://www.icann.org/epp#OK
Registry Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: University of Mumbai
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province:
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: IN
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext: REDACTED FOR PRIVACY
Registrant Fax: REDACTED FOR PRIVACY
Registrant Fax Ext: REDACTED FOR PRIVACY
Registrant Email: Please contact the Registrar listed above
Registry Admin ID: REDACTED FOR PRIVACY
Admin Name: REDACTED FOR PRIVACY
Admin Organization: REDACTED FOR PRIVACY
*Offer ends 31st March 2023
On Sale!
.site
.SITE @ $3.98 $33.88
Introducing
WORDPRESS HOSTING
$3.58/mo
VIEW MORE


Whois mu.ac.in
whois.com/whois/mu.ac.in
Registrant Fax: REDACTED FOR PRIVACY
Registrant Fax Ext: REDACTED FOR PRIVACY
Registrant Email: Please contact the Registrar listed above
Registry Admin ID: REDACTED FOR PRIVACY
Admin Name: REDACTED FOR PRIVACY
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin City: REDACTED FOR PRIVACY
Admin State/Province: REDACTED FOR PRIVACY
Admin Postal Code: REDACTED FOR PRIVACY
Admin Country: REDACTED FOR PRIVACY
Admin Phone: REDACTED FOR PRIVACY
Admin Phone Ext: REDACTED FOR PRIVACY
Admin Fax: REDACTED FOR PRIVACY
Admin Fax Ext: REDACTED FOR PRIVACY
Admin Email: Please contact the Registrar listed above
Registry Tech ID: REDACTED FOR PRIVACY
Tech Name: REDACTED FOR PRIVACY
Tech Organization: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech City: REDACTED FOR PRIVACY
Tech State/Province: REDACTED FOR PRIVACY
Tech Postal Code: REDACTED FOR PRIVACY
Tech Country: REDACTED FOR PRIVACY
Tech Phone: REDACTED FOR PRIVACY
Tech Phone Ext: REDACTED FOR PRIVACY
Tech Fax: REDACTED FOR PRIVACY
Tech Fax Ext: REDACTED FOR PRIVACY
Tech Email: Please contact the Registrar listed above
Name Server: dns2.mu.ac.in
Name Server: dns3.mu.ac.in
Name Server: dns4.mu.ac.in
Name Server: dns.mu.ac.in
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of WHOIS database: 2023-03-20T17:11:34Z <<<
For more information on Whois status codes, please visit https://icann.org/epp
Access to .IN WHOIS information is provided to assist persons in determining the co

Data for 'www.google.com'





Raw Whois Data

```
Domain Name: google.com
Registry Domain ID: 2138514_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2019-09-09T15:39:04+0000
Creation Date: 1997-09-15T07:00:00+0000
Registrar Registration Expiration Date: 2028-09-13T07:00:00+0000
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2086851750
Domain Status: clientUpdateProhibited
(https://www.icann.org/epp#clientUpdateProhibited)
Domain Status: clientTransferProhibited
(https://www.icann.org/epp#clientTransferProhibited)
Domain Status: clientDeleteProhibited
(https://www.icann.org/epp#clientDeleteProhibited)
Domain Status: serverUpdateProhibited
(https://www.icann.org/epp#serverUpdateProhibited)
Domain Status: serverTransferProhibited
(https://www.icann.org/epp#serverTransferProhibited)
Domain Status: serverDeleteProhibited
(https://www.icann.org/epp#serverDeleteProhibited)
Registrant Organization: Google LLC
Registrant State/Province: CA
Registrant Country: US
Registrant Email: Select Request Email Form at
https://domains.markmonitor.com/whois/google.com
Admin Organization: Google LLC
Admin State/Province: CA
Admin Country: US
Admin Email: Select Request Email Form at
https://domains.markmonitor.com/whois/google.com
Tech Organization: Google LLC
Tech State/Province: CA
Tech Country: US
Tech Email: Select Request Email Form at
https://domains.markmonitor.com/whois/google.com
Name Server: ns2.google.com
Name Server: ns4.google.com
Name Server: ns1.google.com
Name Server: ns3.google.com
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System:
http://wdprs.internic.net/
>>> Last update of WHOIS database: 2023-03-20T08:47:05+0000 <<<

For more information on WHOIS status codes, please visit:
   https://www.icann.org/resources/pages/epp-status-codes

If you wish to contact this domain's Registrant, Administrative, or
Technical contact, and such email address is not visible above, you may
do so via our web form, pursuant to ICANN's Temporary Specification. To
verify that you are not a robot, please enter your email address to
receive a link to a page that facilitates email communication with the
relevant contact(s).
```

Web-based WHOIS:
https://domains.markmonitor.com/whois
If you have a legitimate interest in viewing the non-public WHOIS details, send your request and the reasons for your request to whoisrequest@markmonitor.com and specify the domain name in the subject line. We will review that request and may ask for supporting documentation and explanation.

The data in MarkMonitor's WHOIS database is provided for information purposes, and to assist persons in obtaining information about or related to a domain name's registration record. While MarkMonitor believes the data to be accurate, the data is provided "as is" with no guarantee or warranties regarding its accuracy.

By submitting a WHOIS query, you agree that you will use this data only for lawful purposes and that, under no circumstances will you use this data to:
(1) allow, enable, or otherwise support the transmission by email, telephone, or facsimile of mass, unsolicited, commercial advertising, or spam; or
(2) enable high volume, automated, or electronic processes that send queries, data, or email to MarkMonitor (or its systems) or the domain name contacts (or its systems).

MarkMonitor reserves the right to modify these terms at any time.

By submitting this query, you agree to abide by this policy.

MarkMonitor Domain Management(TM)
Protecting companies and consumers in a digital world.
Visit MarkMonitor at https://www.markmonitor.com
Contact us at +1.8007459229
In Europe, at +44.02032062220
--

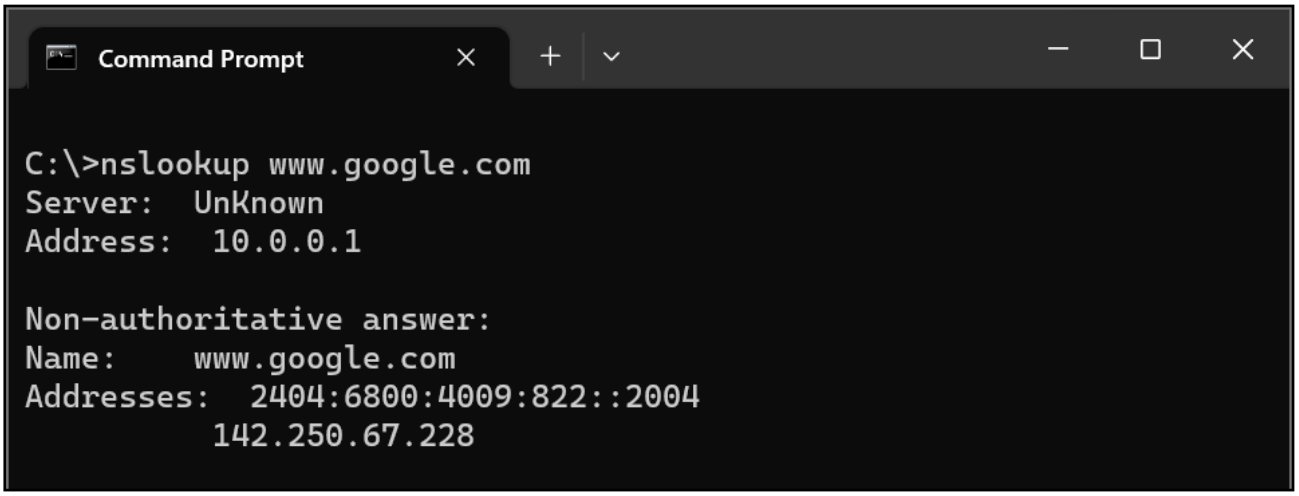
3. Using 'NS lookup' to perform foot printing.

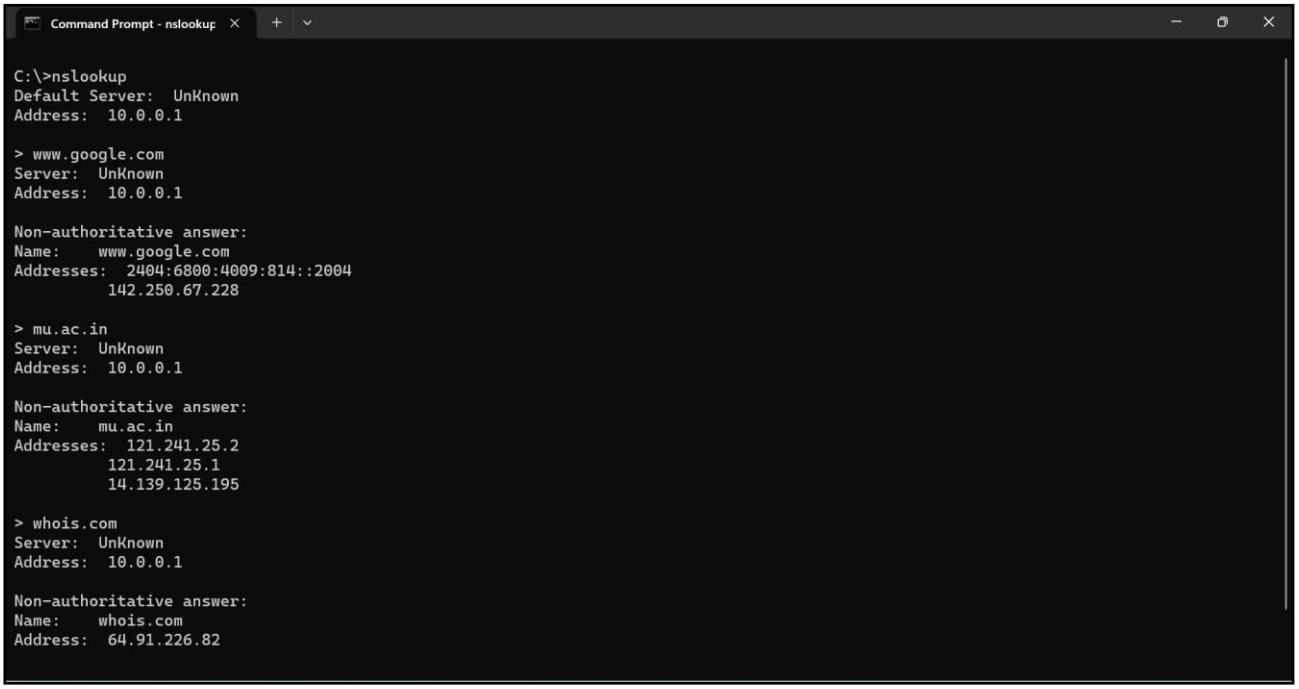
- Name server lookup (nslookup) is a command-line tool that lets you find the internet protocol (IP) address or domain name system (DNS) record of a specific hostname.
- This command also allows reverse DNS lookup by inputting the IP addresses of the corresponding domains.

a. Using nslookup command to get IP

In command prompt type nslookup and hit enter then type any of the desired domain name to get IP or write nslookup and domain name together.

```
Command: nslookup <any domain name>
Example: nslookup www.google.com
```

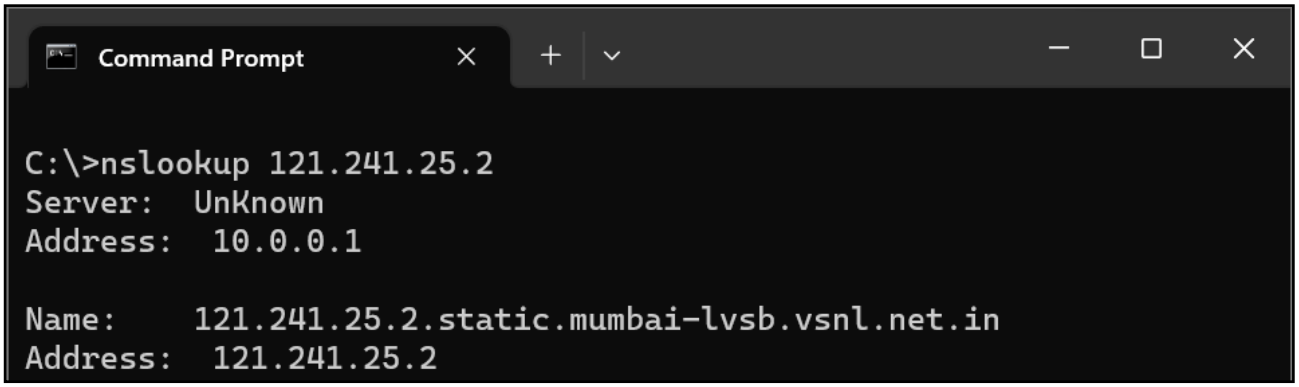




b. Using nslookup command in a reverse manner.

In this case we get the name from the IP.

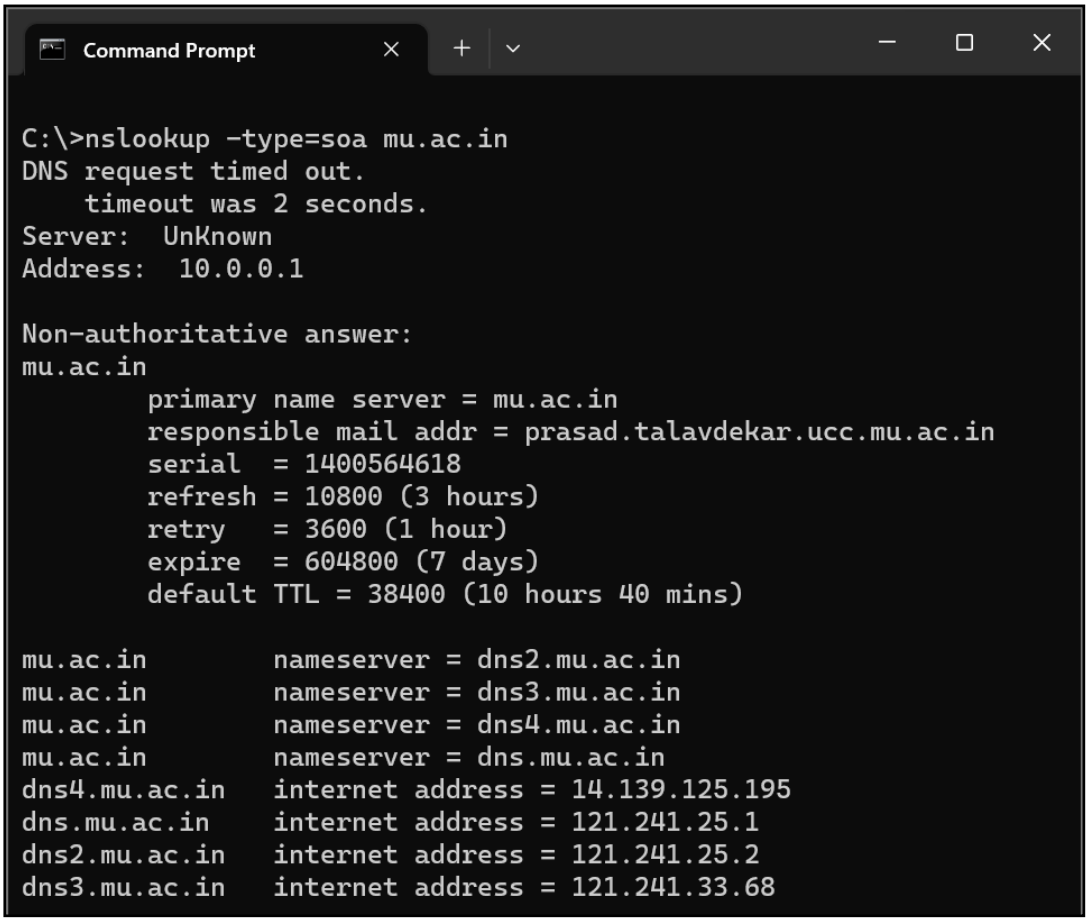
```
Command: nslookup <any ip address>
Example: nslookup 121.241.25.2 (mu.ac.in)
```



c. Using nslookup command to get important information regarding the domain.

This will query the standard of authority (SOA) record containing important information about the specified domain. For example, you want to get an authoritative response for the domain mu.ac.in:

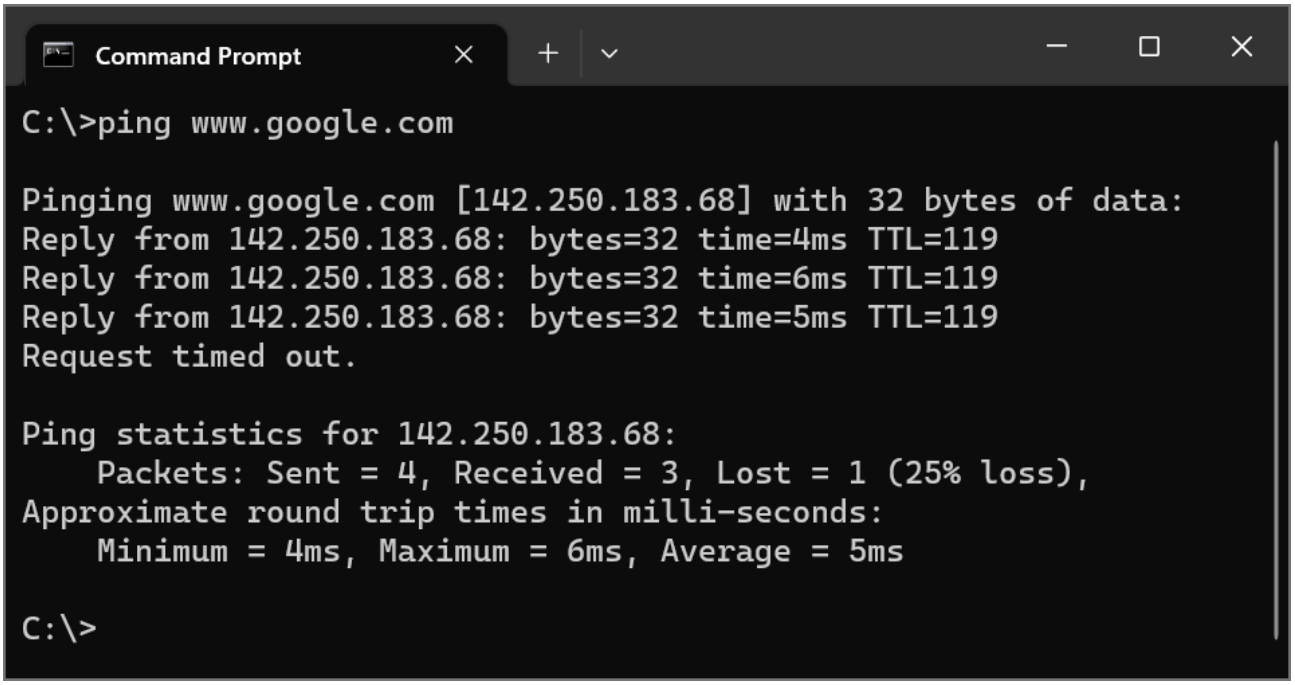
```
Command: nslookup -type=soa domainname.tld
Example: nslookup -type=soa mu.ac.in
```

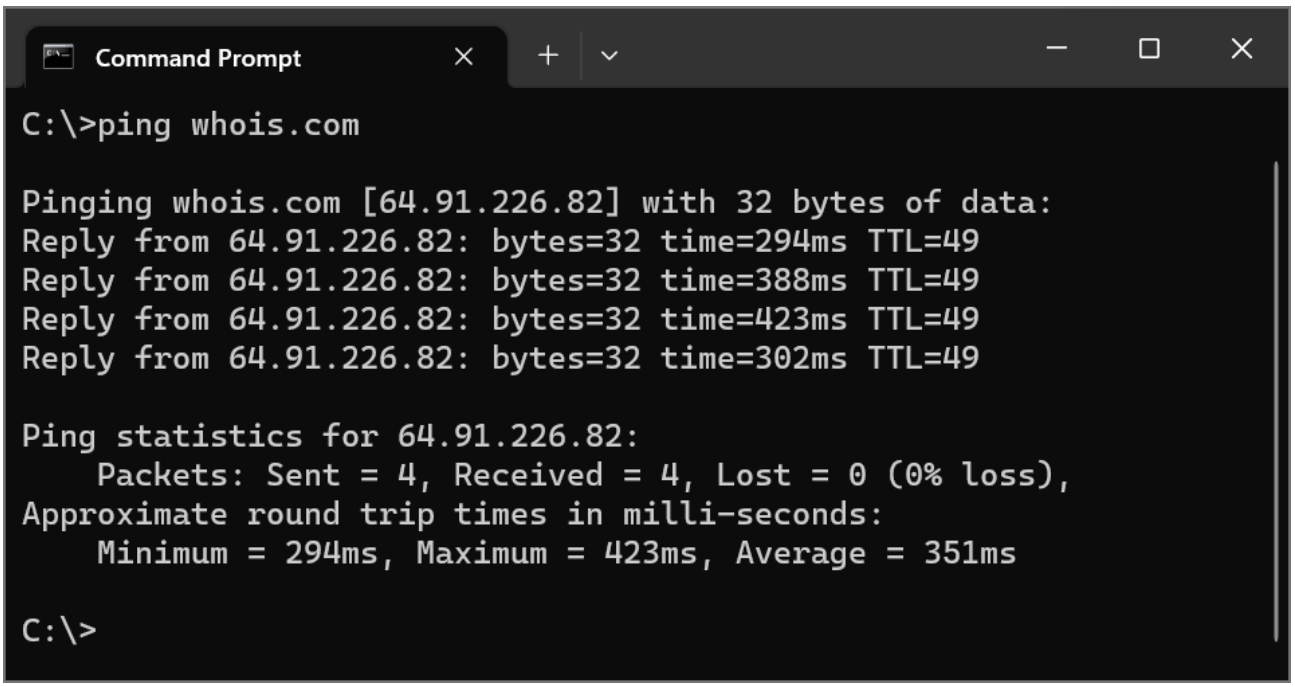


4. Using 'ping' to perform foot printing.

- Ping is a command-line utility, available on virtually any operating system with network connectivity, that acts as a test to see if a networked device is reachable.
- The ping command sends a request over the network to a specific device. A successful ping results in a response from the computer that was pinged back to the originating computer.

```
Command: ping <domain name>
Example: ping www.google.com or ping mu.ac.in
```





SCANNING NETWORKS, ENUMERATION AND SNIFFING

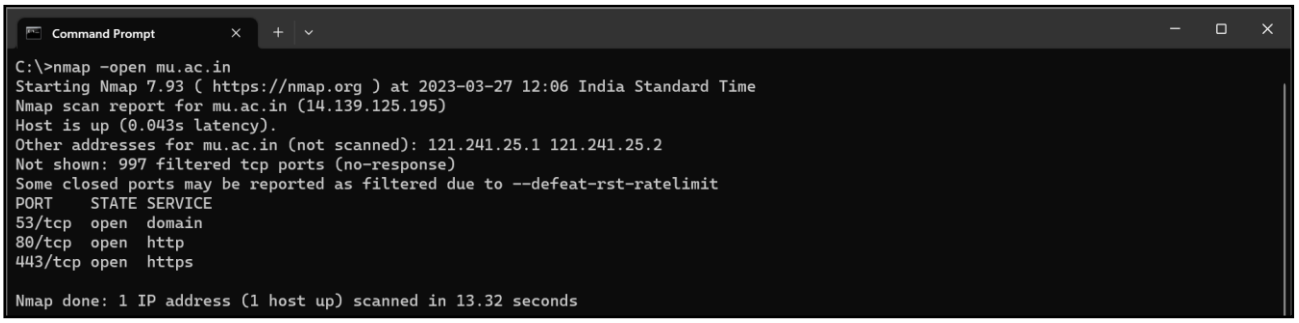
- ***Port Scanning***:
  - A port is a virtual location where networking communication starts and ends (in a nutshell).
  - A port scanner is a computer program that examines network ports for one of three possible condition – open, closed, or filtered.
  - Port scanning can provide information such as:
    - Services that are running.
    - Users who own services.
    - Whether unknown logins are allowed.
    - Which network services require authentication.
  - Port scanners are valuable tools in diagnosing network and connectivity issues.
  - However, attackers use port scanners to detect possible access points for intrusion and to identify what kinds of devices you are running on the network, like firewalls, proxy servers or VPN servers.
  - Some of the Port Scanning Tools are as follows:
    - Nmap
    - SolarWinds Port Scanner
    - Netcat
    - Advanced Port Scanner
    - Net Scan Tools

- ***Nmap Tool***
  - Nmap is a free, open source and multi-platform network security scanner used for network discovery and security auditing.
  - Nmap can be extremely useful for helping you get to the root of the problem you are investigating, verify firewall rules or validate your routing tables are configured correctly.

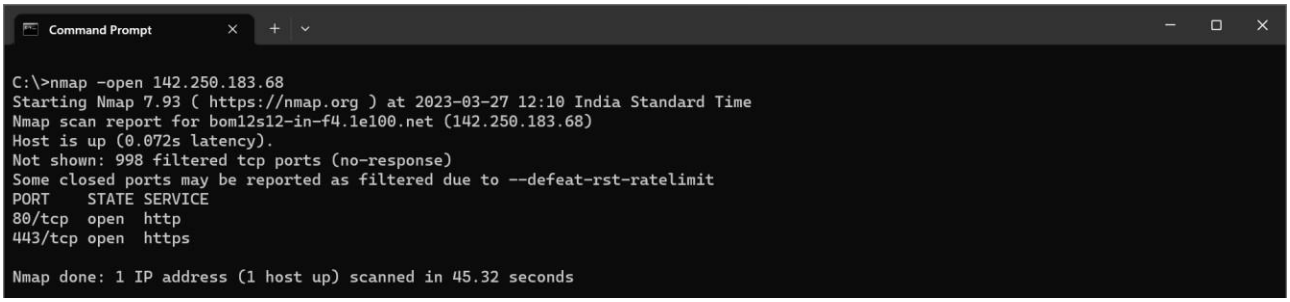
1. Using 'Nmap' to perform scan for ports.

i. *Scan open ports:* This functionality is used to scan for open ports.

Command: nmap -open <ip address / URL>
Example: nmap -open mu.ac.in

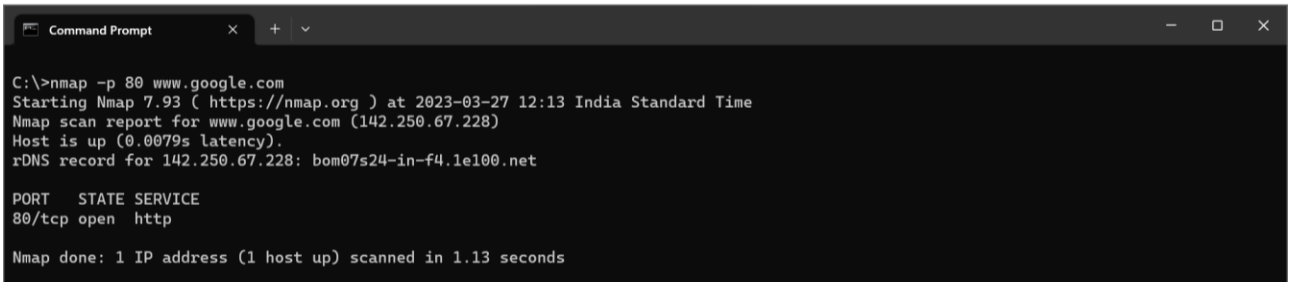


Example: nmap -open 142.250.183.68

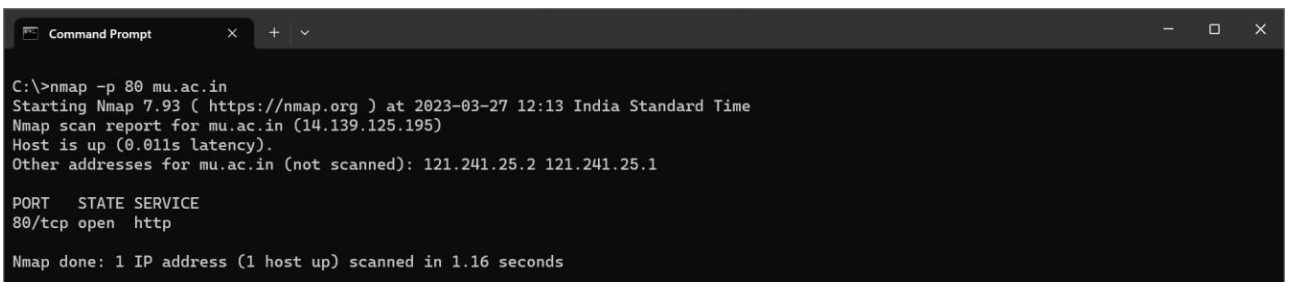


ii. *Scan single ports:* This functionality is used to scan for specified port.

Command: nmap -p <port number> <ip address / URL>
Example: nmap -p 80 www.google.com

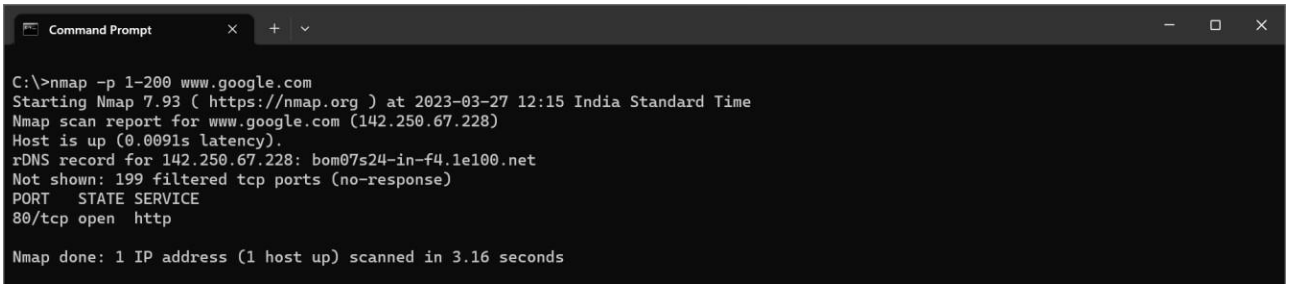


Example: nmap -p 80 www.google.com

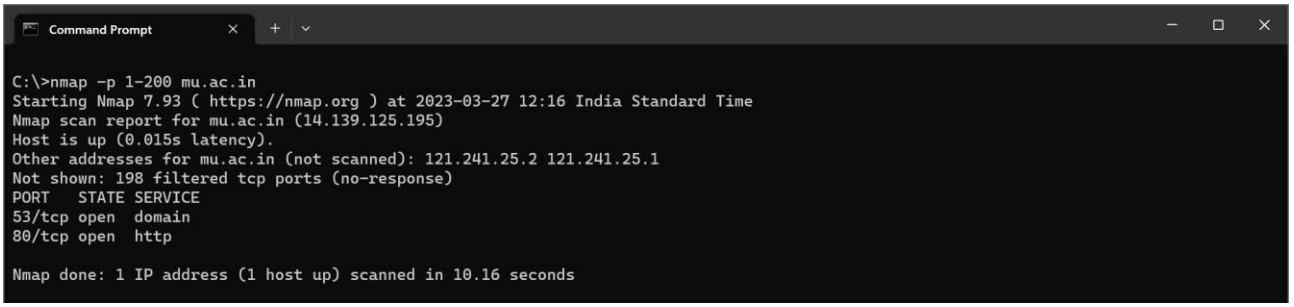


iii. *Scan specified range of ports:* This functionality scans the specified range of ports.

Command: nmap -p <port range> <ip address / URL>
Example: nmap -p 1-200 www.google.com

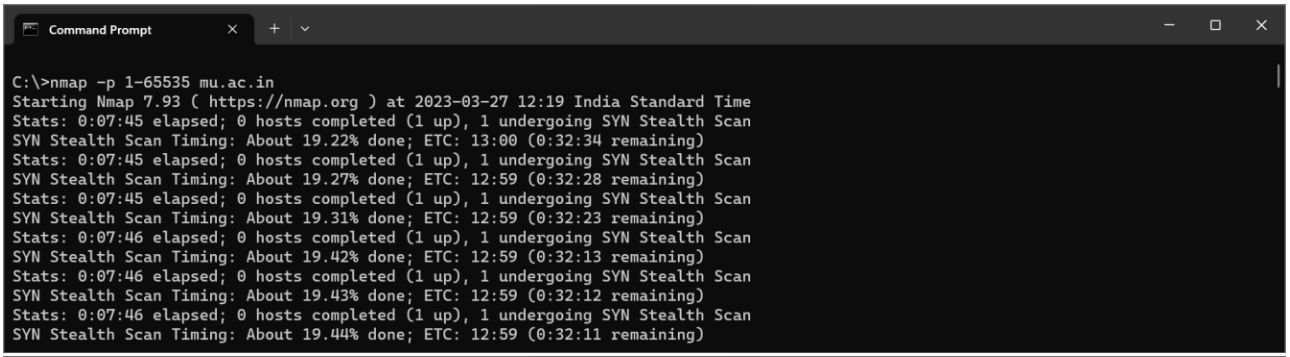


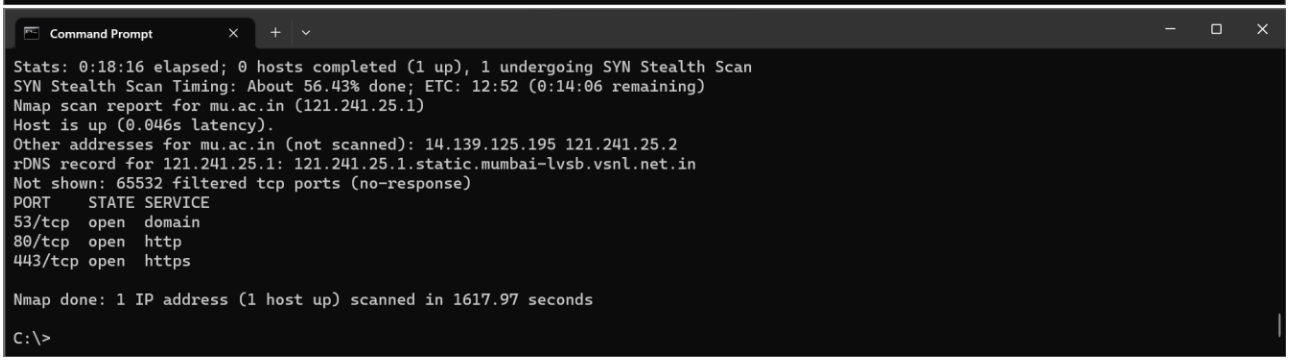
Example: nmap -p 1-200 mu.ac.in



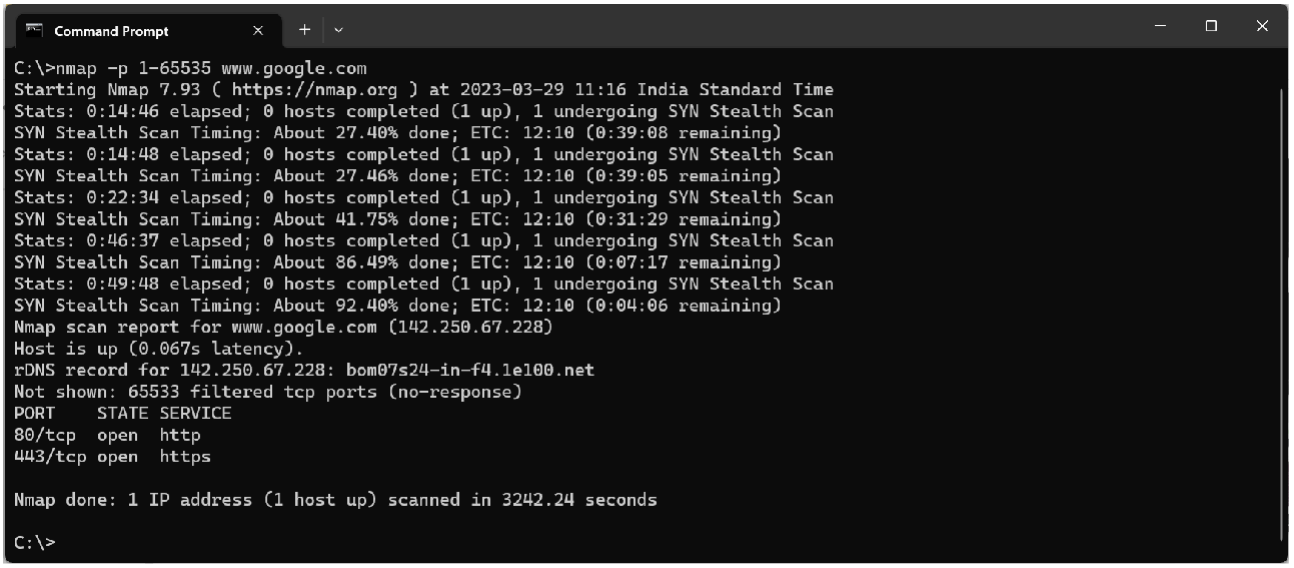
iv. *Scan entire range of ports:* This functionality scans the entire range of ports.

Command: nmap -p <port range> <ip address / URL>
Example: nmap -p 1-65535 mu.ac.in



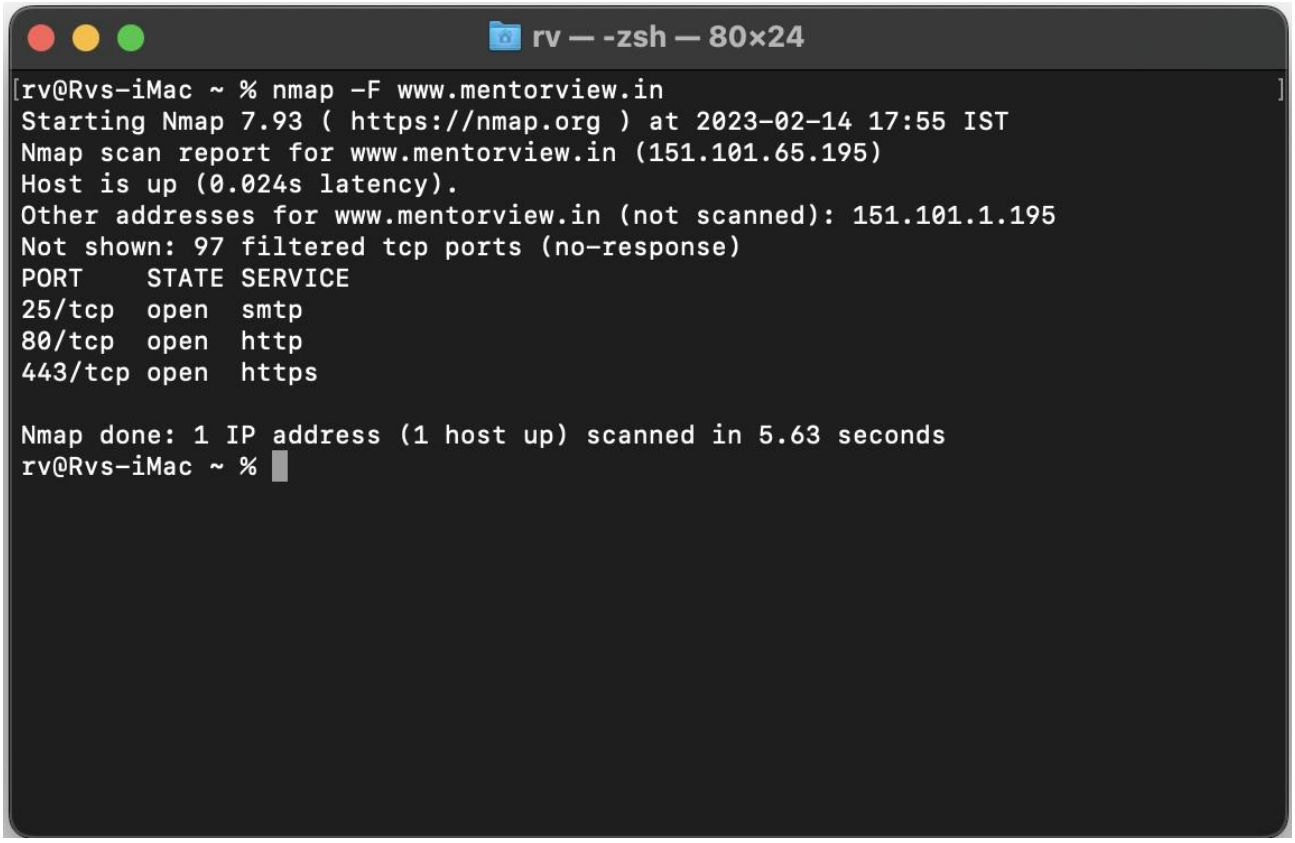


Example: nmap -p 1-65535 www.google.com



v. *Scan top 100 ports (fast scan):* This functionality scans the top 100 ports and its done very fast.

Command: nmap -F <ip address / URL>
Example: nmap -F www.mentorview.in

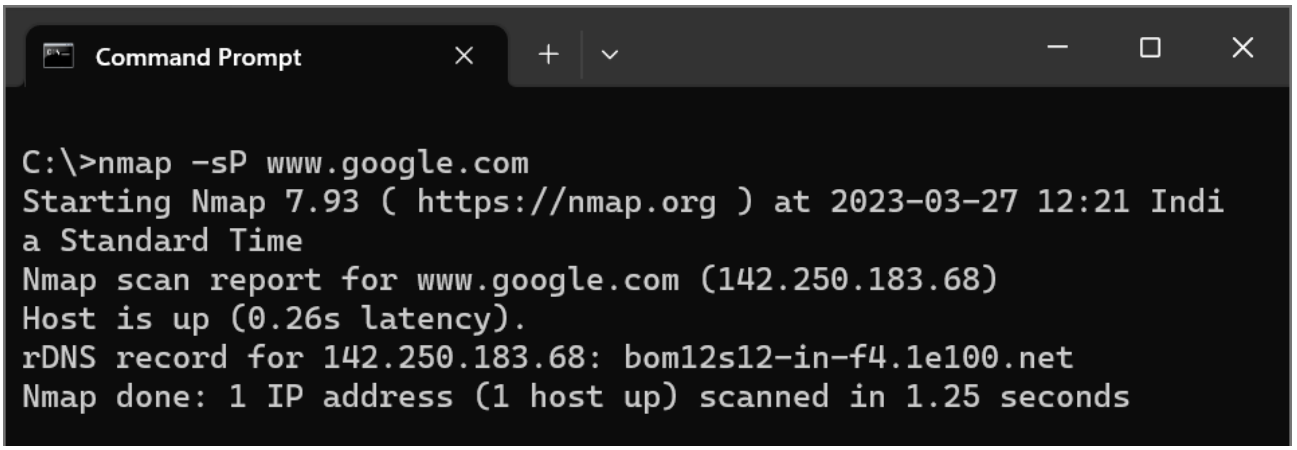


- ***Network Scanning***:
  - Network scanning is a technique that is used to gather information regarding computing systems by making the use of a computer network.
  - Network scanning is mainly used for security assessment, system maintenance, and also for performing attacks by hackers.
  - The purpose of network scanning is as follows:
    - Recognize available UDP and TCP network services running on the targeted hosts.
    - Recognize filtering systems between the user and the targeted hosts.
    - Determine the operating systems (OSs) in use by assessing IP responses.
    - Evaluate the target host's TCP sequence number predictability to determine sequence prediction attack and TCP spoofing.
  - Some of the Top Network Scanning Tools (IP and Network Scanner) are as follows:
    - SolarWinds Network Device Scanner
    - Wireshark
    - Angry IP Scanner
    - Advanced IP Scanner
    - Qualys Freescan
    - Nmap
- Nmap Tool:
  - Nmap is also used to scan networks.
  - Nmap is now one of the core tools used by network administrators to map their networks.
  - The program can be used to find:
    - Live hosts on a network
    - Perform port scanning
    - Ping sweeps
    - OS detection
    - Version detection

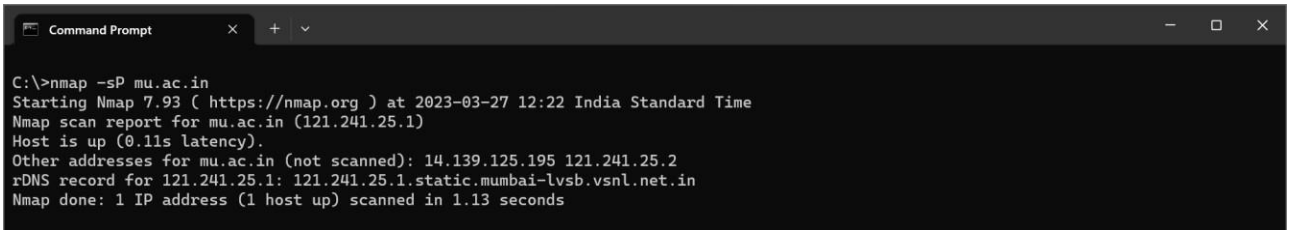
2. Using 'Nmap' to perform scan for network.

i. *Ping Scan:* It returns a list of hosts on your network and the total number of assigned IP addresses. If you spot any hosts or IP addresses on this list that you cannot account for, you can then run further commands to investigate them further.

```
Command: nmap -sP <ip address / URL>
Example: nmap -sP www.google.com
```

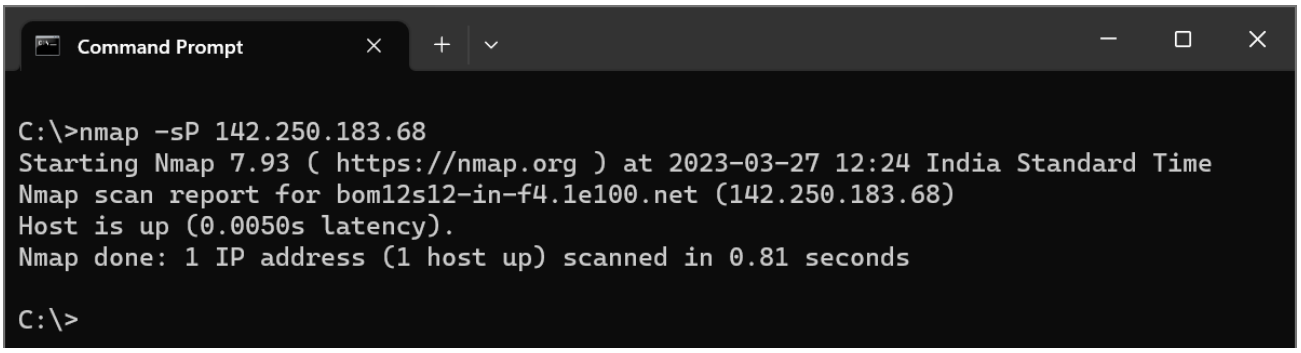



```
Example: nmap -sP mu.ac.in
```



ii. *Host Scan:* A host scan actively sends ARP request packets to all the hosts connected to your network. Each host then responds to this packet with another ARP packet containing its status and MAC address. This can be a powerful way of spotting suspicious hosts connected to your network.

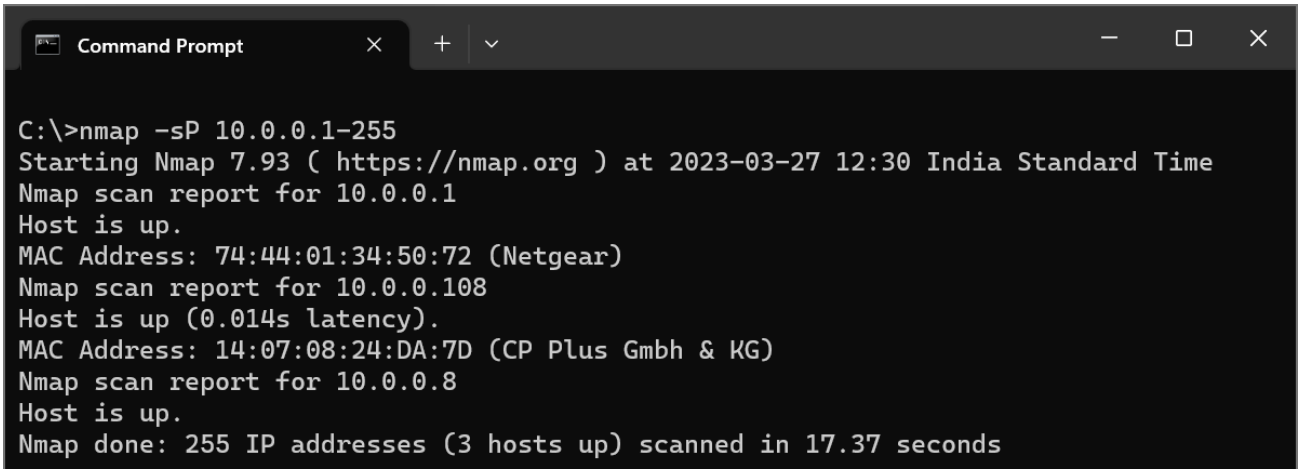
```
Command: nmap -sP <ip address / URL>
Example: nmap -sP 142.250.183.68 (www.google.com ip)
```



Host scan can also be used to:

- Identify active host(s) in a network.
- It sends ARP request packets to all systems in the target.
- Host Scan Results, “Host is up” by receiving MAC address from each active host.

```
Command: nmap -sP <ip address / URL>
Example: nmap -sP 10.0.0.1-255 (it’s current working network
ip)
```

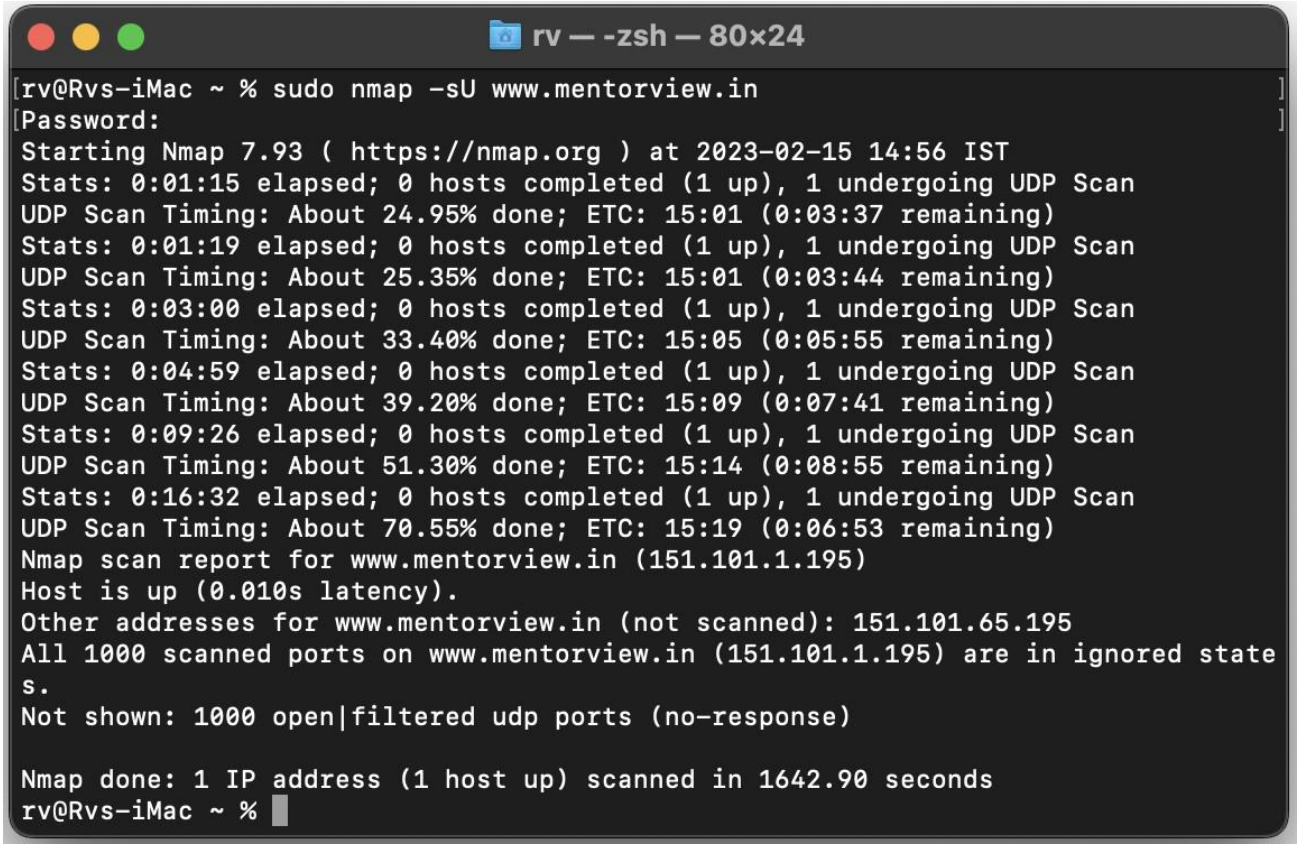


The output shows all the host connected to current network with its MAC address.

iii. UDP Scan:

- UDP scan works by sending a UDP packet to every destination port and analyses the response to determine the port's state; it is a connection-less protocol.
- For some common ports such as 53 and 161, a protocol-specific payload is sent to increase the response rate:
    - A service will respond with a UDP packet, proving that it is "open".
    - If the port is "closed", an ICMP Port Unreachable message is received from the target.
    - If no response is received after retransmissions, the port is classified as "open | filtered". This means that the port could be open, or perhaps packet filters are blocking the communication.
    -

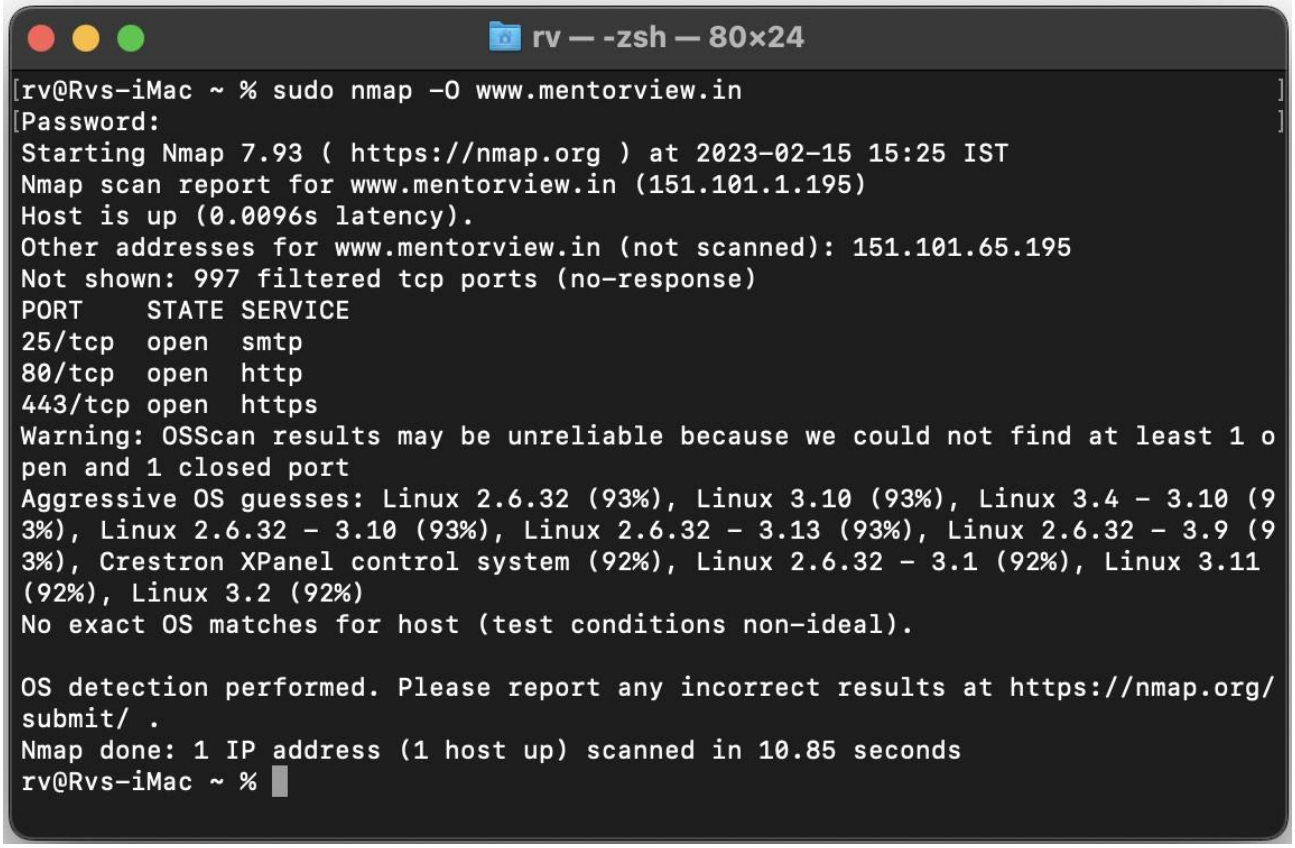
```
Command: nmap -sU <ip address / URL>
Example: nmap -sU www.mentorview.com
```



iv. *OS Detection Scan*: - nmap -O <target>

- Apart from the open port enumeration Nmap is quite useful in OS fingerprinting
- After running the command, we will get the information about:
  - Device type
  - Running
  - OS CPE (Common Platform Enumeration)
    - cpe:/o –> OS and cpe:/h –> hardware
  - OS details –> human readable report of the operating system.
- The option -O inform Nmap to enable OS detection that identifies a wide variety of systems, including residential routers, IP webcams, operating systems, and many other hardware devices.
- You can also execute the following command for os detection:
  - nmap -O -p- –osscan-guess in case OS identification fails, try to guess the operating system.
  - nmap -O –osscan-limit try to launch OS detection if scan conditions are ideal.

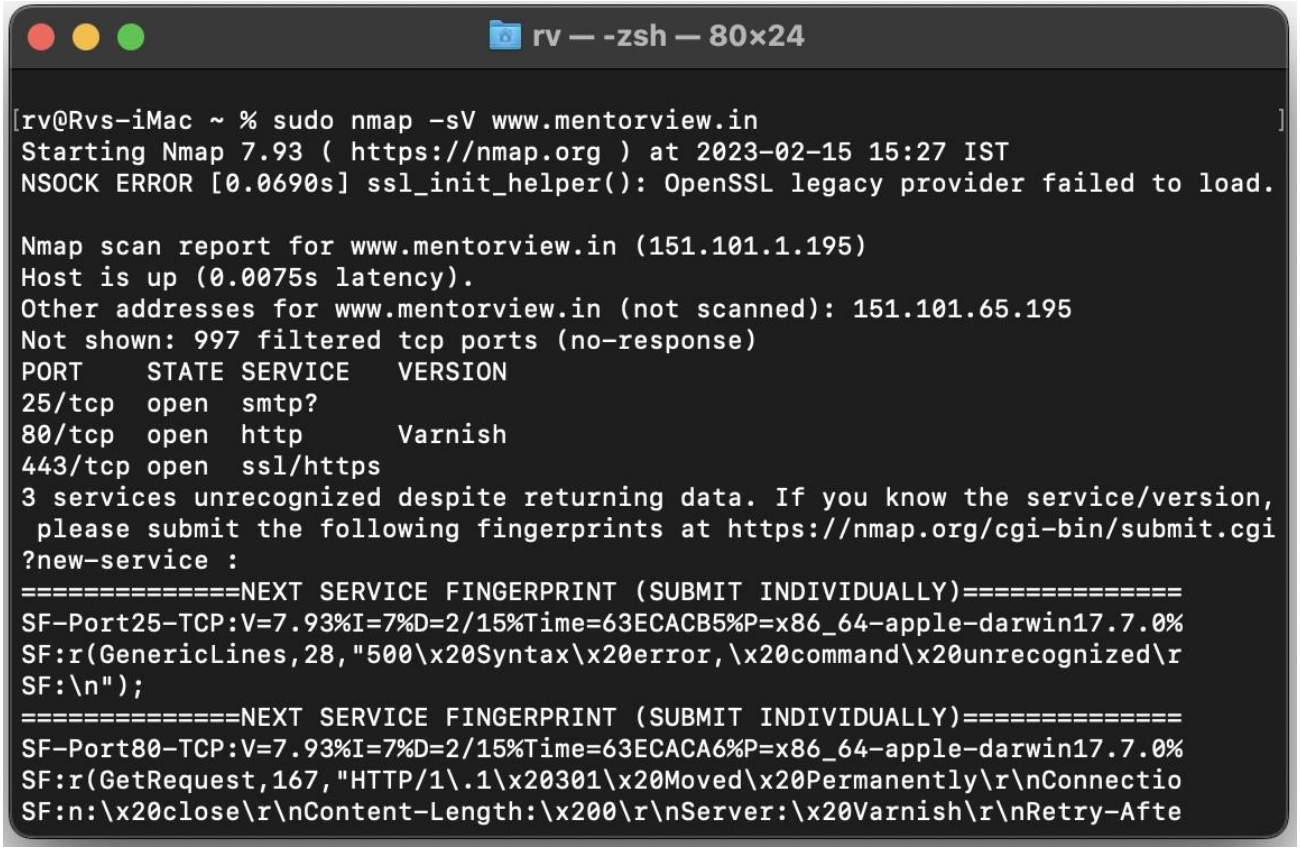
```
Command: nmap -O <ip address / URL>
Example: nmap -O www.mentorview.com
```



v. *Version Scan:*

- When doing vulnerability assessments of your companies or clients, you really want to know which mail and DNS servers and versions are running.
- Having an accurate version number helps dramatically in determining which exploits a server is vulnerable to.
- Fingerprinting a service may also reveal additional information about a target, such as available modules and specific protocol information.
- Version scan is also categorized as Banner Grabbing in penetration testing.

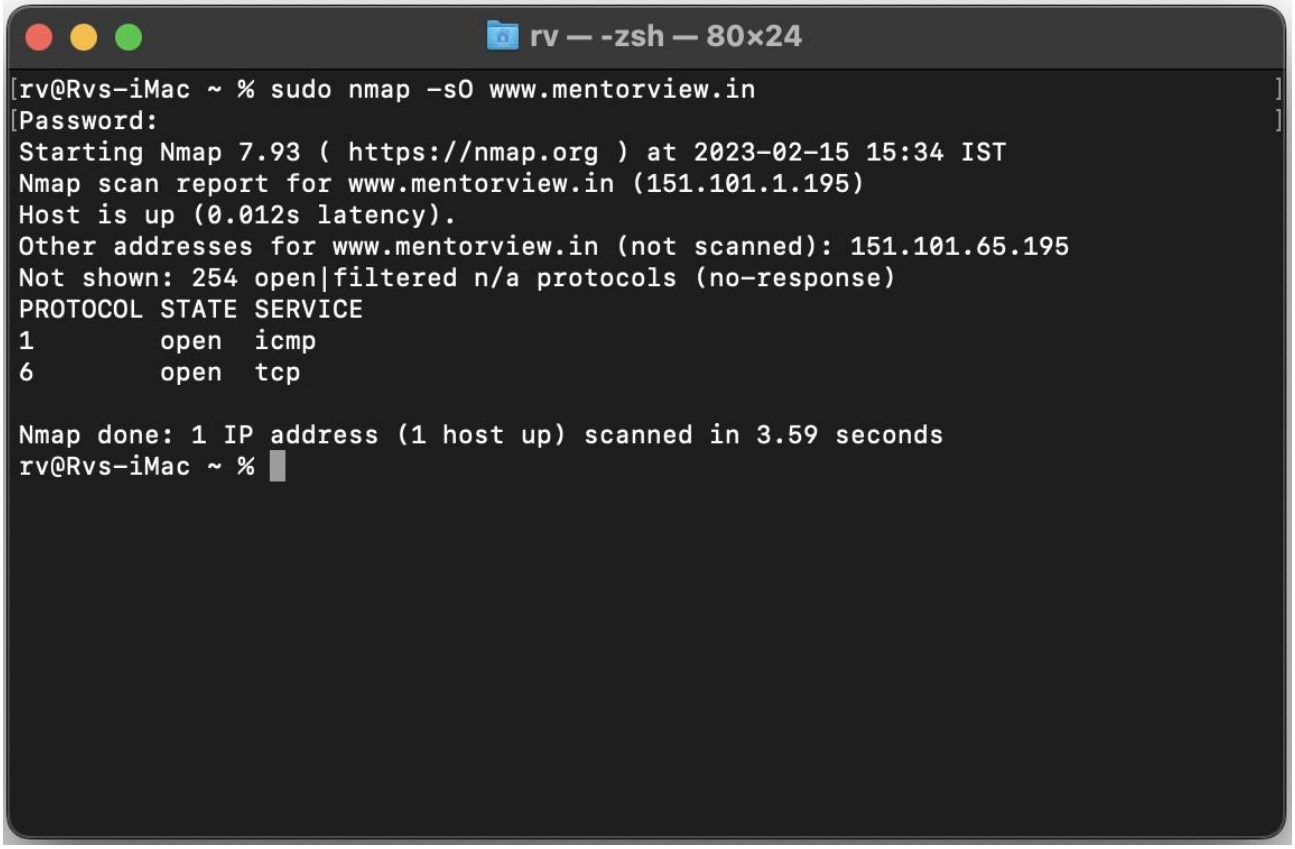
```
Command: nmap -O <ip address / URL>
Example: nmap -O www.mentorview.com
```



vi. *Protocol Scan:*

- IP Protocol scan is very helpful for determining what communication protocols are being used by a host.
- This method shows how to use Nmap to compute all of the IP protocols, where sends a raw IP packet without any additional protocol header, to each protocol on the target machine.
- For the IP protocols TCP, ICMP, UDP, IGMP, and SCTP, Nmap will set valid header values but for the rest, an empty IP packet will be used.

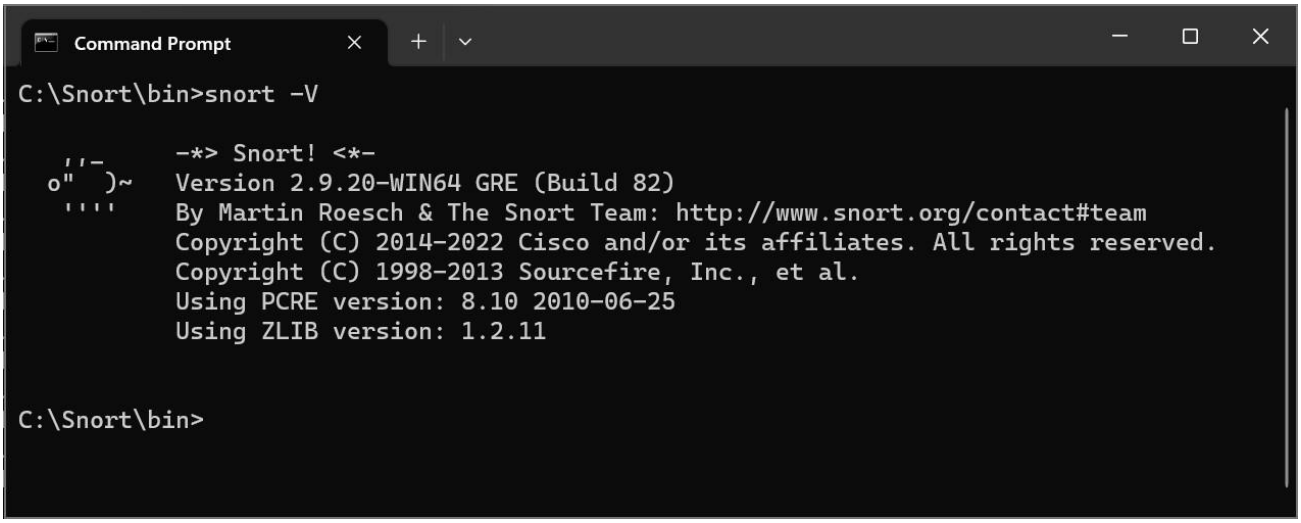
```
Command: nmap -sO <ip address / URL>
Example: nmap -sO www.mentorview.com
```



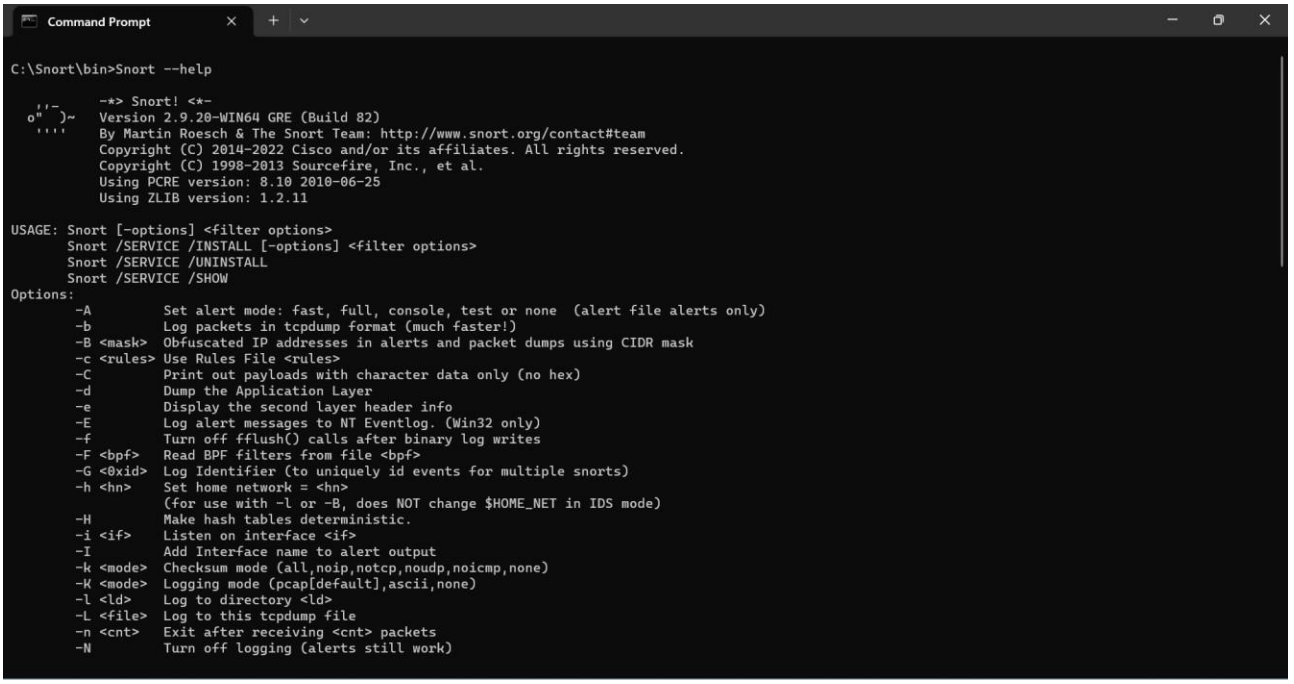
- ***IDS (Intrusion Detection Systems) Tool:***
  - An Intrusion Detection System (IDS) monitors network traffic for unusual or suspicious activity and sends an alert to the administrator.
  - Detection of strange activity and reporting it to the network administrator is the primary function of IDS.
  - However, some IDS software can take action based on rules when malicious activity is detected, for example blocking certain incoming traffic.
  - Some of the best Intrusion Detection System Software and Tools are as follows:
    - **Snort**: Provided by Cisco Systems and free to use, leading network-based intrusion detection system software.
    - **Solar Winds Security Event Manager EDITOR'S CHOICE**: Analyses logs from Windows, Unix, Linux, and Mac OS systems. It manages data collected by Snort, including real-time data. SEM is also an intrusion prevention system, shipping with over 700 rules to shut down malicious activity.
    - **Security Onion**: Network monitoring and security tool made up of elements pulled in from other free tools.
  - Types of Intrusion Detection Systems:
    - There are two main types of intrusion detection systems:
      - ***Host-based Intrusion Detection System (HIDS):***
        - This system will examine events on a computer on your network rather than the traffic that passes around the system.
      - ***Network-based Intrusion Detection System (NIDS):***
        - This system will examine the traffic on your network.
  - **Snort:**
    - Snort is a free open-source network intrusion detection system (NIDS) and intrusion prevention system (IPS).
    - Snort IPS uses a series of rules that help define malicious network activity and uses those rules to find packets that match against them and generates alerts for users.
    - Snort can be configured in three main modes:
      - ***Sniffer Mode:*** The program will read network packets and display them on the console.
      - ***Packet Logger Mode:*** The program will log packets to the disk.
      - ***Network Intrusion Detection System Mode:*** The program will monitor network traffic and analyse it against a rule set defined by the user. The program will then perform a specific action based on what has been identified.

- In order to start working with the 'Snort' we need to change the current working direct to `C:\Snort\bin`

i. Command: To check version of 'snort' → snort -V



ii. Command: To get help → snort --help



iii. Command: To find the list of interfaces running → snort -W

```
Command Prompt

C:\Snort\bin>snort -W

          -*> Snort! <*-
  o"  )~  Version 2.9.20-WIN64 GRE (Build 82)
   ''''   By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
          Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
          Copyright (C) 1998-2013 Sourcefire, Inc., et al.
          Using PCRE version: 8.10 2010-06-25
          Using ZLIB version: 1.2.11

Index   Physical Address        IP Address      Device Name     Description
-----   ----------------        ----------      -----------     -----------
    1   00:00:00:00:00:00       disabled        \Device\NPF_{07637146-340B-49E2-820D-3685B7716F26}      WAN Miniport (Network Monitor)
    2   00:00:00:00:00:00       disabled        \Device\NPF_{867714B3-4A6C-4931-A535-C5A318EF44BB}      WAN Miniport (IPv6)
    3   00:00:00:00:00:00       disabled        \Device\NPF_{0FB90408-02AF-4758-BD3C-A542796A761E}      WAN Miniport (IP)
    4   5C:BA:EF:08:05:B6       169.254.34.132  \Device\NPF_{C1C75E81-C10E-4422-BA74-07227FCDF533}      Bluetooth Device (Personal Area Network)
    5   5C:BA:EF:08:05:B5       10.0.0.8        \Device\NPF_{8E966D0B-93E4-4436-AF40-9D373A862115}      Realtek 8822BE Wireless LAN 802.11ac PCI-E NIC
    6   00:50:56:C0:00:08       192.168.186.1   \Device\NPF_{E3585292-011D-439E-A36F-DAE2B5525E9C}      VMware Virtual Ethernet Adapter for VMnet8
    7   00:50:56:C0:00:01       192.168.10.1    \Device\NPF_{3BC08BD7-4F27-4572-97DC-0894BF4010C2}      VMware Virtual Ethernet Adapter for VMnet1
    8   DE:BA:EF:08:05:B5       169.254.152.78  \Device\NPF_{0E272545-BA71-4EEC-A320-6601ADB87026}      Microsoft Wi-Fi Direct Virtual Adapter #4
    9   5C:BA:EF:08:05:B5       169.254.46.118  \Device\NPF_{0695E965-AF34-4AD0-BCC2-FC6B45EC8EB0}      Microsoft Wi-Fi Direct Virtual Adapter #3
   10   00:00:00:00:00:00       0000:0000:0000:0000:0000:0000:0000:0000 \Device\NPF_Loopback    Adapter for loopback traffic capture

C:\Snort\bin>
```

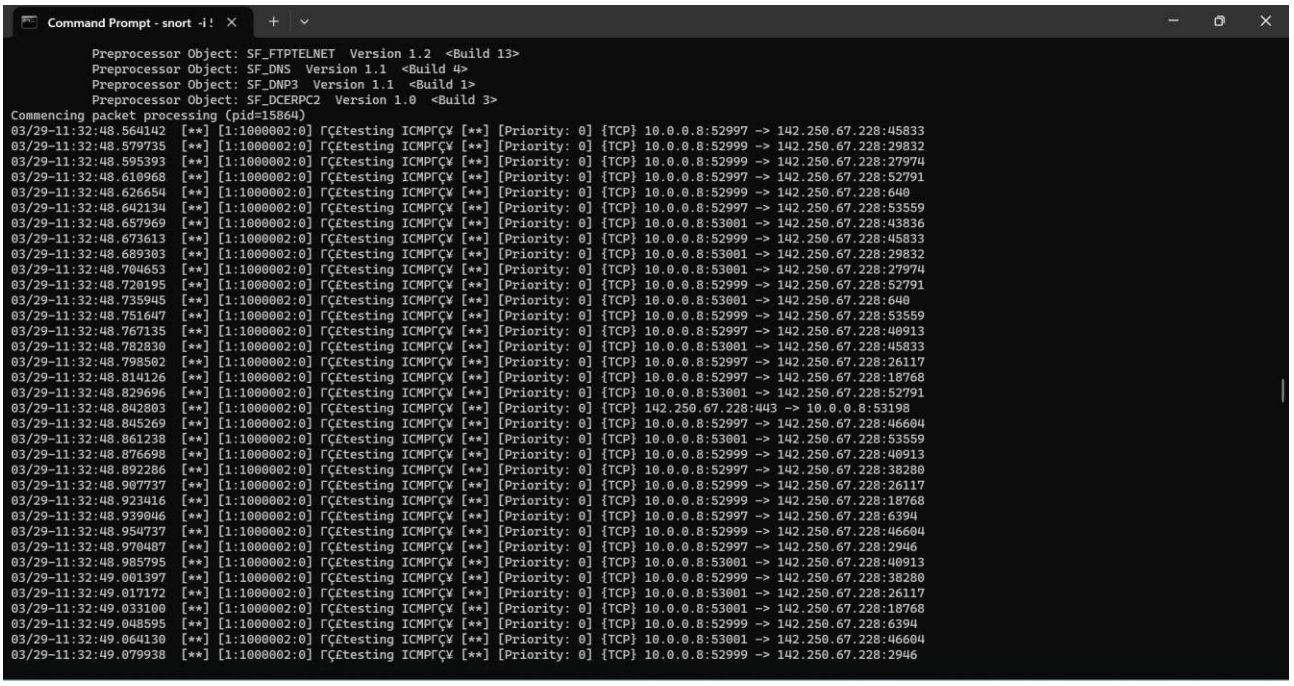
vi. Command: To carry out work of sniffing the network interface → snort -i 5 -c c:\Snort\etc\snort.conf -A console (here 5 indicates current working network)

- Where:
  - i – stands for interface, here is where you tell snort what network interface it should sniff on (it should be followed by the interface number which is active that we have get information from above command)
  - c – is where you tell snort the location of the file you want it to run
  - A – means print output in the terminal

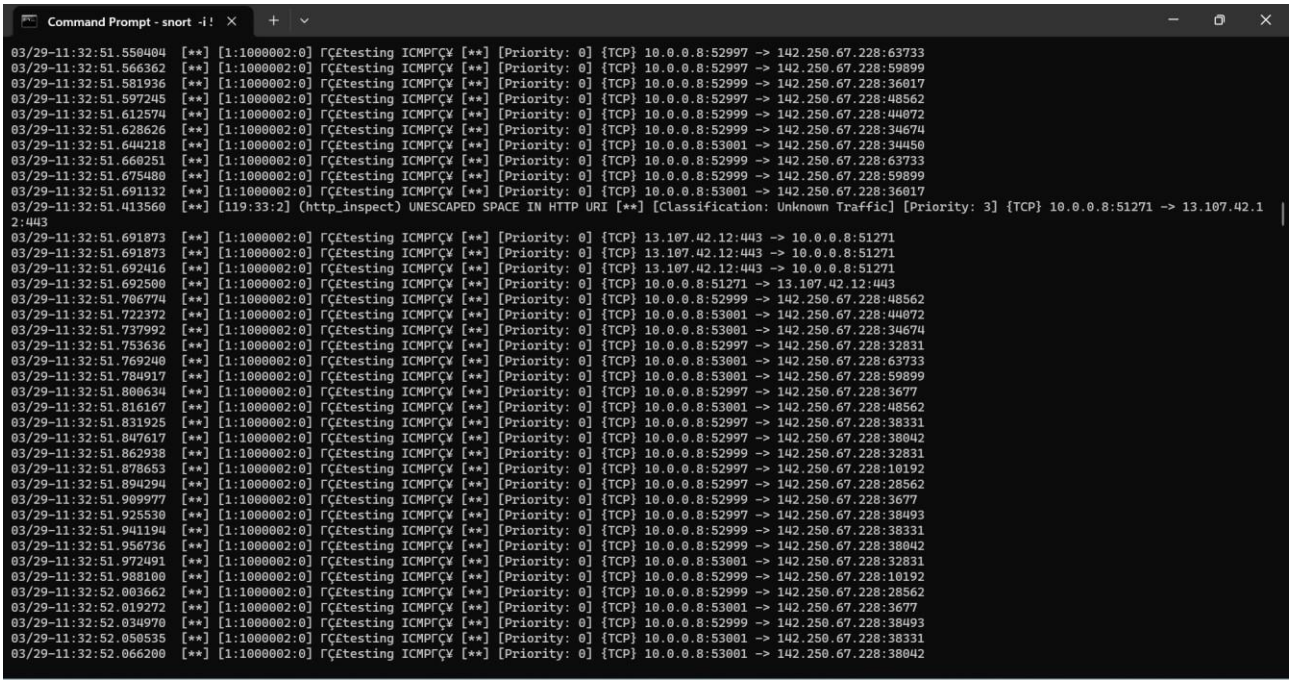
Command run:

```
Command Prompt - snort -i!

C:\Snort\bin>snort -i 5 -c c:\Snort\etc\snort.conf -A console
Running in IDS mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "c:\Snort\etc\snort.conf"
PortVar 'HTTP_PORTS' defined :  [ 36 80:90 311 323 383 443:444 555 591 593 623 631 664 801 808 818 901 972 1158 1220 1270 1414 1533 1581 1719:1720 1741 1801 1812 1830 194
2 2231 2301 2375 2381 2578 2809 2869 2980 3000 3029 3037 3057 3128 3323 3443 3702 4000 4343 4444 4848 5000 5054 5060:5061 5117 5222 5250 5416 5443 5450 5480 5555 5600 581
4 5894 5984:5986 6060 6080 6173 6988 7000:7001 7005 7070:7071 7080 7144:7145 7180:7181 7510 7770 7777:7779 8000:8001 8008 8014:8015 8020 8028 8040 8080:8082 8085 8088 809
0 8095 8118 8123 8161 8180:8182 8222 8243 8280 8300 8333 8344 8393 8400 8443 8484 8500 8509 8511 8694 8787 8800 8848 8852 8880 8888 8899 8983 9000:9002 9050 9060 9080 909
0:9091 9111 9200:9201 9290 9443 9447 9502 9700 9710 9788 9830 9850 9990 9999:10000 10080 10100 10250 10255 10297 10443 11371 12601 13014 15489 16000 16992:16995 17000 180
81 19980 20000 29991 30007 30018 30888 33300 34412 34443:34444 36099 37215 40007 41080 44449 49152:49153 50000 50002 50452 51423 53331 54444 55252 55555 56712 ]
PortVar 'SHELLCODE_PORTS' defined :  [ 0:79 81:65535 ]
PortVar 'ORACLE_PORTS' defined :  [ 1024:65535 ]
PortVar 'SSH_PORTS' defined :  [ 22 ]
PortVar 'FTP_PORTS' defined :  [ 21 2100 3535 ]
PortVar 'SIP_PORTS' defined :  [ 5060:5061 5600 ]
PortVar 'FILE_DATA_PORTS' defined :  [ 36 80:90 110 143 311 323 383 443:444 555 591 593 623 631 664 801 808 818 901 972 1158 1220 1270 1414 1533 1581 1719:1720 1741 1801
1812 1830 1942 2231 2301 2375 2381 2578 2809 2869 2980 3000 3029 3037 3057 3128 3323 3443 3702 4000 4343 4444 4848 5000 5054 5060:5061 5117 5222 5250 5416 5443 5450 5480
5555 5600 5814 5894 5984:5986 6060 6080 6173 6988 7000:7001 7005 7070:7071 7080 7144:7145 7180:7181 7510 7770 7777:7779 8000:8001 8008 8014:8015 8020 8028 8040 8080:8082
8085 8088 8090 8095 8118 8123 8161 8180:8182 8222 8243 8280 8300 8333 8344 8393 8400 8443 8484 8500 8509 8511 8694 8787 8800 8848 8852 8880 8888 8899 8983 9000:9002 9050
9060 9080 9090:9091 9111 9200:9201 9290 9443 9447 9502 9700 9710 9788 9830 9850 9990 9999:10000 10080 10100 10250 10255 10297 10443 11371 12601 13014 15489 16000 16992:16
995 17000 18081 19980 20000 29991 30007 30018 30888 33300 34412 34443:34444 36099 37215 40007 41080 44449 49152:49153 50000 50002 50452 51423 53331 54444 55252 55555 5671
2 ]
PortVar 'GTP_PORTS' defined :  [ 2123 2152 3386 ]
Detection:
   Search-Method = AC-Full-Q
    Split Any/Any group = enabled
    Search-Method-Optimizations = enabled
    Maximum pattern length = 20
Tagged Packet Limit: 256
Loading dynamic engine C:\Snort\lib\snort_dynamicengine\sf_engine.dll... done
Loading all dynamic preprocessor libs from C:\Snort\lib\snort_dynamicpreprocessor...
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_dce2.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_dnp3.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_dns.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_ftptelnet.dll... done
```

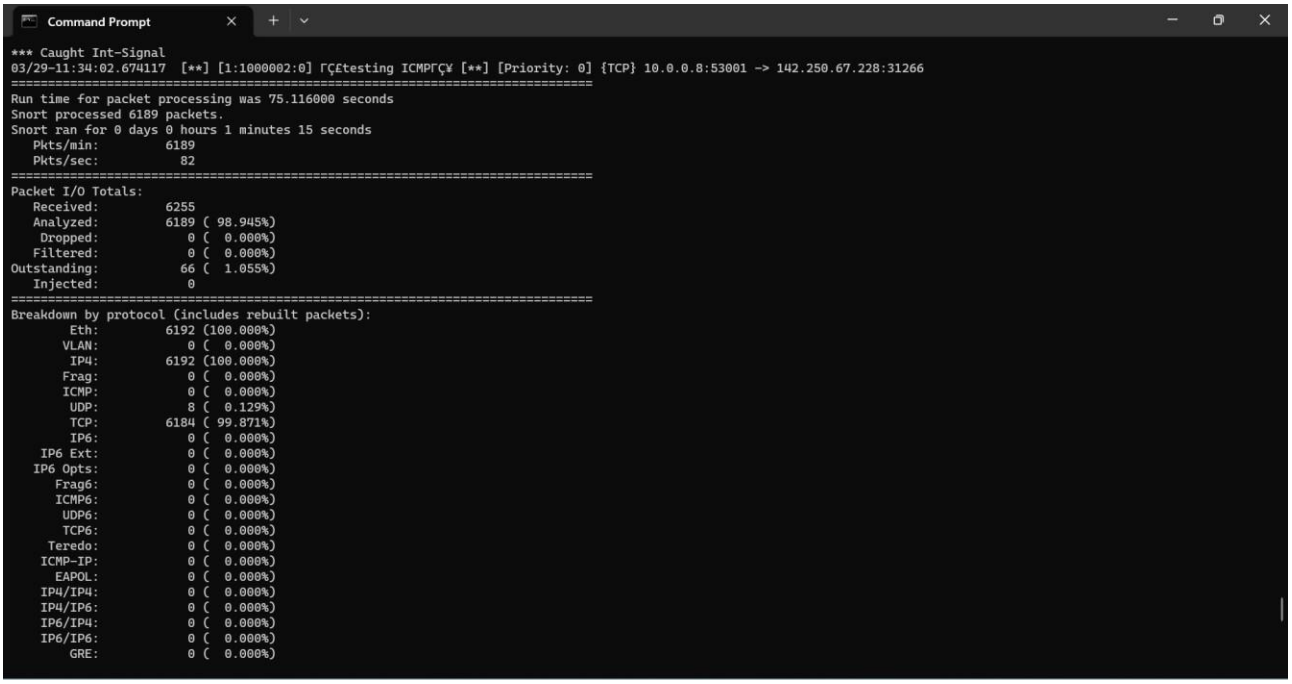
Packet sniffing in progress:



Unidentified traffic (the longest line in the output):



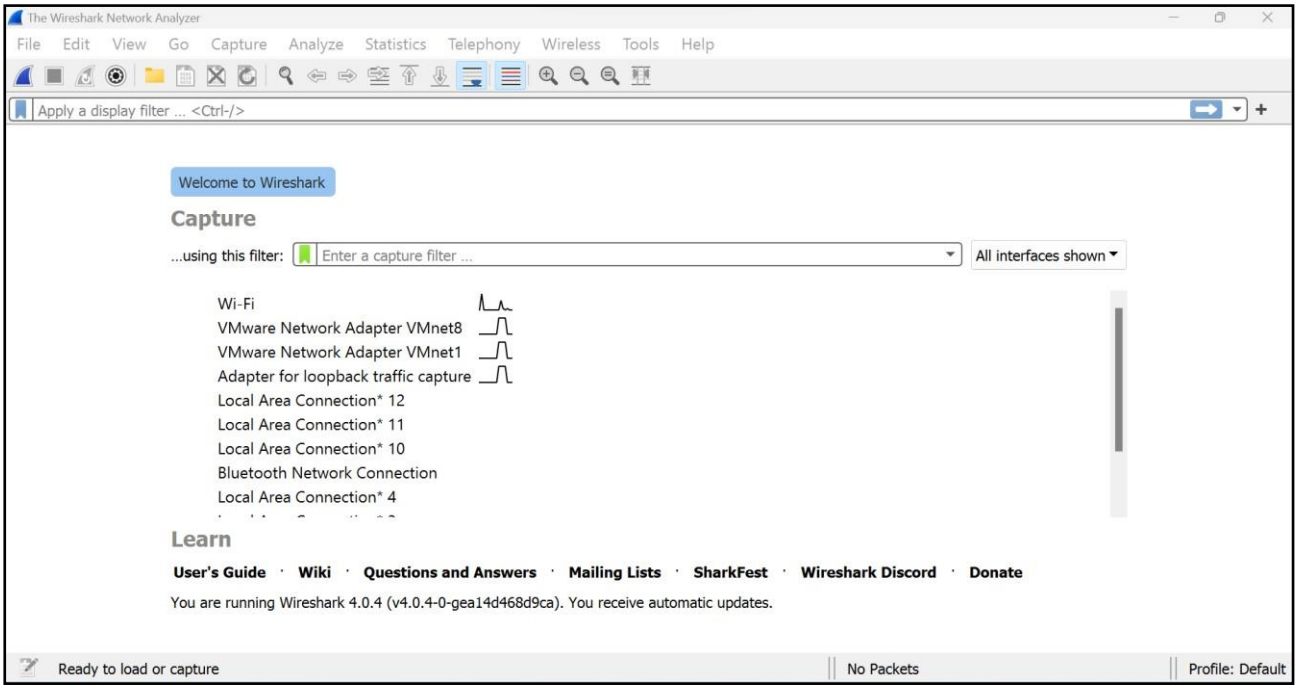
Report of Output:



- ***Network Sniffing***:
  - Computers communicate using networks. These networks could be on a local area network LAN or exposed to the internet.
  - Network Sniffers are programs that capture low-level package data that is transmitted over a network.
  - An attacker can analyse this information to discover valuable information such as user ids and passwords.
  - Network sniffing is the process of capturing data packets sent over a network.
  - This can be done by the specialized software program or hardware equipment.
  - Sniffing can be used to:
    - Capture sensitive data such as login credentials
    - Eavesdrop on chat messages
    - Capture files that have been transmitted over a network.
  - The following are protocols that are vulnerable to sniffing:
    - Telnet
    - Rlogin
    - HTTP
    - SMTP
    - NNTP
    - POP
    - FTP
    - IMAP
  - The above protocols are vulnerable if login details are sent in plain text.

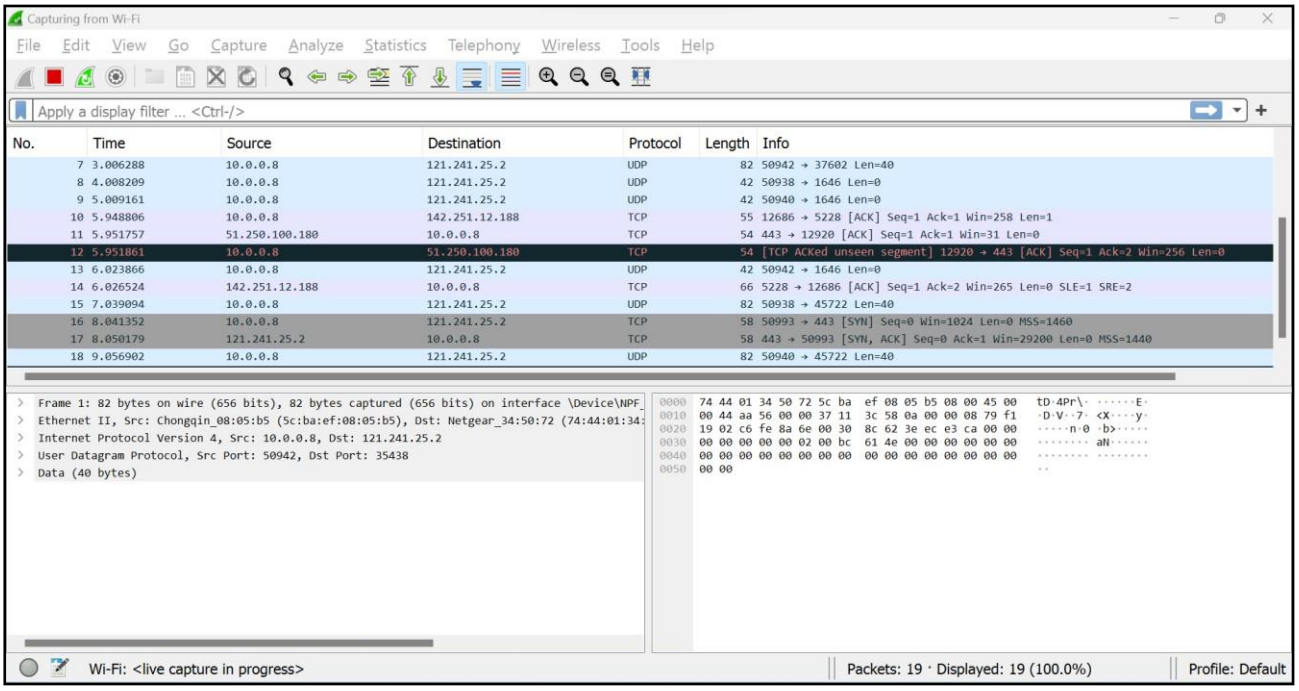
- Network sniffing using Wireshark:
  - Wireshark is a free and open-source packet analyser.
  - It is used for network troubleshooting, analysis, software and communications protocol development, and education.
  - Wireshark is cross-platform, using the Qt widget toolkit in current releases to implement its user interface, and using pcap to capture packets.
  - It runs on Linux, macOS, BSD, Solaris, some other Unix-like operating systems, and Microsoft Windows.
  - There is also a terminal-based (non-GUI) version called TShark.
  - Wireshark is used to capture and analyse packets in network.
  - It is also used as a sniffer, network protocol analyser, and network analyser.
  - We can also apply specific filter on network traffic to get more filtered data packets.

i. Wireshark User Interface:

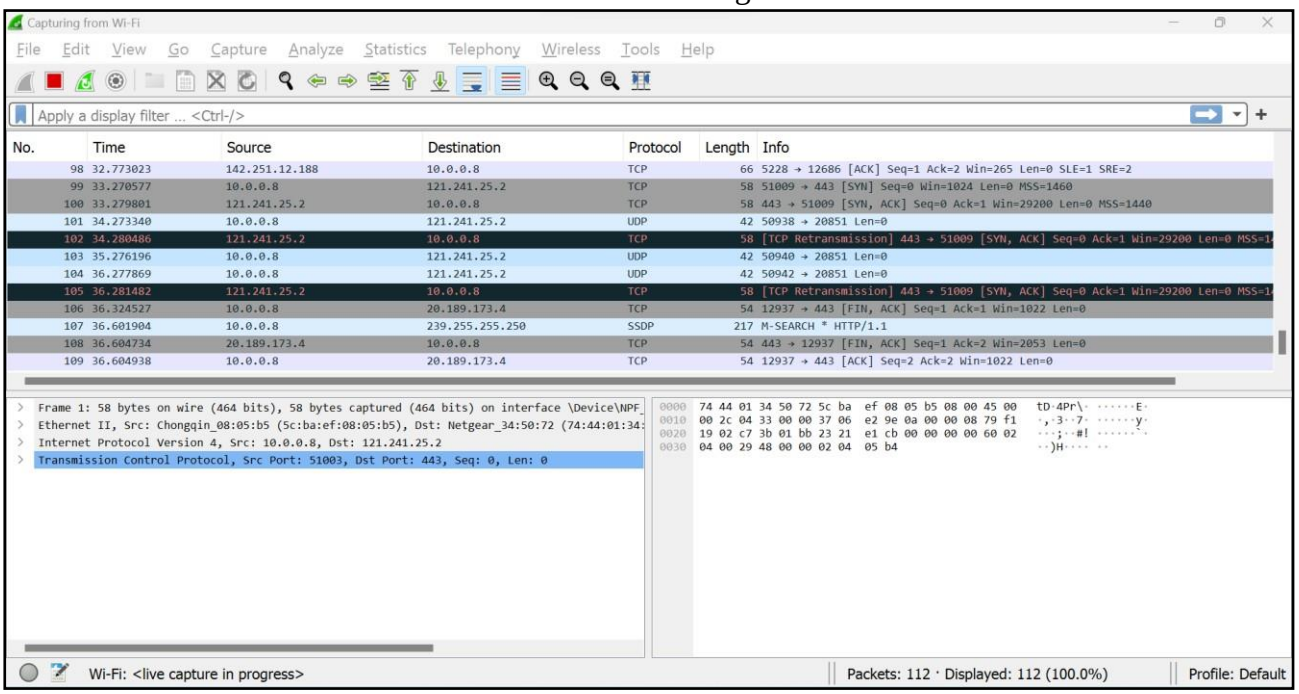


ii. Capturing Live Network Data:

a. To capture Live Network Data double, click on any of the interface in the above UI screen.
b. Once you doble click on the inface you will start getting packet detail entering and leaving the network as shown below:

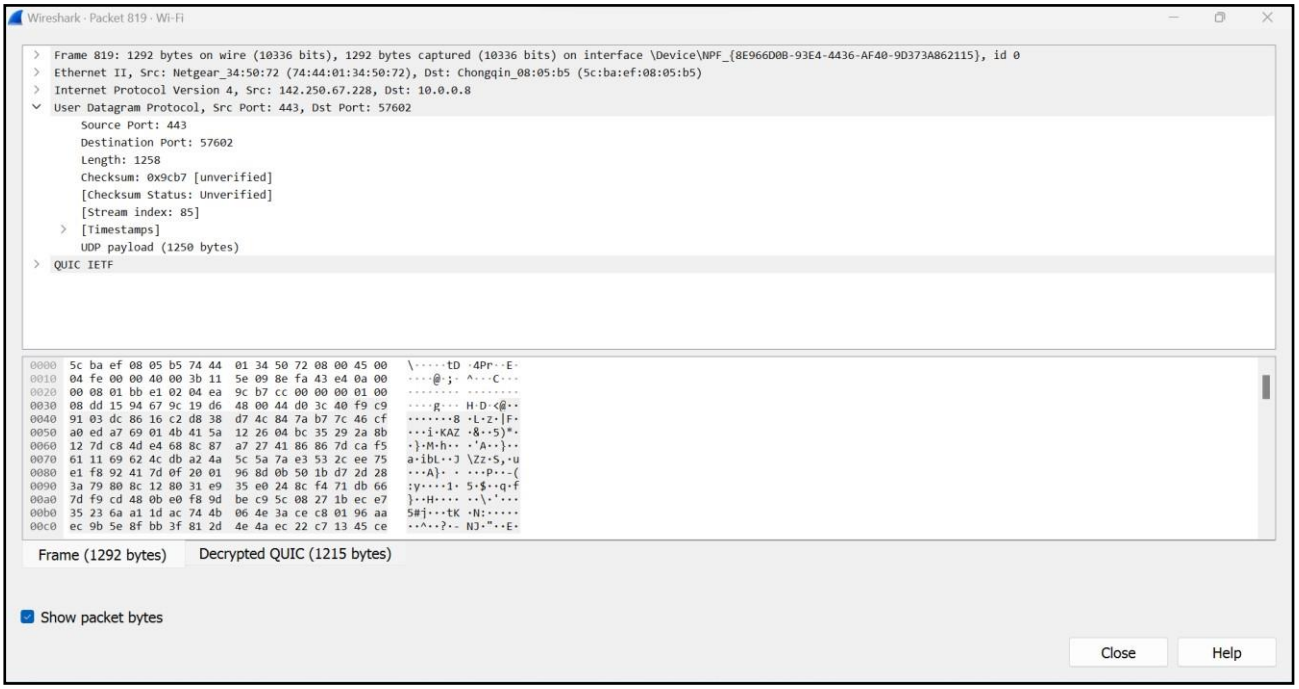


c. Packet based on different colour coding scheme.

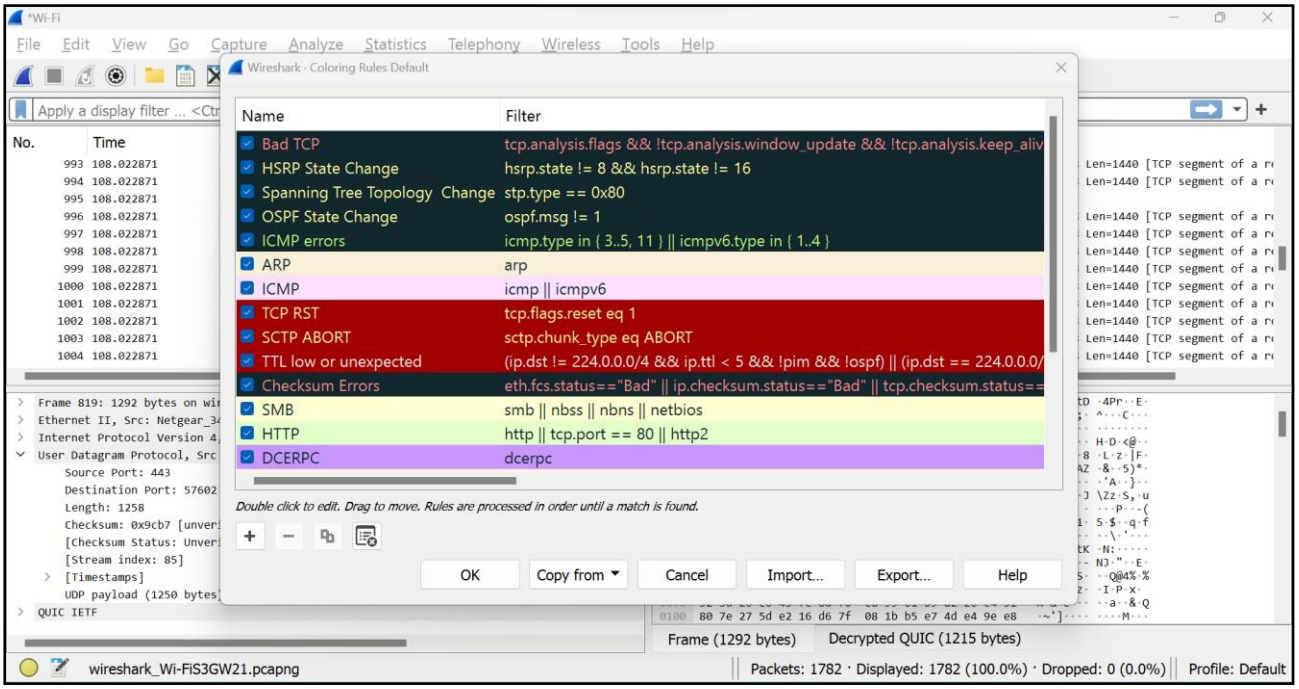


iii. Viewing Captured Packets:

a. Double click on any of the packet that you want to view. Another window will open, showing the details of the selected packet as shown below:



iv. Colour Coding Scheme for various Protocols in Wireshark:



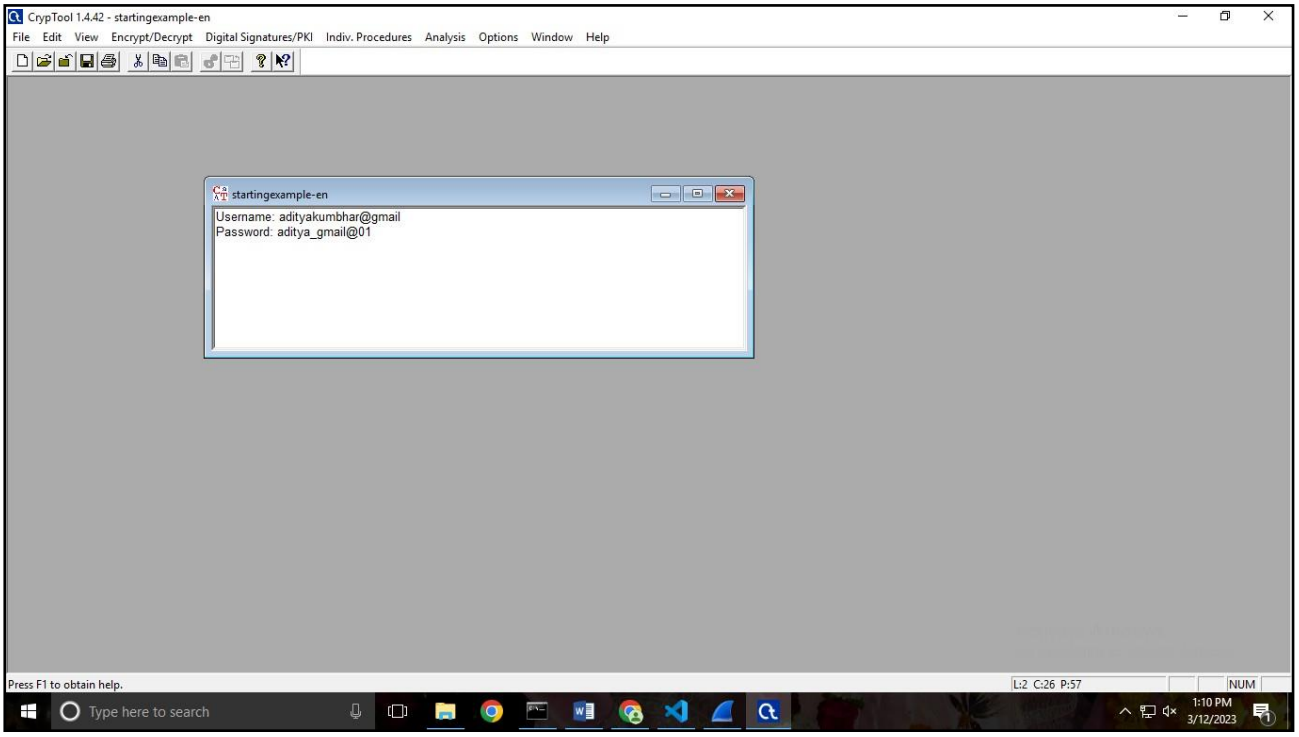
ENCRYPTION AND DECRYPTION

- ***Using CrypTool***:
  - CrypTool 1 (CT1) is a comprehensive and free educational program about cryptography and cryptanalysis offering extensive online help and many visualizations.
  - We are basically using it to the process of encryption and decryption techniques.
  - CrypTool provides a variety of range of Encryption methods some are:
    - Symmetric (Classic):
      - Caesar / Rot – 13
    - Symmetric (Modern):
      - RC2
      - RC4
      - DES
      - Triple DES
    - Asymmetric:
      - RSA Encryption
      - RSA Decryption

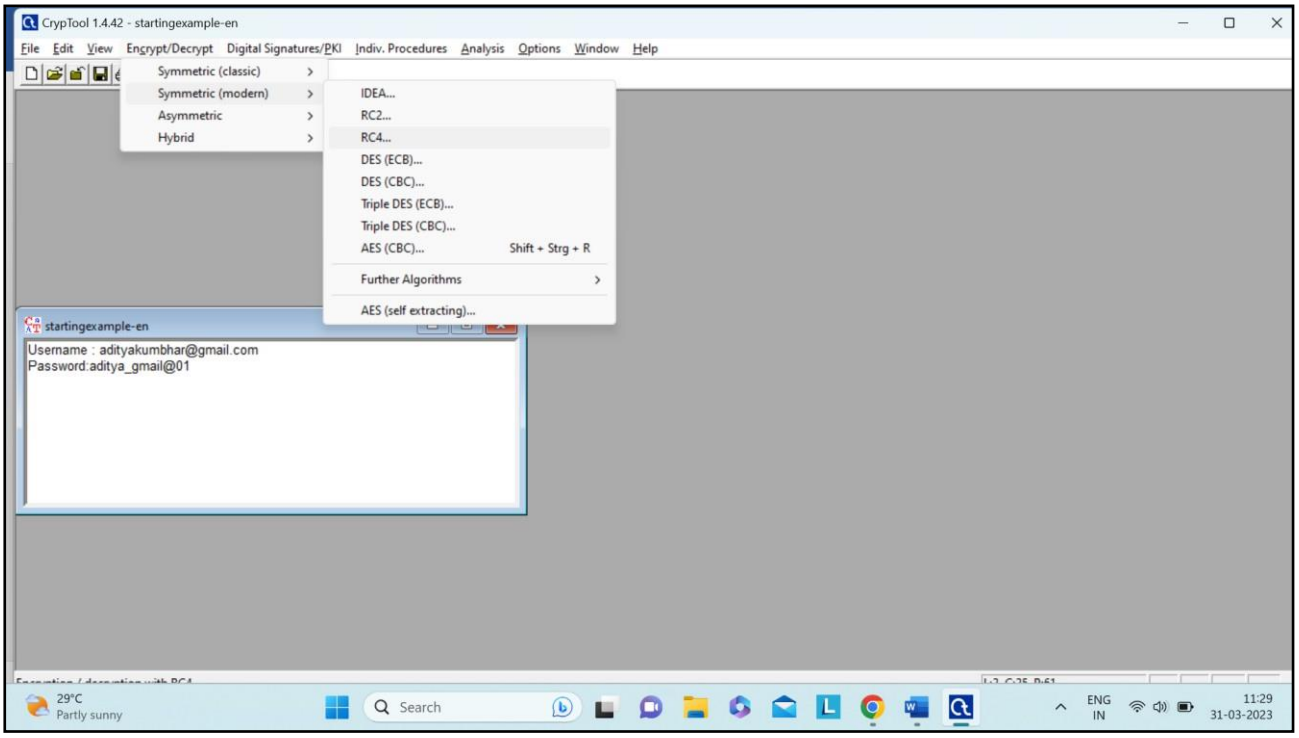
RC4 Algorithm:

Practical Work: Performing Encryption using RC4 algorithm

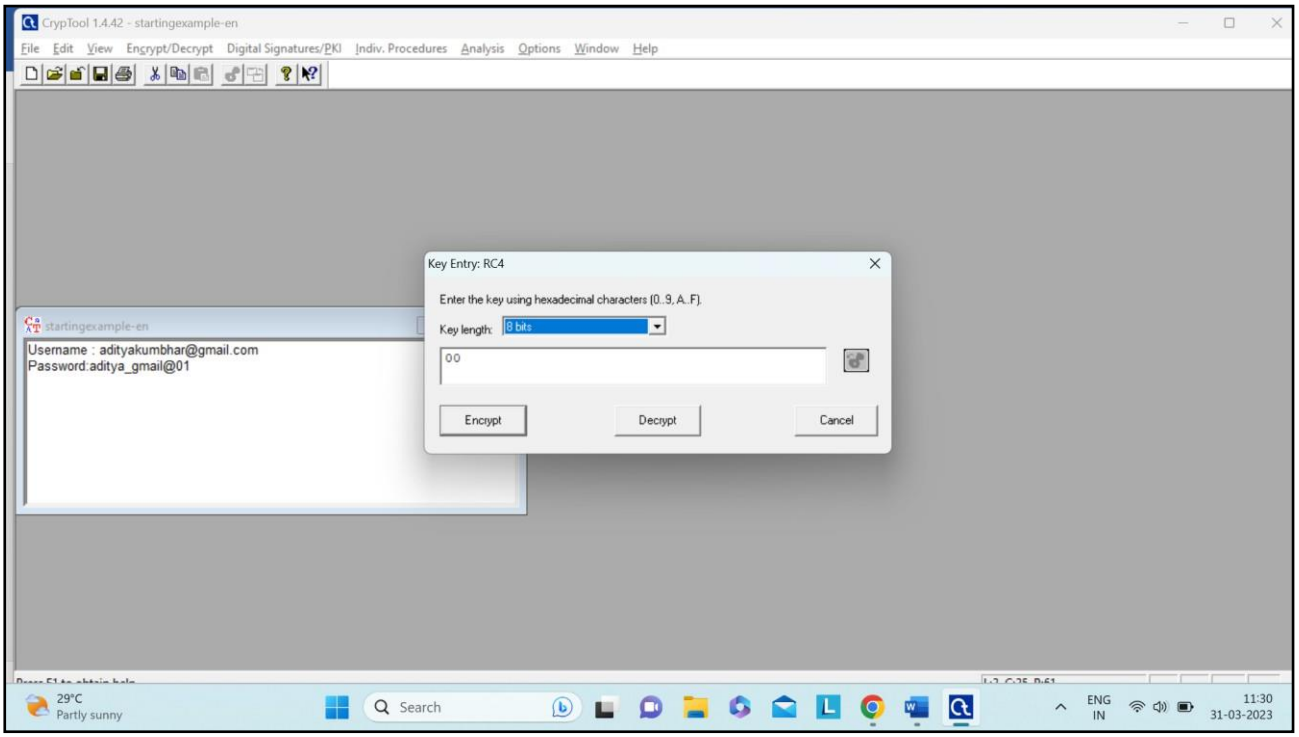
Step 1: Type the content that you need to encrypt.



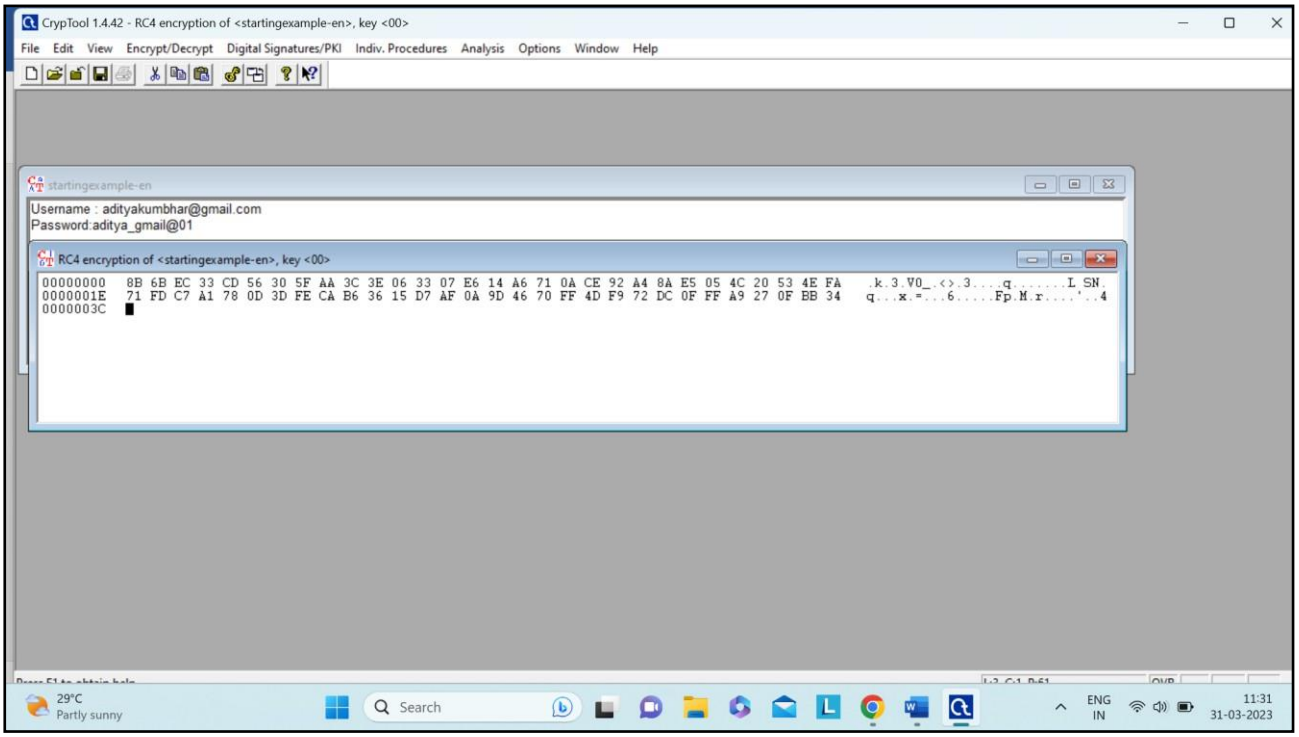
Step 2: Select the type of Encryption technique from the available list. (Here we are using RC4 algorithm for encryption)



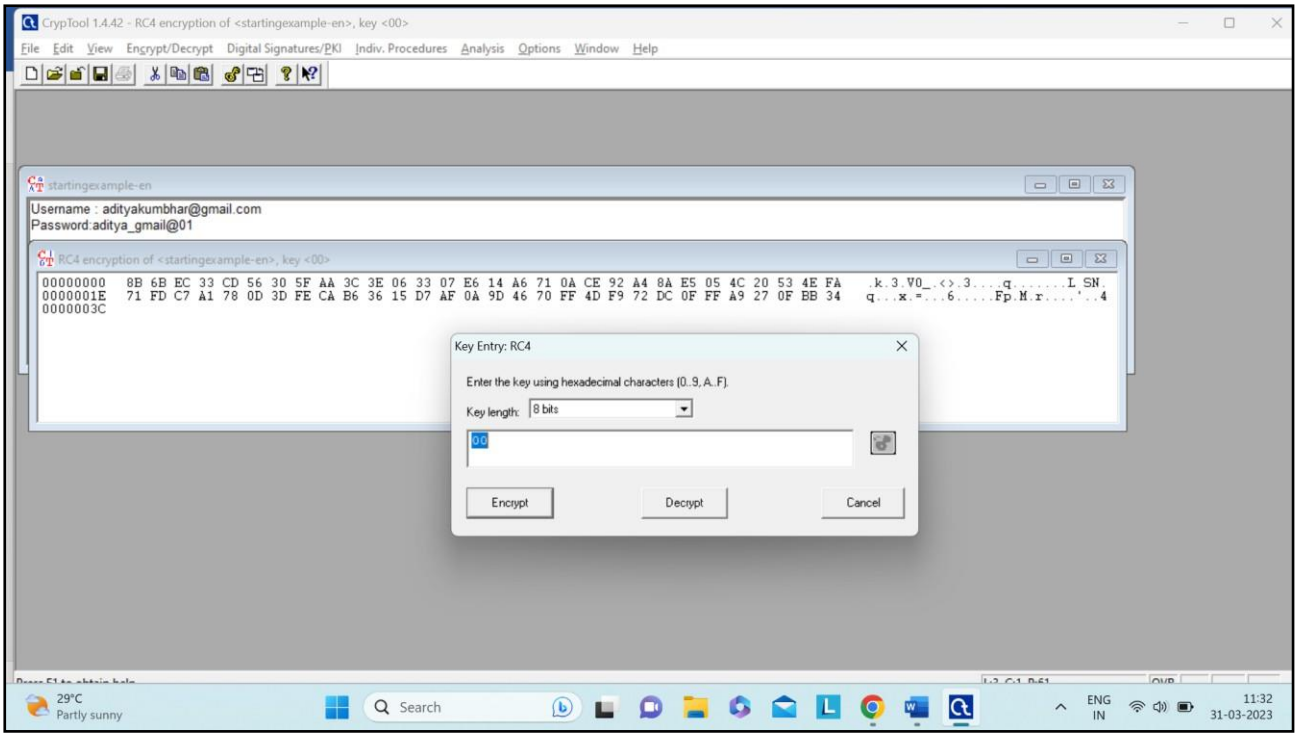
Encryption goes here:



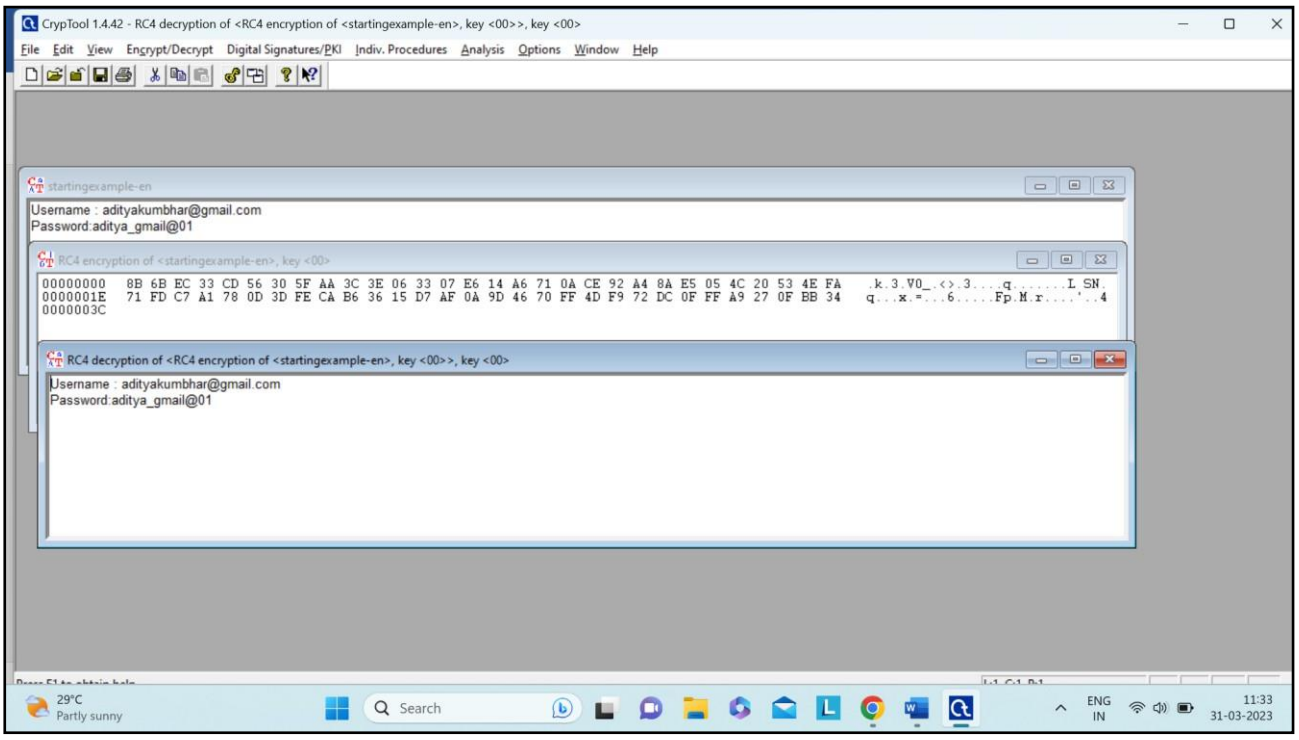
Step 3: Select Encrypt and the encrypted message will appear



Decryption goes here:



Decrypted Message:

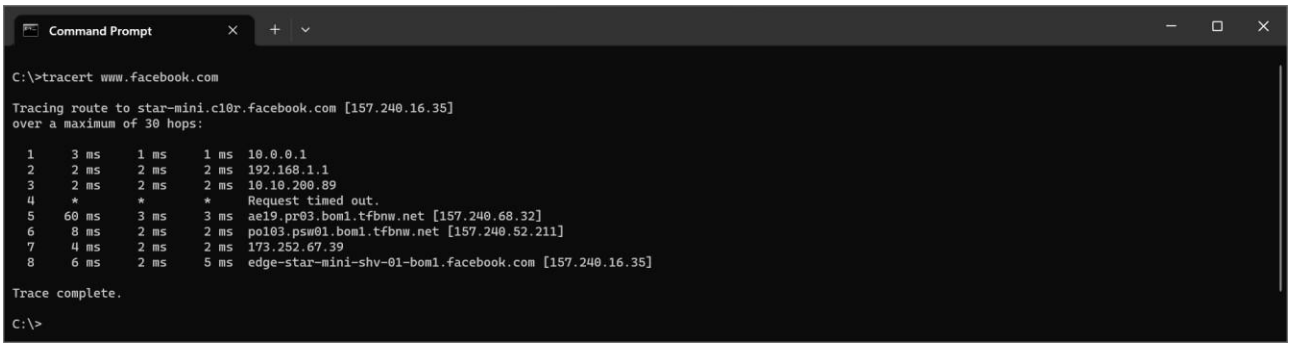


Using traceroute, ping, ipconfig, netstat Command

1. tracert:

a. The ‘tracert’ command is a Command Prompt command that's used to show several details about the path that a packet takes from the computer or device you're on to whatever destination you specify.
b. Traceroute is a command which can show you the path a packet of information tak es from your computer to one you specify.
c. It will list all the routers it passes through until it reaches its destination, or fails to and is discarded.
d. In addition to this, it will tell you how long each 'hop' from router to router takes.

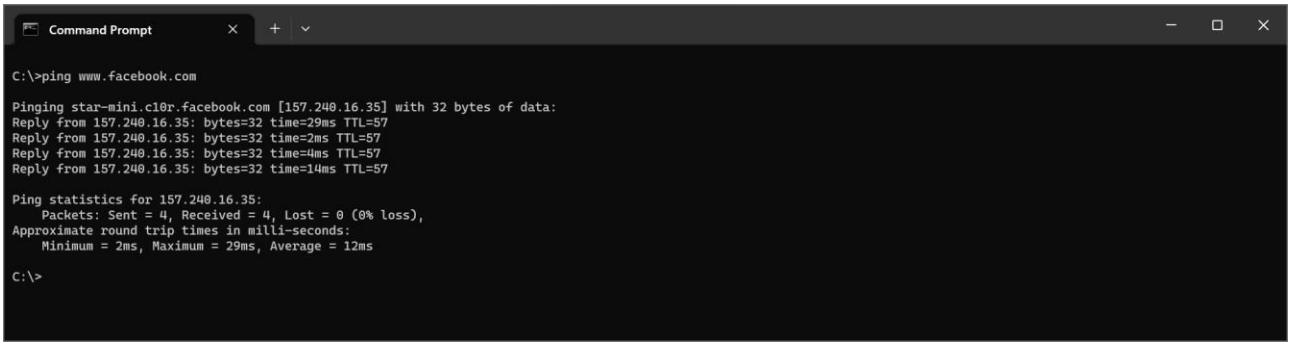
```
Command: tracert <ip address / URL>
Example: tracert www.facebook.com
```



2. ping:

a. The ping command is a Command Prompt command used to test the ability of the source computer to reach a specified destination computer.
b. The ping command is usually used as a simple way to verify that a computer can communicate over the network with another computer or network device.

```
Command: tracert <ip address / URL>
Example: tracert www.facebook.com
```

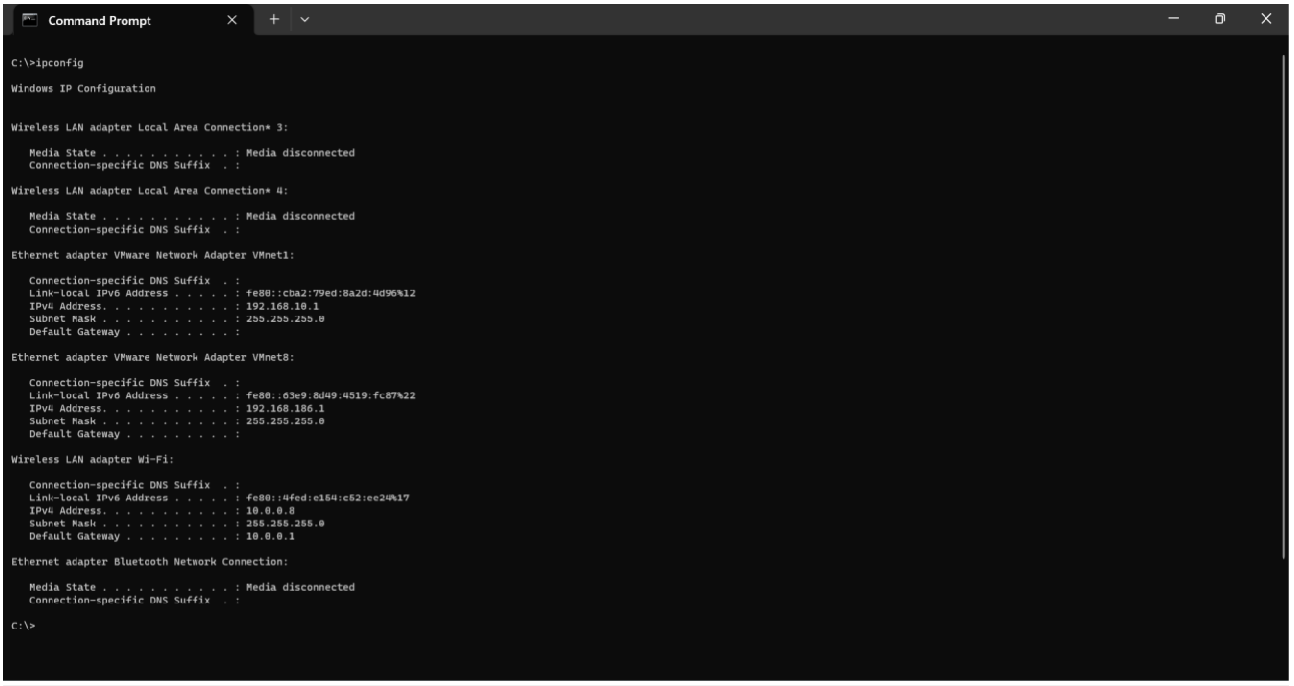


3. ipconfig:

a. Ipconfig is a DOS utility that can be used from MS-DOS and the Windows command line to display the network settings currently assigned and given by a network.

b. This command can be utilized to verify a network connection as well as to verify your network settings.

```
Command: ipconfig
Example: ipconfig
```

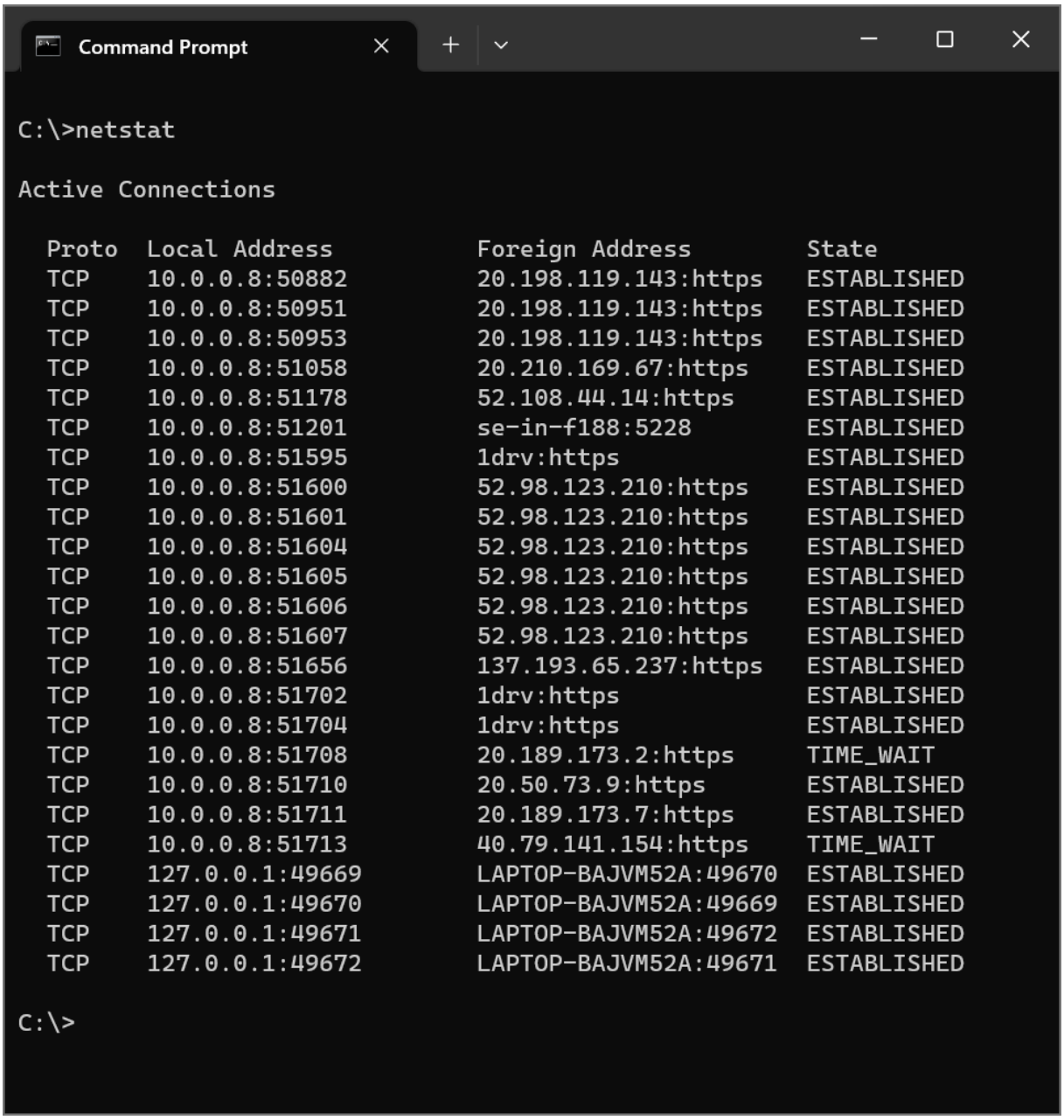


4. netstat:

a. The netstat command, meaning network statistics, is a Command Prompt command used to display very detailed information about how your computer is communicating with other computers or network devices.

b. Specifically, the netstat command can show details about individual network connections, overall and protocol-specific networking statistics, and much more, all of which could help troubleshoot certain kinds of networking issues.

```
Command: netstat
Example: netstat
```



5. **arp:**
   a. ARP command to view and modify the ARP (Address Resolution Protocol) table entries on the local computer.
   b. This may display all the known connections on your local area network segment (if they have been active and, in the cache,). The arp command is useful for viewing the ARP cache and resolving address resolution problems.

```
Command: arp -a (to display the arp table)
Example: arp -a (to display the arp table)
```