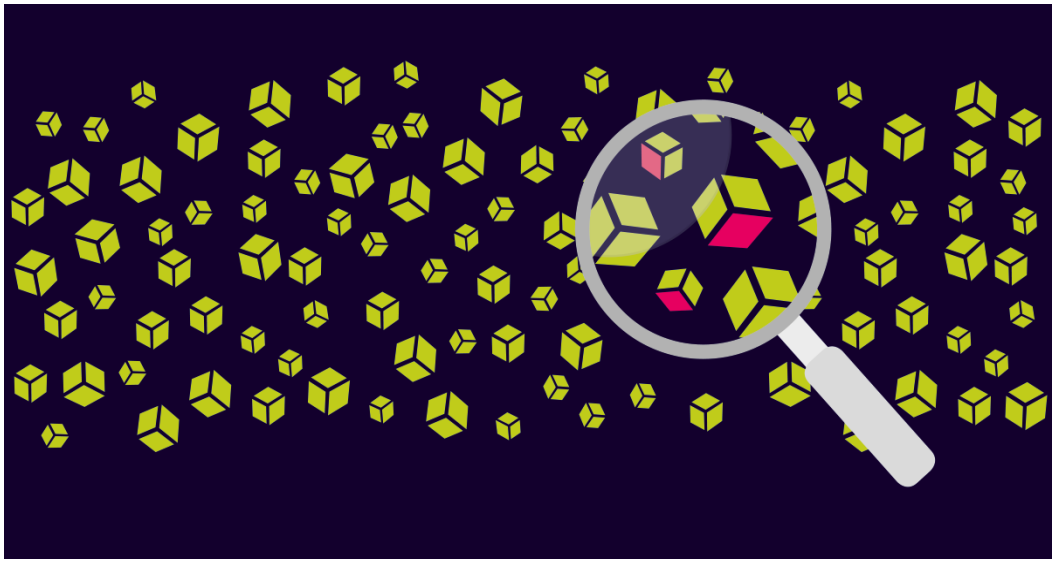
LAB MANUAL
ON
A PRACTICAL APPROACH TO NETWORK SNIFFING



ESTABLISHMENT OF ADVANCED LABORATORY FOR CYBER SECURITY TRAINING TO TECHNICAL TEACHERS

DEPARTMENT OF INFORMATION MANAGEMENT AND EMERGING ENGINEERING

MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

GOVERNMENT OF INDIA

Principal Investigator: Prof. Maitreyee Dutta

Co Investigator: Prof. Shyam Sundar Pattnaik

PREPARED BY:

Prof. Maitreyee Dutta and Ms. Shweta Sharma (Technical Assistant)

Table of Contents

MANUAL-2:

A Practical Approach to Network Sniffing

INTRODUCTION TO NETWORK SNIFFING

- Network sniffing is a process to sniff the network traffic in real-time.
- It works by capturing and analyzing packets of data that flow through a particular network.
- Figure 1 shows the process of network sniffing where data is travelling through a network in the form of packets. The sniffer intercepts the network traffic and captures the raw data packets.
- The captured data packet is analyzed by the packet sniffing software and presented to the network administrators.

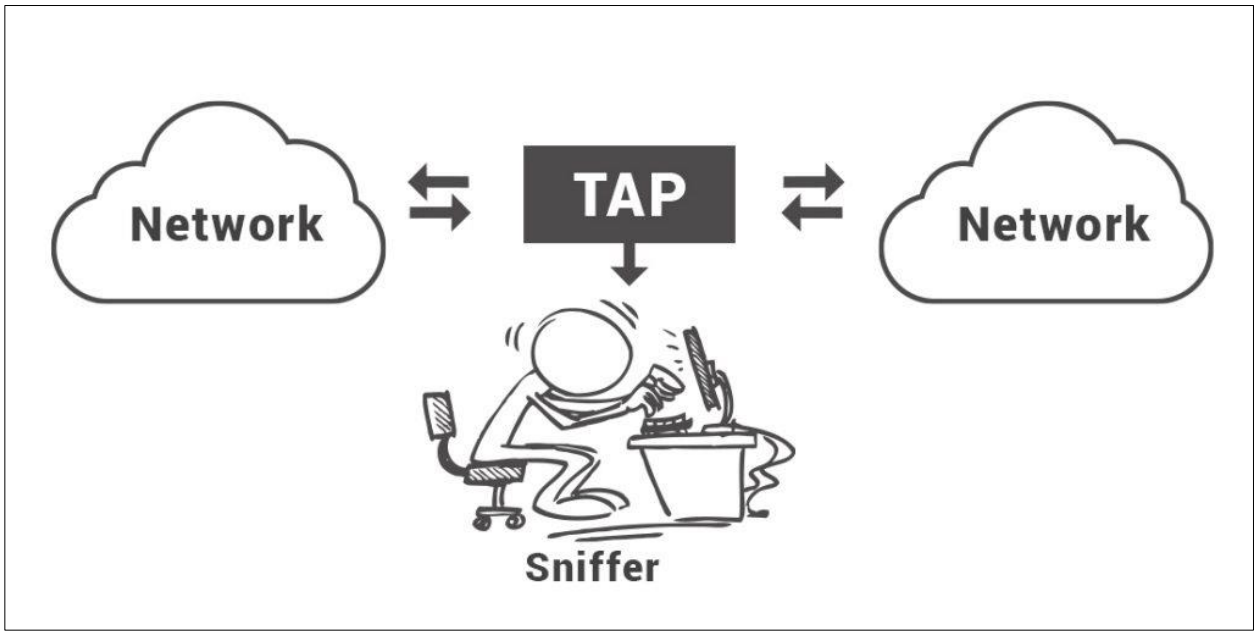


Figure 1: Process of network sniffing

CAIN AND ABEL TOOL

- The Cain and Abel tool [1] is a password recovery and network sniffing tool which is freely available for Windows operating system.
- This tool is useful for network administrators, teachers, security consultants/professionals, forensic staff, security software vendors, professional penetration tester and everyone else that plans to use it for ethical reasons.
- This tool contains features such as Arp Poison Routing (APR) which enables sniffing on switched LANs and wireless network.
- The sniffer can also analyze protocols such as HTTP, SSH-1 and HTTPS and contains filters to capture credentials from a wide range of authentication mechanisms.

Figure 2: Cain & Abel tool

NETWORK SNIFFING WITH CAIN AND ABEL TOOL

Before downloading and installing Cain & abel tool, it is advised to turn off the Windows firewall and anti-virus tool. The network sniffing can be performed with Cain and abel tool with following steps:

Step 1: Search for Cain & Abel in a searching engine and download the tool as shown in Figure 3 and Figure 4 respectively.

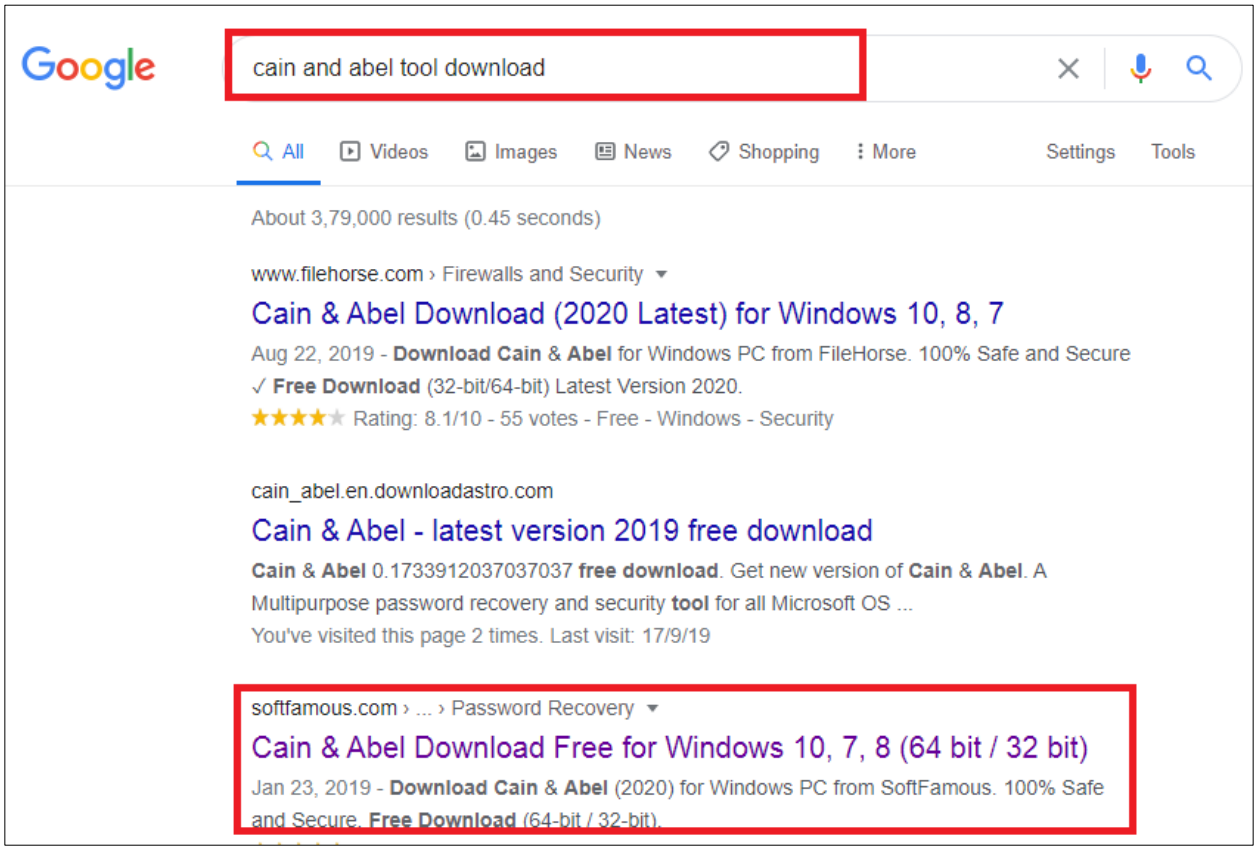


Figure 3: Search Cain and abel tool

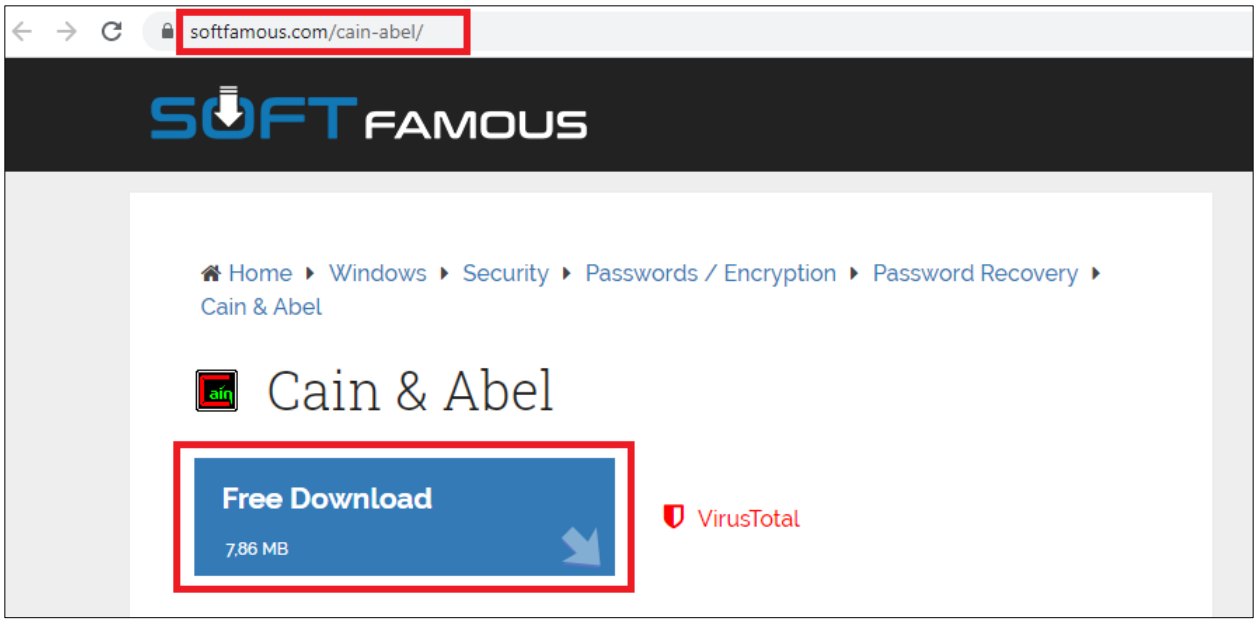


Figure 4: Download Cain and abel tool

Step 2: Download WinPcap for Windows operating system. Figure 5 shows WinPcap for Windows 10 operating system and Figure 6 shows WinPcap for rest of the versions of Windows operating system.

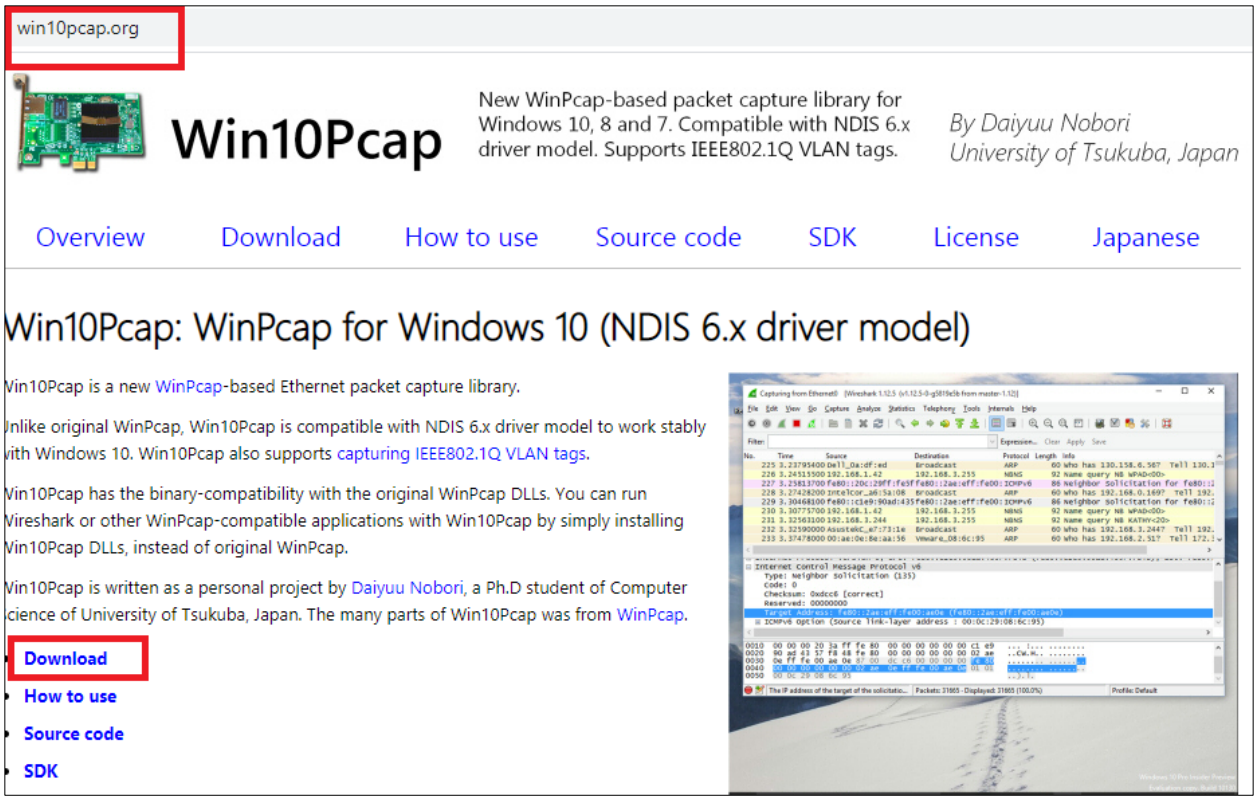


Figure 5: Download WinPcap for Windows 10 operating system

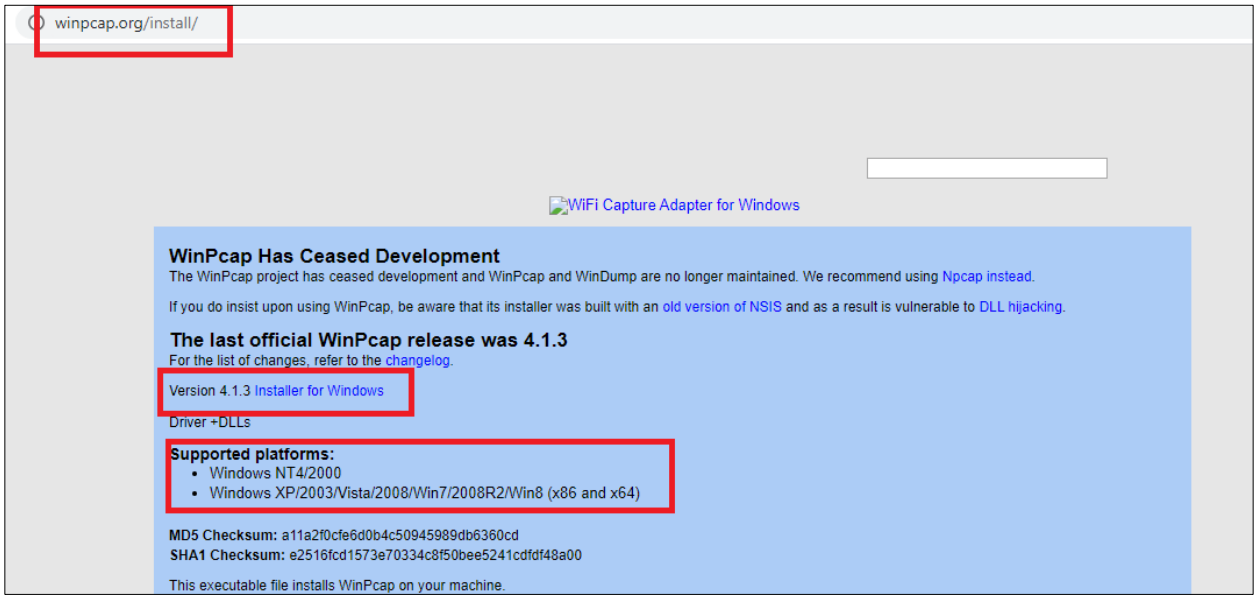


Figure 6: Download WinPcap for Windows NT/XP/…./Win8 operating system

Step 3: Figure 7 shows icon of Cain & Abel tool on Desktop of Windows operating system after installation.

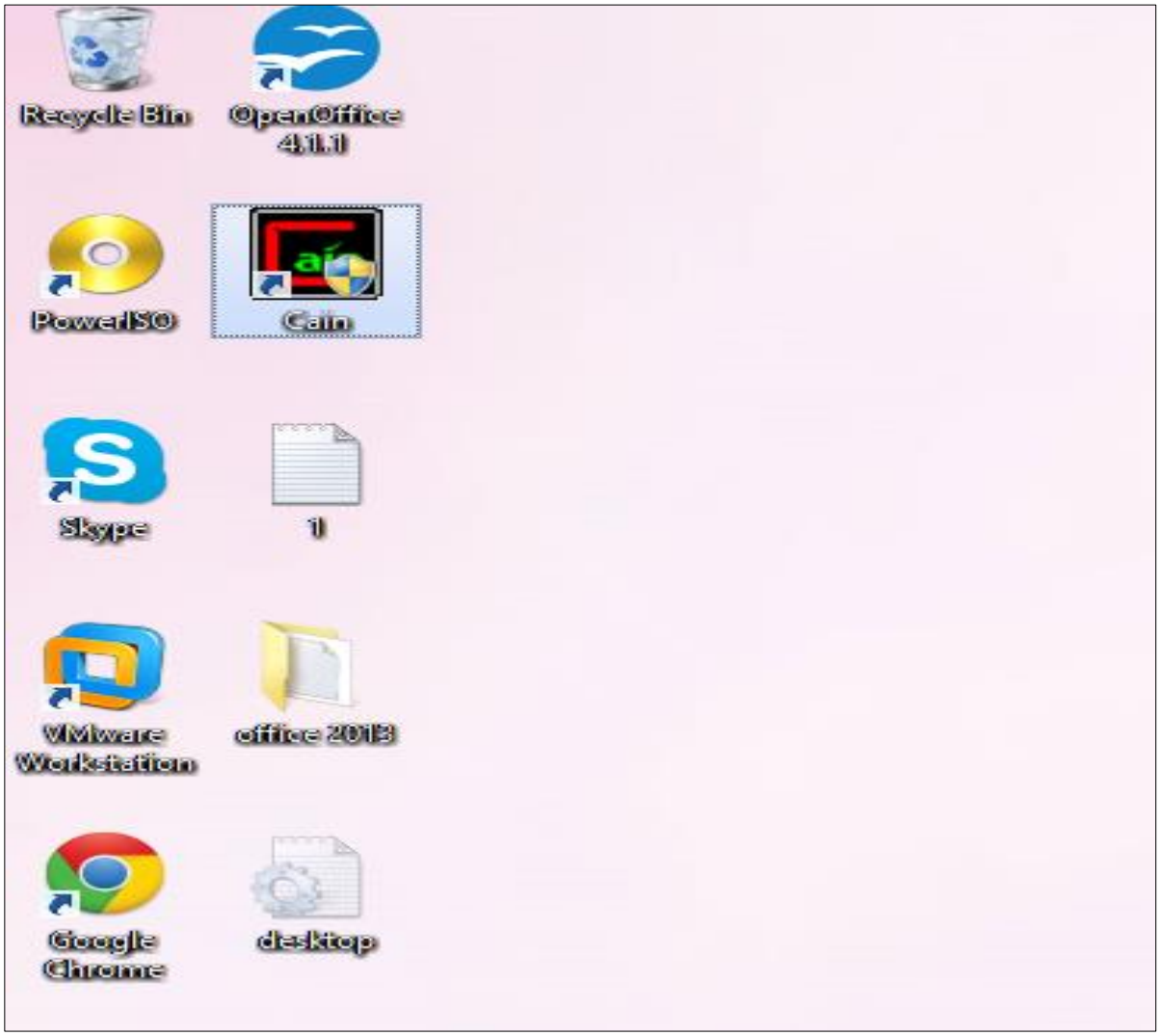


Figure 7: Cain & Abel tool on Windows operating system

Step 4: Double click on this icon to open Cain & Abel tool as shown in Figure 8.

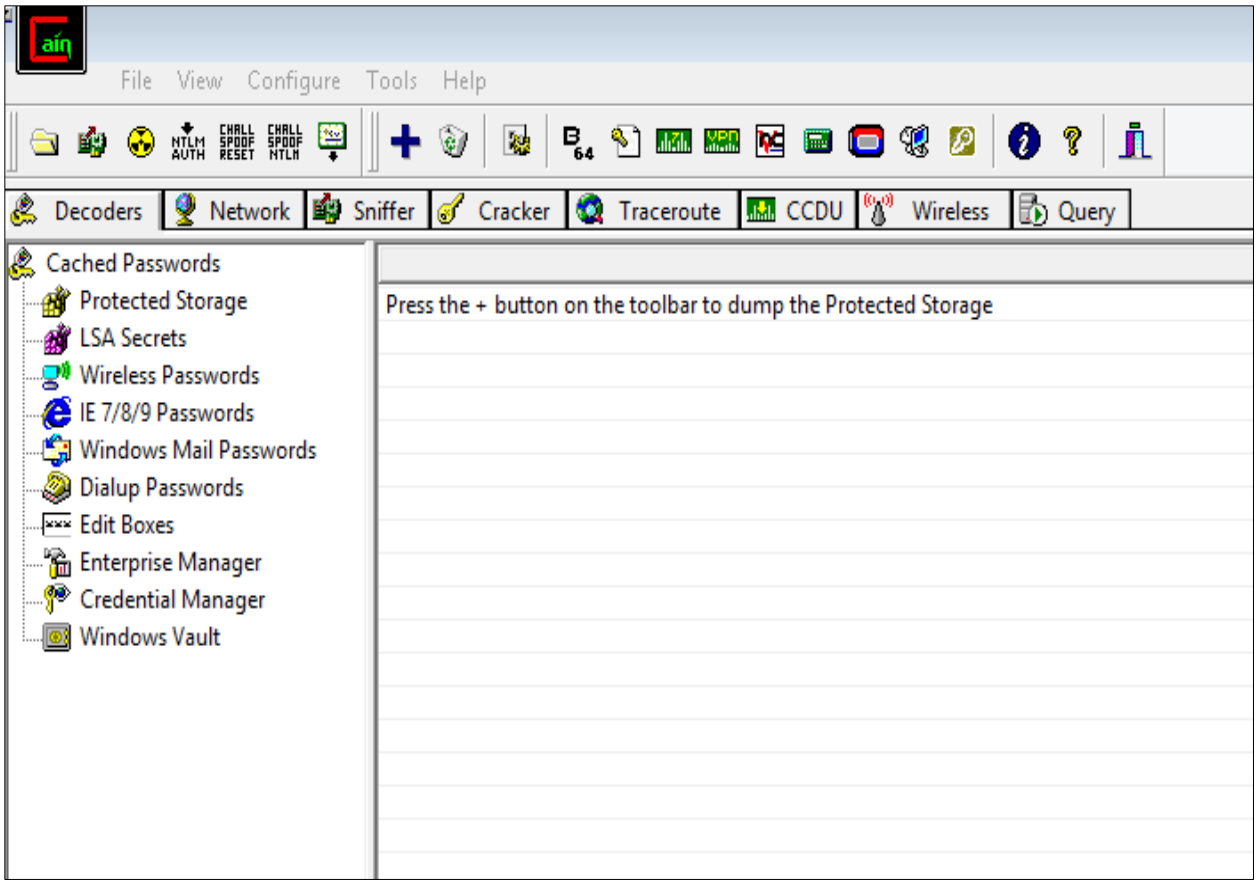


Figure 8: Opening Cain & Abel tool

Step 5: Click the sniffer tab and press “configure” to open configuration dialog. Select an adapter from the configuration dialog box and click “ok” as shown in Figure 9.

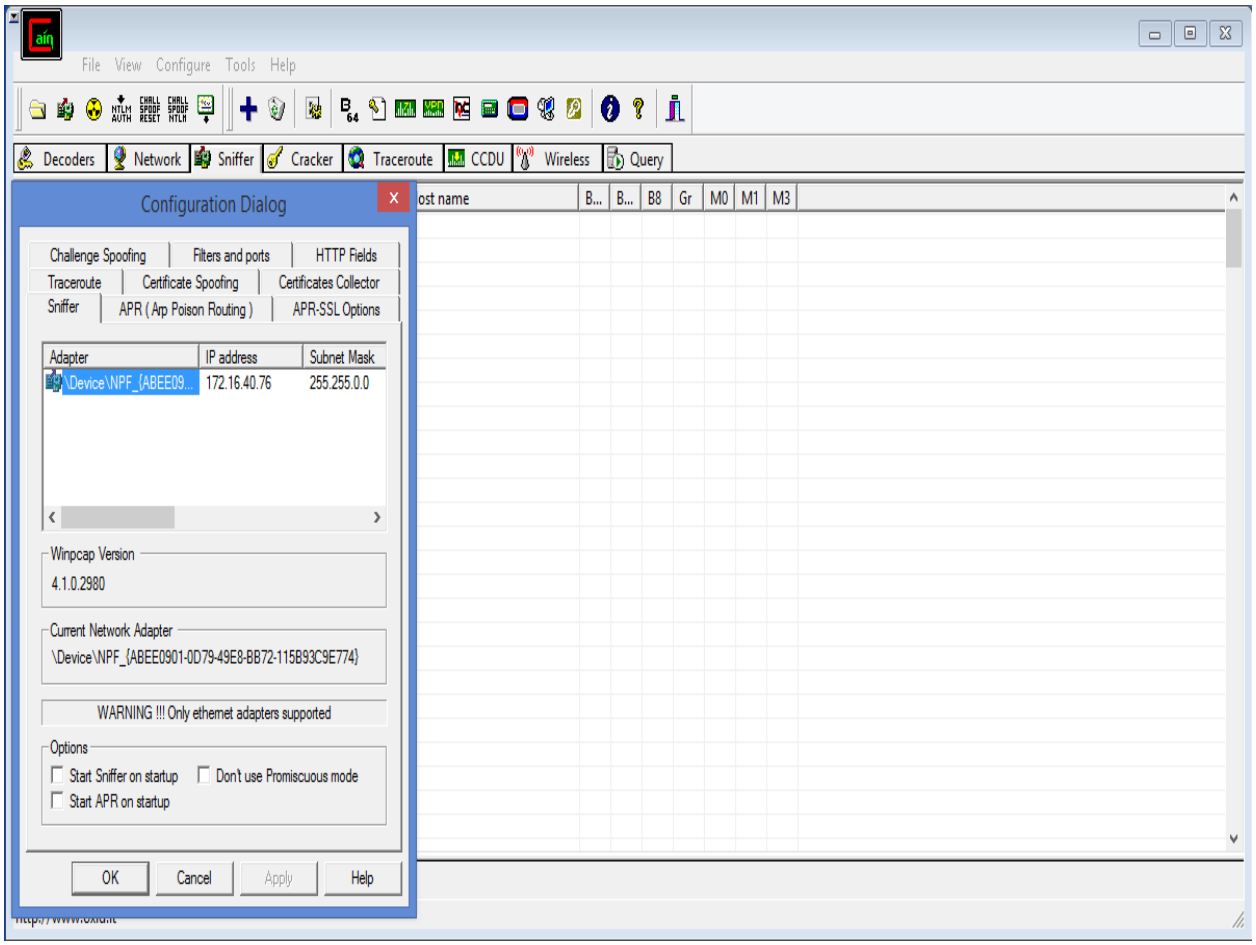


Figure 9: Opening configuration dialog to select the router

Step 6: Turn on the sniffer and click the "+"icon to select all host in the subnet or give a range of IP address. Click "ok" as shown in Figure 10.

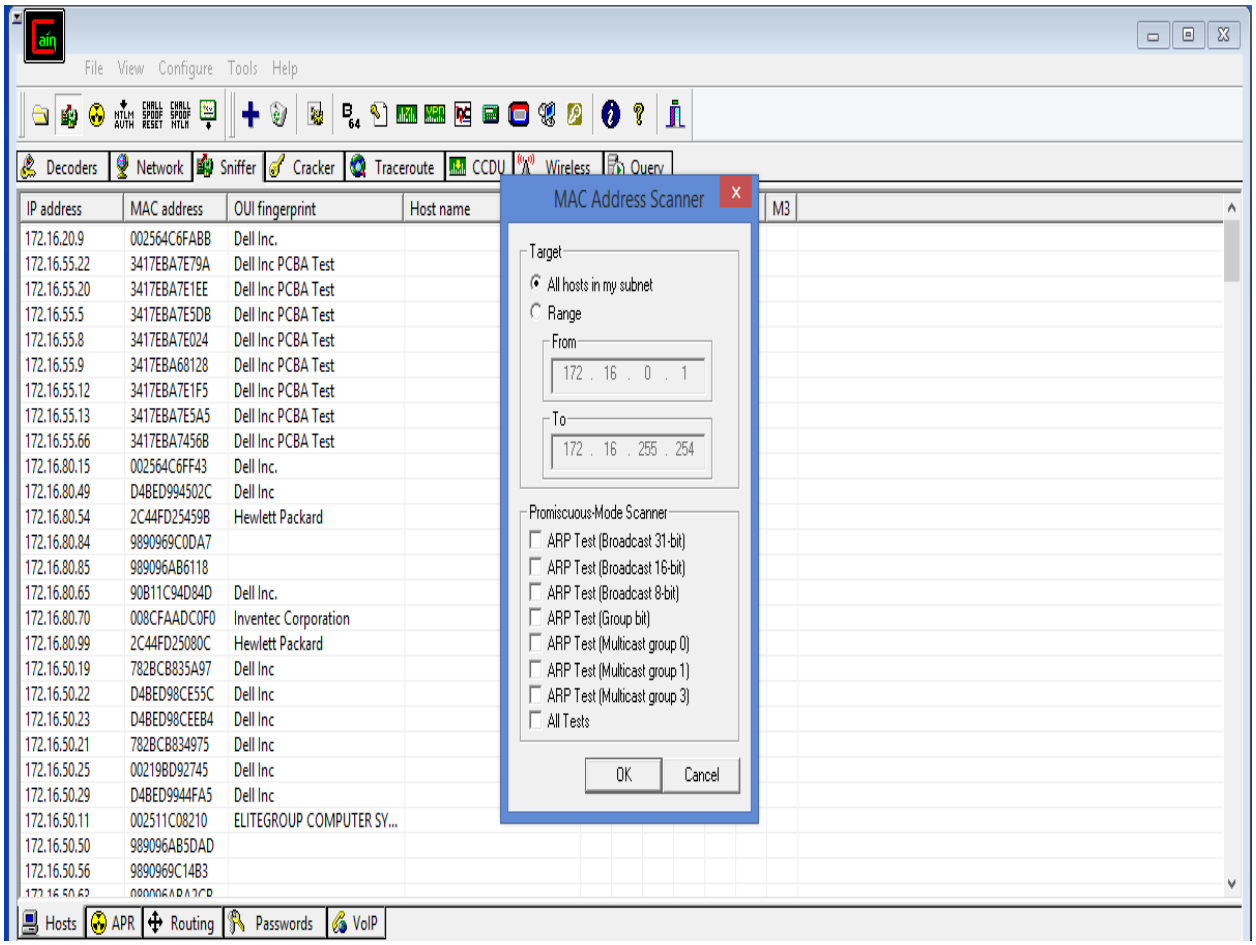


Figure 10: MAC address scanner

Step 7: Select the IP address of target host (172.16.55.9) from the list of hosts as shown in Figure 11.

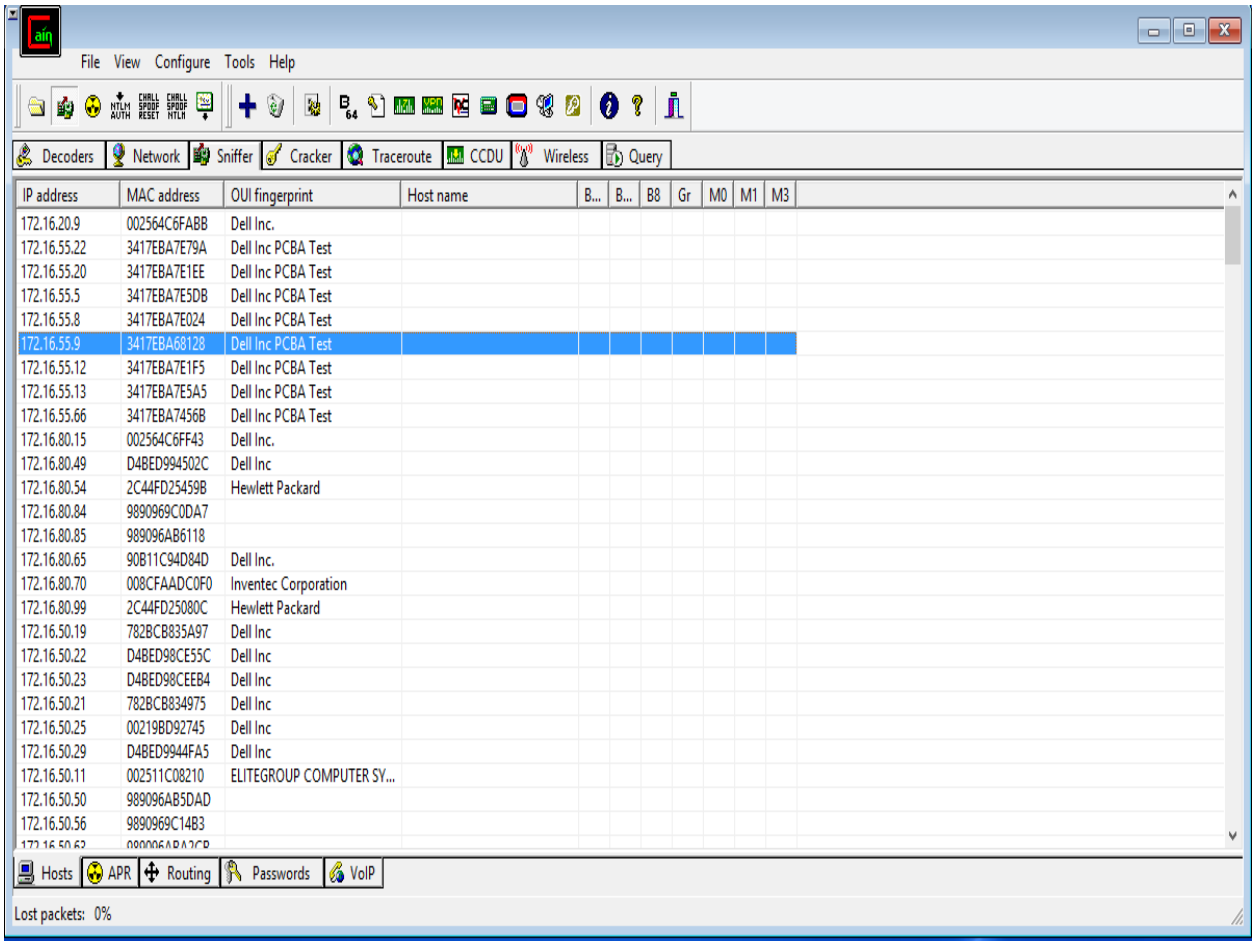


Figure 11: Selecting a target

Step 8: Select APR tab and perform ARP route poisoning to poison the route and sniff the network packets. Select the IP address of router on left side of the table and IP address of the target host (or we can select all IP addresses) on the right side of the table as shown in Figure 12 and Figure 13 respectively.

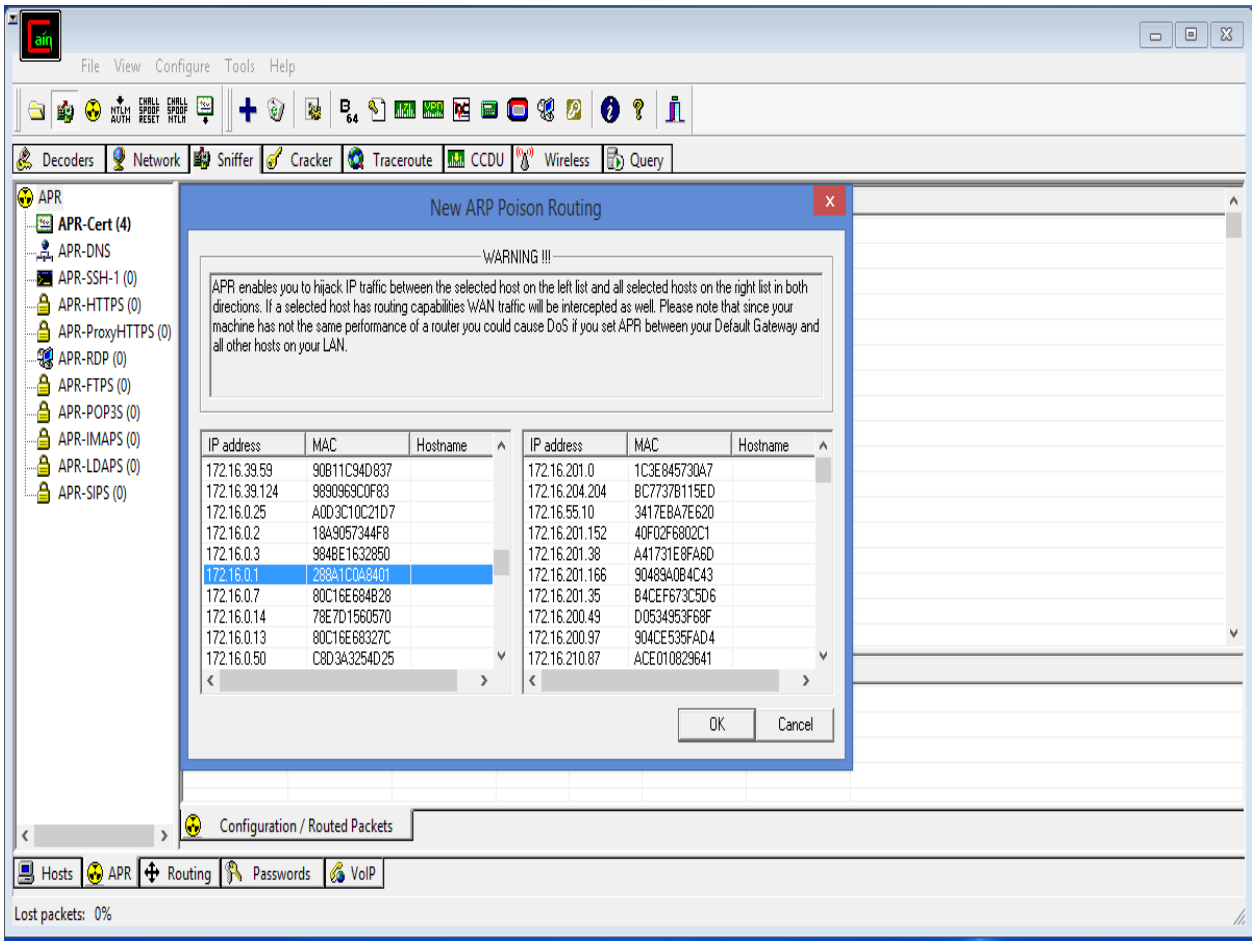


Figure 12: ARP route poisoning

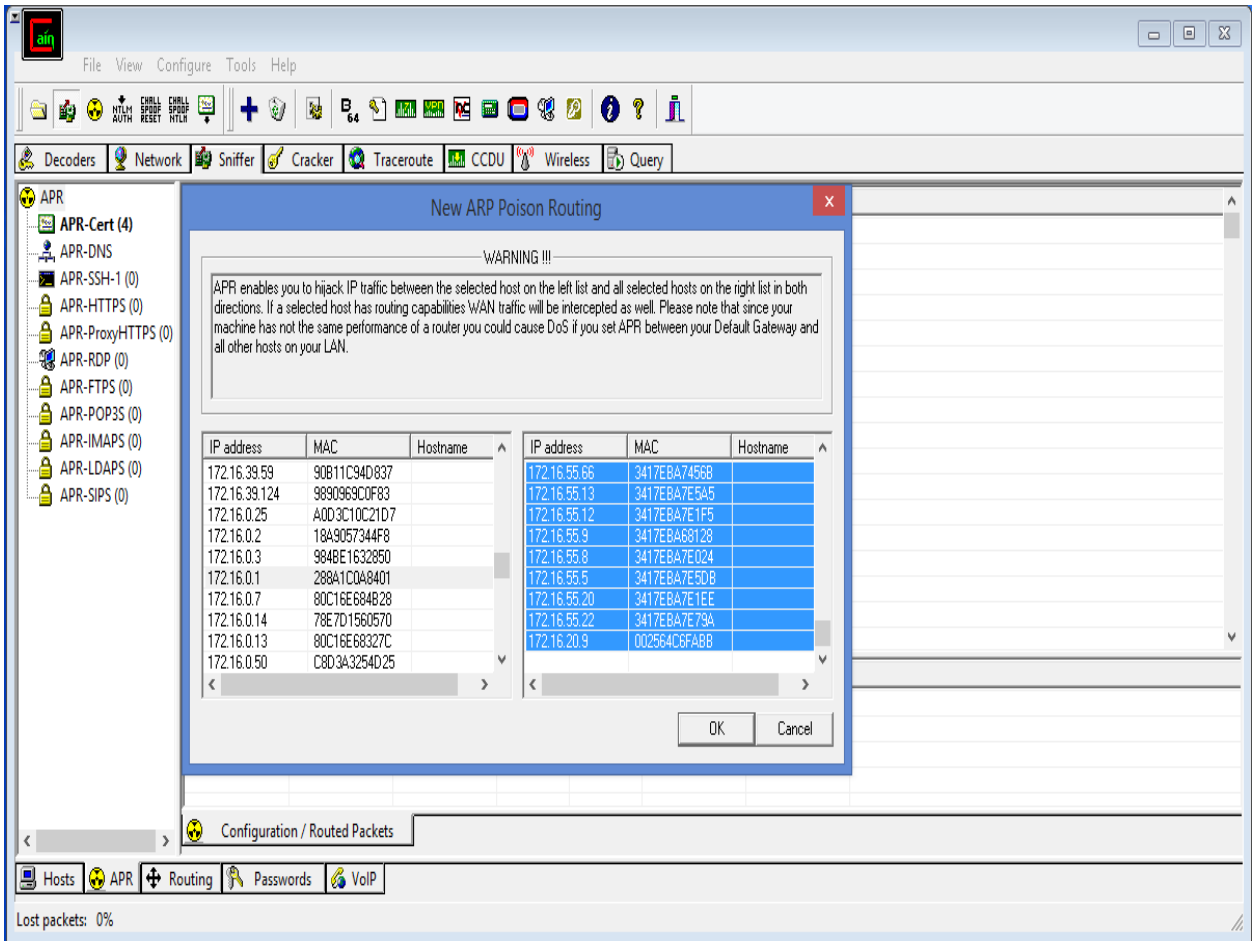


Figure 13: Selecting IP address of router and target host

Step 9: As shown in Figure 14, the IP address of the target host (172.16.55.9) is displayed with the IP address of the router (172.16.0.1)

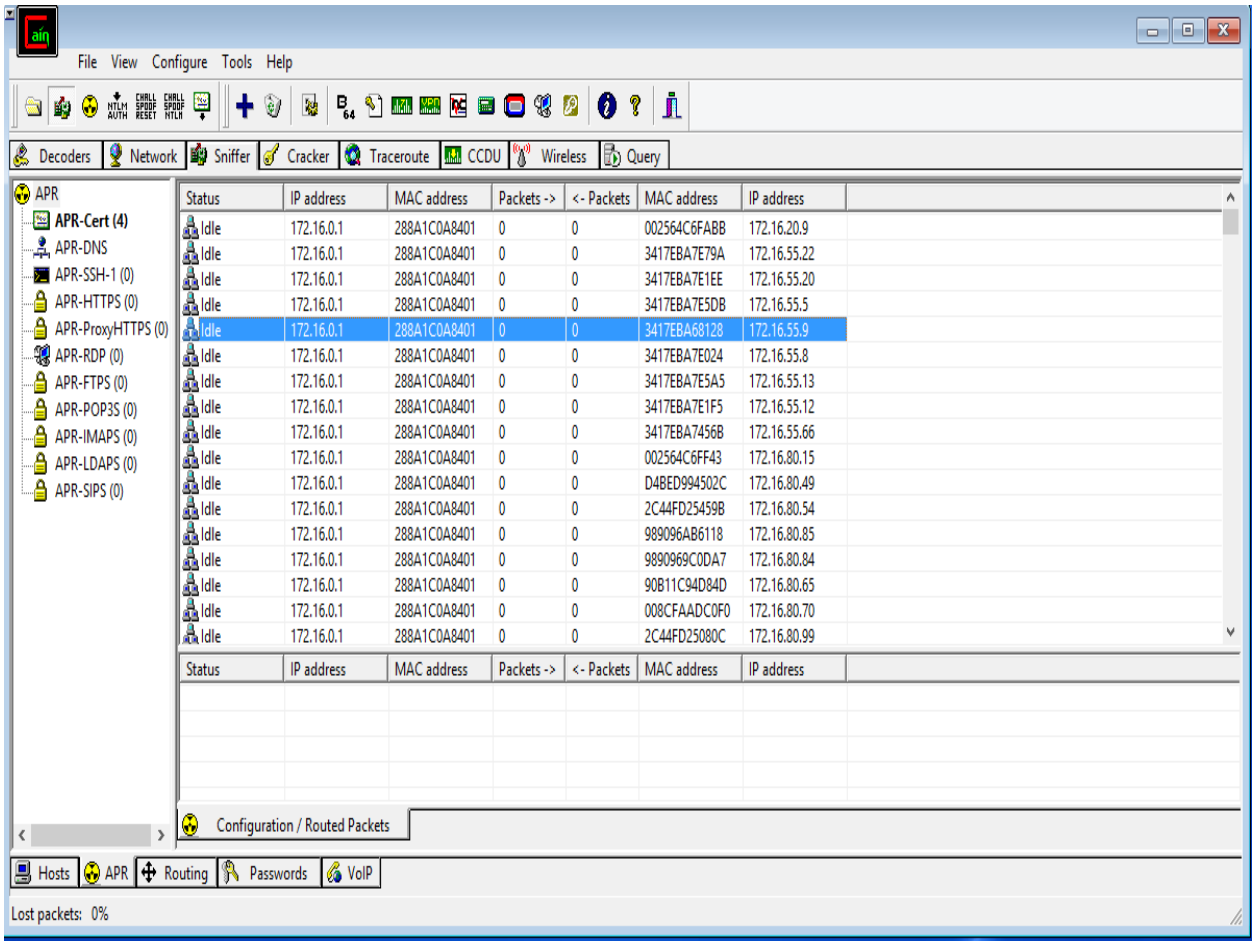


Figure 14: Idle status

Step 10: Now open an HTTP website on the target host machine (172.16.55.9) and create an account on that website as shown in Figure 15 and Figure 16 respectively.

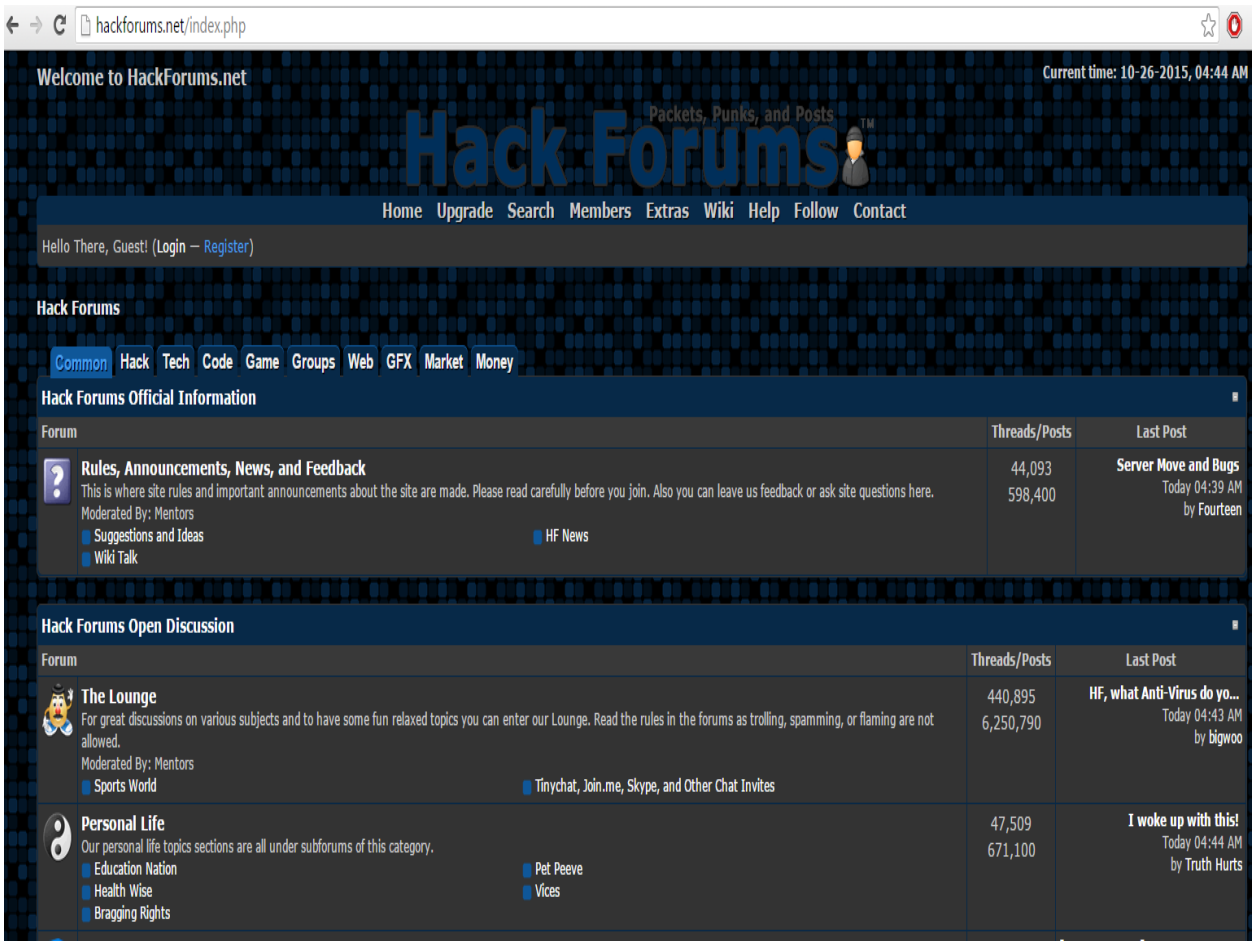


Figure 15: Open an HTTP website on target host

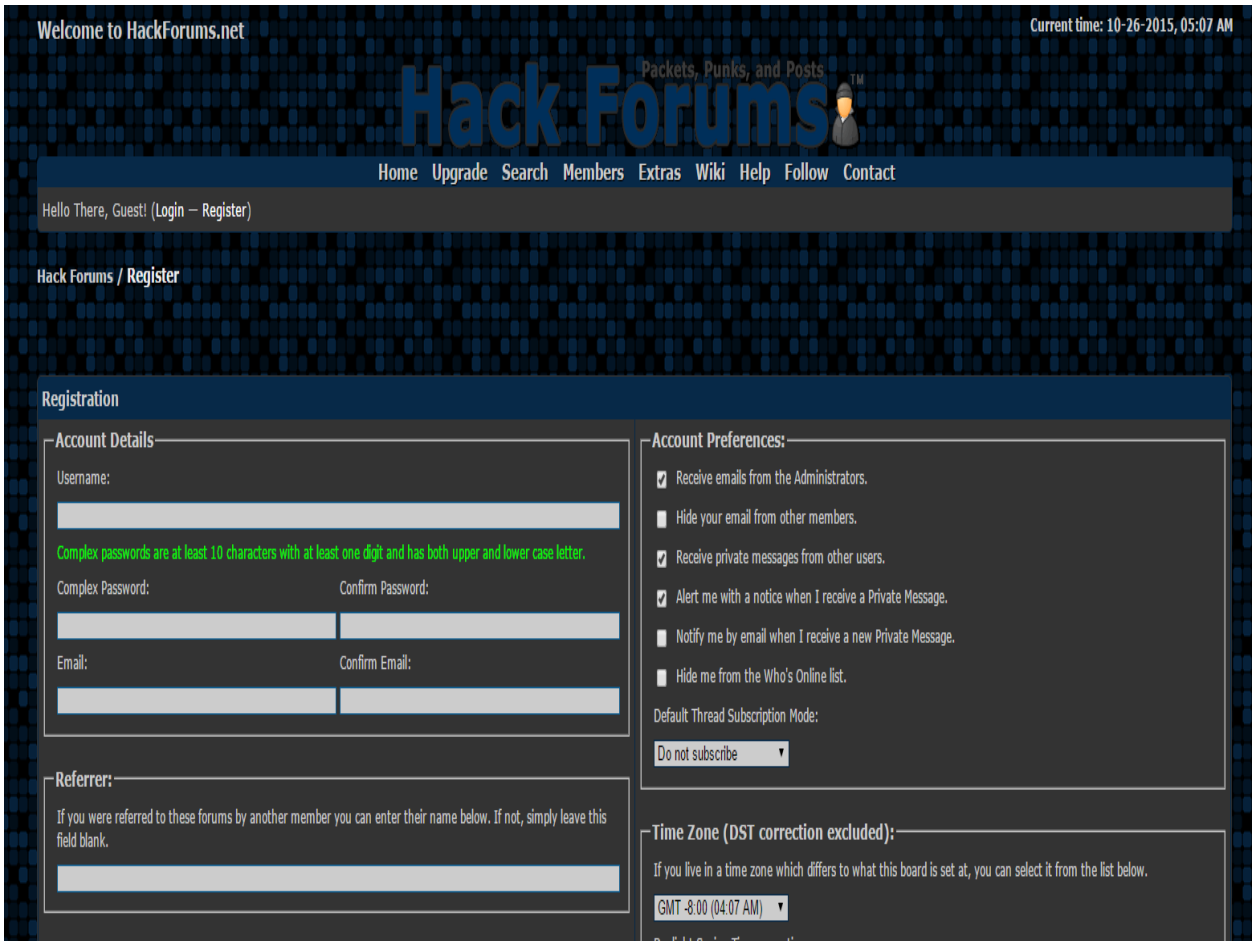


Figure 16: Creating an account in the website

Step 11: Now start poisoning the route to sniff the network packets by clicking the APR icon and the status will be changed from “Idle” to “Poisoning” as shown in Figure 17 and Figure 18 respectively.

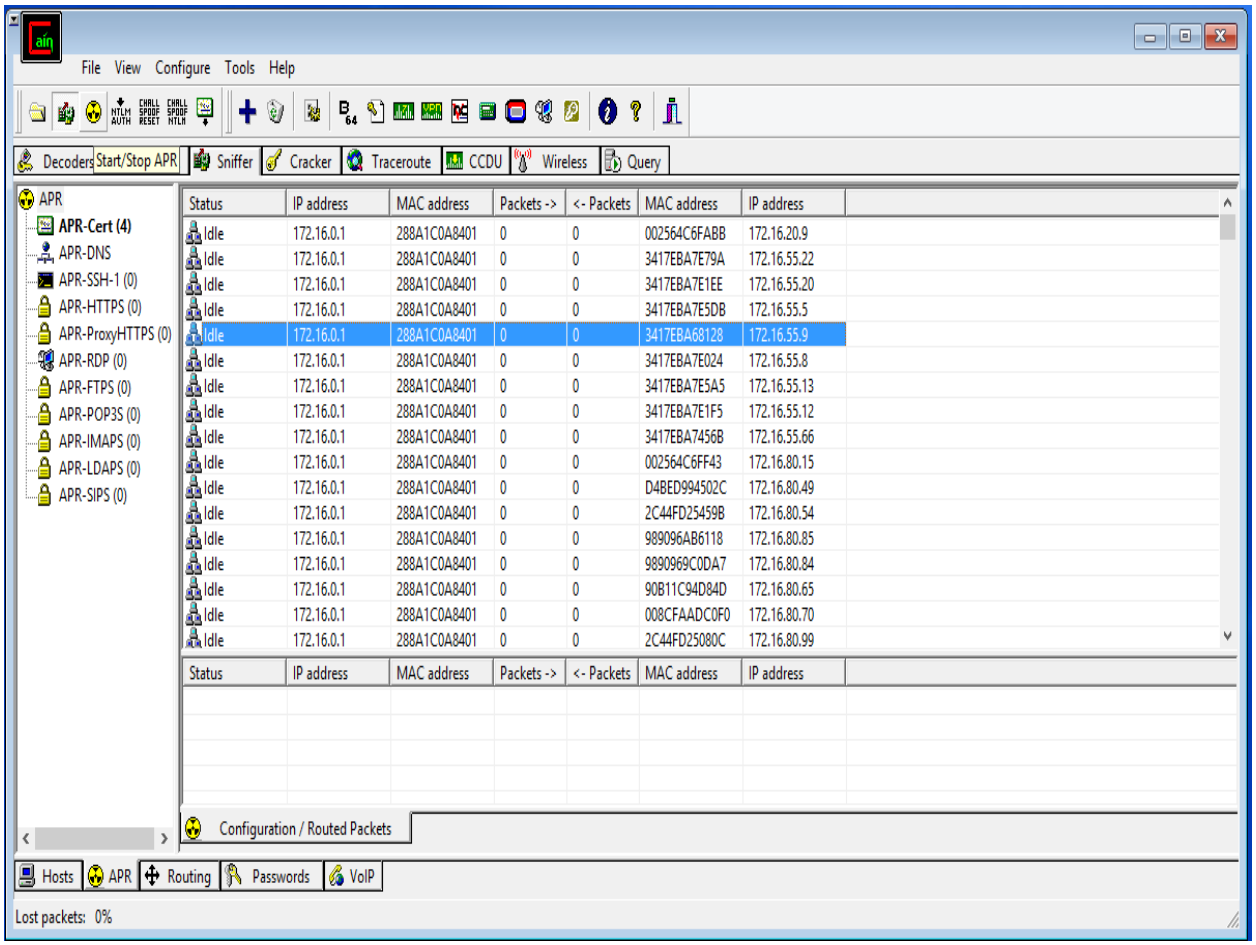


Figure 17: Before poisoning the route

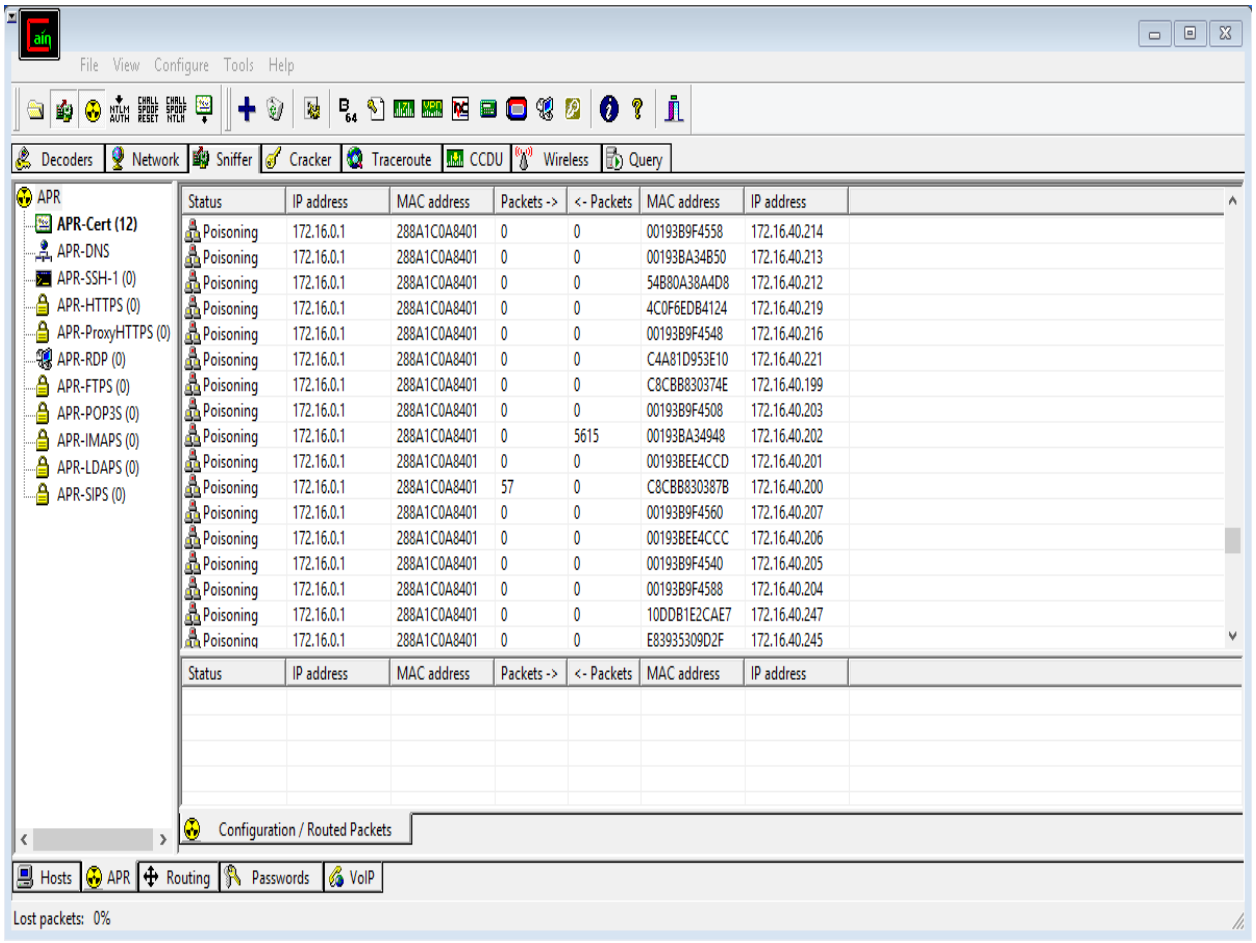


Figure 18: After poisoning the route

Step 12: Select “HTTP” tab to check the username, password, and URL captured after sniffing the network as shown in Figure 19 and Figure 20 respectively.

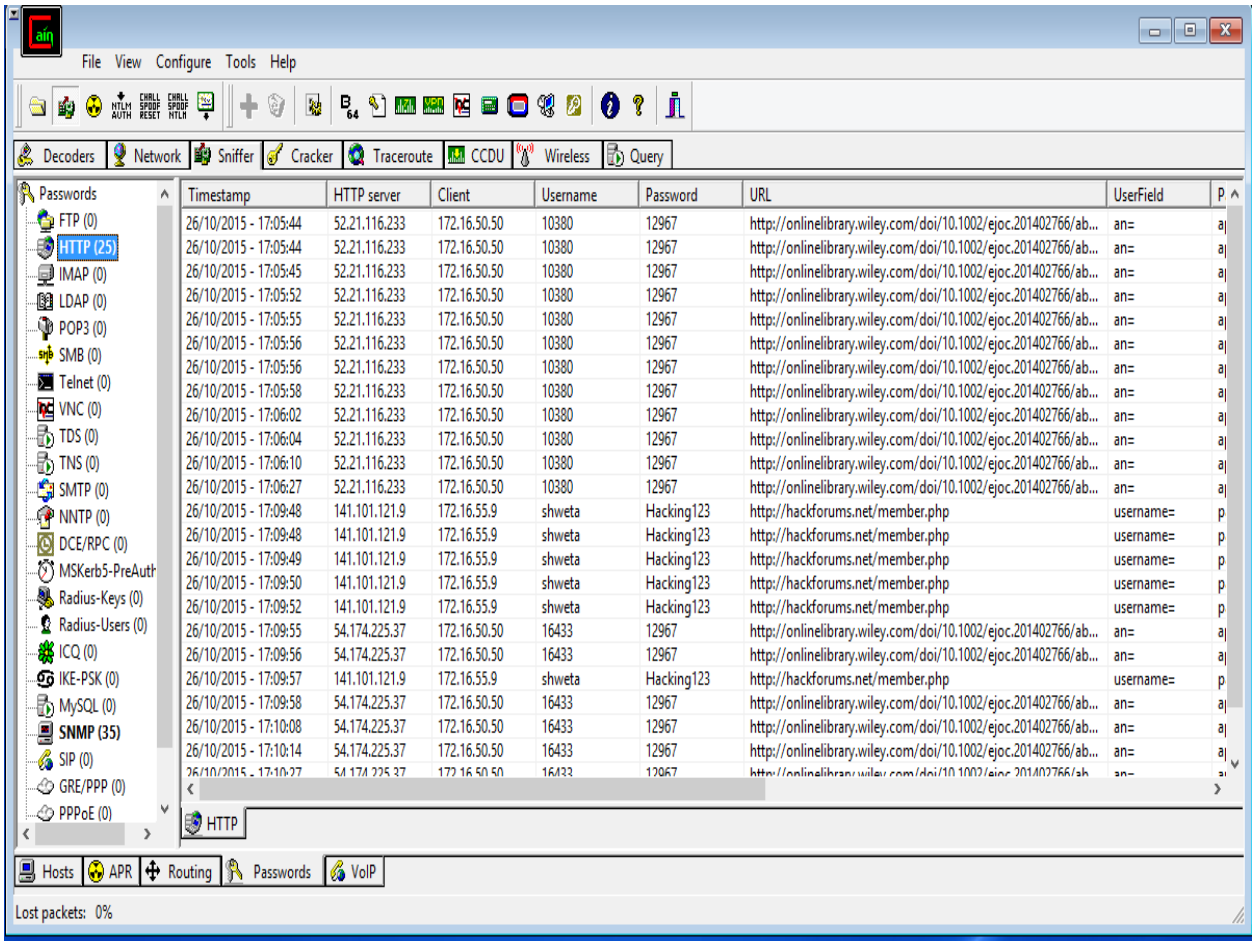


Figure 19: Selecting HTTP tab

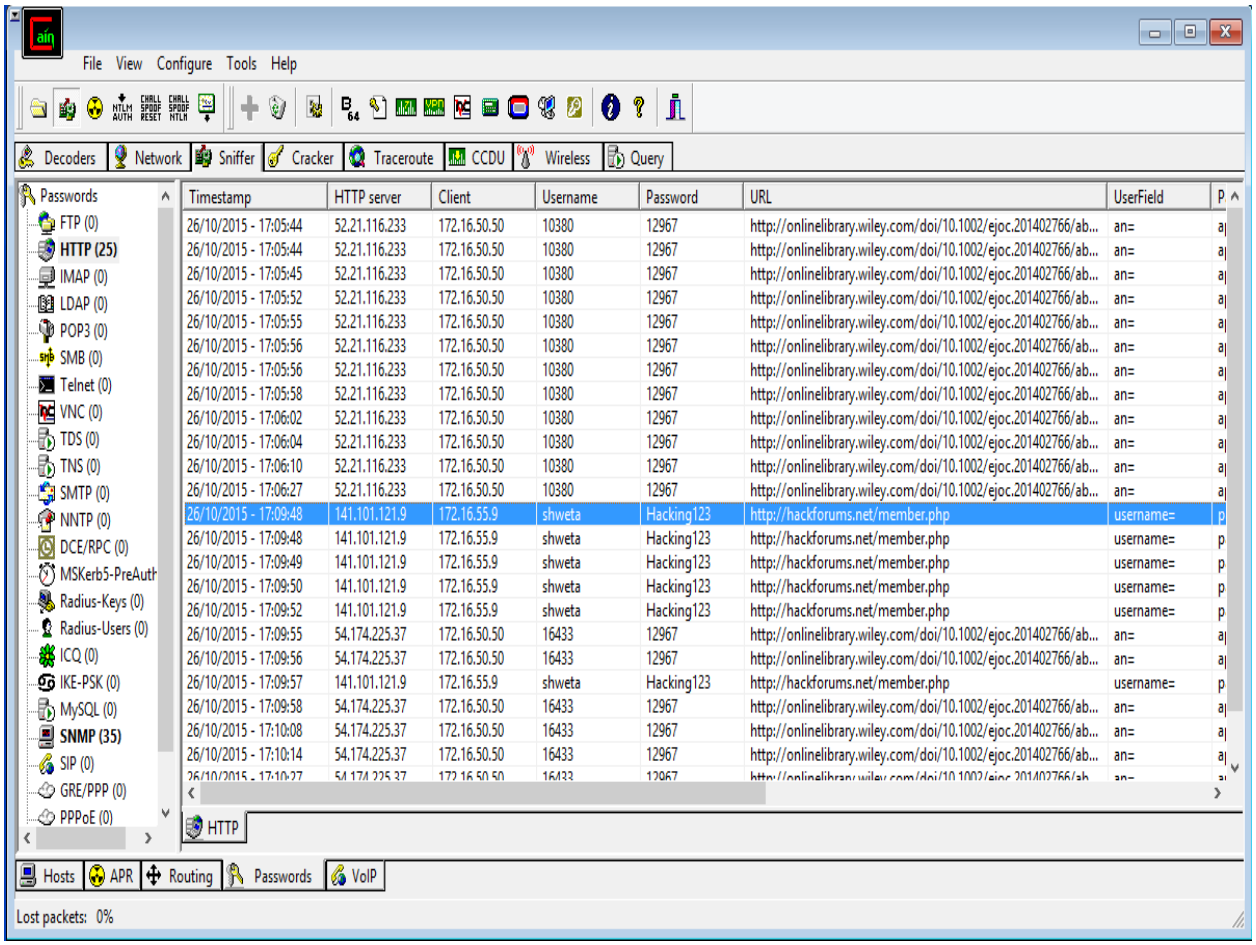


Figure 20: Captured username and password on host machine

Step 13: Now login the website with captured username and password on your host machine as shown in Figure 21 and Figure 22 respectively.

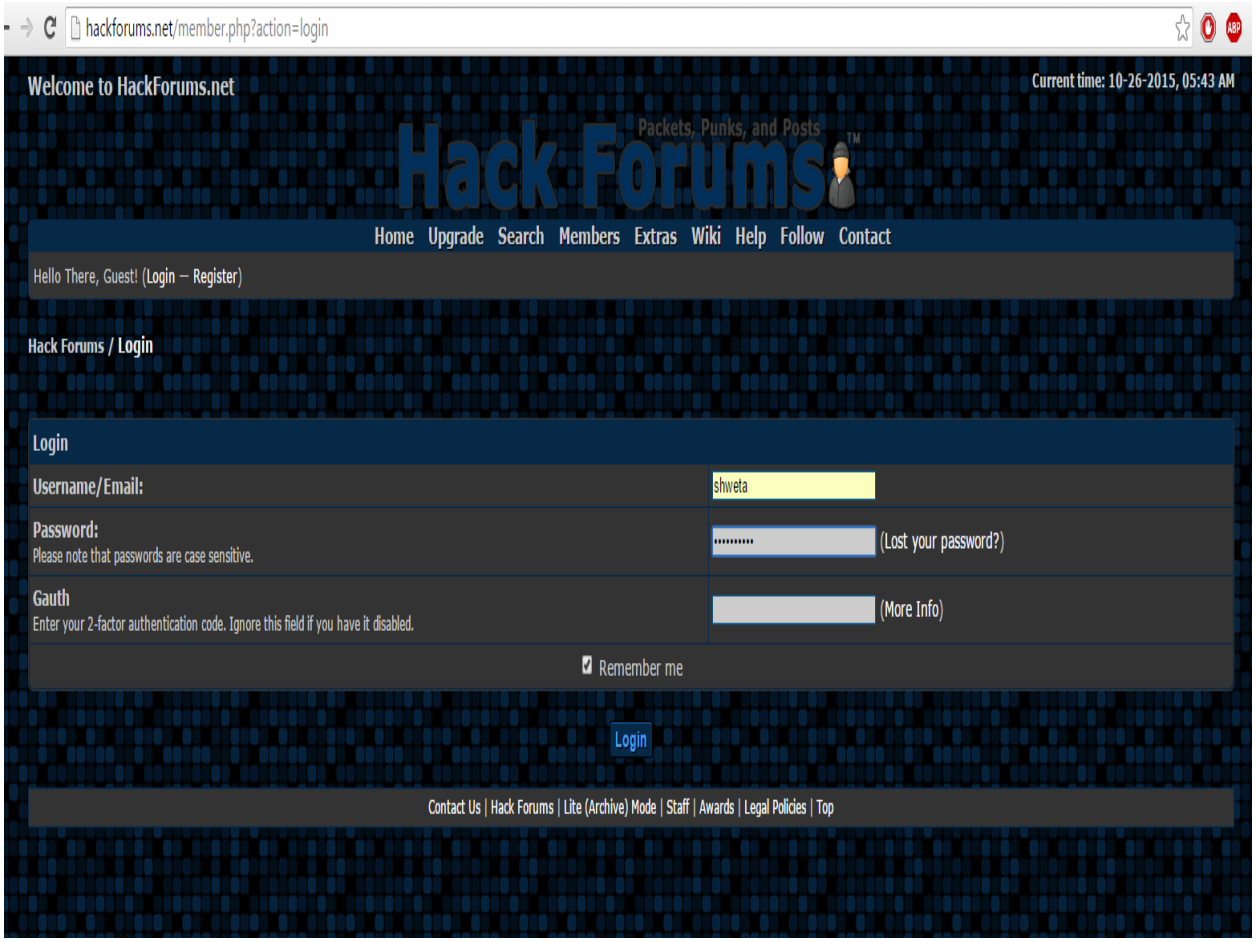


Figure 21: Typing the captured username and password

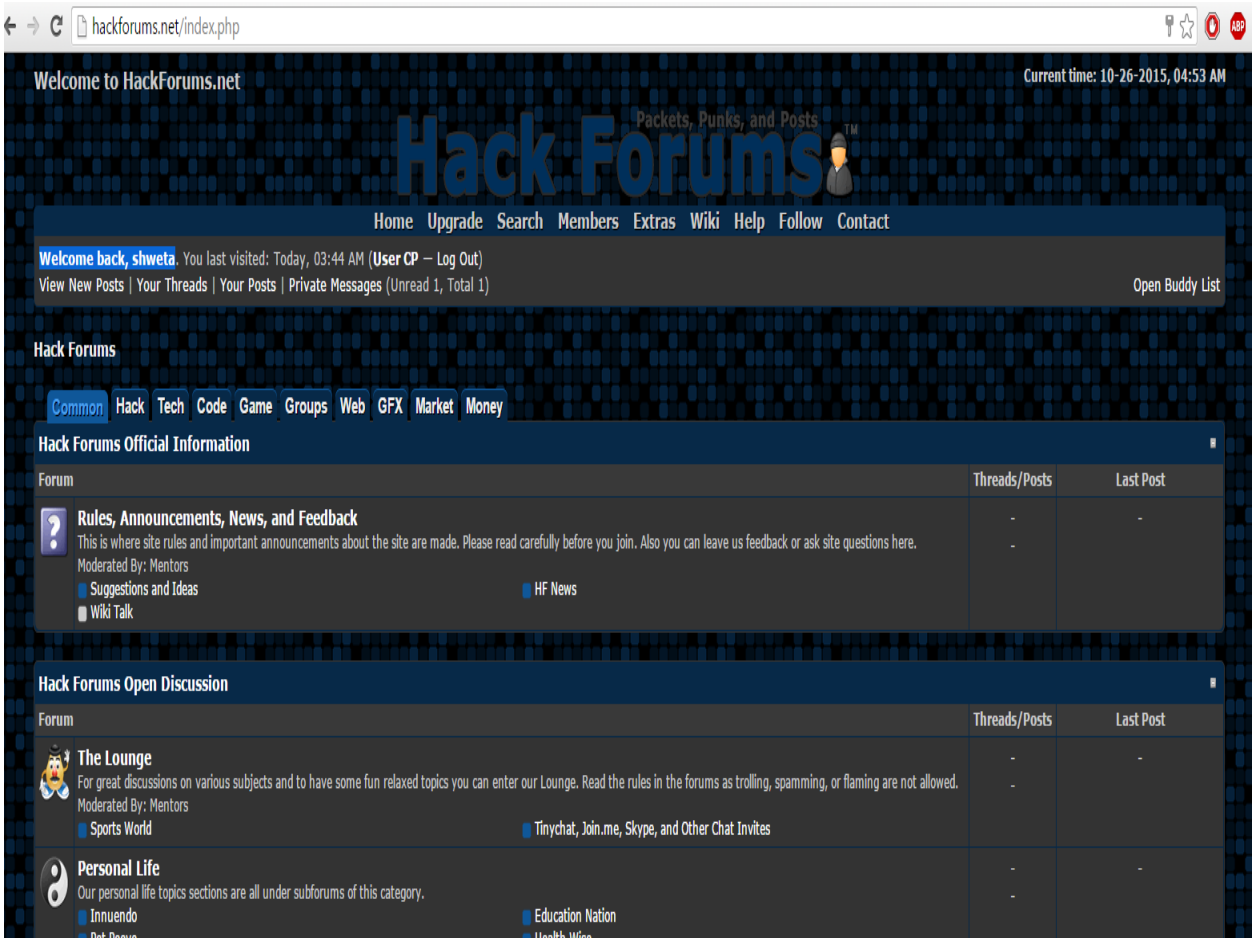


Figure 22: Successfully authenticated

COUNTERMEASURES

The following countermeasures must be followed to prevent sniffing of usernames and passwords:

- **Use HTTPS websites:** Always make account on HTTPS website. In HTTPS, 'S' stands for security which implies the passwords are stored in encrypted form.
- **Don't make accounts in HTTP websites:** The passwords stored in HTTP websites are in plain text and are not

encrypted. That's why they are easily readable by the hackers.

- **Wrong Policy:** While developing a website, an error message of wrong username should not be displayed as "incorrect username" as shown in Figure 23 because hackers can get an idea that the password is correct while the user name is incorrect. Similarly, an error message of wrong password should not be displayed as "incorrect password" as shown in Figure 24 and Figure 25 because hackers can get an idea that the password is incorrect while the username is correct.
- **Correct policy:** The correct policy of showing an error message is- "incorrect username or password" as shown in Figure 25. This will increase the permutation and combination computations of hackers because they need to spend more time to get the username and password.

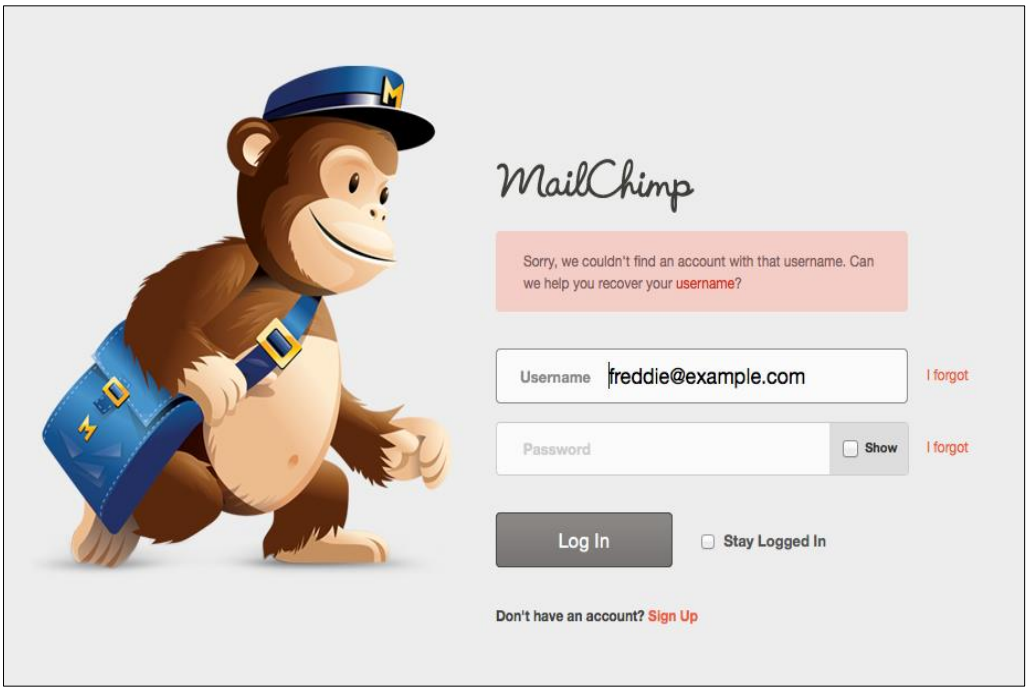


Figure 23: Wrong policy-I

Figure 24: Wrong policy-II

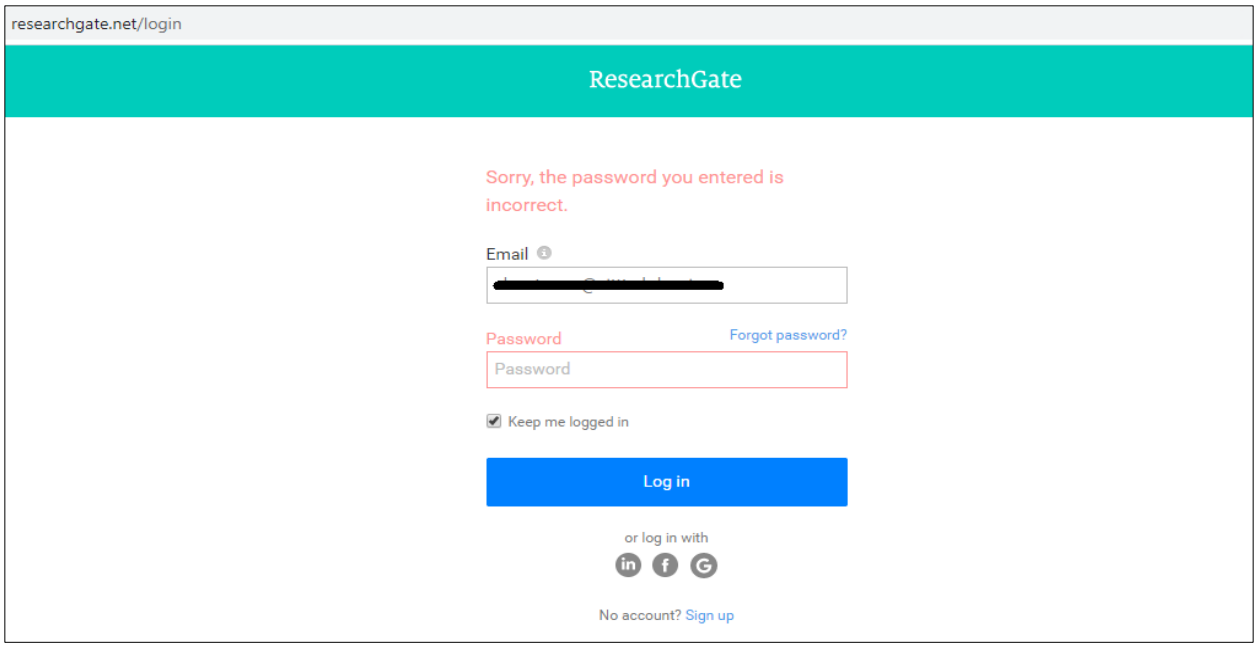


Figure 25: Wrong policy-III

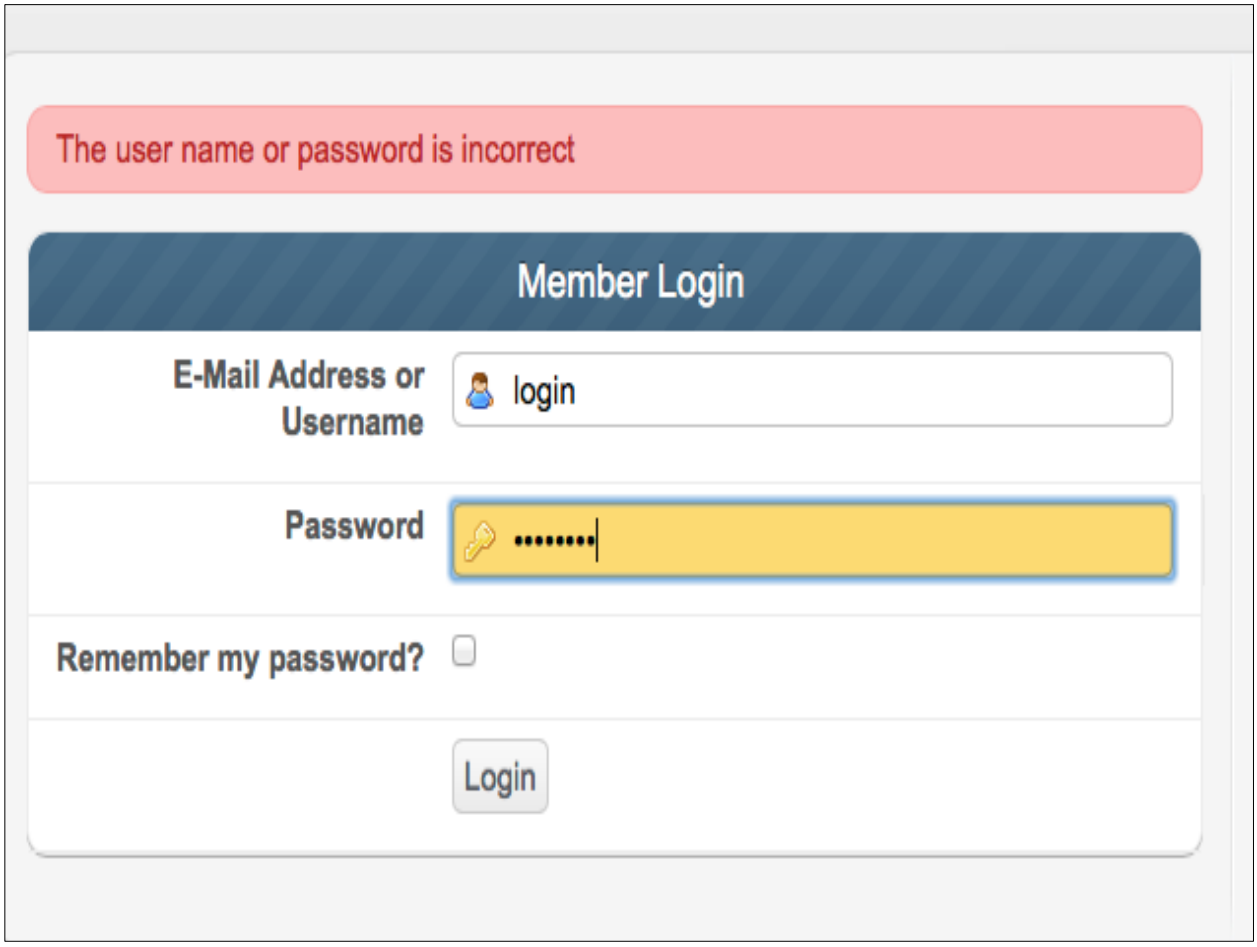


Figure 25: Correct policy

REFERENCES

[1] Darknet, “Cain And Abel Download – Windows Password Cracker,” 2017. https://www.darknet.org.uk/2007/01/cain-and-abel-download-windows-password-cracker/ (accessed Apr. 11, 2020).