**DELHI TECHNOLOGICAL UNIVERSITY**

Bawana Rd, Shahbad Daulatpur Village, Rohini, New Delhi, Delhi 110042



**ETHICAL HACKING (G-2)**

**LAB FILE**

**SUBMITTED BY: SUBMITTED TO:**

**Ritik Singh Ms. Swetha Allam**

**2K19/CO/319**

## PRACTICAL NO.1

**AIM: To learn about hacking tools and skills.**

**Learning Objective** : At the end of the session you will be able to

• familiarize withpopular hacking tools.

• understand various hacking techniques in brief.

• learn some of the skills that you would require to become an expert in Ethical Hacking

**Introduction**

In this manual, we will discuss in brief some of famous tools that are widely used to prevent hacking and getting unauthorized access to a computer or network system.

* + 1. **NMAP**

Nmap stands for Network Mapper. It is an open source tool that is used widely for network discovery and security auditing. Nmap was originally designed to scan large networks, but it can work equally well for single hosts. Network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.

Nmap uses raw IP packets to determine:

• what hosts are available on the network,

• what services those hosts are offering,

• what operating systems they are running on,

• what type of firewalls are in use, and other such characteristics.

Nmap runs on all major computer operating systems such as Windows, Mac OS X, and Linux.

* + 1. **Metasploit**

Metasploit is one of the most powerful exploit tools. It’s a product of Rapid7 and most of its resources can be found at: www.metasploit.com. It comes in two versions − commercial and free edition. Metasploit can be used with command prompt or with Web UI.

With Metasploit, you can perform the following operations: • Conduct basic penetration tests on small networks. • Run spot checks on the exploitability of vulnerabilities. • Discover the network or import scan data. • Browse exploit modules and run individual exploits on hosts.

* + 1. **Burp Suite**

Burp Suite is a popular platform that is widely used for performing security testing of web applications. It has various tools that work in collaboration to support the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities.

Burp is easy to use and provides the administrators full control to combine advanced manual techniques with automation for efficient testing. Burp can be easily configured and it contains features to assist even the most experienced testers with their work.

* + 1. **Angry IP Scanner**

Angry IP scanner is a lightweight, cross-platform IP address and port scanner. It can scan IP addresses in any range. It can be freely copied and used anywhere. In order to increase the scanning speed, it uses multithreaded approach, wherein a separate scanning thread is created for each scanned IP address.

Angry IP Scanner simply pings each IP address to check if it’s alive, and then, it resolves its hostname, determines the MAC address, scans ports, etc. The amount of gathered data about each host can be saved to TXT, XML, CSV, or IP-Port list files.

* + 1. **Cain & Abel**

Cain & Abel is a password recovery tool for Microsoft Operating Systems. It helps in easy recovery of various kinds of passwords by employing any of the following methods:

• sniffing the network,

• cracking encrypted passwords using Dictionary, Brute-Force and Cryptanalysis attacks,

• recording VoIP conversations,

• decoding scrambled passwords,

• recovering wireless network keys,

• revealing password boxes,

• uncovering cached passwords and analyzing routing protocols.

Cain & Abel is a useful tool for security consultants, professional penetration testers and everyone else who plans to use it for ethical reasons.

* + 1. **Ettercap**

Ettercap stands for Ethernet Capture. It is a network security tool for Man-in-the-Middle attacks. It features sniffing of live connections, content filtering on the fly and many other interesting tricks. Ettercap has inbuilt features for network and host analysis. It supports active and passive dissection of many protocols.

You can run Ettercap on all the popular operating systems such as Windows, Linux, and Mac OS X.

* + 1. **EtherPeek**

EtherPeek is a wonderful tool that simplifies network analysis in a multiprotocol heterogeneous network environment. EtherPeek is a small tool (less than 2 MB) that can be easily installed in a matter of few minutes. EtherPeek proactively sniffs traffic packets on a network. By default, EtherPeek supports protocols such as AppleTalk, IP, IP Address Resolution Protocol (ARP), NetWare, TCP, UDP, NetBEUI, and NBT packets.

* 1. **Hacking Skills**

As an ethical hacker, you will need to understand various hacking techniques such as: • Password guessing and cracking

• Session hijacking

• Session spoofing

• Network traffic sniffing

• Network traffic sniffing

• Denial of Service attacks

• Exploiting buffer overflow vulnerabilities

• SQL injection

* 1. **Basic Skills**

Computer Hacking is a Science as well as an Art. Like any other expertise, you need to put a lot of effort in order to acquire knowledge and become an expert hacker. Once you are on the track, you would need more effort to keep up-to-date with latest technologies, new vulnerabilities and exploitation techniques.

• An ethical hacker must be a computer systems expert and needs to have very strong programming and computer networking skills.

## PRACTICAL NO.2

**AIM : Learn about the basic Networking Commands in Windows-Command Line.**

**THEORY:**

**1. Windows - Command Line:**

**cmd.exe** is the default command-line interpreter for the OS/2, eComStation, ArcaOS, Microsoft Windows (Windows NT family and Windows CE family), and ReactOS operating systems. The name refers to its executable filename. It is also commonly referred to as **cmd** or the **Command Prompt**, referring to the default window title on Windows. The implementations differ on the various systems but the behaviour and basic set of commands is generally consistent. cmd.exe is the counterpart of COMMAND.COM in DOS and Windows 9x systems, and analogous to the Unix shells used on Unix-like systems. The initial version of cmd.exe for Windows NT was developed by Therese Stowell. Windows CE 2.11 was the first embedded Windows release to support a console and a Windows CE version of cmd.exe. On Windows CE .NET 4.2, Windows CE 5.0 and Windows Embedded CE 6.0 it is also referred to as **Command Processor Shell**. The ReactOS implementation of cmd.exe is derived from FreeCOM, the FreeDOS command line interpreter.

**2. Ipconfig**

**ipconfig** (standing for "Internet Protocol configuration") is a console application program of some computer operating systems that displays all current TCP/IP network configuration values and refreshes Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) settings.

**3. Nslookup**

➢ **nslookup** (from ***n****ame* ***s****erver* ***lookup***) is a network administration command-line tool for querying the Domain Name System (DNS) to obtain the mapping between domain name and IP address, or other DNS records.

➢ nslookup was a member of the BIND name server software. Early in the development of BIND 9, the Internet Systems Consortium planned to deprecate nslookup in favor of host and dig. This decision was reversed in 2004 with the release of BIND 9.3 and nslookup has been fully supported since then.

➢ Unlike dig, nslookup does not use the operating system's local Domain Name System resolver library to perform its queries, and thus may behave differently. Additionally, vendor-provided versions may include output of other sources of name information, such as host files, and Network Information Service. Some behaviours of nslookup may be modified by the contents of resolv.conf.

➢ The ReactOS version was developed by Lucas Suggs and is licensed under the GPL.

**4. Ping**

➢ Ping comes from a term used in sonar technology that sends out pulses of sound, and then listens for the echo to return. On a computer network, a ping tool is built into most operating systems that works in much the same way. You issue the ping command along with a specific URL or IP address. Your computer sends several packets of information out to that device, and then waits for a response. When it gets the response, the ping tool

shows you how long each packet took to make the round trip—or tells you there was no reply.

➢ It sounds simple, and it is. But you can use it to good effect. You can test whether your computer can reach another device—like your router—on your local network, or whether it can reach a device on the Internet. This can help you determine if a network problem is somewhere on your local network, or somewhere beyond. The time it takes packets to return to you can help you identify a slow connection, or if you’re experiencing packet loss.

➢ And it pretty much doesn’t matter what operating system you’re using. Pull up a terminal or Command Prompt window, and you can use ping on macOS, Linux, or any version of Windows.

**5. Tracert**

➢ In computing, **traceroute** and **tracert** are computer network diagnostic commands for displaying possible routes (paths) and measuring transit delays of packets across an Internet Protocol (IP) network. The history of the route is recorded as the round-trip times of the packets received from each successive host (remote node) in the route (path); the sum of the mean times in each hop is a measure of the total time spent to establish the connection. Traceroute proceeds unless all (usually three) sent packets are lost more

than twice; then the connection is lost and the route cannot be evaluated. Ping, on the other hand, only computes the final round-trip times from the destination point.

➢ For Internet Protocol Version 6 (IPv6) the tool sometimes has the name **traceroute6** and **tracert6** .

**6. Netstat**

➢ In computing, **netstat** (***net****work* ***stat****istics*) is a command-line network utility that displays network connections for Transmission Control Protocol (both incoming and outgoing), routing tables, and a number of network interface (network interface controller or software-defined network interface) and network protocol statistics. It is available on Unix, Plan 9, Inferno, and Unix-like operating systems including macOS, Linux, Solaris and BSD. It is also available on IBM OS/2 and on Microsoft Windows NT-based operating systems including Windows XP, Windows Vista, Windows

7, Windows 8 and Windows 10.

➢ It is used for finding problems in the network and to determine the amount of traffic on the network as a performance measurement. On Linux this program is mostly obsolete, although still included in many distributions.

➢ On Linux, netstat (part of "net-tools") is superseded by ss (part of iproute2). The replacement for netstat -r is ip route , the replacement for netstat -i is ip -s link , and the

replacement for netstat -g is ip maddr , all of which are recommended instead.

**7. Shutdown**

➢ The command follows the following syntax:

**shutdown** [**/i** | **/l** | **/s** | **/r** | **/g** | **/a** | **/p** | **/h** | **/e** | **/o**] [**/hybrid**] [**/f**] [**/m \\***computername*] [**/t** *xxx*] [**/d** [**p:**|**u:**]*xx***:***yy*] [**/c "***comment***"**] [**/?**]

➢ The shutdown command is a Command Prompt command that powers off, restarts, logs off, or hibernates your computer. The same one can be used to remotely shut down or restart a computer you have access to over a network.

➢ In some ways, it's similar to the *logoff* command.

**8. Color command**

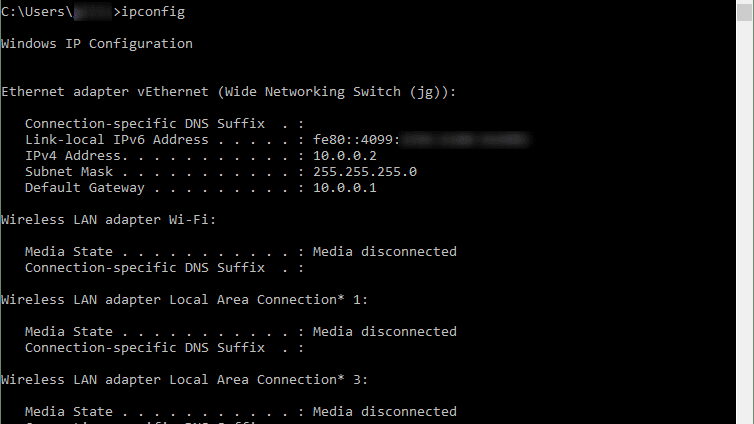
Color is an inbuilt command found inside the Windows Command Processor (cmd.exe), that is used for changing the colors for the console’s foreground and background. By default, the console has white foreground color and black background color (07 color code). The command is generally used either to personalize the aesthetics of the console window, or the make the colors more appropriate for Dim or Dark Displays (ex. TN

panels). In this article, we will learn about the color command and will also take a look at the various uses it

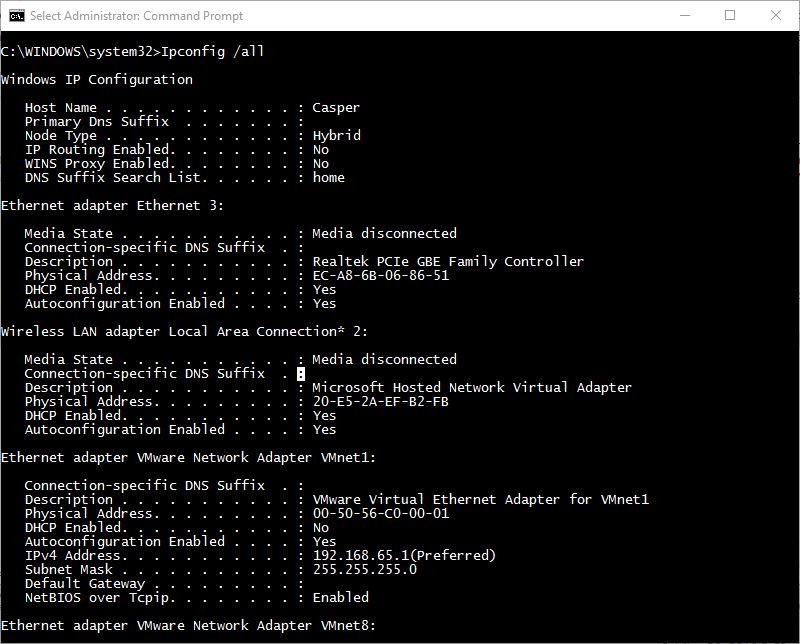
offers.

**OUTPUTS:**

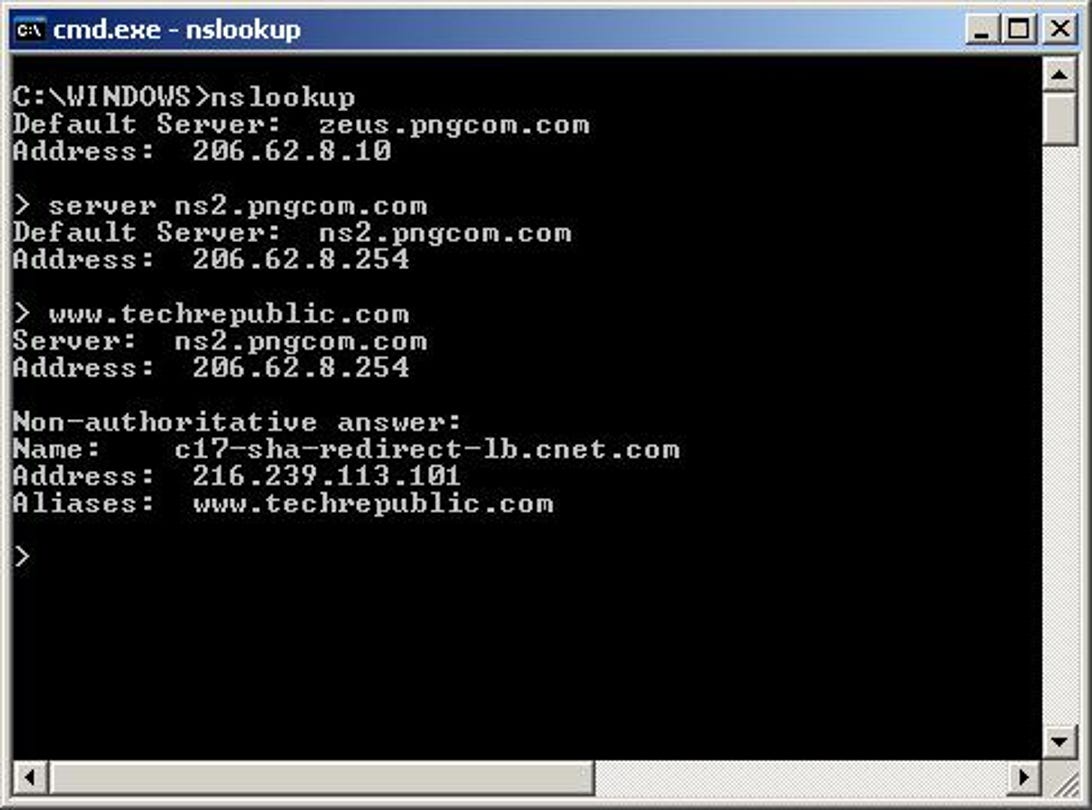
**1. Ipconfig**



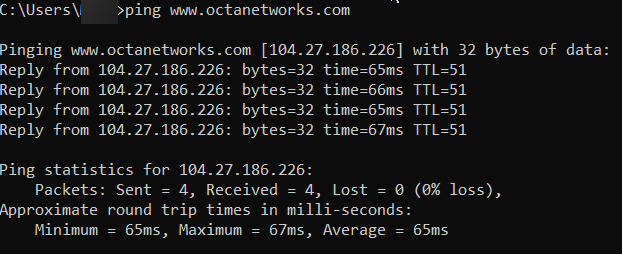
1. **Ipconfig/all**



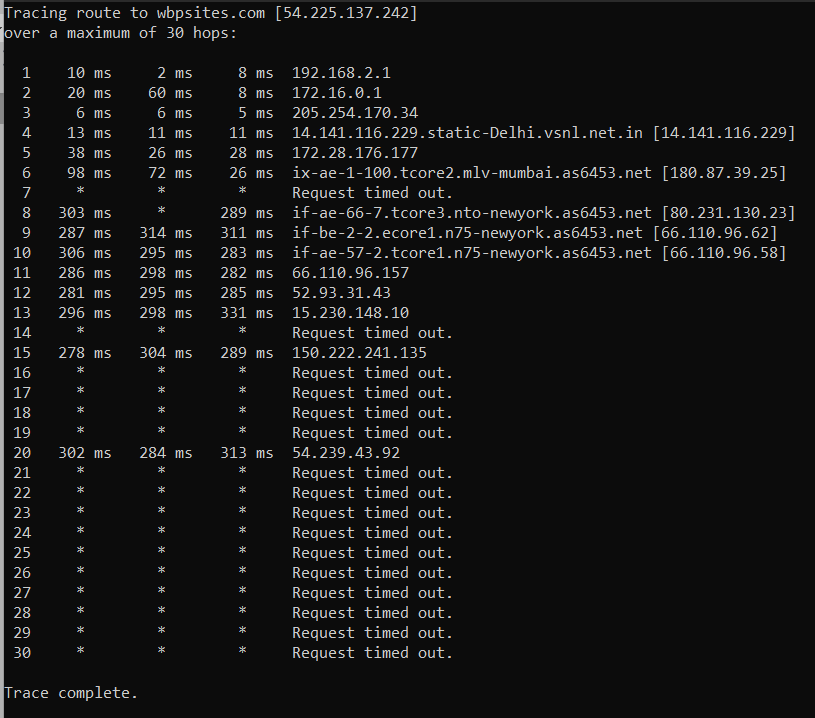
1. **Nslookup**



1. **Ping**



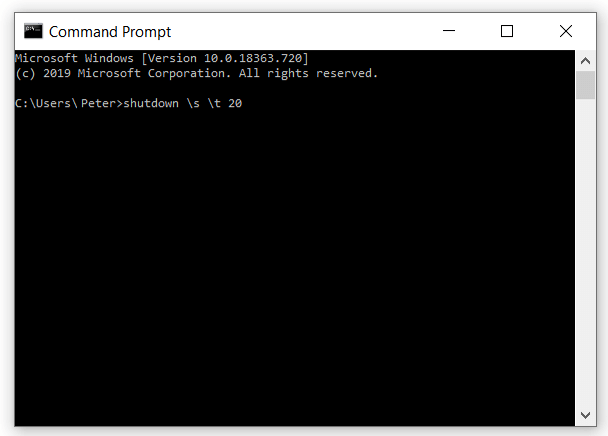
1. **Tracert**



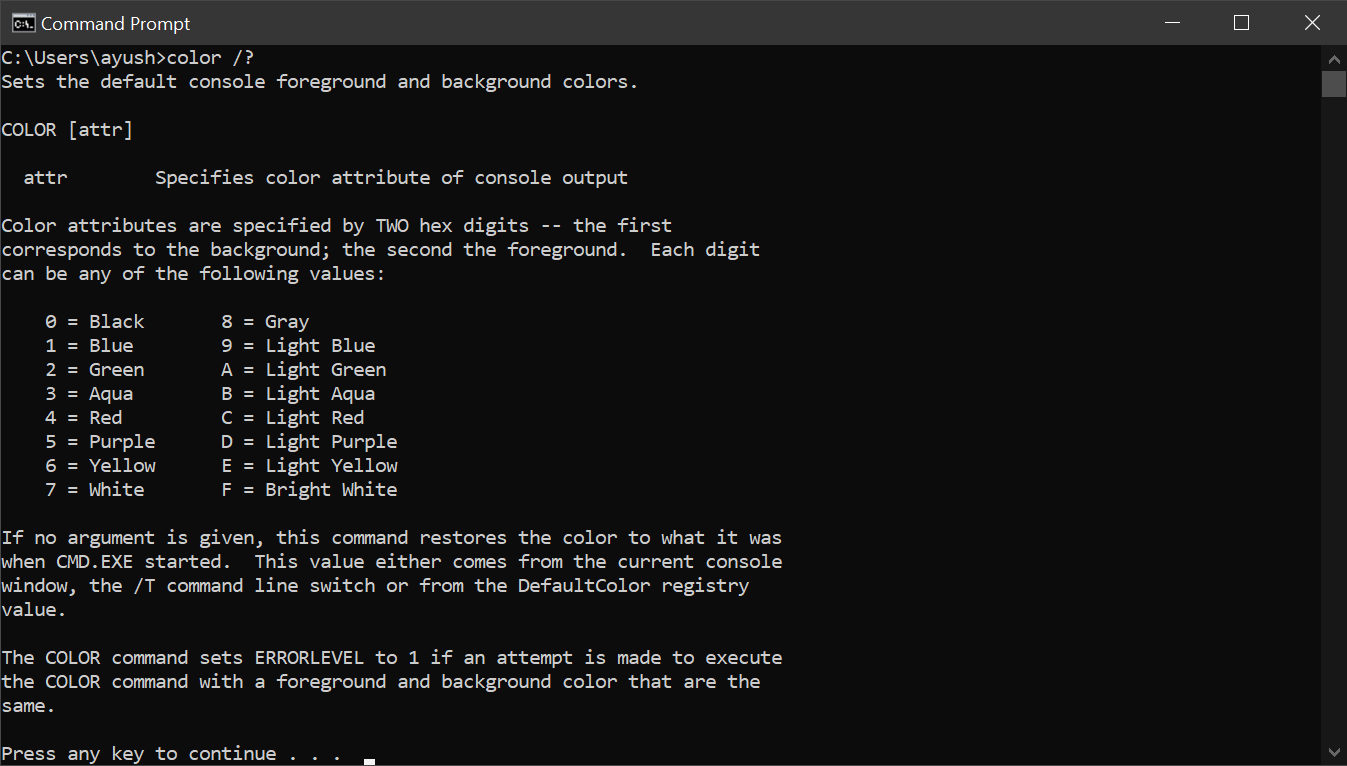
1. **Netstat**



1. **Shutdown /?**



**8. Color -help & color 4**

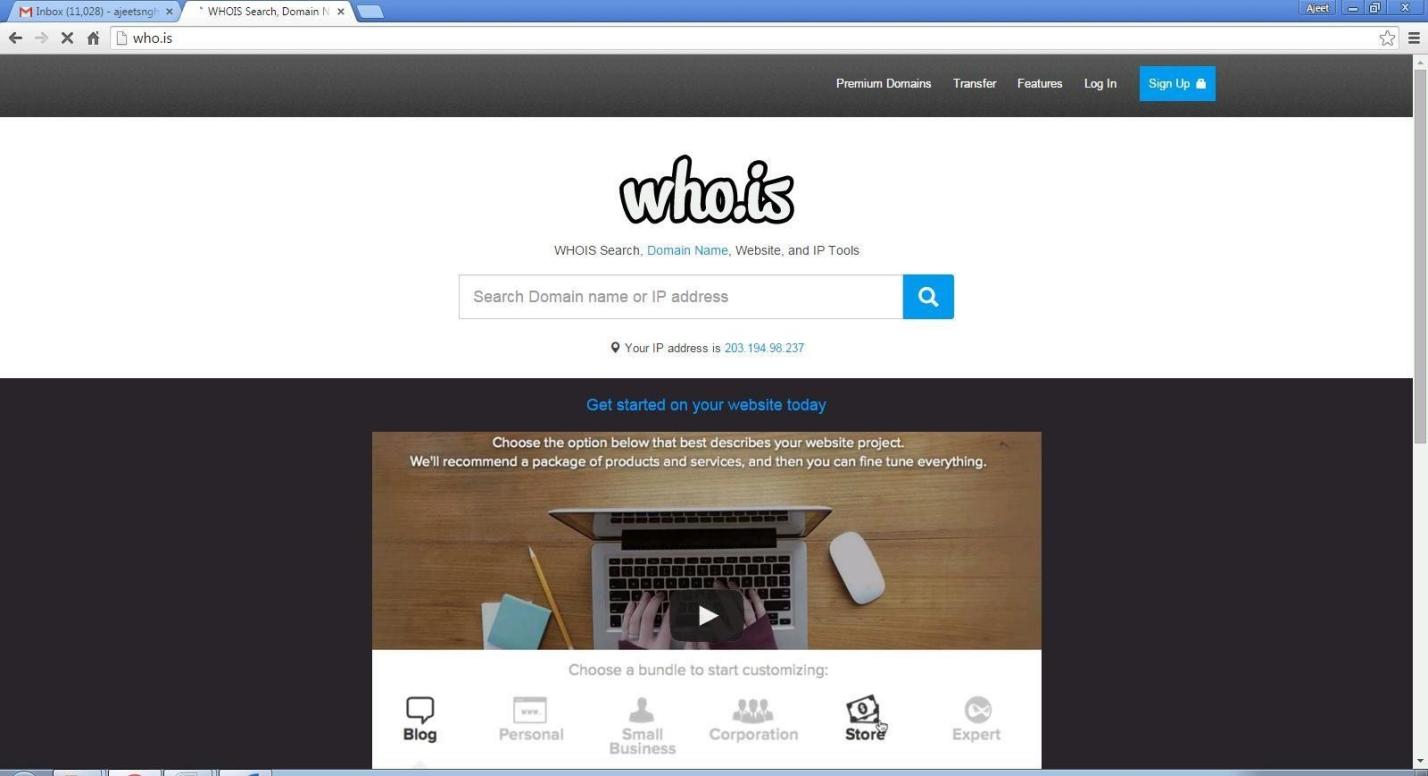


## PRACTICAL NO.3

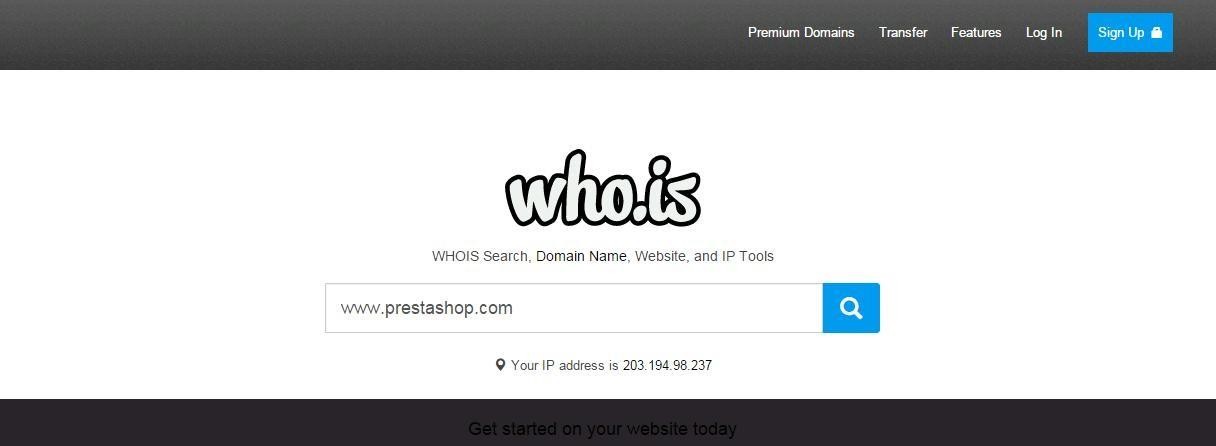
**AIM : Use Google and Whois for Reconnaisasance.**

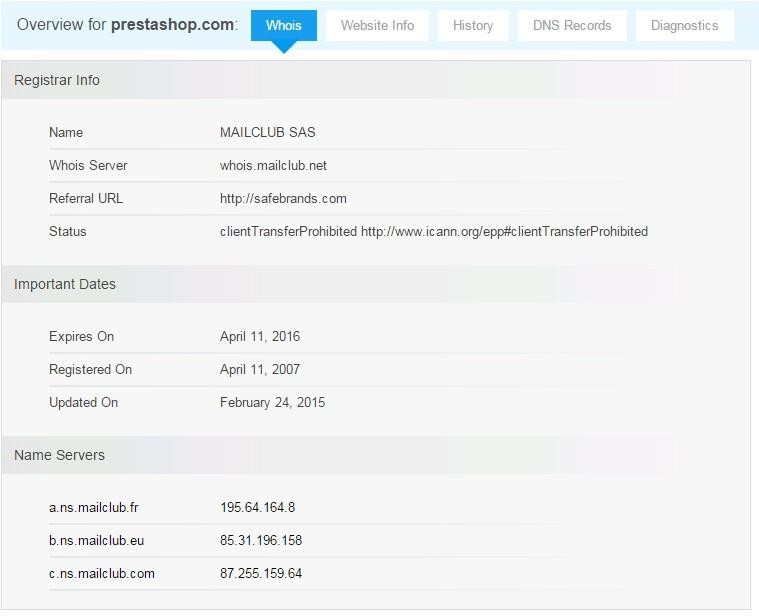
**Using who.is**

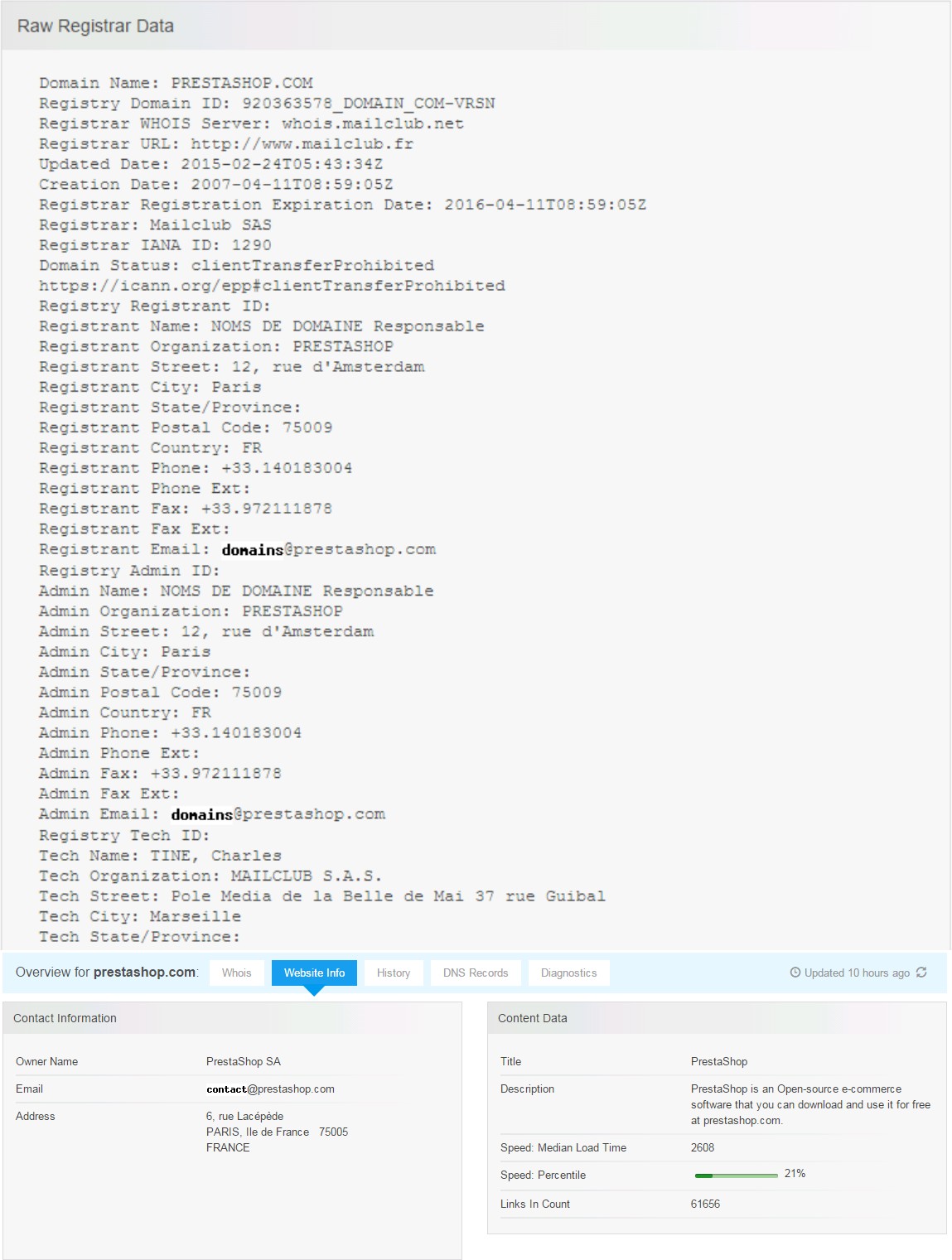
Step1: Open the WHO.is website

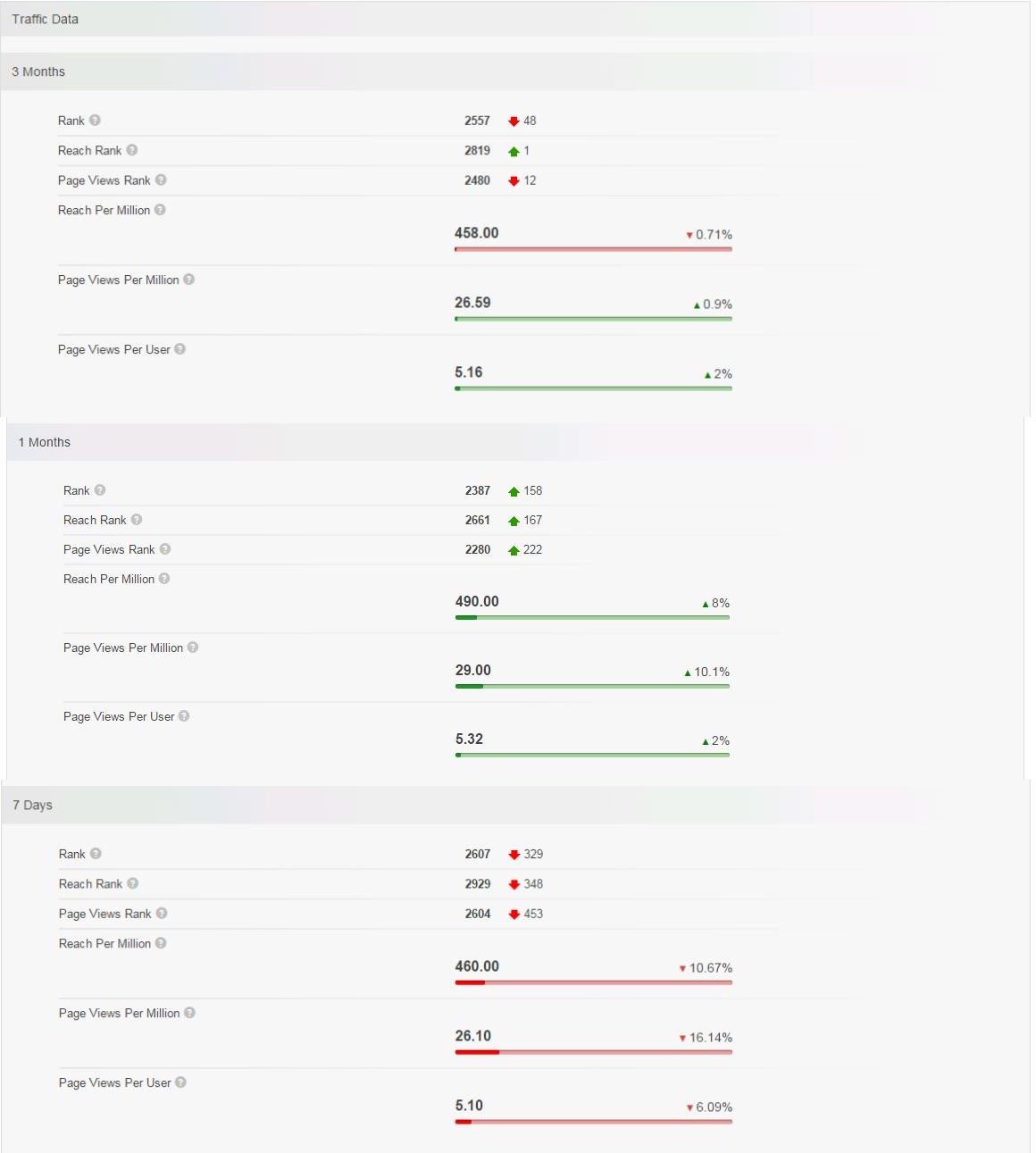


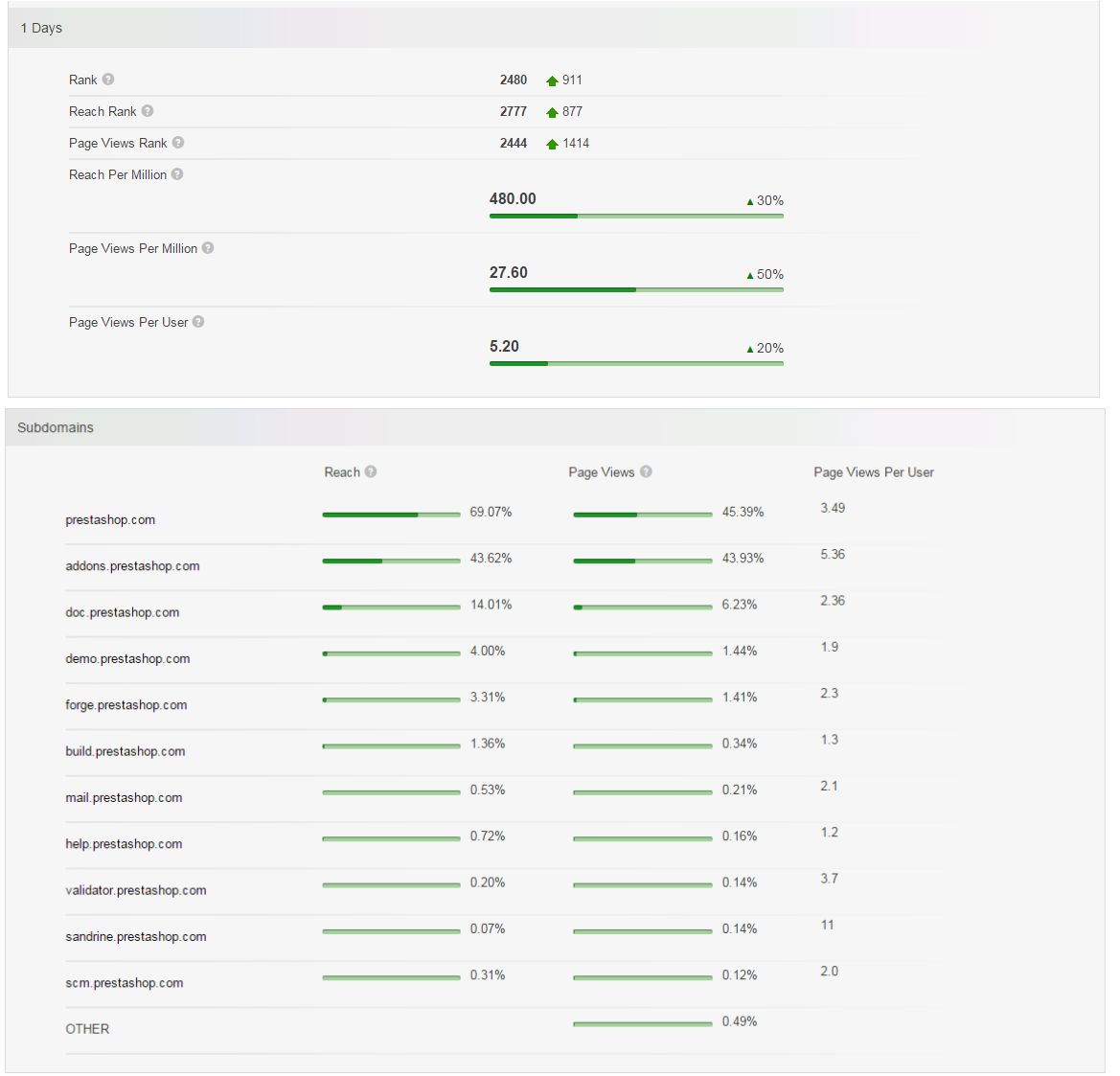
Step 2: Enter the website name and hit the “Enter button”.



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









**LEARNING OUTCOME:**

At the end of the session you will be able to

• familiarize with popular networking tool – “who.is”.

• understand how are we able to gather server information of any target website using this tool.

• learn some of the skills that you would require to become an expert in Ethical Hacking.

## PRACTICAL NO. 4

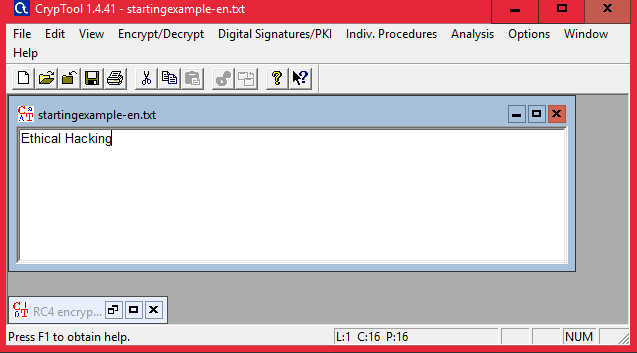
**AIM: Use "CrypTool" to encrypt and Decrypt Password using RC4 Algorithms...**

**THEORY:**

CrypTool is an open-source project that is a free e-learning software for illustrating cryptographic and cryptanalytic concepts. According to "Hakin9", CrypTool is worldwide the most widespread e-learning software in the field of cryptology.

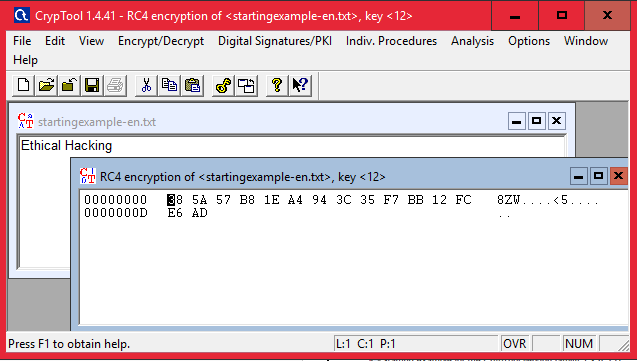
Use CryptTool to encrypt and decrypt passwords using RC4 algorithm.

Step 1:

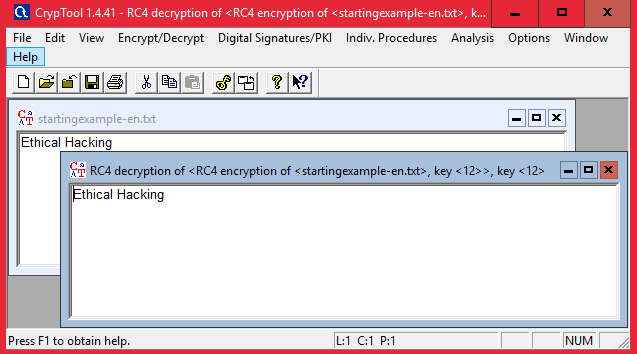


Step 2 : Using RC4.

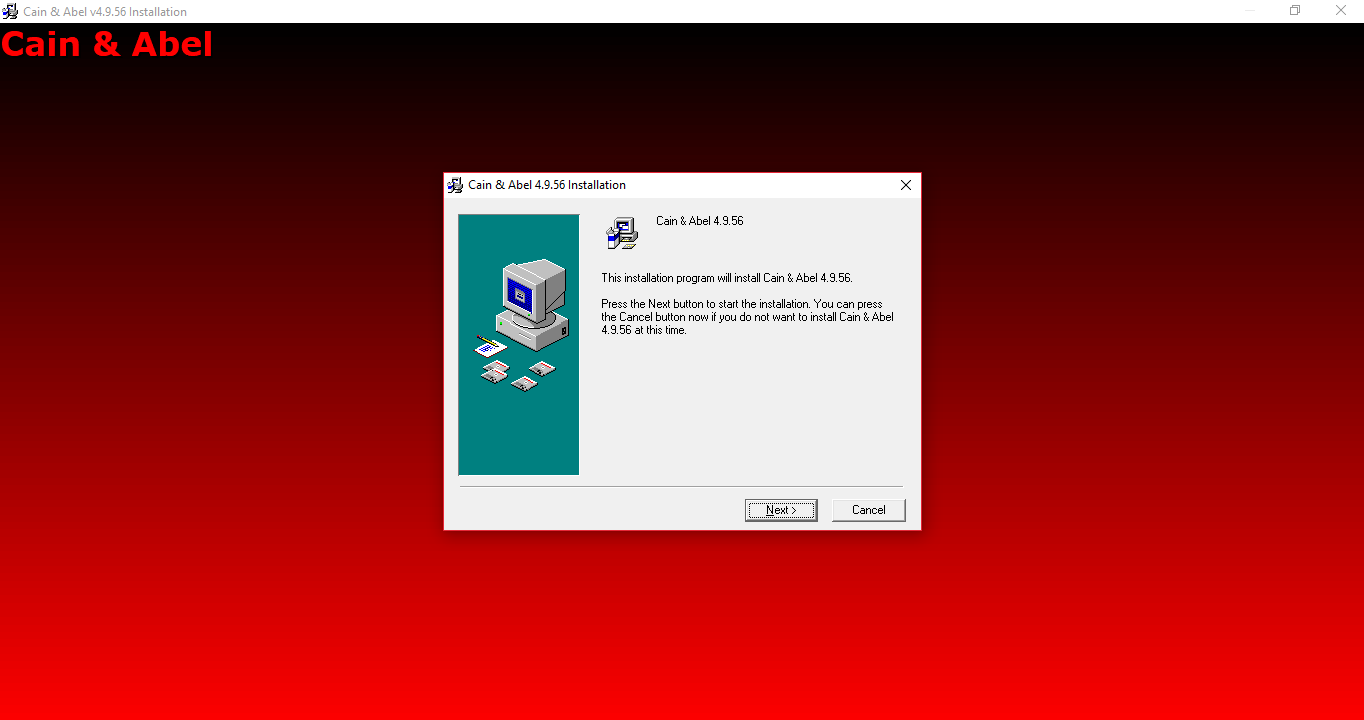
**Encryption using RC4**



**Decryption**

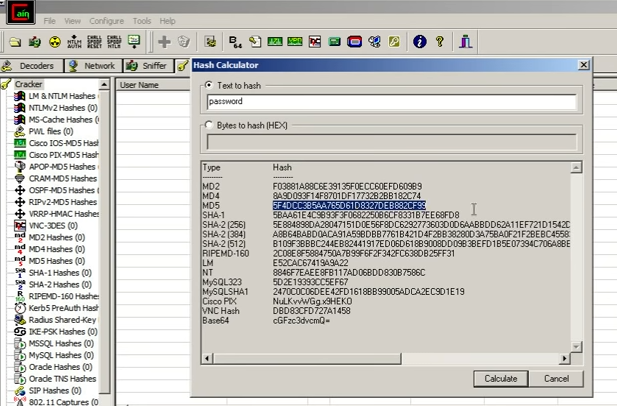


**2.2) Use Cain and Abel for cracking Windows account password using Dictionary attack and to decode wireless network passwords**

****

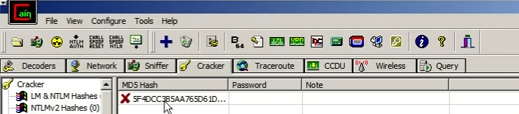
Click on HASH Calcuator

Enter the password to convert into hash



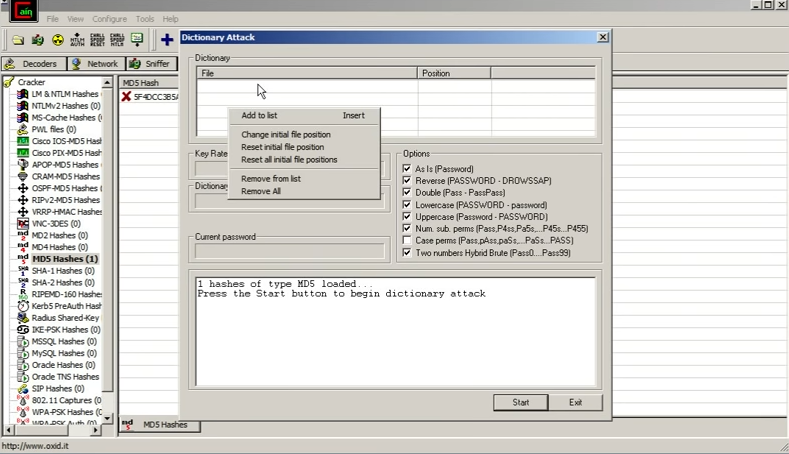
Paste the value into the field you have converted

e.g(MD5)

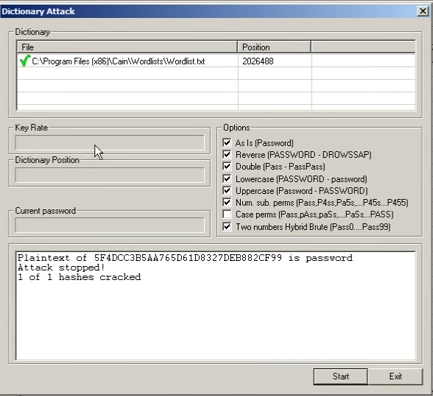


Right Click on the hash and select the dictionary attack

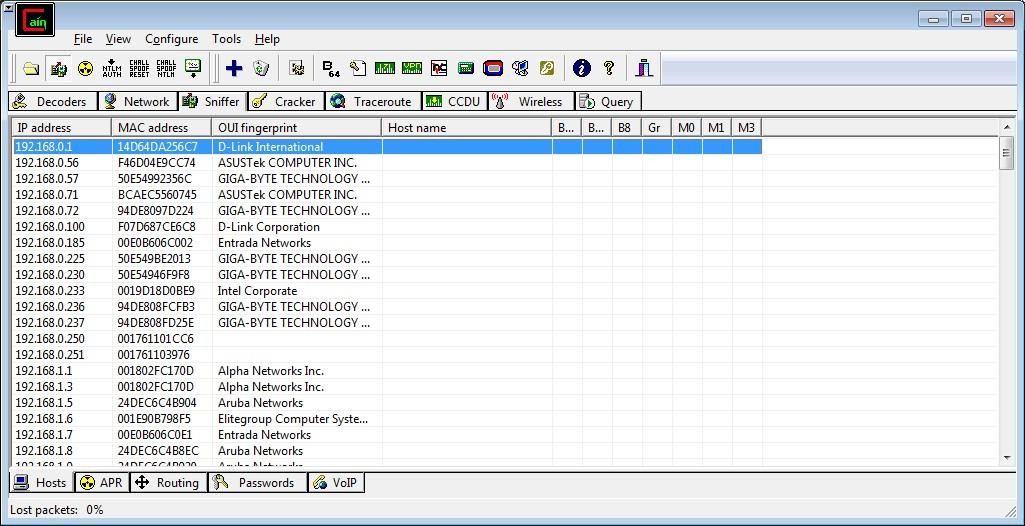
Then right click on the file and select (Add to List) and then select the Wordlist



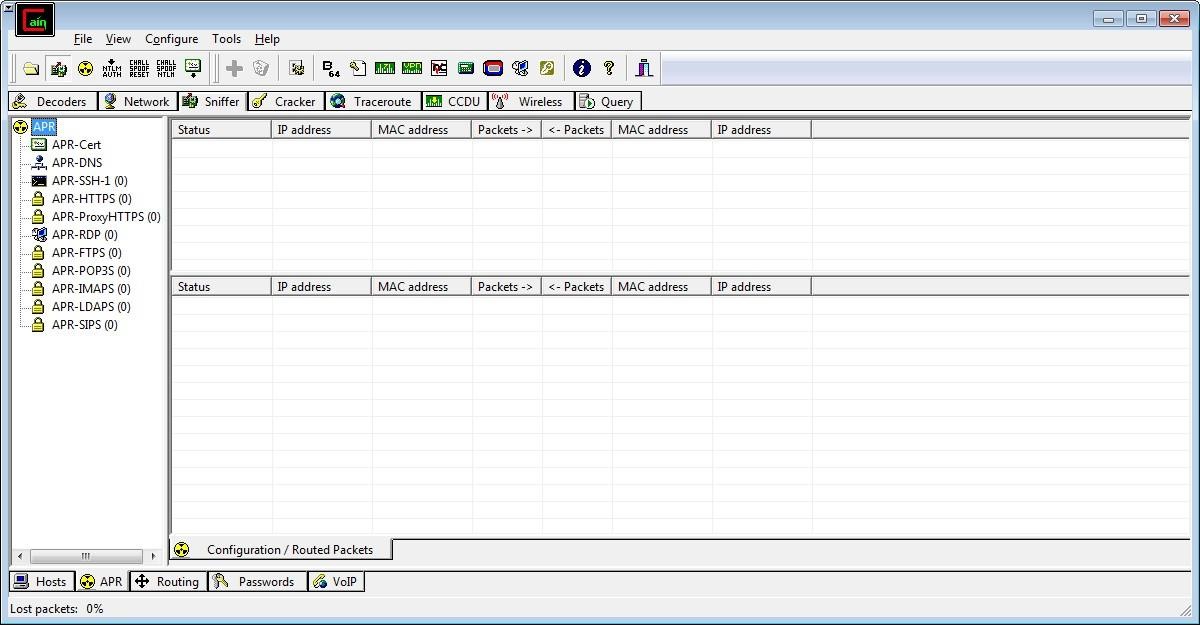
Select all the options and start the dictionary attack



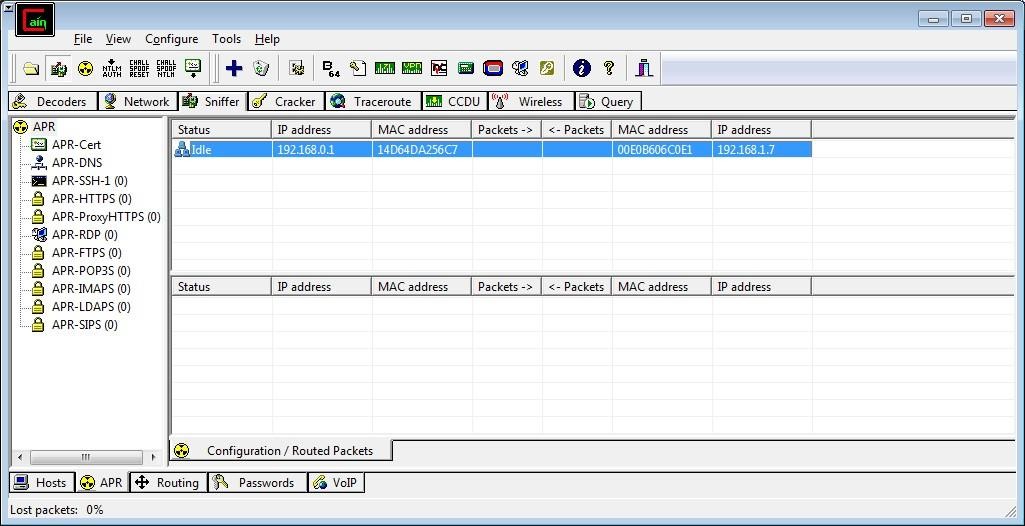
Step 5 : Shows the Connected host.



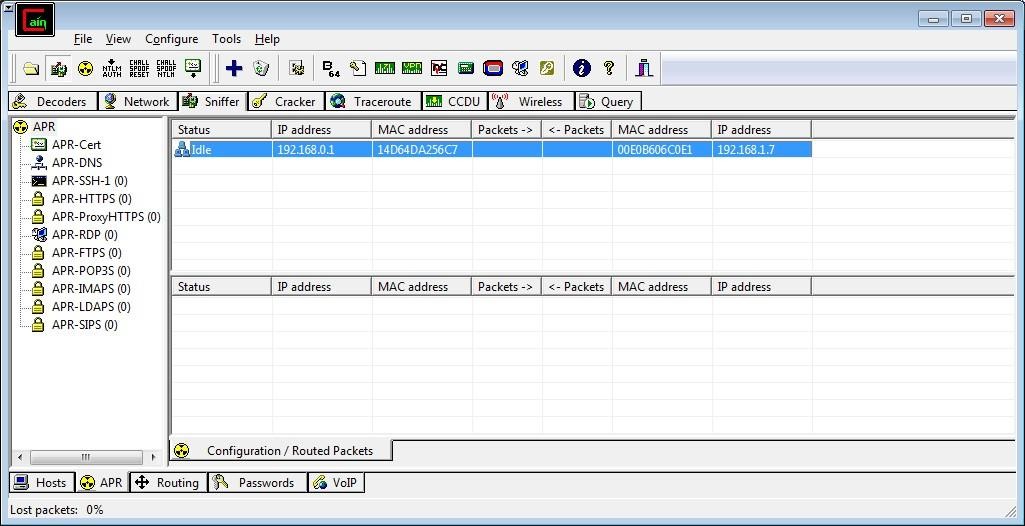
Step 6 : Select Arp at bottom.



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



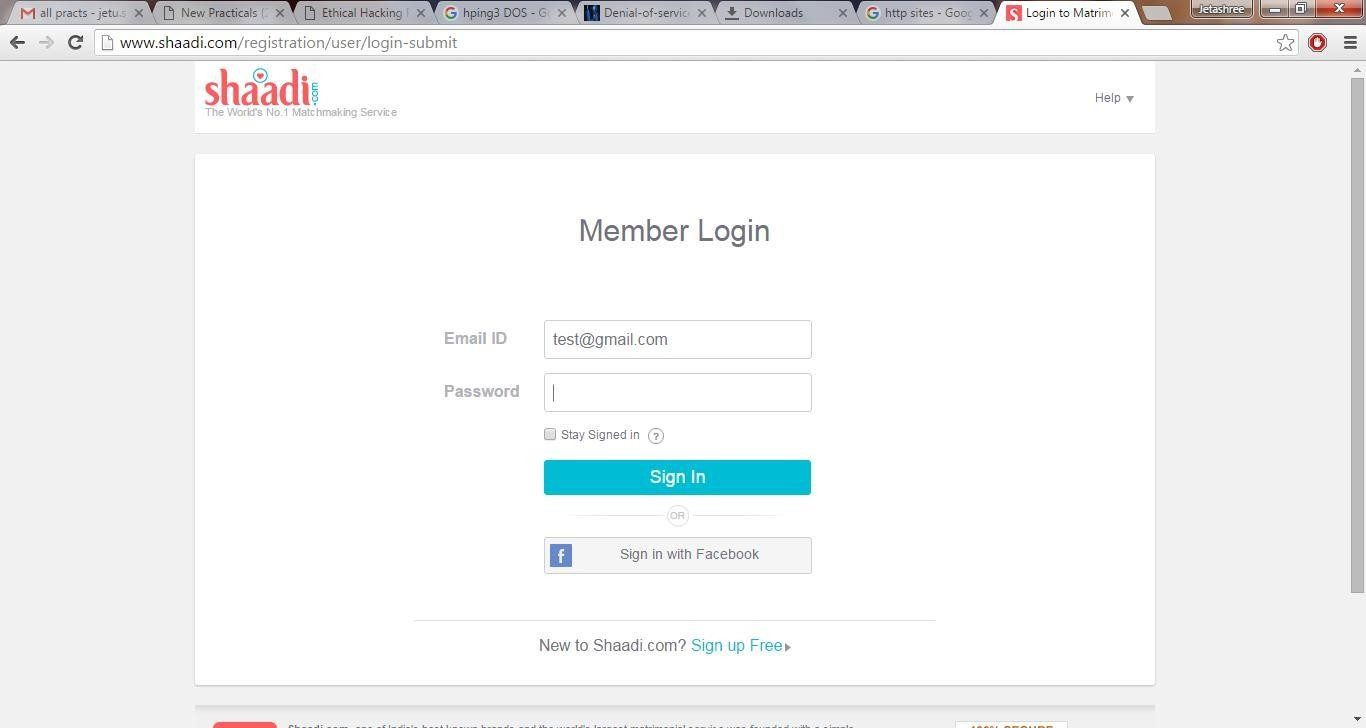
Step 8 : Click on start/stop ARP icon on top.



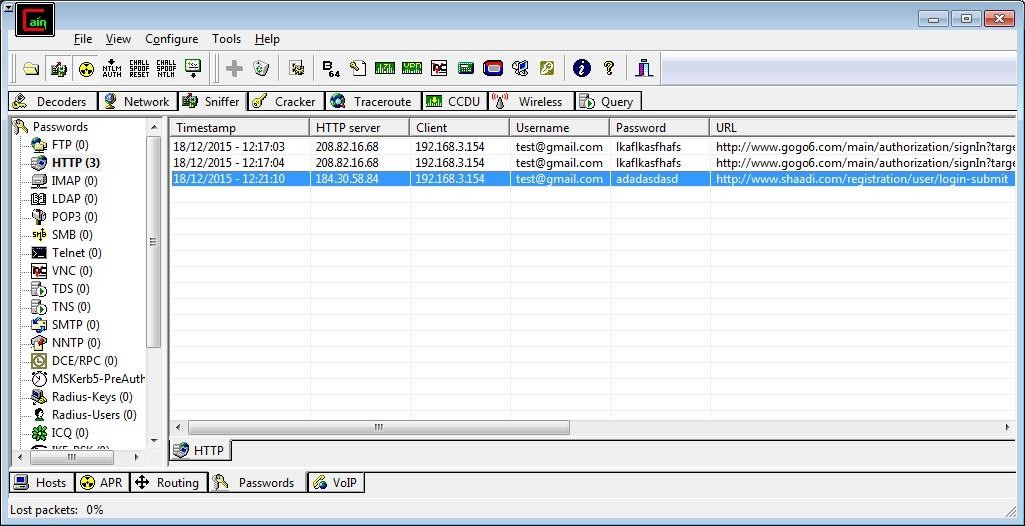
Step 9 : Poisoning the source.



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.



**LEARNING OUTCOME:**

At the end of the session you will be able to

• familiarize with popular “Cryptography” tool-“Cryptool”.

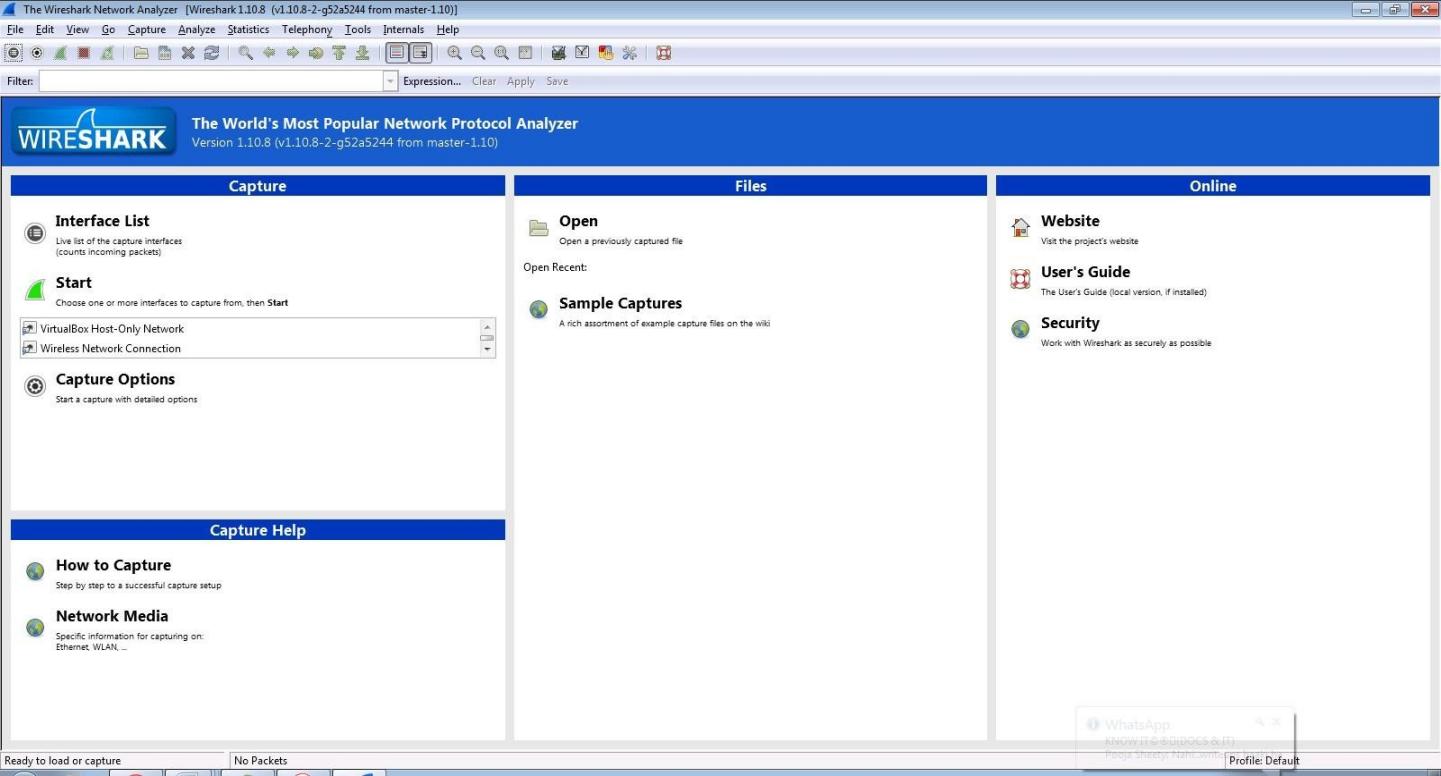
• understand how we are able to encrypt a password or a passphrase using the “RC4” Algo.

• learn some of the skills that you would require to become an expert in Ethical Hacking.

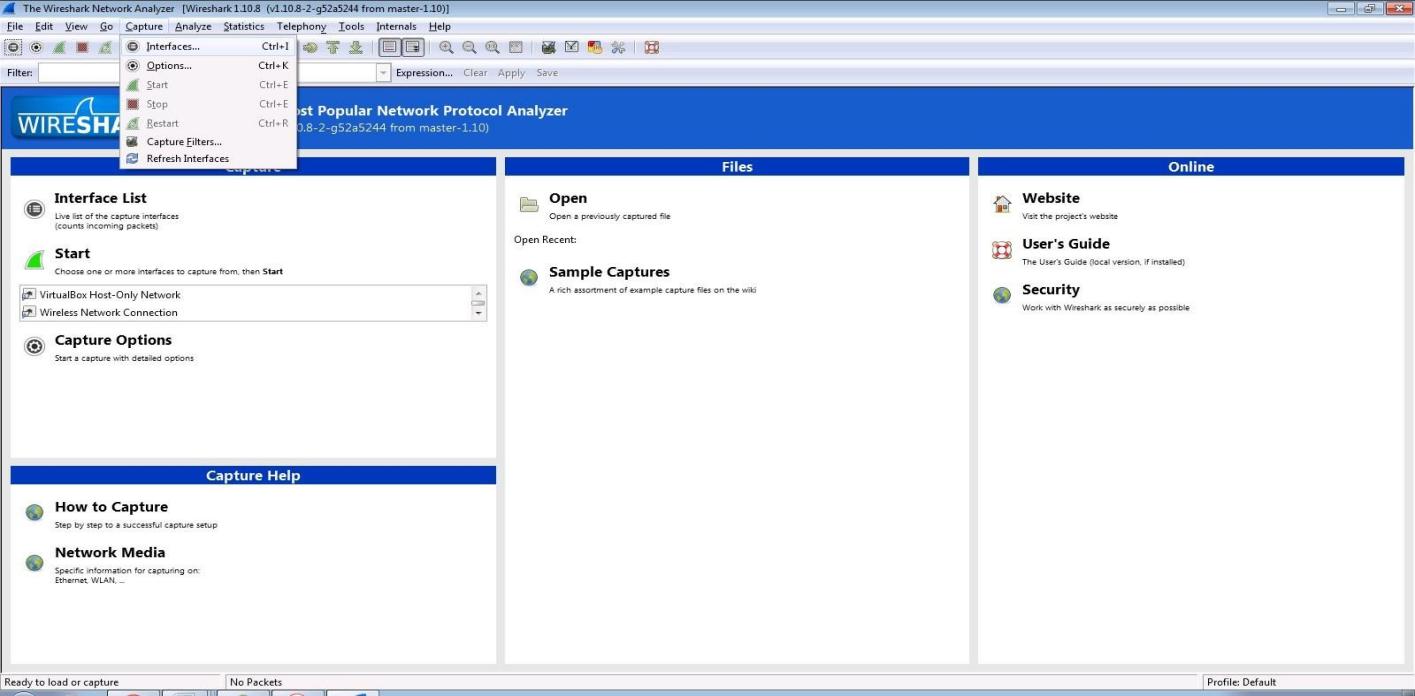
**PRACTCAL NO. 5**

## 5.1) Use WireShark sniffer to capture network traffic and analyze.

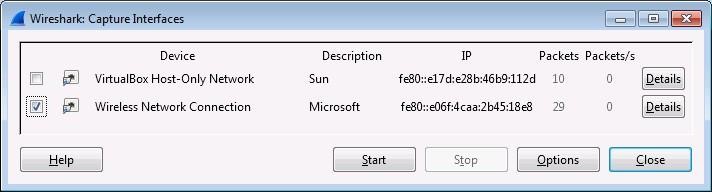
Step 1: Install and open WireShark .



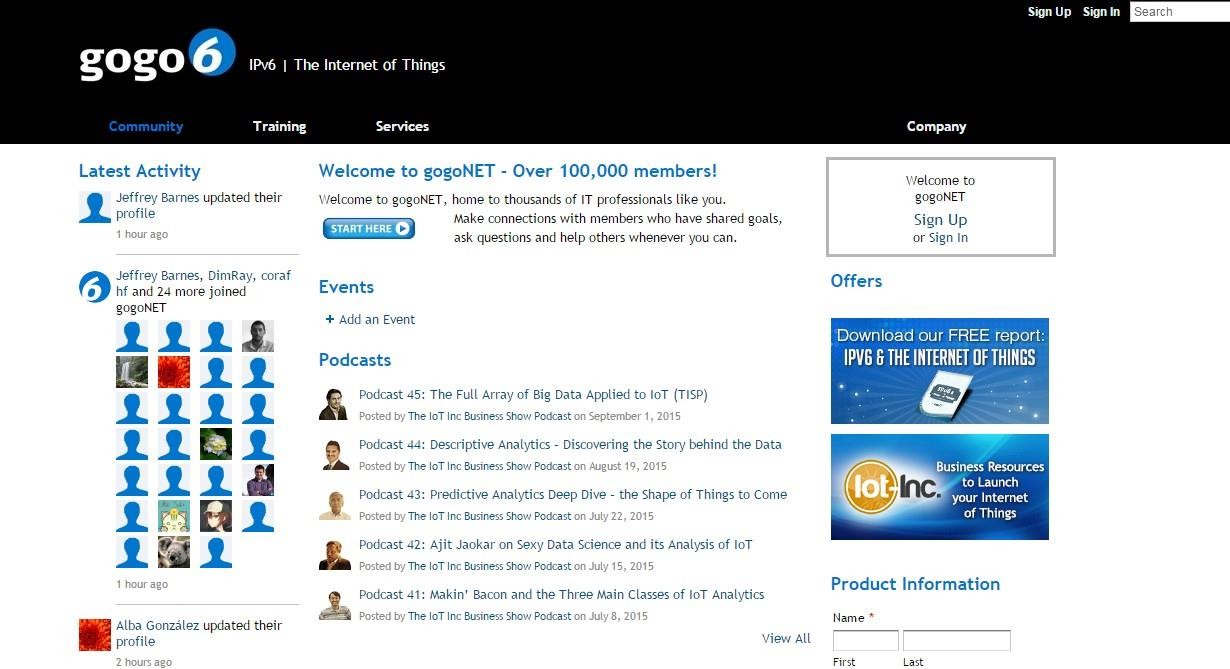
Step 2: Go to Capture tab and select Interface option.

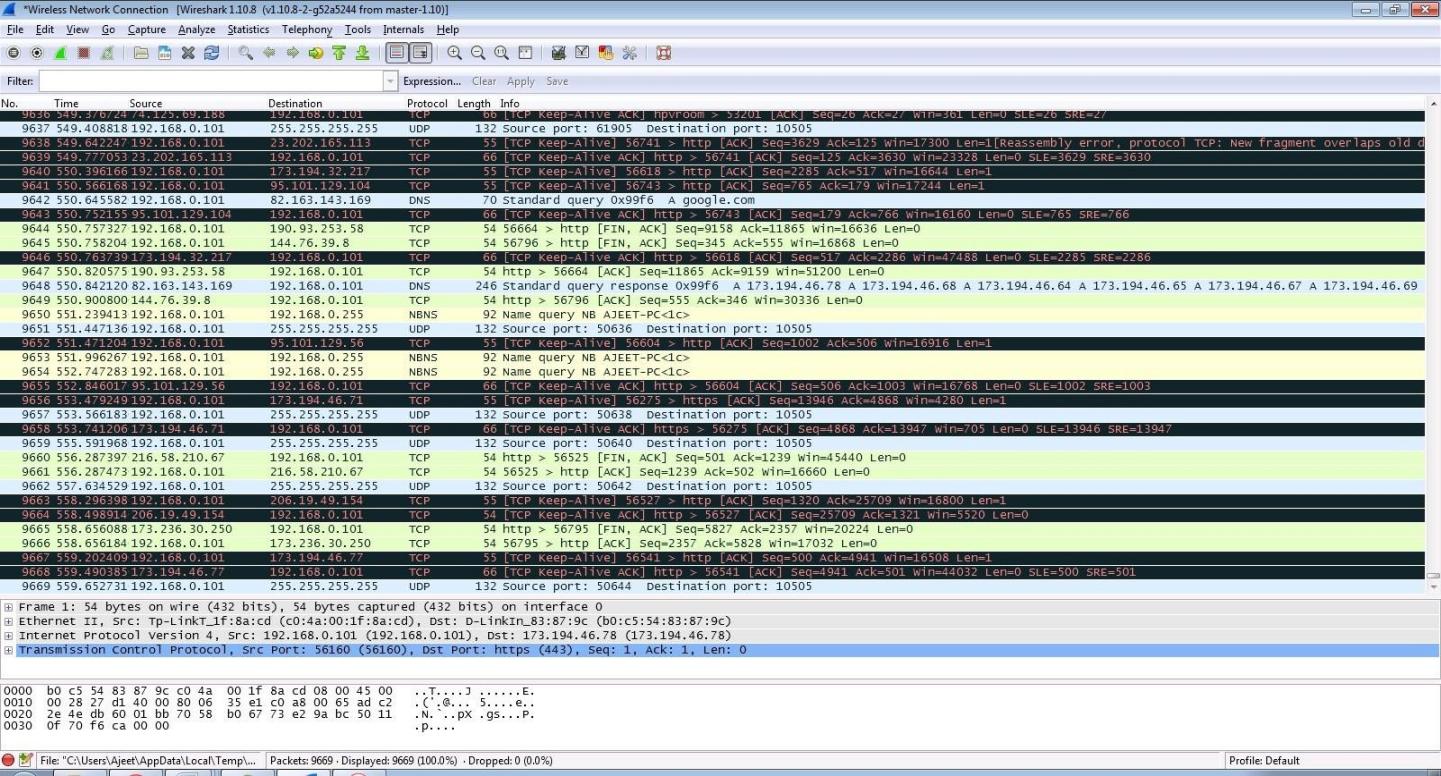


Step 3: In Capture interface, Select Local Area Connection and click on start.



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

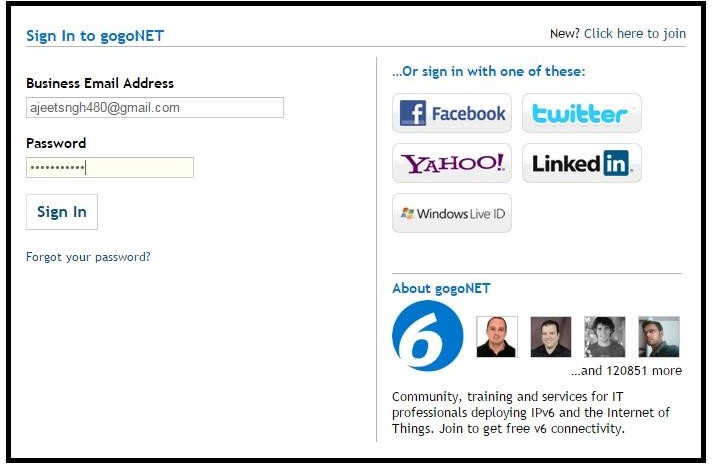




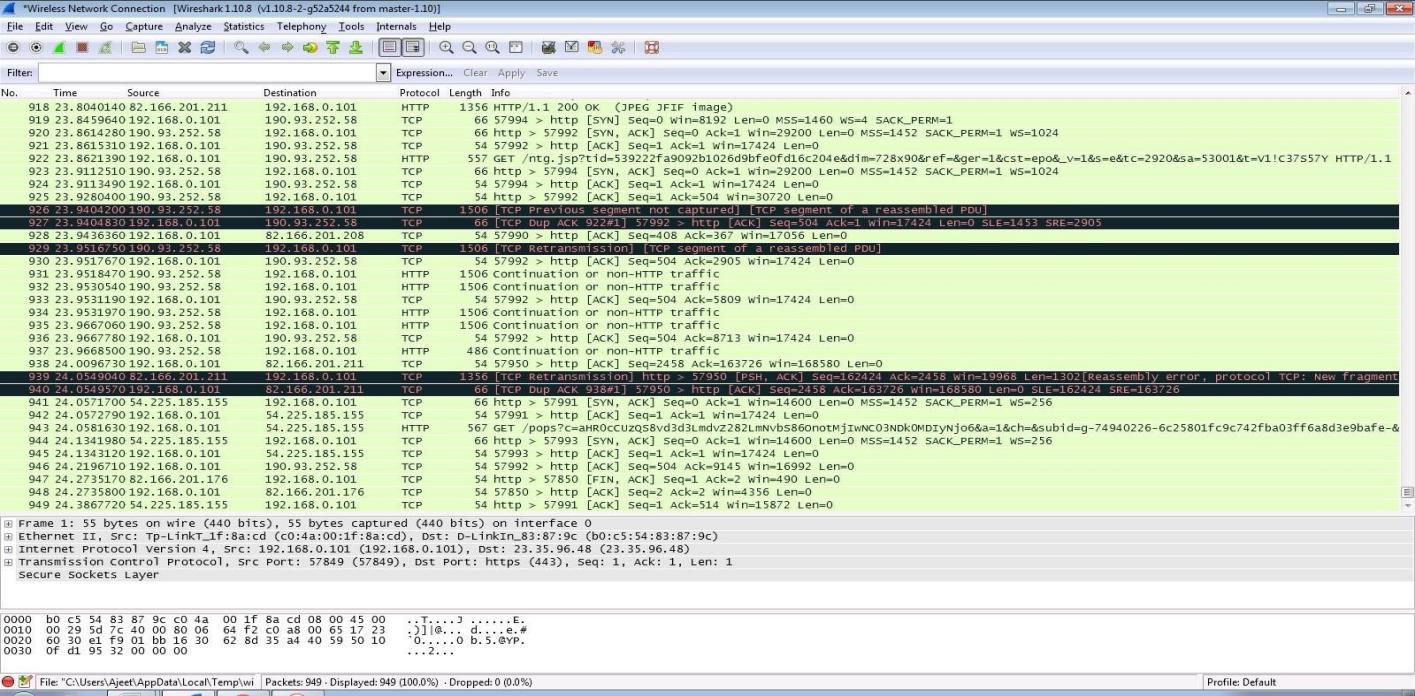
Step 5: Open a website in a new window and enter the user id and password. Register if needed.



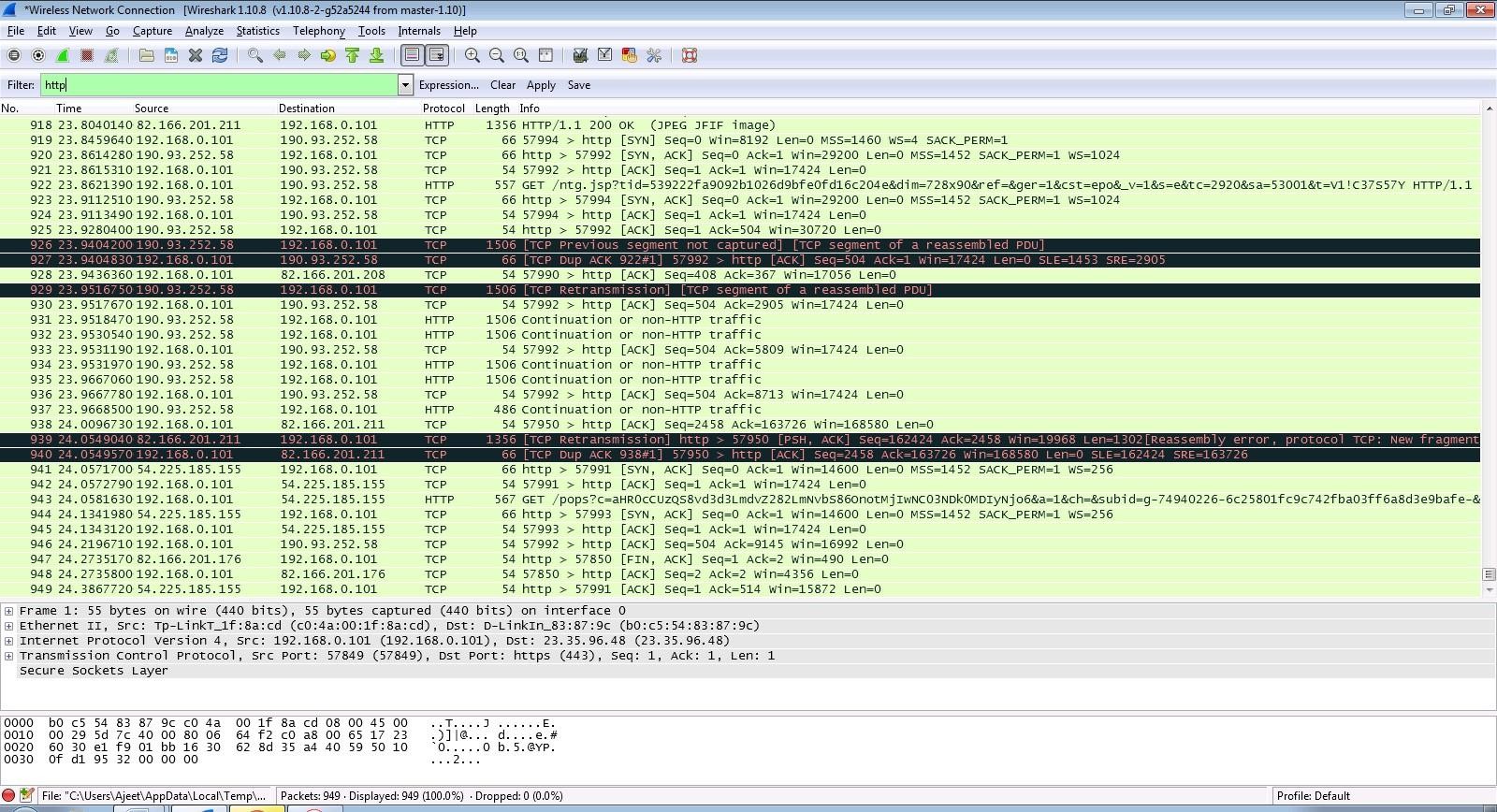
Step 6: Enter the credentials and then sign in.



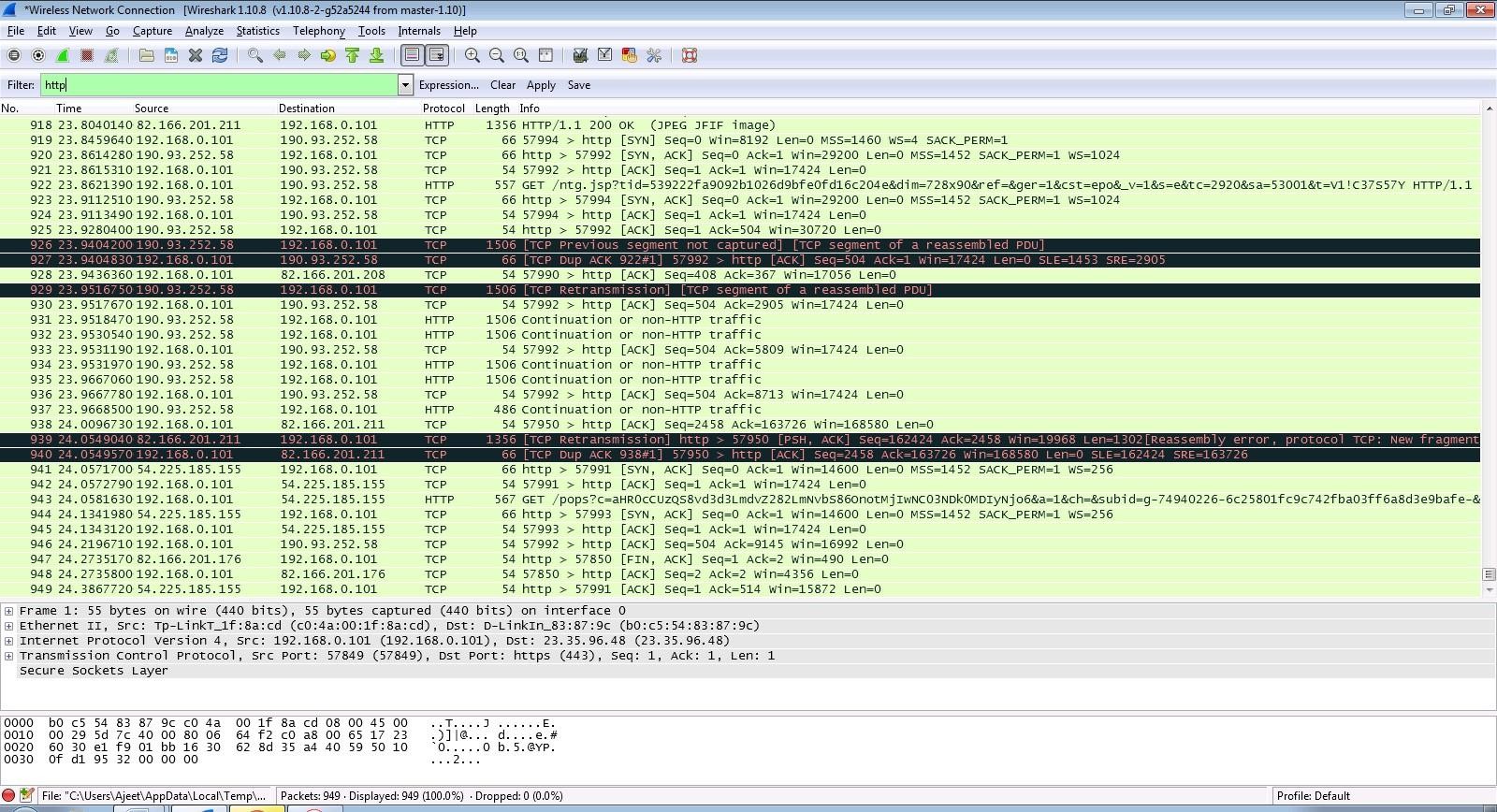
Step 7: The wireshark tool will keep recording the packets.



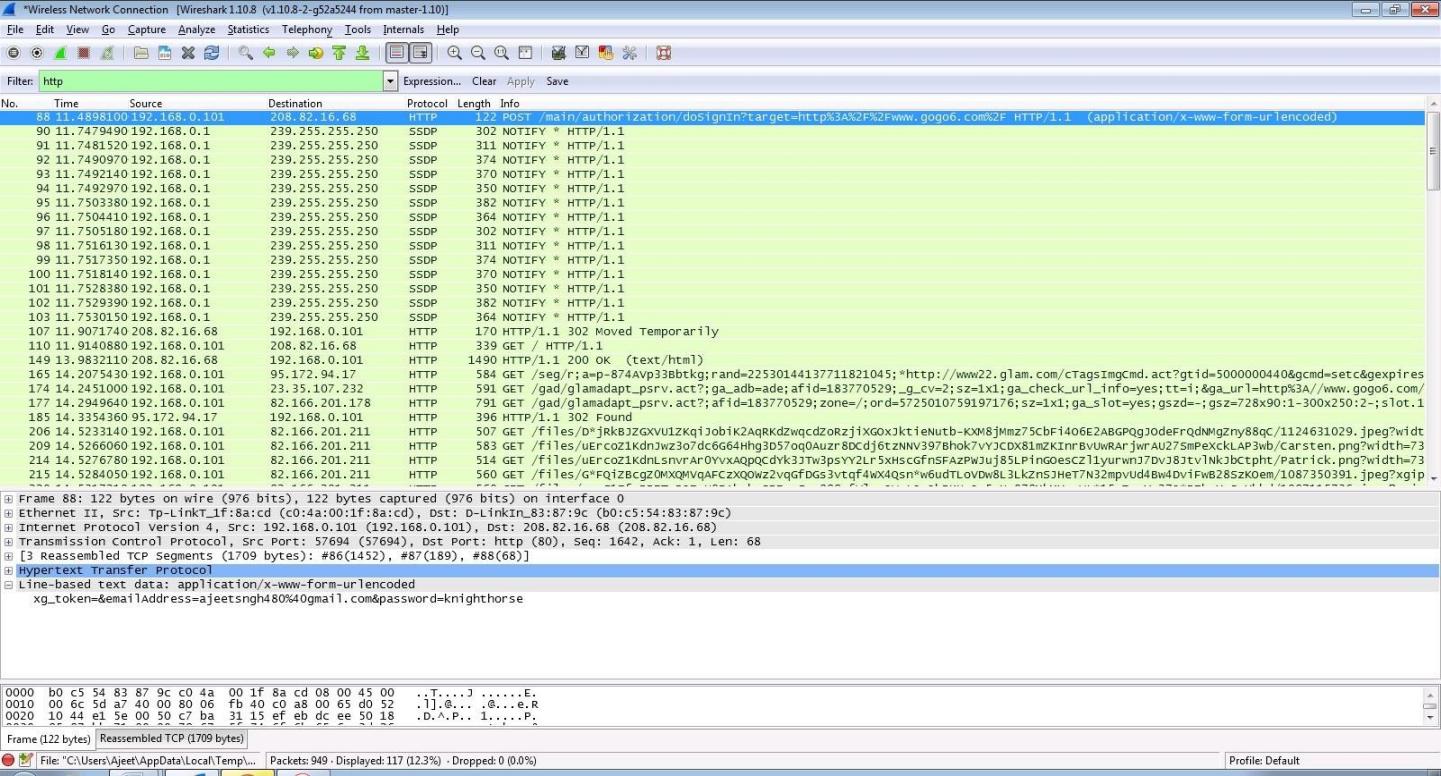
Step 8: Select filter as http to make the search easier and click on apply.



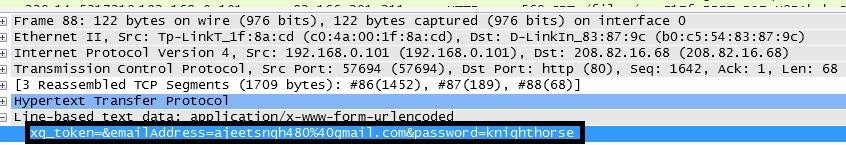
Step 9: Now stop the tool to stop recording.



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.



**LEARNING OUTCOME:**

At the end of the session you will be able to

• familiarize with popular hacking tool- “Wireshark”.

• Understand how we are able to find the username and pass word from a unsecured site using “wireshark”.

• learn some of the skills that you would require to become an expert in Ethical Hacking.

# PRACTICAL NO. 6

## AIM: To Learn & study about Sniffing & their tools.

**Learning Objective :**

At the end of the practical you will be able to • gain access to a genuine network connection of another user

**Introduction**

Sniffing is the process of monitoring and capturing all the packets passing through a given network using sniffing tools. It is a form of “tapping phone wires” and get to know about the conversation. It is also called wiretapping applied to the computer networks.

There is so much possibility that if a set of enterprise switch ports is open, then one of their employees can sniff the whole traffic of the network. Anyone in the same physical location can plug into the network using Ethernet cable or connect wirelessly to that network and sniff the total traffic.

In other words, Sniffing allows you to see all sorts of traffic, both protected and unprotected. In the right conditions and with the right protocols in place, an attacking party may be able to gather information that can be used for further attacks or to cause other issues for the network or system owner.

**What can be sniffed?**

One can sniff the following sensitive information from a network:

• Email traffic

• FTP passwords

• Web traffics

• Telnet passwords

• Router configuration

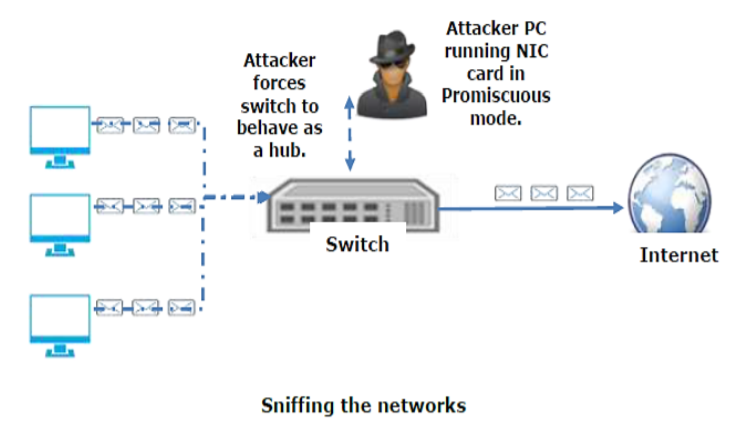
• Chat sessions

• DNS traffic

**How it works?**

A sniffer normally turns the NIC of the system to the promiscuous mode so that it listens to all the data transmitted on its segment.

Promiscuous mode refers to the unique way of Ethernet hardware, in particular, network interface cards (NICs), that allows an NIC to receive all traffic on the network, even if it is not addressed to this NIC. By default, a NIC ignores all traffic that is not addressed to it, which is done by comparing the destination address of the Ethernet packet with the hardware address (a.k.a. MAC) of the device. While this makes perfect sense for networking, non-promiscuous mode makes it difficult to use network monitoring and analysis software for diagnosing connectivity issues or traffic accounting



A sniffer can continuously monitor all the traffic to a computer through the NIC by decoding the information encapsulated in the data packets.

**Types of Sniffing**

**Passive Sniffing**

In passive sniffing, the traffic is locked but it is not altered in any way. Passive sniffing allows listening only. It works with Hub devices. On a hub device, the traffic is sent to all the ports. In a network that uses hubs to connect systems, all hosts on the network can see the traffic. Therefore, an attacker can easily capture traffic going through.

The good news is that hubs are almost obsolete nowadays. Most modern networks use switches. Hence, passive sniffing is no more effective.

**Active Sniffing**

In active sniffing, the traffic is not only locked and monitored, but it may also be altered in some way as determined by the attack. Active sniffing is used to sniff a switch-based network. It involves injecting address resolution packets (ARP) into a target network to flood on the switch content addressable memory (CAM) table. CAM keeps track of which host is connected to which port.

Following are the Active Sniffing Techniques:

• MAC Flooding

• DHCP Attacks

• DNS Poisoning

• Spoofing Attacks

• ARP Poisoning

**Protocols which are affected**

Protocols such as the tried and true TCP/IP were never designed with security in mind and therefore do not offer much resistance to potential intruders. Several rules lend themselves to easy sniffing:

• **HTTP**: It is used to send information in the clear text without any encryption and thus a real target. • **SMTP** (Simple Mail Transfer Protocol): SMTP is basically utilized in the transfer of emails. This protocol is efficient, but it does not include any protection against sniffing.

• **NNTP** (Network News Transfer Protocol): It is used for all types of communications, but its main drawback is that data and even passwords are sent over the network as clear text.

• **POP** (Post Office Protocol): POP is strictly used to receive emails from the servers. This protocol does not include protection against sniffing because it can be trapped.

• **FTP** (File Transfer Protocol): FTP is used to send and receive files, but it does not offer any security features. All the data is sent as clear text that can be easily sniffed.

• **IMAP** (Internet Message Access Protocol): IMAP is same as SMTP in its functions, but it is highly vulnerable to sniffing.

• **Telnet**: Telnet sends everything (usernames, passwords, keystrokes) over the network as clear text and hence, it can be easily sniffed. Sniffers are not the dumb utilities that allow you to view only live traffic. If you really want to analyze each packet, save the capture and review it whenever time allows.

**Sniffing Tools**

There are so many tools available to perform sniffing over a network, and they all have their own features to help a hacker analyze traffic and dissect the information. Sniffing tools are extremely common applications. We have listed here some of the interesting ones:

• **BetterCAP**:BetterCAP is a powerful, flexible and portable tool created to perform various types of MITM attacks against a network, manipulate HTTP, HTTPS and TCP traffic in real-time, sniff for credentials, and much more.

• **Ettercap**: Ettercap is a comprehensive suite for man-in-the-middle attacks. It features sniffing of live connections, content filtering on the fly and many other interesting tricks. It supports active and passive dissection of many protocols and includes many features for network and host analysis.

• **Wireshark**: It is one of the most widely known and used packet sniffers. It offers a tremendous number of features designed to assist in the dissection and analysis of traffic.

• **Tcpdump**: It is a well-known command-line packet analyzer. It provides the ability to intercept and observe TCP/IP and other packets during transmission over the network. Available at www.tcpdump.org.

• **WinDump**: A Windows port of the popular Linux packet sniffer tcpdump, which is a command-line tool that is perfect for displaying header information.

• **OmniPeek**: Manufactured by WildPackets, OmniPeek is a commercial product that is the evolution of the product EtherPeek.

• **Dsniff**: A suite of tools designed to perform sniffing with different protocols with the intent of intercepting and revealing passwords. Dsniff is designed for Unix and Linux platforms and does not have a full equivalent on the Windows platform.

• **EtherApe**: It is a Linux/Unix tool designed to display graphically a system's incoming and outgoing connections.

• **MSN Sniffer**: It is a sniffing utility specifically designed for sniffing traffic generated by the MSN Messenger application.

# PRACTICAL NO. 7

**AIM: -** **Create a simple keylogger using python**

**THEORY:**

Keyloggers are a type of monitoring software designed to record keystrokes made by a user. One of the oldest forms of cyber threat, these keystroke loggers record the information you type into a website or application and send to back to a third party

**How hackers use keyloggers**

Today spyware such as keystroke loggers are a common part of the cybercriminal toolset to capture financial information such as banking and credit card details, personal information such as emails and password or names and addresses, or sensitive business information around processes or

intellectual property. They may sell that information or use it as part of a larger attack depending on what was gathered and their motives.

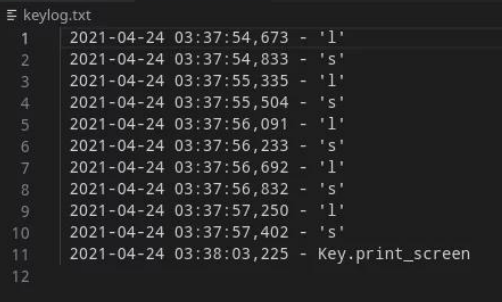
**How keyloggers infect devices**

Keyloggers can be placed on machines in a number of different ways. Physical loggers require a person to be physically present to be placed on a machine, meaning such attacks are harder (but not impossible) to achieve, and more likely to come from an insider threat. Wireless keyboards can also be snooped on remotely. Software-based keyloggers are far more common and have multiple routes for entry. Infected domains are a common attack method.

**Code:**



**Output: -**



**PRACTICAL NO. 8**

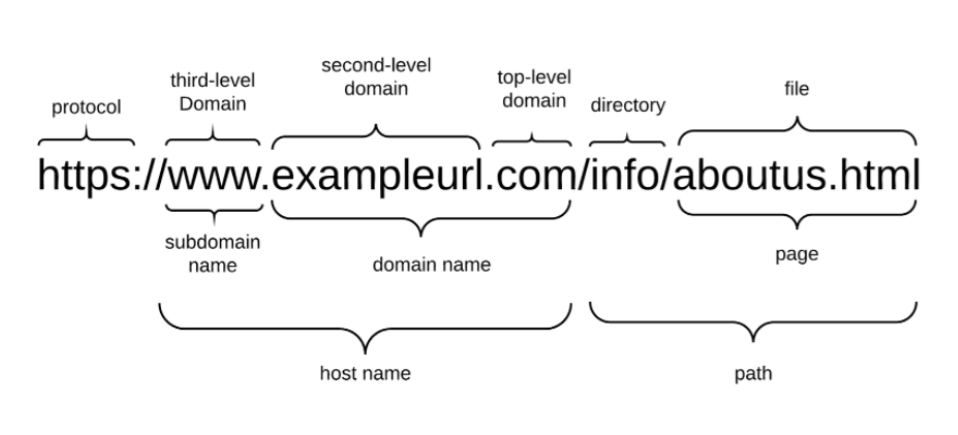
**AIM:** To learn about Phising URL detection.

**Introduction:** Phishing is a form of fraud in which the attacker tries to learn sensitive information such as login credentials or account information by sending as a reputable entity or person in email or other communication channels.

Many users unwittingly click phishing domains every day and every hour. The attackers are targeting both the users and the companies. According to the 3rd Microsoft Computing Safer Index Report, released in February 2014, the annual worldwide impact of phishing could be very high as $5 billion.

**Characteristics of Phishing Domains**

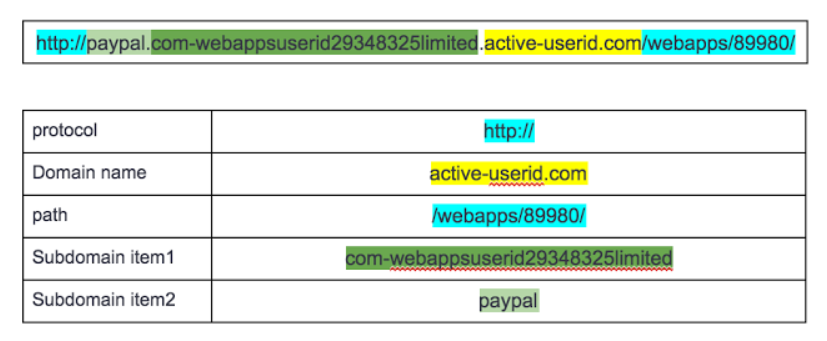
Lets check the URL structure for the clear understanding of how attackers think when they create a phishing domain. Uniform Resource Locator (URL) is created to address web pages. The figure below shows relevant parts in the structure of a typical URL.



* It begins with a protocol used to access the page. The fully qualified domain name identifies the server who hosts the web page.
* It consists of a registered domain name (second-level domain) and suffix which we refer to as top-level domain (TLD). The domain name portion is constrained since it has to be registered with a domain name Registrar.
* A Host name consists of a subdomain name and a domain name. An phisher has full control over the subdomain portions and can set any value to it.
* The URL may also have a path and file components which, too, can be changed by the phisher at will. The subdomain name and path are fully controllable by the phisher.

The attacker must intelligently choose the domain names because the aim should be convincing the users,and then setting the FreeURL to make detection difficult.

Lets analyse an example given below.



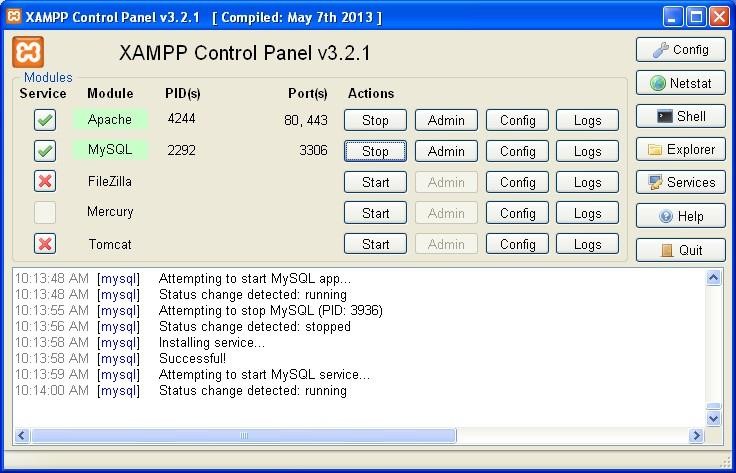
# **Detection Process**

* Detecting Phishing Domains is a classification problem, so it means we need labeled data which has samples as phish domains and legitimate domains in the training phase. The dataset which will be used in the training phase is a very important point to build successful detection mechanism.
* We have to use samples whose classes are precisely known. So it means, the samples which are labeled as phishing must be absolutely detected as phishing. Likewise the samples which are labeled as legitimate must be absolutely detected as legitimate. Otherwise, the system will not work correctly if we use samples that we are not sure about.
* For this purpose, some public datasets are created for phishing. Some of the well-known one is [PhishTank](https://www.phishtank.com/" \t "https://towardsdatascience.com/_blank).

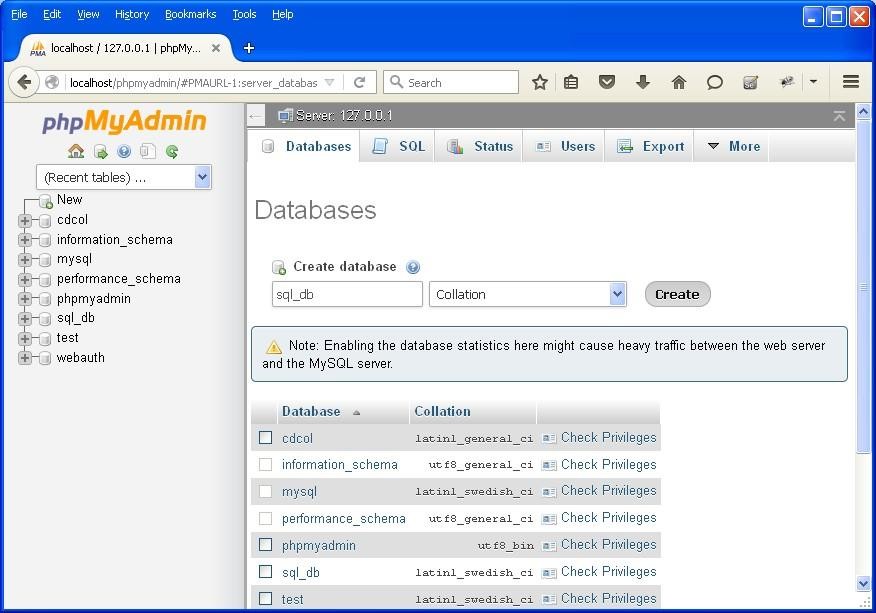
**PRACTICAL NO. 9**

## AIM: Perform SQL injection attack.

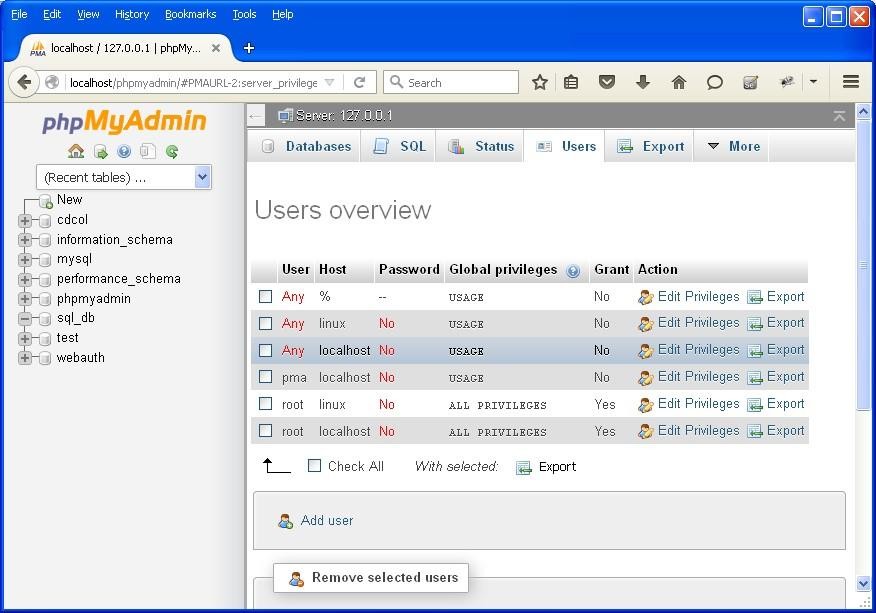
Step 1 : Open XAMPP and start apache and mysql.



Step 2 : Go to web browser and enter site localhost/phpmyadmin



Step 3 : Create database with name sql\_db.



Step 4 : Go to site localhost/sql\_injection/setup.php and click on create/reset database.



Step 5 : Go to login.php and login using admin and .



Step 6 : Opens the home page.

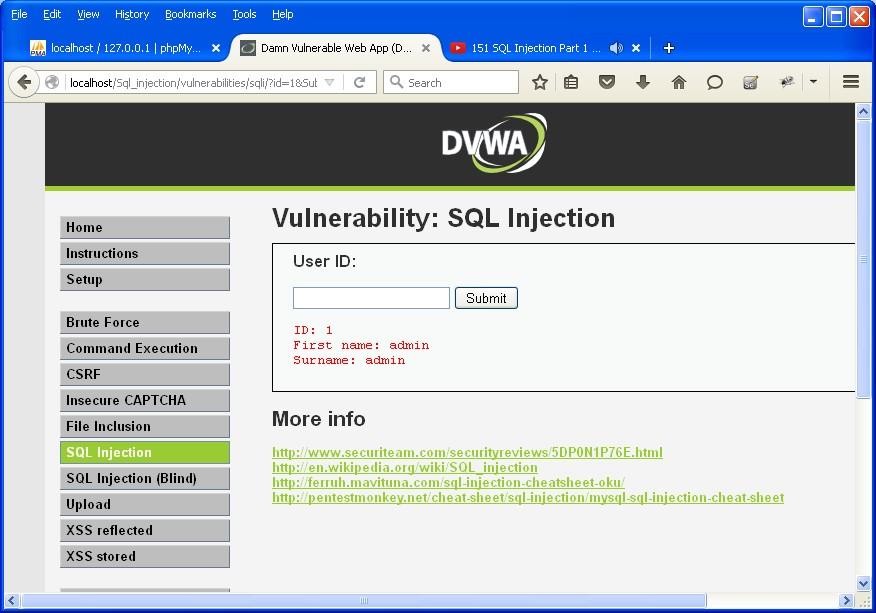


Step 7 : Go to security setting option in left and set security level low.

Step 8 : Click on SQL injection option in left.



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



Step 10 : Write "a' or ''='" in text box and click on submit.



Step 11 : Write "1=1" in text box and click on submit.



Step 12 : Write "1\*" in text box and click on submit.

# PRACTICAL NO. 10

**AIM: Using Metasploit to exploit**

**Steps:**

**Download and open metasploit**

**Use exploit to attack the host**

**Create the exploit and add the exploit to the victim’s PC**

# 