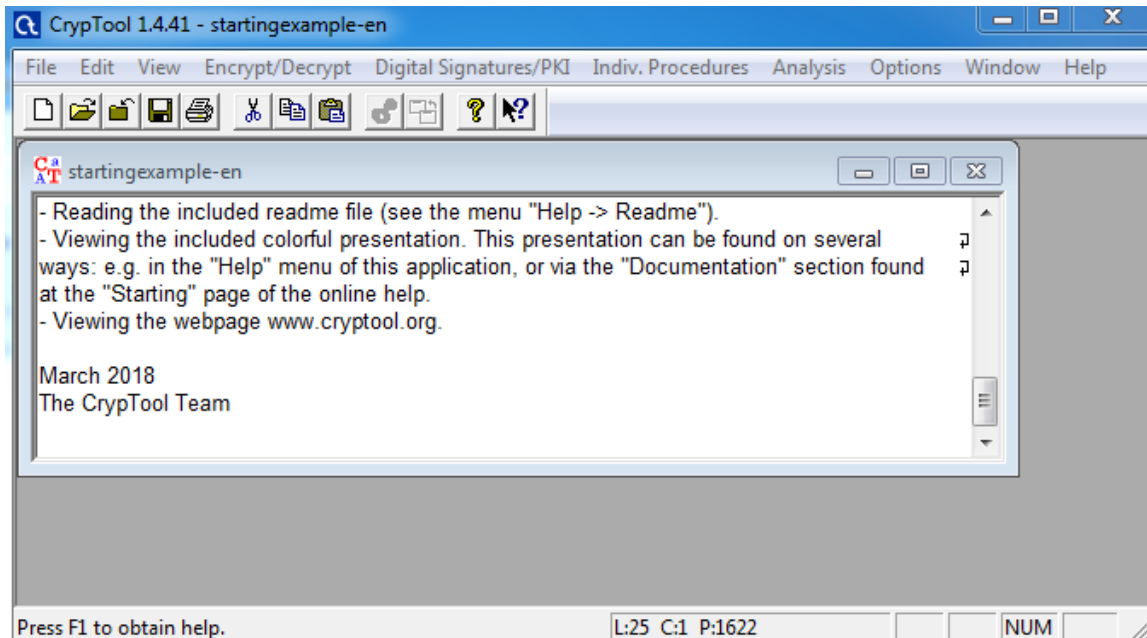
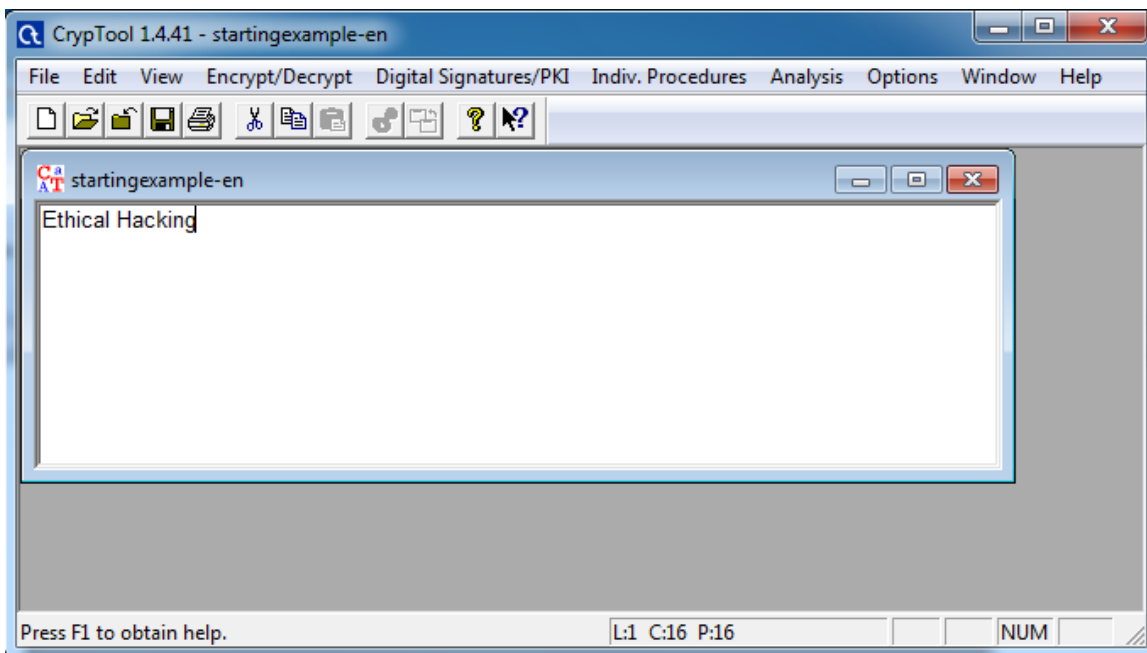


Practical 2

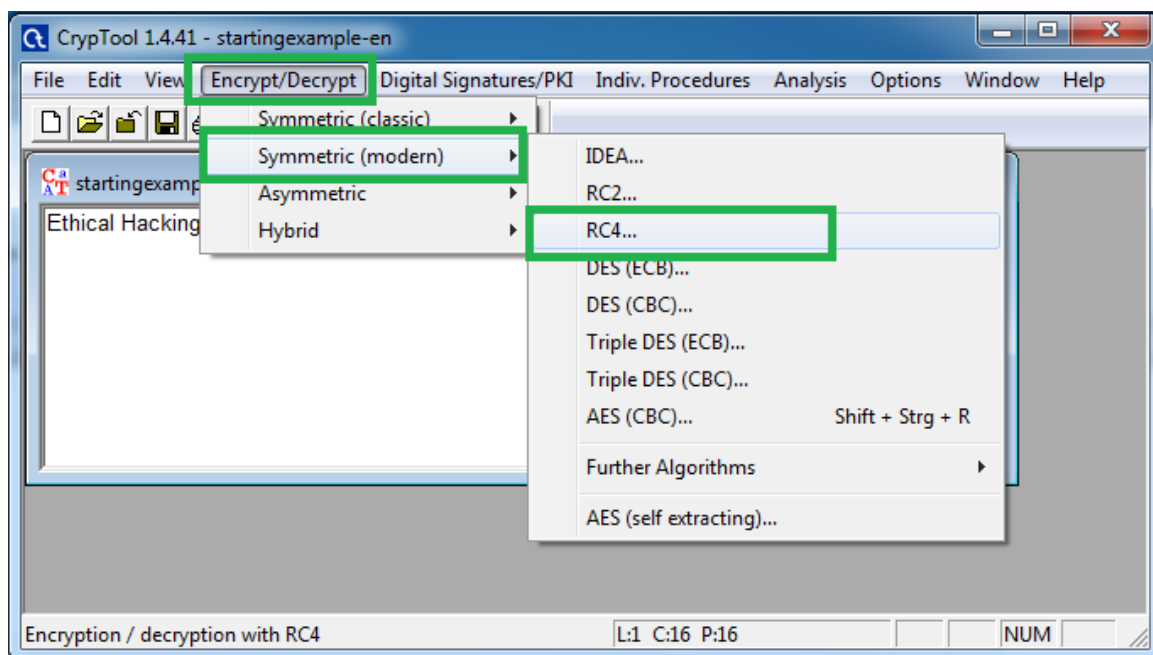
2.1 - Use cryptTool to encrypt and decrypt passwords using RC4 algorithm



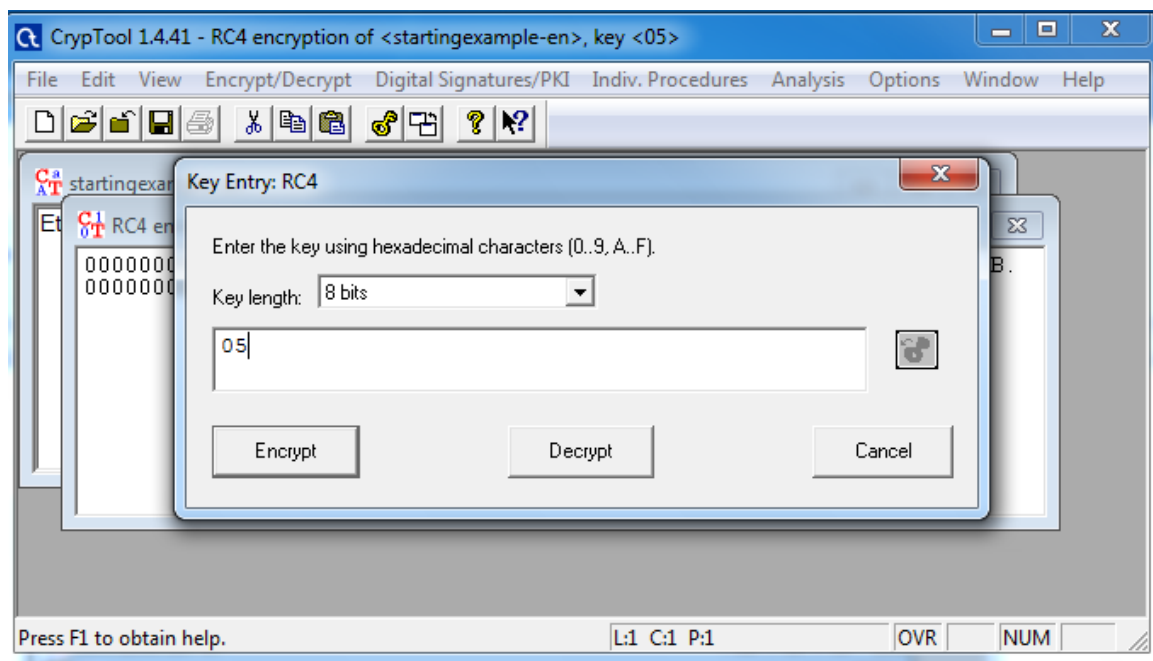
then type the password required



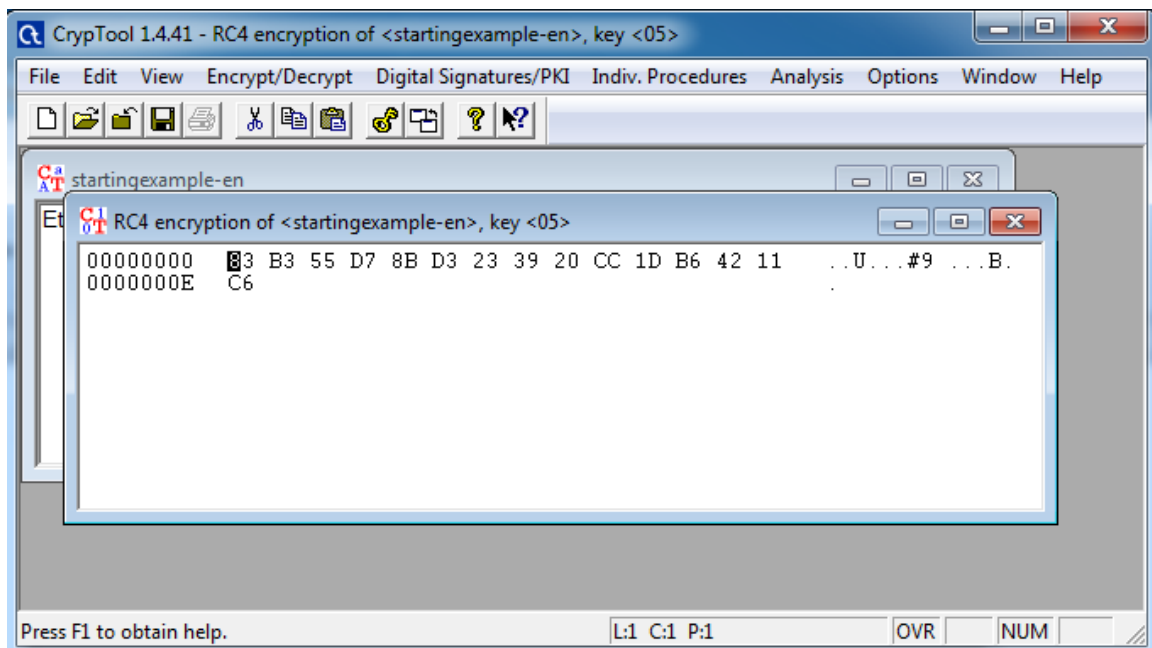
then select the RC4 algorithm



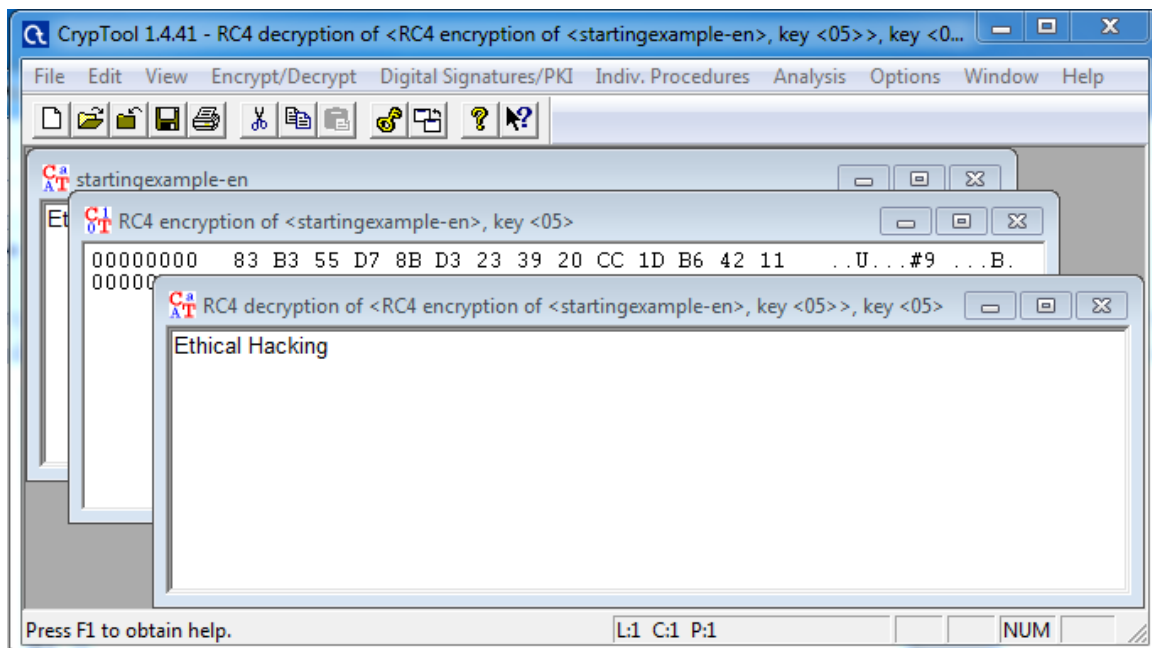
then give the encryption value



here we see the encryption

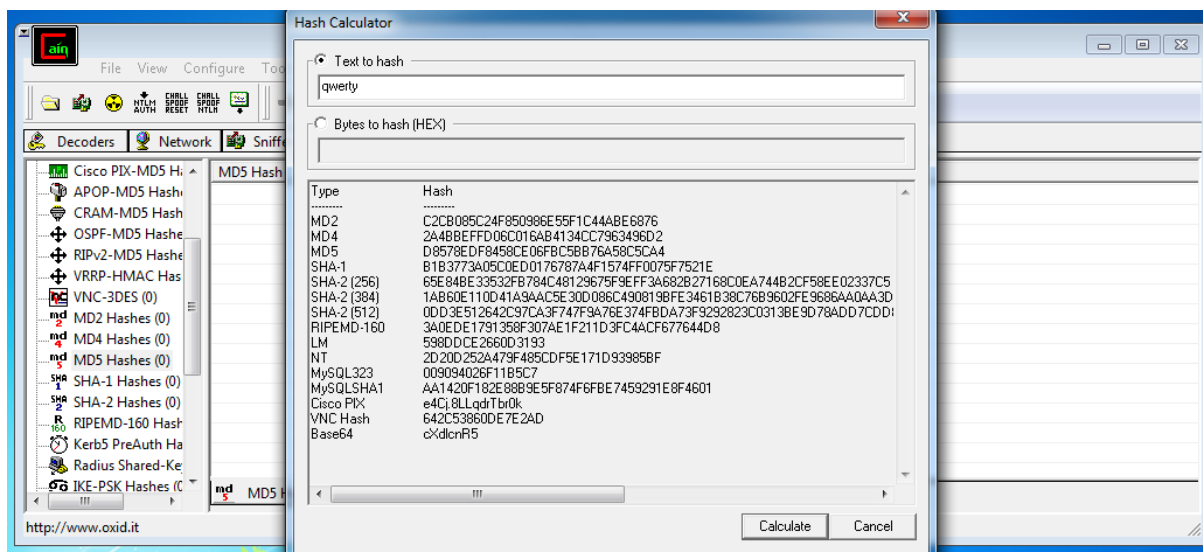
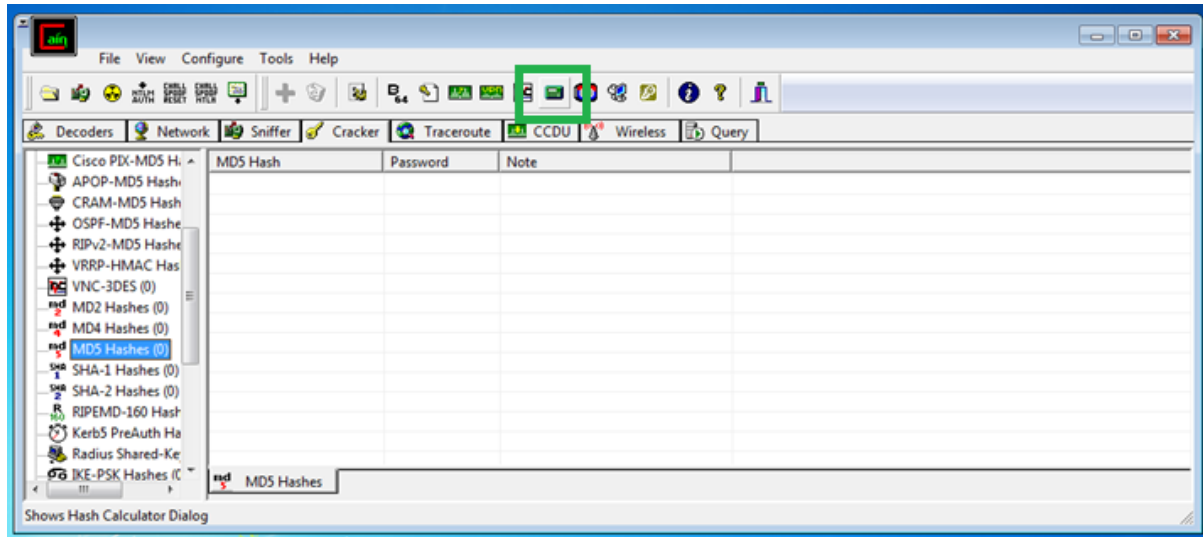


now we see the decryption do the same but instead of encrypt do decrypt

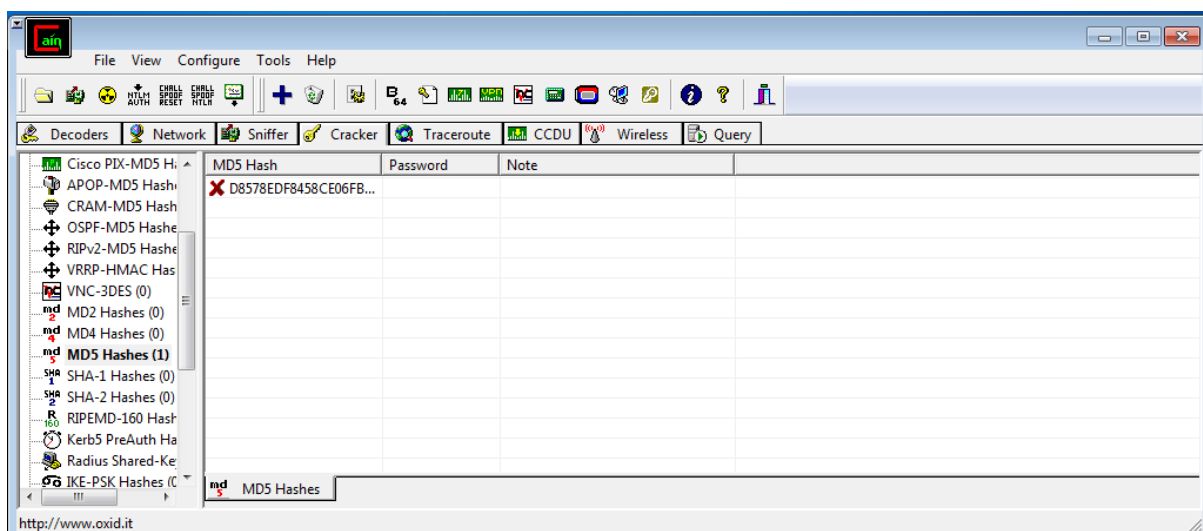
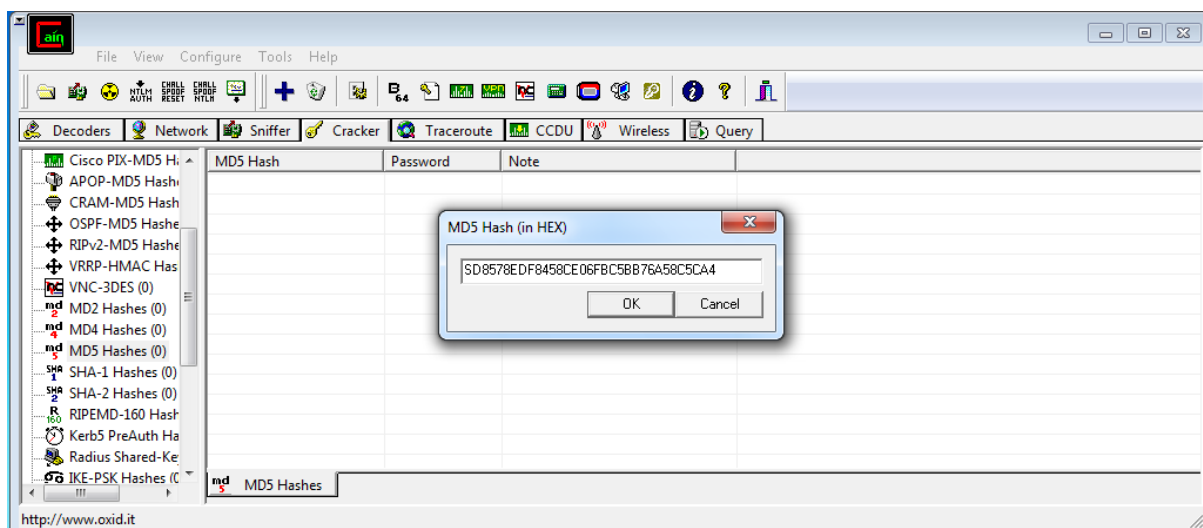
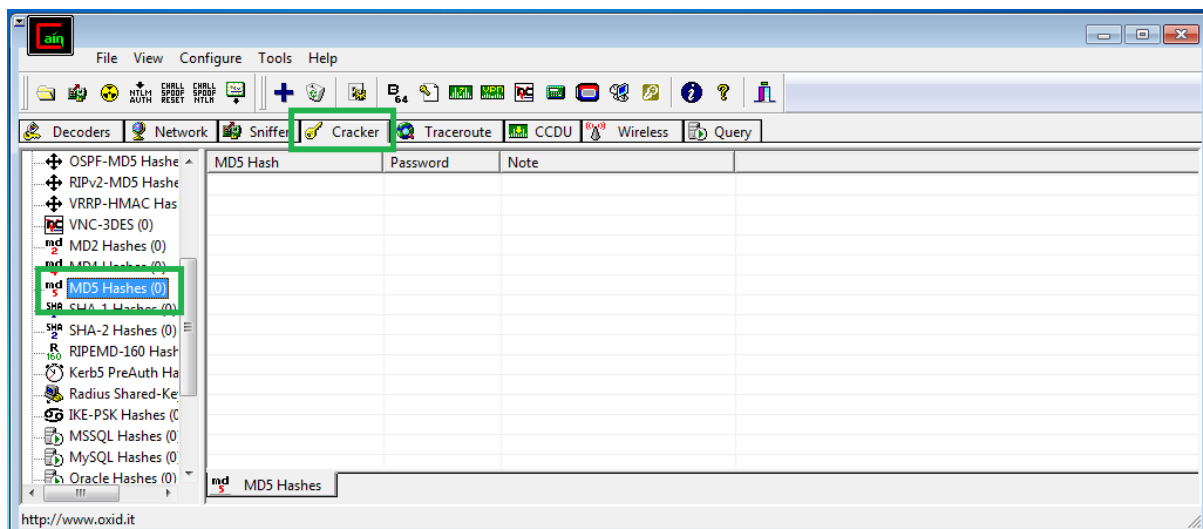


2.2 – Use Cain and Abel for cracking Windows account password using Dictionary attack and to decode wireless network passwords

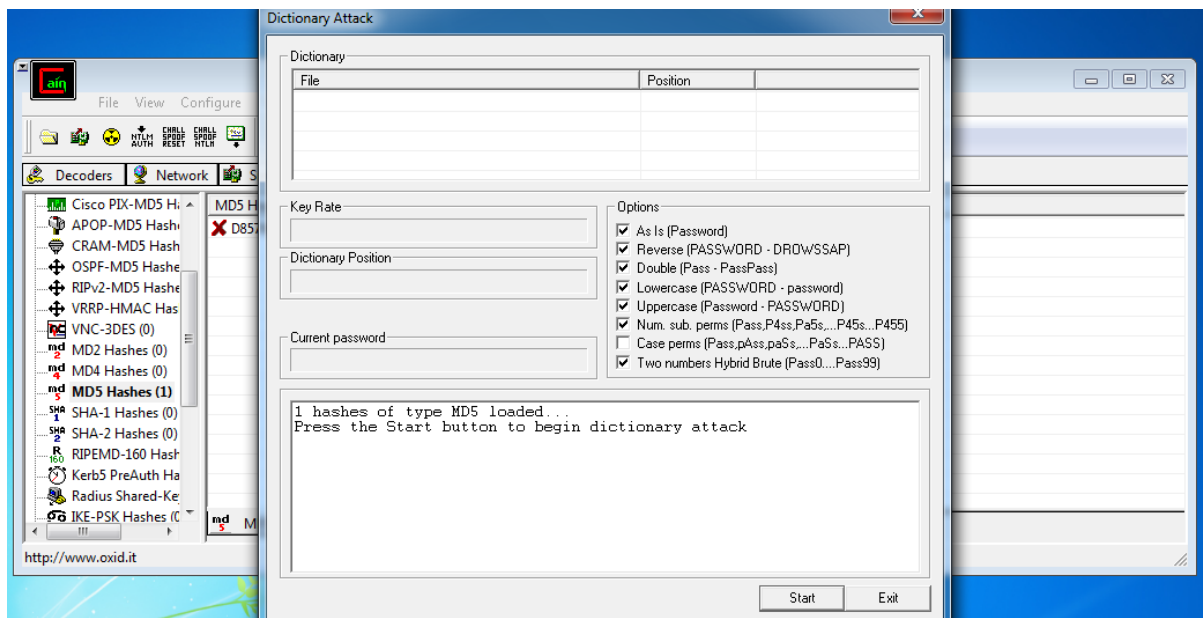
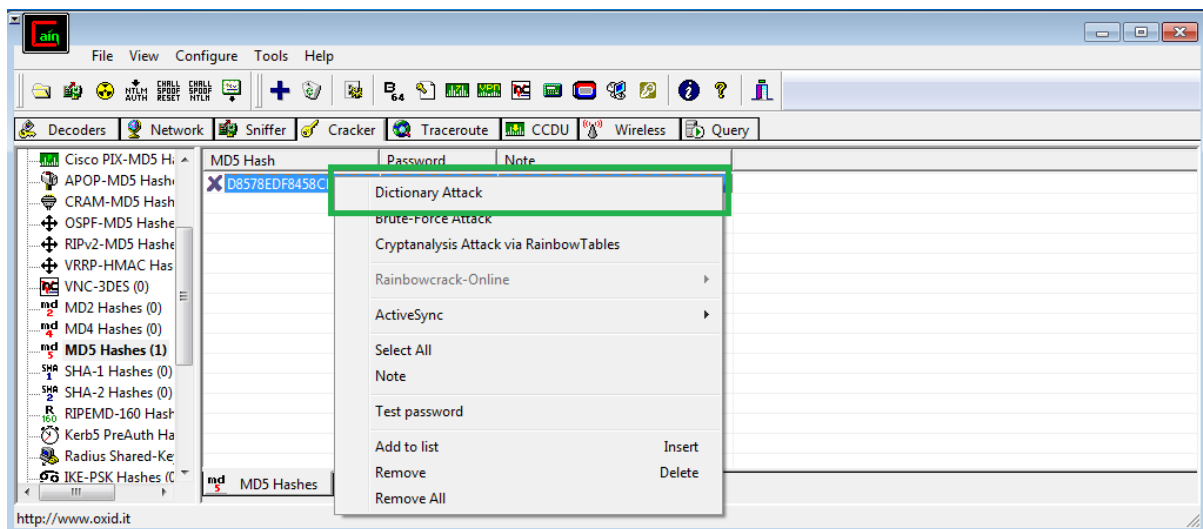
Go to the hash calculator



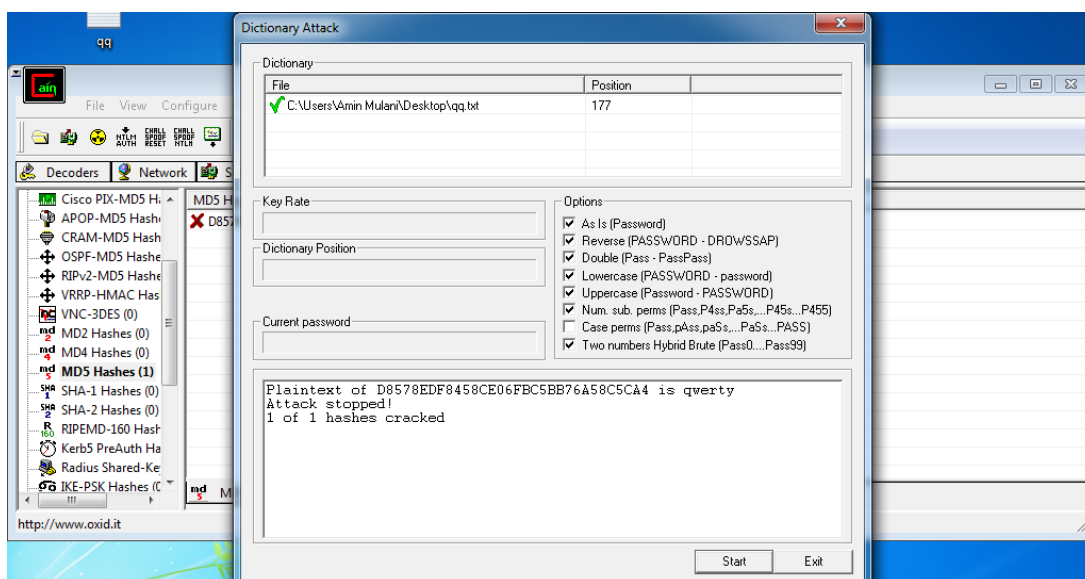
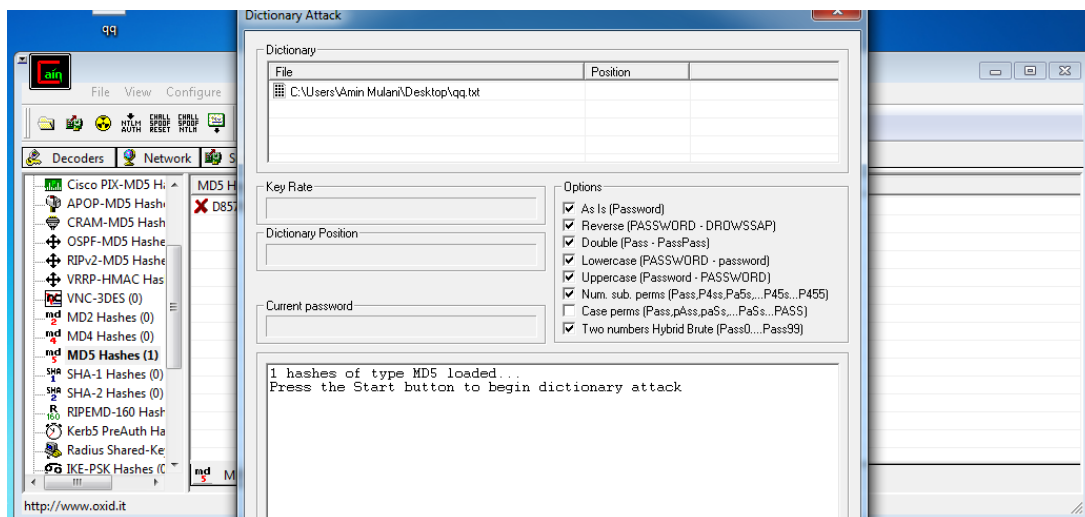
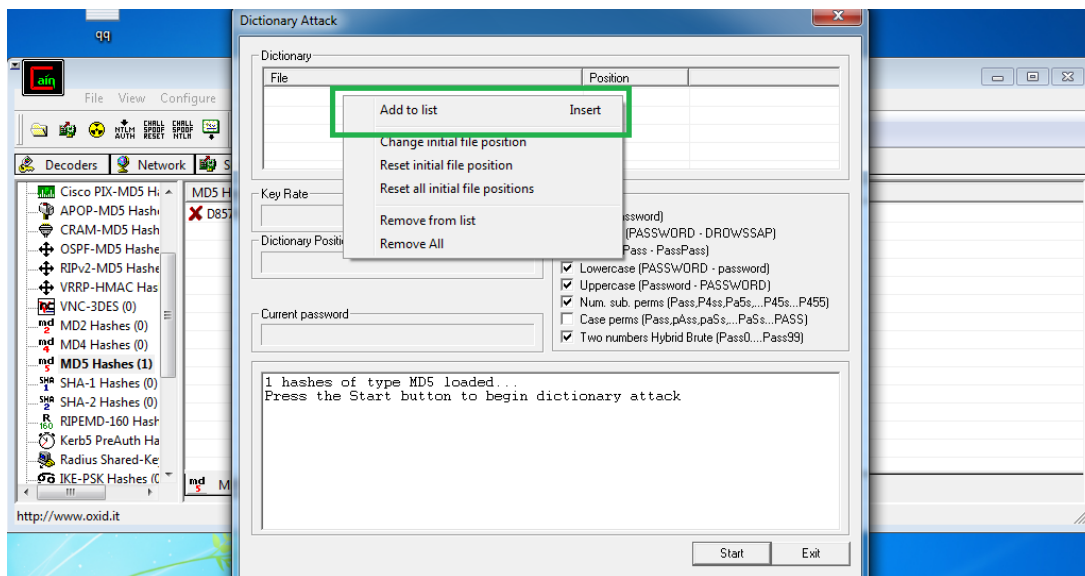
Copy the MD5 hash and paste it to the cracker of MD5



Right click on the Hash value and select Dictionary Attack



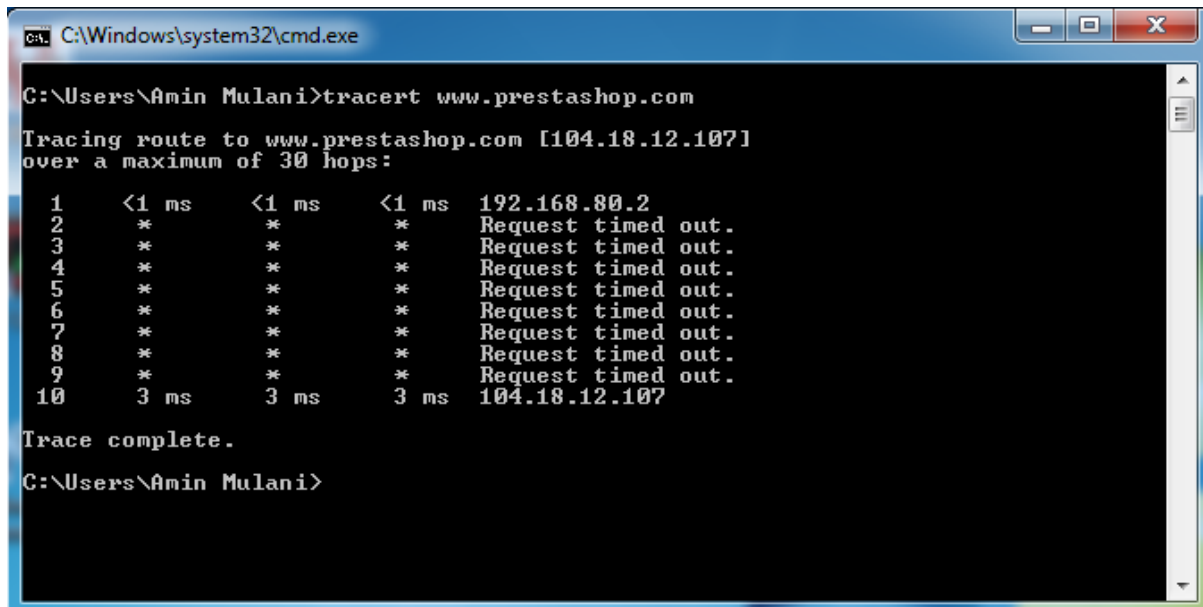
make a dictionary list and add to the attack



Practical 3

3.1 - Using TraceRoute, ping, ifconfig, netstat command

1 - tracert



```
C:\Windows\system32\cmd.exe

C:\Users\Amin Mulani>tracert www.prestashop.com

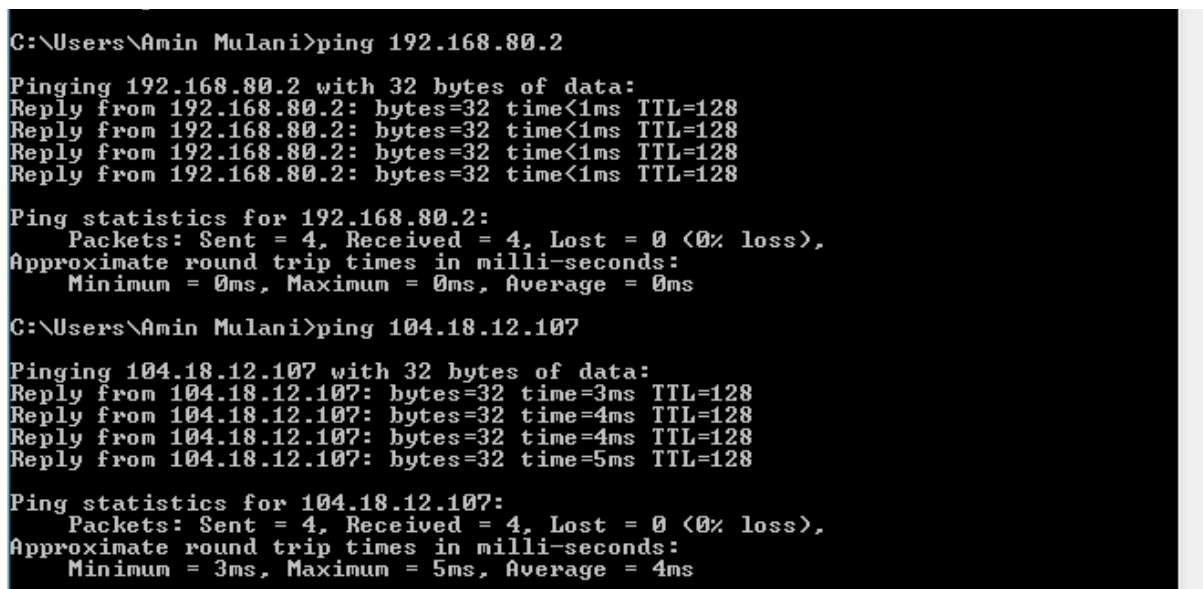
Tracing route to www.prestashop.com [104.18.12.107]
over a maximum of 30 hops:

  1  <1 ms    <1 ms    <1 ms    192.168.80.2
  2  *         *         *         Request timed out.
  3  *         *         *         Request timed out.
  4  *         *         *         Request timed out.
  5  *         *         *         Request timed out.
  6  *         *         *         Request timed out.
  7  *         *         *         Request timed out.
  8  *         *         *         Request timed out.
  9  *         *         *         Request timed out.
 10  3 ms     3 ms     3 ms     104.18.12.107

Trace complete.

C:\Users\Amin Mulani>
```

2 - ping



```
C:\Users\Amin Mulani>ping 192.168.80.2

Pinging 192.168.80.2 with 32 bytes of data:
Reply from 192.168.80.2: bytes=32 time<1ms TTL=128
Reply from 192.168.80.2: bytes=32 time<1ms TTL=128
Reply from 192.168.80.2: bytes=32 time<1ms TTL=128
Reply from 192.168.80.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.80.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Amin Mulani>ping 104.18.12.107

Pinging 104.18.12.107 with 32 bytes of data:
Reply from 104.18.12.107: bytes=32 time=3ms TTL=128
Reply from 104.18.12.107: bytes=32 time=4ms TTL=128
Reply from 104.18.12.107: bytes=32 time=4ms TTL=128
Reply from 104.18.12.107: bytes=32 time=5ms TTL=128

Ping statistics for 104.18.12.107:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 5ms, Average = 4ms
```


3 ifconfig

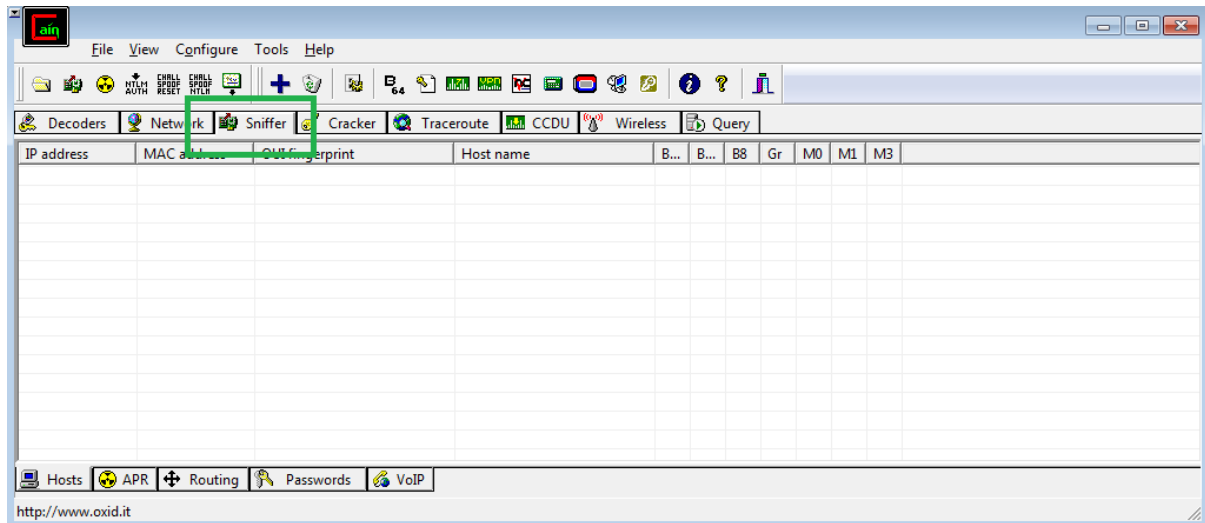
```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.80.130 netmask 255.255.255.0 broadcast 192.168.80.255  
    inet6 fe80::bbd7:6bcf:9bc6:447c prefixlen 64 scopeid 0x20<link>  
    ether 00:0c:29:3d:f2:65 txqueuelen 1000 (Ethernet)  
    RX packets 282 bytes 31662 (30.9 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 53 bytes 6888 (6.7 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 4 bytes 240 (240.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 4 bytes 240 (240.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
(kali@kali)-[~]  
$
```

4 – netstat

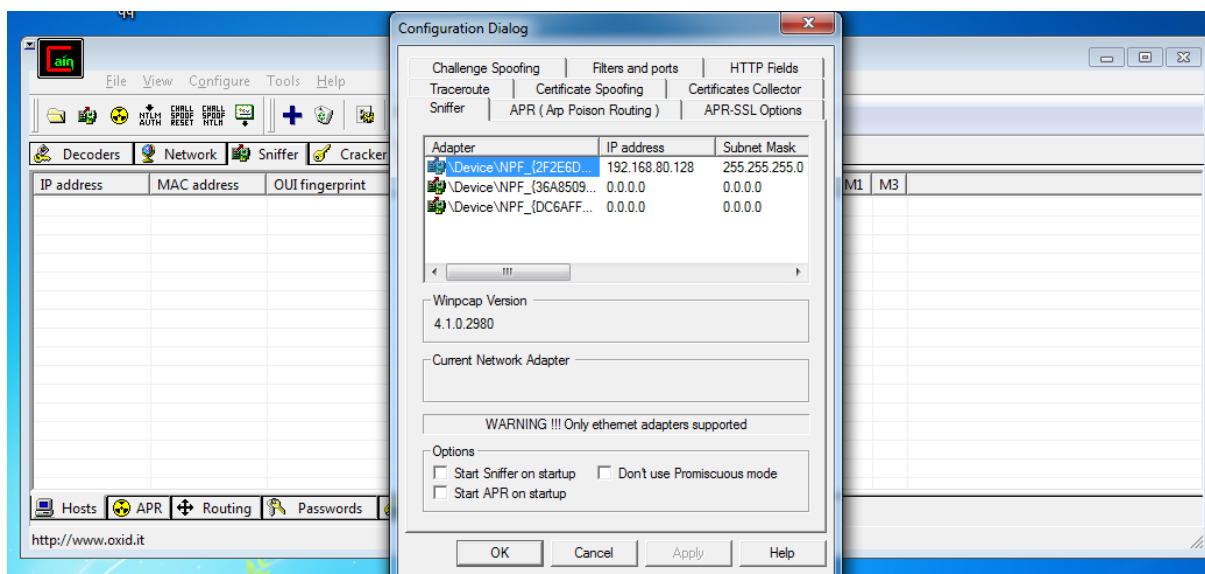
```
(kali@kali)-[~]  
$ netstat  
Active Internet connections (w/o servers)  
Proto Recv-Q Send-Q Local Address           Foreign Address         State  
udp        0      0 192.168.80.130:bootpc   192.168.80.254:bootps   ESTABLISH  
ED  
Active UNIX domain sockets (w/o servers)  
Proto RefCnt Flags       Type       State         I-Node  Path  
unix    3      [ ]          STREAM     CONNECTED    11578    /run/user/1000/bus  
unix    3      [ ]          STREAM     CONNECTED    10836  
unix    3      [ ]          STREAM     CONNECTED    11494  
unix    2      [ ]          DGRAM      CONNECTED    10563  
unix    3      [ ]          STREAM     CONNECTED    11337    /run/user/1000/pip  
ewire-0  
unix    2      [ ]          DGRAM      CONNECTED    3932  
unix    3      [ ]          STREAM     CONNECTED    10144    /run/user/1000/bus  
unix    3      [ ]          STREAM     CONNECTED    11557    @/tmp/.X11-unix/X0  
unix    3      [ ]          STREAM     CONNECTED    10872    /run/systemd/journ  
al/stdout  
unix    3      [ ]          STREAM     CONNECTED    8856    /run/user/1000/bus  
unix    3      [ ]          STREAM     CONNECTED    11496    @/tmp/.X11-unix/X0  
unix    3      [ ]          STREAM     CONNECTED    102446  
unix    3      [ ]          STREAM     CONNECTED    11092    /run/dbus/system_b  
us_socket  
unix    3      [ ]          STREAM     CONNECTED    10912  
unix    3      [ ]          STREAM     CONNECTED    11516  
unix    3      [ ]          STREAM     CONNECTED    11666  
unix    3      [ ]          STREAM     CONNECTED    11632    /run/dbus/system_b  
us_socket  
unix    3      [ ]          STREAM     CONNECTED    10141    /run/user/1000/at-  
spi/bus_0  
unix    3      [ ]          STREAM     CONNECTED    9927
```

3.2 Perform ARP Poisoning on Windows

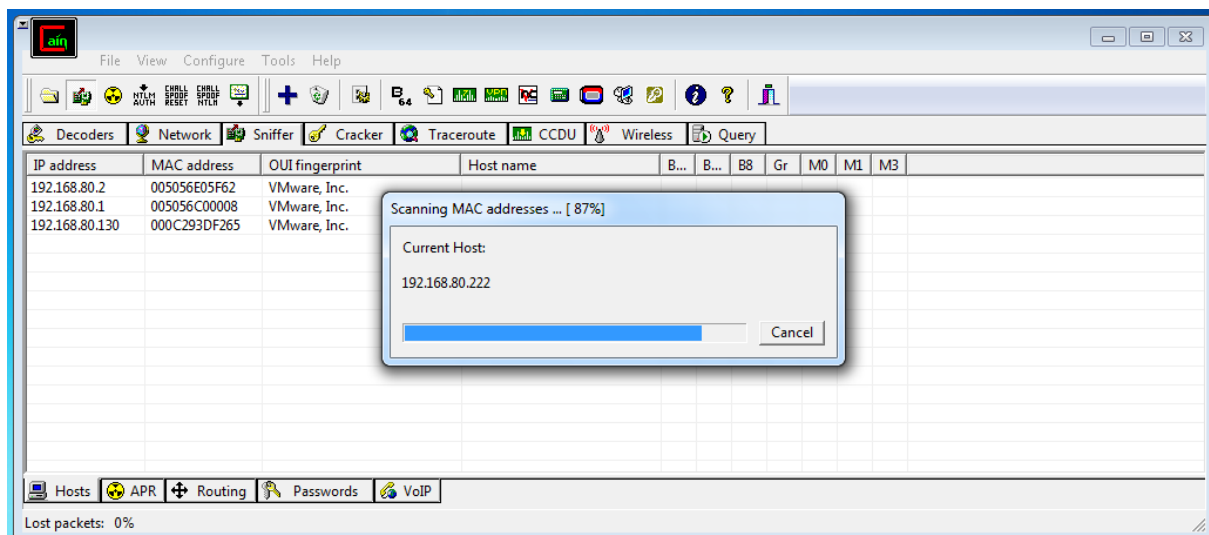
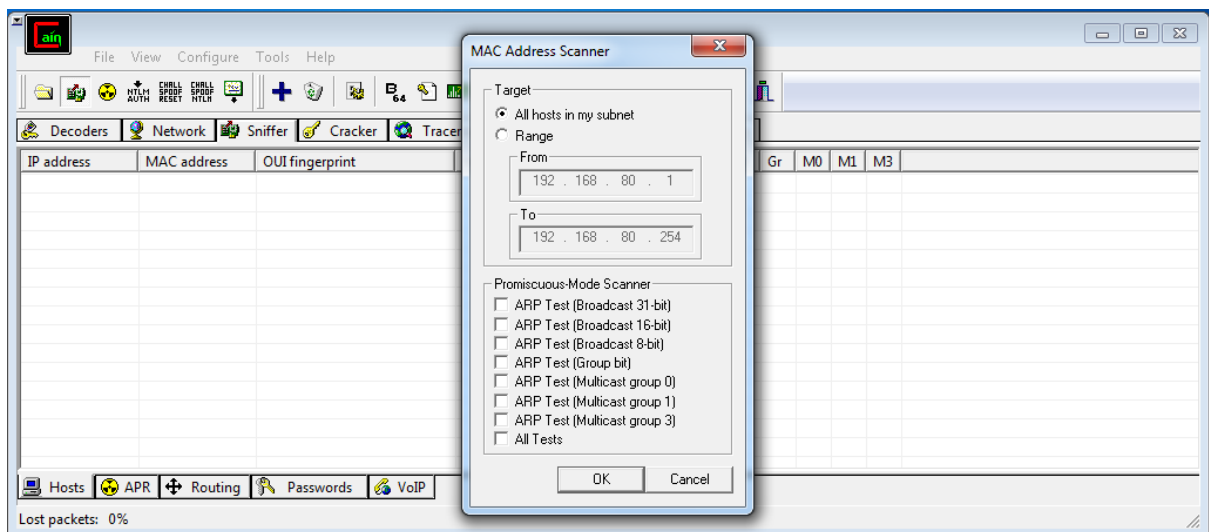
Open Cain and Abel and go to sniffer



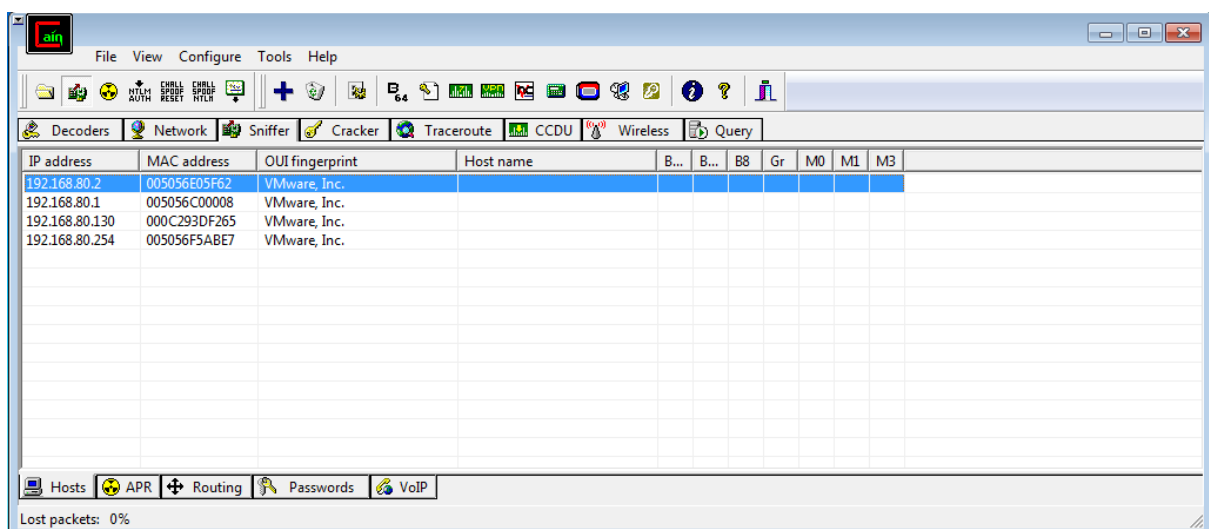
Next to folder icon there is the icon for Start/Stop Sniffer



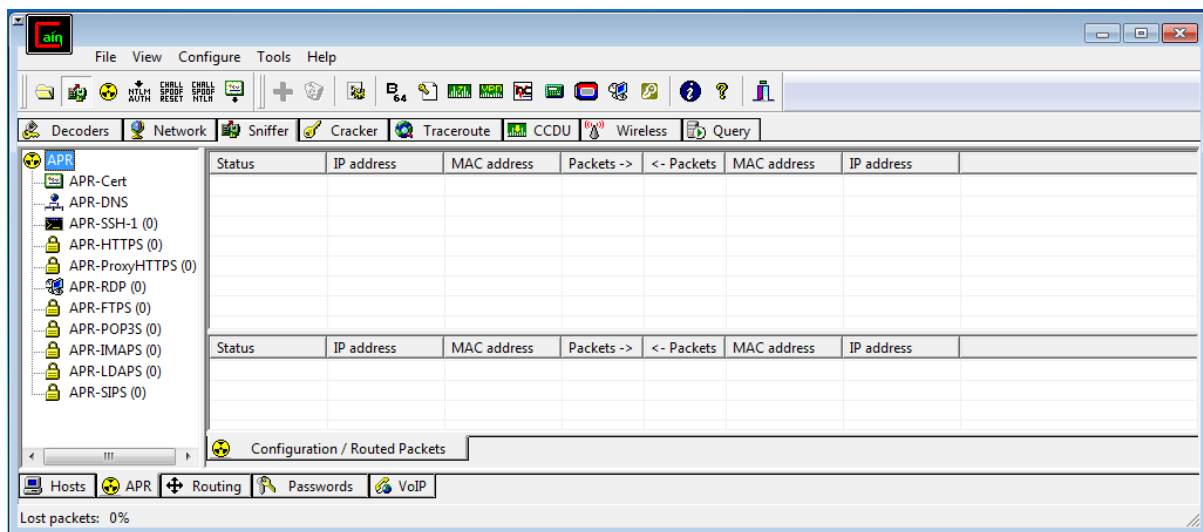
Click on + symbol on the taskbar



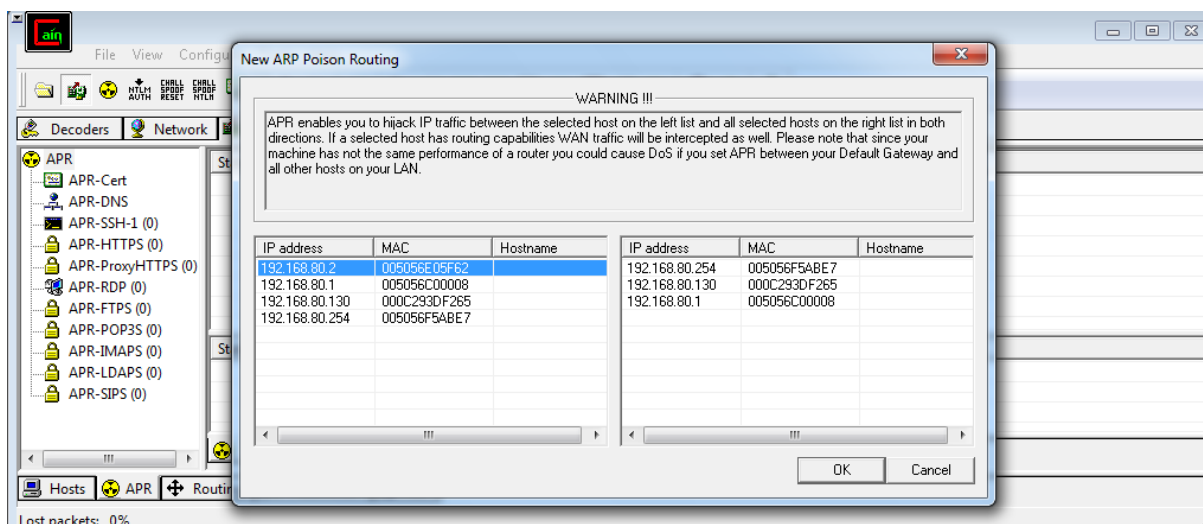
Show the connected host



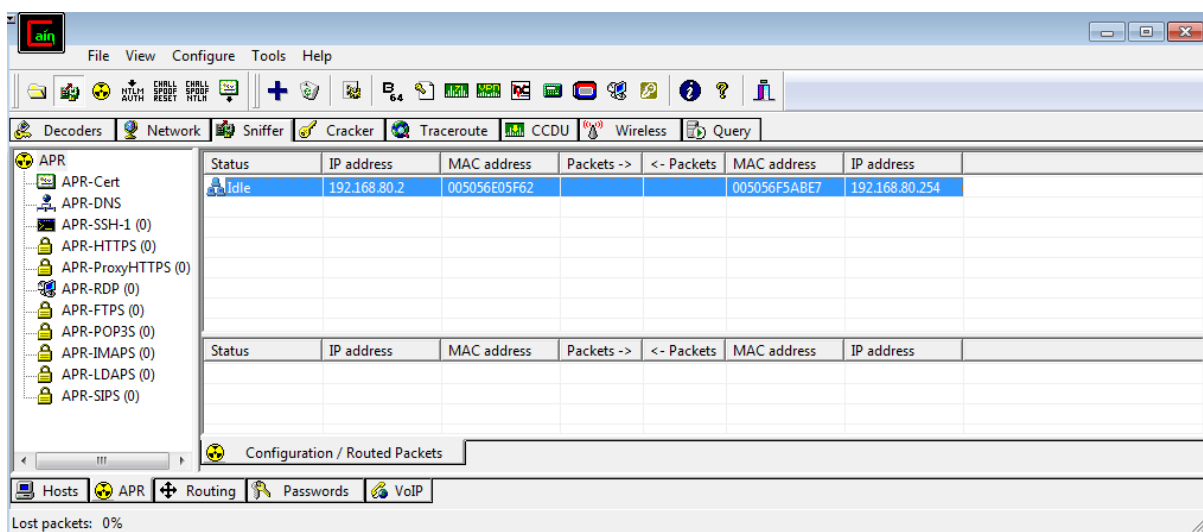
Select the APR option below



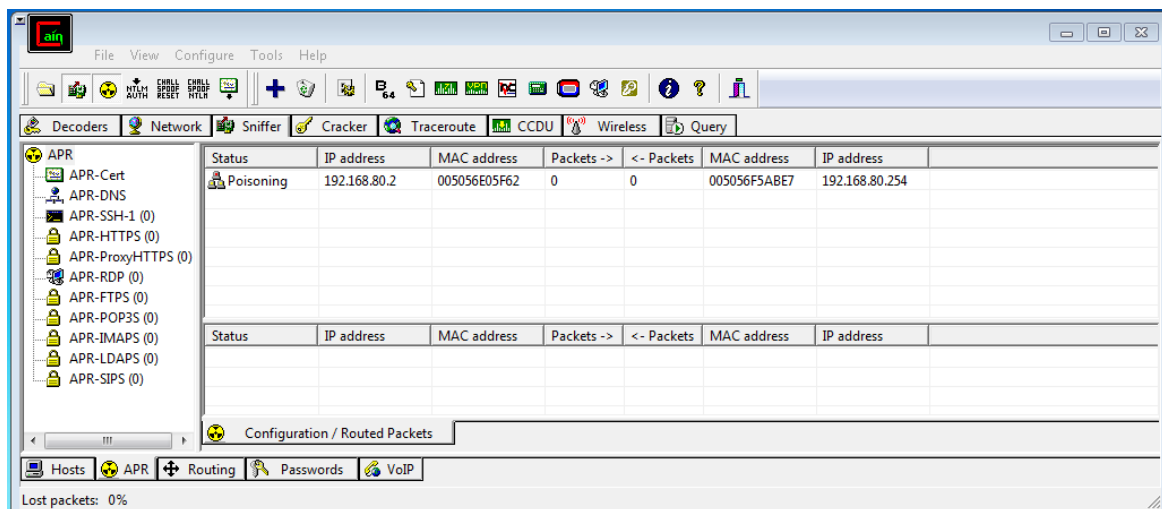
Click on + symbol on the taskbar



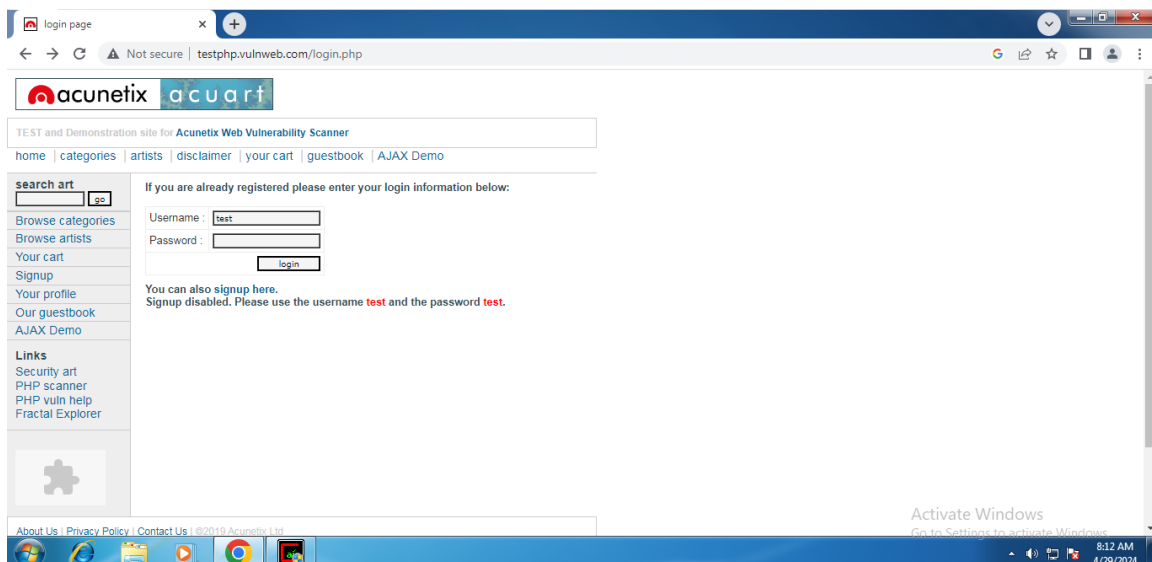
Select the host and add it the select the target and start the poisoning



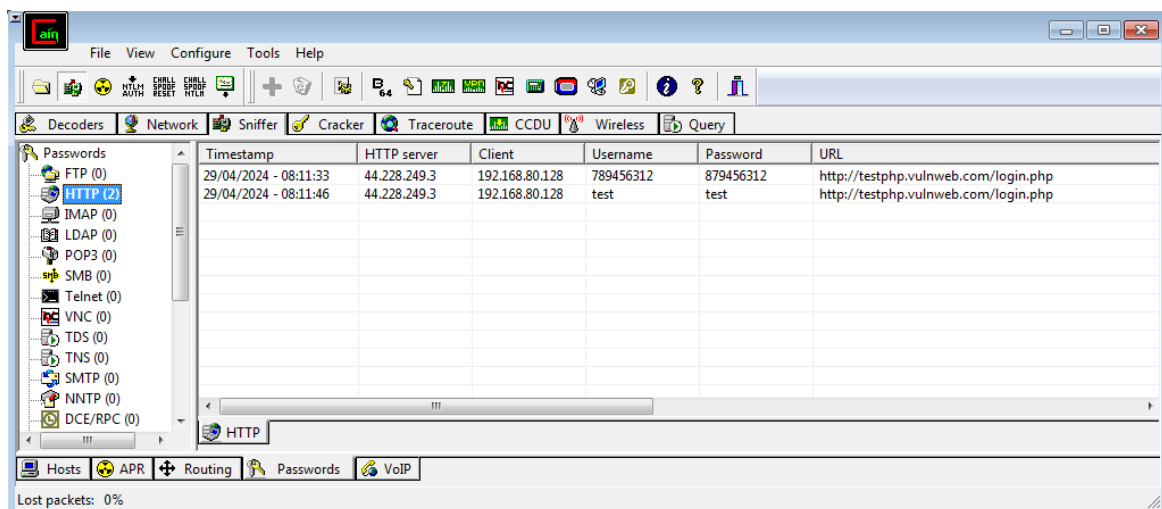
Click on Start/Stop Poisoning



Go to any website that has http protocol only it will work



Go to the passwords below to view the passwords gathered



Practical 4

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.

- 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: `nmap -sA -T4 scanme.nmap.org`

```
(root@kali)-[/home/kali]
# nmap -sA -T4 scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-28 22:53 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.000048s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
All 1000 scanned ports on scanme.nmap.org (45.33.32.156) are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.99 seconds
```

```
C:\Users\Amin Mulani>nmap -sA -T4 scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2024-04-29 08:24 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.00s 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 0.67 seconds
```

- 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: `nmap -p22,113,139 scanme.nmap.org`

```
(root@kali)-[/home/kali]
# nmap -p22,113,139 scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-28 22:56 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.035s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f

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

Nmap done: 1 IP address (1 host up) scanned in 1.61 seconds
```

```
C:\Users\Amin Mulani>nmap -p22,113,139 scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2024-04-29 08:28 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.033s latency).

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

Nmap done: 1 IP address (1 host up) scanned in 1.95 seconds
```

- FIN Scan (-sF) Sets just the TCP FIN bit.

Command: nmap -sF -T4 scanme.nmap.org

```
(root@kali)-[/home/kali]
# nmap -sF -T4 scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-28 23:07 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.00071s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
All 1000 scanned ports on scanme.nmap.org (45.33.32.156) are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 4.16 seconds
```

- NULL Scan (-sN) Does not set any bits (TCP flag header is 0)

Command: nmap -sN -p 22 scanme.nmap.org

```
(root@kali)-[/home/kali]
# nmap -sN -p 22 scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-28 23:03 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.00085s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f

PORT      STATE      SERVICE
22/tcp    open|filtered ssh

Nmap done: 1 IP address (1 host up) scanned in 0.74 seconds
```

```
C:\Users\Amin Mulani>nmap -sN -p 22 scanme.nmap.org
Starting Nmap 7.70 < https://nmap.org > at 2024-04-29 08:34 India Standard Time
Nmap scan report for scanme.nmap.org <45.33.32.156>
Host is up <0.00s latency>.

PORT      STATE      SERVICE
22/tcp    open|filtered ssh

Nmap done: 1 IP address <1 host up> scanned in 0.72 seconds
```

- XMAS Scan (-sX) Sets the FIN, PSH, and URG flags, lighting the packet up like a Christmas tree.

Command: nmap -sX -T4 scanme.nmap.org

```
(root@kali)-[/home/kali]
# nmap -sX -T4 scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-28 23:08 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.00064s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
All 1000 scanned ports on scanme.nmap.org (45.33.32.156) are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 4.50 seconds
```

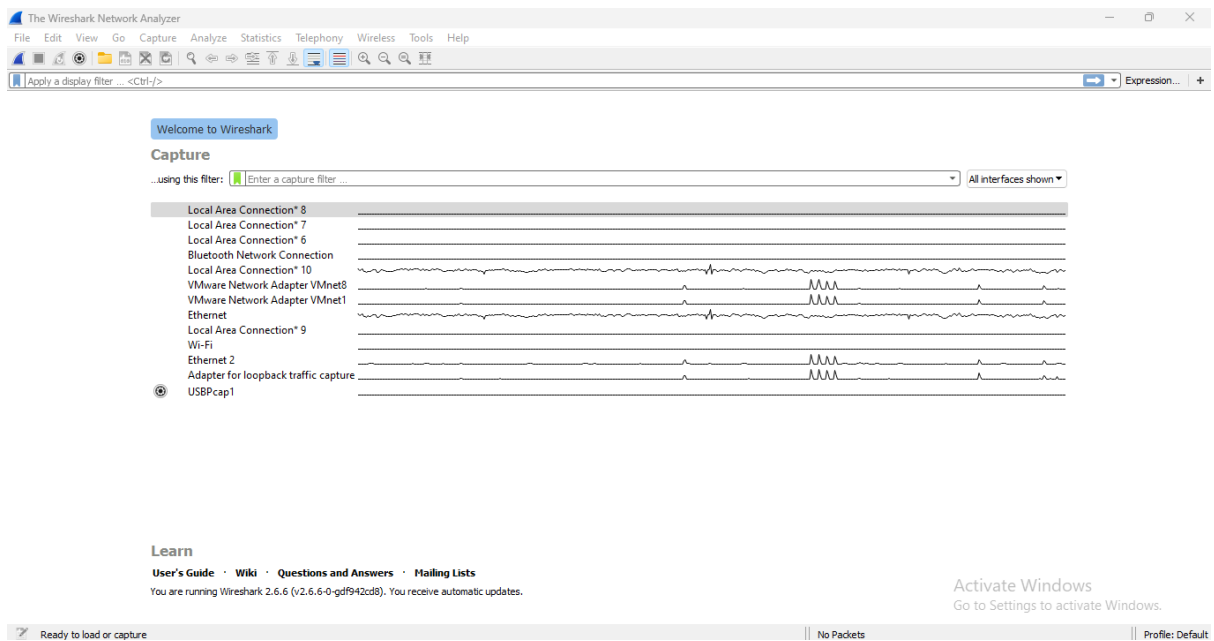
```
C:\Users\Amin Mulani>nmap -sX -T4 scanme.nmap.org
Starting Nmap 7.70 < https://nmap.org > at 2024-04-29 08:38 India Standard Time
Nmap scan report for scanme.nmap.org <45.33.32.156>
Host is up <0.00s latency>.
All 1000 scanned ports on scanme.nmap.org <45.33.32.156> are open|filtered

Nmap done: 1 IP address <1 host up> scanned in 4.63 seconds
```

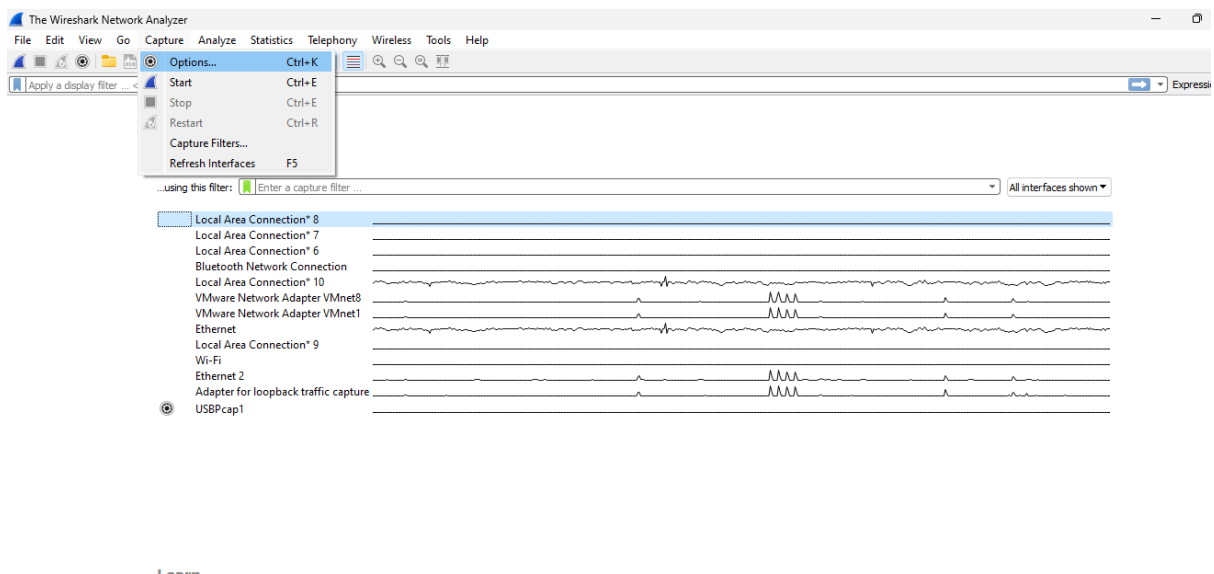
Practical 5

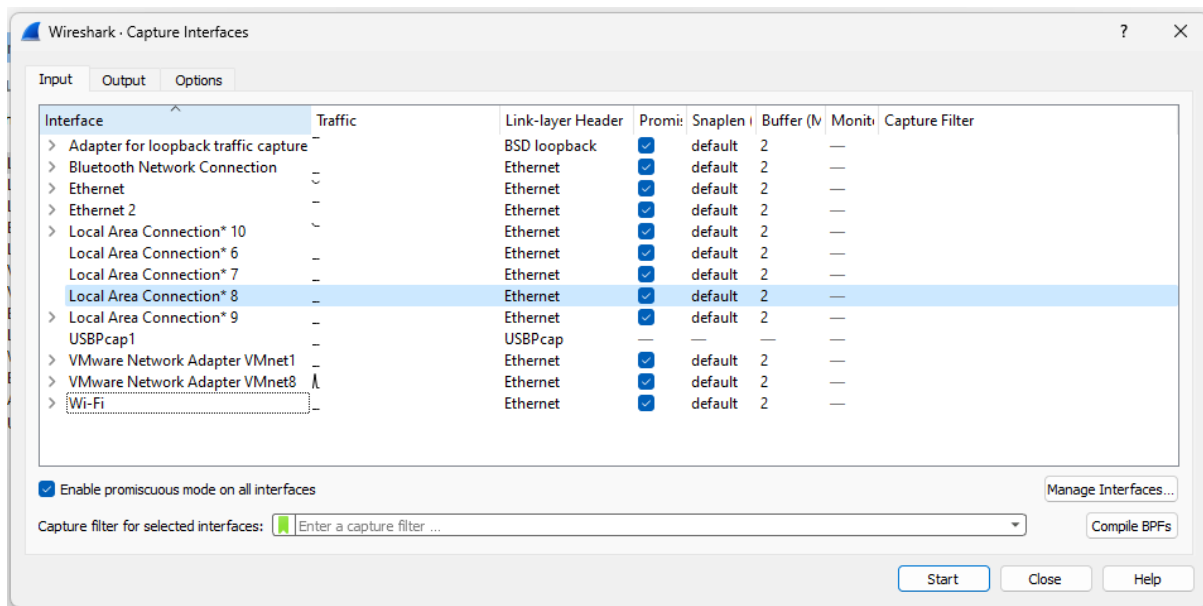
5.1) Use Wireshark sniffer to capture network traffic and analyze.

Step 1: Install and open WireShark .

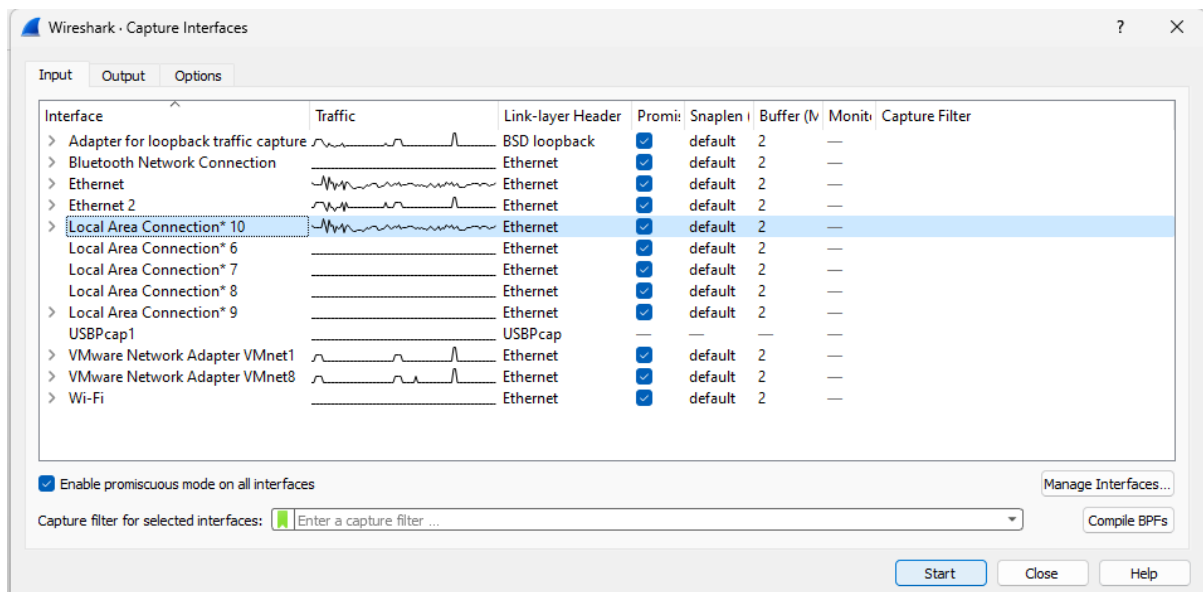


Step 2: Go to Capture tab and select Interface option.

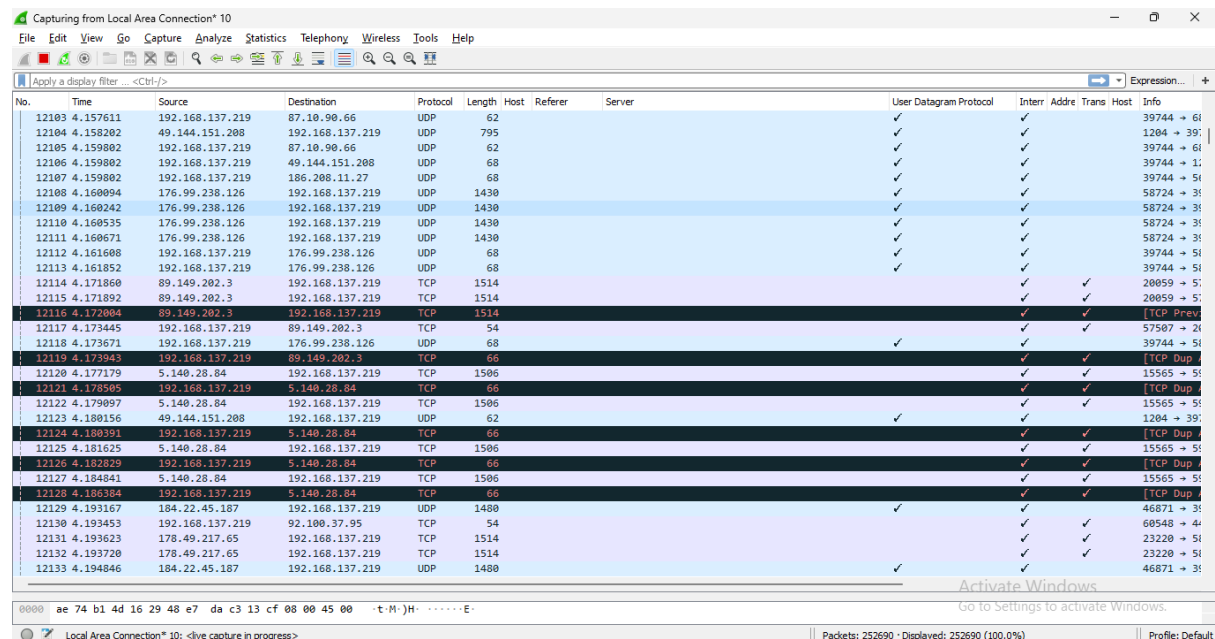




Step 3: In Capture interface, Select Local Area Connection and click on start.

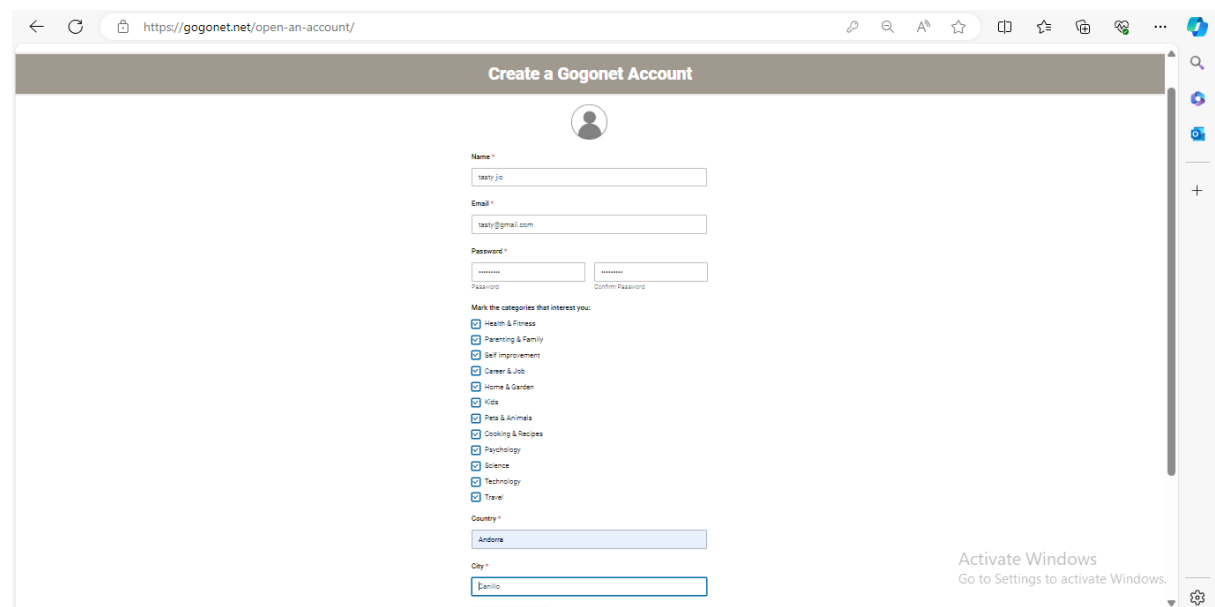


Step 4: The source, Destination and protocols of the packets in the LAN network are displayed.



| No. | Time | Source | Destination | Protocol | Length | Host | Referer | Server | User Datagram Protocol | Interr | Adresse | Trans | Host | Info |
|-------|----------|-----------------|-----------------|----------|--------|------|---------|--------|------------------------|--------|---------|-------|------|------------|
| 12103 | 4.157611 | 192.168.137.219 | 87.10.90.66 | UDP | 62 | | | | ✓ | | | | | 39744 → 61 |
| 12104 | 4.158202 | 49.144.151.208 | 192.168.137.219 | UDP | 795 | | | | ✓ | | | | | 1204 → 39: |
| 12105 | 4.159802 | 192.168.137.219 | 87.10.90.66 | UDP | 62 | | | | ✓ | | | | | 39744 → 61 |
| 12106 | 4.159802 | 192.168.137.219 | 49.144.151.208 | UDP | 68 | | | | ✓ | | | | | 39744 → 1: |
| 12107 | 4.159802 | 192.168.137.219 | 186.206.11.27 | UDP | 68 | | | | ✓ | | | | | 39744 → 5: |
| 12108 | 4.160094 | 176.99.238.126 | 192.168.137.219 | UDP | 1430 | | | | ✓ | | | | | 58724 → 3: |
| 12109 | 4.160242 | 176.99.238.126 | 192.168.137.219 | UDP | 1430 | | | | ✓ | | | | | 58724 → 3: |
| 12110 | 4.160535 | 176.99.238.126 | 192.168.137.219 | UDP | 1430 | | | | ✓ | | | | | 58724 → 3: |
| 12111 | 4.160671 | 176.99.238.126 | 192.168.137.219 | UDP | 1430 | | | | ✓ | | | | | 58724 → 3: |
| 12112 | 4.161608 | 192.168.137.219 | 176.99.238.126 | UDP | 68 | | | | ✓ | | | | | 39744 → 5: |
| 12113 | 4.161852 | 192.168.137.219 | 176.99.238.126 | UDP | 68 | | | | ✓ | | | | | 39744 → 5: |
| 12114 | 4.171860 | 89.149.202.3 | 192.168.137.219 | TCP | 1514 | | | | | ✓ | | | | 20059 → 5: |
| 12115 | 4.171892 | 89.149.202.3 | 192.168.137.219 | TCP | 1514 | | | | | ✓ | | | | 20059 → 5: |
| 12116 | 4.172004 | 89.149.202.3 | 192.168.137.219 | TCP | 1514 | | | | | ✓ | | | | [TCP Prev |
| 12117 | 4.173445 | 192.168.137.219 | 89.149.202.3 | TCP | 54 | | | | | ✓ | | | | 57507 → 2: |
| 12118 | 4.173671 | 192.168.137.219 | 176.99.238.126 | UDP | 68 | | | | ✓ | | | | | 39744 → 5: |
| 12119 | 4.173943 | 192.168.137.219 | 89.149.202.3 | TCP | 66 | | | | | ✓ | | | | [TCP Dup |
| 12120 | 4.177179 | 5.140.28.84 | 192.168.137.219 | TCP | 1506 | | | | | ✓ | | | | 15565 → 5: |
| 12121 | 4.178505 | 192.168.137.219 | 5.140.28.84 | TCP | 66 | | | | | ✓ | | | | [TCP Dup |
| 12122 | 4.179097 | 5.140.28.84 | 192.168.137.219 | TCP | 1506 | | | | | ✓ | | | | 15565 → 5: |
| 12123 | 4.180156 | 49.144.151.208 | 192.168.137.219 | UDP | 62 | | | | ✓ | | | | | 1204 → 39: |
| 12124 | 4.180391 | 192.168.137.219 | 5.140.28.84 | TCP | 66 | | | | | ✓ | | | | [TCP Dup |
| 12125 | 4.181625 | 5.140.28.84 | 192.168.137.219 | TCP | 1506 | | | | | ✓ | | | | 15565 → 5: |
| 12126 | 4.182629 | 192.168.137.219 | 5.140.28.84 | TCP | 66 | | | | | ✓ | | | | [TCP Dup |
| 12127 | 4.184841 | 5.140.28.84 | 192.168.137.219 | TCP | 1506 | | | | | ✓ | | | | 15565 → 5: |
| 12128 | 4.188364 | 192.168.137.219 | 5.140.28.84 | TCP | 66 | | | | | ✓ | | | | [TCP Dup |
| 12129 | 4.193167 | 184.22.45.187 | 192.168.137.219 | UDP | 1400 | | | | ✓ | | | | | 46871 → 3: |
| 12130 | 4.193453 | 192.168.137.219 | 92.100.37.95 | TCP | 54 | | | | | ✓ | | | | 68548 → 4: |
| 12131 | 4.193623 | 178.49.217.65 | 192.168.137.219 | TCP | 1514 | | | | | ✓ | | | | 23220 → 5: |
| 12132 | 4.193720 | 178.49.217.65 | 192.168.137.219 | TCP | 1514 | | | | | ✓ | | | | 23220 → 5: |
| 12133 | 4.194846 | 184.22.45.187 | 192.168.137.219 | UDP | 1400 | | | | ✓ | | | | | 46871 → 3: |

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



https://gogonet.net/open-an-account/

Create a Gogonet Account

Name *

lasty jo

Email *

lasty@gmail.com

Password *

Password Confirm Password

Mark the categories that interest you:

- ☒ Health & Fitness
- ☒ Parenting & Family
- ☒ Self Improvement
- ☒ Career & Job
- ☒ Home & Garden
- ☒ Kids
- ☒ Pets & Animals
- ☒ Cooking & Recipes
- ☒ Psychology
- ☒ Science
- ☒ Technology
- ☒ Travel

Country *

Andorra

City *

Lanillo

Activate Windows
Go to Settings to activate Windows.

Step 6: Enter the credentials and then sign in

https://gogonet.net/log-in/

GOGONET

★★★★★

Log in to Your Account

Email

Password

GOGONET ★★★★★

GOGONET is your destination for premium digital resources on personal development, healthy nutrition, meditation, fitness, sports, and much more. Discover content that will inspire you, enrich your everyday life, and guide you to the best version of yourself. Our carefully crafted ebooks, audios, and courses are designed to provide practical insights and techniques that you can immediately implement. Time into a world of knowledge and transformation. Begin your journey towards top-notch achievement now!

[Blog](#)
[Contact us](#)
[About us](#)
[Privacy Policy](#)
[Terms and Conditions](#)

Copyright © 2024 GOGONET LLC. All rights reserved.

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

Capturing from Local Area Connection* 10

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F>

| No. | Time | Source | Destination | Protocol | Length | Host | Referred | Server | User Datagram Protocol | Interr | Adre | Trans | Host | Info |
|------|------------|-----------------|-----------------|----------|--------|------|----------|--------|------------------------|--------|------|-------|------|------------|
| 1826 | 789.301754 | 49.144.151.208 | 192.168.137.219 | UDP | 62 | | | | ✓ | ✓ | | | | 1284 → 39 |
| 1826 | 789.400673 | 192.168.137.219 | 49.144.151.208 | UDP | 1480 | | | | ✓ | ✓ | | | | 39744 → 1 |
| 1826 | 789.416307 | 192.168.137.219 | 62.44.138.125 | TCP | 122 | | | | ✓ | ✓ | ✓ | ✓ | | [TCP Retr |
| 1826 | 789.431805 | 192.168.137.219 | 95.59.196.62 | TCP | 66 | | | | ✓ | ✓ | ✓ | ✓ | | [TCP Retr |
| 1826 | 789.431805 | 192.168.137.219 | 201.95.176.159 | TCP | 66 | | | | ✓ | ✓ | ✓ | ✓ | | [TCP Retr |
| 1826 | 789.431805 | 192.168.137.219 | 46.232.210.71 | UDP | 62 | | | | ✓ | ✓ | | | | 39744 → 1 |
| 1826 | 789.431805 | 192.168.137.219 | 51.75.75.103 | UDP | 62 | | | | ✓ | ✓ | | | | 39744 → 61 |
| 1826 | 789.494364 | 192.168.137.219 | 201.95.176.159 | UDP | 62 | | | | ✓ | ✓ | | | | 39744 → 2 |
| 1826 | 789.494364 | 192.168.137.219 | 95.59.196.62 | UDP | 62 | | | | ✓ | ✓ | | | | 39744 → 2 |
| 1826 | 789.550817 | 49.144.151.208 | 192.168.137.219 | UDP | 62 | | | | ✓ | ✓ | | | | 1284 → 39 |
| 1826 | 789.552108 | 192.168.137.219 | 49.144.151.208 | UDP | 398 | | | | ✓ | ✓ | | | | 39744 → 1 |
| 1826 | 789.566465 | 46.232.210.71 | 192.168.137.219 | ICMP | 90 | | | | ✓ | ✓ | | | | Destinati |
| 1826 | 789.604508 | 192.168.137.219 | 142.251.223.67 | TCP | 55 | | | | ✓ | ✓ | ✓ | ✓ | | [TCP Keep |
| 1826 | 789.605359 | 192.168.137.219 | 49.144.151.208 | UDP | 1480 | | | | ✓ | ✓ | | | | 39744 → 1 |
| 1826 | 789.619174 | 192.168.137.219 | 151.101.1.229 | TCP | 55 | | | | ✓ | ✓ | ✓ | ✓ | | [TCP Keep |
| 1826 | 789.626429 | 151.101.1.229 | 192.168.137.219 | TCP | 66 | | | | ✓ | ✓ | ✓ | ✓ | | [TCP Keep |
| 1826 | 789.678565 | 142.251.223.67 | 192.168.137.219 | TCP | 66 | | | | ✓ | ✓ | ✓ | ✓ | | [TCP Keep |
| 1826 | 789.729612 | 192.168.137.219 | 49.144.151.208 | UDP | 1480 | | | | ✓ | ✓ | | | | 39744 → 1 |
| 1826 | 789.744537 | 192.168.137.219 | 185.68.193.205 | TCP | 55 | | | | ✓ | ✓ | ✓ | ✓ | | [TCP Keep |
| 1826 | 789.769106 | 49.144.151.208 | 192.168.137.219 | UDP | 65 | | | | ✓ | ✓ | | | | 1284 → 39 |
| 1826 | 789.823770 | 192.168.137.219 | 185.68.193.205 | TCP | 55 | | | | ✓ | ✓ | ✓ | ✓ | | [TCP Retr |
| 1826 | 789.854650 | 192.168.137.219 | 49.144.151.208 | UDP | 1480 | | | | ✓ | ✓ | | | | 39744 → 1 |
| 1826 | 789.909169 | 192.168.137.179 | 192.168.137.1 | DNS | 75 | | | | ✓ | ✓ | | | | Standard i |
| 1826 | 789.913691 | 192.168.137.179 | 163.70.143.63 | UDP | 1242 | | | | ✓ | ✓ | | | | 43007 → 4 |
| 1826 | 789.980046 | 192.168.137.219 | 49.144.151.208 | UDP | 1480 | | | | ✓ | ✓ | | | | 39744 → 1 |
| 1826 | 789.993286 | 65.49.14.172 | 192.168.137.219 | TCP | 54 | | | | ✓ | ✓ | ✓ | ✓ | | 56637 → 6 |
| 1826 | 789.994807 | 185.68.193.205 | 192.168.137.219 | TCP | 54 | | | | ✓ | ✓ | ✓ | ✓ | | [TCP Zero |
| 1826 | 790.004297 | 192.168.137.219 | 65.49.14.172 | TCP | 54 | | | | ✓ | ✓ | ✓ | ✓ | | 61207 → 51 |
| 1826 | 790.004297 | 192.168.137.219 | 65.49.14.172 | TCP | 54 | | | | ✓ | ✓ | ✓ | ✓ | | 61207 → 51 |
| 1826 | 790.004610 | 49.144.151.208 | 192.168.137.219 | UDP | 65 | | | | ✓ | ✓ | | | | 1284 → 39 |
| 1826 | 790.006640 | 192.168.137.219 | 49.144.151.208 | UDP | 398 | | | | ✓ | ✓ | | | | 39744 → 1 |

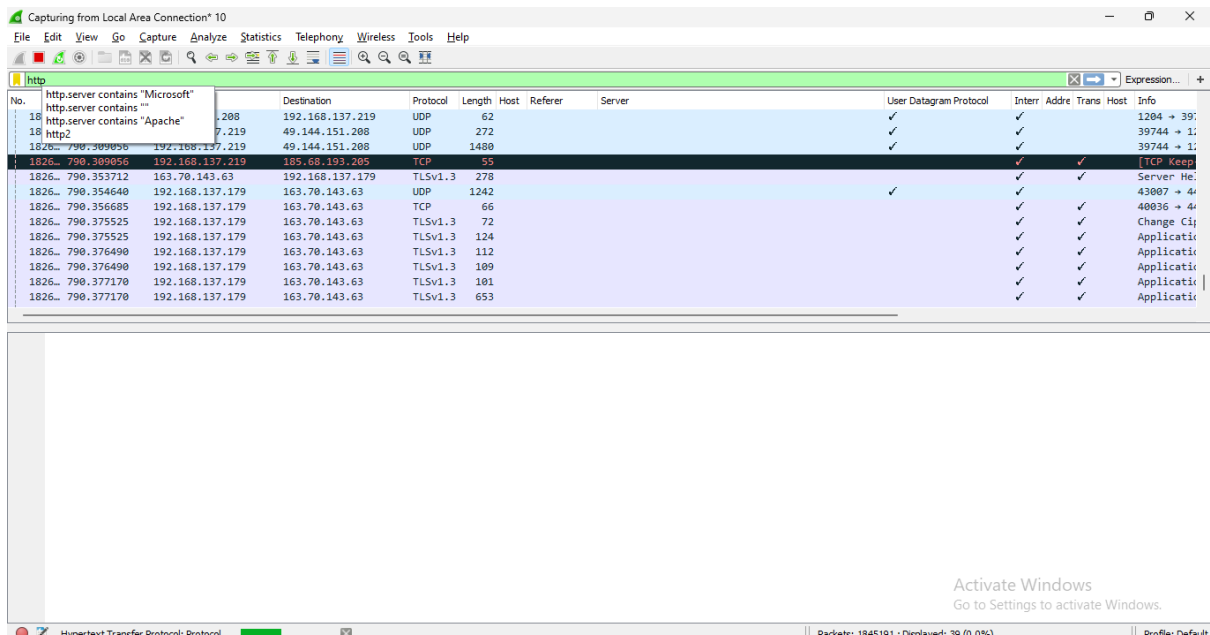
Activate Windows
Go to Settings to activate Windows.

Local Area Connection* 10: <live capture in progress>

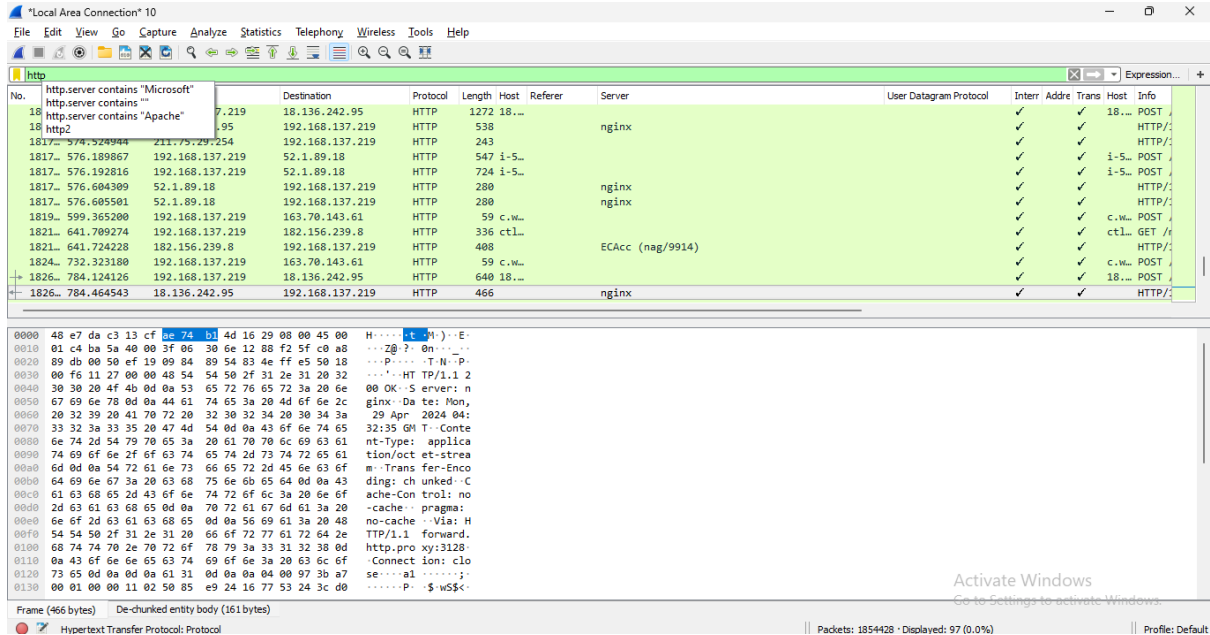
Packets: 1827345 · Displayed: 1827345 (100.0%)

Profile: Default

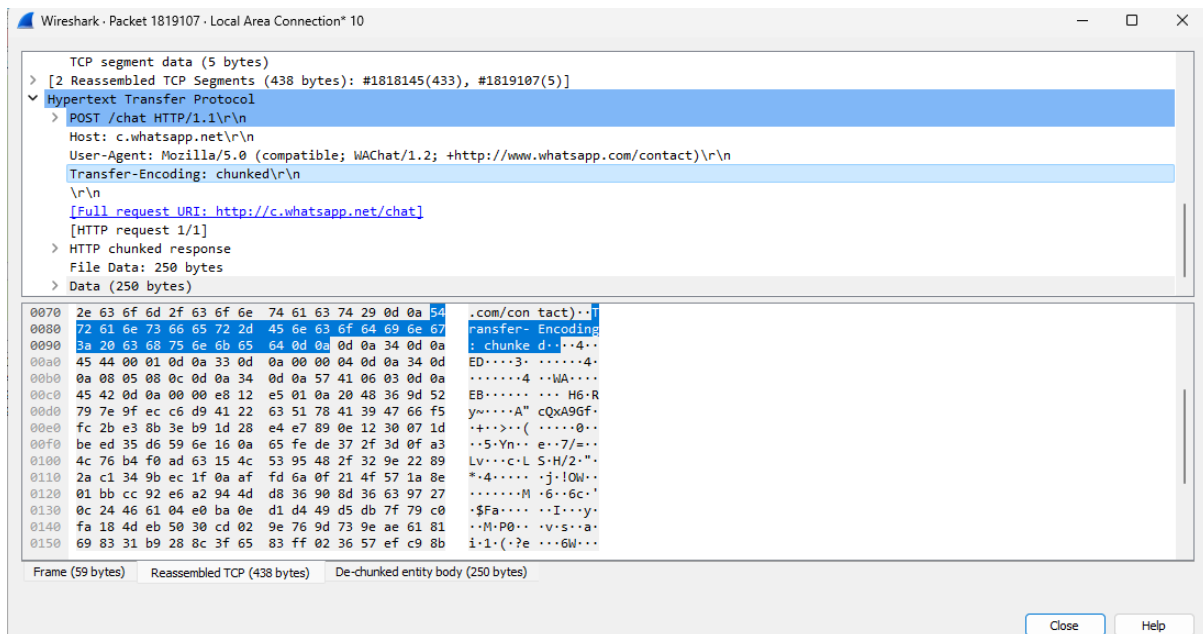
Step 8: Select filter as http to make the search easier and click on apply.



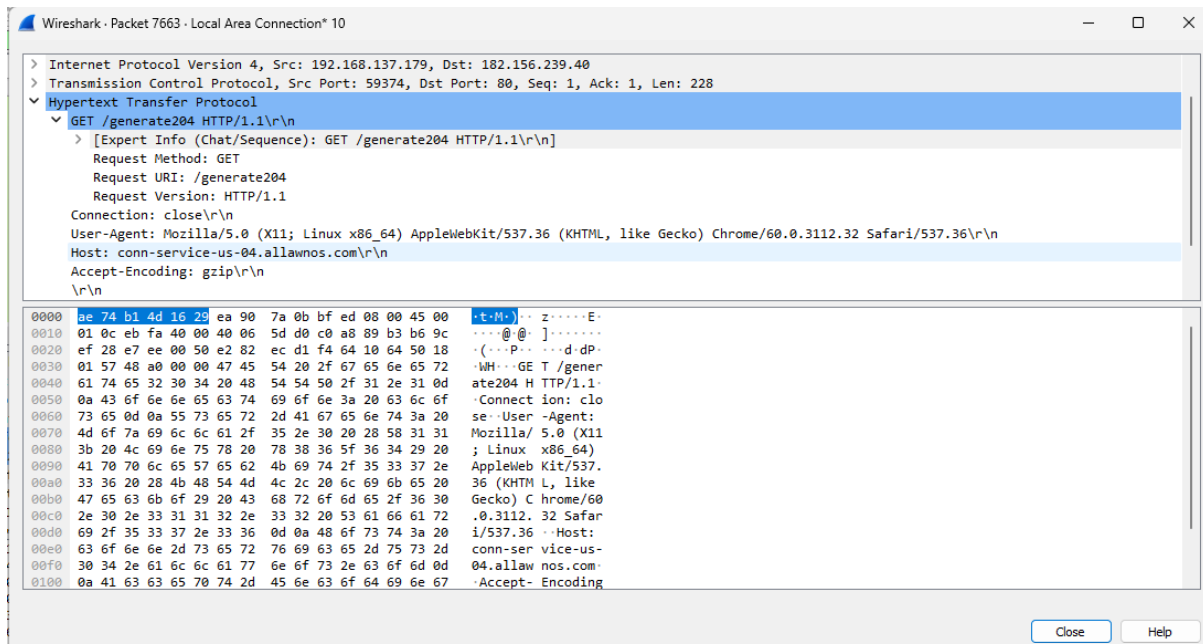
Step 9: Now stop the tool to stop recording.



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

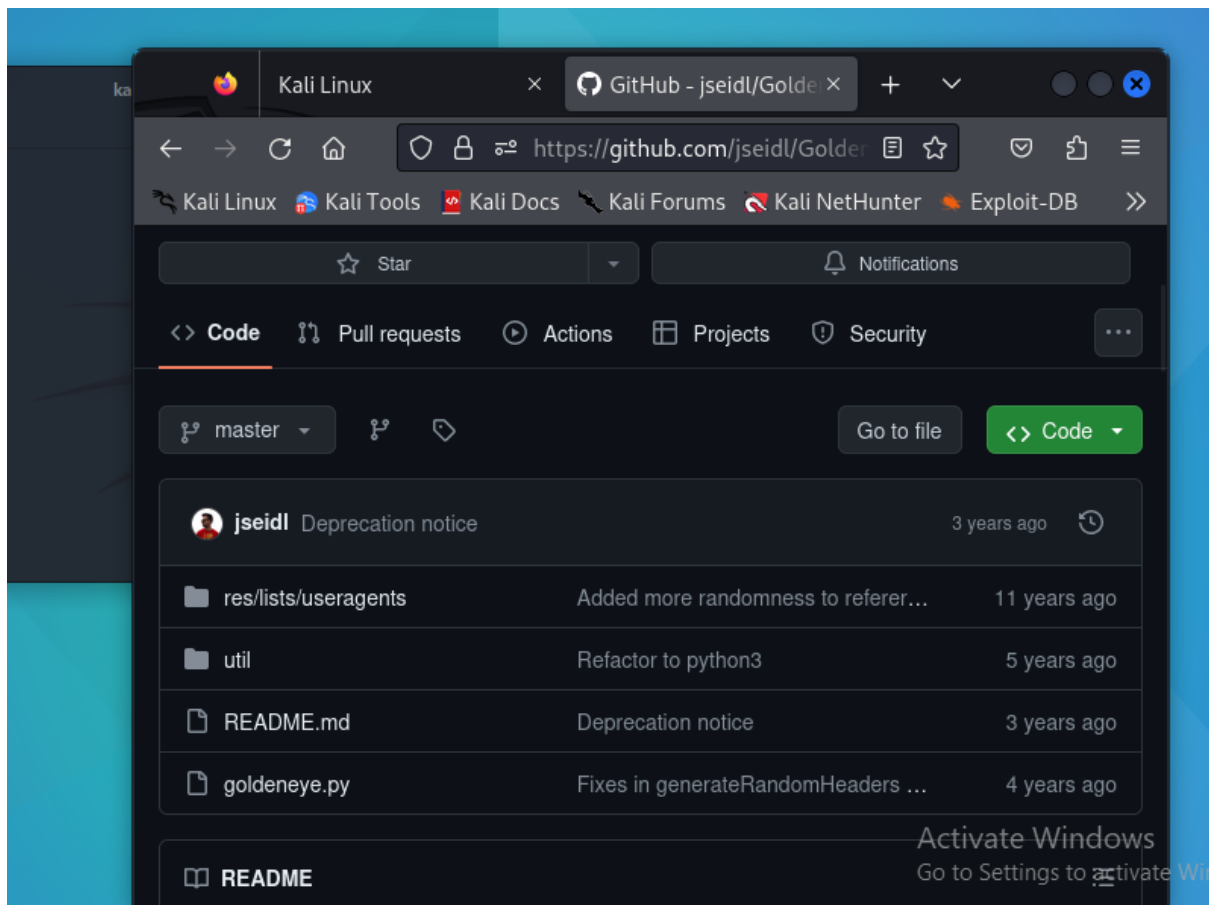


Step 11: You will see the email- id and password that you used to log in.



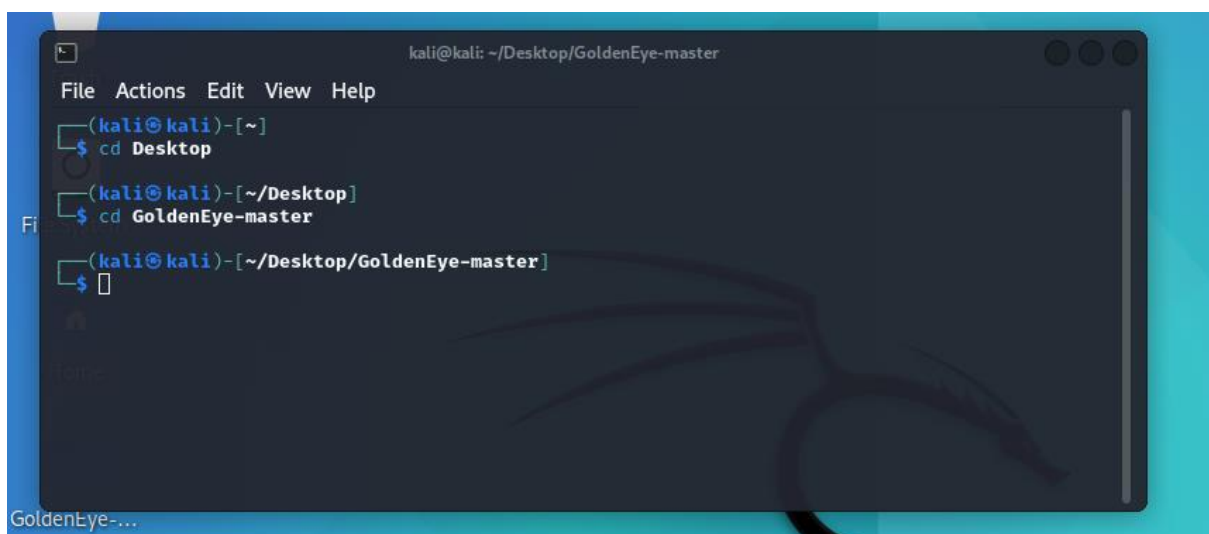
5.2 DOS Using GoldenEye on Kali Linux

First install Golden Eye from github

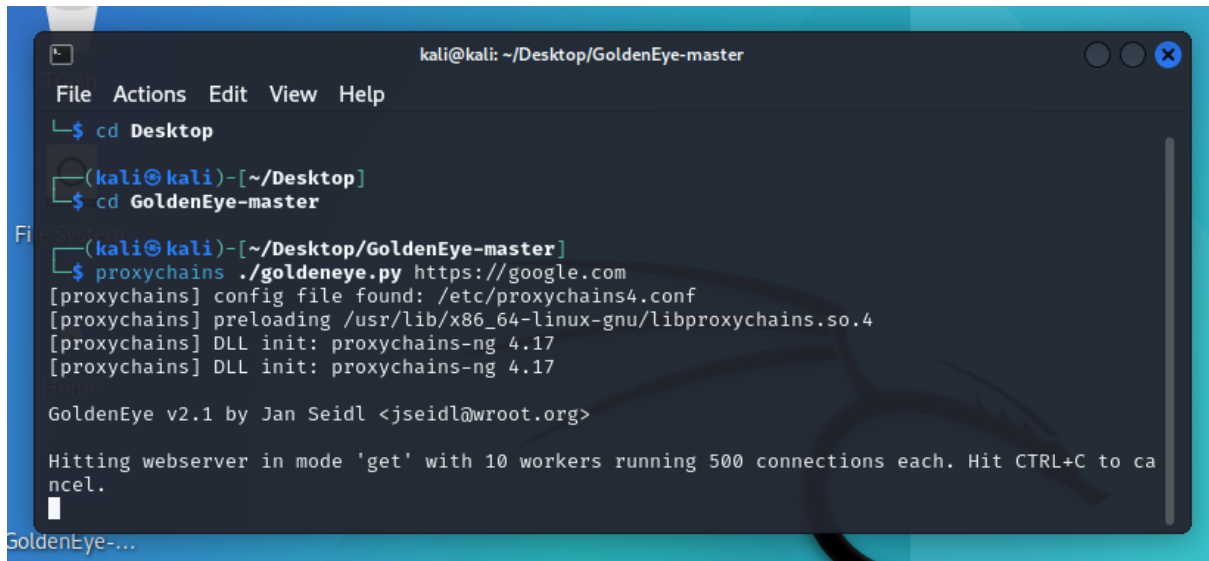


Keep It on desktop and then unzip it

Then redirect to the directory where golden eye is placed on the terminal



Then type proxychains ./goldeneye.py <https://google.com>

A terminal window titled 'kali@kali: ~/Desktop/GoldenEye-master' with a menu bar (File, Actions, Edit, View, Help). The terminal shows the following commands and output:

```
$ cd Desktop
(kali@kali)~[~/Desktop]
$ cd GoldenEye-master
(kali@kali)~[~/Desktop/GoldenEye-master]
$ proxychains ./goldeneye.py https://google.com
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] DLL init: proxychains-ng 4.17

GoldenEye v2.1 by Jan Seidl <jseidl@wroot.org>

Hitting webserver in mode 'get' with 10 workers running 500 connections each. Hit CTRL+C to cancel.
█
```

GoldenEye-...

Here the DOS attack is completed

Practical 6

AIM: Persistent Cross-Site Scripting Attack

1. Set up a vulnerable web application that is susceptible to persistent XSS attacks
2. Craft a malicious script to exploit the XSS vulnerability and execute arbitrary code.
3. Observe the consequences of the attack and understand the potential risks associated with XSS vulnerabilities.

Step 1- Visit to <http://www.techpanda.org>

Login | Personal Contacts Manager v1.0

Email*

Password*

☐ Remember me

Step 2: Enter email as admin@google.com and password as Password2010

Dashboard | Personal Contacts Manager v1.0

| ID | First Name | Last Name | Mobile No | Email | Actions |
|-------|----------------------|-----------|-------------|----------------------------------|----------------------|
| 1 | mynams | jenefry | 9898989898 | admin@gmail.com | |
| 81116 | Dark | m | 3 | sd08@gmail.com | Edit |
| 81117 | Shivani | Pingili | 09573642468 | piddy234@gmail.com | Edit |
| 81118 | Pingili | Reddy | 09573125879 | pingilishivanireddy234@gmail.com | Edit |
| 81119 | Pingili | Reddy | 09573125879 | pingilishivanireddy234@gmail.com | Edit |
| 81120 | y | e | 4567 | eya27@gmail.com | Edit |
| 81121 | abc123 | abc123 | 9393277588 | abc@gmail.com | Edit |
| 81122 | HARRY | HARRY | 9746657688 | abc@gmail.com | Edit |

Total Records Count: 8

Step 3: Click on Add new contact button and fill details as First name= [CS](http://www.mu.ac.in) Last Name
Mobile no Email address

Editor | Personal Contacts Manager v1.0

[Back to Dashboard](#)

First Name

Last Name

Mobile No

Email

[Save Changes](#)

| Dashboard Personal Contacts Manager v1.0 | | | | | |
|--|----------------------|-----------|-------------|----------------------------------|----------------------|
| Add New Contact | | | | Log Out | |
| ID | First Name | Last Name | Mobile No | Email | Actions |
| 1 | mynams | jenefry | 9898989898 | admin@gmail.com | |
| 81116 | Dark | m | 3 | sd08@gmail.com | Edit |
| 81117 | Shivani | Pingili | 09573642468 | piddy234@gmail.com | Edit |
| 81118 | Pingili | Reddy | 09573125879 | pingilishivanireddy234@gmail.com | Edit |
| 81119 | Pingili | Reddy | 09573125879 | pingilishivanireddy234@gmail.com | Edit |
| 81120 | y | e | 4567 | eya27@gmail.com | Edit |
| 81121 | abc123 | abc123 | 9393277588 | abc@gmail.com | Edit |
| 81122 | HARRY | HARRY | 9746657688 | abc@gmail.com | Edit |
| 81123 | abc123 | abc123 | 9999999999 | abc@gmail.com | Edit |
| 81124 | abc123 | abc123 | 9999999999 | abc@gmail.com | Edit |
| 81125 | CS | L | 7895462310 | sdbf@yahoo.com | Edit |
| Total Records Count: 11 | | | | | |

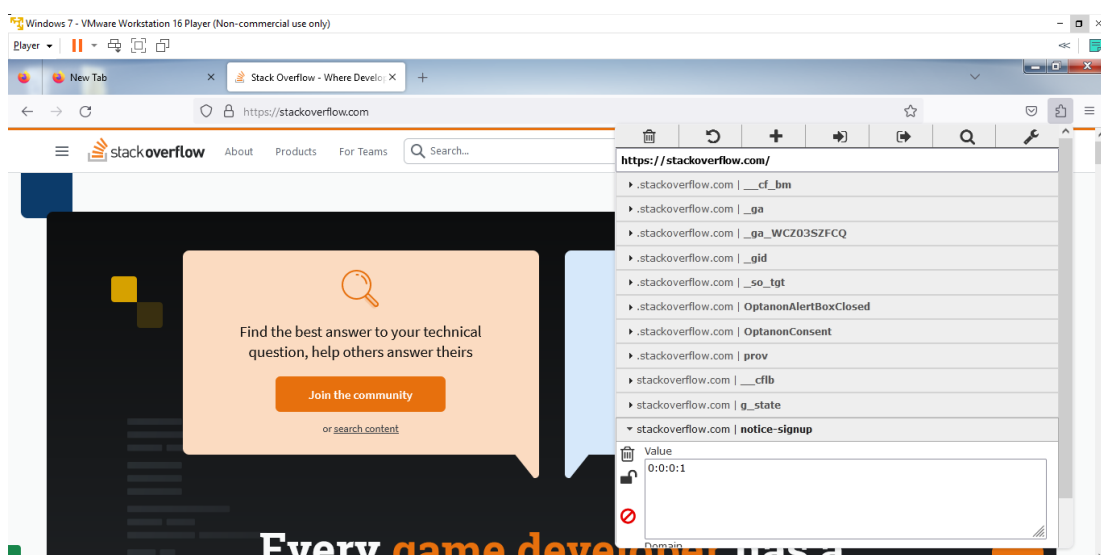
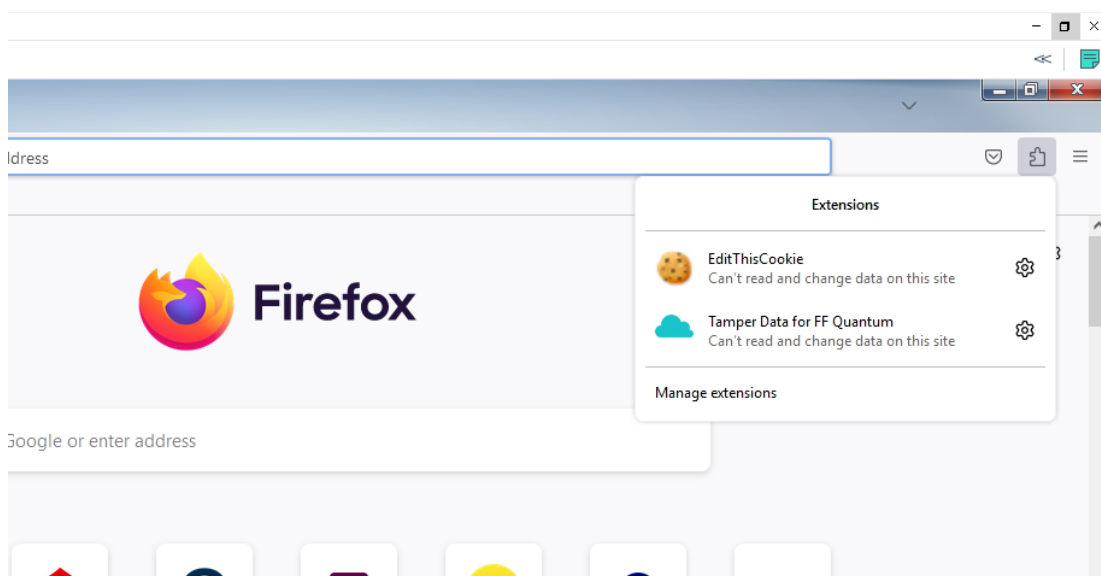
PRACTICAL NO. 7

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

A] Session Impersonation

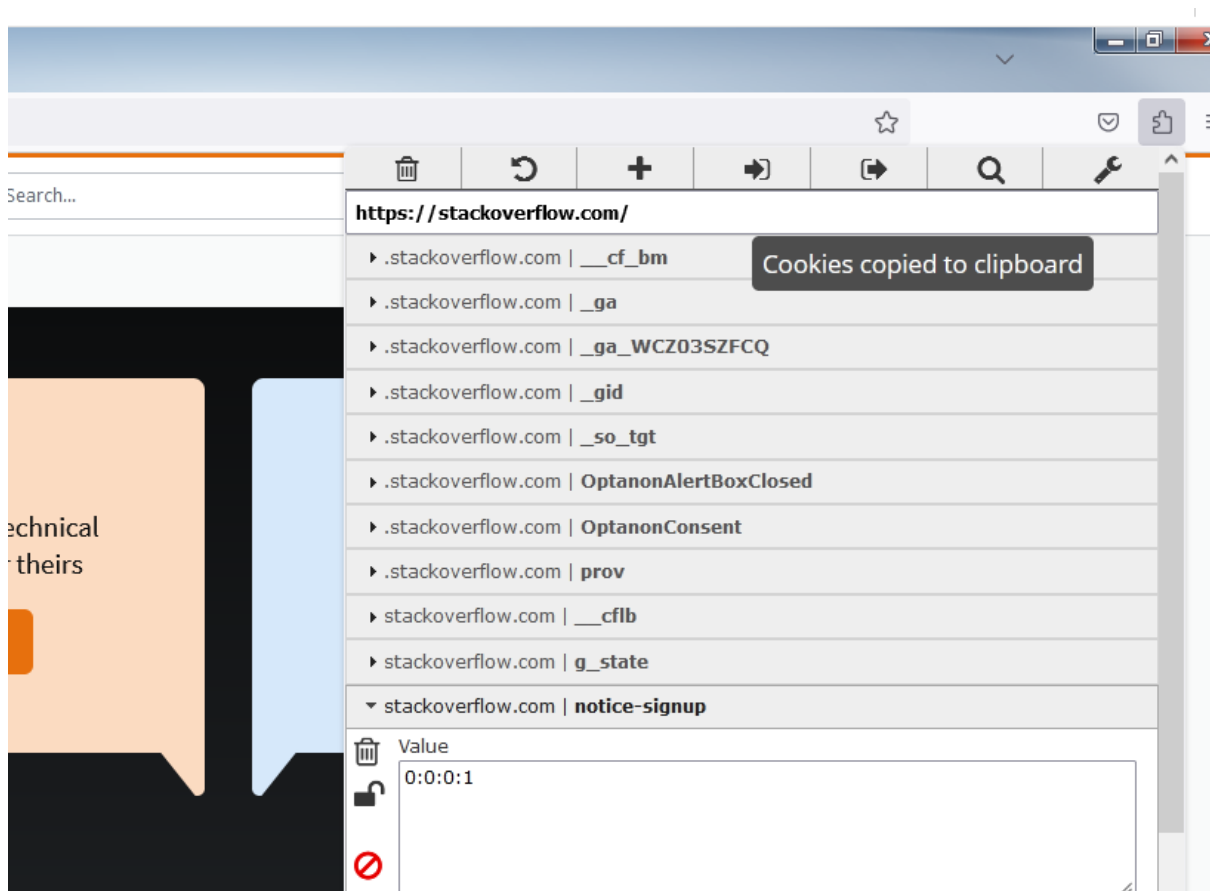
STEPS

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



Logout from the webpage once the cookie got exported

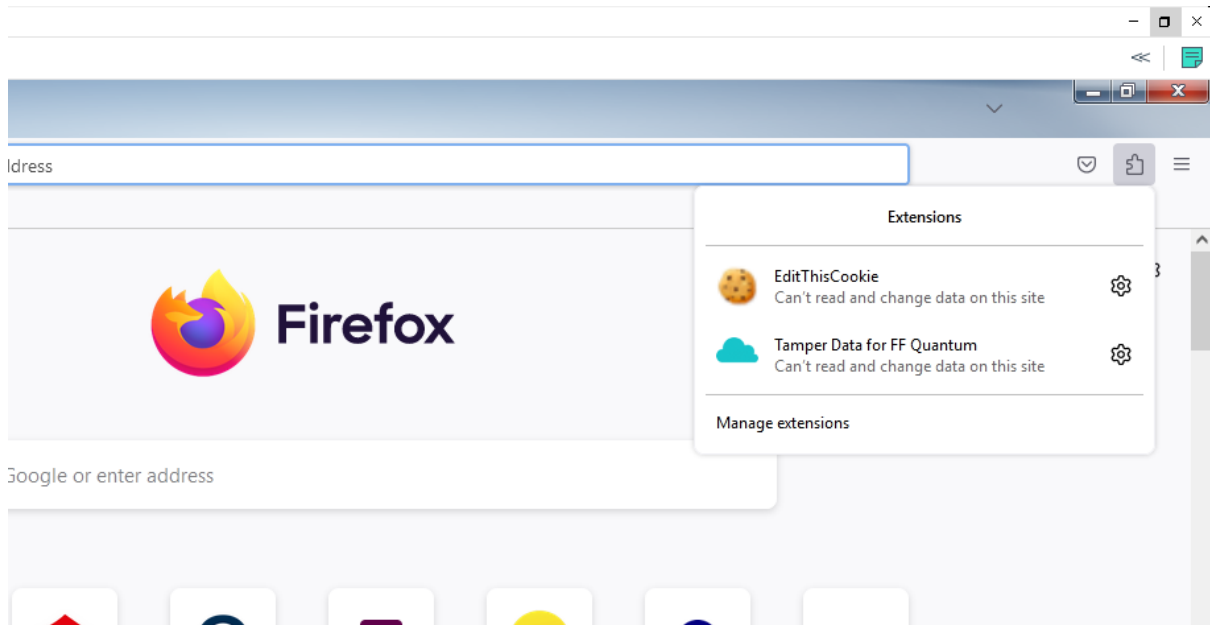
Paste the cookie in the tool which you have exported and click on green tick



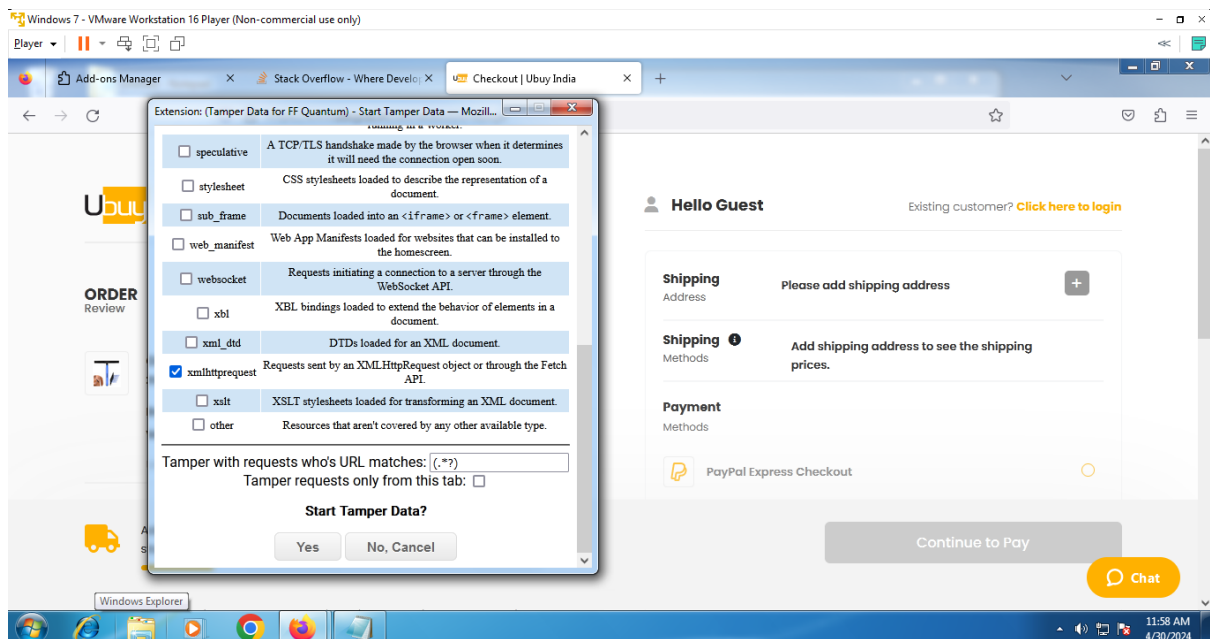
```
File Edit Format View Help
{"id": 9
},
{
  "name": "g_state",
  "value": "{\"i_p\":\"1714465093751\",\"i_l\":\"1\"}",
  "domain": "stackoverflow.com",
  "hostonly": true,
  "path": "/",
  "secure": false,
  "httponly": false,
  "sameSite": "no_restriction",
  "session": false,
  "firstPartyDomain": "",
  "partitionKey": null,
  "expirationDate": 1730009893,
  "storeId": "firefox-default",
  "id": 10
},
{
  "name": "notice-signup",
  "value": "0:0:0:1",
  "domain": "stackoverflow.com",
  "hostonly": true,
  "path": "/",
  "secure": false,
  "httponly": false,
  "sameSite": "no_restriction",
  "session": true,
  "firstPartyDomain": "",
  "partitionKey": null,
  "storeId": "firefox-default",
  "id": 11
}
}
```

Tamper DATA add-on

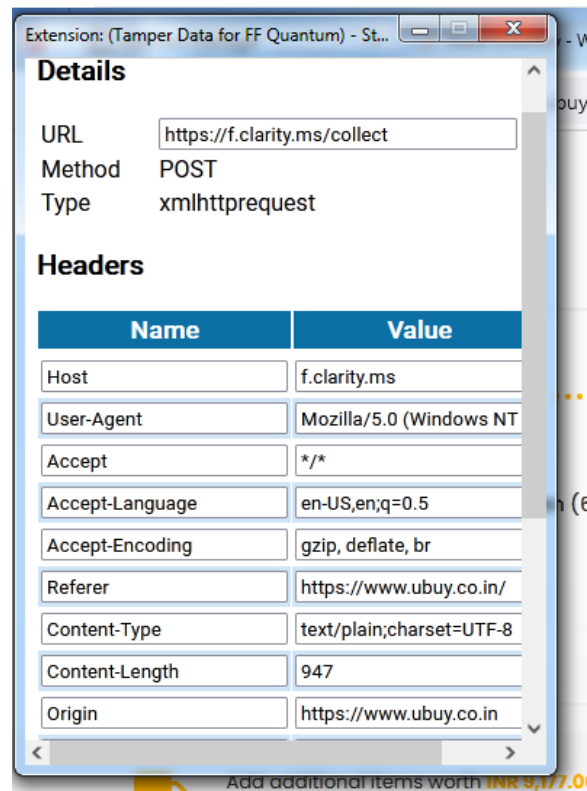
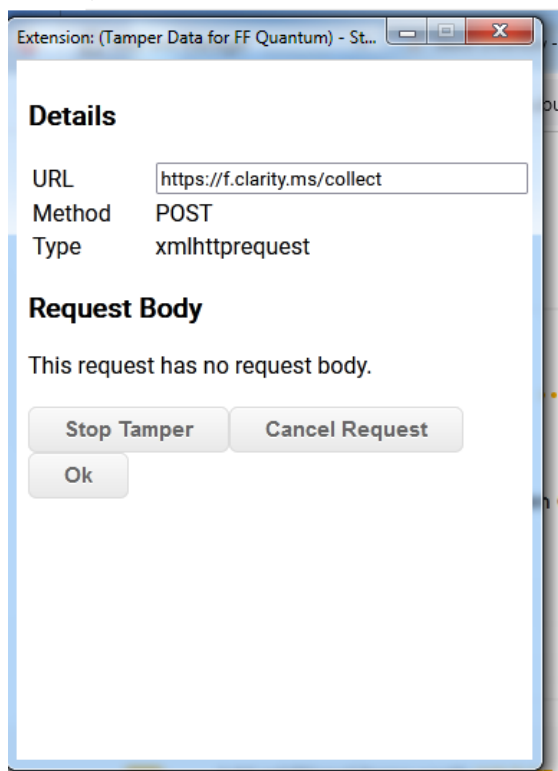
1. Open FireFox
2. Go to Tools > Addons > Extension
3. Search and install Temper Data Select a website for tempering data e.g(razorba)



Select any item to but Then Click to add cart Then Click on tool for tempering Data



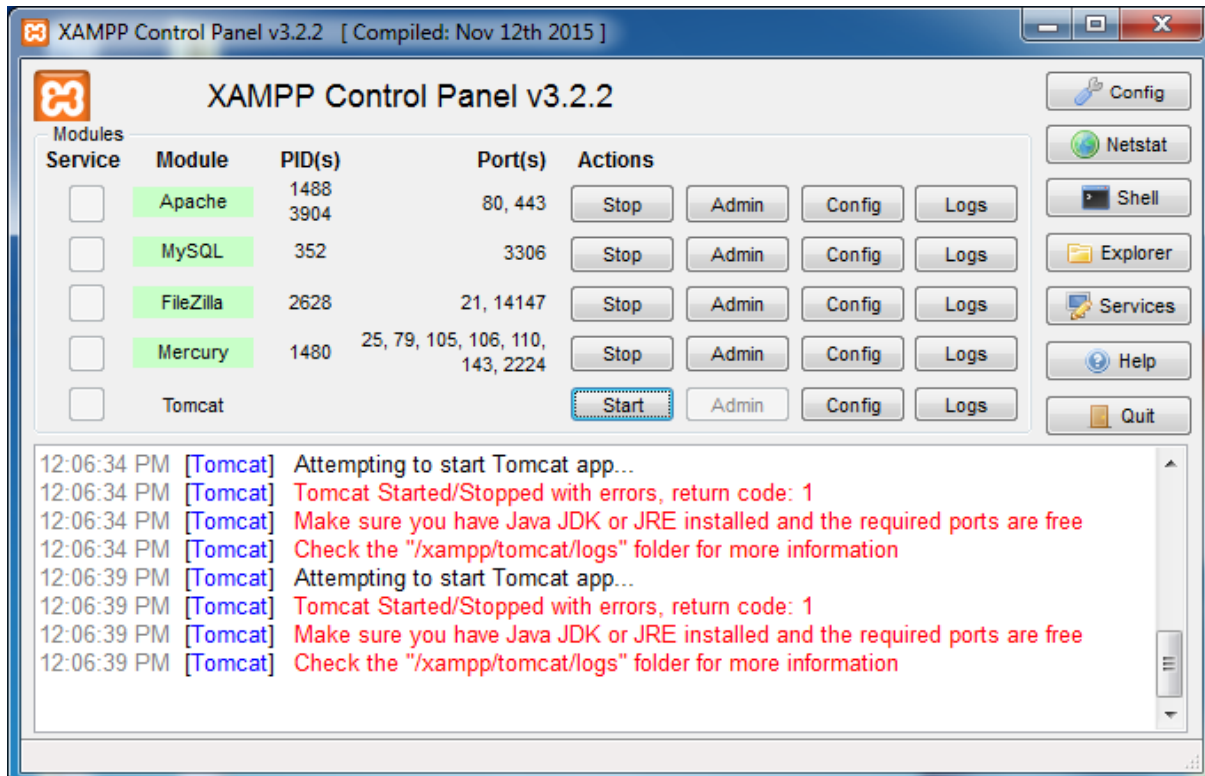
Then Start tempering the data Here you go



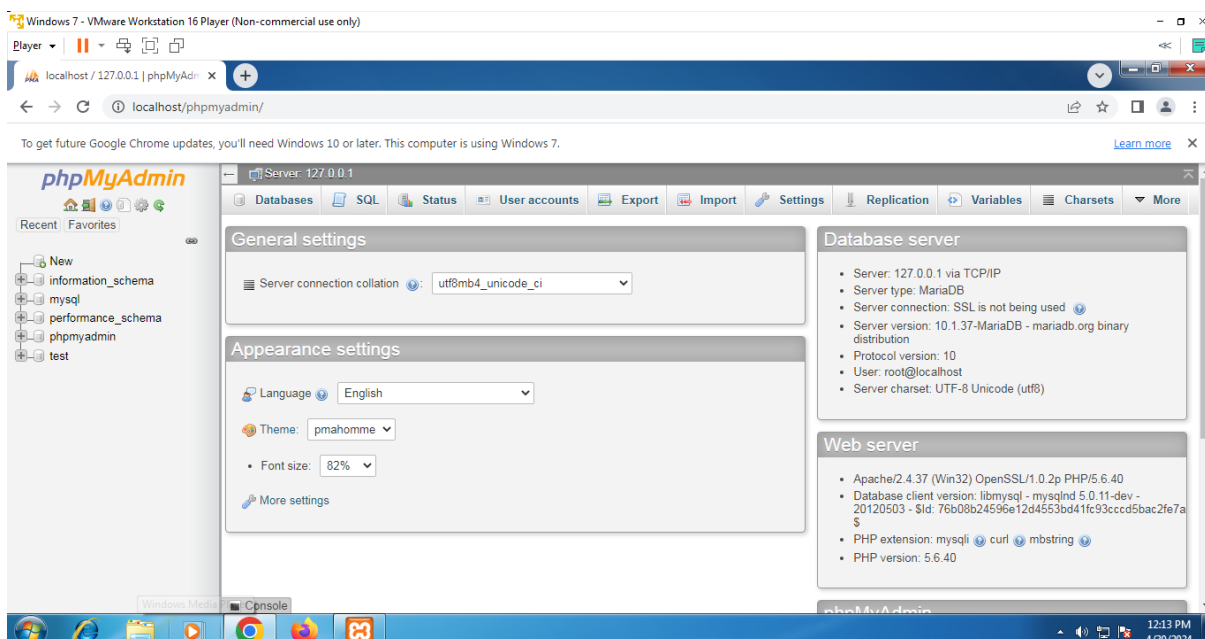
PRACTICAL NO. 8

AIM: Perform SQL injection attack.

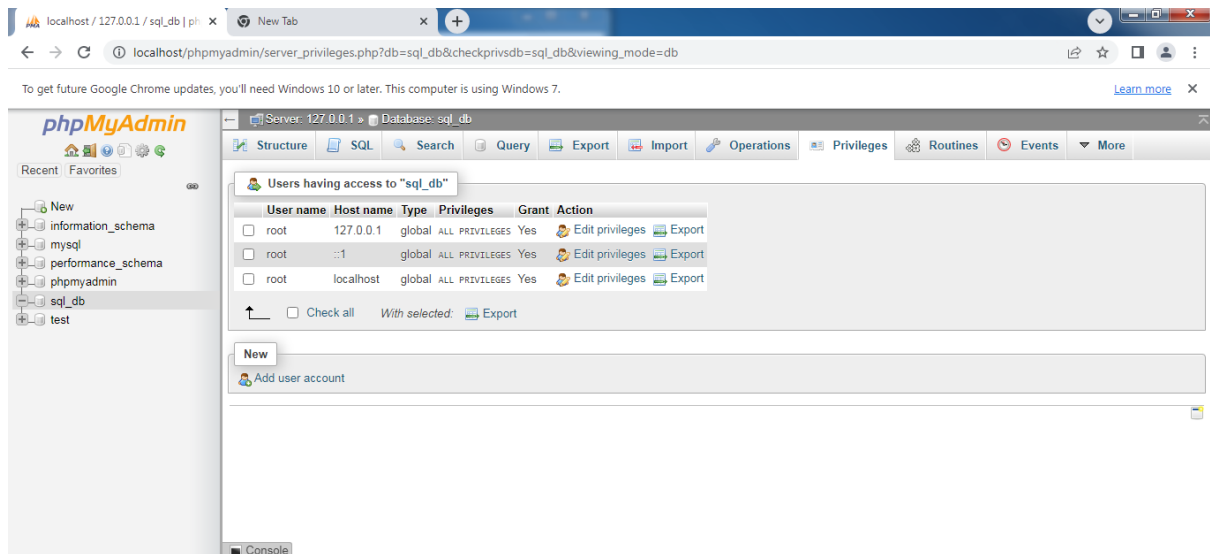
Step 1 : Open XAMPP and start apache and mysql.



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

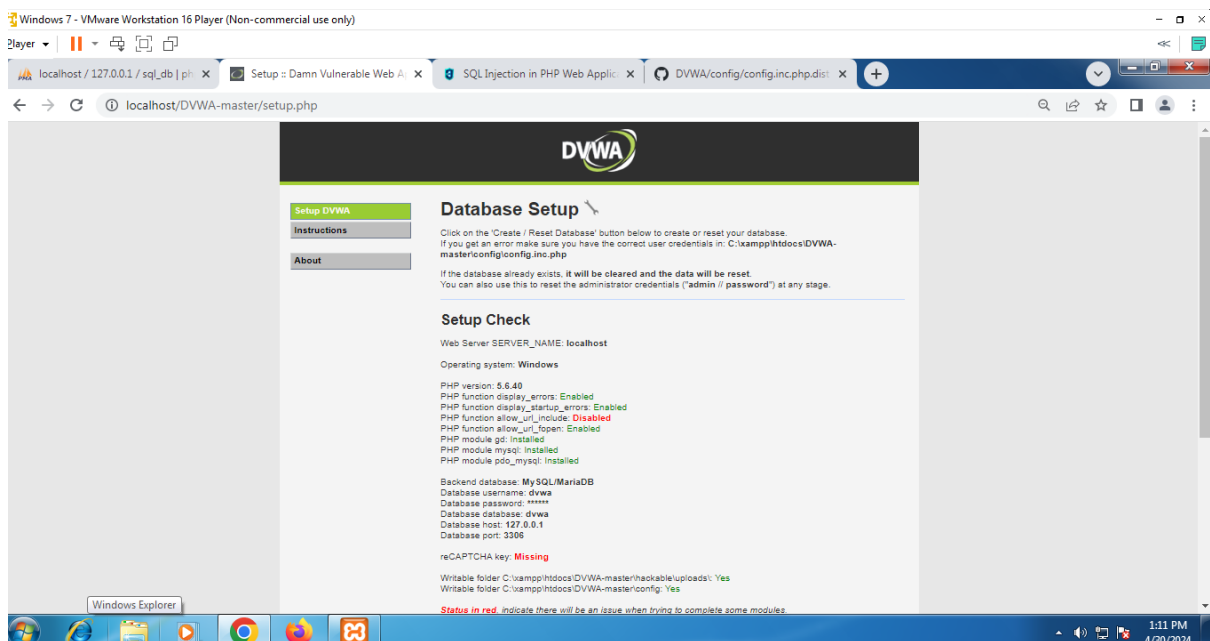


Step 3 : Create database with name sql_db.



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

Download the DVWA setup from github and change the config.inc.php.dist to config.inc.php in the config



Step 5 : Go to login.php and login using admin and .

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.