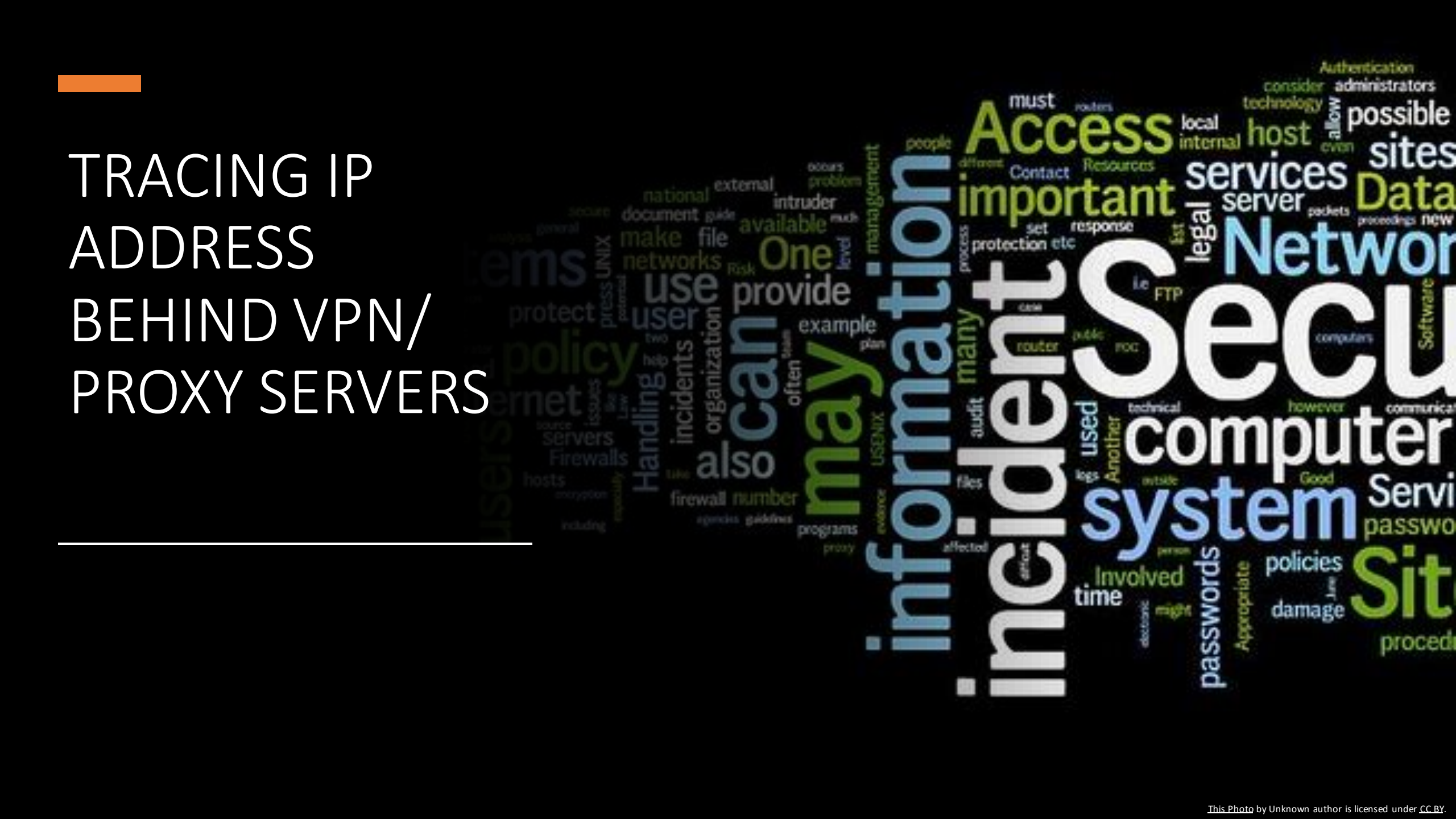
TRACING IP ADDRESS BEHIND VPN/ PROXY SERVERS



This Photo by Unknown author is licensed under CC BY.

Solution By:
CyberDominators
PSID: INTL-CCR-12:
Team Leader Name:
Shreyansh Dadheech

Team Slide

MANTHAN
राष्ट्रीय सुरक्षा सर्वोपरि

Azadi Ka Amrit Mahotsav

Divya Bhanushali

Shreyansh Dadheech

Shubhanshu Bhagat

Idea Introduction

Tracking actual IP behind VPNs

Tech Stack
1. python
2. bash
3. linux

Any Third Party API/Services used
1. getipintel

Find actual IP addresses for legal purposes

VPNs provide people anonymous access to internet but is often used for wrong means. Being able to track actual IP addresses will not only reduce cybercrimes but also make the world of internet safer

Your Approach Towards Idea

MANTHAN
राष्ट्रीय सुरक्षा सर्वोपरि

Azadi Ka Amrit Mahotsav

Narrowing down the possibilities of ip addresses used.

Finding out the type of IP used and classifying in into classes

Any functional requirement in further development ?

Data Mining to find actual IP from large data of logs

Input

- This python script takes IP as an input and detects whether it is masked using a proxy or a VPN. If masked it finds out the VPN provider

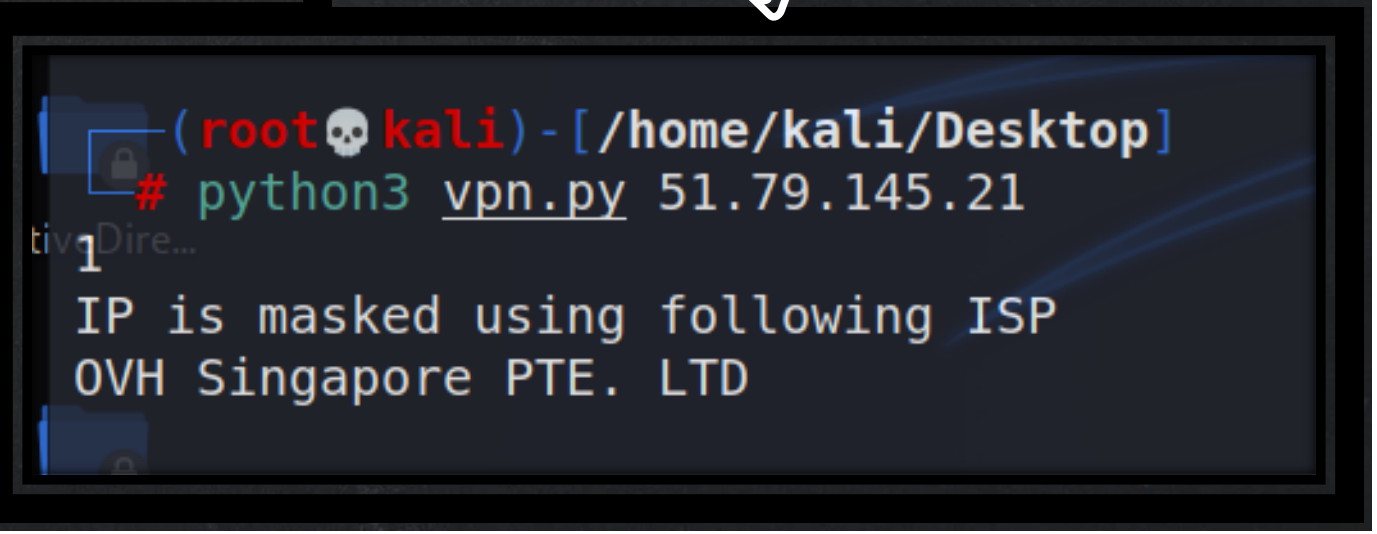
```
#!/usr/bin/env python
import requests
import sys
import os


def checkIP(ip, contactEmail):
    # change this variable to your email address

    # if probability from getIPIntel is grater than this value, return 1
    maxProbability = 0.99
    timeout = 5.00
    # if you wish to use flags or json format, edit the request below
    result = requests.get("http://check.getipintel.net/check.php?ip=" +
                          ip+"&contact="+contactEmail, timeout=timeout)
    print(result.text)
    if (result.status_code != 200) or (float(result.content) < 0):
        sys.stderr.write("An error occured while querying GetIPIntel")
    if (float(result.content) > maxProbability):
        return 1
    else:
        return 0


flag = checkIP(sys.argv[1], 'manthan@htb.in')

if flag==1:
    print("IP is masked using following ISP")
    IP = sys.argv[1]

    VPN ="""wget -q -O - whoismyisp.org/ip/{} | grep -oP -m1 '(?<=isp">).*(?=
</p)'"""
    ISP=os.popen(VPN.format(IP)).read()
    print(ISP)


else:
    print("not a masked ip")
```

OUTPUT

- The following screenshots show the implementation and the test case scenario for a normal IP and a masked IP

PUBLIC IP not masked by any vpn

NORD VPN masked IP



VPN Provider

VPN providers are supposed to log the actual IP of the machine using their servers. These logs should be kept secret but are supposed to be provided to government in any situation of crime and illegal activity.

The data provided by VPN contains actual IP of the machine which can be geolocated and the search can be narrowed down.

INFORMATION THEORY

$$\triangle S = -\log_2(x)$$

- This method can be used when using multiple VPN/TOR relay.
- The amount of info a fact gives about an entity is measured in bits.
- Entropy (S) measures information in bits.
- $\triangle S$ measures how many bits of information the fact X reveals about a target.
- Population of earth is *7714576923
- Therefore we need $\text{Log2}(1 / 7714576923) = 32.8$ bits of information to deduce the identity of a person!

Identity of a person!

https://coveryourtracks.eff.org/

Our tests indicate that you are not protected against tracking on the Web.

IS YOUR BROWSER:

Blocking tracking ads?	**No**
Blocking invisible trackers?	**No**
Protecting you from fingerprinting?	**Your browser has a unique fingerprint**

Still wondering how fingerprinting works?

LEARN MORE

Note: because tracking techniques are complex, subtle, and constantly evolving, Cover Your Tracks does not measure all forms of tracking and protection.

Your Results

Your browser fingerprint **appears to be unique** among the 227,675 tested in the past 45 days.

Currently, we estimate that your browser has a fingerprint that conveys **at least 17.8 bits of identifying information.**

The measurements we used to obtain this result are listed below. You can **read more about our methodology, statistical results, and some defenses against fingerprinting here**.

Specific info about user's browser

https://coveryourtracks.eff.org/

Headers

USER AGENT

Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.71 Safari/537.36

WHAT IS THIS?

A web header that relays information to the web server about your browser and its version.

HOW IS THIS USED IN YOUR FINGERPRINT?

This information can be very specific. *If customized* can single-handedly identify a specific user's browser.

Bits of identifying information: *9.01*
One in *x* browsers have this value: *516.27*

HTTP_ACCEPT HEADERS

text/html, */*; q=0.01 gzip, deflate, br en-IN,en-GB;q=0.9,en-US;q=0.8,en;q=0.7

Location and type of laptop

https://coveryourtracks.eff.org/

TIME ZONE

Asia/Calcutta

WHAT IS THIS?

This metric is a string which indicates your time zone, like 'America/Los_Angeles'.

HOW IS THIS USED IN YOUR FINGERPRINT?

This metric can be used to figure out your general location, especially if you live in a time zone wit
many other users.

Bits of identifying information: ***4.85***
One in x **browsers have this value:** ***28.8***

SCREEN SIZE AND COLOR DEPTH

1440x900x30

WHAT IS THIS?

The dimensions of your current browser window, and its color depth.

Canvas Fingerprint

https://coveryourtracks.eff.org/

HASH OF CANVAS FINGERPRINT

d12c83e8f7ab986c7a8e301ec89dc6c4

WHAT IS THIS?

A tracking site can perform a specific test on the HTML5 <canvas> element in your browser. This metric is the unique identification the tracker assigns to your browser after it performs this test.

Canvas fingerprinting is invisible to the user. A tracker can create a "canvas" in your browser, and generate a complicated collage of shapes, colors, and text using JavaScript. Then, with the resulting collage, the tracker extracts data about exactly how each pixel on the canvas is rendered. Many variables will affect the final result. These include your operating system, graphics card, firmware version, graphics driver version, and installed fonts.

HOW IS THIS USED IN YOUR FINGERPRINT?

This is a complex and very reliable fingerprinting metric for trackers.

Slightly different images will be rendered due to small differences in:

- video card hardware,
- video drivers,
- operating system, and
- installed fonts.

These settings are different from one computer to the next. But they tend to be consistent enough on a single machine to clearly identify a user.

Bits of identifying information: ***8.32***
One in x browsers have this value: ***320.67***

WebGL (JavaScript API)

https://coveryourtracks.eff.org/

HASH OF WEBGL FINGERPRINT

1a3e209b8a01e12cf8f50d109dbbb764

WHAT IS THIS?

WebGL is a JavaScript API for rendering interactive 2D and 3D graphics. The method for generating a “hash of WebGL fingerprint” is very similar to generating a “hash of canvas fingerprint.” Its method is to use your browser to generate graphics, extracting data from how each pixel is rendered, serialize the result, and hash it.

HOW IS THIS USED IN YOUR FINGERPRINT?

The WebGL and canvas fingerprinting results are closely linked. They both examine browser-rendered graphics for tiny differences between users.

Bits of identifying information: ***11.94***
One in x browsers have this value: ***3925.43***

WEBGL VENDOR & RENDERER

Google Inc. (Apple)~ANGLE (Apple, Apple M1, OpenGL 4.1 Metal - 71.7.1)

WHAT IS THIS?

WebGL is a library that allows browsers to render 3D graphics. As with other graphics-based tracking methods, trackers look for any tiny differences between how your device displays 3D on the web compared to other users.

HOW IS THIS USED IN YOUR FINGERPRINT?

This metric provides some level of granularity, depending on how unique your video card is. The WebGL Vendor and renderer is directly searchable using JavaScript, so trackers can access it without issue.

Additional information

https://coveryourtracks.eff.org/

HARDWARE CONCURRENCY

8

WHAT IS THIS?

This metric notes the number of CPU cores in your current machine.

HOW IS THIS USED IN YOUR FINGERPRINT?

This can provide some additional information when combined with other fingerprinting metrics, but is not identifying on its own.

Bits of identifying information: ***2.22***
One in x **browsers have this value:** ***4.65***

DEVICE MEMORY (GB)

8

WHAT IS THIS?

This metric notes the amount of memory on your current machine, rounded to the nearest gigabyte.

HOW IS THIS USED IN YOUR FINGERPRINT?

The usefulness of this metric is like hardware concurrency. It is useful when combined with other metrics, but is not identifying on its own.

Bits of identifying information: ***2.22***
One in x **browsers have this value:** ***4.66***

HOW CAN TRACKERS TRACK YOU?

Trackers use a variety of methods to identify and track users. Most often, this includes tracking cookies, but it can also include browser fingerprinting. Fingerprinting is a sneakier way to track users and makes it harder for users to regain control of their browsers. This report measures how easily trackers might be able to fingerprint your browser.

The above slides shows you how good logging in a website can help to identify the real person even if the person is using VPN/TOR to attempt cybercrime.

All the information laptop screen size , R.A.M,C.P.U cores, Unique fingerprints can be combined to reveal the identity of real person or can help to investigate a cybercrime.

Thank You!!!