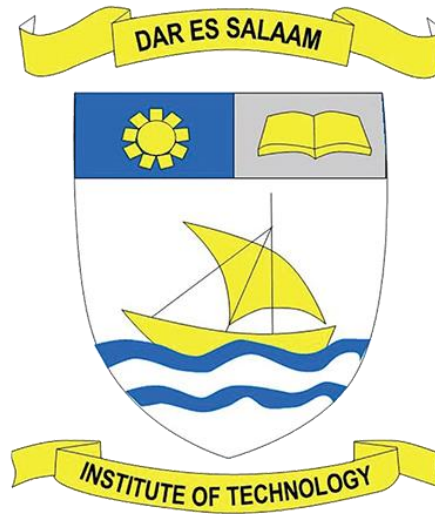


DAR ES SALAAM INSTITUTE OF TECHNOLOGY



Course: Bachelor in Computer Engineering
Class: BENG22COE-1
Module Cyber Security
Report Name Geolocation And Social Engineering Tool

Group Members

Name	Registration number
Nziku, Stephen I	220242468965
Kirumbi, Ummy H	220242475234
Hamisi, Shabilu A	220242427383
Hassan, Nasra K	220242409274

Table of Contents

1. INTRODUCTION	3
2. OBJECTIVES.....	3
3. TOOLS AND ENVIROMENT	4
3.1 Operating System	4
3.2 Geolocation Tools	4
3.3 Social Engineering Tools	4
4. GEOLOCATION TOOLS.....	5
4.1 CSI Geolocator.....	5
4.1.1 What is it.....	5
4.1.2 Procedures:.....	5
4.2 Route Converter	14
4.2.1 WHAT IS IT	14
4.2.2 Procedures.....	14
4.3 Google Map and OpenStreet map	17
4.3.1. Purpose:.....	17
4.3.2 Steps to Use:	17
4.4 WXtoImg.....	18
4.4.1 Purpose:.....	18
4.4.2 Steps to Use:	18
6. SOCIAL ENGINEERING TOOLS.....	19
6.1 HiddenEye-Legacy.....	19
6.1.1 Purpose:.....	19
6.1.2 Scenario: Creating Facebook Phishing Page	20
6.1.3 Steps to follow:	20
6.2 Storm-Breaker	24
6.2.1 Purpose:.....	24
6.2.2 Steps to Use:	24

1. INTRODUCTION

In today's digital landscape, geolocation and social engineering have become powerful tools, both for legitimate purposes and malicious activities. Geolocation tools leverage metadata, GPS coordinates, and satellite imagery to determine and analyse the physical location of objects or individuals. On the other hand, social engineering exploits human behaviour to gather sensitive information through techniques like phishing and reconnaissance.

This documentation explores the practical implementation of geolocation and social engineering tools within **CSI Linux**, a specialized operating system for Open-Source Intelligence (OSINT) and cybersecurity. Tools such as **CSI Geolocator**, **Route Converter**, and **WXtoIMG** were utilized for geolocation tasks, while tools like **Hidden Eye-Legacy** and **Storm-Breaker** were employed for simulating social engineering scenarios.

The activity provides critical insights into how attackers use publicly available tools and techniques to extract location data and manipulate targets. By understanding these methods, cybersecurity professionals can better detect, mitigate, and prevent such threats. This report outlines the tools used, their functionality, the steps performed, and the observations made during the activity.

2. OBJECTIVES

The primary objectives of this activity are:

1. To determine geolocation using metadata and coordinates.
2. To visualize and analyse GPS data using various tools.
3. To explore social engineering techniques for ethical hacking purposes.
4. To simulate reconnaissance tasks using open-source tools.

3. TOOLS AND ENVIROMENT

3.1 Operating System

- **CSI Linux** – A cybersecurity-focused operating system for OSINT tasks.

3.2 Geolocation Tools

1. **CSI Geolocator**

Extracts and determines geolocation using metadata and GPS coordinates.

2. **Route Converter**

Converts GPS route data into visual formats for easy analysis.

3. **WXtoIMG**

Decodes weather satellite images for geolocation analysis.

4. **Google Maps**

Popular tool for geolocation and route visualization.

5. **OpenStreetMap**

Open-source platform for geographic information analysis.

3.3 Social Engineering Tools

1. **HiddenEye-Legacy**

A phishing and social engineering toolkit for ethical hacking.

2. **Storm-Breaker**

Gathers IP-based geolocation and reconnaissance data

4. GEOLOCATION TOOLS

4.1 CSI Geolocator

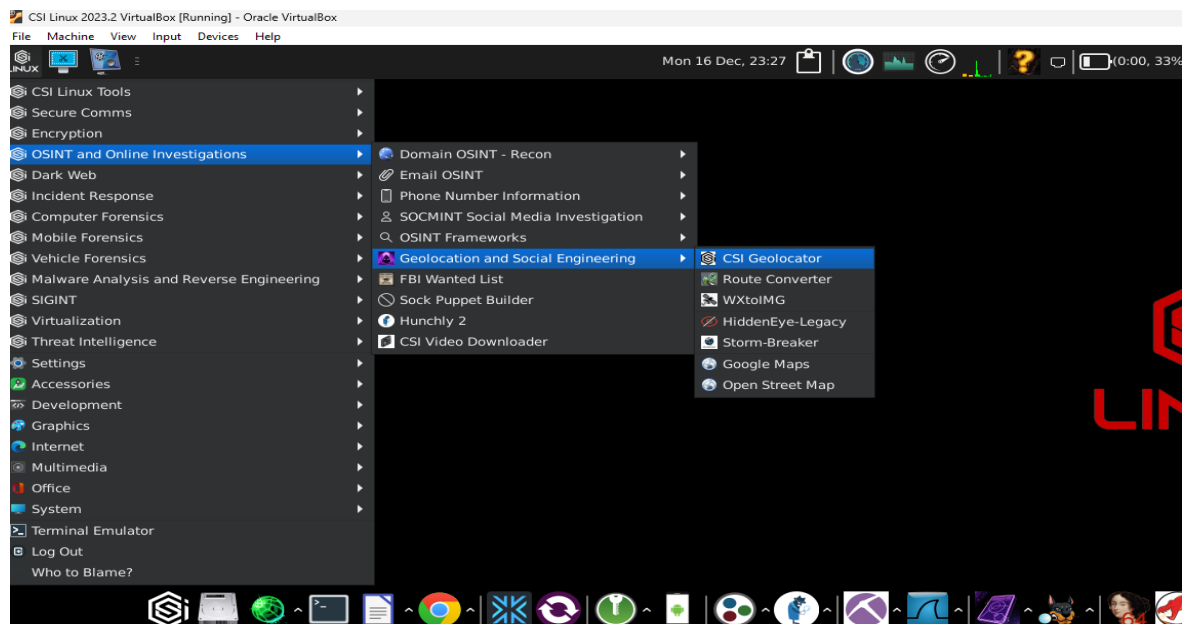
4.1.1 What is it

CSI Geolocator is a tool within CSI Linux that extracts geolocation information from various sources, such as image metadata (EXIF) or network-based location data. By integrating APIs like Wigle.net, it enables users to locate devices or networks using Wi-Fi SSIDs and MAC addresses, providing precise GPS coordinates. Also using Shodan.

Wigle.net is a platform that collects and maps wireless networks worldwide, offering APIs to retrieve geolocation data based on Wi-Fi information.

4.1.2 Procedures:

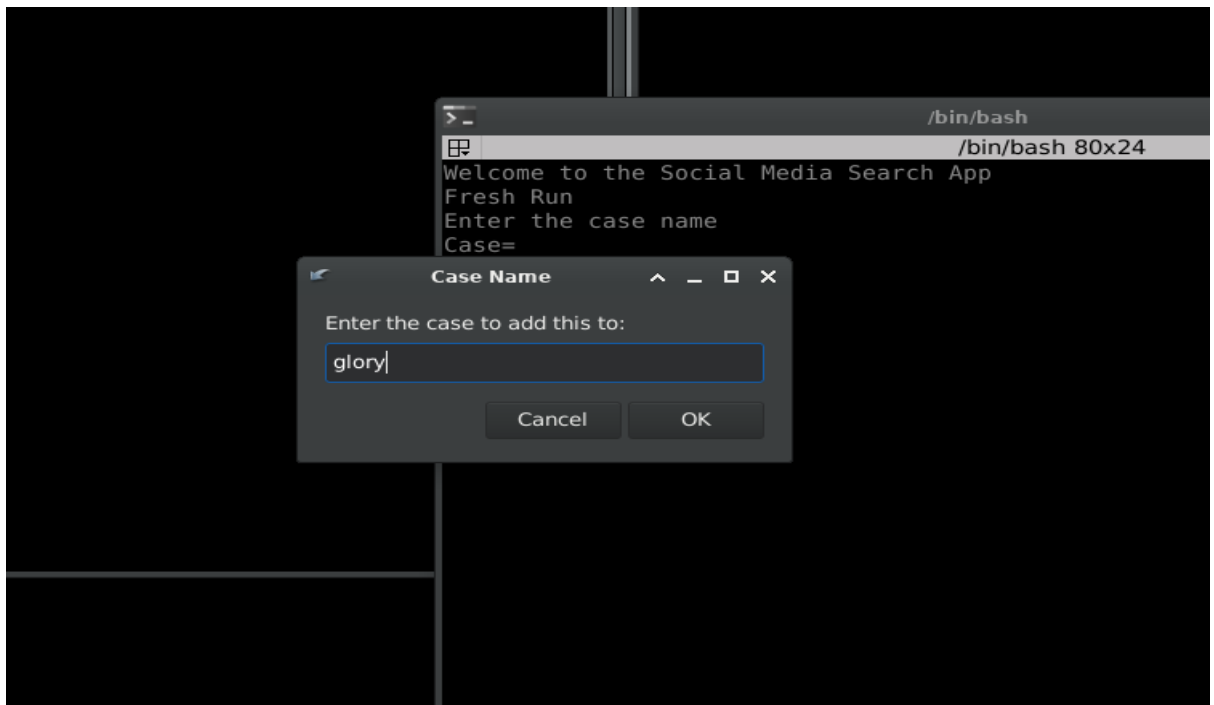
1. Open **CSI Linux** and navigate to the **Geolocation Tools** section.
2. Launch the **CSI Geolocator** tool.



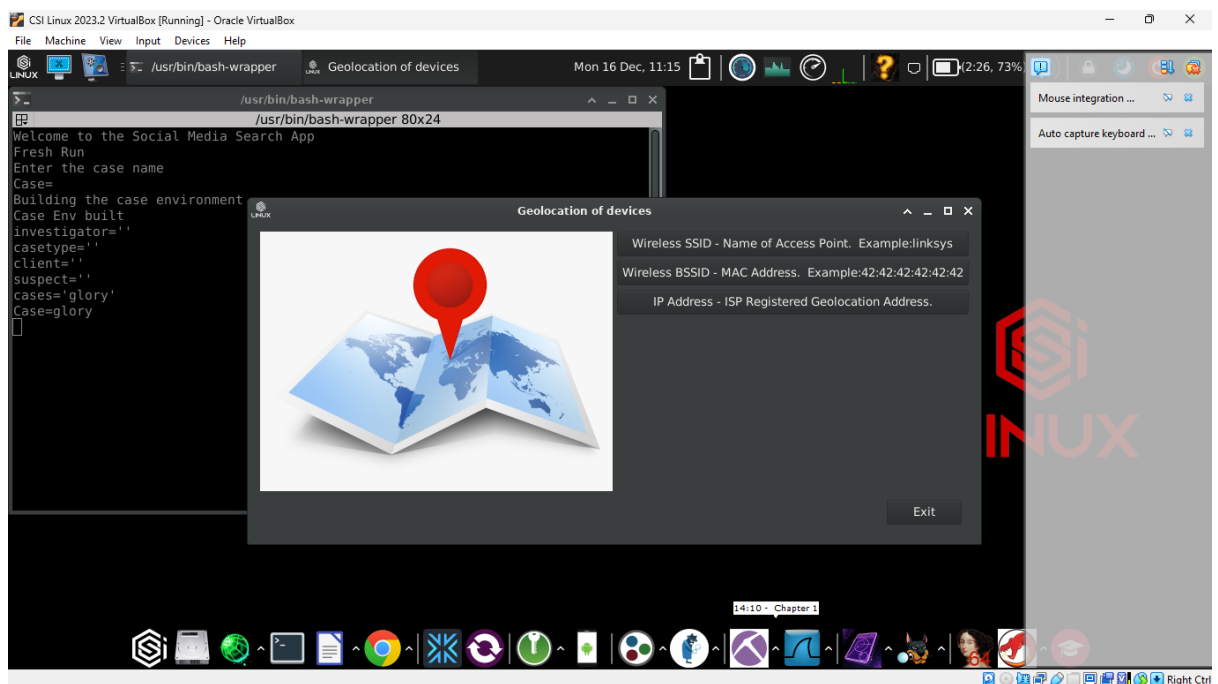
3. Enter a Case

When prompted, you need to enter a case to organize and manage the investigation data:

1. Enter a descriptive case name (e.g., "WiFi Investigation - HiddenNetwork123",glory).



2. A page will occur showing geolocation of devices using 3 ways using access point name, MAC address, ISP registered geolocation address



3. **choosing the first option wireless SSD-Name of Access point**

In this first option you are able to locate the position or location of devices using their access point names.

You are told to enter wiggles.net API, hence you need to create a wiggles.net account

Step A: Set Up API and Token from Wigle.net

1. Create an Account:

- Go to wifle.net and create an account.

The screenshot shows the 'Join WIGLE' registration form on the website. The form includes fields for First Name (glory), Last Name (hassan), E-Mail (amarasahir30@gmail.com), User Name (gloria02), Password, and Confirm Password. There is a checkbox for 'Allow WIGLE to use my points for commercial purposes?' and a CAPTCHA challenge. The background of the page shows a map of the world with various network data points.

2. Generate API Key:

- Log in and navigate to **Account Settings > API**.
- Generate an API token and copy both the **API Key** and **Token** for later use

The screenshot shows the 'Your Account' page on Wigle.net. The page displays the user's account status, including email status (unverified), query limits, and API token information. There is a 'Create my token' button and a 'Delete your account' button. The page also includes a footer with links to social media, site information, and user management.

and password in Basic authentication, you will be able to access to the API without session-based authentication. Many libraries support Basic authentication, but you can either use the "Encoded for Use" token directly below, or perform the operation manually by concatenating them as `<api user>:<api key>` and Base64 encoding the result. The encoded string must be placed in the **Authorization** HTTP Header in a string reading `Basic <encoded string>`.

You can test your credentials by placing the **API Name** and **API Token** into the `username` and `password` inputs (respectively) in the *Basic Authentication* dialog you can access by clicking the *Authorize* button in [our interactive API documentation](#). To avoid confusion during testing, we recommend that you log out, or test in a private/incognito window to ensure that you're accessing the system with your token, rather than session-based authentication as a web user.

Encoded for use:

Your Header value should be:

To test with curl:

API Name: **API Token:**

Tools

Activate WIGLE WiFi Android Device: [view QR code](#) **Delete your account:** [Delete Account](#)

SOCIAL	SITE INFORMATION	/DEV/RANDOM	USER MANAGEMENT	NEWS
WIKI	FAQ	CAFEPRESS GEAR	PASSWORD CHANGE	FORUMS
MASTODON	END-USER AGREEMENT	LINKS		NEWS RSS
BSKY	PRIVACY			STATS RSS
TWITTER	OUR TODO LIST			

Step B: Enter the name of the access point to search

File Machine View Input Devices Help

x-terminal-emulator Geolocation of dev... zenity Mon 16 Dec, 23:58

```

/bin/bash
/bin/bash 80x24
Welcome to the Social Media Search App
Fresh Run
Enter the case name
Case=
Building the case environment
Case Env built
case found
glory
Case=glory

```

Geolocation of devices

Wireless SSID - Name of Access Point. Example:linksys

Wireless BSSID - MAC Address. Example:42:42:42:42:42

ID Address - ISP Registered Geolocation Address.

Access Point Name

Enter SSID of WiFi Access Point to Search

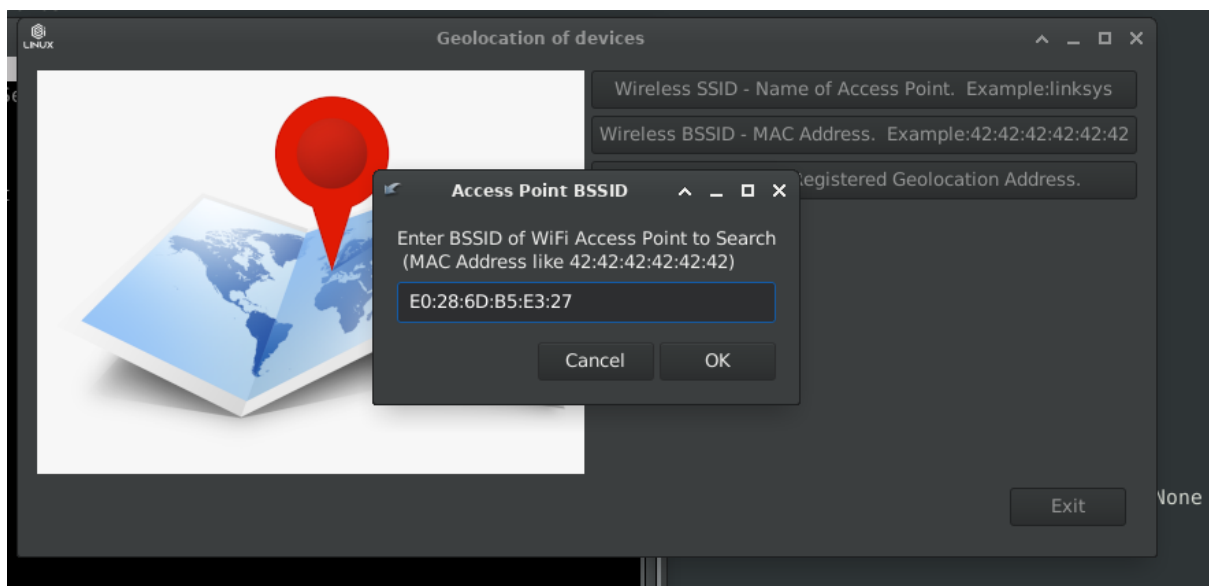
RESULT OF THE SEARCH OR THE OUTPUT


```
1 sSSID: BIG
2 BSSID|MAC Address: E0:28:6D:B5:E3:27
3 Last Seen: 2024-10-09T05:03:05.000Z
4 Latitude: -25.19680023
5 Longitude: -90.34596205
6 Google Maps Link: https://www.google.com/maps/?q=-25.19680023,-90.34596205
7 Likely Address: None None
8 None None, None None
9 ---
10 SSID: BIG
11 BSSID|MAC Address: 00:24:01:33:D6:14
12 Last Seen: 2024-01-04T02:34:52.000Z
13 Latitude: -58.56541872
14 Longitude: -98.58733892
15 Google Maps Link: https://www.google.com/maps/?q=-58.56541872,-98.58733892
16 Likely Address: None None
17 None None, None None
18 ---
19 SSID: BIG
20 Last Seen: 2020-06-09T00:07:11.000Z
21 Latitude: 17.67638683
22 Longitude: 35.88525295
23 Google Maps Link: https://www.google.com/maps/?q=17.67638683,35.88525295
24 Likely Address: None None
25 ---
26 SSID: BIG
27 BSSID|MAC Address: DE:CB:AC:A4:78:2D
28 Last Seen: 2012-08-24T06:48:40.000Z
29 Latitude: 26.59327984
30 Longitude: 62.5722456
```

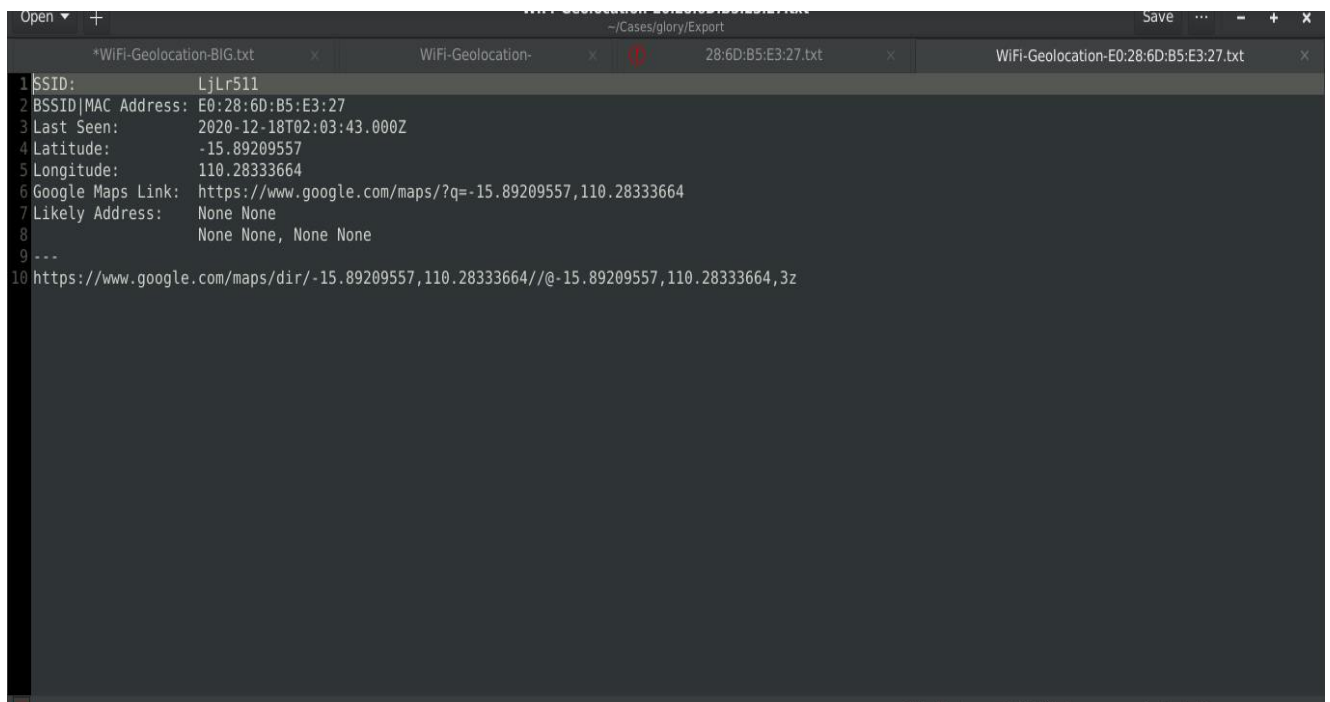
As you can see in the output we are able to get MAC address, last seen, latitude and longitude of BIG location, Google maps link. Now we can use google maps to find the location of BIG.

Step 5: Choosing the second option wireless BSSID-MAC ADDRESS

Here you need to enter the MAC-ADDRESS of the device in order to locate the location of the device.



And the result is shown as the following:

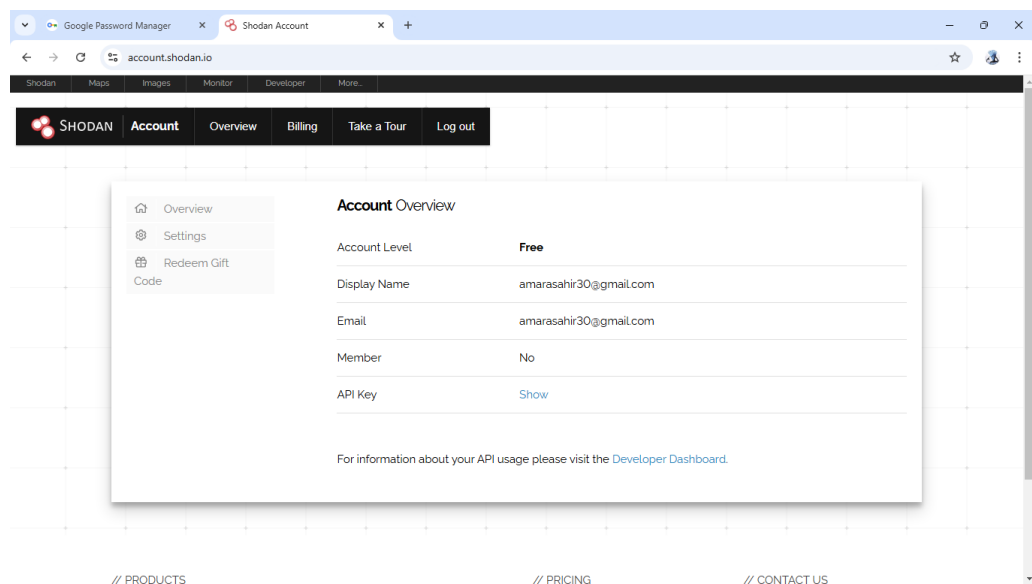
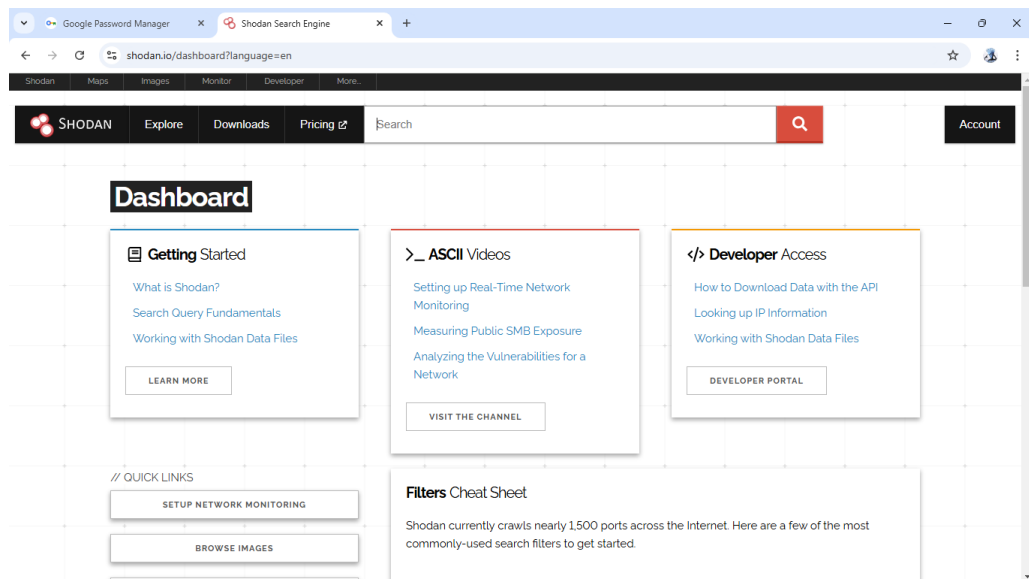


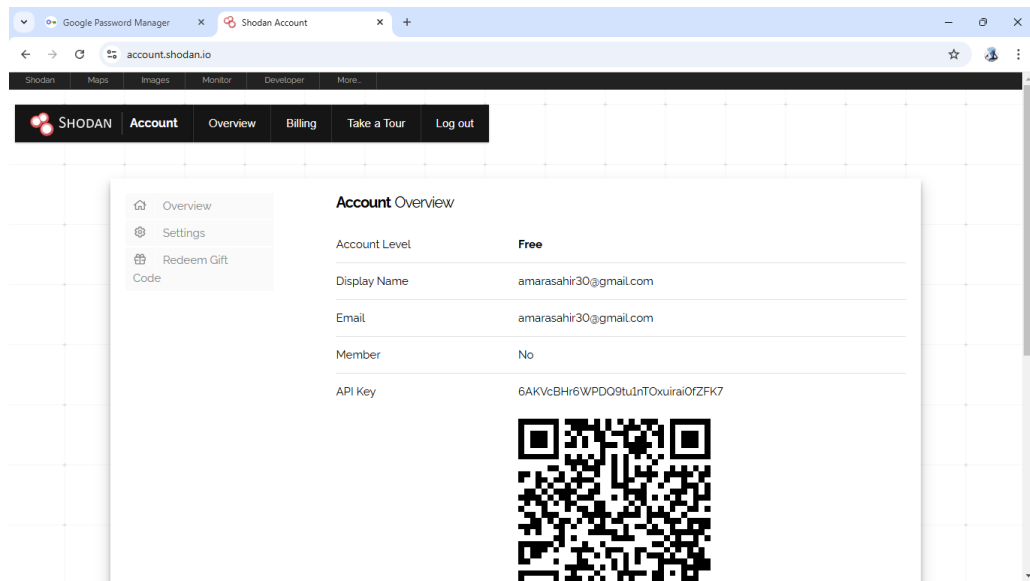
The image shows a text editor window with a dark theme. The title bar indicates the file path is ~/Cases/glory/Export. The editor contains a list of geolocation data for a WiFi network. The data is as follows:

Line	Field	Value
1	SSID:	LjLr511
2	BSSID MAC Address:	E0:28:6D:B5:E3:27
3	Last Seen:	2020-12-18T02:03:43.000Z
4	Latitude:	-15.89209557
5	Longitude:	110.28333664
6	Google Maps Link:	https://www.google.com/maps/?q=-15.89209557,110.28333664
7	Likely Address:	None None
8		None None, None None
9	---	
10		https://www.google.com/maps/dir/-15.89209557,110.28333664/@-15.89209557,110.28333664,3z

Step 6: choosing the third option IP Address- ISP Registered Geolocation Address

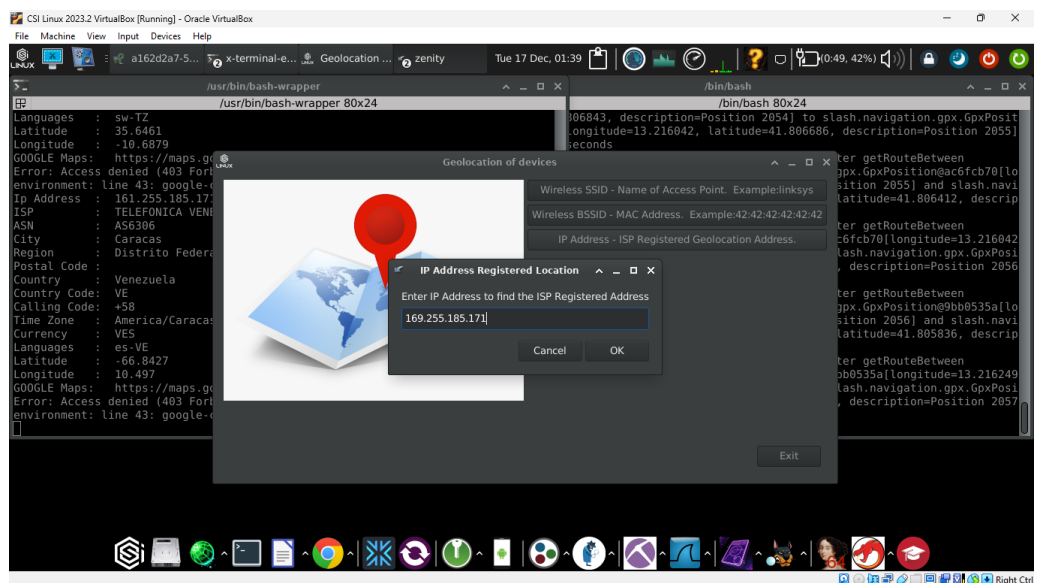
1. First of all, we create shodan account through shodan.io in order to get API key to connect with the tools in the tool



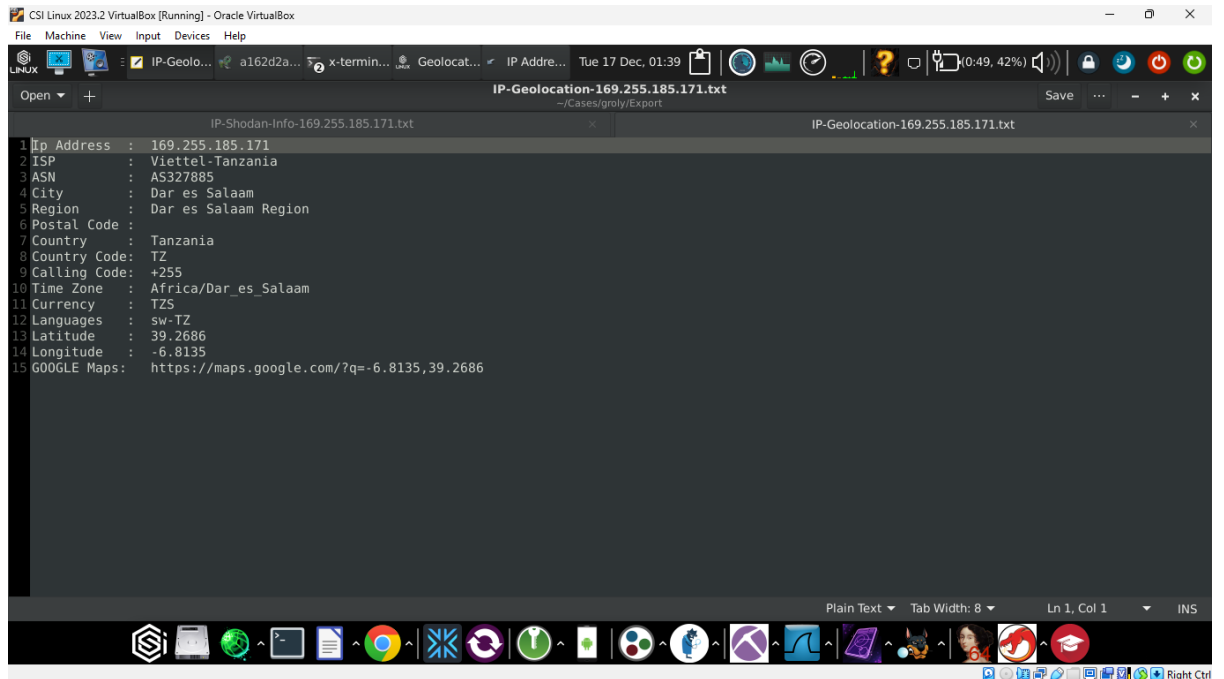


Then we use the API key to connect tool with shodan the we can continue to use the tools as follows

1. Write IP address of the target



2. Then result will appear by showing the ip address, isp ,city region country code and geolocation



The screenshot shows a Linux terminal window titled "CSI Linux 2023.2 VirtualBox [Running] - Oracle VirtualBox". The terminal displays the output of an IP geolocation tool for the IP address 169.255.185.171. The results are as follows:

```
1 IP Address : 169.255.185.171
2 ISP       : Viettel-Tanzania
3 ASN       : AS327885
4 City      : Dar es Salaam
5 Region    : Dar es Salaam Region
6 Postal Code :
7 Country   : Tanzania
8 Country Code: TZ
9 Calling Code: +255
10 Time Zone : Africa/Dar_es_Salaam
11 Currency  : TZS
12 Languages : sw-TZ
13 Latitude  : 39.2686
14 Longitude : -6.8135
15 G00GLE Maps: https://maps.google.com/?q=-6.8135,39.2686
```

Therefore, from the tools above we can get geolocation of data that can help to now the movement of device. It can help in forensics investigation.

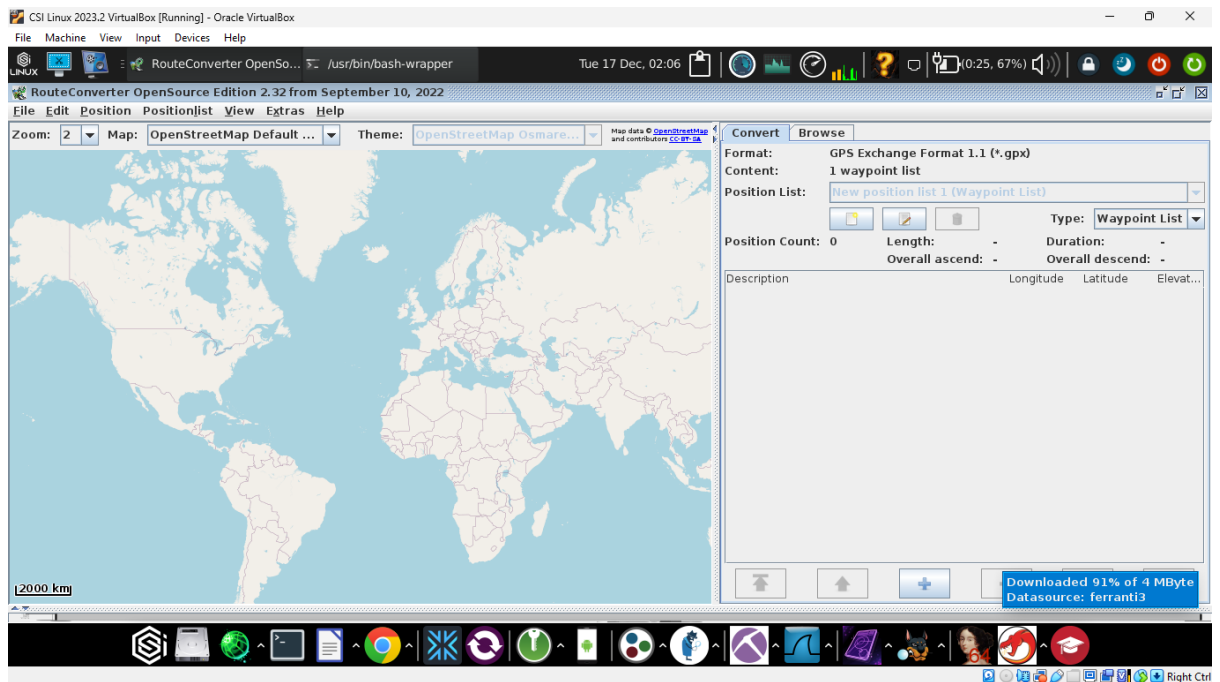
4.2 Route Converter

4.2.1 WHAT IS IT

Route Converter is a geolocation tool used for converting, editing, and visualizing GPS route data. It supports a wide range of file formats (e.g., GPX, KML, KMZ, NMEA) and helps users transform raw GPS data into a visually meaningful format. This tool is particularly useful for analysing travel paths, mapping routes, and converting between different geospatial formats.

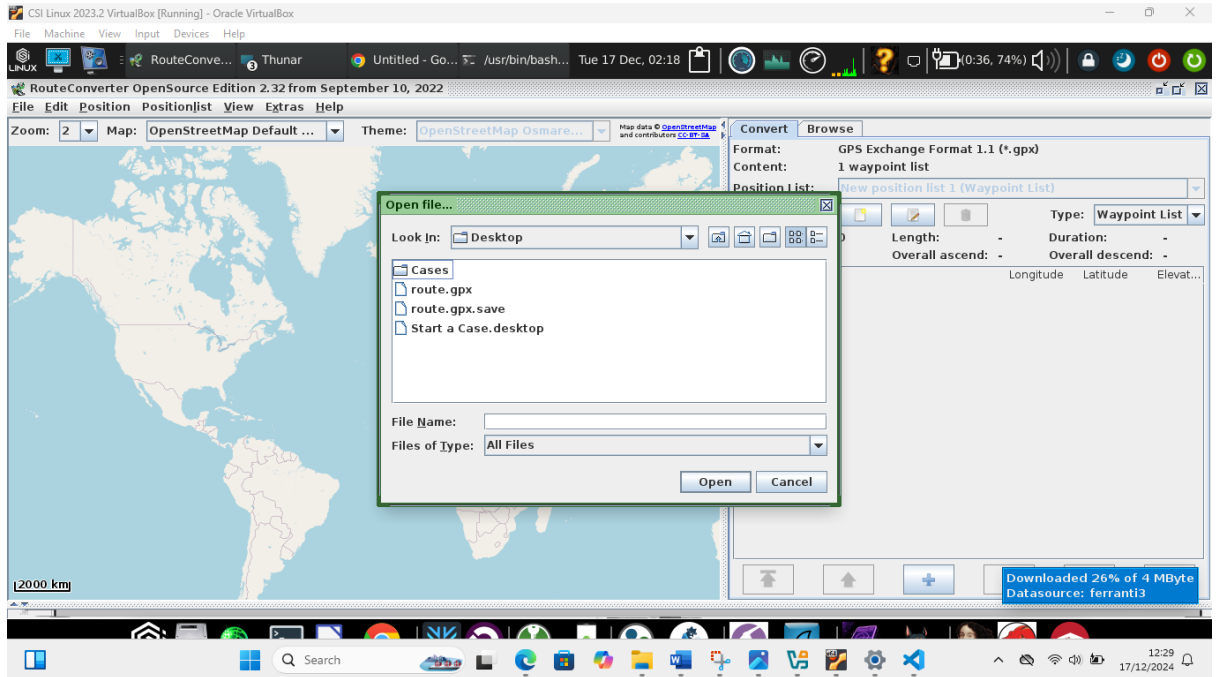
4.2.2 Procedures

Step 1: Launch Route Converter

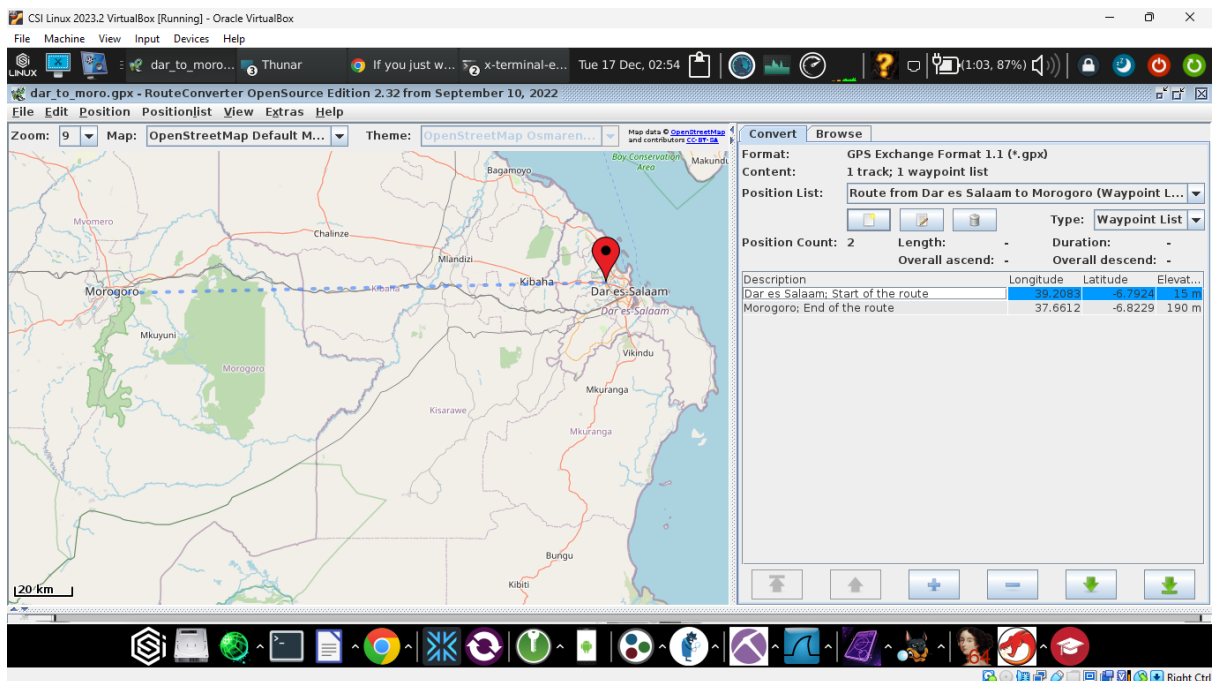


Step 2: Import GPS Route Data

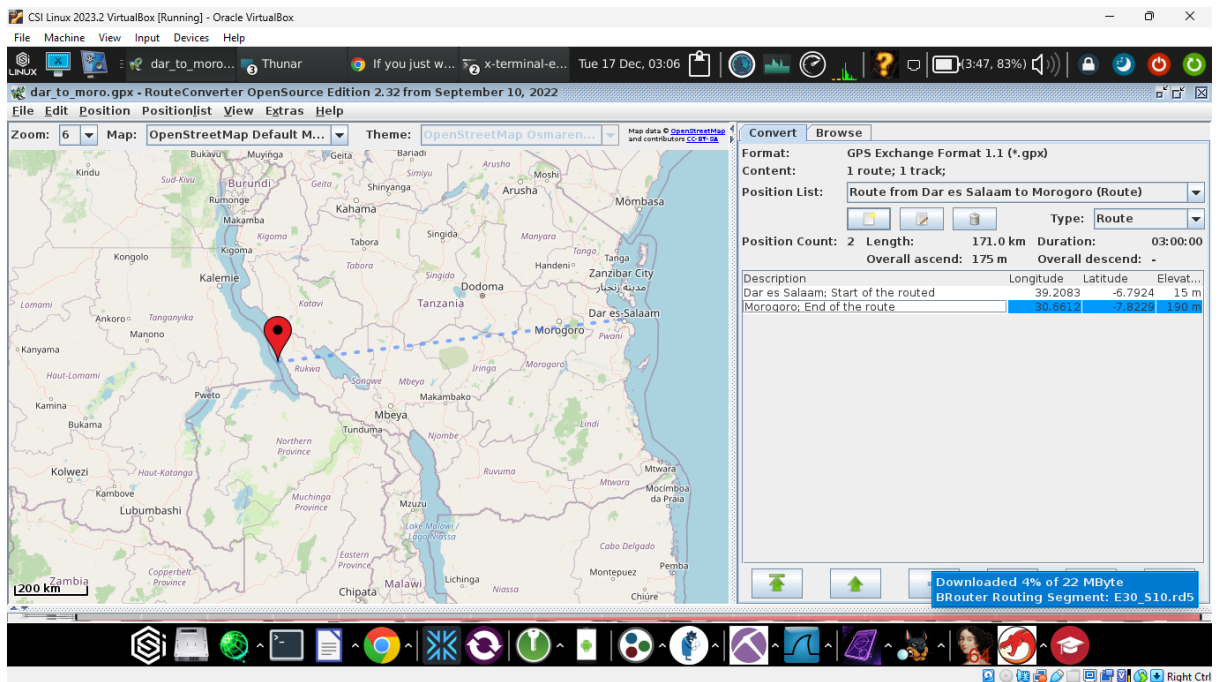
1. Click on "**Open**" or "**Load File**" to import GPS data.
2. Choose a compatible file format such as:
 - **GPX** (GPS Exchange Format)
 - **KML/KMZ** (Google Earth files)
 - **NMEA** (Raw GPS data logs)
3. Browse to the file location and load the GPS route data.



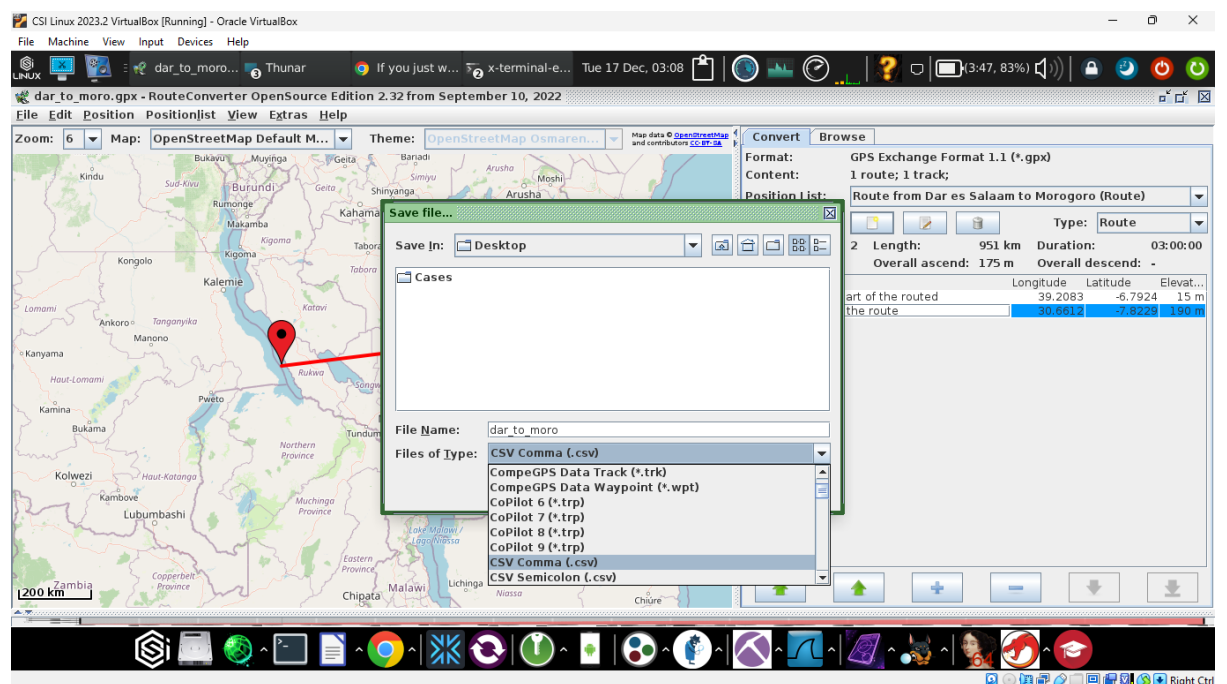
4. Convert the Route: After loading the route



5. After route being converted



6. Save the converted file to your preferred location.



4.3 Google Map and OpenStreet map

4.3.1. Purpose:

Primary mapping services for manual geolocation and route planning.

4.3.2 Steps to Use:

1. **Access Google Maps:**
 - Open a browser and visit [Google Maps](#).
 - Use satellite view and street view for detailed investigation.
2. **Use OpenStreet Map:**
 - Visit [OpenStreet Map](#).
 - Utilize the "Edit" feature to analyze geographic data.
3. **Search for Data:**
 - Input coordinates, addresses, or landmarks for detailed mapping.
4. **Export Data:**
 - Save map views as images or export GPS data.
5. **Combine with Tools:**
 - Use map data in conjunction with CSI Geolocator and Route Converter for enhanced results.

4.4 WXtoImg

4.4.1 Purpose:

A software application for decoding weather satellite images from audio files.

4.4.2 Steps to Use:

1. **Install the Tool:**

- Download the WXtoImg software from its official website or CSI Linux repositories.
- Use the terminal to install:

```
sudo dpkg -i wxtoimg_*.deb  
sudo apt-get install -f
```

2. **Setup SDR (Software-Defined Radio):**

- Connect your SDR device (e.g., RTL-SDR) to your system.
- Use a compatible SDR application like GQRX or SDR# to tune into the appropriate frequency for weather satellites.

3. **Record Audio Files:**

- Record the satellite's signal as a WAV file while tuned to the correct frequency.

4. **Launch WXtoImg:**

- Open the software from the menu or terminal by typing `wxtoimg`.

5. **Decode the Signal:**

- Load the recorded WAV file into WXtoImg.
- Select a decoding mode (e.g., APT) and process the file.

6. **Analyze and Save Images:**

- View the decoded weather satellite images.
- Save them in formats like JPG or PNG for further analysis.

7. **Advanced Features:**

- Experiment with enhancement modes like false color, thermal imaging, or map overlays.

6. SOCIAL ENGINEERING TOOLS

6.1 HiddenEye-Legacy

6.1.1 Purpose:

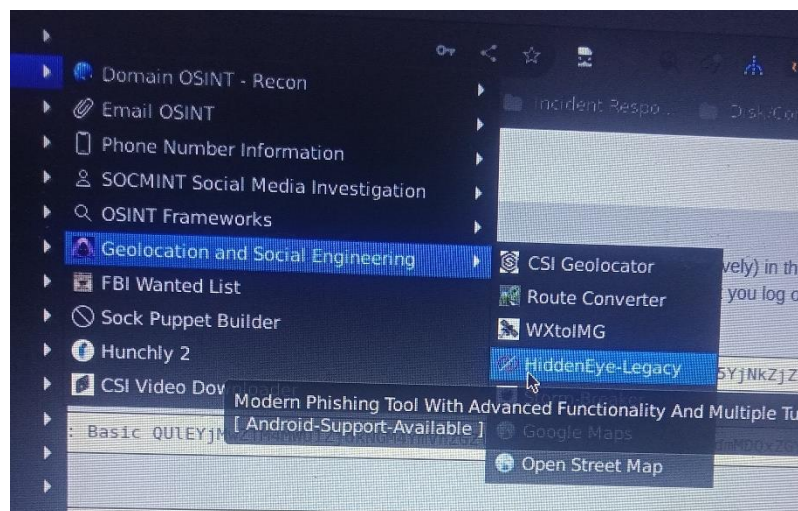
Hidden eye is social engineering tool for phishing attacks (educational and ethical hacking purposes only).

Hidden Eye is an all in one tool that can be used to perform a variety of online attacks on user accounts. It's well loaded, therefore it can be used as keylogger (keystroke logging), phishing tool, information collector, social engineering tool, etc.

As a modern phishing tool, Hidden Eye is very good at what it does. The perfect combination of all its functional components gives it an upper hand when attacking accounts. By using brute force attacks it can effectively access the user's personal information.

Hidden Eye can easily crack user passwords and can also collect other personal data belonging to the victim. Features:

Can perform live attacks (IP, geolocation, country, etc.) Captures victim's keystrokes (using keylogger function) Serveo URL type selection (selects between RANDOM URL and CUSTOM



6.1.2 Scenario: Creating Facebook Phishing Page

In this scenario, we will be creating a Facebook Phishing page. We have selected Option 1 for Facebook.

6.1.3 Steps to follow:

1. Open HiddenEye

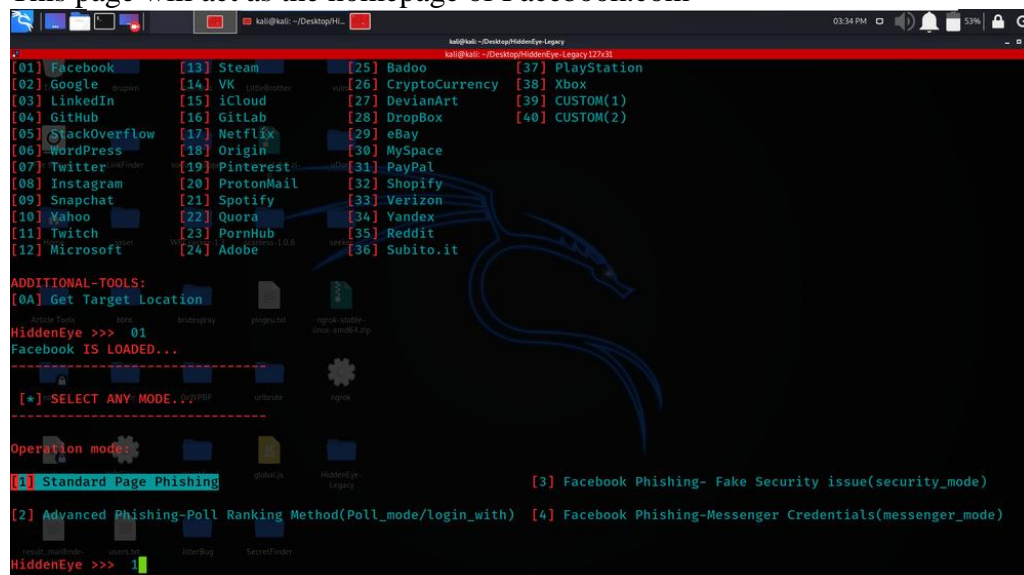
This can be done graphically by clicking HiddenEye from the tool list present in CSI Linux and it will open in terminal as shown below



2. Select option 1 for Facebook phishing Attack by typing 1 then press enter:

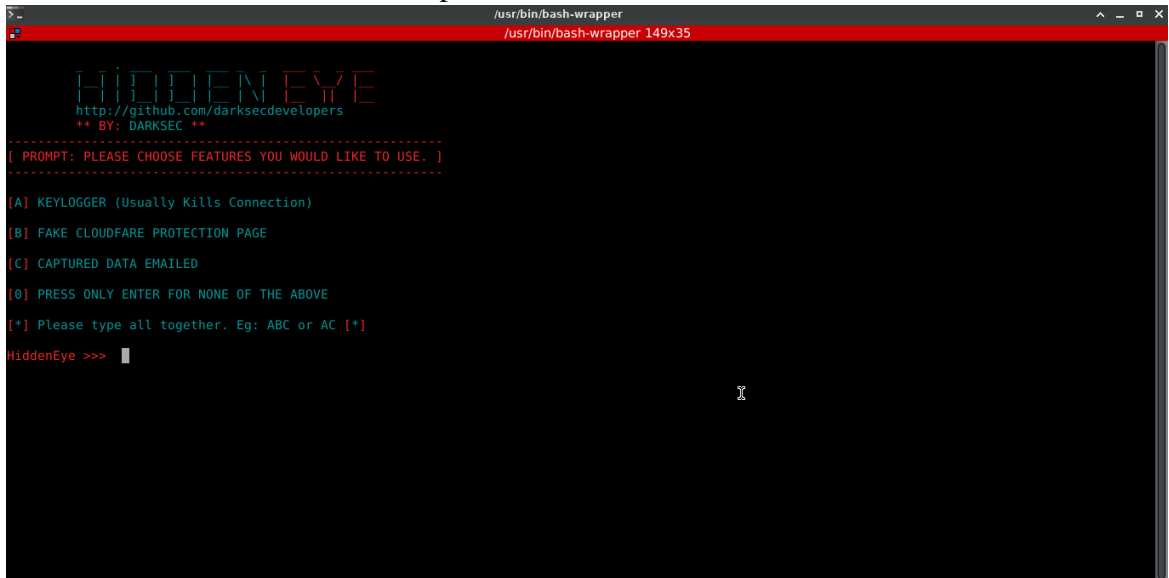
3. Select standard page:

This page will act as the homepage of Facebook.com



4. Select option B FAKE CLOUDFARE PROTECTION PAGE

This will be seen as on the below picture



```

/usr/bin/bash-wrapper
/usr/bin/bash-wrapper 149x35

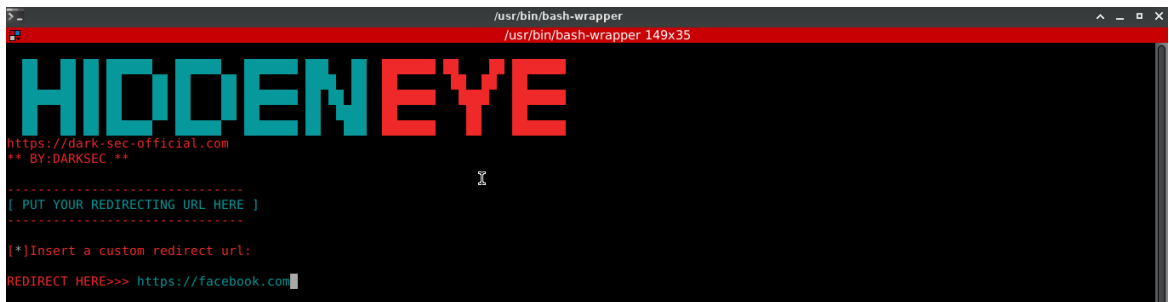
HIDDEN EYE
http://github.com/darksecdevelopers
** BY: DARKSEC **

[ PROMPT: PLEASE CHOOSE FEATURES YOU WOULD LIKE TO USE. ]

[A] KEYLOGGER (Usually Kills Connection)
[B] FAKE CLOUDFLARE PROTECTION PAGE
[C] CAPTURED DATA EMAILED
[D] PRESS ONLY ENTER FOR NONE OF THE ABOVE
[*] Please type all together. Eg: ABC or AC [*]

HiddenEye >>> 
```

5. Enter custom redirecting URL



```

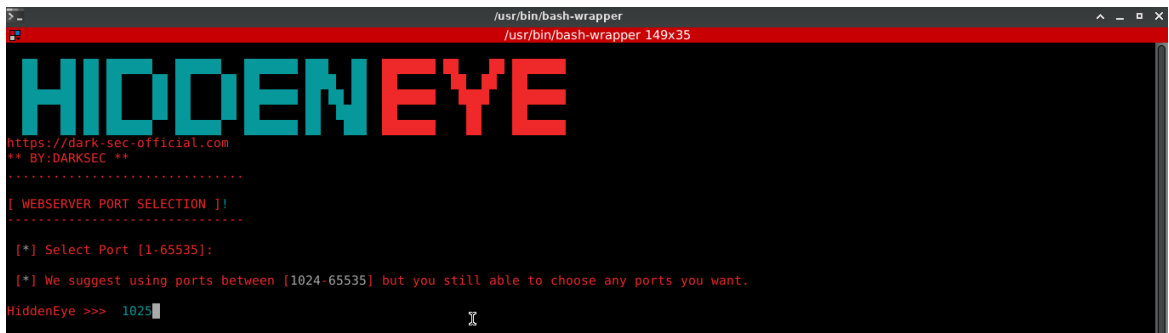
/usr/bin/bash-wrapper
/usr/bin/bash-wrapper 149x35

HIDDEN EYE
https://dark-sec-official.com
** BY: DARKSEC **

[ PUT YOUR REDIRECTING URL HERE ]

[*]Insert a custom redirect url:
REDIRECT HERE>>> https://facebook.com
```

6. Specify the port number for where the URL will be hosted



```

/usr/bin/bash-wrapper
/usr/bin/bash-wrapper 149x35

HIDDEN EYE
https://dark-sec-official.com
** BY: DARKSEC **

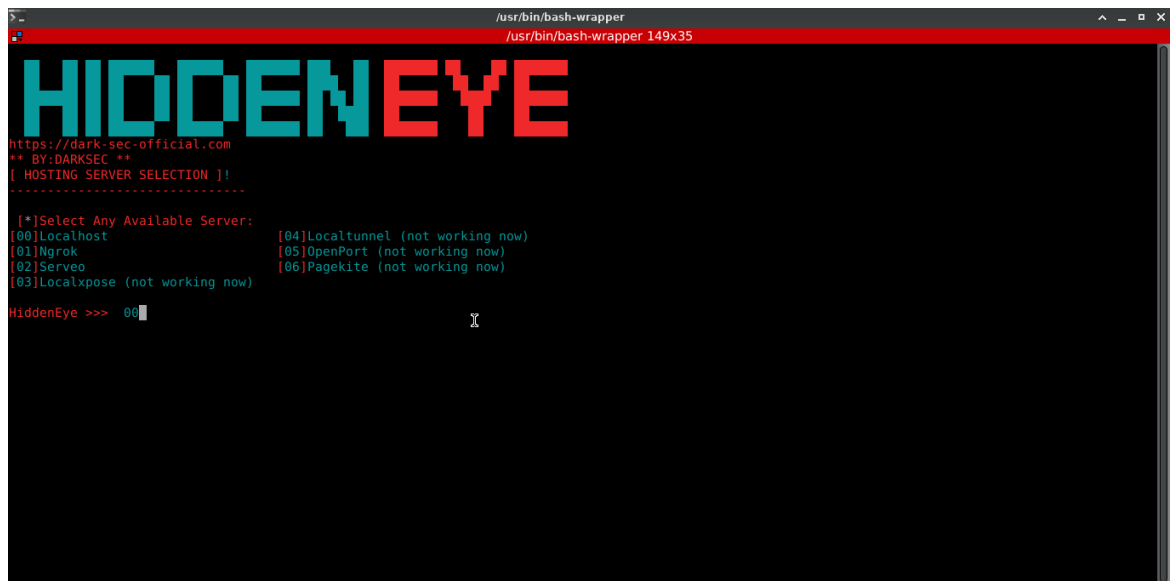
[ WEBSERVER PORT SELECTION ]!

[*] Select Port [1-65535]:

[*] We suggest using ports between [1024-65535] but you still able to choose any ports you want.

HiddenEye >>> 1025
```

7. Select Localhost as your server



```
/usr/bin/bash-wrapper
/usr/bin/bash-wrapper 149x35

HIDDEN EYE

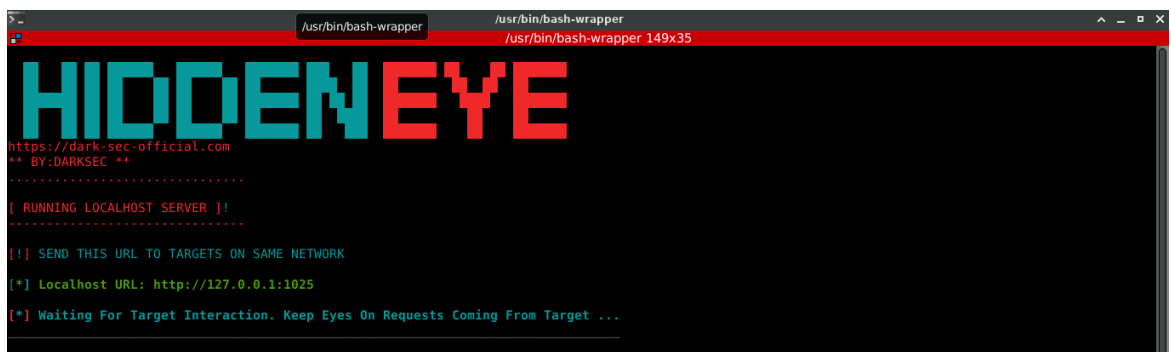
https://dark-sec-official.com
** BY:DARKSEC **
[ HOSTING SERVER SELECTION ]!

[*]Select Any Available Server:
[00]Localhost
[01]Ngrok
[02]Serveo
[03]Localxpose (not working now)
[04]Localtunnel (not working now)
[05]OpenPort (not working now)
[06]Pagekite (not working now)

HiddenEye >>> 00
```

8. Share the link

After selecting the server computer and press enter you will be provided with a link for which you could share this to anyone who is connected within your network



```
/usr/bin/bash-wrapper
/usr/bin/bash-wrapper 149x35

HIDDEN EYE

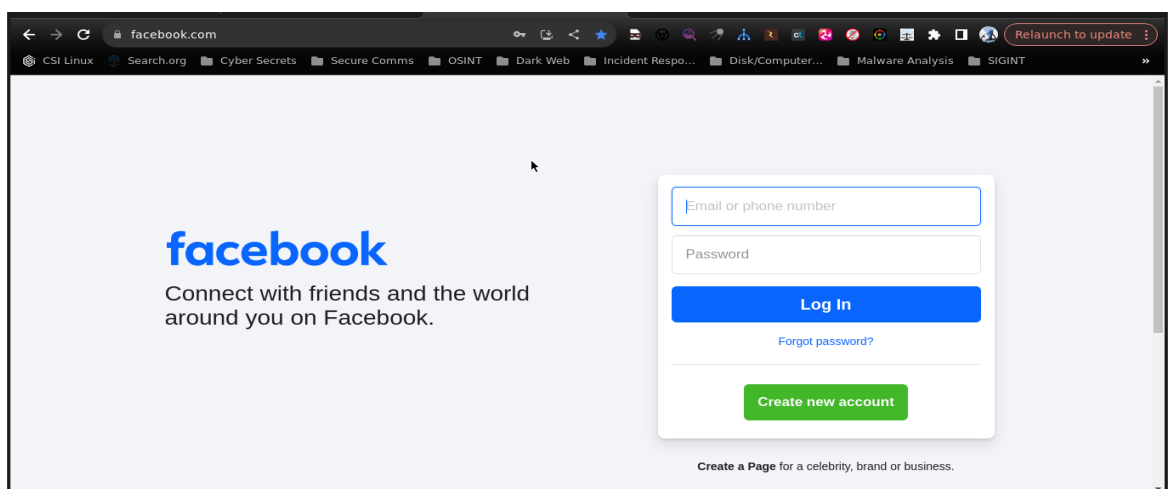
https://dark-sec-official.com
** BY:DARKSEC **
[ RUNNING LOCALHOST SERVER ]!

[!] SEND THIS URL TO TARGETS ON SAME NETWORK

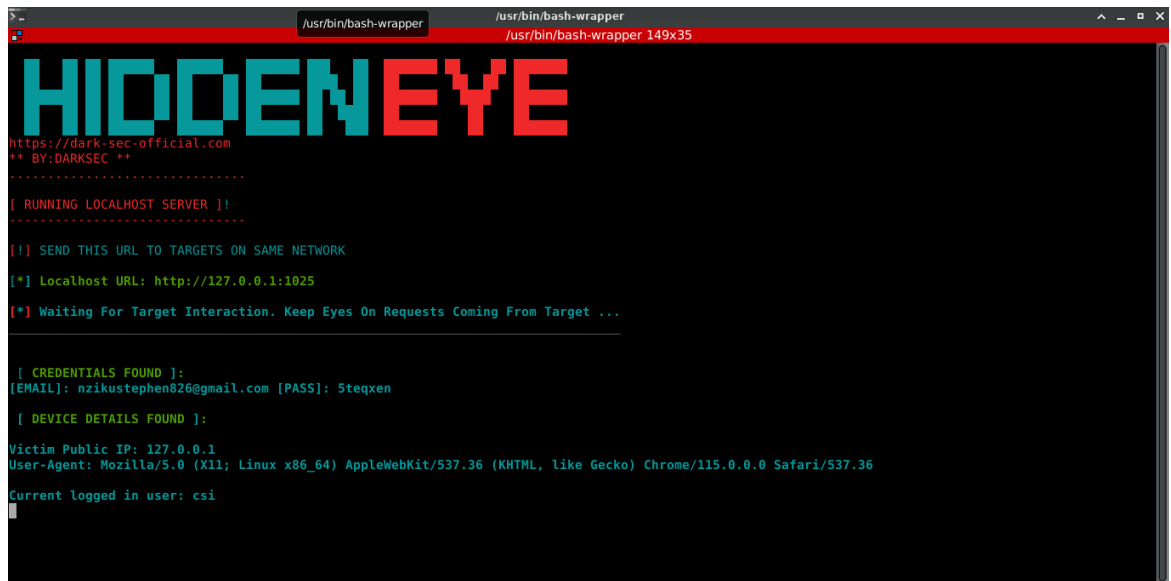
[*] Localhost URL: http://127.0.0.1:1025

[*] Waiting For Target Interaction. Keep Eyes On Requests Coming From Target ...
```

9. The below page will open when the link will be clicked by a target



10. Wait for a target to enter credentials and they will appear on the terminal as shown below



```

/usr/bin/bash-wrapper /usr/bin/bash-wrapper 149x35
HIDDEN EYE
https://dark-sec-official.com
** BY:DARKSEC **
[ RUNNING LOCALHOST SERVER ]!
[!] SEND THIS URL TO TARGETS ON SAME NETWORK
[*] Localhost URL: http://127.0.0.1:1025
[*] Waiting For Target Interaction. Keep Eyes On Requests Coming From Target ...

[ CREDENTIALS FOUND ]:
[EMAIL]: nzikustephen826@gmail.com [PASS]: 5teqxen

[ DEVICE DETAILS FOUND ]:
Victim Public IP: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.0.0 Safari/537.36
Current logged in user: csi
```

6.2 Storm-Breaker

6.2.1 Purpose:

Storm breaker is a social engineering tool that can be used to access the location, webcam, microphone, and OS Password Grabber Using Ngrok Link.

Features:

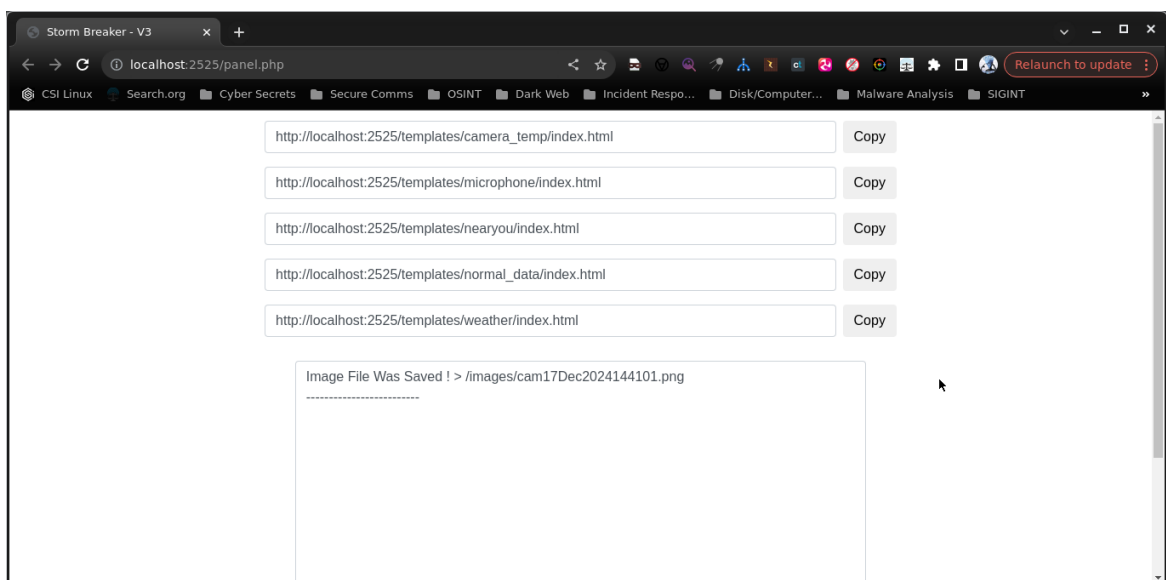
- It can get device information.
- It can provide location.
- Fetch OS Password.
- It can access Webcam.
- It can access the microphone.

6.2.2 Steps to Use:

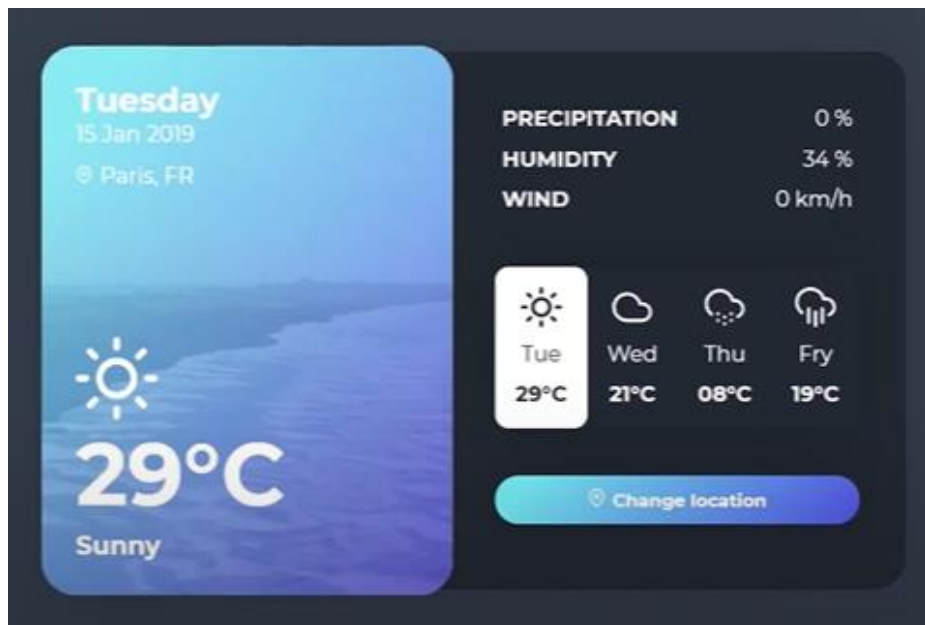
1. Launch the Tool:

Run the tool graphically or through terminal using python3 like on the below example

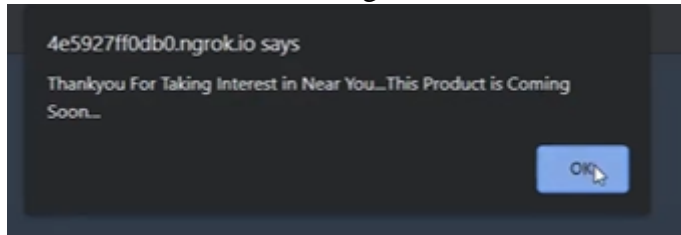
```
python3 st.py
```



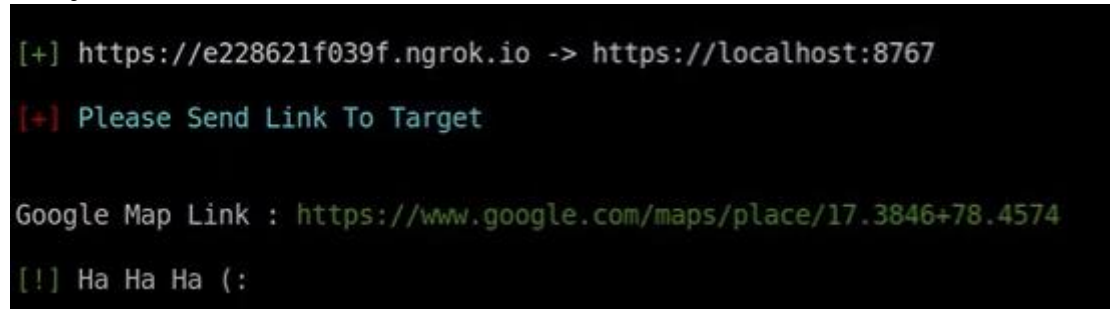
2. Choose a template 4 for example [*nearyou*] to access location:
3. Copy Links and send it to your target
4. The target will be shown the below simple page:



5. When he clicks on the change location button, an alert is generated showing.



6. And just like that, we receive the link to see his location.



7. Open this link in your web browser

