OSINT TECHNIQUES FOR INVESTIGATING PEOPLE

BY
MANJESH SHETTY, GCIH, GCFA
DATA SECURITY COUNCIL OF INDIA

OSINT

- Data is new oil, large amount of data is posted online about people, and it is up 24x7x365 days.

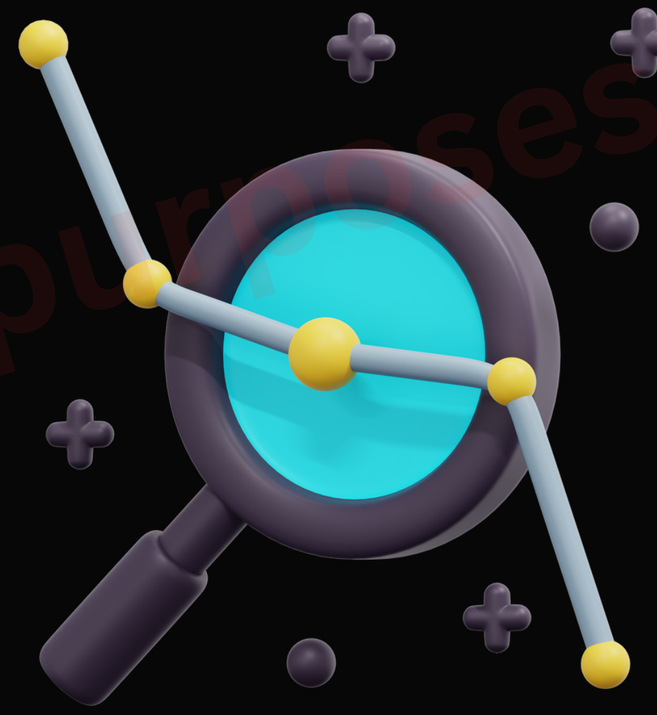
- Open-source intelligence (OSINT) the process of searching, gathering and analysing information collected from public sources from the Internet. Information can be collected manually or using OSINT Tools by the analyst.

OSINT can be used by for different purposes:

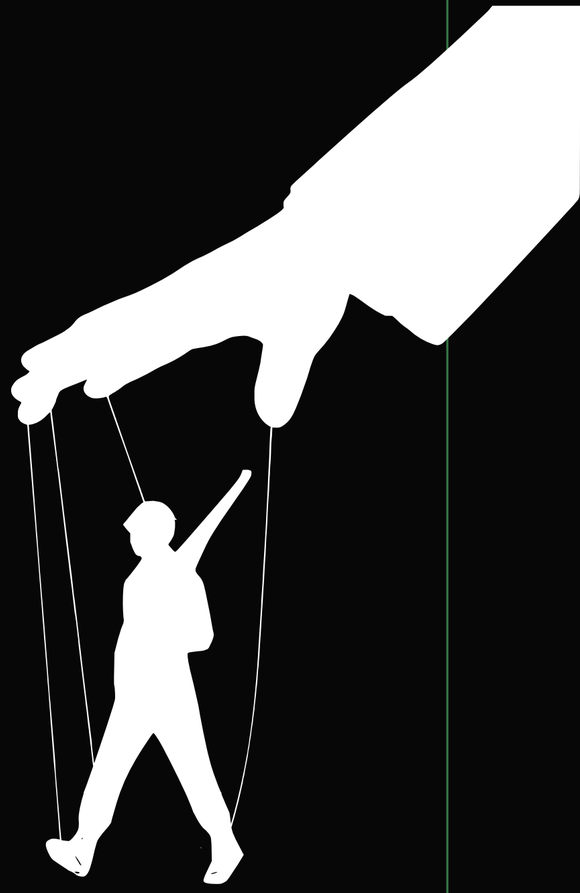
- Sentiment analysis for maintenance of public order
- Intelligence collection
- To trace and arrest offenders
- Gathering evidence against the accused
- Tracing of missing persons
- To verify real and fake news
- For background check

INVESTIGATION PEOPLE

- EMAIL ID
- PHONE NUMBERS
- SOCIAL MEDIA
- USERNAME
- PHOTOS
- DATA LEAK
- PEOPLE CENTRIC SEARCH API



Sock Puppet & HUMINT



Sock Puppet is ficitious identity used on a forum, marketplace, social network & other platform

This will hide your real identity, in case if you're using any OSINT Tool

Sock Puppets Account creation Tips

Tip #1

Use Proton Mail or Tutanato Mail for any Account Creation

Tip #2

Use Textverified.com

Google Services
Whatsapp
Facebook, Instagram, twitter

Tip #3

Use emailondeck/33mail for work email

EMAIL ID OSINT

Epios Tool

Retrieve information linked to an email address, without notifying its user

epios.com

Note: Register using temp-mail.org

search.0t.rocks

Retries information like Full Name,Phone number, IP Address,

Note: No Registration is required

SPYCLOUD

Retrieve information like plaintext password, phone numbers, address, location

spycloud.com

Note: you need to register from an email ID of the target

HAVEIBEENPAWNED

Search whether email ID is part of any databreach

RETRIEVE PASSWORDS FROM EMAIL ID

- **LEAKPEEK**
- **BREACHDIRECTORY**

PHONE NUMBER OSINT

TWILLIO

- **Twillio: VOIP Number Analyzer**

CONTACT EXPLOITATION

Many applications allow (and encourage) you to locate your friends' profiles within the service by their email address or telephone number

WHITE PAGES

Find people, contact info & background checks

SOCIAL MEDIA OSINT

FACEBOOK ,INSTAGRAM & TWITTER

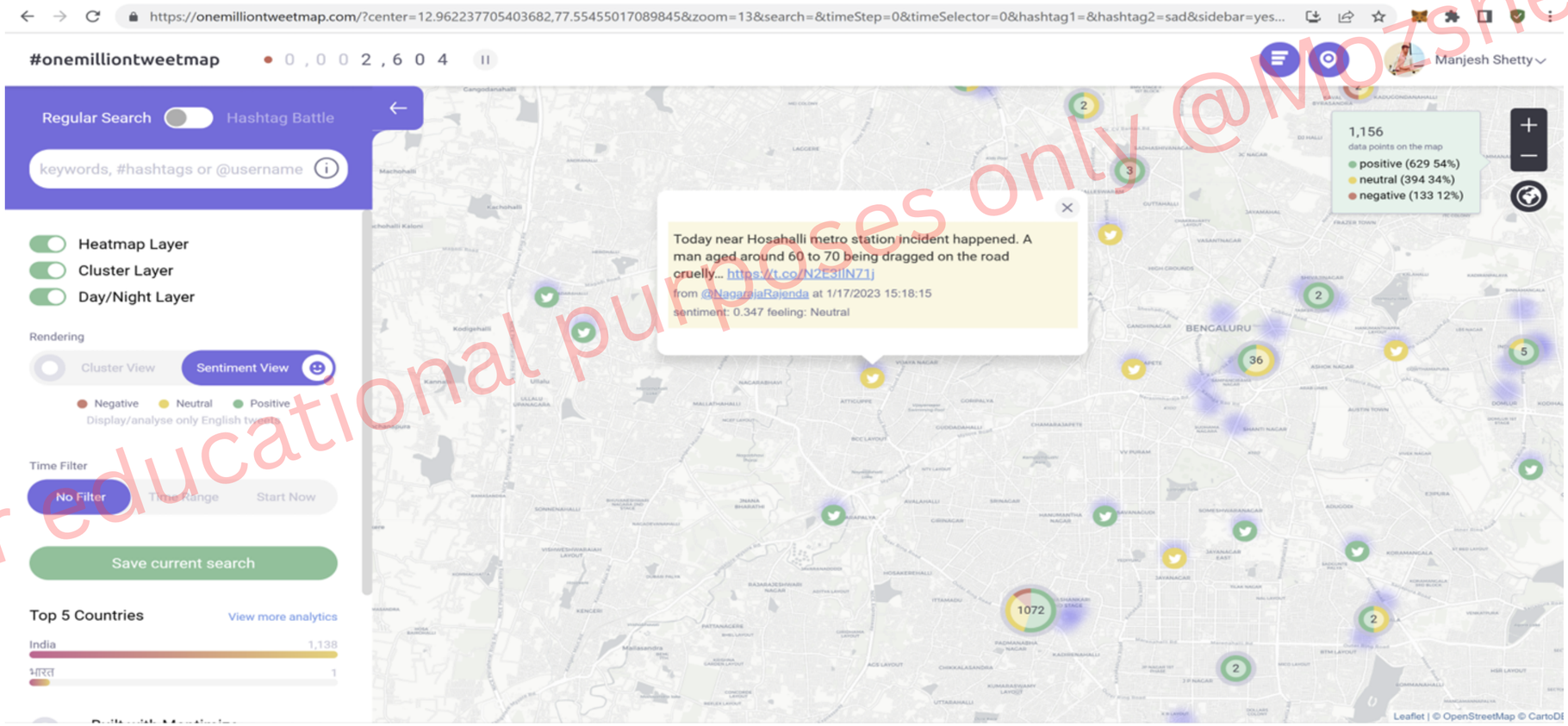
Inteltechniques: Social Media OSINT Analyzer

SNAPCHAT MAP

Snapchat Map surveillance

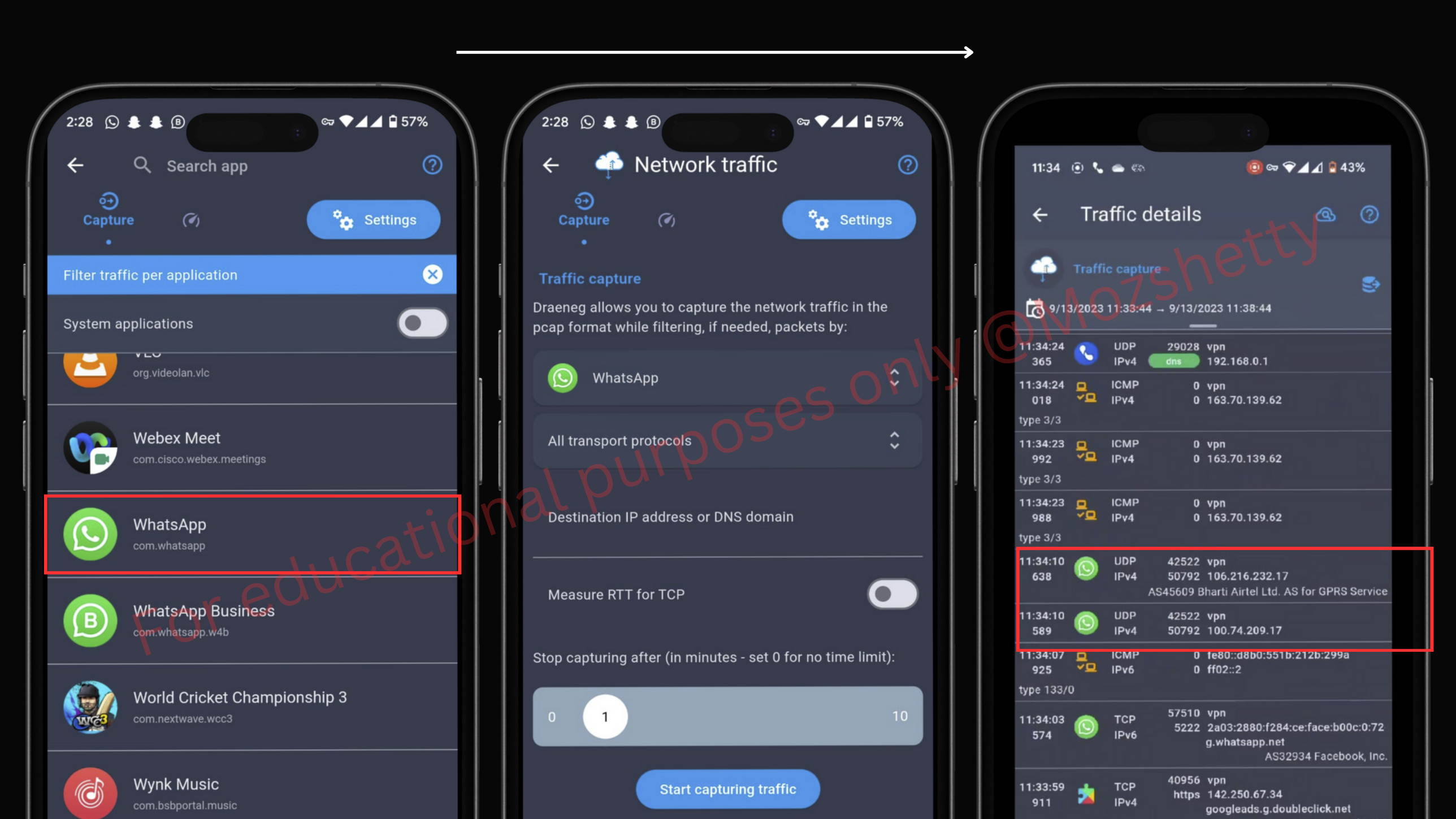
Twitter Analysis - Spoonbill.io

Twitter Analysis: onemilliontweetmap



Whatsapp calls

- Grab IP Address of the whatsapp/Instagram or different social media app call users



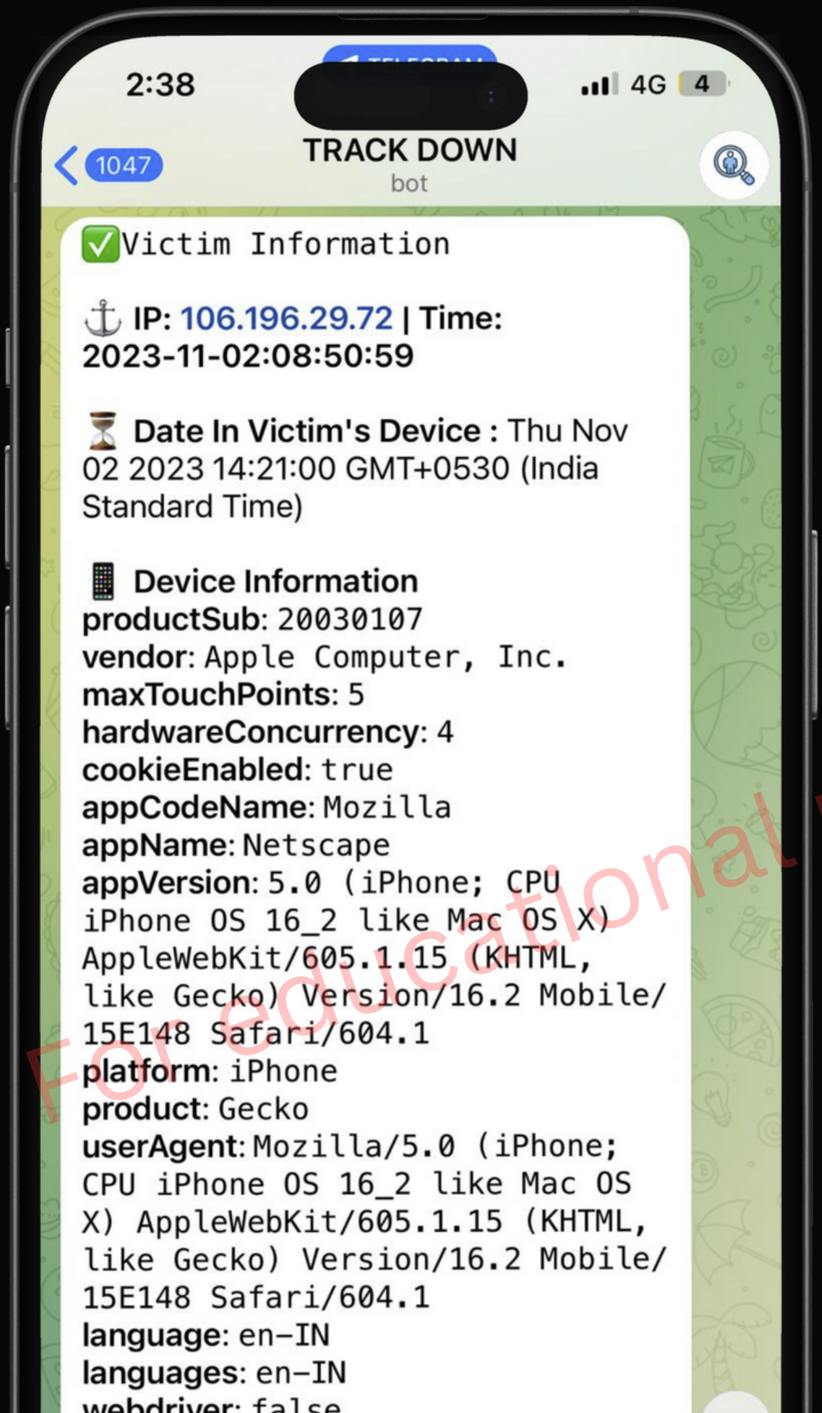
IP Grabber

- **Scenario 1:** One person was harassing and blackmailing a girl to do a video call with him in the telegram app.

- **Scenario 2:** Smuggler who is active only in WhatsApp with VOIP Number.

IP Grabber Tools

- Grabify.link
- IP Logger
- https://t.me/Trackdownpeoplebot



IP Grabber - Advanced Method

Buy domain from Godaddy.com

Host it in Wordpress

Monitor it using Wordfence Plugin

Domain Name: Bengalurunews.com

USERNAME OSINT

USERNAME FINDER

- namecheckr.com
- Namevine.com

PHOTOS OSINT

EXIF VIEWER

ONLINE TOOLS

- Extract Metadata (extractmetadata.com)
- Jeffrey’s Viewer (exif.regex.info/exif.cgi)
- Exifinfo (exifinfo.org)
- Get Metadata (get-metadata.com)

OFFLINE TOOLS

- ExifTool by Phil Harvey

EXIF INFORMATION

- GPS (Lat, Long)
- Make, Model
- Owner Information
- Timestamp Information
- Thumbnail (Preview) Image

REDDIT TOOLS

- **Reddit.com/r/picrequests:** Free Photo Enchacement and editing service
- **Reddit.com/r/whatisthisthing:** For the identification of mysterious objects

IMAGE REVERSE SEARCH

- Google Reverse Image Search (Images.google.com)
- Bing Image Search (bing.com/images)
- Tin Eye Rever search (Tineye.com)
- Yandex Images
- Baidu Images
- PimEyes

People Centric Search API

PEOPLEDATALABS

People data" collection company offers 1,000 free queries of their premium data sets to anyone, and they accept masked email addresses such as 33mail, Anonaddy, and Simple Login.

DSCI
PROMOTING DATA PROTECTION

OSINT INVESTIGATION WITH OS-BASED FRAMEWORKS

There are 3 types of OSINT

- Passive Collection
- Semi-passive Collection
- Active Collection

Passive Collection

This is the most used type when collecting OSINT intelligence, by default most OSINT gathering methods should use passive collection because the main aim of OSINT gathering is to collect information about the target via publicly available resources.

Semi-passive Collection

In this way, you are not implementing in-depth investigation of the target’s online resources, but only investigating lightly without launching any alarm within the group you are investigating.

Active Collection

You interact directly with the system to gather intelligence about it, but the target can become aware of the reconnaissance process since the person/entity collecting information will use advanced techniques to harvest technical data about the target IT infrastructure such as accessing open ports, scanning vulnerabilities (unpatched Windows systems), scanning web server applications, and more.

CLI & Linux Based Application

Trace Labs
VM

Tracelab.org

whois

'Whois' is a widely used Internet record listing that identifies who owns a domain/IP and how to get in contact with them.

To get 'whois' information for site, type in Linux terminal 'whois' followed by domain name

```
> whois gopcsoft.com
```

whois

To get detailed information about network owner of the site, first you need get IP address from hostname. In terminal windows type command **'host'**, **'nslookup'** or **'dig'** followed by hostname.

> host gopcsoft.com

> nslookup gopcsoft.com

To get authoritative DNS server(s) for specific domain

```
> dig gopcsoft.com NS
```

To get mail server(s) for specific domain

```
> dig gopcsoft.com MX
```

OSINT - OSRFramework

Open Sources Research Framework - OSRFramework Software has different applications related to username checking, DNS lookups, information leaks research, deep web search, regular expressions extraction and many others.

OSRFramework' install following components

- **mailfy** - find information about emails taken as a reference nickname or email list
- **searchfy** - find profiles linked to a full name
- **usufy** - identify social media profiles using a given nickname
- **checkfy** - guesses possible emails based on a list of candidate nicknames and a pattern

UserRecon

'UserRecon' allows to find usernames across over 75 social networks.

Now we can start search for usernames from social media networks. Type in following command and then enter desired username at 'Input Username' prompt

```
> ./userrecon.s
```

Metdata

Many files contain extra or even hidden data other than the visual data you see at first glance. E-books, photographs, movies, music and even documents can contain data that you don’t see at first glance.

To view 'exif' information from the image, run 'exiftool' command followed by image name

```
> exiftool “FileName”
```

By default, 'exiftool' show GPS coordinates in human readable format, Google maps do not understand this format.

Let's print Google-maps friendly GPS data from photo

> exiftool -gpslatitude -gpslongitude -n filename.jpg

```
> exiftool -G filename.jpg | grep -i -E
'(Make )|(Model)|(Software)|(Device)|
(Lens)'.jpg | grep -i -E '(Make )|
(Model)|(Software)|(Device)|(Lens)'
```

Spiderfoot

SpiderFoot is an open source intelligence (OSINT) automation tool. It integrates with just about every data source available and utilises a range of methods for data analysis, making that data easy to navigate.

>Spiderfoot -l 127.0.0.1:8001

usage of different spiderfoot API

use 33mail for signup

Sherlock

Sherlock, a powerful command line tool provided by Sherlock Project, can be used to find usernames across many social networks.

Maltego

Maltego is a link analysis software used for open-source intelligence, forensics and other investigations, originally developed by Paterva

WebHTTrack Website Copier

It allows you to download a World Wide Web site from the Internet to a local directory, building recursively all directories, getting HTML, images, and other files from the server to your computer.

Tracelabs Browser Bookmarks

Thank You