Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 07, July-2021

TIGMINT, Open Source Intelligence: An era of Evolution

Rishabh Sharma
11th Grade, The Shri Ram School,
Aravali Gurgaon- Haryana INDIA

Abstract **: An OSINT (Open Source Intelligence) software framework with the goal of making cyber investigations easier by implementing abstraction mechanisms to hide the background technical complexity, as well as bundling different social media intelligence analysis techniques and providing a user-friendly web interface. The term OSINT comes from many decades ago, in fact, US military agencies started using the term OSINT in the late 1980's as they were re-evaluating the nature of information requirements in tactical levels under battlefields. Then in 1992, the Intelligence Reorganization Act determined the main goals of intel gathering included key concepts like:**

● Must be objective intelligence free of bias
● Data must be available on public and non-public sources
While the concept of OSINT has evolved since then, as it does not include the non-public sources, the concept originates from that time.

Keywords : OSINT, Investigations, Modules, Geotagging, Domain search

INTRODUCTION

Internet and its active users are spread across the vast expanse of India so much that it makes it rank second in the world and is expected to cross 639 million users by December 2020, be it urban or rural areas internet has got no boundaries or limitations. The Internet provides anonymity, which is misused to commit cybercrimes. The majority of the internet consumed is on social media, it is particularly estimated that by 2021 we will have around 448 million social network users in India. As of 2019 data, social media sites/applications such as Instagram and Twitter have over 191.1 Million and 125.2 million monthly visits respectively. The increase in the consumption of social media is directly related to the number of online crimes happening through social media or misusing social media. It is impossible to trace and act against every crime without the help of automation and the latest technological advances. Considering the large amount of data generated using these social networks it is nowhere possible to manually analyze information. OSINT (Open Source Intelligence) tools are often used to gather different kinds of information from social networks. But these tools are complex to use and require a lot of technical expertise. So, to tackle this problem we made a tool which can be used by LEA's (Law Enforcement Agencies) to analyze social media information. The primary focus is on synthesising findings from existing research on cyber intelligence and open source intelligence using TIGMINT profiling to identify both threats and vulnerabilities on online social networks for mitigation purposes. This tool implements abstraction mechanisms to hide the background technical complexity and bundles different analysis techniques for social networks together providing a simple intuitive web interface for the user to work with. TIGMINT entails the gathering of data and profiling of individuals from publically available private and public sector information sources for business intelligence purposes.

MODULE SELECTOR

Fig : Module Selector

Based on the tool documentation, we can select modules. The tool itself is capable of handling multiple modules such as Social media analysis, Geotagging, Metadata analyzer,etc.

MODULE I

The very first module is the Account finder module in which it can find social media accounts from various platforms. This module contains various platforms like Instagram, Facebook, Twitter, Reddit, youtube, Github and medium. In Account finder, it simply demands username as input and tries to find the particular username on the various platforms and return the social media account link as output. If the person uses the same username in his/her social media account then we can get maximum output and gather more information about the particular person. This module can be useful for tracing the social media account of an individual. Working Process:- This module is coded in python programming language and python requests library is used for scraping the user social media account. As we can see in the image 1 below, the account finder module demands username as an input and then it starts digging the social media platforms and gives us the possible output in the URL form of the social media account.

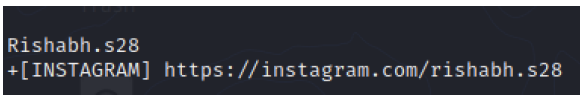

Fig 1: Account Finder

MODULE II

Twitter is one of the most popular social media used throughout the world. The platform provides a good medium to communicate and interact with the different peoples and give a viewpoint for any topic.
The reach of twitter has increased in the past few years as the internet has taken a huge gain in its audience. So, keeping that in mind we thought of building an application that would help the investigators to get hold of the activity of the user on Twitter.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 07, July-2021

Fig : Twitter and Facebook search

The Twitter module is further divided into sub-modules:

***Module 2.1**: Sentiment Analysis*
For the analysis of tweets first, we need to get all the tweets and perform sentiment analysis on them. To do so, we first scrape all the tweets using the TWINT -(Twitter Intelligence Tool) library that is available in python.

***Module 2.2**: Top 'N' Hashtags & Mentions*

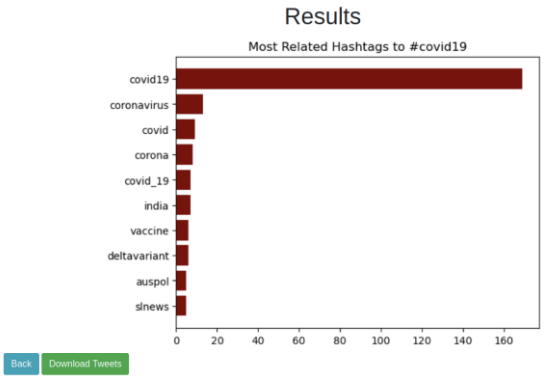

Fig : Hashtag (#Covid19)

In the current cyberspace, social media sites are prevailing, their users are increasing every day, and the users are sharing pictures, posts, and other stuff. This stuff consists of hashtags(#) which have become the most prominent tool to raise your voice on any platform.

***Module 2.3**: Geo-Tagging / Analysis*

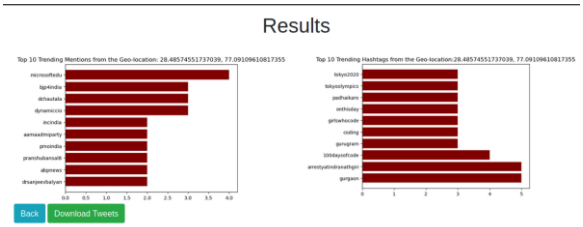

Fig : Geo-Tagging Analysis

Using twitter tweet data, there are two types of geographical metadata information we can extract and work with.

***Module 2.4**: Similar Hashtags Analysis*
Hashtags are used as a way to connect social media information to a specific conversation, theme, event or topic.

```
def main():
  seed_hashtags =["#tiktok" , "#BlackLivesMAtter"]
  limit = 1000  # limits the number of tweets to pull
  for seed_hashtag in seed_hashtags:
    get_similar_hashtags(seed_hashtag, limit)
main()
```

Fig : Hashtag (#) python backend input

Hashtags also make it easy for people to discover posts around those specific topics of interest because hashtags aggregate all social media posts with the same hashtag.

MODULE III

This module is based on the extensively used social media site Instagram, a majority of crimes comes from Instagram which includes stocking, harassment, bullying, etc. Keeping that in mind, our team was intended to develop a tool which could be helpful in the investigation of such crimes by analysing the public profile available on the platform. This module will be covering the public profile available on Instagram and will give you a brief of that particular profile with the last 24 hr stories and the highlights of the same.
Working Process: Using the request library in python at the backend, the module is intended to scrape the user data that is available in the public profile, this data is scraped and stored in JSON format, which can be called directly from the frontend in the form of an API call, and would be displayed to the user. The other part of this module consists of getting the public profile stories and highlights, which is done using the open-source API available of storiesig.

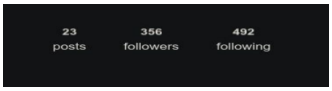

Fig : Instagram Module

This would store the result (images) in a folder at the server which is then called using an API and the result would be available to the user.

MODULE IV

Metadata is data which can be described as data that provides us with information of the other data we had entered as the input. In simple words we can say, it is "data about data". For example; metadata for a document might include data/ information regarding the size, author, date of creation of the document and keywords that describe the document and similarly for music information like artist's name, the album, year of production and release etc could serve as metadata. Basically, talking in layman terms metadata provides us with the behind-the-scenes information that's used anywhere and in any industry in different ways. It's ubiquitous in information systems, social media, websites, software, music services, and online retailing. Metadata can be created manually to pick and choose what's included, but it can also be generated automatically based on the data. Social Media Metadata: Multimedia forms the backbone of the social media we consume in our daily lives. In social media platforms like facebook, instagram, linkedin etc, huge amounts of multimedia and document information is being uploaded every day. These files contain meta-information which can be retrieved and analyzed further. An image taken with a GPS enabled professional camera may contain a lot of meta-information like exact GPS location, used camera, software used, Copyright, Author etc. There are many instances where Lea's (Law Enforcement Agencies) used metadata to track and arrest criminals all around the world. The following are examples of such cases.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 07, July-2021

John McAfee, the millionaire software executive turned semi-fugitive, was caught by using location metadata found in his picture uploaded via social network.

MODULE V

This module provides overall information about a particular target and represents the scanned data graphically. This is a very powerful tool ,containing more than 200 modules over which the scans are conducted to gather maximum information over a target, domain scanning being its most effective tool. It can scan perimeters like:

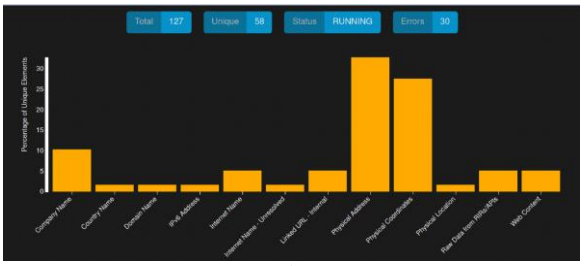

Fig : Scanning of parameters in Module V

I. Domain Name: e.g. example.com
II. IPv4 Address: e.g. 1.2.3.4
III. IPv6 Address: e.g. 2606:4700:4700::1111
IV. Hostname/Sub-domain: e.g. abc.example.com
V. Subnet: e.g. 1.2.3.0/24
VI. Bitcoin Address: e.g. 1OesYJSP1QqdyPEjnQ9vzBL1wujruNGe7R
VII. E-mail address: e.g. alex@example.com
VIII. Phone Number: e.g. +12345678901 (E.164 format)
IX. Human Name: e.g. "John Smith" (must be in quotes)
X. Username: e.g. "jsmith2000" (must be in quotes)
XI. Network ASN: e.g. 1234

Working Process: The aim of the module is to provide precise information of a target. For example, If I want to run a search under the domain facebook.com, a search will be run finding information related to Linked URLs, web content, IPv6 Address, Physical coordinates, Raw data from APIs and much more. Here is a graph for the working of the tool.

Domain search run on facebook.com

Tech Stack of Module:

- Spiderfoot: Spiderfoot is a popular python library used to retrieve open-source information.
- Python: Python programming language is used to perform a backend scan for information over the internet.

Type : Domain Name
Input : youtube.com
Output : The output gives information about the company name, internet name, Linked URLs, Physical address, Physical coordinates, Web content.

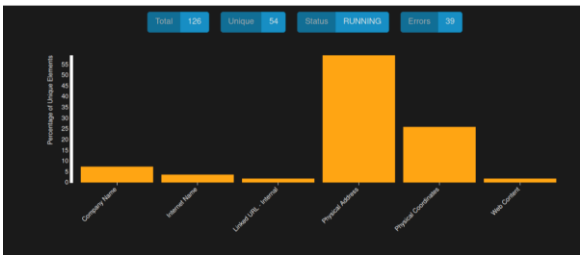

Fig : Domain Name Analysis

Type : IPv4
Input : 8.8.8.8
Output : The output gives information about the Affiliate- Email Address, IP address, Raw data from APIs, Netblock Membership.

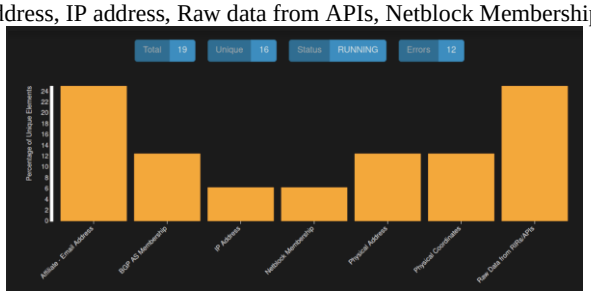

Fig : IPv4 Analysis

Type : Bitcoin Address
Input : 16ftSEQ4ctQFDtVZiUBusQUjRrGhM3JYwe
Output : The output gives information about the Bitcoin Address and The Bitcoin Balance.

Fig : Bitcoin Address Analysis

Type : Email Address
Input : Rishabhsharmafeb2005@gmail.com
Output:The output gives information about the Accounts on External Sites, Usernames, Raw data fromAPI's.

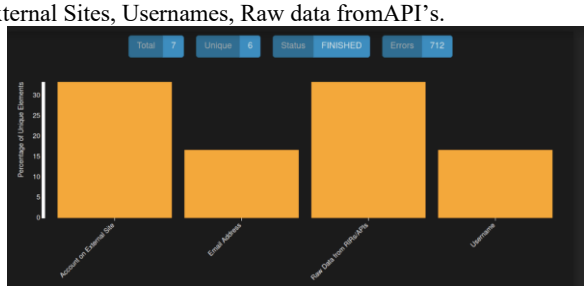

Fig : Email Address Analysis

Type : Phone Number
Input : (+1)2029462405
Output: The output gives information about the Country Name, Physical Location. It can also give us information about the Network service providers.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 07, July-2021

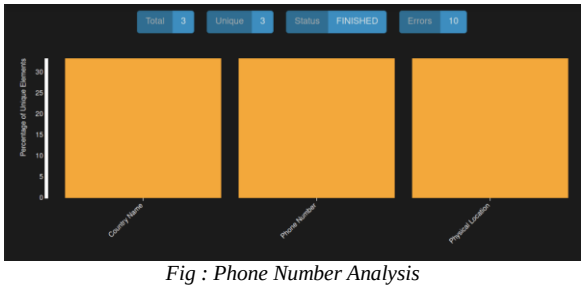

Fig : Phone Number Analysis

IMPORTANCE

Based on the published resources, The United States of America is in the top list for publishing articles/researches based on OSNIT.

Fig : Open source Intelligence across the globe (Based on research publication)

It's important to remember that intelligence helps you to anticipate both possibilities and threats, the latter of which is crucial for an organization's or country's survival. Security, in general, is concerned with preventing risks and hazards. As a result, given the various scenarios existing in social, political, and a security context, the integration of intelligence and security becomes critical. Because Google has disallowed robots, a user agent from the Firefox browser running on Kali Linux was utilised for the site scraping design.

Fig : Step-by-step Design

CONCLUSION

In terms of the utilisation of open source intelligence and the threat and vulnerabilities that exist on social media platforms, the review includes classified research findings. Hence we can conclude this is a very powerful OSINT tool with endless capabilities with 5 modules (as discussed in my article, and many more can be embedded) importing data from over 250+ resources to ensure maximum data extraction. The Twitter modules are highly accurate and fast in importing data and presenting it in a graphical form. Module 5 provides information in an interactive graphical manner, which is easy to use and powerful at the same time.

Because the study was targeted at looking at the dangers from narrative, qualitative, and quantitative approaches, the meta-analysis had limitations owing to time restrictions. Lack of resources, conflict of interest, and inability to obtain secondary data, as well as budgetary limits and gaining confidence from individual sources, will all be implications for future study.

Although academic scientific dissemination of OSINT resources is increasing, it still does not reflect a high level of engagement within repositories and databases, with non-profit and free-to-use sources having the biggest presence of OSINT resources.

Mr. Rishabh Sharma , 16 years old teenager is a 11th grade student at The Shri Ram School - Aravali, Gurgaon, Haryana, IN. He is passionate about technology and creator of TIGMINT, an Open Source Intelligence Tool. He has completed an internship with Gurugram Police on Cybersecurity and Ethical Hacking, where he designed TIGMINT. He has participated in CTF's and has conducted Cyber awareness presentations in school. In his free time, he enjoys playing guitar, listening to music and practices horse riding as a sport. He is passionate about reading different business models and entrepreneurs biopics.

REFERENCES

[1] Coyne, J. W. & Bell, P. 2011. The Role of Strategic Intelligence In Anticipation Transnational Organised Crime: A Literature Review. International Journal of Law, Crime & Justice. Queensland University of Australia. Australia. *(1) (PDF) Cyber Intelligence and OSINT: Developing Mitigation Techniques Against Cybercrime Threats on Social Media*. Available from: https://www.researchgate.net/publication/323579431_Cyber_Intelligence_and_OSINT_Developing_Mitigation_Techniques_Against_Cybercrime_Threats_on_Social_Media [accessed Jul 03 2021].

[2] Horn, J. L, 1979. Trends in the measurement of intelligence. Intelligence, 3, 229-240.

[3] Swoyer, S. It's Official: Metadata Management Is a Strategic Problem. UpSide Where Data Means Business. 2016. Available online: https://tdwi.org/articles/2016/11/02/metadata-management-is-a-strategic-problem.aspx (accessed on 30 June 2020)

[4] Swoyer, S. It's Official: Metadata Management Is a Strategic Problem. UpSide Where Data Means Business. 2016. Available online: https://tdwi.org/articles/2016/11/02/metadata-management-is-a-strategic-problem.aspx (accessed on 30 June 2020).

[5] BMC Informatics Web Page [Tigmint: correcting assembly errors using linked reads from large molecules] https://bmcbioinformatics.biomedcentral.com/articles/10.1186/s12859-018-2425-6

[6] TIGMINT : OSINT Framework by Rishabh Sharma https://github.com/TIGMINT