International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 5, May 2020 ||

MALTEGO: OSINT Framework and Research Analysis

Ramesh Amgai[1]

U.G. Student, Department of Computer Engineering, Jamia Hamdard University, New Delhi, Delhi, India[1]

ABSTRACT: Today the internet is an integral part of our life. We share various information in this digital world either intentionally or unintentionally. Therefore, extracting the data and information has been a lot easier than before. Various tools like Maltego, Dimitry,etc have been used for the extraction of those crucial data. Though sometimes the information which could play a game changing role is present openly and free to access if we know where to find it. Here I will demonstrate how to look up for the information required to conduct investigation and various cases to support it.

KEYWORDS: Maltego, OSINT framework, reconnaissance

I. INTRODUCTION

Reconnaissance is crucial for successful hacking/pentesting. Maltego is a unique tool for finding data via open source intelligence (OSINT) across the World Wide Web (WWW) and displays the relationships between this information in a graphical format.
According to Paterva'sMaltego's developer "Maltego is an interactive data mining tool that renders directed graphs for link analysis. The tool is used in online investigations for finding relationships between pieces of information from various sources located on the internet. Maltego uses the idea of transforms to automate the process on a node based graph suited for performing link analysis." The tool can be used to obtain information for various areas and from various sources. Maltego uses the idea of transformation to automate the process of querying different data sources. This information is then displayed in a node-based graph. Such a visual representation is ideally suited for link analysis. It is used by intelligence agencies, banks, Pentesters,security/threat analyst and many others. It takes care of the process of data import, processing, transformations, analysis, and visualization with a single click. In particular, it focuses on social media and technical infrastructure, tracking of people, organizations, and physical hardware.

II. MALTEGO CONCEPT

The combination of entities, transforms and machines (building blocks of Maltego) are explained here.
Entities- They are real objects, such as a person, DNS name, phone number, email address. On the graph, an entity is visually represented as a node. Maltego client contains approximately 20 entities but you can specify your own entities also.

Transforms- It is a piece of code that takes an entity as an input and extracts data in the form of an entity based upon the relationship. They are represented by icons over the entity names. The sources of the data are places like DNS servers, search engines, social networks, whois information, etc.

Machines- It is basically a set of transforms linked programmatically. It is very useful in cases where the starting data and the desired output are not directly linked through a single transform but can be reached through a series of transforms in a custom fashion. They either run completely on their own or wait for interaction with the user at predefined points.

III. EXPERIMENTS

OSINT Framework

It is a useful way to get valuable information by querying free search engines, resources, and tools publicly available on the internet. They are focused on bringing the best links to valuable sources of OSINT data. This tool is mostly used by security researchers and penetration testers for digital footprinting, OSINT research, intelligence gathering, and so on.

The framework provides links to a large collection of resources for a huge variety of tasks from harvesting emails to searching social media. Below are its capabilities and scope of the search.

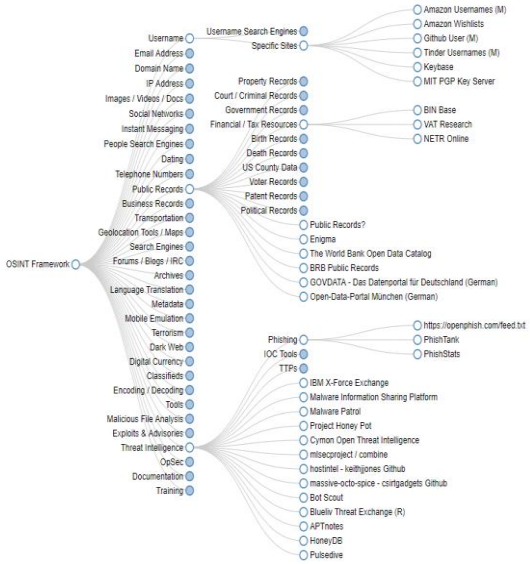

Fig1. OSINT Framework Map

But why use it with Maltego? Well, the answer is simple: to recon the data obtained in the Maltego graph. Maltego collaborated with the OSINT tool to help get the sketch of graph and information provided through it a lot faster and in a broader way. It represents the graphical view of discovered data and its links.

Sample Cases

For the purpose of showing a demo. I am using Maltego CE which is a free version with limited Transforms. Below is the first appearance of Maltego window after the first launch of software.

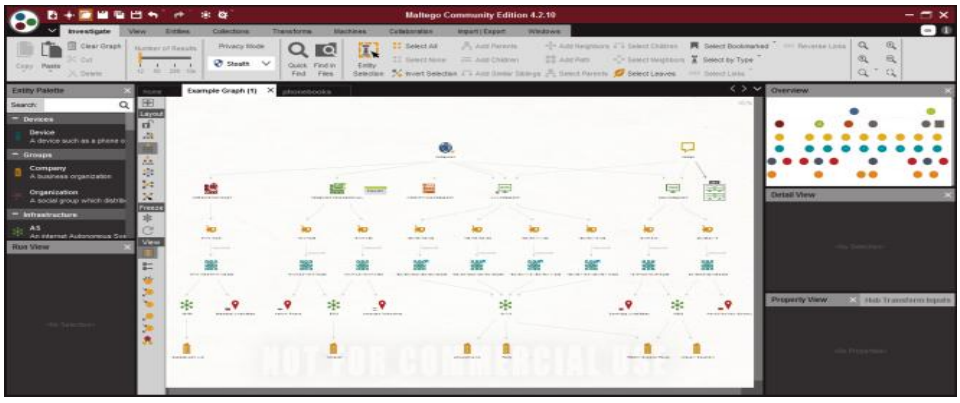

Fig2: Sample interface of Maltego

Performing simple recon

We will perform simple recon on a simple webpage. For your exploration, you can use your own site or any other sites. In this, we performed a query on all transforms. As a result, we can see details of websites and their links, Domain, Location, MX record, and so on.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 5, May 2020 ||

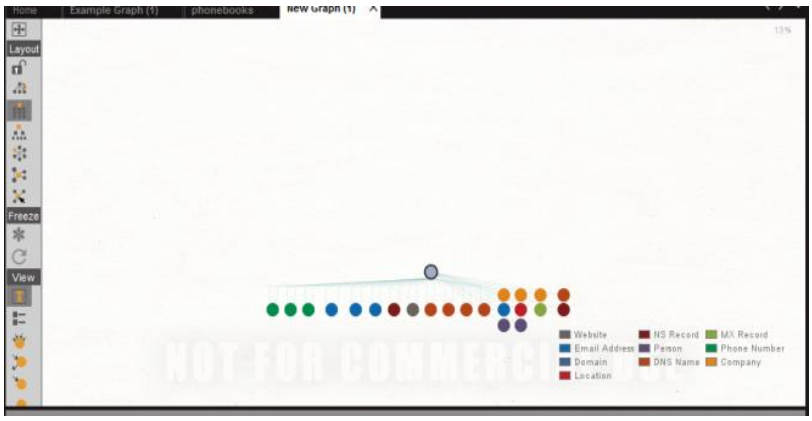

Fig3: Recon on a simple webpage

Cell Phone Analysis

Maltego can be used for a recon of cell phones and data associated with it like last call, time, IMEI numbers, and so on. In the field of cyber forensics and investigation, Maltego is widely used as a powerful investigative tool and especially in the OSINT context. When an investigator is confronted with sets of cell phone records, the analysis thereof can be laborious. Cell phones can run into the thousands, and when having form links between persons and locations. Below is a sample of cell phone analysis although it is not complete illustration, still does offer an example to investigators of additional ideas of what can be done.

Fig4: Cell phone analysis

The above figure provides the information about call history, date of the call, the device used, and duration of call between two users. This approach is generally used to trace the information from the device found in the crime scene and even the government uses this method to eavesdrop the information being conducted between citizens. If any suspicion is recorded, there might be a legal problem.

Mapping a social account to physical locations

Extraction sequence

1. Choose a social media site. Footprint the URL. Apply the transforms to the URL.
2. Capture IP addresses and run those in Google or on IP WHOIS look-up.
3. Check for EXIF data on images for location tagging.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 5, May 2020 ||

Below is a demo on Twitter.

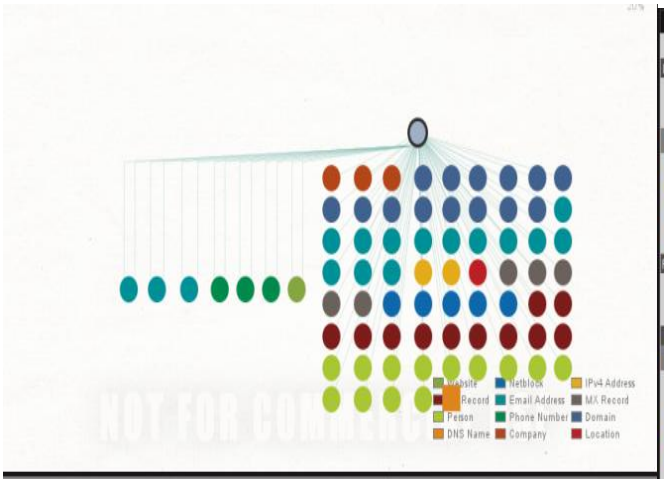

Fig5. Demo on Twitter

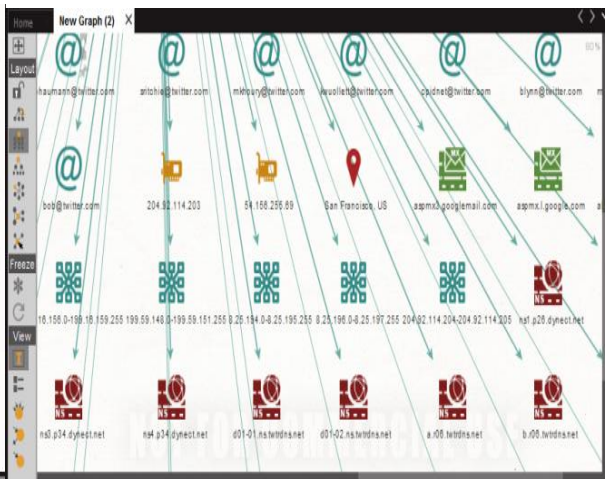

Fig6. Demo with location

Corporate Investigations

The focus here is "corporate investigations" like fraud analysis happening through banking, emails, business, and so on. Finding the identity of the possible "real" person behind the game is a real challenge during the investigation process. It is also the matter of identifying the connection between various aspects like emails, domain, IP addresses, and other similar aspects. So security analysts or investigators must be able to deal with such frauds and always be ready to analyzethe situation if any arises.

According to Reserve Bank of India, in 2018-19, Banks reported a total fraud of Rs 71,543 crore happened in Mumbai, a 74 % rise as against Rs.41,167crore in the previous financial year. Financial firms and companies should regularly check their transactions and maintain the balance between in and out of money flow. Below is a sample of the bank fraud graph.

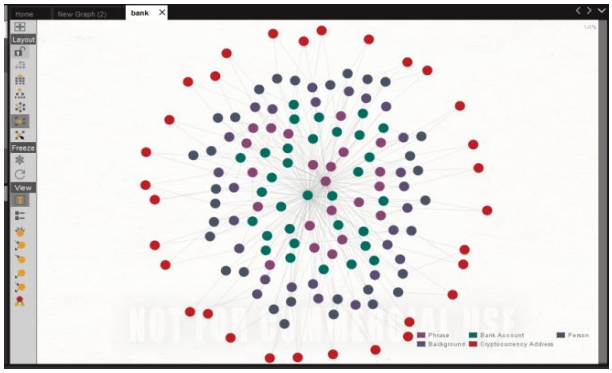

Fig6. Graph Sample of Bank Fraud.

IV. CONCLUSION

Maltego is a quick and effective information gathering tool that allows us to pull information from multiple sources all into one place for analysis. Since it generates graphs it gives a rapid overview of the target structure, differently from command line tools. The above demos provides enough support and explanation about the tools and how it is used in the recon phase. The exploration of information depends upon the explorer like security analyst, forensics, and many other investigators.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 5, May 2020 ||

REFERENCES

[1]. Hacking Web Intelligence: Open Source Intelligence and Web Reconnaissance Concepts and Techniques by Nutan Kumar Panda and Sudhanshu Chauhan
[2]. Beginning Ethical Hacking with Kali Linux: Computational Techniques for Resolving Security Issues by Sanjib Sinha
[3].Maltego Tungsten To explore The Cyber-Physical Confluence by Shalin Hai-Jew.