ORIGINAL RESEARCH PAPER
Volume - 9 | Issue - 7 | July - 2020 | PRINT ISSN No. 2277 - 8179 | DOI : 10.36106/ijsr
INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH

DIGITAL FORENSIC INVESTIGATION OF CYBER-CRIMES ON TWITTER USING DIFFERENT TOOLS AND TECHNIQUES

Forensic Science

Dr. Deepak Raj Rao G Asst. Prof. (Comp. Forn.) LNJN National Institute of Criminology and Forensic Science, MHA, Govt. of India, Delhi, India,

Kumarshankar Raychaudhuri* JRF, LNJN National Institute of Criminology and Forensic Science, MHA, Govt. of India, Delhi, India,*Corresponding Author

ABSTRACT

In this paper, we will discuss about how evidential information about any incident with regard to Twitter can be acquired not only from the social media account of the user but also from different memory locations such as RAM, browser cache, browsing history etc. The available proprietary Social Media Forensic tools are expensive and might not be able to gather all evidences at a given time. Therefore, we have elucidated different open-source tools and in-built native techniques for acquisition of user information and other artifacts from Twitter and the hard disk of computer system, which can help in investigation of an incident related to the social site. Although the scope of this study is limited to Twitter, the findings would be useful for Digital Forensic Investigators and Law Enforcement Personnel to investigate social media crimes in an efficient manner.

KEYWORDS

Twitter, OSINT, RAM Analysis, Browser Cache, Manual Backup

INTRODUCTION

A social network is platform for people all around the world, to mix with each other having varied interests, personalities, hobbies and other habitual preferences. Social networking sites have gained immense popularity over the last decade, since the time people have started using smartphones. Every individual social networking site is available in the form of app, which can be downloaded very easily, free of cost from the playstore, and used without any difficulty. It has become such user-friendly, that even it is possible for a layman to understand and use them in no time. These networks join individuals into groups that, in many ways, resemble small rural communities or neighborhood sub-divisions [1].

Twitter is a social networking site, launched in 2004, which is owned and operated by Twitter Inc. [2]. Using Twitter, it is possible to follow other users, get followed by other users, post tweets, pictures and videos on the public timeline, re-tweet the tweets posted by other users and also reply to another tweet. Over the years, there has been a gradual transformation in the ways of interaction and sharing of information over Twitter. The cyber-criminals have revolutionized their strategies and modus operandi in order to hunt down users on various social-network platforms, using more advanced and improved technologies to target the Web 2.0 applications (Facebook, Instagram, Snapchat etc.) [3]. The connections of every individual in the virtual social world is a crucial component of the services offered by the social networking site, which makes them vulnerable at the hands of perpetrators. With the huge amount of information available on social media, criminals find it easier to leverage it as per their advantage. Not only crimes take place, but a lot of fake content is also propagated through the social media site, which might result as a threat to the national security [4,5].

The emergence of the data privacy laws around the world has made it extremely difficult for Law Enforcement Agencies to investigate any crime related to any social media platform. This is because the various social media platforms have upgraded their security measures, which does not allow any third-party software application to acquire any information from these sites. Hence, the objective of this research article is to discuss and perform experiments using different tools and techniques using which it might be possible for an investigator to acquire any useful artifact related to the Twitter account of a user, whether the information is acquired from the user's account itself, volatile memory of the computer system or from the hard disk of the computer system.

INFORMATION ACQUISITION USING MANUAL BACKUP

Manual Backup refers to the information that one can acquire from the Twitter account of a user [6]. This can help the investigator acquire the username, the phone number using which account has been created, the email ID used for the account, account access history by any third-party application. The access history also shows the date and time on which the app accessed the account and the IP address using which the account has been accessed. This IP address can be used for investigation purposes. It is also possible to acquire information on the devices and browsers that have not been used by the user for logging into the account. It also shows the different applications to which the user's account is connected, the date/time on which the access was given by the user and to which user information the app has an access. All the information, to which investigator has access to, can also be downloaded from the Twitter site. However, the investigator should have an access to the user's credentials for accessing this information. A snapshot of the same is shown in Fig. 1

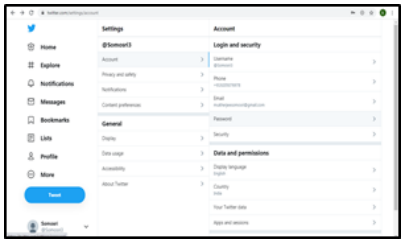

Figure 1: Snapshot of User Information acquiring option in Twitter

INFORMATION ACQUISITION FROM BROWSER CACHE USING WIN-UFO

One of the most useful techniques for collecting information (evidences) related to user activities on Twitter is to check the browser cache. One can find the URL of the particular webpage, the date and timestamps, frequency of visits, web browser and search engine used for searching, and the user account in the computer system from which the particular user was logged in. Even if the perpetrator uses the computer system of the victim with a different user account (unknown to the victim), for committing the crime, the evidence in the web browser cache can reveal this fact. Otherwise, it would appear as if the victim is involved in the particular incident (since the computer system of the victim is involved). This information can be accessed using an open-source tool "Win-UFO (Windows Ultimate Forensics Toolkit)". A snapshot of the analysis of information in browser cache using Win-UFO is given in Fig. 2.

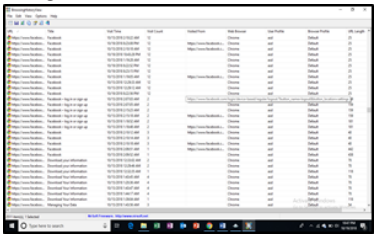

Figure 2: A snapshot of information about the use of Twitter from Browser Cache using tool Win-UFO

ANALYSIS OF RAM TO ACQUIRE INFORMATION

RAM is the volatile memory in the computer, which stores information for a temporary period of time. The password and traces of other evidences are stored in the RAM, irrespective of secured transmission over the network, when the user logs into their account. Other artifacts that can be acquired from the RAM include Facebook feeds, messages, comments and chats [7]. Even if the computer system (seized from crime scene) is found in hibernate state, the RAM is stored in the form of hiber.sys file, which can be analyzed using suitable tool. In case, the seized computer system is in sleep mode, the RAM still keeps working due to continuous power supply to the RAM, due to which analysis can be done easily.

INFORMATION ACQUISITION FROM TWITTER USING OSINT TOOLS

OSINT tools are Open-Source Intelligence tools, which are available on the internet and can acquire information about user accounts and user activities from Twitter, using the API of the microblogging site. These tools can extract information without the user aware that his/her data is being acquired. Some of the tools, which have been used for the purpose of this research include:

a) All My Tweets – This tool can acquire all the tweets of a user from the user account, including date and time of the tweet and embedded links shared, if any. However, it cannot extract multimedia contents from the tweets or from an account, which is private.

b) Twitter Audit – This is an OSINT tool, which can disclose the number of fake and real followers of a Twitter account based on an audit score generated for the account. A snapshot of the tool's result is given in Fig. 3

Figure 3: Identifying number of fake followers of Twitter account using Twitter Audit

c) Foller.me – This OSINT tool can provide a comprehensive analysis of the user's twitter account by analysing the followers, tweets, hashtags, topics and timeline analysis. A snapshot of the same is provided in Fig. 4

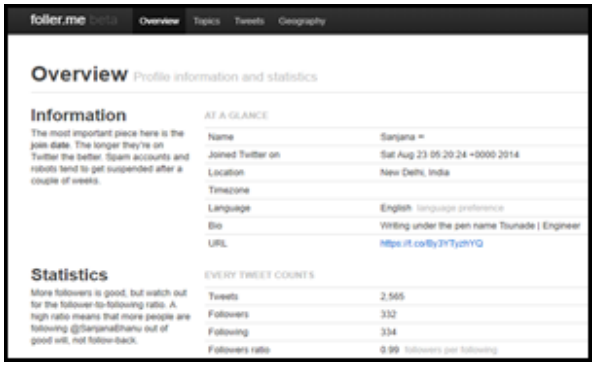

Figure 4: Comprehensive analysis of Twitter account using tool Foller.me

(d) OneMillionTweetMap – This is an open-source tool, which maps the last one million rela-time geo-localized tweets collected from the Twitter stream API. Using this tool, it is possible to collect all the tweets containing a particular hashtag, or analyze trend around the world, perform sentiment analysis etc., as shown in the snapshot in Fig. 5

(e) Advanced Twitter Search - Advanced Twitter Search is an in-built feature of the microblogging site, which allows the user to perform searching of tweets by customization of the search parameters. The search parameters include keywords/phrases, date range, people and locations/places.

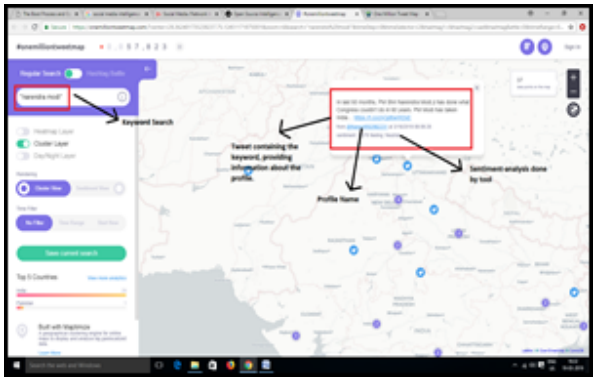

Figure 5: Identification and analysis of real-time geo-localized tweets using tool OneMillionTweetMap

CONCLUSION AND FUTURE SCOPE

On the basis of the experiments performed in this research work, it can be concluded that it is possible to perform forensic analysis of an incident related to Twitter by acquiring various information about a user with the use of different techniques and digital forensic tools available. Even if the user credentials are not available, the information can be acquired by indirect means with the use of OSINT tool or by analysis of browser cache and RAM, where it might be feasible to get hold of the username and the password.

In the future, we wish to extend this research work by using more tools and techniques and not by limiting our scope only to Twitter but also experimenting with other social media platforms like Facebook, Instagram, Snapchat etc.

REFERENCES:

[1] Ratkeiwicz J., Conover M.D., Meiss M., Goncalves B., Flammini A. and Menczer F. (2011), "Detecting and Tracking Political Abuse in Social Media." In: Proceedings of the 5th International AAAI Conference on Weblogs and Social Media, 297-304.

[2] Norouzizadeh D., Dehghantanha A., Choo K.K.R and Eterovic S. (2016), "Investigating Social Networking applications on Smartphones detecting Facebook, Twitter, LinkedIn and Google+ artefacts on Andoid and iOS platforms." In: Australian Journal of Forensic Sciences, 48(4), 469-488.

[3] M.G. de Paula A. (2010), "Security Aspects and Future Trends of Social Networks." In: The International Journal of Forensic Computer Science, 1, 60-79.

[4] Gupta A., Lamba H., Kumaraguru P. and Joshi A. (2013), "Faking Sandy: Characterizing and Identifying Fake Images on Twitter during Hurricane Sandy." International World Wide Web Conference (IW3C2), ACM-978-1-4503-2038, 729-736.

[5] Rubin V.L. (2017), "Deception Detection and Rumour Debunking for Social Media." The SAGE Handbook of Social Media Research Methods, London.

[6] Raychaudhuri K. and Nikita M. (2019), "An Empirical Study on Acquisition of Digital Evidences from Facebook Using Various Tools and Techniques." In Proceedings of International Conference on Emerging Trends and in Information Technology, LNEE-605, Springer, 1-14.

[7] Wong K., CT Lai A., Yeung J. C. K., Lee W. L. and Chan P. H. (2011). "Facebook Forensics." Valkyrie-X Security Research Group.