International Journal of Engineering and Management Research e-ISSN: 2250-0758 | p-ISSN: 2394-6962
Volume-12, Issue-4 (August 2022)
www.ijemr.net https://doi.org/10.31033/ijemr.12.4.1

The Role of Social Media Forensics in Digital Forensics

Dr. Vivekananth.P
HOD-IT/Senior Lecturer, Blue Crest University College, Accra, GHANA

Corresponding Author: vivek.jubilant@gmail.com

ABSTRACT

Social media forensics collects evidence from social media sites such as Facebook, WhatsApp, TikTok, and Snapchat to identify criminals. This paper discusses social media crimes such as hacking, photo morphing, shopping scams, cyberbullying, and link baiting. The paper deliberates the social media forensics techniques such as evidence collection, storing, analyzing, and preserving; the paper discusses the process of forensics examination in social media forensics. The paper examines the social media forensics tools such as WebPreserver, make a Website Hub, Pipl Search, TinEye, and TweetBeaver and discusses the applications of each device. The paper concludes by discussing the future of social media forensics.

Keywords— Social Media, Forensics, Cyber, Hacking

I. INTRODUCTION

"Social media forensics" collects evidence from social media sites such as Facebook, WhatsApp, TikTok, and Snapchat to identify criminals. “Digital forensics is a branch of forensic science encompassing the recovery and investigation of material found in digital devices, often associated with computer crime” (Pasquini et al., 2021). As technology continues to advance also, cyber-criminal cases continue to increase. Currently, 15% of social media users have encountered cybercrimes during their activities on various social platforms (Pasquini et al., 2021). They continue to rise. Hence, social media platforms majorly contain private and personal information; therefore, they tend to be hackers' targets to steal information and use it for criminal activities. Typical social media cyber-attacks include shopping scams, photo-morphing, link-baiting, cyberbullying, and hacking. Cybercriminals typically use cookies or denial of service (DoS) to steal; hence, they tend to be hackers' targets to steal information and personal information on social media platforms (Prieto Curiel et al., 2020). Investigators use social media forensics tools such as WebPreserver, make a Website Hub, Pipl Search, TinEye, and TweetBeaver to investigate social media crimes.

II. TYPES OF SOCIAL MEDIA CRIMES

Hacking

Hacking refers to compromising technological devices such as computers and networks via illegal access to computer systems or an account (Pasquini et al., 2021). Hacking is not always criminal activity, but it is often defined as unlawful when it harms someone. The current most famous hackers are "white, dark, dim, and blue cap hackers"(Pasquini et al., 2021). White hat hackers assume a considerable part in contemporary society. A current instance of hacking is the hacking of the Twitter accounts of Jeff Bezos, Elon Musk and Bill gates (Choi et al., 2022). The hackers tweeted promising to double the Bitcoin so that people would surrender to the Bitcoin addresses posted.

Photo Morphing

Photo morphing implies changing flawlessly, starting with one picture and then onto another, using morphing instruments accessible on the web (Bhongale, 2021). Typically, young Young ladies are impacted because of these kinds of transforming who download young ladies' pictures from different social sites through their phones or genuine profiles and afterwards change them. These altered images might be used to extort the young lady or her family by taking steps to distribute the altered pictures. An instance of photo morphing was the Indian case in which an “attacker used a local woman's face and morphed it onto a nude photograph, and circulated the doctored image on social media” (Choi et al., 2022).

Shopping Scams

Internet scams are various types of frauds that are carried out by cybercriminals on the internet. Scams like phishing emails, SMS messages, and social media posts happen differently. Shopping scams involve criminals who pretend to be trustworthy online sellers with fake websites. Scammers request one to pay via a pre-loaded money card or other online money transfer platforms. For instance, the case of Berrylook.com on Facebook is one of the current scams (Choi et al., 2022). Many people have reported purchasing items via this website but never received what they bought even after paying online.

Cyberbullying

Cyberbullying is terrorizing and niggling people using the web, especially for virtual entertainment. Melanie Griffith, an actress, explains that she has been cyberbullied through hateful tweets concerning her plastic

surgery and her general physical appearance. According to her interview, many people tweeted that she looked horrible (Choi et al., 2022).

Link Baiting

Link baiting is also another way that is used by cybercriminals (Basumatary & Kalita, 2022). In this, users are lured into opening unsecured links that steal their personal and financial information. Instances of link baiting are the fraudulent links that scammers tell people that they will direct them to forex trading sites such as cryptocurrency. Many victims report having lost their money in banks, and after investigation, many of them are found to have opened insecure links on their devices that steal their personal information.

III. PROCEDURE OF SOCIAL MEDIA FORENSICS

The increased rates of social media crimes have led to an increasing need for social network forensics. Social media forensics incorporates digital analysis and cyber investigation evaluation methods to collect, store, analyze, and preserve information that could be useful in courts of law in the event of criminal activity.

Determining the Crime Scene and Evidence Collection

The first step of social media forensics is inspecting and determining the crime scene that is worth investigating. After identifying the source, the forensic investigators can use the following methods for evidence collection; manual documentation. Open-source tools (HTTrack), web services (page freezer), content subpoena, commercial toll (X1), and forensic recovery (Basumatary & Kalita, 2022).

Storing of Forensic Evidence

As the investigation continues and for evidence, the information can be stored in digital storage such as hard disk drives and other external storage such as flash memory. Storage of forensic evidence is either physical or computerised capacity frameworks, or ideally in a savvy board framework that can coordinate with proof administration frameworks.

Analysis of Forensic Evidence

Files and information acquired during evidence collection need specific tools for decoding and analysis. Tools such as file viewers and file analysis tools, email analysis tools, registry analysis tools, database forensics tools, mobile device analysis tools, and network and internet tools are used to analyze social media forensics.

IV. FORENSICS EXAMINATION IN SOCIAL MEDIA FORENSICS

The primary stages of forensic examination are extraction, storing, analysis, and documentation (Bhongale, 2021). The concerned team must determine the crime scene and locate the device or software affected. This step involves a primary search to choose the social media accounts linked to the crime. It can involve a search for friends or any other close person. The forensic examiner would then record all the sources identified and how they acquired the evidence. This means that the second step is to collect the electronic evidence from various social media platforms using the possible tools for the social media data extraction method. The last step is the examination and organization of the evidence. Utilizing the examination tools for viewing and decoding the collected evidence offers data on malicious cyber activity (Powell & Haynes, 2020). Documentation is vital since it aids in recreating the crime scene and future reviews.

IV. SOCIAL MEDIA FORENSICS TOOLS

Social media forensic tools for investigations all focus on offering detailed information concerning cybercrime involving various social media platforms.

Pipl

Pipl collects information about online archives; hence, it can be collected on all social media platforms. It only requires one data point, such as an email address or phone number, and can provide all other data (Tan & Zhang, 2021).

WebPreserver

WebPreserver is an auto-preservation tool for web material and social media that can gather information within a short period. It can extend collapsed responses and comments (Thouvenin et al., 2018). The threads and articles expose the evidence required; it can record profiles of various social media platforms.

Makeawebsitehub

Makeawebsitehub regularly keeps a rundown of the most recent interpersonal interaction applications, which might be exceptionally gainful for expanding your web examinations and finding those less popular locales that might be hiding important information (Spencer, 2021). Thus, it aids in determining the issues that might arise in social media applications and networks.

TinEye

TinEye is a simple tool for getting original images and doing reverse image searches. Once one uploads a picture, TinEye can see other places on the internet where the image has been used. It helps find the source of social media images (Kondal & Singh).

TweetBeaver

Tweetbeaver is a tool that enables one to get a lot of data from any public Twitter account in a short period. It detects and analyses relationships between Twitter accounts (Lyndon et al., 2022).

V. THE FUTURE OF SOCIAL MEDIA FORENSICS

As technology advances, various social media platforms continue to be discovered, and the cybercrimes associated with these platforms continue to increase. According to recent reports, the market size of social media forensics may continue to grow. This is because of the increasing number of cases. For instance, in 2020, Google registered two million, which was the highest number compared to the previous years (Alonso-Fernandez et al., 2021). The future of social media forensics will be to digitalize everything and ensure guards that would help quickly to detect any criminal activity. Social media platforms depend on the most recent technology, and forensics should keep in touch with the new technology. There is a need to increase the social media forensics team. More comprehensive data strategies continue to assist in evidence collection and analysis. The future social media forensic industry is thus predicted to grow by 17% before 2026, as per the Bureau of Labor Statistics (Powell & Haynes, 2020). More developments, such as the Incognito Forensic Foundation, continue to be implemented to provide a wide range of social media forensics services.

REFERENCES

[1] Alonso-Fernandez, F., Belvisi, N. M. S., Hernandez-Diaz, K., Muhammad, N. & Bigun, J. (2021). Writer identification using microblogging texts for social media forensics. *IEEE Transactions on Biometrics, Behavior, and Identity Science*, *3*(3), 405-426.

[2] Arshad, H., Jantan, A. & Omolara, E. (2019). Evidence collection and forensics on social networks: Research challenges and directions. *Digital Investigation*, *28*, 126-138.

[3] Basumatary, B. & Kalita, H. K. (2022, Ma). Social media forensics-A holistic review. In: *9th International Conference on Computing for Sustainable Global Development (INDIACom)*, pp. 590-597.

[4] Bérubé, M., Tang, T. U., Fortin, F., Ozalp, S., Williams, M. L. & Burnap, P. (2020). Social media forensics applied to the assessment of post-critical incident social reaction: The case of the 2017 Manchester Arena terrorist attack. *Forensic science international*, *313*, 110364.

[5] Bhongale, J. (2021). *Crime against women in cyber world*. Available at: SSRN 3903959.

[6] Chang, M. S. & Yen, C. P. (2019). Forensic analysis of social networks based on instagram. *Int. J. Netw. Secure.*, *21*(5), 850-860.

[7] Kondal, M. & Singh, V. (2020). *Comparative analysis of tineye and google reverse image search engines*.

[8] Lyndon, R., Tse, V., Moore, L. & May-Hobbs, M. (2022). *Disinformation in Brazil: The 2019 Amazon Fires on social media*.

[9] Pasquini, C., Amerini, I. & Boato, G. (2021). Media forensics on social media platforms: a survey. *EURASIP Journal on Information Security*, *2021*(1), 1-19.

[10] Powell, A. & Haynes, C. (2020). Social media data in digital forensics investigations. In: *Digital Forensic Education*, pp. 281-303. Springer, Cham.

[11] Prieto Curiel, R., Cresci, S., Muntean, C. I. & Bishop, S. R. (2020). Crime and its fear in social media. *Palgrave Communications*, *6*(1), 1-12.

[12] Spencer, J. (2021). *101 social networking sites you need to know about in 2022*.

[13] Tan, Z. & Zhang, C. (2021). China's PIPL and DSL: Is China following the EU's approach to data protection?. *Journal of Data Protection & Privacy*, *5*(1), 7-25.

[14] Thouvenin, F., Hettich, P., Burkert, H. & Gasser, U. (2018). 4 web archives. In: *Remembering and Forgetting in the Digital Age*, pp. 84-101. Springer, Cham.

[15] Choi, K. S., Lee, H., Park, G. & Han, C. (2022). Virtual reality program in cybercrime investigation: a pilot study examining search and seizure of digital evidence practice. *Cyberpsychology, Behavior, and Social Networking*, *25*(1), 43-50.