The Role of Digital Forensics in Cybercrime on Twitter Social Media

Rahma Azzahra[1)], Intan Rachma Dina[2)]

[1-2)] Informatics Engineering Student, Faculty of Science and Technology, Nahdlatul Ulama University Sunan Giri Bojonegoro

Correspondence Author: rahmaazzahra333@gmail.com

Article Info :

Article History :

Received :
26 January 2024
Revised :
27 February 2024
Accepted :
03 April 2024
Available Online :
03 April 2024

Keyword :
Digital Forensics, Cybercrime, Social media, Twitter

ABSTRACT

The rapid advancements in information technology in the current era have significant positive and negative effects. One notable benefit of these developments is the ease with which individuals can access information and communicate with others through social media platforms. However, a major drawback is the irresponsible behavior exhibited by some users, leading to an increase in cybercrime. Twitter, in particular, is frequently targeted for such criminal activities. Digital forensics, a specialized branch of forensic science, focuses on the identification and recovery of data, particularly related to computer crimes. This initiative aims to highlight the risks of cybercrime associated with social media platforms like Twitter. The research conducted seeks to gather digital evidence by utilizing one specific method endorsed by the National Institute of Justice (NIJ), which encompasses the following stages: Collection, Examination, Analysis, and Reporting.

1. INTRODUCTION

Rapidly developing technology offers the same benefits and effects depending on the user of the technology. The positive benefit of technology is that it makes it easier for individuals or groups to carry out their activities, while the negative impact is the misuse of technology by individuals or groups to commit crimes that can harm other people. However, the various advances that exist are also accompanied by the development of technology, which on the other hand can make it easier for users to commit crimes using computers as a tool for committing crimes, or what is usually called cybercrime.

Cybercrime itself is a term for any person, group of people, or legal entity that uses computers as a means to commit crimes that use computers as the object. In general, crimes committed by cybercrime leave traces so that they can be used as evidence (Riskiyadi, 2020). So it is necessary to implement a forensic investigation which aims to carry out investigations related to criminal incidents and other legal issues and find out the facts. Handling cybercrime cases through an investigation process is known as digital forensics (Khotimah, 1970). Digital forensics/digital forensics is a branch of material examination (computers, laptops, network devices, storage media and the like) (World Health Organization; London School of Hygiene and Tropical Medicine, 2017). In another sense, digital forensics is the process of collecting and analyzing data from

ISSN Print : 1979-7141
ISSN Online : 2541-1942

computer systems, networks and storage devices that can be used as evidence in law enforcement (Prayudi and Afrianto, 2005).

Apart from the digital divide, cybercrime in the current era most frequently occurs on social media, especially on Twitter. Social media itself is online media that users can follow easily. In the sense that someone easily shares information, creates content or comments on content that other people want to share, feedback received, etc. (World Health Organization; London School of Hygiene and Tropical Medicine, 2017). Because social media is one of the main means for people to obtain important information (Dwipayana, Setiyono and Pakpahan, 2020) which cannot be separated from people's lives with fast and unlimited access (Ramadhan and Nurnawati, no date). The most frequently used social media today is Twitter. Twitter is a social media that is used as a place to express oneself, but in reality users misuse this media as a means of conflict (Debora Maria Paramita Pasaribu, 2015). A special feature of Twitter is that users can send messages with a minimum of 140 characters (World Health Organization; London School of Hygiene and Tropical Medicine, 2017). But people use Twitter apart from being a source of the latest information, they also use this social media as a means of protest, political campaigns and emergency communication (Of et al., 2020).

Even though the use of social media can be easy to use, in the case of this development it has several problems due to the increasing sophistication of technology on Twitter social media.

2. METHOD

According to (Of et al., 2020) research methods are a way to achieve the expected goals through research using techniques that have been determined using tools and materials.

The method used in this research is the National Institute of Justice (NIJ). The National Institute of Justice (NIJ) method is a research method that aims to explain how the research steps will be carried out so that the flow and steps can be systematically identified so that they can be used as a guide for solving existing problems (Agustian and Ramadhani, 2022).

The research stages are:

1. Collection is the initial stage of analyzing needs to collect items that you want to carry out, such as visualization and recording, based on certain data sources.
2. Examination at this stage reviews the stages of data collected during the collection phase.
3. Analysis is an analysis of examination results using established methods to obtain all the necessary information.
4. Reporting: At this final stage, what is done is to complete the report and explain what was analyzed and then present the evidence found.

3. RESULTS AND ANALYSIS

It can be said that digital forensics is a step to safeguard, collect, store, analyze and present evidence related to digital objects. This action is a step in the acquisition and analysis of information in digital form to be used as evidence in court. Fast-growing technological advances also involve security systems that continue to develop. Responding to cybercrime activities which continue to increase drastically. As a result, cybercrime is increasingly active and faster to achieve new successes against the security systems created by digital cyber forensics. A very worrying condition occurs when cybercrime perpetrators are experts in anti-cybercrime, so new areas of cybercrime are difficult for digital forensic investigators to detect and solve.

Digital forensics has the goal of securing and analyzing digital evidence, various objective facts from information systems, supporting the process of identifying and investigating evidence, facilitating the evidentiary process in a relatively quick time, and calculating the potential impact of criminal acts committed by perpetrators on victims (Frayitno , 2021).

Gen Z always wants to express themselves quickly through various portable devices or media and publish them on various types of social networking platforms. What is most likely to happen in social networking crime is providing or sending a link that looks very interesting, but after accessing the link it turns out to contain malware or spyware which will send all the accessing information to the sender of the link. The mechanism or method for using social networks safely and comfortably, especially among young people or Gen Z, is to be careful when sharing personal

ISSN Print : 1979-7141
ISSN Online : 2541-1942

data, don't click on links that look suspicious, avoid downloading unknown files, use two factor authentication, verify the email sender. , enable spam filters, and antivirus. Installing antivirus on a device is a way to minimize the risk of impacts caused by various computers (Amin, 2022).

These positive and negative impacts tend to become more open so that some people take advantage of them to carry out various kinds of internet abuse which tends to lead to criminal acts in cyberspace. The emergence of various crimes in cyberspace must be balanced by adequate law enforcement. Understanding for all of us (society), especially regarding crimes that may occur in cyberspace. Based on the literature analysis, seven main forms of cyber abuse and their operational characteristics were identified:

1. Carding:
   Financial fraudulent activity through the illegal use of credit card numbers and other parties' identities for electronic transactions. This practice causes direct economic losses to victims and financial institutions (Moore & Clayton, 2008).

2. Hacking:
   Refers to the actions of individuals with high technical competence in computer system analysis, including the ability to modify and understand program structures. Although technically neutral, this term is often associated with unauthorized system exploitation (Taylor, 1999).

3. Cracking:
   Unlike hacking, cracking specifically targets violations of software security mechanisms (such as license protection or authentication) for commercial purposes or vandalism (Turgeman-Goldschmidt, 2005).

4. Defacing:
   A form of digital vandalism by forcibly changing the appearance of the interface (usually a website). Although often motivated by a demonstration of ability (for fun), this activity is often accompanied by the theft of sensitive data to be sold to third parties (Denning, 2010).

5. Phishing:
   A psychological manipulation-based fraud technique to trick victims into sharing vital credentials (passwords, credit card details), particularly targeting online banking users through fraudulent electronic communications (Jakobsson & Myers, 2006).

6. Spamming:
   The sending of mass electronic messages (especially emails) containing unsolicited advertisements or promotions. In addition to being annoying, this activity is a vector for the distribution of malicious links and scams (Hansell, 2007).

7. Malware:
   Malicious programs designed to infiltrate, damage, or take over systems by exploiting software vulnerabilities. This category includes viruses, worms, Trojan horses, adware, and browser hijackers (Szor, 2005).

Crime on the internet shows that almost every activity in cyberspace can occur. This vigilance does not mean that we have to switch and leave the internet, but instead we have to deepen our knowledge of the features on the internet. Irresponsible third parties cannot use it as a flaw.

ISSN Print : 1979-7141
ISSN Online : 2541-1942

3.1 Types of Crime That Often Occur on the Internet or Cyberspace

1. Illegal Acces

   It is a crime committed by infiltrating/penetrating a computer network system illegally and without permission or without the knowledge of the user of the computer network system he is entering (Arifah, 2011).

2. Illegal Contents

   It is a crime to enter information on the internet about something wrong, unethical and pretentious that violates the law or disturbs public order (Arifah, 2011).

3. Data Forgery

   It is a crime to falsify important document information stored as written documents via the internet (Arifah, 2011).

4. Cyber Espionage

   It is a crime to use the internet to carry out spying activities against other parties, by entering the target computer network system (Fitriani and Pakpahan, 2020).

5. Cyber Sabotage and Extortion

   It is a crime committed by causing interference, destroying or destroying data, a computer program or a computer network system connected to the internet (Arifah, 2011).

6. Offense Against Intellectual Property (Violation of Intellectual Property Rights).

   It is a crime that violates other people's intellectual property rights on the internet (Arifah, 2011).

7. Infringements of Privacy (privasi Infringements)

   This is a crime that is usually directed at personal data stored in computerized personal information forms (Arifah, 2011).

8. Denial of Service Attack / DoS Attack

   It is an attack aimed at a computer system or network which can cause the system to be unable to provide services to users (Murti, 2005).

3.2 Reasons for the Emergence of Cybercrime

Based on literature analysis, there are three main causal factors that drive cyber abuse activities:

1. Economic Factors (Financial Problems):
   Financial motives are the main driver of cybercrime, where perpetrators exploit system vulnerabilities to obtain material benefits illegally (Leukfeldt et al., 2017).

2. Geopolitical and Ideological Factors:
   Cyber activities are often motivated by political, military, or nationalist sentiment agendas, including hacktivism aimed at disrupting opposing entities (Denning, 2010).

3. Perpetrator's Psychological Factor (Perpetrator's Satisfaction Factor):
   Psychological aspects such as the need for recognition, demonstration of technical competence, or intrinsic gratification also explain non-instrumental motivation in cyber vandalism (Turgeman-Goldschmidt, 2005).

Technological Evolution and the Role of Social Media. In line with technological developments, there has been a significant increase in the use of social media. The latest data shows that the annual growth of social media users has reached 9.2% globally (We Are Social,

ISSN Print : 1979-7141
ISSN Online : 2541-1942

2023). This platform has transformed private communication into public information dissemination, creating an interactive ecosystem based on internet technology. Twitter, as one of the main dissemination channels, facilitates the acceleration of information dissemination through two key mechanisms:

1. Search Bar Catalog Feature: Enables real-time tracking of high-frequency keywords that reflect public interest (Karami et al., 2020).

2. Trending Topics Algorithm: Amplifies content visibility through analysis of the volume and velocity of user interactions (Borra et al., 2015).

These two features synergistically increase the potential for content virality while dynamically forming public agenda-setting.

3.3 Cyber Crime Cases (Cybercrime) on Twitter

1. Defamation Case

   In 2014, a person with the initials EE, a resident of Gedongan, Bantul, Yogyakarta, who was reported to the police, allegedly uploaded a status to the media regarding her husband's mutation. And after the examination, EE was named a suspect in the case. The prosecution of perpetrators guilty of defamation via Twitter depends on the ITE Law Article 27 paragraph 3 because defamation cannot be prosecuted under the Criminal Code. Article 27 paragraph 3 of the ITE Law is a dissemination offense so it focuses on who deliberately disseminated the tweet upload (Debora Maria Paramita Pasaribu, 2015).

2. Cases of Spreading or Hate Speech

   In 2017, a case of hate speech by someone with the initials AD was reported to the police for spreading information that caused hatred by tweeting on his personal Twitter account. One of the criminal laws that regulates cases of hate speech is contained in Article 156 of the Criminal Code. Article 156 of the Criminal Code regulates that "Anyone who in public expresses feelings of enmity, hatred or insult towards some group of Indonesian people" faces a penalty of six years in prison or a fine (Hastak and Risal, 2021).

3. Case of Spreading Fake News (Hoax)

   In 2019, there were 26 reports regarding the spread of incorrect information on social media, of course Twitter about child kidnapping. This makes people anxious, especially parents who have small children. In Law No. 1 of 1946, article 14 paragraph 1 states that perpetrators of spreading hoax news that can cause trouble in the community receive a maximum criminal penalty of 10 years in prison. Meanwhile, Law No. 1 of 1946 paragraph 2 states that perpetrators who spread hoaxes that cause trouble among the people, and the perpetrators think that the hoax news is in fact a lie, will be sentenced to 3 years in prison (Trisna, 2016).

4. Online Buying and Selling Fraud Cases

   In 2017 there was a disclosure of a case by the victim which started with a victim buying a Channel brand bag through an account for IDR 37.5 million. The victim who was offered the item was interested and interested so he made a transaction by transferring money for that amount but the item was never sent. In Law No.11 of 2008 concerning

ISSN Print : 1979-7141
ISSN Online : 2541-1942

Electrical Information and Transactions and Law. No. 17 of 2016 as amended into Law No. 1 of 2008 which explains Electronic Information and Transactions (UU ITE). The ITE Law itself is the first law that regulates electronic transaction activities in Indonesia, and provides legal reforms aimed at guaranteeing the interests of society so that legal certainty is guaranteed for transactions using electronic media (Kamran and Maskun, 2021).

4. CONCLUSION

Digital forensic science has a very important role in detecting cybercrime, namely recovering data deleted by criminals and assisting investigators in carrying out analysis related to digital evidence used by cybercriminals. Likewise, the increasing development of the internet world can have positive and beneficial impacts on users, as well as negative impacts that follow along with the development of the internet. One of them is Cybercrime or cybercrime. And social media is a platform that is very easy to misuse for cybercrime. Where many cybercrime cases occur on various social media, one of which is Twitter.

5. DECLARATION OF COMPETING INTEREST

We declare that we have no conflict of interest.

6. REFERENCES

Agustian, S. and Ramadhani, S. (2022) 'Jurnal Computer Science and Information Technology (CoSciTech) menggunakan algoritma lexrank', 3(3), pp. 371–381.

Amin, M. (2022) 'Antisipasi Kejahatan Dunia Maya (Cyber Crime) Terhadap Media Jejaring Sosial Pada Gen-Z'.

Arifah, D.A. (2011) 'KASUS CYBERCRIME DI INDONESIA Indonesia's Cybercrime Case', *Jurnal Bisnis dan Ekonomi (JBE)*, 18(2), pp. 185–195.

Debora Maria Paramita Pasaribu, S. &Sri S. (2015) 'Diponegoro law journal', *Serambi Hukum*, 6(02), pp. 1–13. Available at: https://www.academia.edu/34113996/EKSISTENSI_HUKUM_KONTRAK_INNOMINAT_DALAM_RANAH_BISNIS_DI_INDONESIA.

Dwipayana, N.L.A.M., Setiyono, S. and Pakpahan, H. (2020) 'Cyberbullying Di Media Sosial', Bhirawa *Law Journal*, 1(2), pp. 63–70. Available at: https://doi.org/10.26905/blj.v1i2.5483.

Fitriani, Y. and Pakpahan, R. (2020) 'Analisa Penyalahgunaan Media Sosial untuk Penyebaran Cybercrime di Dunia Maya atau Cyberspace', *Cakrawala : Jurnal Humaniora*, 20(1), pp. 2579–3314. Available at: http://ejournal.bsi.ac.id/ejurnal/index.php/cakrawala.

Frayitno, D. (2021) 'Kementerian pendidikan, kebudayaan, riset, dan teknologi universitas borneo tarakan fakultas hukum 2021', p. 2052558.

Hastak, H. and Risal, M.C. (2021) 'Tinjauan Yuridis Terhadap Tindak Pidana Ujaran Kebencian Di Media Sosial', *Alauddin Law Development Journal*, 3(1), pp. 148–157. Available at: https://doi.org/10.24252/aldev.v3i1.14766.

Kamran, M. and Maskun, M. (2021) 'Penipuan Dalam Jual Beli Online: Perspektif Hukum Telematika', *Balobe Law Journal*, 1(1), p. 41. Available at: https://doi.org/10.47268/balobe.v1i1.501.

Khotimah, K. (1970) 'Islam dan Globalisasi: Sebuah Pandangan tentang Universalitas Islam', *KOMUNIKA: Jurnal Dakwah dan Komunikasi*, 3(1), pp. 114–132. Available at: https://doi.org/10.24090/komunika.v3i1.118.

Murti, H. (2005) 'Cybercrime-2214-Article Text-1828-1-10-20140306', X(1), pp. 37–40.

Of, C. *et al.* (2020) 'Komparasi Kejahatan Di Twitter Dan Instagram Dengan Pendekatan Digital Forensic Investigation Comparison of Crime on Twitter and Instagram With a', *Jurnal*

ISSN Print : 1979-7141
ISSN Online : 2541-1942

Bina Komputer, 3, pp. 1–8.

Prayudi, Y. and Afrianto, D.S. (2005) 'Antisipasi Cybercrime Menggunakan', *Jurnal Fakultas Hukum UII*, 2005(Snati). Available at: https://www.neliti.com/publications/88691/antisipasi-cybercrime-menggunakan-teknik-komputer-forensik.

Ramadhan, I.H. and Nurnawati, E.K. (no date) 'Analisis Kesadaran Mahasiswa Terhadap Bahaya Cybercrime Di Media Sosial', (28).

Riskiyadi, M. (2020) 'Investigasi Forensik Terhadap Bukti Digital Dalam Mengungkap Cybercrime', *Cyber Security dan Forensik Digital*, 3(2), pp. 12–21. Available at: https://doi.org/10.14421/csecurity.2020.3.2.2144.

Trisna, F.R. (2016) 'Tindakan Hukum Terhadap Penyebaran Berita Bohong (Hoak) Di Media Sosial Berdasarkan Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik', *Jurnal Fakultas Hukum Universitas Airlangga Surabaya*, pp. 1–23.

World Health Organization; London School of Hygiene and Tropical Medicine (2017) 'No 主観的健康感を中心とした在宅高齢者における 健康関連指標に関する共分散構造分析Title', *BMC Public Health*, 5(1), pp. 1–8. Available at: https://ejournal.poltektegal.ac.id/index.php/siklus/article/view/298%0Ahttp://repositorio.unan.edu.ni/2986/1/5624.pdf%0Ahttp://dx.doi.org/10.1016/j.jana.2015.10.005%0Ahttp://www.biomedcentral.com/1471-2458/12/58%0Ahttp://ovidsp.ovid.com/ovidweb.cgi?T=JS&P.

Zuhriyanto, I., Yudhana, A. and Riadi, I. (2018) 'Perancangan Digital Forensik pada Aplikasi Twitter Menggunakan Metode Live Forensics', *Seminar Nasional Informatika 2008 (semnasIF 2008)*, 2018(November), pp. 86–91.

ISSN Print : 1979-7141
ISSN Online : 2541-1942