International Journal of Education and Life Sciences (IJELS)
Vol. 2, No. 12, 2024 : 1387-1394

Detecting Cyber Crime for Forensic Computer Handling using OSINT

Salza Aulia Fitri[1], Muhammad Ramadhan[2], Raffi Ciputra[3], Emis Sita Eriana[4], M.Irham[5]
Pamulang University

Corresponding Author: Salza Aulia Fitri: **salzaaf03@gmail.com**

A R T I C L E I N F O
Keywords: Cyber Crime, OSINT, Computer Forensics

Received : 12, Oktober
Revised : 20, November
Accepted: 3, December

A B S T R A C T
In handling computer forensics with backward chaining, the cybercrime detection expert system serves to detect cybercrime crimes committed by criminals. Problems encountered include how to detect cybercrime crimes committed, articles that correspond to cybercrime crimes committed, and what punishment should be given to cybercrime offenders. This article provides a brief explanation of the meaning of forensics, techniques, and applications with various applications available: This expert system uses observation, interviews, and literature studies. into a system that uses hypertext preprocessor programming (PHP) and MySQL database. The design that uses HTML and CSS during the process of making this system can help in the process of detecting and handling internet violations. to supervise the forensic stove, so as to be able to find out with the type of crime committed easily and cyber crime law. The search results show that live forensic, network forensic, and mobile forensic are the most handled crimes, with a trend topic graph above 10. In contrast, computer and database forensics only have two courses.

DOI: https://doi.org/10.59890/ijels.v2i12.2788
https://journal.multitechpublisher.com/index.php/ijels

INTRODUCTION

The world of information and computer technology (ICT) has progressed very rapidly, especially since the advent of networking, or technology that connects computers, and the Internet. However, this progress has been followed by the development of the other side gof technology, which has resulted in the use of computers as a tool to commit various types of crimes. The term "cybercrime" then emerged.

Based on the Honeynet Project 2021 annual report by the National Cyber and Crypto Agency (2021), Indonesia ranks second internationally as the country with the highest source of cyberattacks with a total of 32,091,240 attacks. Therefore, cybersecurity is an important sector to develop, especially through research in line with the industrial revolution.

The practice of collecting, analyzing and reporting digital data is the foundation of digital forensics. Digital forensic investigations have many applications. The term "forensic sciencefield" or "forensics" refers to the investigation of crimes using scientific methods or is used to describe crime detection in general. It is an attempt to answer questions of interest to the legal system using various sciences. The onset of infringing, violating, and inappropriate behavior leads to the emergence of forensics. (Rahayu Selamat et al. 2013).

Nowadays, cybercrime, or what we commonly know as cybercrime, is increasing in number and varying in type, such as piracy of computer programs, cracking, carding, pornography, bank break-ins, and various other types of crimes. In many cases, the law dealing with cybercrime still has limitations in determining the perpetrators of cybercrimes that occur. This has resulted in many perpetrators receiving no punishment or who still have not received punishment in accordance with their actions. Because of the many problems, the author intends to conduct a research entitled "Detecting Cyber Crime for Computer ForensicHandling using OSINT".

RASEARCH METHOD

To gather information relevant to the topic or problem to be discussed in this paper, the author uses a literature study. Namely, data collection techniques by conducting a study of books, literature, notes, and existing reports. Efforts to collect such information can be obtained from scientific books, research reports, scientific essays, theses and dissertations, regulations, decrees, yearbooks, encyclopedias and other printed and electronic written sources. Furthermore, to obtain clear characteristics of the discourse in the form of theories and concepts studied, the author uses the content analysis method, which is a research technique to make inferences that can be replicated (replicated) and valid data by paying attention to the context.

LITERATURE REVIEW

Cybercrime is a group of acts committed by people by creating disruptions in networks, stealing other people's important and personal data, documents, hacking bank and account details, and transferring money to their own accounts (Goni 2021). According to some online sources (Cyber Crime Increases Sharply During the Pandemic-Faculty of Social and Political Sciences-Universitas Indonesia, n.d.), cybercrime is defined as an illegal act committed by perpetrators who use the technology of the victim's computer network information system to directly attack their information system (Cyber Crime Increases Sharply During the Pandemic-Faculty of Social and Political Sciences-Universitas Indonesia, n.d.). In a broader sense, cybercrime can also be defined as illegal acts committed by perpetrators who use the victim's computer network information system technology to directly attack their information system. In a broader sense, cybercrime can also be defined as illegal activities facilitated by technology.

Cybercrime is a type of crime that uses the internet as its main tool and falls under the category of lawlessness (Jubaidi and Fadilla 2020). As a result, these sources conclude that cybercrime involves criminal activities that use computer technology, especially the internet, to commit various types of crimes, such as data theft, hacking, and network disruption. One type of law violation is cybercrime.

Digital forensics is the investigation and analysis of computer data to find possible legal evidence. It differs from the general definition of forensics, and can be interpreted as the collection and analysis of data from various computer resources, such as computer systems, networks, communication lines, and various storage media that can be used in a trial. In a publication titled "Problems and Solutions of the Digital Custody Chain in Cybercrime Investigations" (Prayudi and SN 2015) the relationship with evidence is an important component in the investigation process. Electronic and digital evidence are two terms that are almost synonymous in this context. Digital evidence is electronic evidence, which is visually recognizable and physical in nature, such as computers, mobile phones, cameras, CDs, and hard drives, etc.). Digital evidence, on the other hand, is evidence extracted or obtained from electronic items, such as files, emails, SMS, photos, videos, logs, and texts. The basic definition is "The use of a set of procedures to thoroughly test a computer system using software and tools to extract and preserve evidence of criminal acts". According to Judd Robin, a computer forensic expert: "The simple application of computer investigation and analysis techniques to determine possible legal evidence". New Technologies expands Robin's

DOI: https://doi.org/10.59890/ijels.v2i12.2737
https://journal.multitechpublisher.com/index.php/ijels

definition with: "Computer forensics is concerned with the preservation, identification, extraction and documentation of computer evidence stored as magneticinformation".

DISCUSSION

Digital Forensics is a branch of forensic science that focuses on the investigation anddiscovery of content from digital devices, especially in relation to computer crimes. While the terms Digital Forensics and Computer Forensics were originally considered synonymous, they have now been expanded to include all devices capable of storing digital data and are the subject of digital forensic investigations. Digital Forensics was first used when personalcomputing became popular in the late 1970s and early 1980s. As the internet began to develop in the 1990s, the use of digital forensics expanded. It was not until the early 21st century thatcountries around the world slowly began to form policies and guidelines in theimplementation of digital forensics (Wijatmoko, 2021). Like other forensic sciences, Digitalforensics involves the use of technology, tools, and complex procedures that must befollowed to ensure accurate evidence collection and proper outcomes. The basic principles of computer forensics are similar to the processes used by the police in the investigation of crime evidence. However, in computer forensics, the processes and events take place in cyberspace. In addition to collecting relevant evidence, the proper use of computer forensics can result inthe exoneration of innocent individuals or bring perpetrators of crimes to justice.(Agri Chairunisa Isradjuningtias and Pradana 2023)

The process in cyber crime investigation is also organized into several steps as a reference in the development of the investigation. Several frameworks in digital forensic investigation are applied depending on the specific case or objective to achieve the desired result by the investigator. Generally, frameworks are suggested for specific fields and are based on practitioners' experience and previous work. These frameworks or process models are essential to speed up the process of digital forensic investigations. (Arshad et al. 2022) Likethe CDFIPM model, which is a process model for dealing with identified problems, such as harmonizing and building on existing models (Montasari 2016). (Montasari 2016). Other models focus on a specific area and make modifications to focus on online social networking(Virmani et al. 2022). (Virmani et al. 2022)..

Open-Source Intelligence (OSINT) is one of the fields of data collection (Pai U. and K. 2021). OSINT consists of the collection, processing, and correlation of public information from open data sources such as mass media, social networks, forums and blogs, government public data, publications, or commercial data. (Pastor-Galindo et al. 2020)]. By utilizing OSINT to collect data, it can help in the process of investigating cybercrime cases. The amount of data available from forensic digital evidence analysis suggests that there is a wealth of information that could potentially be enhanced with

open-source intelligence data to enable a better understanding of events or people, and greater decision-making opportunities.

Open Source Intelligence (OSINT) is the right place to gather information and conduct investigations on terror groups that play in the online space. With a computer device with a stable internet connection, security forces can get as much information as possible without requiring specific skills because all online investigative tools and databases are publicly available.(Lavinia 2023)

Case Scenario

The simulation data used in this study was obtained from a Huawei Y3II smartphone device. The scenario was prepared because the National Institute of Standards and Technology (NIST), a non-regulatory body under the Technology Administration section of the United States Department of Commerce, states that in order to conduct testing, all tools and devicesmust be registered. Simulation procedures are necessary in this study to mimic the behavior of the actual system to prove the problem formulation. Since it is not possible to investigate real-world scenarios, simulation was used. The data used in the investigation is collected from the device under investigation.

According to research references from (Tajuddin et al. 2019) the scenarios that will be carried out at this stage are as follows:

The suspect is a cyber actor who has the data from the data leak incident and istrying to sell and buy it.

Digital evidence in the form of media that carries data obtained from the suspect.

By storing evidence in local storage, the media in question will be found on the smartphone as primary evidence.

Anti-forensic techniques such as tampering, data hiding, and data deletion on the transmission medium are used.

A smartphone was then purchased as primary evidence, which was then analyzed.

Acquisition evidence analysis is performed to collect appropriate digital evidence.

Use OSINT to investigate the information gathered from the acquisition.

The next stage is the profiling of suspects from previous events using OSINT information.

DOI: https://doi.org/10.59890/ijels.v2i12.2737
https://journal.multitechpublisher.com/index.php/ijels

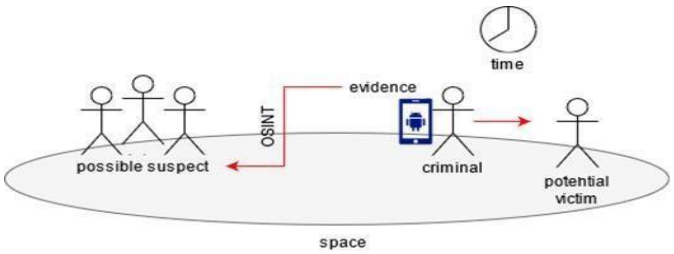

Fig. 1 case illustration

The computer forensic framework as shown in Figure 2

The computer forensic flow is expected to adjust the digital forensic investigation process to detect more deeply related anti-forensic applications and use OSINT to further enhance the investigation process to determine the profile of a person or organization. A series of tools to aid digital forensic procedures are also included. Following the steps taken in this research

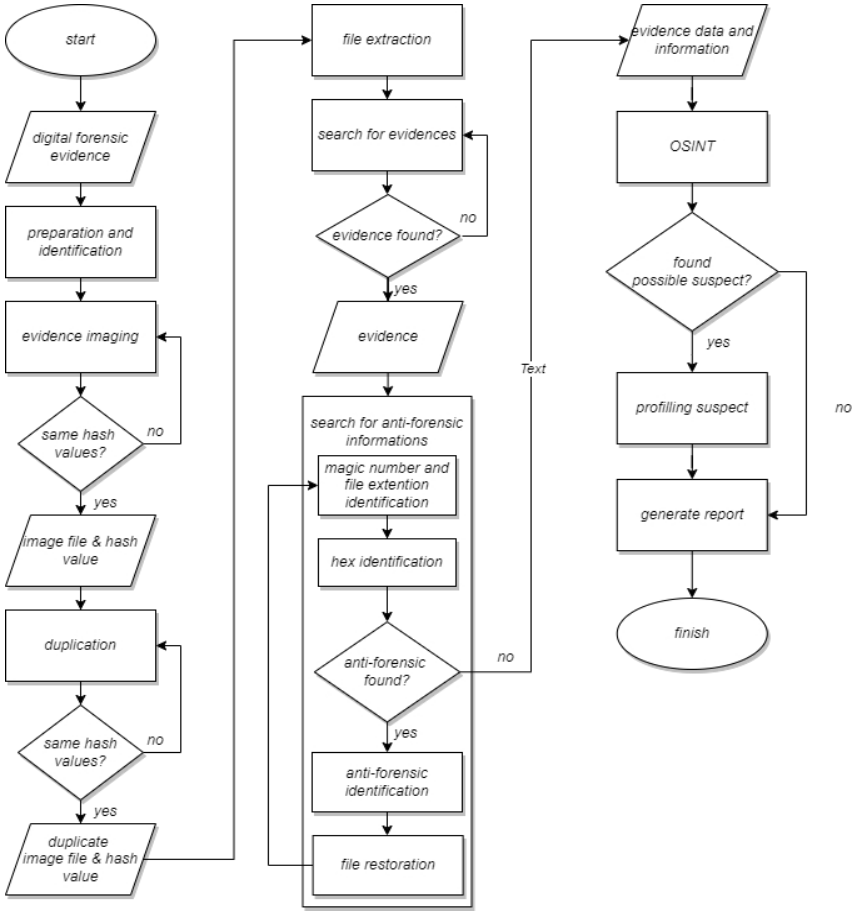

Fig. 2 Computer forensics framewor

CONCLUSION

Based on the results of research and discussion related to the analysis and investigation of anti-forensics on mobile forensics with open-source intelligence as a crime suspect profile, the following conclusions can be drawn. The investigation process on mobile forensics in identifying anti-forensics consists of the stages of preparation, preservation, acquisition, examination, analysis, reporting, presentation. The identification of anti-forensics and the use of OSINT is carried out at the analysis stage with several toolsets used. The use of OSINT the analysis stage can expand the information from the data obtained in the previous processin the form of some new username information.

Reference

Agri Chairunisa Isradjuningtias, Agri Chairunisa Isradjuningtias, and Leonardo Bagas Pradana. 2023. "Utilization of Digital Forensics in Preventive Efforts to Suppress the Spread of Hoaxes." *Postulate* 1 (2): 51–55. https://doi.org/10.37010/postulat.v1i2.1212.

Arshad, Humaira, Saima Abdullah, Moatsum Alawida, Abdulatif Alabdulatif, Oludare Isaac Abiodun, and Omer Riaz. 2022. "A Multi-Layer Semantic Approach for Digital Forensics Automation for Online Social Networks." *Sensors* 22 (3): 1–24. https://doi.org/10.3390/s22031115.

Goni, Osman. 2021. "Cyber Crime and Its Classification." *International Journalof Electronics Engineering and Applications* 10 (2): 01–17. https://doi.org/10.30696/ijeea.x.i.2022.01-17.

Jubaidi, Muhamad, and Nurul Fadilla. 2020. "The Influence of the Cyberbullying Phenomenon as Cyber-Crime on Instagram and its Negative Impact." *Shaut Al-Maktabah: Journal of Libraries, Archives and*

Documentation **12 (2): 117–34. https://doi.org/10.37108/shaut.v12i2.327.**

Lavinia, Nia. 2023. "The Urgency of Utilizing Open Source Intelligent (Osint)in Efforts to Prevent Acts of Terrorism in Indonesia." *Journal of Applied Social Humanities* 6 (1). https://doi.org/10.7454/jsht.v6i1.1105.

DOI: https://doi.org/10.59890/ijels.v2i12.2737
https://journal.multitechpublisher.com/index.php/ijels

Montasari, Reza. 2016. "A Comprehensive Digital Forensic Investigation Process Model." *International Journal of Electronic Security and Digital Forensics* 8 (January): 285. https://doi.org/10.1504/IJESDF.2016.079430.

Pai U., Yogish, and Krishna Prasad K. 2021. "Open Source Intelligence and Its Applications in Next Generation Cyber Security - A Literature Review." *International Journal of Applied Engineering and Management Letters*, no.

August 2021: 1-25. https://doi.org/10.47992/ijaeml.2581.7000.0100.

Pastor-Galindo, Javier, Pantaleone Nespoli, Felix Gomez Marmol, and Gregorio Martinez Perez. 2020. "The Not yet Exploited Goldmine of OSINT: Opportunities, Open Challenges and Future Trends." *IEEE Access*8: 10282-304. https://doi.org/10.1109/ACCESS.2020.2965257.

Prayudi, Yudi, and Azhari SN. 2015. "Digital Chain of Custody: State of theArt." *International Journal of Computer Applications* 114 (5): 1–9. https://doi.org/10.5120/19971-1856.

Rahayu Selamat, Siti, Shahrin Sahib, Nor Hafeizah, Robiah Yusof, and MohdFaizal Abdollah. 2013. "A Forensic Traceability Index in Digital Forensic Investigation." ***Journal of Information Security*** **04 (01): 19–32. https://doi.org/10.4236/jis.2013.41004.**

Tajuddin, Taniza, Azizah Abd Manaf, Nor Fatimah Awang, Siti Rafidah Muhamat Dawam, Noor Rasidah Ali, and Rafidah Amat. 2019. "CrimeSuspect Profiling (CSP) for Forensic Investigation on Smartphone." In *2019 4th International Conference and Workshops on Recent Advances and*

Innovations in Engineering (ICRAIE), 1-6.

https://doi.org/10.1109/ICRAIE47735.2019.9037772.

Virmani, Charu, Tanu Choudhary, Anuradha Pillai, and Manisha Rani. 2022. "Applications of Machine Learning in Cyber Security." *Research Anthology on Machine Learning Techniques, Methods, and Applications*, 621-41.https://doi.org/10.4018/978-1-6684-6291-1.ch033.

DOI: https://doi.org/10.59890/ijels.v2i12.2737
https://journal.multitechpublisher.com/index.php/ijels