Ratio Legis Journal
ISSN 2830-4624
published by
Master of Law, Faculty of Law
Universitas Islam Sultan Agung
Volume 4 No. 4, December 2025

Application of Digital Forensics as an Investigation System Cybercrime

Muhammad Ibnu Sina
Faculty of Law, Universitas Islam Sultan Agung (UNISSULA) Semarang, Indonesia,
E-mail: Mibnusina42@gmail.com

Abstract. *The purpose of this research is toknowing and analyzinglegal procedures for digital forensic efforts in the investigation stage of cybercrimeIn this paper, the author uses a normative juridical method with descriptive analysis as the research specification. The function of digital evidence in some cybercrime cases is indeed very complex. The use of digital evidence also often raises debate. The digital forensic testing that must be present to support this digital evidence also still lacks legal certainty. Proving using electronic evidence in special criminal cases that are specifically regulated by law as one of the valid evidence does indeed guarantee legal certainty compared to the use of electronic evidence. However, the question remains about the legality of the results of digital forensic testing presented in court as evidence. Another debate that often arises relates to the process of testing electronic evidence, the process of maintaining electronic evidence, and the often debated ability of a digital forensic expert to conduct electronic evidence testing because a series of these processes have not been regulated in more detail.*

Keywords: *Evidence; Digital; Forensic; Question.*

1. Introduction

Human-created laws aim to create orderly, safe, and secure conditions. Likewise, criminal law is one such law.[1]Law exists because individuals desire legal protection and have the right to a comfortable and peaceful living environment. A characteristic of a state governed by the rule of law is the existence of protection against criminal acts.

In criminal law, a crime is defined as an offense or criminal act, and the perpetrator is subject to criminal penalties. Criminal cases are resolved through several stages, including investigation, prosecution, trial, and verdict. Within the criminal justice

[1] Supriyono. (2020), Criminology Study of the Crime of Fencing the Stolen Goods. Jurnal Daulat Hukum, 3 (1) March. p. 185

system, the first step in upholding law and justice (access to justice) is through investigation and inquiry.[2]

In criminal investigations, investigators gather evidence to substantiate the allegation that a person suspected of committing a crime actually committed a crime. Indonesian criminal law recognizes evidence and instrumental evidence. According to Andi Hamzah, evidence is a material object that encompasses a criminal case, but evidence is not limited to bullets, knives, firearms, jewelry, televisions, and so on.[3]

In addition to developments in evidence, criminal case handling, particularly during the investigation process, must also evolve and develop in line with developments in modern science and technology. This can be seen, among other things, in how competent investigators utilize other supporting knowledge to expedite the resolution of criminal cases. This is particularly true in cases involving information technology, where various forms of electronic evidence are involved in cybercrime.[4]

Cybercrime requires a significant amount of electronic evidence to explain a criminal case. According to Christopher, a digital forensics expert, in handling crimes involving information technology, original evidence cannot be analyzed in the digital and electronic world because its authenticity must be maintained.[5]However, among the characteristics of electronic evidence, one of them is that it can be easily duplicated and is identical to the original, so it is necessary to investigate further whether the data is the result of duplication or the original data.[6]

Digital traces are the focus of investigative efforts in digital forensics, strengthening or weakening physical evidence in a case. The term was originally associated with computer forensics, but now encompasses the analysis of all digital data storage devices. The practice of digital forensics has evolved with the popularity of personal computing and the internet era.[7]

Based on the description of the background of the selection of legal material as described above, the researcher is interested in conducting research withThe aim

[2]Mutia Hafina Putri, et al. (2023), Investigation Process in the Criminal Justice System, Rewang Rencang: Jurnal Hukum Lex Generalis. 4 (7). p. 8
[3]Andi Hamzah, (2008). Indonesian Criminal Procedure Law, Sinar Grafika, Jakarta, p.120
[4]Synthiana Rachmie, (2020), The Role of Digital Forensic Science in Website Hacking Case Investigations, Jurnal Litigasi, 21 (1) April. p. 106
[5]Ibid, p. 120
[6]Ibid, p. 107
[7]N. Aisyah, et al. (2022), Analysis of the Development of Digital Forensics in Cybercrime Investigations in Indonesia Using a Systematic Review. Jurnal Esensi Infokom, 6 (1). p 22.

of this research is to determine and analyze the legal procedures for digital forensic efforts in the investigation stage of cybercrime..

2. Research Methods

To conduct the study in this research, the author used a normative legal method or written legal approach (statutory/statutory approach). The normative legal approach is an approach carried out based on primary legal materials by examining theories, concepts, legal principles and regulations related to this research. This approach is also known as a library approach, namely by studying books, laws and other documents related to this research.

3. Results and Discussion

1) Overview of Cybercrime

Cybercrime or computer-based crime, is a crime that involves computers and networks. [8]The computer may have been used in the commission of the crime, or it may have been the target.[9] Cybercrimes can be defined as: "Offenses committed against an individual or group of individuals with a criminal motive to intentionally harm the victim's reputation or cause physical or mental harm or loss to the victim either directly or indirectly, using modern telecommunications networks such as the Internet (networks including but not limited to Chat rooms, email, notice boards and groups) and mobile phones.[10] Cybercrime can threaten a person, national security or financial health.[11]

Issues surrounding this type of crime have become very popular, especially around hacking, copyright infringement, unwarranted wiretapping, and pornography. There are also privacy concerns when confidential information is intercepted or disclosed, whether lawfully or not. Debarati Halder and K. Jaishankar further define cybercrime from a gender perspective and define “cybercrime against women” as “Crimes targeted at women with the motive to intentionally harm the victim psychologically and physically, using modern telecommunications networks such as the internet and mobile phones.” Both governments and private individuals are intentionally involved in cybercrimes, including espionage, financial theft, and other cross-border crimes. Activities that cross national borders and

[8]R. Moore, (2005). Cyber Crime: Investigating High-Technology Computer Crime, Cleveland, Mississippi: Anderson Publishing.
[9]Warren G. Kruse, Jay G. Heiser. (2002), Computer Forensics: Incident Response Essentials. Addison-Wesley. p 392
[10]Debarati Halder & K. Jaishankar, (2011). Cybercrime and the Victimization of Women: Laws, Rights, and Regulations. Hershey, Pennsylvania USA: IGI
[11]Steve Morgan, (2016). Cyber Crime Costs Projected To Reach $2 Trillion by 2019. Forbes. Retrieved September 22

involve the interests of at least one country are sometimes referred to as cyberwarfare.

2) Digital Forensics

Digital forensics is the use of science and methods to find, collect, secure, analyze, interpret and present digital evidence related to cases that occur for the purposes of reconstructing events and the validity of the judicial process.[12]Digital forensics is the process of identifying, preserving, analyzing, and presenting digital evidence in a manner that is legally admissible in any legal proceeding (i.e., a court of law).

Digital forensics is a tool to assist investigators in their authority to conduct investigations and inquiries as regulated in the ITE Law and the Criminal Procedure Code (KUHAP). To be able to apply digital forensics in the investigation process, a deeper understanding of technological science is needed in addition to the legal science that is usually applied in criminal court proceedings. The application of digital forensics is divided into 4 (four), namely: (1) Computer Forensics, namely investigations carried out related to data and/or applications located on the computer which are recorded in various log files; (2) Network/Internet Forensics, namely investigations carried out on data obtained based on observations on the network; (3) Application Forensics, namely investigations carried out using certain applications. These applications have an audit function because the application has a feature to leave traces of a device; (4) Device Forensics, namely investigations with the aim of obtaining and collecting data and traces of certain activities in a digital device.[13]

3) Legal Procedures for Digital Forensic Efforts in the Investigation Stage of Cybercrime Acts

In the face of cybercrime, one of the main challenges is the process of establishing evidence for criminal acts. In the context of criminal law, evidence is a crucial aspect of the judicial process because it influences the verdict against the accused. Evidence encompasses legally valid procedures for proving the truth of allegations, as well as evidence recognized and accepted by law. This process is crucial because if the evidence fails, the accused can be acquitted. Conversely, if the evidence is sufficient, the accused can be found guilty and sentenced.[14]

The evidentiary process typically begins upon the appearance of an indication of a criminal incident. An investigation is conducted to determine whether an incident can be categorized as a crime. Further investigation is conducted to gather

[12]Ankit Agarwal, et.all., (2011), Systematic Digital Forensic Investigation Model, International Journal of Computer Science and Security (IJCSS), 5 (1). p 118-131
[13]Budi Raharjo. (2013), A Glance at Digital Forensics, Journal of Sociotechnology, 12 (29). p. 384
[14]Ira Irmansyah, (2024). The Power of Digital Forensics in Revealing Cyber Crime (Case Study: Hackers Illegally Access Payments for the Indonesian Commuter Train (KCI), Jispendiora: Journal of Social Sciences, Education and Humanities, 3 (3) December. p 122

relevant evidence, in accordance with the provisions of Article 1, number 13 of Law Number 2 of 2002 concerning the Police. In cybercrime cases, digital evidence such as data logs, metadata, and electronic documents is vital. Article 5 of the Electronic Information and Transactions Law (UU ITE) expressly states that electronic information and its printouts can be used as valid evidence in court.

The ITE Law, as a special legal regulation, contains new legal principles that differ from the legal systems in the Criminal Code and the Criminal Procedure Code. One of these is the recognition of electronic evidence as valid evidence in Indonesian evidentiary law. Since the ITE Law was enacted, there has been an increase in the types of evidence in court, namely electronic information and/or electronic documents. In the general provisions of the ITE Law, it is known that types of electronic data such as writing, photos, sounds, and images are considered electronic information, while types of electronic information such as writing, photos, sounds, and images stored on a flash drive that can be accessed via a computer device are considered electronic documents.

Article 1 number 4 of the ITE Law, electronic documents refer to data or information created, forwarded, sent, received, or stored in analog, digital, electromagnetic, optical, or other forms that can be seen, displayed, and/or heard through a computer or electronic system. Electronic documents include writing, sound, images, maps, designs, photographs, or other forms, and include letters, signs, numbers, access codes, symbols, or perforations that have meaning or significance and can be understood by people who are able to understand them. Meanwhile, the definition of electronic information based on Article 1 number 1 of the ITE Law is one or a collection of electronic data, including writing, sound, images, maps, designs, photographs, electronic data interchange (EDI), electronic mail, telegrams, telecopies, or other forms, and include letters, signs, numbers, access codes, symbols, or perforations that have been processed and have meaning or can be understood by people who are able to understand them. In the context of the ITE Law, it is stipulated that electronic information or electronic documents, along with their printouts, constitute valid evidence and constitute an extension of valid evidence in accordance with applicable procedural law in Indonesia. Electronic evidence created in the form of electronic information and electronic documents is considered valid under the ITE Law. This is in line with Article 184 of the Criminal Procedure Code (KUHAP), which states that valid evidence consists of witness testimony, expert testimony, letters, instructions, and statements from the accused.[15]

As a cyber crime, the examination of evidence found by the police must be carried out in accordance with the stages that should be carried out, namely by using

[15]M Qahar Awaka and Alhadiansyah, (2023), Utilization of Digital Forensics in Proving the Crime of Disseminating Indecent Videos Through Facebook Social Media in the Legal Area of West Kalimantan Police, Sehasen Law Journal. 9 (2) October. p 463

digital forensic techniques which are all stages of retrieval, recovery, storage, examination of electronic information and documents using responsible methods and tools to obtain evidence that can be presented in court.

Digital forensic science has 4 (four) basic principles, namely (1) Digital data as evidence must not be changed, because its authenticity will affect the strength of legal evidence in court; (2) The competence of experts in analyzing digital data because it will impact the actions taken against the digital data evidence; (3) There are technical and practical standard operating procedures (SOPs) regarding the steps taken on storage media during the digital data examination process as a basis for treatment if carried out later by different people but the results will be the same and security is guaranteed; (4) The responsibility of each person involved in the investigation, examination and analysis process is carried out in accordance with applicable provisions.[16]

According to Kemmish, the stages that will be carried out in a digital forensic examination to examine evidence obtained from a cyber crime are:

1) Evidence Identification

Identification of evidence is the main stage of digital forensics, and the identification carried out at this stage generally involves identifying where the evidence is located, where the evidence is stored, and how the evidence should be stored, so that the data stored in the evidence has the same characteristics.[17]The storage process must be carried out using secure devices and methods to prevent damage or alteration to the evidence, which could affect its validity in court. Storing digital evidence also involves creating backup copies of the original data, so that if the digital evidence is lost or damaged, a copy can still be used for further investigation. Furthermore, in the process of storing digital evidence, investigators must strictly maintain its confidentiality and integrity, so that the evidence cannot be accessed or manipulated by unauthorized parties. All steps in the process of identifying and storing digital evidence must be carried out carefully and in accordance with applicable digital forensic standards. This aims to ensure that the evidence found can be recognized as valid evidence and can be used in court to prosecute perpetrators involved in cybercrime.[18]

2) Digital evidence analysis

At this stage, the evidence obtained is re-explored in an investigation-related scenario, including examining metadata. Typically, files contain metadata that

[16]Ruuhwan, Imam Riadi, and Yudi Prayudi. (2016), Feasibility Analysis of an Integrated Digital Forensics Investigation Framework for Smartphone Investigations. Jurnal Buana Informatika, 7 (4). p. 265
[17]Farol Medeline, Elis Rusmiati & Rully Herdita Ramadhani, (2022). Digital Forensics in Proving Hate Speech Crimes on Social Media, PAMPAS: Journal of Criminal Law, 3 (3). p 318
[18]M Qahar Awaka and Alhadiansyah, (2023). Op.Cit, 9 (2) October. p 464

includes information about the file, such as the number of times the file was edited, the number of editing sessions, the computer name, the number of times it was saved, where the file was printed, and the date and time it was modified. "Then, at this stage, the recovery process also involves recovering deleted files and folders, recovering passwords, recreating partitions, unformatting drives, rebuilding visited web pages, and recovering deleted emails.[19]

3) Presentation

The presentation stage is where the existing evidence is validated and its relationship to the case at hand. At this stage, the test results will be presented on evidence relevant to the case being examined.[20]

The results of the investigation, in the form of a digital forensic examination, as described above, will ultimately assist the judge in making a decision by evaluating and assessing the suitability of the evidence presented and examining its relationship to each element of the article charged. This relates to Article 183 of the Criminal Procedure Code, which states that a judge's conviction is based on valid evidence. The results of digital forensics also align with the purpose of evidence itself, namely to seek and obtain material truth, not simply to find fault.[21]

The results of digital forensic examinations in the form of letters include forensic laboratory reports, expert reports, and digital forensic test reports. According to Article 187 b of the Criminal Procedure Code, the results of digital forensic examinations in the form of forensic laboratory reports and forensic expert reports must be prepared in accordance with the provisions of laws and regulations. This indicates that the results of digital forensic testing produce a letter from an official regarding a matter within the government that is his responsibility and is intended to prove a matter or condition.[22]

Digital forensic evidence in court proceedings not only produces documentary evidence but also expert testimony. Digital forensic experts must understand and adhere to computer science and legal procedures recognized nationally and internationally. They must also be well-versed in the theory related to the digital evidence recovered and familiar with the use of forensic software or applications to ensure proper and accurate examination of digital evidence.

Based on Article 43 (5) letter j of the ITE Law, in cybercrime investigations in the realm of expert involvement, which is legally stipulated to request expert

[19]Farol Medeline, Elis Rusmiati & Rully Herdita Ramadhani, (2022). Op.Cit, 3 (3). p 319
[20]Ibid
[21]Ibid, p. 322
[22]Christloy Totota Karo-Karo & Handar Subhandi Bakhtiar, (2024). Analysis of Social Media Hacking Cases Through Digital Forensics as a Preventive Effort by Investigators to Prevent Wrongful Arrests (Case Study of the Ravio Patra Hacking), TERANG: Journal of Social, Political and Legal Studies, 1 (4). p. 182

assistance as needed in investigations of criminal acts in the field of Information Technology and Electronic Transactions. This means that a digital forensic expert is someone with certain expertise in the field of information technology who is academically and practically responsible for that knowledge.[23]

The role and function of digital forensics in this case can be seen from the investigation phase. During the investigation phase, the Police use digital forensics to find and collect existing evidence. The role and function of digital forensics in cybercrime cases can also be seen from the available evidence. During the investigation phase, the Police must still adhere to the principle of unus testis nullus testis or one witness is not a witness, which means there must be at least two pieces of evidence. This principle of unus testis nullus testis can explain that if there is an investigation and then only has one witness, it is declared null and void by law. This is also stated in Article 184 of the Criminal Procedure Code, which explains that proof must be at least two pieces of evidence.[24]This evidence is mentioned in the article to prove the elements that a cyber crime has occurred.

Thus, it can be seen how the role of digital forensics as a tool for the police is quite important, serving as a scientific basis for determining suspects. Digital forensic examination of evidence related to cybercrime will guide investigators from the initial investigation stage to identifying the cybercrime suspect. Digital forensics will play a role in identifying the perpetrator and reconstructing their behavior. Digital forensics in the forensic process will be more responsible because it is a form of applying scientific techniques and analyzing existing evidence.

4. Conclusion

According to Article 187 b of the Criminal Procedure Code, the results of digital forensic examinations in the form of forensic laboratory BAP and forensic expert BAP must be made in accordance with the provisions of laws and regulations. This shows that the results of digital forensic tests produce a letter from an official regarding a matter within the government that is his responsibility and is intended to prove a matter or condition. Based on Article 43 (5) letter j of the ITE Law, in cybercrime investigations in the realm of expert involvement which is legally stipulated to request expert assistance needed in investigations of criminal acts in the field of Information Technology and Electronic Transactions. This means that a digital forensic expert means someone with certain expertise in the field of information technology who is academically and practically responsible for that knowledge.

[23]Article 43 (5) letter j of Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions
[24]Maulana Daffa Ilhami and Wiwik Afifah, (2023). Carving Out the Nature of Unus Testis in Proving Sexual Crimes, Bureaucracy Journal: Indonesia Journal of Law and Social-Political Governance, 3 (2) May-August. p 1634

5. References

Journals:

Ankit Agarwal, et.all., (2011), Systematic Digital Forensic Investigation Model, *International Journal of Computer Science and Security (IJCSS)*, 5 (1)

Budi Raharjo. (2013), Sekilas Mengenai Forensik Digital, *Jurnal Sosioteknologi*, 12 (29)

Christloy Totota Karo-Karo & Handar Subhandi Bakhtiar, (2024). Analisis Kasus Peretasan Media Sosial melalui Digital Forensik sebagai Upaya Preventif Penyidik Mencegah Kejadian Salah Tangkap (Studi Kasus Peretasan Ravio Patra), *TERANG: Jurnal Kajian Ilmu Sosial, Politik dan Hukum*, 1 (4).

Farol Medeline, Elis Rusmiati & Rully Herdita Ramadhani, (2022). Forensik Digital dalam Pembuktian Tindak Pidana Ujaran Kebencian di Media Sosial, *PAMPAS: Journal of Criminal Law*, 3 (3)

Ira Irmansyah, (2024). Kekuatan Digital Forensik dalam Mengungkap Tindak Pidana Cyber Crime (Studi Kasus: Hacker Ilegal Akses Pembayaran Kereta Commuter Indonesia (KCI), *Jispendiora: Jurnal Ilmu Sosial, Pendidikan dan Humaniora*, 3 (3) Desember

Maulana Daffa Ilhami dan Wiwik Afifah, (2023). Mengukir Sifat Unus Testis Terhadap Pembuktian Tindak Pidana Seksual, *Bureaucracy Journal: Indonesia Journal of Law and Social-Political Governance*, 3 (2) Mei-Agustus

M Qahar Awaka dan Alhadiansyah, (2023), Utilization of Digital Forensics in Proving the Crime of Disseminating Indecent Videos Through Facebook SocialMedia in the Legal Area of West Kalimantan Police, *Jurnal Hukum Sehasen*. 9 (2) Oktober

Mutia Hafina Putri, dkk. (2023), Proses Penyidikan dalam Sistem Peradilan Pidana Investigation Process in the Criminal Justice System, *Rewang Rencang: Jurnal Hukum Lex Generalis*

N. Aisyah, dkk. (2022), Analisa Perkembangan Digital Forensik Dalam Penyidikan Cybercrime di Indonesia Secara Systematic Review. *Jurnal Esensi Infokom*, 6 (1)

Ruuhwan, Imam Riadi, and Yudi Prayudi. (2016), Analisis Kelayakan Integrated Digital Forensics Investigation Framework untuk Investigasi Smartphone. *Jurnal Buana Informatika*, 7 (4)

Steve Morgan, (2016). Cyber Crime Costs Projected To Reach $2 Trillion by 2019. *Forbes*. Retrieved September 22

Synthiana Rachmie, (2020), Peranan Ilmu Digital Forensik Terhadap Penyidikan Kasus Peretasan Website, Jurnal Litigasi, 21 (1) April

Supriyono. (2020), Criminology Study of Crime of Fencing the Stolen Goods. *Jurnal Daulat Hukum*, 3 (1) March

Books:

Andi Hamzah, (2008). *Hukum Acara Pidana Indonesia*, Sinar Grafika, Jakarta

Debarati Halder & K. Jaishankar, (2011). *Cybercrime and the Victimization of Women: Laws, Rights, and Regulations*. Hershey, Pennsylvania USA: IGI

R. Moore, (2005). *Cyber Crime: Investigating High-Technology Computer Crime*, Cleveland, Mississippi: Anderson Publishing

Warren G. Kruse, Jay G. Heiser. (2002), *Computer Forensics: Incident Response Essentials*. Addison-Wesley