Proceeding of the 4th Malikussaleh International Conference on Law, Legal Studies and Social Sciences (MICoLLS) 2024

THE ROLE OF FORENSIC TECHNOLOGY IN CYBER CRIME INVESTIGATION AND PROSECUTION

Nadia Khairunnisa Iswani
Faculty of Law, Universitas Malikussaleh
nadia.200510261@mhs.unimal.ac.id

Muhammad Nur
Faculty of Law, Universitas Malikussaleh
mnur@unimal.ac.id

Husni
Faculty of Law, Universitas Malikussaleh
husni@unimal.ac.id

ABSTRACT
In the era of globalization, technological advances offer various conveniences but also bring challenges in the form of increasingly complex digital crimes. Cybercrimes such as online fraud, which occurred for example in Banyuwangi in June 2020, show how technology can be used for crimes with a low risk of detection. Digital forensics plays an important role in the investigation and investigation of cyber crimes, identifying perpetrators, and revealing important evidence from the electronic devices used. This study uses a quantitative approach with a normative legal framework, analyzing the role of digital forensics in uncovering cyber crimes based on Law No. 19 of 2016 concerning Amendments to Law No. 11 of 2008 concerning Information and Electronic Transactions (ITE) and the Criminal Procedure Code. The results of the study show that digital forensics is effective in tracking digital evidence, such as application conversations and online transaction traces, which support investigations and inquiries. The use of electronic evidence as regulated in Article 5 paragraph (1) of the ITE Law is very important in ensuring valid evidence in court. This study suggests the need for continuous innovation in digital forensic techniques and supporting regulations so that law enforcement can keep up with technological developments and prevent misuse of technology in cyberspace.

Keywords: Forensic Investigation Technology, Investigation, Criminal Acts, Cyber Crime

1. PROBLEM BACKGROUND

The Great Dictionary of the Indonesian Language (KBBI) defines technology as a systematic scientific approach designed to meet practical goals. Technology includes applied science and includes all the tools and methods needed to ensure the continuity and improvement of human life. Meanwhile, the term "technology" comes from the Greek word "technologia," where "techno" means "skill" and "logia" means "knowledge." In essence, technology is the embodiment of the application of scientific knowledge for practical purposes, which essentially changes and improves the human experience and our interactions with the environment.[1]

In today's era of globalization, technology presents a double-edged sword, offering both extraordinary advantages and significant challenges for its users. On the one hand, the various benefits and conveniences obtained from technological advances cannot be denied. On the other hand, we cannot ignore the dark side of the internet, which has transformed traditional crimes such as threats, theft, and fraud into digital crimes that can be committed with minimal risk of detection.[2] This shift not only increases the potential dangers to individuals and society, but also gives rise to new forms of criminal activity that pose a major threat to society and the state.

Digital forensics has proven to be very useful in various cases, most notably the Banyuwangi Online Fraud case in June 2020. A sophisticated syndicate exploited hacked mobile phone numbers, using the WhatsApp application to pose as individuals seeking to borrow money from unsuspecting victims. Once the funds were obtained, the perpetrators attempted to evade arrest. The case involved not only disguises but also various fraudulent tactics. However, diligent efforts by the Banyuwangi Police resulted in a significant breakthrough after reports of hacked mobile phone and WhatsApp accounts. Using advanced digital tracking techniques through forensic computing, the police were able to trace the hacked numbers and applications to several locations. This thorough investigation resulted in the recovery of dozens of ATM cards, hundreds of fraudulent accounts, several mobile phones used in the crime, and an impressive amount of money amounting to billions.

[1] Hansen, Mark. *Embodying technesis: Technology beyond writing*. University of Michigan Press, 2000.

[2] Johnson, Mark. *Cyber crime, security and digital intelligence*. Routledge, 2016.

While three perpetrators have been arrested, fourteen are still at large, underscoring the need for continued vigilance and innovation in digital forensics.

Through the application of computer forensics, law enforcement was able to identify the perpetrators and determine their locations.[3] In addition, they were able to trace several accounts associated with the syndicate, further demonstrating the efficacy of this sophisticated investigative technique.

The latest case comes from Surabaya, where someone's hobby of testing website security for unexpected rewards led to a shocking discovery: a website linked to the FBI. The suspects, all sixth-semester students at Stikom Surabaya, are Katon Primadi Sasmitha who is also a member of my community Nizar Ananta, also from Surabaya, and Triwardhana from Bayuwangi. These young scholars are believed to have hacked into more than 600 websites in 44 countries using SQL Intelligence Techniques.

In particular, Katon Primadi, whom I know personally, is known as the champion of the Cyber Jawara hacking competition organized by the Indonesian National Armed Forces. His passion for identifying vulnerabilities in websites is well-known, and he often shares his insights and tutorials on Facebook. The campus is currently conducting its own investigation into the circumstances surrounding the arrest and has not received any information from the FBI or local law enforcement. Officials noted that the suspect is an intelligent individual, as evidenced by his impressive GPA of 3.00. Computer network lecturer Anjik Sukma Aji said that the hacking incident started from curiosity, because the vastness and complexity of the web can be interesting and time-consuming to explore. He further explained that the hacker's intention was most likely rooted in the desire to explore, test their skills, or simply satisfy their curiosity. Article 27 paragraph (4) of Law No. 19 of 2016 concerning Amendments to Law No. 11 of 2008 concerning Electronic Information Technology (UU ITE) states that anyone who intentionally and unlawfully distributes or transmits financial resources or makes accessible information or electronic documents containing elements of blackmail or threats, shall be subject to criminal penalties. The impact of technology on society and the

[3] Marcella Jr, Albert, and Doug Menendez. *Cyber forensics: a field manual for collecting, examining, and preserving evidence of computer crimes*. Auerbach Publications, 2010.

environment is enormous and broad, shaping our ever-evolving world order. Its potential to improve various aspects of our lives is undeniable, especially in driving economic growth and development.

Article 5 paragraph 1 of the ITE Law states that Electronic Information, Electronic Documents, and their printouts have the status of valid evidence. In addition, paragraph 2 emphasizes that electronic information is an extension of valid evidence as referred to in the Procedural Law applicable in Indonesia. We sincerely hope that the ITE Law can become a solid legal basis for judicial institutions, which serves as a guideline in enforcing order in the use of information technology. The development of legislation in the realm of cyberspace is essentially based on the aspirations of the community for a sense of security, justice, and legal certainty.[4] As a basic norm of cyberspace law, cyberspace law requires everyone to obey and enforce the provisions stipulated therein. In addition, this technological advancement significantly increases the ability of law enforcement to uncover evidence of criminal acts that have occurred. Digital forensics is a very important branch of forensic science, which is dedicated to the careful investigation and analysis of digital data and the contents of electronic devices. This discipline plays a vital role in empowering investigative authorities, supporting their mandate to conduct thorough investigations in accordance with the provisions set out in Law Number 19 of 2016, which amended Law Number 11 of 2008 concerning Electronic Information Technology, together with the Criminal Procedure Code.

Through the lens of digital forensics, the search for truth and justice is enhanced, ensuring that the complexities of the digital realm are navigated with precision and integrity. Achieving mastery in digital forensics goes beyond mere technical proficiency; forensics intricately intersects multiple disciplines, most notably the legal field. The technical dimensions of an investigation can be delineated into several specialized subdisciplines, each tailored to the specific type of digital device in question.[5] Beyond identifying direct evidence relevant to a crime,

[4] Hunter, Dan. "Cyberspace as Place and the Tragedy of the Digital Anticommons." In *Law and Society Approaches to Cyberspace*, pp. 59-139. Routledge, 2017.

[5] Shinn, Terry. "New sources of radical innovation: research-technologies, transversality and distributed learning in a post-industrial order." *Social Science Information* 44, no. 4 (2005): 731-764.

digital forensics has broader goals: it can shed light on the relationship between a suspect and a case, support alibis or statements, and uncover ulterior motives.

2. RESEARCH METHODS

This study uses a quantitative approach with a normative legal framework to analyze the role of forensic technology in the investigation and prosecution of cyber crime. The data used comes from primary legal materials, such as the Criminal Procedure Code (KUHAP), Law No. 8 of 1981 concerning Criminal Procedure Law, and Law No. 19 of 2016 concerning Amendments to Law No. 11 of 2008 concerning Information and Electronic Transactions (ITE). Secondary data sources include relevant books, journals, and papers, while tertiary legal materials include legal dictionaries and the Great Dictionary of the Indonesian Language. The data collection method is carried out through library research, and data analysis uses literature review to ensure a comprehensive understanding of the topic being studied.

3. DISCUSSION

3.1. The Power of Electronic Evidence in Cyber Crime Investigation and Prosecution

In today's digital era, the use of information technology has changed many aspects of life, including in the legal field. Technology has made human life easier, but has also opened up opportunities for the emergence of new crimes, known as cyber crime.[6] This cyber crime is characterized by the implementation of criminal acts involving information technology and electronic devices as a means to carry out evil intentions. Along with the development of technology, law enforcement in cyberspace must also follow these changes. Therefore, the existence of electronic evidence is very important in the investigation and prosecution of cyber crime cases.

Electronic evidence, based on Article 5 paragraph (1) of Law No. 19 of 2016 concerning Amendments to Law No. 11 of 2008 concerning Information and Electronic Technology (UU ITE), is considered valid in legal trials. Electronic

[6] Wall, David S. *Cybercrime: The transformation of crime in the information age*. John Wiley & Sons, 2024.

information, electronic documents, and their printouts can be valid evidence in accordance with the procedural law in force in Indonesia.[7] This article provides a strong legal basis for law enforcement officers to use electronic evidence in uncovering crimes that occur in cyberspace. Digital forensics is also present as a very important branch of science to assist law enforcement officers in the process of investigating and analyzing evidence contained in electronic devices used by criminals.[8] The application of this science allows officers to obtain very valuable clues from digital data, such as conversations via messaging applications, activities on social media, and records of online transactions carried out by suspects.

The application of forensic technology in investigating cybercrime is increasingly important in facing the challenges and obstacles that exist in cyberspace. Cybercriminals tend to use methods that are very hidden and difficult to detect, such as hiding their real identities or deleting existing digital traces. Therefore, digital forensics has a major role in identifying evidence that may have been overlooked by investigators. Advanced digital forensic techniques, such as data tracking through servers, recovering deleted files, and analyzing IP address traces and metadata, allow officers to uncover who is behind the crime and what their modus operandi is.[9] For example, in the case of online fraud that occurred in Banyuwangi in June 2020, the use of digital forensics has proven to be very effective. With the help of technology, the police were able to track hacked cellphone numbers and reveal the identities of the perpetrators along with the illegal transactions they made.

Not only in larger cases, forensic technology also plays a big role in smaller cases involving personal electronic devices, such as mobile phones or computers. Evidence found on these devices can be the key to uncovering previously undetected criminal acts. For example, in the case of a website hack involving students in Surabaya, the use of SQL Intelligence techniques allowed investigators to track more than 600 compromised websites, even though the perpetrators tried to remain anonymous.

---

[7] Wardani, Kusuma, Dian Eka, and Slamet Sampurno Soewondo. "Electronic evidence in criminal procedural law." *JL Pol'y & Globalization* 104 (2020): 1.

[8] Casey, Eoghan. *Handbook of digital forensics and investigation*. Academic Press, 2009.

[9] Årnes, André, ed. *Digital forensics*. John Wiley & Sons, 2017.

The implementation of laws governing electronic evidence is very important to ensure that evidence obtained through this technology can be accepted in court. The ITE Law itself provides ample room for law enforcement officers to use electronic evidence in legal proceedings. Article 27 paragraph (4) of the ITE Law emphasizes that anyone who intentionally disseminates information containing elements of blackmail or threats can be punished. Therefore, electronic evidence such as recordings of conversations, photos, videos, or online transactions found on the perpetrator's electronic device can be used as valid evidence to prove the criminal acts committed.

However, although technology makes it easier for law enforcement, there are major challenges that must be faced by law enforcement officers. One of the main challenges is the technical skills required to access, analyze, and investigate evidence contained in electronic devices. In this case, officers who are trained in digital forensics are needed to ensure that the process of collecting and analyzing evidence is carried out correctly and in accordance with applicable procedures. In addition, issues related to the protection of privacy and human rights must also be considered in every investigation and inquiry process involving electronic evidence.

Thus, forensic technology plays a vital role in the investigation and prosecution of cyber crime cases in Indonesia. The application of digital forensics allows law enforcement to obtain more accurate and valid evidence that can be used in court.[10] In addition, existing laws and regulations, such as the ITE Law, provide a clear legal basis for making electronic evidence an integral part of the legal process in Indonesia. Therefore, success in uncovering cyber crime crimes is highly dependent on technological advances, the ability of investigators to use the technology, and the existence of regulations that support its use in the justice system.

3.2. Efforts Made in Optimizing Forensic Technology Evidence in Cyber Crime

In the increasingly developing digital era, technological advances have had a huge impact, both in everyday life and in the legal world. One area that has benefited

[10] Daniel, Larry, and Lars Daniel. *Digital forensics for legal professionals: understanding digital evidence from the warrant to the courtroom*. Elsevier, 2011.

significantly from technology is digital forensics. In cases of cyber crime, digital forensics plays a vital role in helping investigators uncover evidence in cyberspace, which was previously difficult to access. The use of forensic technology evidence, especially in cases of online fraud, account hacking, and website hacking, opens up opportunities for law enforcement to investigate cases in more detail and accurately.[11]

In Indonesia, Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE) provides a strong legal basis in terms of recognizing electronic evidence. Article 5 paragraph (1) of the ITE Law emphasizes that electronic information and electronic documents, as well as their printouts, have a legitimate position as evidence in court. This is of course very relevant in the investigation of cybercrimes involving electronic devices, such as computers, mobile phones, and internet networks, which are the main means of committing digital crimes.

In the investigation of crimes involving technology, digital forensics becomes a very valuable tool. Digital forensics is a science that specializes in the collection, analysis, and presentation of electronic evidence involved in a crime.[12] For example, in the case of online fraud that occurred in Banyuwangi, the police succeeded in utilizing digital tracking techniques to identify the perpetrators by examining the electronic traces left by the perpetrators. Through forensic analysis, the police were able to track the location of the devices used by the perpetrators and recover a number of pieces of evidence, such as ATM cards and mobile phones used in the crime. This proves that digital forensics does not only rely on technical skills in analyzing data, but also the ability to connect the evidence to the suspect.

Not only that, digital forensics also has a role in understanding the relationship between the suspect and the crime committed, as well as revealing the motive or purpose of the crime.[13] For example, in the hacking case involving students from Stikom Surabaya, investigations using digital forensic techniques

[11] Marcella Jr, Albert, and Doug Menendez. *Cyber forensics: a field manual for collecting, examining, and preserving evidence of computer crimes*. Auerbach Publications, 2010.

[12] Casey, Eoghan. *Digital evidence and computer crime: Forensic science, computers, and the internet*. Academic press, 2011.

[13] Kruse II, Warren G., and Jay G. Heiser. *Computer forensics: incident response essentials*. Pearson Education, 2001.

such as digital footprint analysis and the use of SQL injection to infiltrate websites have uncovered how the perpetrators exploited system weaknesses to carry out their crimes. Although the perpetrators tried to cover their tracks, forensic technology was able to uncover the information needed to clarify the violations committed.

Forensic technology can track evidence from devices used in cybercrime, whether in the form of information stored on hard drives, traces left on networks, or electronic communications made by the perpetrators.[14] In fact, this technique can recover data that has been deleted or hidden. The use of this technology is increasingly recognized as a legitimate method in the legal process, which not only examines the existing evidence but can also reveal alibis or strengthen charges against suspects.

However, although forensic technology has great potential in uncovering cybercrime, its application still faces major challenges. One of the main challenges is the need for special skills in operating the devices and tools used in forensic analysis. In addition, the very rapid development of technology often makes it difficult for law enforcement to keep up with the changes and innovations that occur. Therefore, to achieve success in optimizing forensic technology evidence, close cooperation is needed between the police, investigators, and digital forensic experts.

From a legal perspective, it is important to update existing laws and regulations to keep up with existing technological developments. Along with technological advances, there are more and more new forms of cybercrime that need to be regulated within the legal framework. Therefore, updates to the ITE Law and related regulations need to be made to ensure that the law remains relevant and effective in dealing with ever-evolving cybercrime.

4. CONCLUSION

Overall, forensic technology plays a major role in accelerating the process of investigating and prosecuting cyber crimes. The use of legal electronic evidence in Indonesian law, as regulated in the ITE Law, makes it easier for law enforcement to

[14] Marcella Jr, Albert, and Doug Menendez. *Cyber forensics: a field manual for collecting, examining, and preserving evidence of computer crimes*. Auerbach Publications, 2010.

uncover digital crimes in a more efficient and accurate manner. In facing the increasingly sophisticated development of cyberspace, forensic technology will continue to be a key component in ensuring fair and appropriate law enforcement in Indonesia. Therefore, it is important for law enforcement officers to continue to improve their capacity in utilizing this technology, so that they can provide a sense of security and justice for the community.

5. REFERENCES

Årnes, André, ed. *Digital Forensics*. John Wiley & Sons, 2017.

Casey, Eoghan. *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*. Academic Press, 2011.

Casey, Eoghan. *Handbook of Digital Forensics and Investigation*. Academic Press, 2009.

Daniel, Larry, and Lars Daniel. *Digital Forensics for Legal Professionals: Understanding Digital Evidence from the Warrant to the Courtroom*. Elsevier, 2011.

Hansen, Mark. *Embodying Technesis: Technology Beyond Writing*. University of Michigan Press, 2000.

Hunter, Dan. "Cyberspace as Place and the Tragedy of the Digital Anticommons." In *Law and Society Approaches to Cyberspace*, pp. 59-139. Routledge, 2017.

Johnson, Mark. *Cyber Crime, Security and Digital Intelligence*. Routledge, 2016.

Kruse II, Warren G., and Jay G. Heiser. *Computer Forensics: Incident Response Essentials*. Pearson Education, 2001.

Marcella Jr, Albert, and Doug Menendez. *Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes*. Auerbach Publications, 2010.

Shinn, Terry. "New Sources of Radical Innovation: Research-Technologies, Transversality and Distributed Learning in a Post-Industrial Order." *Social Science Information* 44, no. 4 (2005): 731-764.

Wall, David S. *Cybercrime: The Transformation of Crime in the Information Age*. John Wiley & Sons, 2024.

Wardani, Kusuma, Dian Eka, and Slamet Sampurno Soewondo. "Electronic Evidence in Criminal Procedural Law." *JL Pol'y & Globalization* 104 (2020): 1.