THE USE OF DIGITAL FORENSICS IN REVEALING INFORMATION AND ELECTRONIC TRANSACTION (ITE) CRIMES

Agung Ahmad Sulton Saputra 1[1], Heni Susanti 2[2]

[1] Fakultas Hukum, Universitas Islam Riau
email: agungsaputrasipss@gmail.com
[2] Fakultas Hukum, Universitas Islam Riau
email: heni@law.uir.ac.id

Abstract

Currently, the most common crimes in society are the manipulation and fabrication of digital evidence. The use of digital forensics to spread disinformation or hoaxes can be carried out by anyone. These crimes can occur due to several main factors related to the development of digital technology, regulations, the political situation, and understanding of the internet world. Information and Communication Technologycrimes can also occur due to a combination of technological developments, lack of digital literacy, economic motives, regulatory weaknesses, and the existence of security holes in digital systems. Therefore, preventing information and communication technology crimes requires a cooperative approach, including increasing digital literacy, strengthening regulations, improving information and communication technology security systems, and international cooperation in enforcing digital law.
From the results of the author's research, in handling cases of crime in the field of Information and Electronic Transactions, digital evidence has a legal standing as evidence even though it is not explicitly mentioned in the Criminal Procedure Code, with further regulations in the ITE Law that recognizes the validity of digital evidence such as electronic information, electronic documents, hardware and software. Success in digital forensic analysis requires strict procedures in the collection, analysis of deleted data, and metadata recovery, with the aim of maintaining the authenticity of the evidence. To optimize the use of digital forensic tools, such as UFED Cellebrite, in the Riau Regional Police, it is necessary to improve human resource competency through training and certification, optimize the use of devices by utilizing advanced features, and collaboration with other institutions.

Keywords: Digital Forensics, Information Crime and Electronic Transactions, UFED Cellebrite

Abstrak

Saat ini kejahatan yang paling umum di masyarakat adalah manipulasi dan pemalsuan bukti digital. Penggunaan digital forensik untuk menyebarkan disinformasi atau hoaks dapat dilakukan oleh siapa saja. Kejahatan ini dapat terjadi akibat beberapa faktor utama yang terkait dengan perkembangan teknologi digital, regulasi, situasi politik dan pemahaman tentang dunia internet. Kejahatan Teknologi digital, regulasi, situasi politik dan pemahaman tentang dunia internet. Kejahatan Teknologi Informasi dan Komunikasi juga dapat terjadi akibat kombinasi perkembangan teknologi, kurangnya literasi digital, motif ekonomi, kelemahan regulasi dan adanya celah keamanan dalam sistem digital. Oleh karena itu, pencegahan kejahatan memerlukan pendekatan kolaboratif, termasuk peningkatan literasi digital, penguatan regulasi, perbaikan sistem keamanan, dan kerjasama international dalam penegakan hukum digital.
Berdasarkan hasil penelitian penulis, dalam menangani kasus kejahatan di bidang Transaksi Elektronik, Bukti digital memiliki kedudukan hukum sebagai bukti meskipun tidak secara eksplisit disebutkan dalam Kitab Undang-Undang Hukum Acara Pidana, dengan peraturan lebih lanjut dalam Undang-Undang ITE yang mengakui keabsahan bukti digital seperti informasi elektronik, dokumen elektronik, perangkat keras dan perangkat lunak. Kesuksesan dalam analisis forensik digital memerlukan prosedur ketat dalam pengumpulan, analisis data yang dihapus, dan pemulihan metadata dengan tujuann menjaga keaslian bukti.
Untuk mengoptimalkan penggunaan alat forensik digital, seperti UFED Cellebrite di Kepolisian Daerah Riau, diperlukan peningkatan kompetensi sumber daya manusia melalui pelatihan dan

sertifikasi, optimalisasi penggunaan perangkat dengan memanfaatkan fitur canggih, serta kolaborasi dengan lembaga lain.
***Kata Kunci:** Digital Forensik, Tindak Pidana Informasi dan Transaksi Elektronik, UFED Cellebrite*

INTRODUCTION

Currently, crimes that frequently occur in society are manipulation and engineering of digital evidence, misuse of personal data and violation of privacy, illegal wiretapping, illegal destruction of evidence (Tampering or Destroying Evidence), abuse of authority in digital forensic investigations, digital data leaks from forensic processes, misuse of digital forensic technology for personal or group interests, the use of digital forensics in engineering legal cases, human rights violations (HAM) in digital forensic processes, the use of digital forensics to spread disinformation or hoaxes, these can be committed by anyone. These crimes can occur due to several main factors related to the development of digital technology, regulations, political situations and understanding of the internet world. Information and Electronic Transaction (ITE) crimes can also occur due to a combination of technological developments, lack of digital literacy, economic motives, regulatory weaknesses and the existence of security holes in digital systems. Therefore, preventing Information and Electronic Transaction crimes requires a cooperative approach, including increasing digital literacy, strengthening regulations, improving Information and Electronic Transaction security systems and international cooperation in enforcing digital world laws. Prof. Widodo explained that Electronic Information and Transactions (ITE) is any activity of a person, group of people, or legal entity that uses a computer as a means to commit a crime or uses computer media as a means to commit a crime.[1]

As part of modern society's culture, the internet has developed rapidly and is considered a cultural tool because it enables various Information and Electronic Transaction (ITE) activities, such as thinking, creating, and acting, to be carried out anywhere and at any time. With its presence, cyberspace has been formed.[2] Many people believe that advances in information technology, particularly the internet, offer numerous benefits, including security, convenience, and speed. One example is the use of the internet as a tool to help book and reserve airline tickets, train tickets, hotels, and pay telephone and electricity bills. This has made customers feel more comfortable and secure when conducting their activities.

Criminal policy, according to Barda Nawawi Arief, is a policy to determine an act that was originally not a criminal act (not a crime).[3] Therefore, the policy of criminalizing information technology crimes is part of the criminal policy using

[1] Widodo, *Aspek Hukum Kejahatan Mayantara* (Aswindo, 2011).

[2] Amiruddin & Asikin, *Pengantar Metode Penelitian Hukum* (PT. Raja Grafindo Persada, 2004).

[3] Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana* (2010).

criminal law means, and therefore is included in the criminal law policy, specifically the policy formulated through a comprehensive understanding of Information and Electronic Transaction (ITE) crimes, the role of the community is very important in monitoring efforts, especially when the community experiences a lack of information. Conversely, when people know that Information and Electronic Transactions (ITE) crimes are crimes that must be handled, they will anticipate them or report them to the local police. Currently, Indonesia has the Information and Electronic Transactions (ITE) Law to regulate cyberspace and establish sanctions for violations occurring within and outside Indonesian jurisdiction, which impacts Indonesian society.[4]

The interpretation of the Criminal Code (KUHP), especially laws related to the advancement of information technology, is used to implement the law on Information and Electronic Transactions (ITE) crimes such as:

1. Law Number 36 of 1999 concerning Telecommunications.
2. Law Number 19 of 2002 concerning Copyright.
3. Law Number 25 of 2003 concerning Amendments to Law Number 15 of 2002 concerning Money Laundering.
4. Law Number 15 of 2003 concerning the Eradication of Terrorism.

To address this issue, the Indonesian government has enacted stricter regulations and legal frameworks in recent years. The effectiveness of these efforts in protecting citizens and reducing Information and Electronic Transaction (ITE) crimes still requires further research. Human life, including in Indonesia, is greatly influenced by the rapid development of information and communication technology (ICT). Information and Communication Technology (ICT) has facilitated many aspects of human activity, such as communication, business, and governance. Conversely, advances in Information and Communication Technology (ICT) have also increased the opportunities for Information and Electronic Transaction (ITE) crimes, defined as crimes that utilize information and communication technology (ICT). Fraud, the spread of false information, data theft, and Information and Electronic Transaction (ITE) attacks are examples of this type of crime. Information and Electronic Transaction (ITE) crimes have become a major threat to the state and society.[5]

Internet crimes have emerged due to technological advances. These include various types of crimes such as fraud, identity theft, data breaches, computer viruses, and other malicious acts exploited by criminals through vulnerabilities in computer systems and networks. However, Electronic Information and Transactions (ITE) also have positive effects, such as the use of

[4] Iqbal Rifa'i Dkk, 'Dampak Positif Penagakan Hukum ITE Crime Di Indonesia', *Journal of Internacional Multidisciplinary Research*, 2.1 (2024).

[5] Agus Raharjo, *ITEcrime Pemahaman Dan Upaya Pencegahan Kejahatan Berteknologi* (Citra Adhitya Bakti, 2002).

information for education and culture. Information and Electronic Transactions (ITE) crimes such as phishing, carding, ransomware, identity theft, SIM swapping, skimming, online fraud, website and email hacking, data forgery, illegal content, OTP fraud, cyber terrorism, cyber espionage, and plagiarism of other people's websites continue to increase as a result of advances in information technology. To eradicate and investigate these crimes, digital forensics has become crucial.[6] The rapid growth of digital technology has created new complexities and challenges in the collection and analysis of digital evidence. Because the workings and data structures of each hardware and software differ, sophisticated forensic techniques are required. Digital forensics must be conducted with specific methods to ensure the integrity and validity of the evidence is maintained throughout the investigation process because digital evidence is very easily altered and destroyed. The need for clear rules and regulations in the use of digital forensics is crucial for the collection and analysis of evidence so that it can be accepted in court. The need for specialized resources for members of the Indonesian National Police is not commensurate with the demand for digital forensic experts. The production of human resources in the field of digital forensics that are professional, with integrity, and competent requires sufficient education and competence. Based on the above background, the author is interested in conducting research with the title "The Use of Digital Forensics in Revealing Information and Electronic Transaction (ITE) Crimes".

PROBLEM

How effective are criminal law regulations in handling crimes at the Riau Regional Police, Particularly in terms of the implementation of laws and regulations such as the ITE Law?

How can the use of digital forensic tools such as Cellebrite UFED be optimised in uncovering ITE crimes, and what are the obstacles faced such as human resource competence and forensic technical sophistication in the investigation process?

RESEARCH METHOD

Observational research through a survey best describes this research methodology, specifically, this study took a sample from a single population and used interviews as its primary data collection instrument. The author of this study collected all necessary materials, data, and information by conducting direct research at the specified location. Descriptive and analytical research characterizes this study, which aims to provide a clear picture of the use of digital forensics in uncovering information crimes and electronic transactions, especially its application in the Riau Regional Police. The sources of this research are primary legal sources, namely applicable legal regulations relating to the formulation of this problem, as well as secondary legal sources, namely literature or previous research.

RESULT AND DISCUSSION

[6] Miftakhur Rokhman Habibi and Isnatul Liviani, 'Kejahatan Teknologi Informasi (ITE Crime) Dan Penanggulangannya Dalam Sistem Hukum Di Indonesia'.

Discovery of Digital Evidence That Can Be Used as Evidence in the Crime of Informastion and Electronic Transactions (ITE)

Several important steps in the digital forensics process include finding digital evidence that can be used as evidence in Information and Electronic Transactions (ITE) crimes. Digital forensics is a scientific discipline used to identify, collect, analyze, and preserve digital evidence that can be used in criminal investigations. Data stored on computers, mobile devices, networks, or servers can be examples of this digital evidence.

The history of digital evidence's inclusion in Indonesian law has been a long one. Prior to the enactment of the Electronic Information and Transactions Law (ITE Law), electronic evidence was already prevalent in several laws and regulations, namely Law No. 8 of 1997 concerning Company Documents, Law No. 15 of 2003 concerning the Eradication of Terrorism, Law No. 15 of 2003 concerning Money Laundering, Law No. 20 of 2001 concerning the Eradication of Corruption, and Law No. 30 of 2002 concerning the Corruption Eradication Commission.

The presence of digital evidence in the Indonesian legal system was further strengthened by the enactment of the Electronic Information and Transactions Law (ITE Law), which is contained in Article 5 paragraph 1, which reads:

> *"Electronic Information and/or Electronic Documents and/or printouts thereof constitute valid legal evidence."*

This law also emphasizes that the digital evidence contained in the ITE Law is an extension of the legal evidence stipulated in the Criminal Procedure Code. The article concerning this is Article 5, paragraph 2, which reads:

> *"Electronic Information and/or Electronic Documents and/or printouts thereof as referred to in paragraph (1) constitute an extension of valid evidence in accordance with the Procedural Law in force in Indonesia."*

Indonesia's Electronic Information and Transactions Law (ITE Law), first enacted in 2008 and subsequently revised in 2016, is an attempt to regulate and address the growing number of cybercrimes and electronic transactions. In general, the ITE Law plays a significant role in addressing cybercrimes, but several aspects influence its effectiveness, including regulation, implementation, and public acceptance. Overall, the ITE Law plays a crucial role in addressing cybercrimes in Indonesia, but several challenges remain in its implementation and improvement. Updates are needed to adapt to rapid technological developments, as well as clearer boundaries regarding freedom of expression in cyberspace. Furthermore, increased law enforcement capacity, enhanced international cooperation, and strengthened personal data protection are also needed to make the ITE Law more effective in addressing cybercrimes in the future.

Indonesia's legal system has experienced significant developments in recent years related to digital technology and forensics. However, challenges remain to be addressed to better accommodate the needs of digital technology and forensics. While there have been some positive steps, several aspects need to be improved to make the legal system more efficient in

addressing issues related to cybercrime, electronic transactions, and digital forensic investigations. The need for digital technology and forensics is addressed through regulations such as the Electronic Information and Transactions Law and the Personal Data Protection Law. However, many challenges remain, such as inadequate law enforcement capacity, limited forensic infrastructure, and regulations that are not yet fully relevant to current technological developments. Therefore, regulatory reforms, increased human resource capacity, and more intensive collaboration between national and international institutions are needed to make the Indonesian legal system more effective in addressing cybercrime and digital technology.

In order for digital evidence to be used as valid evidence in court, it must meet the criteria:

a. Legal, meaning the evidence was obtained legally (in accordance with legal procedures, confiscation, digital forensic examination).
b. Authentic, meaning the evidence can be proven to be genuine and has not been altered or manipulated.
c. Reliable, meaning the evidence can be trusted and relied upon.
d. Relevant, meaning the evidence is directly related to the crime being tried and meets the elements of the crime.
e. Admissible, meaning the evidence is admissible in court.

This digital evidence is evidence that has been previously analyzed by a team of digital forensic analysts, consisting of experts specialized in digital expertise, particularly the use of digital evidence for legal purposes. The digital evidence analysis process consists of the following: After the evidence is secured, it must be analyzed. Several methods for analyzing digital evidence are:

a. File Analysis: Searching for evidence within files, including metadata, to trace their origin.
b. Log Analysis: Using network and device access logs to track user activity, find entry points, and uncover attack patterns.
c. Data Recovery: In some cases, deleted data can be recovered through data recovery techniques. This includes files intentionally deleted by criminals to cover their tracks.
d. Digital Footprint Analysis: Using digital tools to examine the perpetrator's digital footprint on the internet, such as digital transactions, browsing history, and IP addresses.

Digital evidence also has weaknesses, namely that digital evidence is easily deleted, obscured, or manipulated. Therefore, it is important for law enforcement to maintain the integrity of digital evidence. Maintaining the integrity of digital evidence so that it is legally valid is very important in the digital forensics process, especially to ensure that the evidence produced is admissible in court and is not damaged or modified during the collection, analysis, and storage process. There are several key steps that must be followed to maintain the integrity of digital evidence:

a. Securing the Chain of Custody

b. Using Write-Blocking Devices
c. Creating Forensic Images
d. Verifying Data Integrity with Hashing
e. Securing and Storing Digital Evidence
f. Using Legitimate Methods for Evidence Collection
g. Auditing and Monitoring
h. Storing and Using Trusted Software
i. Preparing Transparent Forensic Reports
j. Testimony in Court

To improve cybercrime and information and electronic transactions (ITE) handling at the Riau Regional Police, several legal policies worth considering include strengthening legal infrastructure, increasing human resource capacity, inter-agency collaboration, and updating investigative regulations and procedures. The following are several legal policy recommendations that can be adopted to improve the effectiveness of cybercrime handling at the Riau Regional Police:

a. Strengthening Human Resources (HR) Capacity
    1) Education and Training
    2) Improving Digital Forensic Skills

b. Strengthening Infrastructure and Forensic Tools
    1) Provision of Advanced Forensic Tools
    2) Provision of Adequate Digital Infrastructure

c. Updates and Improvements to Cybercrime Regulations
    1) Updates to the Electronic Information and Transactions Law and Cybercrime Regulations
    2) More Specific Regulations in Cybercrime Investigations

d. Cross-Institutional and International Cooperation
    1) Coordination with BSSN and Kominfo
    2) Cooperation with International Institutions

e. Improving Coordination with the Technology Industry and Digital Service Providers
    1) Partnership with Technology Companies
    2) Counseling and Cooperation with E-Commerce Companies

f. Increasing Community Involvement in Preventing Cybercrime
    1) Legal Socialization on Cyber Crime
    2) Establishment of a Cybercrime Complaint Center

g. Increased supervision and law enforcement
    1) Digital Traffic Monitoring
    2) Firm and Transparent Law Enforcement

h. Legal Process Facilities for Cybercrime Cases
    1) Assistance from Digital Forensics Experts
    2) Strengthening Adequate Investigation Procedures

To improve cybercrime and Electronic Information and Transactions (ITE) handling within the Riau Regional

Police, it is crucial to strengthen human resource capacity, provide adequate infrastructure, update relevant regulations, and enhance inter-agency and international cooperation. These collaborative efforts will help the Riau Regional Police handle cybercrime more effectively, efficiently, and in line with the rapid development of digital technology.

Application of Forensic Analysis Methods During Crimes in The Digital World

Forensic analysis methods are used in digital crime cases. They involve a series of established procedures and techniques to identify, collect, analyze, and present digital evidence that can be used in legal proceedings. These methods focus not only on finding evidence but also on maintaining its integrity so that it can be admissible and valid in court. The digital forensic process will identify digital evidence from an electronic system, which will then be analyzed to ensure it can be used as credible evidence. The output of this digital forensic process is digital evidence.[7] Laws dealing with digital evidence address two issues: integrity and authenticity. Integrity ensures that the act of seizing and obtaining digital media does not alter the evidence (either the original or a copy). Authenticity refers to the ability to confirm the integrity of the information; for example, that the imaged media matches the original evidence. The ease with which digital media can be modified means that documenting the chain of custody—from the crime scene through analysis, to the court—is crucial to maintaining the authenticity of evidence derived from digital systems.[8]

The main process in applying forensic analysis techniques when digital world crimes occur:

a. Preparation and Planning
   Before beginning a forensic analysis, law enforcement needs to make several preparations. This includes identifying the type of crime that occurred, which is necessary to select appropriate forensic tools based on the crime's criteria. After that, a forensic team consisting of digital forensic experts, legal investigators, and information technology experts is formed to handle the case.

b. Evidence Management
   Before the evidence is managed, digital evidence must first be secured. Evidence security ensures that the evidence is not damaged or altered during the analysis process. Evidence is first collected. Collecting relevant digital evidence is necessary after physical evidence has been secured. This data collection is carried out using forensic tools to identify various types of evidence that can be used in digital crimes. The process of taking bit-by-bit

[7] Oheo Kaimuddin Haris and others, 'Penggunaan Digital Forensik Dalam Pembuktian Tindak Pidana Pencemaran Nama Baik Di Media Sosial Berdasarkan UU ITE Use of Digital Forensics in Proofing the Criminal Offense of Damage to Good Name in Social Media Based on the Law of Information and Electro', *Journal Halu Oleo*, 6.2 (2024), pp. 588–603.

[8] Riston, Basoddin, and La ode Muhram, 'Fungsi Digital Forensik Dalam Pembuktian Tindak Pidana Siber (Studi Kasus Di Polda Sutra)', *Sultra Law Review*, 7.1 (2025).

[9] *Mayantara* (Aswindo, 2011)

copies of storage devices such as hard drives, smartphones, or servers to isolate the devices involved in the case from the network or other sources to prevent further data alteration. Everyone involved in the evidence collection must record and verify the process.

c. Digital Evidence Analysis
An important stage in the forensic process is analysis, where important information from the collected evidence can be revealed. Digital forensics can.

d. Preparation of Forensic Reports
After the evidence has been analyzed, a report should be prepared explaining the procedures and results. This report should be objective and include the following information:
   1) Case Description, a summary of crimes that occurred in the digital world.
   2) Methods Used, explains the equipment and methods used during the process of collecting and analyzing evidence.
   3) Evidence Findings, shows the evidence found and explains how the evidence is relevant to the crime.
   4) Conclusions and Recommendations,
   presenting the evidence found, providing conclusions about the perpetrator and how the crime was committed, and providing suggestions on what can be done to prevent similar incidents from occurring.

e. Presentation of Evidence in Court
Evidence that has been analyzed must meet the requirements before it can be presented in court, so digital evidence must be:
   1) Meeting the Validity Standards of evidence must be able to be proven to be original and not altered during the collection and analysis process.

It is to be assumed that the forensic expert handling the evidence must be prepared to provide an explanation in court regarding the process carried out and how the evidence can prove the perpetrator's involvement in the crime.

Optimizing Forensic Evidence Toold Such as Cellebrite UFED to Review and Analyze ITE Cases at the Riau Regional Police

There are several steps that can be taken to improve digital forensic tools such as Cellebrite's UFED in reviewing and analyzing ITE cases at the Riau Regional Police, including further development of these tools and their application in the context of digital law and investigations, including:

a. Human Resource Competency Improvement
Improving the capabilities of officers at the Riau Regional Police is a crucial component in optimizing the use of Cellebrite's UFED and other digital forensic tools. Officers involved in investigating Information and Electronic Technology (ITE) cases must receive ongoing training and

certification. They must be familiar with the latest digital forensic analysis methods and understand how to properly use forensic tools.

Steps taken:

1) Technical training on Cellebrite UFED, comprehensive training on how to best use Cellebrite UFED software, including the latest information on features and how to handle locked devices or encrypted data.
2) Enhanced skills in data interpretation, forensic team members must be skilled at analyzing data found on digital devices in addition to understanding how to access and download data.
3) Professional certification, implementing the Cellebrite Certified Logical Operator (CCLO) or Cellebrite Certified Physical Analyst (CCPA) certification program.

b. Optimizing the Use of Cellebrite UFED

Cellebrite UFED is a highly sophisticated digital forensic investigation tool. The Riau Regional Police must ensure its proper use to successfully solve Electronic Information and Telecommunications (ITE) cases.

Steps that can be taken:

1) Maximize Cellebrite's UFED features. Cellebrite's advanced UFED features include application data analysis, the ability to access data on locked mobile devices, and the ability to access hidden data. These features can be further utilized in the investigation of Electronic Information and Telecommunications (ITE) cases involving mobile devices.
2) Deeper Data Analysis Using Cellebrite to perform deeper analysis on data captured from devices, such as finding communication patterns, monitoring online activity, and finding relevant information from chat applications (such as WhatsApp and Telegram) frequently used by online criminals.
3) Selecting the Type of Examination, In the Cellebrite UFED Software there are several examination options including mobile devices, auto detect, search devices, device wizard.

In today's technological era, cybercrime, or crimes based on digital technology, are increasingly complex and difficult to track. Therefore, for strong, effective, efficient, and accurate law enforcement, digital evidence optimization is essential. The steps the Riau Regional Police can take to optimize digital evidence include:

a. Proper Evidence Collection Protocol

Following digital evidence collection protocols that comply with international standards such as Standard Operating Procedure (SOP) 1 on Digital Forensic

Examination Procedures, SOP 10 on Mobile Phone and Simcard Acquisition, SOP 11 on Mobile Phone and Simcard Examination and Analysis which refers to the Regulation of the Head of the Criminal Investigation Unit of the Indonesian National Police Number 1 of 2014 on Standard Operating Procedures for Digital Forensic Examination and Analysis, Good Practice Guide for Digital Evidence from the Association of Chief Police Officers (ACPO), England, 2012, and ISO/IEC 17025 on General Requirements for Chief Police Officers (ACPO), England, 2012, and ISO/IEC 17025 on General Requirements for the Competence of Testing and Calibration Laboratories, as well as ISO/IEC 27037 on Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence. It is also important to maintain transparency in the process so that each phase of the forensic analysis is properly recorded to maintain the integrity of the evidence and protect the results of the investigation that are acceptable to the court.

b. Technology and Software Improvements
Constantly update Cellebrite's UFED software and hardware, as well as other digital forensic tools, to ensure that they can handle emerging new types of data, such as encrypted data or data connected to new applications used in Electronic Information and Telecommunications (ITE) crimes.

c. Collaboration-Based Approach with the Technology Industry
Collaboration with technology providers or application platforms is also important to update digital forensic capabilities so that perpetrators of Information and Electronic Transaction (ITE) crimes can handle the new technology they use.

d. Internal Policy Development
The Riau Regional Police must create internal policies that support the effective and legal use of digital forensic tools. Possible steps include:
1) Consistent Digital Forensic Tools Use Policy. Establish rules about who is authorized to use forensic tools and ensure that the tools are used properly and not misused privately.

Preparation of Standard Operating Procedures (SOP), to ensure order in each investigation, create clear standard operating procedures (SOP) related to data collection, use of tools, and reporting of analysis results.

CONCLUSION

In handling cases of Information and Electronic Transactions (ITE) crimes, digital evidence has a legal standing as evidence even though it is not explicitly mentioned in the Criminal Procedure Code (KUHAP). Regulations regarding digital

evidence are regulated in the ITE Law, which provides legitimacy to the use of electronic information, electronic documents, hardware, software, as valid legal evidence in court. The digital forensic process which includes identification, analysis, security and documentation of digital evidence is very important to ensure that the evidence meets legal requirements such as authenticity, relevance and admissibility in court, and is not affected by data manipulation or changes.

The application of forensic analysis methods in handling crimes in the digital world involves a series of strict procedures to ensure the integrity of digital evidence, starting from the preparation and planning stage, through securing evidence, to analysis and presentation in court. Each stage, such as evidence collection, analysis of deleted data, and metadata recovery, focuses on maintaining the authenticity of the evidence and ensuring that the evidence found is accountable and admissible in court. Success in this process depends on the use of digital forensic tools relevant to the type of crime that occurred.

To optimize the use of digital forensic tools such as Cellebrite's UFED in investigating Electronic Information and Transactions (ITE) cases at the Riau Regional Police, a series of strategic steps are needed, including improving the competence of Human Resources (HR) through training and certification, optimizing the use of forensic tools by utilizing all available advanced features, and collaborating with other institutions to improve technical capabilities. Furthermore, it is important to ensure the implementation of consistent procedures in accordance with international standards in the collection and analysis of digital evidence, regularly renew software licenses, and develop internal policies that support the proper and legal use of forensic tools.

References

Agus Raharjo, *ITEcrime Pemahaman Dan Upaya Pencegahan Kejahatan Berteknologi* (Citra Adhitya Bakti, 2002)

Amiruddin & Asikin, *Pengantar Metode Penelitian Hukum* (PT. Raja Grafindo Persada, 2004)

Arief, Barda Nawawi, *Bunga Rampai Kebijakan Hukum Pidana* (2010)

Dkk, Iqbal Rifa'i, 'Dampak Positif Penagakan Hukum ITE Crime Di Indonesia', *Journal of Internacional Multidisciplinary Research*, 2.1 (2024)

Firman Wahyudi, 'EKSISTENSI DAN PERAN ALAT BUKTI ELEKTRONIK DALAM SISTEM PERADILAN INDONESIA', *Pengadilan Agama Bangil*, 2019

Habibi, Miftakhur Rokhman, and Isnatul Liviani, 'Kejahatan Teknologi Informasi (ITE Crime) Dan Penanggulangannya Dalam Sistem Hukum Di Indonesia'

Haris, Oheo Kaimuddin, Sitti Aisah Abdullah, Ali Rizky, and Sri Ratih Indah, 'Penggunaan Digital Forensik Dalam Pembuktian Tindak Pidana Pencemaran Nama Baik Di Media Sosial Berdasarkan UU ITE Use of Digital Forensics in Proofing the Criminal Offense of Damage to Good Name in Social Media Based on the Law of Information and Electro', *Journal Halu Oleo*, 6.2 (2024), pp. 588–603

Riston, Basoddin, and La ode Muhram,

'Fungsi Digital Forensik Dalam Pembuktian Tindak Pidana Siber (Studi Kasus Di Polda Sutra)', *Sultra Law Review*, 7.1 (2025)

Widodo, *Aspek Hukum Kejahatan Mayantara* (Aswindo, 2011)