JURNAL HUKUM Khaira Ummah

Master of Law, UNISSULA

E-ISSN: 2988-3334
ISSN: 1907-3319
Vol. 20 No. 2 June 2025

Police Digital Forensics Functional in Handling Hate Speech Crimes in Cyberspace

Junaidi[1)] & Gunarto[2)]

[1)]Master of Notary Law, Faculty of Law, Sultan Agung Islamic University (UNISSULA) Semarang, Indonesia, E-mail: junaidi.std@unissula.ac.id

[2)]Master of Notary Law, Faculty of Law, Sultan Agung Islamic University (UNISSULA) Semarang, Indonesia, E-mail: gunarto@unissula.ac.id

Abstract. *The Police Criminalistics Laboratory is part of the organizational structure of the Police which has the task or function as a supervisor, implementer of criminalistics or Forensics, as a science whose application is to provide technical support in the investigation/investigation of criminal acts. This study aims to Functional Digital Forensics of the Police in Handling Hate Speech Crimes in Cyberspace. In this study, the approach method used is: a normative legal approach (normative legal research method). library legal research conducted by examining library materials or secondary data alone. The research specification used is Descriptive Analytical, namely an effort to analyze and explain legal problems related to objects with a comprehensive and systematic description of everything related to the Functional Digital Forensics of the Police in Handling Hate Speech Crimes in Cyberspace. In the context of Indonesian law, digital forensics has been legitimized as valid evidence through the recognition of electronic evidence in the Electronic Information and Transactions Law (UU ITE), as well as the Draft Criminal Procedure Code which accommodates electronic evidence as part of legal evidence. Therefore, the use of digital forensics must be carried out by competent experts and follow established procedures so that the results can be legally accepted in court. Digital forensics plays a vital role in proving the perpetrators in hate speech crimes in cyberspace. Through a scientific process that can be accounted for, digital forensics is able to reveal who exactly "everyone" is referred to in the criminal article. Its main function is not only in collecting evidence, but also in validating, authenticating, and presenting digital data as valid legal evidence. In this digital era, the success of law enforcement against hate speech is highly dependent on the sophistication and integrity of digital forensics.*

Keywords: *Crime; Digital Forensics; Law Enforcement.*

1. Introduction

In a state of law, law is the main pillar in moving the joints of social, national, and state life. One of the main characteristics of a state of law lies in its tendency to assess actions taken by society on the basis of legal regulations. This means that a state with the concept of a

E-ISSN: 2988-3334
ISSN: 1907-3319
Vol. 20 No. 2 June 2025

state of law always regulates every action and behavior of its people based on applicable laws.

This is done to create, maintain and defend peace in social life in accordance with what is mandated in Pancasila and the 1945 Constitution, namely that every citizen has the right to feel safe and free from all forms of crime.

Law enforcement is one of the efforts to create order, security and peace in society, especially taking action after a violation of the law. Evidence is the main thing in the examination and action after a criminal case occurs. [1]This is because through the stages of proof, a process, method, act of proving occurs to show whether the defendant is right or wrong in a criminal case, especially in a court hearing.

In dealing with criminal cases that are not supported by at least two valid pieces of evidence, law enforcement officers find it difficult to prove the guilt or innocence of the suspect/defendant. The process of investigating and investigating criminal acts today has experienced much progress with the development of modern science and technology. One of the impacts of the development of science and technology on the investigation and investigation of criminal acts is the construction of a forensic laboratory.[2]

The Indonesian National Police Criminalistics Laboratory is part of the organizational structure of the Indonesian National Police which has the task or function of being a supervisor and implementer of criminalistics or forensics, as a science whose application is to provide technical support in the investigation/prosecution of criminal acts.[3]. This is done through examination of evidence in a forensic laboratory or technical forensic examination at the scene of the crime, in line with the development of the reform movement and the advancement of science and technology.

Presidential Instruction Number 2 of 1999 and MPR Decree Number 6 of 2000 concerning the separation of the Police from the TNI, were also strengthened by MPR Decree Number 7 of 2000 concerning the Role of the TNI and the Indonesian National Police. The Police are trying to build a new image and paradigm. The image of the Police, which was originally militaristic and tended to be repressive, has gradually begun to change with a new paradigm as a protector, guardian, and servant of the community (to serve and protect), professional, modern and trusted. However, it is realized that it is not easy to make changes to the militaristic culture and paradigm of the state apparatus that has taken root in the Police.[4]

The role of the Indonesian National Police Criminalistics Laboratory as an expert in its field according to Article 7 paragraph (1) letter h and Article 120 paragraph (1) of the Criminal Procedure Code in processing the Crime Scene (TKP) by applying the scientific crime investi-

---

[1] Dwi Fahri Hidayatullah, Gunarto, and Lathifah Hanim. Police Role in Crime Investigation of Fencing Article 480 of the Criminal Code (Study in Polres Demak). Jurnal Daulat Hukum Volume 2 Issue 4, December 2019, url: http://jurnal.unissula.ac.id/index.php/RH/article/view/8288/3864

[2] Abdussalam, Buku Pintar Forensik (Pembuktian Ilmiah), Jakarta: Restu Agung, 2006,hlm. 1

[3] Yeremias Tony Putrawan, Jawade Hafiz, and Aryani Witasari. Crime Investigation of Trade of The Human Body Organs on Criminal Investigation Police (Case Study Police Report Number: LP / 43 / I / 2016 / Bareskrim dated 13 January 2016), Jurnal Daulat Hukum Volume 2 Issue 4, December 2019, url: http://jurnal.unissula.ac.id/index.php/RH/article/view/8442/3921

[4] Satjipto Rahardjo, Membangun Polisi Sipil Perspektif Hukum, Sosial & Kemasyarakatan, Penerbit Buku Kompas, Jakarta, 2007, hlm 75.

E-ISSN: 2988-3334
ISSN: 1907-3319
Vol. 20 No. 2 June 2025

gation (SCI) method. Therefore, it is the right momentum for the Indonesian National Police to always empower scientific investigations (Scientific Crime Investigation/SCI). Criminalistics/forensic science is delivered as early as possible to the Indonesian National Police educational institutions, investigators, prosecutors, judges with the hope that later they can become reliable law enforcers (upholding the supremacy of law) who already have a criminalistic insight character. Indonesia adheres to an integrated law enforcement system (Integrated Criminal Justice System) which is the legal spirit of the Criminal Procedure Code. This integration is philosophically an instrument to realize the national goals of the Indonesian nation which have been formulated by the Founding Fathers in the 1945 Constitution, namely protecting society (social defense) in order to achieve social welfare (social welfare).[5]

Considering that crime follows the development of society and the technology required, criminalistics and crime effection are also increasingly advanced and should always be able to overcome the techniques used in each crime pattern, one of which is by having a criminalistics laboratory that tries to help uphold justice and uphold the truth and also so that there are no mistakes in making decisions for innocent people.

The development of information and communication technology has been so rapid that it has affected every aspect of human life. It is undeniable that information and communication technology is the spearhead of the era of globalization that is now sweeping across almost the entire world. This condition has given birth to a new world often referred to as the global village, inhabited by citizens called network citizens (netizens).[6]

Technological advances have changed the structure of society from local to a society with a global structure. This change is caused by the presence of information technology. In the development of information technology combined with media and computers, a new device called the internet was born. The presence of the internet has changed the new paradigm in human life. Life has changed from being only real to being added to a new reality that is virtual. This second reality can be said to be the internet and cyber space. The development of computer technology has also resulted in various forms of computer crime in the cyberspace environment which then gave birth to a new term known as cybercrime.[7]

The problem of hate speech has recently become more of a concern, both among the Government, Law Enforcement, and the Community. The perpetrators of this crime do not only involve the lower middle class (the community in general), but also involve figures or leaders in the community and users of social media facilities (social networks) on the cyberspace/cyber world in Indonesia.10 As social networks are websites that allow users to build connections and relationships with other internet users.

Acts or crimes that need serious attention at this time are Hate Speech, Hate Speech itself is "A communication act carried out by an individual or group in the form of provocation, incitement, or insults to other individuals or groups in terms of various aspects such as skin color, gender, disability, sexual orientation, citizenship, religion and others.

---

[5] Romli Atmasasmita, Sistem Peradilan Pidana; Perspektif Eksistensialisme dan Abilisionisme, Cet II revisi, Bina Cipta, Bandung, 1996, hlm 9-10.

[6] Dikdik M. Arief Mansur dan Elisatris Gultom, Cyber Law; Aspek Hukum Teknologi Informasi. Jakarta: Refika Aditama, 2009, hlm 121

[7] A. Rahmah dan Amiruddin Pabbu, Kapita Selekta Hukum Pidana. Jakarta: Mitra Wacana Media, 2015, hlm 3.

E-ISSN: 2988-3334
ISSN: 1907-3319
Vol. 20 No. 2 June 2025

The problem of violations or crimes against honor in this case, for example, such as the crime of defaming others, slandering, insulting and unpleasant acts are acts that violate the law because they disturb and violate the human rights of others. These acts can not only be done directly with words in public but also lately often done in cyberspace or social media, because in cyberspace people feel freedom in terms of expressing opinions or criticizing someone who is considered not to violate the law and is safe because there is no direct physical contact with other people.

From this problem, ethics in online media now need to be enforced to prevent even greater crimes and violations, considering that online media has become an important part of communication and information infrastructure, especially as more and more parties abuse cyberspace to spread their displeasure about something related to ethnicity, religion and race. This is what is then called Hate Speech.

That almost all countries around the world have laws governing Hate Speech, in Indonesia the articles governing Hate Speech are regulated in Article 156, Article 157, Article 310, Article 311 of the Criminal Code, then Article 28. Article 45 paragraph (2) of Law No. 19 of 2016 concerning information & electronic transactions and Article 16 of Law No. 40 of 2008 concerning the elimination of racial and ethnic discrimination. So far, Hate Speech has resulted in minor to serious human rights violations, always initially just words, either on social media, or through leaflets, but the effect is able to mobilize the masses to trigger conflict and bloodshed.[8]

Law Number 19 of 2016 concerning amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE) is a lex specialis of the Criminal Procedure Code (KUHAP), because the ITE Law regulates new evidence which is an extension of conventional evidence. This is because the ITE Law regulates the validity of law in the cyber realm. The regulation of electronic evidence in the ITE Law is regulated in Chapter III concerning Information, Documents, and Electronic Signatures, and Article 44 of the ITE Law. Article 5 Paragraph 1 of the ITE Law explicitly stipulates that "Information and/or Electronic Documents and/or printouts are an extension of valid evidence in accordance with the applicable Procedural Law in Indonesia". This provision confirms that electronic evidence has been accepted in the legal system of evidence in Indonesia.[9]

In this case, the use of digital forensics is as electronic evidence that can be used to resolve cyber crime. In the world of computer security, there has also been development. Digital evidence that has begun to be used as evidence has begun to raise quite complex problems. However, the most fundamental problem of this digital evidence is about the authenticity and integrity of the digital evidence so that the digital evidence can be trusted. To realize this, a digital evidence investigation process known as digital forensics emerged. Digital forensics is an investigation method with the application of science and technology to examine and analyze digital evidence. This science, which is part of computer security, is developing rapidly following the technology that is also developing. This digital forensics process will find digital evidence from an electronic system which will then be analyzed so that it can be

[8] Surat Edaran Kapolri NOMOR SE/06/X/2015 tentang (Hate Speech) Ujaran Kebencian.
[9] Sitompul, Josua, Cyberspace Cybercrime Cyberlaw Tinjauan Aspek Hukum Pidana, Tata Nusa, Jakarta, 2012, hlm. 279

E-ISSN: 2988-3334
ISSN: 1907-3319
Vol. 20 No. 2 June 2025

used as reliable evidence. The output of the digital forensics process is the digital evidence itself and the results of the digital forensic test.

2. Research Methods

In accordance with the title and problems to be discussed in this study and in order to provide useful results, this study was conducted with normative legal research (normative legal research method). The normative legal research method is a library legal research conducted by examining library materials or secondary data alone. This research was conducted in order to obtain materials in the form of: theories, concepts, legal principles and legal regulations related to the subject matter.[10]

3. Results and Discussion

3.1. What are the Regulations on Digital Forensics in Proving Hate Speech Crimes in Cyberspace?

Forensics in legal language can be interpreted as the results of the examination required in the court process. While forensics in the Indonesian sense means related to the court. Forensic science includes all sciences that are related to criminal problems, or it can be said that in terms of its role in solving criminal cases, forensic sciences play an important role.

Forensic sciences, namely sciences which are the use of various sciences for the benefit of justice:

1. Forensic medicine.
2. Forensic psychology
3. Forensic psychiatry
4. Forensic chemistry

Criminalistics, which is the science of investigation, consists of a collection of other sciences, such as the science of fingerprints (dactylscopy), the science of bullets (ballistics), the science of poisons (toxicology), and includes the science of digital forensics.[11]

Digital Forensics is a science and expertise to identify, collect, analyze and test digital evidence when handling a case that requires handling and identification of digital evidence. Digital forensics is a branch of science that aims to obtain information and investigate digital evidence so that it can be accounted for in court as valid evidence in the eyes of the law. Digital evidence itself means the results of electronic evidence originating from personal computers, mobile phones, notebooks, servers, or technological aids that can be categorized as storage media and can be analyzed as evidence.[12]

There are several definitions that can be used as a reference regarding the meaning of digital forensics:

---

[10] Soerjono Soekanto dan Sri Mahmudji, Penelitian Hukum Normatif, Suatu Tinjauan Singkat, (Jakarta: Raja Grafindo Persada, 2003), hlm. 13.
[11] Frans Maramis, Op.Cit, 2012, hlm.26-27
[12] W. A. Mukti, S. U. Masruroh, and D. Khairani, Analisa dan Perbandingan Bukti Forensik Aplikasi Media Sosial Facebook dan Twitter pada Smartphone Android, Jurnal Tek. Inform., Volume 10 Nomor 1, 2018, hlm.77

E-ISSN: 2988-3334
ISSN: 1907-3319
Vol. 20 No. 2 June 2025

1. According to Budhisantoso, "Digital forensics is a combination of legal disciplines and computer science in collecting and analyzing data from computer systems, networks, wireless communications, and storage devices so that they can be brought as evidence in law enforcement."

According to SC. Gupta, “Digital forensics is defined as the use of proven and established scientific methods for the preservation, collection, validation, identification, analysis, interpretation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of a criminal event or helping to anticipate unlawful acts that are proven to interfere with planned operations.”

2. According to Seema Yadav, “Digital forensics is a branch of forensic science that is used to cover the recovery and investigation of data in digital devices, often in relation to crime investigation”.

From the definition above, it can be concluded that digital forensics is a branch of forensic science that identifies, analyzes, and validates digital evidence of computer crime (cyber crime). Digital Forensics is the application of computer science and technology for the purpose of legal evidence, which is to prove high-tech crimes or computer crimes scientifically so that digital evidence can be obtained that can be used to ensnare the perpetrators of the crime. Therefore, the importance of digital forensics in revealing computer crime cases is an urgency for law enforcement, so digital forensics must always be developed following the development of computer science and technology.

Based on the results of an interview with a digital forensics analyst, Hugeng Purwatmadi explained that Digital Forensics includes several sub-branches related to the investigation of various types of devices, media or artifacts.

1. Computer Forensics

The goal of computer forensics is to explain the current state of digital artifacts, such as computer systems, storage media or electronic documents. The discipline typically includes computers, embedded systems (digital devices with basic computing power and onboard memory) and static memory (such as USB pen drives). Computer forensics can concern a wide range of information, from logs (such as internet history) through to the actual files on the drive.

2. Mobile device forensics

Mobile device forensics is a sub-branch of digital forensics that deals with the recovery of digital evidence or data from mobile devices. It differs from computer forensics in that mobile devices will have an inbuilt communication system (e.g. GSM) and usually, a proprietary storage mechanism. Investigations usually focus on simple data such as call and communication data (SMS/Email) rather than in-depth recovery of deleted data. Mobile devices are also useful for tracking or through location information, either from inbuilt GPS line/location tracking or through cell site logs, which track devices within their range.

3. Forensic Network

Network forensics deals with the monitoring and analysis of computer network traffic, both local and WAN/internet, for the purpose of gathering information.

information, gathering evidence, or intrusion detection. Traffic is typically intercepted at the

E-ISSN: 2988-3334
ISSN: 1907-3319
Vol. 20 No. 2 June 2025

packet level, and either stored for analysis or filtered in real time. Unlike other areas of digital forensics, data networks are often stable and rarely logged, making the discipline often reactionary.

4. Database forensics

Database forensics is a branch of digital forensics that deals with the forensic study of databases and their metadata. Investigations use database contents, log files and RAM data to construct time-lines or recover relevant information.58

Proof is a provision that contains outlines and guidelines on the ways that are legally permitted to prove the guilt charged against the accused. Proof is also a provision that regulates the evidence that is legally permitted and may be used by the judge to prove the guilt charged.[13]

The existence of evidence is very important in the investigation of computer crime cases and computer-related crimes because with this evidence investigators and forensic analysts can reveal these cases with a complete chronology, to then track the whereabouts of the perpetrators and arrest them, therefore the position of this evidence is very strategic, investigators and forensic analysts must understand the types of evidence. It is expected that when he comes to the crime scene related to computer crime and computer-related crime cases, he can recognize the existence of the evidence to then be examined and analyzed further. The classification of digital forensic evidence is divided into electronic evidence. This evidence is physical and can be recognized visually, therefore investigators and forensic analysts must understand so that they can then recognize each of these electronic evidence when searching for evidence at the crime scene.

hate speech in cyberspace as a form of cybercrime. Cyber crime is a crime that is directly related to electronic media produced by a computer network that is used as a place to conduct direct communication (online). Cyber crime is a type of crime related to the use of technology and unlimited communication, and has a strong characteristic with a technological engineering that relies on a high level of security, from information delivered and accessed by internet users.

According to expert Widodo, cyber crime is any activity of a person, group of people, legal entity that uses a computer as a means of committing a crime, or makes a computer a target for a crime. All of these crimes are forms of acts that are contrary to laws and regulations, both in the sense of being against the law materially and against the law formally.[14]

The meaning of Hate Speech itself is an act of communication carried out by an individual or group in the form of provocation, incitement, or insults to other individuals or groups in terms of various aspects such as race, skin color, gender, disability, sexual orientation, citizenship, religion and others. In the legal sense, Hate Speech is words, behavior, writing, or performances that are prohibited because they can trigger acts of violence and prejudice either from the perpetrator of the statement or the victim of the act. Websites that use or implement Hate Speech are called (Hate Sites). Most of these sites use Internet Forums and

[13] M.Yahya Harahap, Pembahasan Permasalahan dan Penerapan KUHAP:Pemeriksaan Sidang Pengadilan, Banding, Kasasi, dan Peninjauan Kembali: Edisi Kedua, Jakarta: Sinar Grafika, 2006, hlm.273.
[14] Widodo, Aspek Hukum Kejahatan Mayantara, Aswindo, Yogyakarta, 2011, hlm. 7

News to emphasize a particular point of view. Hate Speech is an act of communication carried out by an individual or group in the form of provocation, incitement, or insults to other individuals or groups in terms of various aspects such as race, skin color, gender, disability, sexual orientation, citizenship, religion and others.

In the Circular Letter of the Chief of Police Number SE/6/X/2015, it is explained that hate speech can be a criminal act regulated in the Criminal Code (KUHP) and other criminal provisions outside the Criminal Code, which include insults, defamation, slander, provoking, inciting, spreading fake news. All of the above actions have the aim or can have an impact on discrimination, violence, loss of life, and/or social conflict; Furthermore, in letter (g) it is stated that hate speech that aims to incite and create hatred towards individuals or groups of people, in various communities that are distinguished from aspects of Tribe, Religion, Religious Movement, Belief or belief, Race, Inter-group, Skin color, Ethnicity, Gender, Disabled (disabled), Sexual orientation.

Digital forensic methods and process models have been widely developed by forensic practitioners and investigators, based on personal experience and expertise, on an ad hoc basis to achieve standardization at the scene of the crime. However, there is currently no standard that formalizes the digital forensic investigation process, although efforts to standardize the process have been initiated within the International Standardization Organization (ISO). Digital forensic investigations, hereinafter referred to as Digital Forensics Investigations (DFI), are the phases of correlating extracted information and digital evidence to build factual information for review by a judicial body.[15]

Digital forensics is one of the means to assist investigators in their authority to conduct investigations and inquiries as regulated in Law Number 11 of 2008 concerning Electronic Information and Transactions in conjunction with the Criminal Procedure Code (KUHAP). In order to be able to apply digital forensics in investigations, a deeper understanding of technological science is needed in addition to the legal science that is usually applied in criminal court proceedings. Currently, the Draft Criminal Procedure Code has also added several pieces of evidence to maximize the judge's considerations in making decisions. This can be seen in Article 175 Paragraph (1) of the Draft Criminal Procedure Code, valid evidence includes:

1. Evidence;
2. Letter-Letter;
3. Electronic Evidence;
4. Expert testimony;
5. Statement of a witness;
6. Statement of a defendant;
7. Judge's observation.

From the draft of the Criminal Procedure Code, there is additional evidence, namely

[15] 0M.Nur Faiz, Studi Komparasi Investigasi Digital Forensik pada Tindak Pidana Kriminal, Jurnal of INISTA. Vol 1 No 1, 2018, hlm.64

E-ISSN: 2988-3334
ISSN: 1907-3319
Vol. 20 No. 2 June 2025

electronic evidence. Although the meaning of electronic evidence itself has not been explained, digital forensics can be one of the means that can be accommodated into electronic evidence by including standards and methods in its application as well as digital forensic examination procedures and experts who conduct examinations so that the evidence is valid and reliable.

Digital forensics expert, Hugeng Purwatmadi, said that in the digital and electronic world, the original evidence is not analyzed, which is why the evidence must be kept, which is different from dissecting the victim's body. The term electronic evidence in Indonesia was introduced in 2001 with the emergence of electronic evidence in Article 26A of Law Number 20 of 2001 concerning Amendments to Law Number 31 of 1999 concerning the Eradication of Corruption. Since then, almost all laws that regulate procedural law also contain rules that recognize the use of electronic evidence as evidence in trials, especially with the enactment of Law Number 11 of 2008 concerning Information and Electronic Transactions. This is explained in Article 5 Paragraph (1) of the ITE Law that: "Electronic Information and/or Electronic Documents and/or printouts are valid evidence". Article 1 of Law Number 19 of 2016 explains the types of electronic evidence in more detail, namely Electronic Information and Electronic Documents, including:

1. Electronic Information is one or a set of electronic data, including but not limited to writing, sound, images, maps, designs, photographs, electronic data interchange (EDI), electronic mail (electronic mall), telegrams, telex, telecopy or the like, letters, signs, numbers, access codes, symbols, or perforations that have been processed which have meaning or can be understood by people who are able to understand them.

2. Electronic transactions are legal acts carried out using computers, computer networks, and/or other electronic media.

3. Information Technology is a technique for collecting, preparing, processing, announcing, analyzing, and/or disseminating information.

4. "Electronic Documents are any Electronic Information created, forwarded, sent, received, or stored in analog, digital, electromagnetic, optical, or similar forms, which can be viewed, displayed, and/or heard via a computer or Electronic System, including but not limited to writing, sound, images, maps, designs, photographs, or the like, letters, signs, numbers, access codes, symbols or perforations that have meaning or significance or can be understood by people who are able to understand them."

In this case, what is meant by Electronic Information and/or Electronic Documents is in principle electronic data that has a form and media that is different from non-electronic data (non-electronic data can be interpreted as data created by humans in a conventional form, for example, human handwriting in the form of a signature written on paper). "Based on Article 1 of the ITE Law, it can be said that this electronic data requires means or media in pouring it such as electronic devices, namely computers, telegram machines, machines, faxes, printers, and so on".71 While referring to the general understanding of electronic evidence, it is data that is stored and/or transmitted via an electronic device, network, or communication system. This data is what is needed to prove a crime that occurs in court later, not the physical form of the electronic device.

Article 5 Paragraph (1) of the ITE Law regulates Electronic Information and/or Electronic

Documents as valid evidence, apart from Article 184 of the Criminal Procedure Code which regulates valid evidence consisting of witness statements, expert statements, letters, instructions and statements from the accused.

According to this article, there are four requirements that must be met so that electronic evidence can be used as valid legal evidence, namely it can be accessed, displayed, its integrity is guaranteed, and it can be accounted for. That the proof of the validity of electronic evidence in the criminal justice process must be carried out by considering the requirements stipulated in Article 6 of the ITE Law. In Indonesia, the position of electronic evidence is the same as evidence whose evidentiary value must still be strengthened through other evidence, including through letters, instructions, or expert/witness statements.

Referring to the provisions of evidence in the Criminal Procedure Code, then in accordance with the applicable procedural law in Indonesia, it means that there must be a test of electronic evidence or a method that must be used to prove the validity of the electronic evidence so that it can be declared as valid evidence in court just like other evidence. This is regulated in the explanation of the ITE Law which determines:

Proof is a very important factor, considering that Electronic Information is not only not yet comprehensively accommodated in the Indonesian legal system, but is also very vulnerable to being changed, tapped, and falsified and sent to various corners of the world in a matter of seconds. Thus, the resulting impacts can be very complex and complicated.72

Electronic Information and/or Electronic Documents can be accurate and reliable if the system used in testing it is also an accurate and reliable system. The system must be certified, so that Electronic Information and/or Electronic Documents also relate to the validity of the evidence. Because when compared to non-electronic evidence, Electronic Information and/or Electronic Documents have a special characteristic, namely in the form of being stored in an electronic device so that it requires a special tool to view and read it. Given the nature of the evidence that is vulnerable to being changed, manipulated and changed, in this case a test is needed that must be carried out on Electronic Information and/or Electronic Documents to examine the electronic evidence, namely by means of digital forensics so that it can be declared as valid evidence in court just like other evidence.

Digital forensics is widely placed in various needs, including to handle several criminal cases involving the law, such as analyzing the validity of evidence, case reconstruction, efforts to restore system damage, solving problems involving hardware or software, and in understanding systems or various cases involving digital devices. This digital forensics specialization has a wide scope of research objects and discussions.

In Circular Letter Number: SE/06/X/2015 concerning Handling of Hate Speech, it is emphasized that this circular letter can be used as a reference, there are various types of hate speech that have been regulated by the Criminal Code and are used by the police internally to understand the steps for handling hate speech by taking preventive action so that perpetrators who are proven to have insulted and carried out hate speech will be handled through mediation first, prioritizing the function of community policing to cooperate with community leaders as a repressive action, however, if there is no agreement

E-ISSN: 2988-3334
ISSN: 1907-3319
Vol. 20 No. 2 June 2025

in mediation and the act is still repeated, then criminal action will be taken, namely charging the perpetrator with a criminal act in accordance with the alleged article.74

The legal basis for the use of electronic evidence in court has become increasingly clear after Law No. 19 of 2016 concerning electronic information and electronic transactions (ITE Law) Article 1 paragraph (1) and (4), ITE Law Article 5 paragraph (1) and

(2) regarding print outs as valid evidence. Article 5 paragraph (3) of the ITE Law states that the validity of this electronic evidence is recognized by the judge if it uses an electronic system in accordance with the provisions stipulated in Article 16 paragraph (1) of the ITE Law. Article 43 paragraph (3) of the ITE Law states that "Searches and/or seizures of electronic systems related to suspected criminal acts must be carried out with the permission of the Head of the local District Court".

3.2. What is the Role and Function of Digital Forensics in Proving the Elements of Each Person as a Perpetrator of Hate Speech Crimes in Cyberspace?

The development of information and communication technology has brought various conveniences, but has also given rise to new challenges in law enforcement, one of which is the rise of hate speech in cyberspace. Hate speech can trigger social conflict, national disintegration, and public unrest. Therefore, law enforcement against perpetrators of hate speech is very important, including proving the elements of the perpetrator. It is in this context that digital forensics plays a central role in exposing and proving the involvement of individuals in the crime.[16]

According to the Circular Letter of the Chief of Police Number SE/6/X/2015 concerning Handling of Hate Speech, hate speech includes acts of spreading hatred or hostility towards individuals or groups based on ethnicity, religion, race, and inter-group (SARA). In cyberspace, it can take the form of social media statuses, video uploads, comments, or provocative memes. When such speech violates the law, the perpetrator can be subject to criminal charges based on Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE), as amended by Law Number 19 of 2016[17]

One of the biggest challenges in proving hate speech crimes in cyberspace is the digital nature of the evidence. Digital evidence is easily deleted, modified, and widely distributed. Therefore, a scientific, systematic, and legally valid method is needed in identifying, collecting, and analyzing digital evidence to reveal who the real perpetrator is.[18]

Digital forensics is a branch of forensic science that focuses on the process of identifying, preserving, analyzing, and presenting digital data as evidence in legal proceedings. In cases of hate speech, digital forensics plays a role starting from collecting evidence on the perpetrator's device (computer, smartphone), to analyzing metadata, activity logs, IP

[16] Nugroho, R. (2020). Hukum dan Teknologi Informasi: Suatu Pengantar. Jakarta: Prenadamedia Group
[17] Indonesia. (2016). Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan Atas UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Lembaran Negara RI Tahun 2016 No. 251
[18] Casey, E. (2011). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Academic Press

E-ISSN: 2988-3334
ISSN: 1907-3319
Vol. 20 No. 2 June 2025

addresses, and other digital traces that lead to the perpetrator's identity.[19]

The first step in the digital forensics process is the identification of digital evidence. The forensics team must determine which devices are relevant to the alleged crime. After that, data acquisition is carried out, which is the process of taking a digital copy without changing the original data, in order to maintain the validity of the evidence. This is important because even the slightest change to the original data can invalidate the validity of the evidence in court.[20]

In hate speech cases, digital forensics analyzes various data such as IP addresses, cookies, server logs, geolocation, and network activity. For example, tracking the IP address of a device that uploads hateful content can lead to the location and identity of the user. In addition, log files also record access times and activities, which can strengthen evidence of when and from where the content was disseminated.[21]

Digital evidence must go through an authentication process to be accepted in legal proceedings. Hash techniques (such as MD5 or SHA-1) are used to ensure data integrity, that is, to ensure that the data has not changed since acquisition. In addition, evidence must be validated with tools and methods that can be scientifically retested, in order to meet the strict chain of custody principle.[22]

In Indonesian criminal law, the element of the perpetrator in a crime must be proven. The phrase "every person" in the ITE Law emphasizes that anyone who actively commits, orders, or participates can be held legally accountable. Digital forensics is the main tool in proving that a particular account was operated by the suspect at the time of the incident, with evidence of login, fingerprint keyboard, and typical digital behavior (digital behavior profiling)[23]

The digital evidence obtained must be understandable to judges and prosecutors who generally do not have a technical background. Therefore, digital forensic experts are tasked with compiling systematic forensic reports, as well as providing expert testimony in court. These experts explain how digital evidence was collected, analyzed, and why it can be relied upon to link the perpetrator to the crime.[24]

Handling hate speech in cyberspace requires cross-agency cooperation: the police, the Ministry of Communication and Information, the National Cyber and Crypto Agency (BSSN), and digital platform providers. Digital forensics often requires data from internet service providers (ISPs), social media platforms, or even servers located abroad. This procedure is carried out through mutual legal assistance (MLA) if it is cross-country, or through an official

---

[19] Kruse, W. G., & Heiser, J. G. (2002). Computer Forensics: Incident Response Essentials. Addison-Wesley

[20] Nelson, B., Phillips, A., & Steuart, C. (2018). Guide to Computer Forensics and Investigations. Cengage Learning

[21] Rogers, M. K. (2006). A Two-Dimensional Circumplex Approach to Digital Investigations. Digital Investigation, 3, 137–147

[22] Reith, M., Carr, C., & Gunsch, G. (2002). An Examination of Digital Forensic Models. International Journal of Digital Evidence, 1(3), 1–12

[23] Sumardjono, MSW (2019). Criminal Law and Information Technology. Yogyakarta: FH UGM Press

[24] Noblett, M. G., Pollitt, M. M., & Presley, L. A. (2000). Recovering and Examining Computer Forensic Evidence. Forensic Science Communications

E-ISSN: 2988-3334
ISSN: 1907-3319
Vol. 20 No. 2 June 2025

request if it is domestic.[25]

While essential for law enforcement, digital forensics practices must adhere to ethical principles and privacy laws. Unauthorized or unauthorized collection of personal data can be a violation of the law. Therefore, digital forensics processes must be based on a warrant, and limitations on the scope of data analyzed, in accordance with the principles of proportionality and subsidiarity.[26]

In several cases in Indonesia, the success of digital forensics in exposing perpetrators of hate speech has proven effective. For example, in cases of hate speech against public figures or certain ethnic groups, the National Police cyber crime team used digital analysis to identify the perpetrators, even though the perpetrators used fake accounts. Techniques such as IP address tracking and recovery of deleted data are key to proving

Digital forensics plays a vital role in proving the elements of the perpetrator in the crime of hate speech in cyberspace. Through a scientific process that can be accounted for, digital forensics is able to reveal who exactly "everyone" is referred to in the criminal article. Its main function is not only in collecting evidence, but also in validating, authenticating, and presenting digital data as valid legal evidence. In this digital era, the success of law enforcement against hate speech is highly dependent on the sophistication and integrity of digital forensics.

4. Conclusion

Based on the results of the research and discussion that the author has conducted, the author concludes as follows: 1. In the context of Indonesian law, digital forensics has been legitimized as valid evidence through the recognition of electronic evidence in the Electronic Information and Transactions Law (UU ITE), as well as the Draft Criminal Procedure Code which accommodates electronic evidence as part of legal evidence. For this reason, the use of digital forensics must be carried out by competent experts and follow the established procedures so that the results can be legally accepted in court. 2. Digital forensics plays a vital role in proving the elements of the perpetrator in the crime of hate speech in cyberspace. Through a scientific process that can be accounted for, digital forensics is able to reveal who exactly "everyone" is referred to in the criminal article. Its main function is not only in collecting evidence, but also in validating, authenticating, and presenting digital data as valid legal evidence. In this digital era, the success of law enforcement against hate speech is highly dependent on the sophistication and integrity of digital forensics.

5. References

Journals:

Pan Mohamad Faiz, 2009,*Teori Keadilan John Rawls*, dalam Jurnal Konstitusi

[25]Wahyudi, A. (2021). Cyber, Privacy, and Law Enforcement. Jakarta: Kencana
[26]Solove, DJ (2007). The Digital Person: Technology and Privacy in the Information Age. NYU Press

Books:

A. Rahmah dan Amiruddin Pabbu. *Kapita Selekta Hukum Pidana*. Jakarta: Mitra Wacana Media, 2015.

Abdussalam, *Buku Pintar Forensik (Pembuktian Ilmiah)*, Jakarta: Restu Agung, 2006,

Abdussalam. *Buku Pintar Forensik (Pembuktian Ilmiah)*. Jakarta: Restu Agung, 2006.

Abu Hamid Al-Ghazali. *Ihya Ulumuddin*, Jilid 3. Beirut: Dar al-Kutub al-'Ilmiyyah, 2004.

Al-Qur'an, Surah Al-Baqarah [2]: 191. Lihat juga: Ibn Kathir. *Tafsir al-Qur'an al-Azhim*, Jilid 1. Kairo: Dar al-Fikr, 2005.

Al-Qur'an, Surah Al-Hujurat [49]: 11-12.

Al-Qur'an, Surah An-Nahl [16]: 125.

Amnesty International. *Toxic Twitter: A Toxic Place for Women*. London: Amnesty International, 2018.

Awaloedi Djamin. *Administasi Kepolisian Republik Indonesia: Kenyataan dan Harapan*. Bandung: POLRI, 1995.

Badan Pengembangan dan Pembinaan Bahasa. *Kamus Besar Bahasa Indonesia Edisi V*. Jakarta: Kemdikbud, 2016.

Brian Carrier. *File System Forensic Analysis*. Boston: Addison-Wesley, 2005.

Casey, Eoghan (ed). *Handbook of Digital Forensics and Investigation*. London: Academic Press, 2010.

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

Dikdik M. Arief Mansur dan Elisatris Gultom. *Cyber Law; Aspek Hukum Teknologi Informasi*. Jakarta: Refika Aditama, 2009.

Dwi Fahri Hidayatullah, Gunarto, dan Lathifah Hanim. "Police Role in Crime Investigation of Fencing Article 480 of the Criminal Code (Study in Polres Demak)." *Jurnal Daulat Hukum*, Volume 2 Issue 4, December 2019. http://jurnal.unissula.ac.id/index.php/RH/article/view/8288/3864

Evi Hartanti. *Tindak Pidana Korupsi: Edisi Kedua*. Jakarta: Sinar Grafika, 2012.

Frans Maramis. *Op. Cit.*, 2012.

Gagliardone, Iginio, et al. *Countering Online Hate Speech*. Paris: UNESCO Publishing, 2015.

H. Pudi Rahardi. *Hukum Kepolisian [Profesionalisme dan Reformasi Polri]*. Surabaya: Laksbang Mediatama, 2007.

HR. Bukhari dan Muslim. *Shahih al-Bukhari*, Kitab al-Adab, Hadis No. 6136.

Ibn Hisyam. *Sirah Nabawiyah*, Jilid 4. Beirut: Dar al-Kutub al-'Ilmiyyah, 1990.

Indonesia. *Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan Atas UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. Lembaran Negara RI Tahun 2016 No. 251.

Ismu Gunadi dan Jonadi Efendi. *Hukum Pidana*. Jakarta: Kencana, 2014.

J.H. Rapar. *Filsafat Politik Plato*. Jakarta: Rajawali Press, 2019.

Jasser Auda. *Maqasid al-Shariah as Philosophy of Islamic Law*. London: IIIT, 2008.

Jeremy Waldron. *The Harm in Hate Speech*. Cambridge: Harvard University Press, 2012.

Josua Sitompul. *Cyberspace Cybercrime Cyberlaw Tinjauan Aspek Hukum Pidana*. Jakarta: Tata Nusa, 2012.

Kejaksaan Republik Indonesia. *Modul Azas-Azas Hukum Pidana*. Jakarta: Pusat Pendidikan dan Pelatihan Kejaksaan Republik Indonesia, 2010.

Kruse, W. G., & Heiser, J. G. *Computer Forensics: Incident Response Essentials*. Addison-Wesley, 2002.

L.J van Apeldoorn. *Inleiding tot de Studie van het Nederlandse Recht*. Zwolle: W.E.J. Tjeenk Willink, 1995.

Lawrence M. Friedman. *System Hukum Dalam Perspektif Ilmu Sosial*. Bandung: Nusa Media, 2009.

M. Nur Faiz. "Studi Komparasi Investigasi Digital Forensik pada Tindak Pidana Kriminal." *Jurnal of INISTA*, Vol. 1 No. 1, 2018.

M. Quraish Shihab. *Tafsir Al-Misbah*, Jilid 12. Jakarta: Lentera Hati, 2002.

Majelis Ulama Indonesia. *Fatwa MUI No. 24 Tahun 2017 tentang Hukum dan Pedoman Bermuamalah Melalui Media Sosial*. Jakarta: MUI, 2017.

Marcus K. Rogers dan Kathryn C. Seigfried-Spellar. "Digital Forensics: An Integrated Approach for the Investigation of Cyber-Crime." Dalam *Handbook of Digital Forensics and Investigation*, ed. Eoghan Casey. London: Academic Press, 2010.

Marsudi Utoyo dkk. "Sengaja Dan Tidak Sengaja Dalam Hukum Pidana Indonesia." *Lex Librum: Jurnal Ilmu Hukum*, Vol. 7, No. 1, 2020.

Moeljatno. *Asas-Asas Hukum Pidana*. Jakarta: Rineka Cipta, 2002.

Momo Kelana. *Hukum Kepolisian*. Jakarta: PT Gramedia Widiasarana Indonesia, 1994.

Nelson, B., Phillips, A., & Steuart, C. *Guide to Computer Forensics and Investigations*. Cengage Learning, 2018.

NIST. *Guide to Integrating Forensic Techniques into Incident Response (Special Publication 800-86)*. National Institute of Standards and Technology, 2006.

Noblett, M. G., Pollitt, M. M., & Presley, L. A. "Recovering and Examining Computer Forensic Evidence." *Forensic Science Communications*, 2000.

Nugroho, R. *Hukum dan Teknologi Informasi: Suatu Pengantar*. Jakarta: Prenadamedia Group, 2020.

Radbruch & Dabin. *The Legal Philosophi*. New York: Harvard University Press, 1950.

Reith, M., Carr, C., & Gunsch, G. "An Examination of Digital Forensic Models." *International Journal of Digital Evidence*, 1(3), 2002.

Romli Atmasasmita. *Sistem Peradilan Pidana; Perspektif Eksistensialisme dan Abilisionisme*. Bandung: Bina Cipta, 1996.

E-ISSN: 2988-3334
ISSN: 1907-3319
Vol. 20 No. 2 June 2025

Ruan Keyun. "Digital Forensic Research: Current State-of-the-Art and the Road Ahead." *Journal of Digital Forensics, Security and Law*, Vol. 6, No. 4 (2011).

Sadjijono. *Fungsi Kepolisian Dalam Pelaksanaan Good Govenance*. Yogyakarta: Laksbang Pressindo, 2005.

Sadjijono. *Hukum Kepolisian, Perspektif Kedudukan Dan Hubungan Dalam Hukum Administrasi*. Yogyakarta: Laksbang Pressindo, 2006.

Satjipto Rahardjo. *Membangun Polisi Sipil Perspektif Hukum, Sosial & Kemasyarakatan*. Jakarta: Penerbit Buku Kompas, 2007.

Setara Institute. *Laporan Tahunan: Intoleransi dan Kebencian dalam Tahun Politik*. Jakarta: Setara Institute, 2019.

Soerjono Soekanto dan Sri Mahmudji. *Penelitian Hukum Normatif, Suatu Tinjauan Singkat*. Jakarta: Raja Grafindo Persada, 2003.

Solove, D. J. *The Digital Person: Technology and Privacy in the Information Age*. NYU Press, 2007.

Sumardjono, M. S. W. *Hukum Pidana dan Teknologi Informasi*. Yogyakarta: FH UGM Press, 2019.

Surat Edaran Kapolri NOMOR SE/06/X/2015 tentang (Hate Speech) Ujaran Kebencian.

Sutan Remy Syahdeini. *Kejahatan dan Tindak Pidana Komputer*. Jakarta: Pustaka Utama Grafiti, 2009.

United Nations. *International Covenant on Civil and Political Rights*. New York: UN, 1966.

United Nations. *Universal Declaration of Human Rights*. New York: UN General Assembly, 1948.

Utrecht. *Hukum Pidana I*. Surabaya: Pustaka Tindak Mas, 1986.

W. A. Mukti, S. U. Masruroh, dan D. Khairani. "Analisa dan Perbandingan Bukti Forensik Aplikasi Media Sosial Facebook dan Twitter pada Smartphone Android." *Jurnal Tek. Inform.*, Volume 10 Nomor 1, 2018.

W.J.S. Purwodarminto. *Kamus Umum Bahasa Indonesia*. Jakarta: Balai Pustaka, 1986.

Wahid Institute. *Laporan Kebebasan Beragama dan Berkeyakinan di Indonesia 2021*. Jakarta: Wahid Foundation, 2022.

Wahyudi, A. *Siber, Privasi, dan Penegakan Hukum*. Jakarta: Kencana, 2021.

Widodo. *Aspek Hukum Kejahatan Mayantara*. Yogyakarta: Aswindo, 2011.

Yusuf al-Qaradawi. *Fiqh al-'Aulaawiyaat*. Kairo: Maktabah Wahbah, 1996

Regulation:

Criminal Code (KUHP)

Law Number 8 of 1981 concerning the Criminal Procedure Code

The 1945 Constitution of the Republic of Indonesia