How to cite item: Hardinanto, Aris, Barda Nawawi Arief, and Joko Setiyono. "The Significance of Computer Forensics in Electronic Documents as Evidence in Criminal Law." *Jurnal Cakrawala Hukum.* 14 no. 2 (2023): 155-166. **DOI:** doi.org/10.26905/idjch.v14i2.10820

Jurnal Cakrawala Hukum

Volume 14 Issue 2, 2023
P-ISSN: 2356-4962, **E-ISSN**: 2598-6538

The Significance of Computer Forensics in Electronic Documents as Evidence in Criminal Law

Aris Hardinanto[1], Barda Nawawi Arief[2], and Joko Setiyono[3].

[1,2,3] Law Doctoral Program, Diponegoro University, Indonesia.

Article history:
Received 2023-05-05
Revised 2023-07-04
Accepted 2023-08-01

Keywords:
Computer Forensics; Illegal Access; Evidence.

DOI:
doi.org/10.26905/idjch.v14i2.10820.

Corresponding Author:
Name Aris Hardinanto
E-mail: aris@students.undip.ac.id

Abstract: Forensic science standards, no crime never leaves traces. Along with the emergence of cybercrime, a new type of evidence emerged as an expansion of conventional evidence in Indonesian criminal procedural law, namely electronic evidence as stated in the Law on Electronic Information or electronic documents whose authenticity can be guaranteed, but there is no further explanation. Further, what is the procedure for guaranteeing its authenticity? Based on this, not all electronic information or documents can be used as evidence. One branch of forensic science that is relevant to proving cybercrimes is computer forensics. The problem that arises is to what extent is the significance of computer forensics to guarantee electronic information or electronic documents as evidence. This article was based on legal research using a conceptual, statutory, and case approach. The result of this study is that computer forensics plays a significant role in the crime of illegal access to electronic devices because it is a tool in criminal procedural law that can be used to guarantee the authenticity of electronic information or electronic documents so that they can be accepted as evidence in court.

1. Introduction

Proof in criminal procedural law is different from proof in civil procedural law. In criminal procedural law, proving is material, which means actual proof to obtain a legal event in a crime. The Criminal Procedure Code (KUHAP) adopts a negative law-based evidence system in Article 183 of the Criminal Procedure Code. Article 184 of the Criminal Procedure Code contains various types of evidence.[1] Outside what the Criminal Procedure Code determines, it is not considered valid as evidence unless regulated in specific laws (lex specialis). Based on Article 184 of the Criminal Procedure Code, valid evidence in criminal procedural law includes witness statements, expert statements, letters, instructions, and statements of the accused.

In connection with the development of technology and information, especially the internet (cyber). Legal issues often encountered are related to the delivery of information, communication, or transactions electronically, especially regarding evidence and matters related to legal actions carried out through the electronic system with criminal acts. The consequence of the existence of

[1] Satria, Hariman. 2018. "Ke Arah Pergeseran Beban Pembuktian". *Integritas : Jurnal Antikorupsi* 3 (1):87-114. https://doi.org/10.32697/integritas.v3i1.142.

the internet world with the emergence of cybercrimes is to bring up new evidence, called electronic evidence.[2]

Several European countries have added electronic evidence to compensate for types of crime due to technological developments. For example, in England, electronic evidence is recognized as evidence under Section 5 of the Police and Criminal Evidence Act 1984.[3] Law no. 11 of 2008 concerning Information and Electronic Transactions (UU ITE) jo. Law No. 19 of 2016 concerning Amendments to Law No. 11 of 2008 concerning Information and Electronic Transactions (in the future referred to as the ITE Law) recognizes the position of electronic evidence as stated in Articles 5 and 6 of the ITE Law.

Based on Articles 5 and 6 of the ITE Law, electronic information or electronic documents and printouts are valid before the law if their authenticity can be accounted for. In the provisions of the Amendment to the ITE Law, as a consequence of the Constitutional Court's decision, amendments and reformulations of the provisions on electronic evidence are made as long as the investigator has preserved the electronic evidence. Based on the extension of electronic evidence to conventional evidence, the nature of electronic evidence is the conformity of a series of evidence from witnesses, experts, and letters that a crime has occurred.

The main problem is that there must be procedures for authenticating electronic information or documents in the ITE Law and the Amendment to the ITE Law. In addition, a procedure or standard procedure that applies nationally regarding this matter has yet to be promulgated. The most recent rationalization, along with the development of technology and information for the authentication of electronic evidence, is forensic computer science. Suppose it needs to be scientifically determined clearly regarding standard procedures in the national realm. In that case, it can result in legal uncertainty so that the goal of seeking the truth will not be achieved. Based on this, the problem formulation is the significant role of computer forensics in maintaining and guaranteeing the integrity of electronic evidence in criminal acts of illegal access to websites.

2. Method

Legal research is a process of finding legal rules, principles, and doctrines to answer the legal issues at hand.[4] In legal research, an approach method is needed as a reference. With this approach, researchers will get information from various aspects regarding the issue being tried to find an answer. The primary approach in this study used conceptual, statutory, and case approaches.

3. Computer Forensics and Electronic Evidence

Electronic information and/or electronic documents (or so-called electronic data) are easily altered and falsified.[5] As a result of the nature of such electronic evidence, electronic evidence cannot be immediately submitted to court as evidence. To anticipate this, the integrity of electronic

---

2 Trisha Soraya Assad," PENEGAKAN HUKUM PIDANA TERHADAP PENYEBARAN BERITA BOHONG (HOAX) DI MEDIA SOSIAL DIHUBUNGKAN DENGAN UNDANG-UNDANG NOMOR 19 TAHUN 2016 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK," *Prosiding Ilmu Hukum* Vol 5, No 2, (Agustus, 2019) http://dx.doi.org/10.29313/.v0i0.16325.

3 Chris Carr dan John Beaumont, *Law of Evidence*, (London: Blackstone Press Limited, 1996) 132.

4 Herman Suryokumoro, Ikaningtyas Ikaningtyas, "Perlindungan Terhadap Penduduk Sipil Pada Saat Terjadi Konflik Bersenjata Berdasarkan Hukum Humaniter Internasional dan Hukum Pertahanan Indonesia," *RechtIdee*, Vol. 15, No. 2, (Desember 2020) 207-244, https://doi.org/10.21107/ri.v15i2.8576.

5 Nyoman Serikat Putra Jaya, *Hukum dan Hukum Pidana di Bidang Ekonomi*, (Semarang: Badan Penerbit Universitas Diponegoro, 2012) 86.

data must be maintained. Based on the rules for maintaining the integrity of electronic data in the international world called Request for Comment No. 3227, electronic information has several criteria to be appropriate as evidence in court. These stages are: 1. Accepted: This must be under applicable legal provisions before going to court; 2. Authentic: This must be binding on the correct evidence for an incident; 3. Complete: This should describe the complete chronology, not of a specific event; 4. Reliable: There must be an explanation of how evidence was collected and handled to remove doubts about its authenticity and correctness; 5. Trusted: Must be easily trusted and understood by the assembly in court.

Based on these criteria, not all electronic information can be accepted as evidence. To maintain the criteria for electronic information, a standard procedure is required that is used by all levels of law enforcement officials, from the central government to the regions. This standard procedure is only owned by computer forensics. In other words, computer forensics determines electronic information and documents as court evidence. Disciplines related to physical evidence or objective evidence are forensic science. According to Eddy O.S. Hiariej, forensic science is a scientific discipline that uses basic science principles and techniques to analyze evidence to retrieve information to solve legal problems. Specifically for electronic evidence, the forensic science discipline used is computer forensics.[6]

Computer forensics is collecting and analyzing data from various digital resources, including digital systems, networks, communication lines (including physical and wireless), and storage media that are said to be suitable for submission in court hearings.[7] Another definition of *computer forensics* is computer investigation and analysis to determine potential legal evidence.[8] Computer forensics is also known as digital forensics.[9] Through computer forensics, investigators trace evidence of a crime by tracing back lost, hidden, and deleted computer files.[10] The nature of electronic evidence itself is easy to falsify and change.[11] So, checking electronic evidence requires adequate competence. Apart from computer forensics, it is also known as network forensics, a scientific discipline that searches for crime-related data in a computer network environment.[12]

The term for people who reveal digital evidence of crimes and help perpetrators to court is forensic computer experts or forensic computer technicians. Based on the results of forensic computer analysis, judges, public prosecutors, experts, and advocates are expected to know about information technology to conclude the relationship between a crime and the basis of electronic evidence.[13] This is because forensic computer experts will more or less speak technical information technology. Thus, legal science, forensic computer science, forensic computer experts, and

---

6 Eddy O.S. Hiariej, *Teori & Hukum Pembuktian*, (Jakarta: Erlangga, 2012) 75.

7 N. Aisyah, Putra, A., Safrizal, S., Valentino, V., Zikriah, Z., Prasetyo, B., Susanti, D., & Nurhayati, N. "Analisa Perkembangan Digital Forensik Dalam Penyidikan Cybercrime di Indonesia Secara Systematic Review." *Jurnal Esensi Infokom : Jurnal Esensi Sistem Informasi Dan Sistem Komputer*, 6(1), (2022): 22-27. https://doi.org/10.55886/infokom.v6i1.452.

8 Christa M. Miller, "A Survey of Prosecutors and Investigators Using Digital Evidence: A Starting Point," *Forensic Science International: Synergy* 6 (January 1, 2023): 100296, https://doi.org/10.1016/j.fsisyn.2022.100296.

9 N.A. Hassan, "Introduction: Understanding Digital Forensics." *In: Digital Forensics Basics. Apress, Berkeley, CA*. (2019). https://doi.org/10.1007/978-1-4842-3838-7_1.

10 Schafer, Burkhard, and Stephen Mason. "The Characteristics of Electronic Evidence." In *Electronic Evidence*, edited by Stephen Mason and Daniel Seng, 4th ed., 18–35. University of London Press, (2017). http://www.jstor.org/stable/j.ctv512x65.9.

11 V.D. Dudeja, *Cyber Crimes and Law, Crime in Cyber Space – Scams and Frauds Volume 1*, (New Delhi: Commonwealth, 2002) 95.

12 W. Yang, Johnstone, M.N., Wang, S., Karie, N.M., Sahri, N.M.b., Kang, J.J. (2022). "Network Forensics in the Era of Artificial Intelligence." In: M. Ahmed, Islam, S.R., Anwar, A., Moustafa, N., Pathan, AS.K. (eds) "Explainable Artificial Intelligence for Cyber Security." *Studies in Computational Intelligence*, vol 1025. Springer, Cham. https://doi.org/10.1007/978-3-030-96630-0_8.

13 Gary C. Kessler, *Judges Awareness, Understanding, and Application of Digital Evidence*, (Longfellow Blvd, Lakeland: Southeastern University, 2010) 2.

electronic information or documents analysis cannot be separated. Computer forensics can only work with law enforcement officials who can use these procedures. Law enforcers eligible to become computer forensic analysts are those who at least understand computer forensic procedures obtained from formal or informal education. Due to the nature of computer forensics as an information technology discipline, an understanding of basic information technology is necessary. Cybercrime is a crime using information technology media, so when a cybercrime occurs, a forensic computer analyst is ideally presented to conduct an investigation, considering that the human resources of Indonesian law enforcement officers are still low to conduct investigations and investigations into cybercrime.

Standard procedures play a critical role in computer forensics. Currently, law enforcement officers who have standard computer forensic procedures are the Indonesian National Police (Polri) and individual computer forensic experts, respectively. This standard procedure is binding on the institution because there is no government regulation or at least a generally binding "written rule" regarding this matter. An example of the standard procedure classification of the National Police is as follows: SOP 1 concerning Digital Forensic Examination Procedures; SOP 2 regarding Working Hours Commitment; SOP 3 concerning Reporting of Digital Forensic Examination Results; SOP 4 regarding Acceptance of Electronic Evidence; SOP 5 regarding Submission of Electronic Evidence; SOP 6 regarding Forensic Triage; SOP 7 regarding Direct Acquisition of Computers; SOP 8 Acquisition of hard drives, flash drives and memory cards; SOP 9 regarding Harddisk, Flashdisk and Memory Card Analysis; SOP 10 regarding Mobile and Simcard Acquisition; SOP 11 regarding Mobile and Simcard Analysis; SOP 12 concerning Audio Forensic Analysis.[14]

Computer forensic experts with certification in computer forensics have their procedures. The following examples of standard computer forensic procedures are procedures created by Eoghan Casey: Preparation, Survey, Documentation, Preservation, Examination and analysis, Reconstruction, and Reporting results.[15]

The stages in the standard procedure are intended so that the integrity of evidence in electronic devices is guaranteed from confiscation and analysis to presentation in court. The standard procedures of the National Police and forensic computer analyst Eoghan Casey can be simplified into three processes: acquisition, analysis, and preparation of reports to be presented in court. The acquisition phase includes confiscating evidence by law enforcement officers from where the crime occurred until analysis is carried out in a forensic computer laboratory. The next stage is to perform a forensic computer analysis. The analysis phase can be carried out using software in the form of paid or free computer forensic programs. The final stage is the presentation stage. Before the presentation stage, it is necessary to make an analysis and report on the electronic information contained in the device related to crime; after completion, the written report can be used as evidence in court, and the statement of a forensic computer analyst can be used as evidence for expert testimony.

Electronic evidence forms the judge's conviction; if there is no documentary evidence from the forensic computer analyst and the analyst's statement, the judge must understand electronic information in electronic data. Knowledge of information technology is required to understand it,

[14] M.N. Al Azhar, *Standart Operating Procedure (SOP),* (DFAT Puslabfor Mabes Polri, 2010) 1-12.
[15] Eoghan Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and The Internet*, (USA, Elsevier. Inc, 2011) 466.

so it is hazardous if the judge has a conviction without the support of a forensic computer analysis report and expert testimony, even though both are optional. This is a logical consequence, considering that computer forensic material is likely not given in lectures at law faculties. Based on this, computer forensics is essential in determining the authenticity of electronic information or documents appropriate for evidence in criminal acts related to electronic information and transactions.

Evidence is crucial in formal criminal law enforcement because evidence forms the judge's conviction in deciding cases to uphold justice. According to Article 184, paragraph (1) of the Criminal Procedure Code, legal evidence is witness statements, expert statements, letters, instructions, and statements of the accused. The evidence becomes valid when submitted in the judicial process in court. According to Eddy O.S. Hiariej, the development of evidentiary law is very influential for the cases being handled and the evidence owned, including technological developments.[16] The consequence is that when there is a crime using or through technological means such as the internet, new evidence emerges, referred to as digital evidence. Regarding electronic evidence as evidence in the judicial system in Indonesia, according to the Criminal Procedure Code, it is not included in the evidence received in court.

Electronic evidence is developing in common law countries, and its arrangements do not form new evidence but expand the scope of evidence included in the documentary evidence category, namely letters and instructions. In Indonesia, the recognition and use of electronic evidence has occurred in the murder case of a human rights activist, Munir. Even though it is not regulated in the Criminal Procedure Code, the panel of judges made a breakthrough by acknowledging the existence of electronic evidence as valid evidence. However, this breakthrough did not reach the jurisdiction of the Supreme Court. Instead, the consideration of the panel of judges in the case was annulled. The considerations of the South Jakarta District Court in the decision are as follows:

Considering that although the laws and regulations on general criminal acts or the Criminal Code and the procedural law (KUHAP) have not yet regulated the results of science and technology from electronic products, computer and digital as well as other new science and technology products that have not yet had a place, the assembly thinks that it must already be accepted as evidence. Because if it is not accepted, this will become an obstacle in proving a crime that can harm the process, interests, and law enforcement in Indonesia. Because of this, the assembly believes that the cloning of a computer product, as evidenced by letter No. R-451/VII/2004, undated July 2004, is confidential regarding the recommendation of the personnel of the internal security team (aviation security) submitted by the prosecutor and can be accepted at this trial as evidence in addition to the evidence as stipulated in Article 184 of the Criminal Procedure Code.[17]

Based on the considerations of the panel of judges, electronic evidence in the form of duplicated computer hard drives can be accepted as valid evidence in addition to those specified in a limited manner in Article 184 of the Criminal Procedure Code. Electronic evidence is any data that is stored or transmitted using a computer.[18] Examples of electronic evidence are electronic mail, spreadsheets, software source code, data in the form of images, web browser bookmarks, and

---

16 Eddy O.S. Hiariej, *Teori & Hukum Pembuktian*, (Jakarta: Erlangga, 2012) 13.

17 Putusan Pengadilan Negeri Jakarta Selatan No. 1488/Pid.B/2008/PN.Jkt.Sel atas nama H. Muchdi Purwopranjono.

18 Burkhard Schafer, and Stephen Mason. "The Characteristics of Electronic Evidence." In *Electronic Evidence*, edited by Stephen Mason and Daniel Seng, 4th ed., 18–35. University of London Press, (2017). http://www.jstor.org/stable/j.ctv512x65.9.

cookies. [19] Alan M. Gathan argues that the existence of electronic evidence as evidence is urgently needed at this time because all public actions cannot be separated from computers, so electronic evidence needs to be recognized.[20] Some literature calls electronic evidence the terms electronic evidence and digital evidence. Indeed, some argue that electronic evidence and digital evidence are something different. According to Muhammad Nuh Al Azhar, electronic evidence is electronic evidence in which digital evidence is stored.[21] In other words, electronic evidence is hardware or electronic media, while digital evidence is information and/or documents stored in the electronic hardware.[22] This classification between electronic and digital evidence creates confusion because, in Indonesia, there is no classification of evidence based on positive law. In short, evidence can be interpreted as goods related to a crime. This definition is not found in the Criminal Procedure Code but can be found in the practice and doctrine of legal scholars.

The dichotomy between the words "electronic" and "digital" also creates confusion because the equivalent word in Indonesian and the prevalence of legal practice for the two words is electronic. In addition, Muhammad Nuh Al Azhar did not distinguish between the definitions of "electronic evidence" and "digital evidence" as evidence, so when he translated the two common words in cybercrime into Indonesian, it biased the understanding of electronic evidence itself.

Based on this, it can be a term common in Indonesian positive law, namely electronic evidence as a translation of digital evidence with the meaning of electronic information or electronic documents stored in computer devices or electronic system devices to form judge beliefs in deciding cases. Law of the Republic of Indonesia No. 11 of 2008 concerning Information and Electronic Transactions (UU ITE) provides space for the existence of electronic evidence, namely Articles 5 and 6 of the ITE Law, electronic information or electronic documents and printouts are legal in the eyes of the law if their authenticity can be accounted for. Article 5, paragraph 2 of the ITE Law needs to be clarified because it only explains that electronic evidence is an extension of legal evidence in Indonesian procedural law. This gives rise to various interpretations because the ITE Law does not explain the evidence in the Criminal Procedure Code, which has undergone an expansion; another consequence is that electronic evidence cannot stand alone because it is only an extension of the evidence already in the Criminal Procedure Code.

Based on Article 5, paragraph 1, if electronic evidence is printed, it is valid in the eyes of the law. The printout of this electronic evidence can be equated with documentary evidence.[23] In this case, Eddy O.S. Hiariej argues that as a consequence of electronic evidence, such as, for example, video, is objective evidence or physical evidence, this evidence must be strengthened by other evidence, including testimony.[24] Based on this opinion, electronic evidence can be an extension

---

[19] S. Saharan, Yadav, B. "Digital and Cyber Forensics: A Contemporary Evolution in Forensic Sciences". In: Singh, J., Sharma, N.R. (eds) "Crime Scene Management within Forensic Science." *Springer, Singapore*. (2022). https://doi.org/10.1007/978-981-16-6683-4_11.

[20] H.P. Panggabean, *Hukum Pembuktian: Teori-Praktik dan Yurisprudensi di Indonesia,* (Bandung: Alumni, 2012) 174-180.

[21] Ben Martini Darren Quick, Kim-Kwang Raymond Choo, "Forensic Collection of Cloud Storage Data: Does the Act of Collection Result in Changes to the Data or its Metadata?" *Cloud Storage Forensics, Syngress*, (2014): 153-174, ISBN 9780124199705, https://doi.org/10.1016/B978-0-12-419970-5.00007-7.

[22] R. S. George Weir, and Stephen Mason. "The Sources of Electronic Evidence." In *Electronic Evidence*, edited by Stephen Mason and Daniel Seng, 4th ed., University of London Press, (2017): 1–17. http://www.jstor.org/stable/j.ctv512x65.8.

[23] Badan Pembinaan Hukum Nasional, *Pengkajian Hukum Tentang Masalah Kekuatan Hukum Alat Bukti Elektronik*, (Jakarta: Badan Pembinaan Hukum Nasional, 1998) 25.

[24] Eddy O.S. Hiariej, *Teori & Hukum Pembuktian*, (Jakarta: Erlangga, 2012) 74.

of evidence as long as it is supported by other evidence as contained in the Criminal Procedure Code. One that strengthens physical evidence or objective evidence as evidence is the existence of expert testimony that sheds light on legal events.[25] This means that electronic evidence can be acknowledged for its existence in court when expert testimony explains electronic information or documents. Based on the possibility of extending electronic evidence to conventional evidence, the nature of electronic evidence is the conformity of a series of evidence from witnesses, experts, and letters that a crime has occurred. Based on this, electronic evidence can be categorized as guided evidence.[26]

Clue means an act, event, or circumstance which, because of its conformity, indicates that a crime has occurred and the culprit. The use of computer forensics can be known, at least in cases related to criminal acts of illegal access to websites. To compare the use of computer forensics in the favorable law regime in Indonesia, this article uses two cases that have become national issues, namely cases before and after the enactment of the ITE Law. A case comparison is intended to determine how law enforcement officials guarantee integrity and secure electronic evidence in different favorable law regimes.

4. Use of Computer Forensics in Cases of Illegal Access Crimes Before and After the Promulgation of the ITE Law

Cases of illegal access to websites before the promulgation of the ITE Law were illegal access to the website and servers of the General Election Commission (KPU) conducted by Dani Firmansyah alias Xnuxer in 2004, and cases after the promulgation of the ITE Law were cases of illegal access to the Polri website by Andi Kurniawan alias Fandiekun in 2011. The selection of the two cases took into account that both cases were illegal access cases which received public attention because they involved state institutions. The perpetrators are people with more knowledge in the field of information security. This is under the nature of illegal access as a new type of crime that existed after the internet was discovered and can only be carried out by people with more knowledge in the field of information technology.

In the case of Dani Firmansyah, evidence of a crime in the form of electronic information was examined by the Australian Federal Police, in this case, Michael Buck Wheeler, because the National Police did not yet have a forensic computer laboratory. The results of the report are outlined in the form of a Forensic Computing Report on the Analysis of Electronic Media[27] Originating from the confiscation of electronic devices: Hard drive Maxtor 20GB serial number 661206052773 entitled "HD HP Vetra 1"; Hard drive Maxtor 20GB serial number 66120606143 titled "HD HP Vetra 2"; Seagate 10.2GB IDE hard drive serial number 7EG1RMFC titled "HD Nokia Check Point"; Maxtor 40GB IDE hard drive serial number F1E4H1DE titled "KPU Harddisk"; Harddisk Quantum 20GB IDE SN 6163024130776 titled "HD Color Warnet".

---

[25] T. Ward, "Explaining and trusting expert evidence: What is a sufficiently reliable scientific basis?" *The International Journal of Evidence & Proof*, 24(3), (2020): 233–254. https://doi.org/10.1177/1365712720927622.

[26] S. Tosza, "All evidence is equal, but electronic evidence is more equal than any other: The relationship between the European Investigation Order and the European Production Order." *New Journal of European Criminal Law*, 11(2), (2020): 161–183. https://doi.org/10.1177/2032284420919802.

[27] Berkas Perkara No. 1322/Pid.b/2004/PN.JKT.PST atas nama Dani Firmansyah.

The results of the forensic computer analysis of evidence in hard disks are as follows: Partition 2 is installed with Windows Server 2003 Operating System. This operating system has a data structure called the "registry," an operating environment database. When an operating system is installed, it will ask the user for certain things, including their name, organization name, operating system key, and time zone setting. The data is stored in the Registry. For partition 1 are as follows: Registered user: "XNUXER"; Registered organization: Operating system: "Microsoft Windows Server 2003"; Install Date/Time: "05/03/04 09:04:54PM"; Time Zone: "SE-A-s-i-a—S-t-a-n-d-a-r—T-i-m-e." Microsoft Windows Server 2003 allows the creation of different profiles to structure users' environments and applications. The profiles of the users in Partition 2 are "_vmware_user_"; "Administrator"; "Guests"; "Devs"; "IUSER_XNUXER"; "IWAM_XNUXER"; ""Support_388945a0".

Appendix AO1 refers to the identified name "mixer" with the following command: Cp pf.conf pf.conf.number, The cp command copies the first argument in the string to the second one. In this case, rename the file "pf.conf" and the new file "pc.conf.xnuxer". The contents of the file are irrelevant to the scope of the analysis. Located in the path "\var\log\" Exhibit 4, this file maintains authentication logs of server operations on the local machine. Also located in the logs are the following sessions, which show that the user "xnuxer" connected to the machine identified as Exhibit 4 (Cafe) and the IP address 202.158.10.117 on port 57997 on April 20 at 14:05:01. Several different connections have been recorded using this username. Stored in Appendix B011, located on the second disk partition identified as Exhibit 1_1, there are fragments of the word that. Also available on the website "tnp.kpu.go. id/Tabulation/default.asp: suspected. Located on the second disk partition identified as Exhibit 1_1 is the installed application "Opera" version 7. This application is a multi-featured web browsing application that also contains email, chat, and contact logging capabilities.

The Opera application was extracted, and a screen capture was taken to show the available contacts and email showing the user "user" and the name "Dani Firmansyah." "Vlink.dat": This file contains the history of visited links with the appropriate date and time. Files located at "\Documents and Settings\Administrator\Apptication\Data\Opera\Opera?\profile\vlink4.dat" were analyzed and found to contain data relevant to investigators. It includes on page 70 the following string relating to the website "tnp.kpu.go.id/Tabulasi/default.asp" and an attempt to write the string "Exnuxer found bug XSS on KPU" Analysis of the Global.dat file located in "\Documents and Settings\Administrator\Application\Data\Opera\Opera7\profile\global.dat" reveals that username "Xnuxer" has used the browser for various activities. In addition, the transaction analysis in this file provides a comprehensive view of the types of activity performed using the browser, including email, based on web and site preferences.

The various files are located in the disk's first partition, identified as Exhibit 1_1; there is a file called "XNUXER-16-04-2004.ISO" in the "C/DATA" directory. An ISO image is an image of a CDROM that has been saved in a format that conforms to the ISO9660 format. Based on the results of an analysis report from the Australian Federal Police's computer forensic laboratory on the hard drive, the National Police have clues that the name "Xnuxer" is another name for Dani Firmansyah as the perpetrator of illegal access to the KPU.

The case after the promulgation of the ITE Law that has become in the public spotlight is the case of changes in appearance and data from the Polri website in 2011 by Andi Kurniawan alias Fandiekun. One of the pieces of evidence used is electronic evidence, in which the electronic

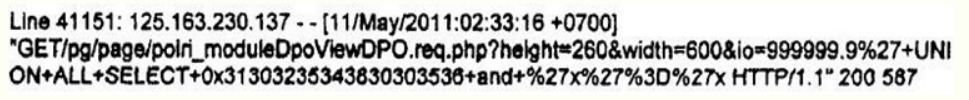
evidence is analyzed based on the data contained in the evidence: Polri website server, namely BB-94/V/2011/Cyber Seagate SCSI hard drive with a capacity of 73 GB SN.3KTSK17R and BB-94/V/2011/Cyber HDD Seagate SCSI 73GB capacity SN.3KT5KM72. Black and white personal computer with western digital hard drive WD 5001AALS caviar black capacity 500 GB, S/N: WMATV5056309.

Furthermore, the results of the analysis of the evidence are as follows: Based on the evidence, BB-94/V/2011/Cyber Seagate SCSI hard drive with a capacity of 73 GB SN.3KTSK17R and BB-94/V/2011/Cyber Seagate SCSI hard drive with a capacity of 73 GB SN. 3KT5KM72 obtained the following analysis results: On 11 May 2011 at 02:28:51 +0700 "GET/HTTP/1.1" 200 33987 from IP 125.163.230.137. Access recorded as many as 16538 hits. On 11 May 2011 at 02:41:36 +0700 "GET/berita/11631 HTTP/1.1" 200 17928 and IP 12.165.142.1 16. Access recorded 30 hits. On 12 Mar 2011 at 13:27:34 +0700 "GET/theme/polri_cssHeader.css HTTP/1.1" 200 8112 from IP 125.160.195.224. Access recorded as many as 461 hits. On May 3, 2011 at 15:05:32 +0700 "GET/file/sd.php?y=/www/wwwpolri/&x=mysql&sqlhost=192.168.10.99&sqluserpoli&sqlpass=3brata&sqlport=&db=mysql&tableuserHTTP/1.1" 200 11165 from IP 114.79.49.92. Access recorded as many as three hits.

On 1 May 2011 at 00:21:15 +0700 "PUT / lndonesia.htm HTTP/1.1" 405 314 from IP 118.136.45.140. Access recorded as much as one hits. Based on a black and white personal computer with a western digital WD 5001AALS caviar black hard drive with a capacity of 500 GB, S/N: WMATV5056309, the following analysis results were obtained: The Havij-Advance SQL Injection Tools program version 1.14 free is installed on the western digital hard drive WD5001AALS caviar black Sn. WMATV5956309, with a capacity of 500 GB, is a program that is used to scan a website to find and detect security holes in that website. The program nmap5.00-3_i386.deb, nmap (network mapper) is used for network exploration or security audits.

Andi Kurniawan's data is in photos contained in my photo folder. Based on the results of forensic computer analysis of the evidence, information was found that Andi Kurniawan used the Havij and NMAP programs to enter the Polri website by first scanning using the NMAP program. Then, after obtaining gaps in information on the Polri website, Andi Kurniawan used the Havij program to break into—the police website. However, there is an oddity in Andi Kurniawan's case because the log file of searches on the internet from Telkom that was used as evidence was a log file dated May 11, 2011, not a log file dated May 16, 2011, while the incident of changing website content through illegal access was carried out on May 16, 2011.

The results of forensic computer analysis of laptops and hard drives owned by the National Police only provide information that Andi Kurniawan installed software in the form of a computer program on his laptop to find loopholes and enter the Polri website using IP 125.163.230.137 on May 11, 2011, and ending on the same date without incident. They are Changing website content unlawfully (website defacement). This is corroborated by log information containing on May 11, 2011, Andi Kurniawan only conducted information gathering and database enumeration (collection of detailed and in-depth information) with the command characteristics "UNION+ALL+SELECT" and "SELECT+FROM." Details are as follows:



Thus, for the crime of illegal access to the website and changes to website content on May 16, 2011, even though they had used computer forensics, the National Police did not have sufficient evidence to charge Andi Kurniawan because there was no connection between changes to the appearance of the website and computer forensics reports—furthermore, the actions committed by Andi Kurniawan. In the cases of Dani Firmansyah and Andi Kurniawan, all evidence was subject to forensic computer analysis by an expert or computer forensic analyst to maintain the integrity of the data contained in the seized evidence, in this case, the hard drive. This is aimed at keeping the electronic information or documents contained therein unchanged so that their authenticity can be guaranteed to become a standard for electronic evidence.[28] Computer forensics can be a guarantor for the authenticity of electronic evidence in criminal procedural law in the future.[29] In both the cases of Dani Firmansyah and Andi Kurniawan, computer forensics was used to dig up electronic information or electronic documents related to the crime of illegal access to websites to be used as evidence.

Computer forensics can anticipate recognizing electronic evidence in the Draft Criminal Procedure Code as a future formal criminal law. Article 175 of the Criminal Procedure Code details legal evidence as follows: evidence, letters, electronic evidence, expert testimony, testimony of a witness, statement of the accused, And—judge's observation. Article 175 letter c of the Draft Criminal Procedure Code (RUU KUHAP) acknowledges the existence of electronic evidence as valid evidence. The elucidation of Article 175 letter c provides the meaning of electronic evidence as follows: information that is spoken, sent, received, or stored electronically with optical devices or something similar to that, including any recorded data or information that can be seen, read, or heard which can be issued with or without the help of some means, whether written on paper, any physical object other than paper or recorded electronically in the form of writing, drawings, maps, plans, photographs, letters, signs, numbers or perforations that have meaning.

Electronic information or documents may only guarantee their integrity with a forensic computer. Based on this, computer forensics is the latest criminal legal aid (procedure) because it tests the reliability of electronic information/electronic documents and crimes using technology and information facilities. The significant location of computer forensics in the crime of illegal access to websites is to maintain the integrity of electronic evidence in the form of electronic information or electronic documents as stipulated in the ITE Law so that it can be used as valid evidence in court.

5. Conclusion

Computer forensics by an expert as an aid in criminal procedural law has been used both before and after the promulgation of the ITE Law. Computer forensics in a crime related to electronic

[28] A.F. Moussa, "Electronic evidence and its authenticity in forensic evidence." *Egypt J Forensic Sci* 11, 20 (2021). https://doi.org/10.1186/s41935-021-00234-6.

[29] Guan Zheng Hong Wu, "Electronic evidence in the blockchain era: New rules on authenticity and integrity," *Computer Law & Security Review*, Volume 36, (2020), 105401, ISSN 0267-3649, https://doi.org/10.1016/j.clsr.2020.105401.

devices has a significant role in maintaining the integrity of electronic information or documents contained in electronic devices to be used as evidence in court. Computer forensics can only be performed by a forensic computer expert/analyst. With computer forensic expertise, it is possible to know the integrity of electronic data in the form of information or electronic documents contained in electronic devices.

References

Ahmed, M., Islam, S.R., Anwar, A., Moustafa, N., Pathan, AS.K. (eds) "Explainable Artificial Intelligence for Cyber Security." *Studies in Computational Intelligence*, vol 1025. Springer, Cham. (2022). https://doi.org/10.1007/978-3-030-96630-0_8.

Aisyah, N., Putra, A., Safrizal, S., Valentino, V., Zikriah, Z., Prasetyo, B., Susanti, D., & Nurhayati, N. "Analisa Perkembangan Digital Forensik Dalam Penyidikan Cybercrime di Indonesia Secara Systematic Review." *Jurnal Esensi Infokom: Jurnal Esensi Sistem Informasi Dan Sistem Komputer*, 6(1), (2022): 22-27. https://doi.org/10.55886/infokom.v6i1.452.

Al Azhar, M.N., *Standart Operating Procedure (SOP)*, DFAT Puslabfor Mabes Polri, 2010.

Badan Pembinaan Hukum Nasional, *Pengkajian Hukum Tentang Masalah Kekuatan Hukum Alat Bukti Elektronik*, Jakarta: Badan Pembinaan Hukum Nasional, 1998.

Berkas Perkara No. 1322/Pid.b/2004/PN.JKT.PST atas nama Dani Firmansyah.

Carr, Chris dan John Beaumont, *Law of Evidence*, London: Blackstone Press Limited, 1996.

Casey, Eoghan, *Digital Evidence and Computer Crime: Forensic Science, Computers and The Internet*, USA, Elsevier. Inc, 2011.

Darren Quick, Ben Martini, Kim-Kwang Raymond Choo, "Forensic Collection of Cloud Storage Data: Does the Act of Collection Result in Changes to the Data or its Metadata?" *Cloud Storage Forensics, Syngress*, (2014): 153-174, ISBN 9780124199705, https://doi.org/10.1016/B978-0-12-419970-5.00007-7.

Dudeja, V.D., *Cyber Crimes, and Law, Crime in Cyber Space – Scams And Frauds Volume 1*, New Delhi: Commonwealth, 2002.

Hassan, N.A "Introduction: Understanding Digital Forensics." *In: Digital Forensics Basics. Apress, Berkeley, CA*. (2019). https://doi.org/10.1007/978-1-4842-3838-7_1.

Hiariej, Eddy O.S., *Teori & Hukum Pembuktian*, Jakarta: Erlangga, 2012.

Hong Wu, Guan Zheng, "Electronic evidence in the blockchain era: New rules on authenticity and integrity," *Computer Law & Security Review*, Volume 36, (2020), 105401, ISSN 0267-3649, https://doi.org/10.1016/j.clsr.2020.105401.

Kessler, Gary C., *Judges Awareness, Understanding, and Application of Digital Evidence*, (Longfellow Blvd, Lakeland: Southeastern University, 2010.

Laporan Komputer Forensik Perkara No. 1322/Pid.b/2004/PN.JKT.PST atas nama Dani Firmansyah.

Laporan Komputer Forensik Perkara No. 97/Pid.Sus/2011/PN.SLMN atas nama Andi Kurniawan alias Fandiekun.

Miller, Christa M., "A Survey of Prosecutors and Investigators Using Digital Evidence: A Starting Point," *Forensic Science International: Synergy* 6 (January 1, 2023): 100296, https://doi.org/10.1016/j.fsisyn.2022.100296.

Moussa, A.F. "Electronic evidence and its authenticity in forensic evidence." *Egypt J Forensic Sci* 11, 20 (2021). https://doi.org/10.1186/s41935-021-00234-6.

Panggabean, H.P., *Hukum Pembuktian: Teori-Praktik dan Yurisprudensi di Indonesia,* Bandung: Alumni, 2012.

Putra Jaya, Nyoman Serikat, *Hukum dan Hukum Pidana di Bidang Ekonomi*, Semarang: Badan Penerbit Universitas Diponegoro, 2012.

Putusan Pengadilan Negeri Jakarta Selatan No. 1488/Pid.B/2008/PN.Jkt.Sel atas nama H. Muchdi Purwopranjono.

Satria, Hariman. "Ke Arah Pergeseran Beban Pembuktian". *Integritas: Jurnal Antikorupsi* 3 (1) (2018): 87-114. https://doi.org/10.32697/integritas.v3i1.142.

Schafer, Burkhard, and Stephen Mason. "The Characteristics of Electronic Evidence." In *Electronic Evidence*, edited by Stephen Mason and Daniel Seng, 4th ed., 18–35. University of London Press, (2017). http://www.jstor.org/stable/j.ctv512x65.9.

Singh, J., Sharma, N.R. (eds) "Crime Scene Management within Forensic Science." *Springer, Singapore*. (2022). https://doi.org/10.1007/978-981-16-6683-4_11.

Suryokumoro, Herman, Ikaningtyas Ikaningtyas, "Perlindungan Terhadap Penduduk Sipil Pada Saat Terjadi Konflik Bersenjata Berdasarkan Hukum Humaniter Internasional dan Hukum Pertahanan Indonesia," *RechtIdee*, Vol. 15, No. 2, (Desember 2020) 207-244, https://doi.org/10.21107/ri.v15i2.8576.

Tosza, S. All evidence is equal, but electronic evidence is more equal than any other: The relationship between the European Investigation Order and the European Production Order. *New Journal of European Criminal Law*, 11(2), (2020): 161–183. https://doi.org/10.1177/2032284420919802.

Trisha Soraya Assad," PENEGAKAN HUKUM PIDANA TERHADAP PENYEBARAN BERITA BOHONG (HOAX) DI MEDIA SOSIAL DIHUBUNGKAN DENGAN UNDANG-UNDANG NOMOR 19 TAHUN 2016 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK," *Prosiding Ilmu Hukum* Vol 5, No 2, (Agustus, 2019) http://dx.doi.org/10.29313/.v0i0.16325.

Ward, T. Explaining and trusting expert evidence: What is a 'sufficiently reliable scientific basis'? *The International Journal of Evidence & Proof*, 24(3), (2020): 233–254. https://doi.org/10.1177/1365712720927622.

Weir, George R. S., and Stephen Mason. "The Sources of Electronic Evidence." In *Electronic Evidence*, edited by Stephen Mason and Daniel Seng, 4th ed., University of London Press, (2017): 1–17. http://www.jstor.org/stable/j.ctv512x65.8.