ENSURING THE ADMISSIBILITY AND CREDIBILITY OF ELECTRONIC EVIDENCE IN INDONESIAN CRIMINAL PROCEEDINGS

*Salmah**

I. PREFACE

Since the 2000s, Indonesia has experienced an increase in the use of digital technology, where more and more individuals are using computers and mobile phones in their daily lives. The development of digital technology is not only limited to the physical form but also in the scope of its use. Along with these developments, the types and methods of crimes that use digital technology are also increasing.

One type and source of electronic evidence is CCTV footage or Closed-Circuit Television. CCTV recording is a medium that can be used to contain recordings of any information that can be seen, read or heard with the help of CCTV recording facilities. CCTV footage is used as evidence, and the system uses video cameras to display and record images at a certain time and place where this device is installed, which means using a closed signal, unlike an ordinary television, which uses a broadcast signal.[1]

Prior to 2001, CCTV had been used as a means of security or monitoring but had not been used as evidence in trials. However, after Law Number 20 of 2001 junto Law Number 31 of 1999 concerning Eradication of Criminal Acts of Corruption, which was later strengthened by Law Number 11 of 2008 concerning Information and Electronic Transactions, CCTV, has become one of the electronic evidence tools that is very helpful in proving the occurrence of criminal acts.

When a suspect and other related party commit an act that is a crime or is part of a criminal process, the investigation is carried out only based on evidence in the form of objects/goods used to commit the crime, the testimony of the related parties and, when applicable, the suspects' admission of guilt. In corruption criminal acts, evidence such as instructions between the suspect and related parties, proof of wrongdoing, electronic objects/goods used to commit crimes and documentary evidence are usually very difficult to obtain. However, if the crime event, such as meetings between the suspect and other parties, was caught on CCTV, then the results of the CCTV footage will become electronic evidence that strengthens the allegation that there is indeed a special relationship between the suspect and other related parties and that they were involved in the corruption act.

II. ELECTRONIC EVIDENCE IN INDONESIA

In the history of legislation in Indonesia, electronic evidence was clearly stated for the first time in Law Number 20 of 2001, which was an amendment to Law Number 31 of 1999 concerning the Eradication of Criminal Acts of Corruption. Valid evidence in the form of a directive in accordance with Article 184 of the Criminal Procedure Code was expanded in regard to the acquisition source to include other evidence in the form of information that is spoken, sent, received or stored electronically with an optical device or similar; or information that can be seen, read and/or heard, that can be issued with or without the help of a means, whether written on paper, any physical object other than paper, or recorded electronically.[2] These were emphasized again in Article 5 of Law Number 11 of 2008 concerning Electronic Information and Transactions,

* Middle Investigator, Investigation Directorate, Corruption Eradication Commission Indonesia.

[1] Surjono, Herman Dwi, *Pengembangan Pendidikan TI di Era Global*., p. 18.

[2] Further Explanation of Law Number 20 of 2001, which was an amendment to Law Number 31 of 1999 concerning the Eradication of Criminal Acts of Corruption.

which states that electronic information, electronic documents and printouts are recognized as legal evidence.

The crime of corruption and money-laundering is one of the economic crimes that is difficult to prove without special handling. Thus, electronic evidence, as one of the valid forms of evidence admissible in court, can increase the judge's confidence in deciding cases.

To ensure the admissibility and credibility of electronic evidence, it was critical for Digital Evidence First Responders or investigators to have core skills, such as how to search and identify digital evidence, choosing the right tools needed, acquiring the digital evidence by following the right procedures and regulations, and how to ensure and maintain and preserve the digital evidence.

A. Electronic Evidence Sources

Muhammad Neil El Himam said that digital evidence can be sourced from[3]:

a) Computer, which consists of e-mail, digital images, electronic documents, spreadsheets, chat logs, illegal software and other copyright materials,
b) Hard disks, which consist of files, both active, deleted or in the form of fragments, file metadata, slack files, swap files, system information, which consists of registry, logs and configuration data,
c) Other sources, which consist of i) cellular telephone, namely in the form of SMS, numbers called, incoming calls, credit/debit card numbers, e-mail addresses, call forwarding numbers; ii) PDAs / smart phones, which consist of everything listed in the cell phone plus contacts, eta, pictures, passwords, documents and others
d) Video games,
e) GPS device containing routes,
f) A digital camera, which contains photos, videos and other information that may be stored on a memory card (SD, CF, etc.).

Identifying the source of electronic evidence is important because the way of handling each electronic device varied depending on its operating system and device structures. Sources of electronic evidence also determine the tools that must be used in accessing digital data, acquiring and preserving it.

B. Securing Electronic Evidence

To secure the electronic evidence in the investigation stage, an investigator needs to gain acquisition/ collection, confiscation permit/approval, before doing search, storage, filing, and finally delivering those evidence to the Prosecutor with identification/category of evidence and minutes related to the examination/ analysis of the electronic evidence. After the electronic evidence in the prosecution stage, the prosecutor must preserve the evidence given and presented those evidence in court. Lastly is the importance of an expert's statement which includes opinions regarding the originality of the evidence, analysis and reports on the electronic evidence. To secure the electronic evidence from the time it is first acquired until presented in court, the electronic evidence chain of custody had to be clear and in accordance with existing Standard Operating Procedures and regulations.

C. Sample Case

During the trial of a bribery case with the defendant DYL (Member of the Indonesian House of Representatives) in 2016, the prosecutor showed CCTV footage showing the defendants meeting at the Bebek Tepi Sawah Restaurant, Pondok Indah Mall, in Jakarta on 18 October 2015. The purpose of the meeting, based on the testimony of the other defendant, RB, was to discuss the project fee. However, DYL denied that statement and insisted that the meeting was coincidental and only small talk happened. DYL also stated that they had only met for 15 minutes, which was then refuted by the duration of the recorded CCTV that showed the meeting last more than 30 minutes. In this case, the CCTV footage shows the indisputable fact that a meeting had taken place between the defendants and DYL's statement as a defendant is doubtful.

To ensure the accuracy and authenticity of the video, the CCTV footage confiscated by investigators was also sent to an expert to be analysed, to compare the faces and body shapes in the footage with the suspects

[3] Muhammad Neil el Himam, Pemeriksaan Alat Bukti Digital dalam Proses Pembuktian, paper presented at Digital Forensik seminar, Semarang, 24 October 2012.

and to ensure that the footage was not tampered with.

III. CHALLENGES

Regarding the legal power of the evidence, electronic evidence has weaknesses because it is virtual, which is very vulnerable or easy to change, falsify, intercept, remove or even engineer as if was made by a specific individual but actually made by someone else, or as if it was made by the authorities, and because it can be sent to various parts of the world within seconds.

Electronic information/data as digital evidence or direct evidence has not been fully accommodated in the procedural law system in Indonesia, and currently there is no standard procedure for searching until analysing electronic evidence that is generally applicable in Indonesia because, in practice, the procedure for searching, procuring and analysing electronic evidence is left to each law enforcement institution that handles the electronic evidence. This leads to different procedures carried out by each institution and makes it difficult for judges to see whether electronic evidence has been searched, procured and examined with the right procedure or not to guarantee its evidentiary value.

For example, CCTV is a tool that is commonly found in various places as a security tool. The footage can be used in many ways, such as digital evidence, to track down criminal suspects or suspicious people or just to check the surrounding area. The other use of CCTV largely depends on the technology level of each country. Regarding CCTV recordings as digital evidence, there are some investigators who only confiscate data taken from CCTV recording storage and store it in other storage areas, but there are also those who confiscate the original CCTV memory storage. The difference in the confiscated goods causes differences in the handling and analysis.

The absence of this setting also causes vulnerability, such as violation of citizens' right to privacy. There is no guarantee for sufficient legal protection on existing private data in the device that had no relation to the suspected crimes that is also stored on a PC, laptop, or cell phone of the owner when the device was confiscated and examined by investigators. On the other hand, the owner of the electronic device can also refuse to hand over his possessions to be confiscated by investigators in the related case.

Another problem that arises is when the required electronic data is stored or was in a cyber-network in the server under the control of a service provider or foreign company domiciled outside the jurisdiction of Indonesia. Fortunately, this problem can be avoided even though Indonesia is not a signatory to the Budapest Convention on cybercrime., Article 32, item b, states, "A Party may, without the authorization of another Party: can access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system".

The digital data acquisition itself can also cause problems such as illegal data collection that violates international law and territorial boundaries of sovereignty, time-consuming MLA process, raising an alarm to the suspect so she/he immediately destroys the digital evidence or device, and lastly, even though we have managed to get the data through foreign assistance, Indonesian law has not yet regulated the procedure for confiscation or obtaining it as evidence.

IV. CONCLUSION

The admissibility and credibility of electronic evidence must be maintained from the time investigators find electronic evidence for the first time until it is finally displayed in court. Every aspect must be considered, starting from human resources, the necessary infrastructure and tools, regulations and standard procedures that are clear and accountable, and admissible analysis results of electronic evidence that support other evidence. The government must also support the obtaining of electronic data from service providers or foreign companies by making the necessary regulations and agreements with these parties.

Also, to ensure the admissibility and credibility of electronic or digital evidence, there are principles that have to be met according to ISO 27037, such as Data Integrity, Competency, Chain of Custody and Regulation.

The electronic or digital evidence must have been procured and examined with the correct and standardized procedures, so that it can be concluded that there is no change in the evidence, or it can be ensured that the integrity of the electronic evidence is well maintained and has evidentiary value in court.

Then the identification, collection, processing, security, analysing and documentation of electronic evidence must be carried out by competent personnel to prevent compromise of such electronic evidence. This requires sufficient certification of skills needed for Digital Evidence First Responders and Digital Evidence Specialists.

Furthermore, a clear and complete chain of custody is essential where the entire process is carried out according to procedures so that an independent third party can audit, examine or analyse the same electronic evidence and obtain the same results.

Finally, persons in charge of electronic evidence are responsible for ensuring that the processes and procedures on electronic evidence are – from the beginning – carried out in accordance with applicable law and can be accounted for. These principles must be known and understood by investigators, public prosecutors and judges so that electronic evidence can be presented in court properly.