

Digitized Archive as Digital Evidence: Readiness Observation at Dinas Perpustakaan dan Kearsipan Provinsi DKI Jakarta

Wiwiet Mardiaty¹, Niko Grataridarga¹, and Dyah Safitri¹

¹Document and Information Management Laboratory, Vocational Education Program, Universitas Indonesia

*Email: wiwietm@ui.ac.id

Abstract. Currently, the process of archive digitization, especially from paper archives to digital format, is an option for companies to store their documents more efficiently and effectively. In addition, it can make document retrieval easier. However, although digitization is supported by Regulation No. 8 of 1997 on electronic documents, according to Hadiwardoyo (2001), the archives digitization process is not necessarily supported by the readiness of other legal instruments. Hadiwardoyo¹ argues that archive digitization involves two main things: the security of the media technology digitization device and the legal considerations related to the validity of the evidence in court. This research explores how the quality of the archive digitization process, especially in government, can be improved so that it is not just an effort toward e-governance but also acceptable for auditing as part of digital forensics.

Keywords: *digital forensics, archive digitization*

1 Introduction

Currently, the archive digitization process, especially from paper archives to digital format, is an option for companies to store their documents more efficiently and effectively. In addition, it can make document searching and retrieval easier. However, although the digitization process is supported by Law No. 8 of 1997 on electronic documents, according to Hadiwardoyo (2001), it is not necessarily supported by the readiness of other legal instruments. Hadiwardoyo argues that archive digitization involves two main things: the security of the media technology transfer device and the legal considerations related to the validity of the evidence in court.

Wiryana in Putra (2017) also argues that although Indonesia already has an Indonesian national standard (SNI) on the handling of digital evidence, many systems used in electronic document storage are not built for forensic sound and thus are not ready to support forensic digital analysis.

Sitompul (2012) adds the formal and material requirements outlined in the 2008 ITE Law that says electronic information and documents must be guaranteed authenticity, integrity, and accessibility. Authentication in electronic documents generated from the digitization process is usually questionable, as there is an assumption that the process reduces the quality of the original document.¹

This is supported by the results of Mayesti and Hariarseto's (2013) research in the Jakarta library and archive office (Dispusip), which showed that Jakarta Dispusip's efforts to maintain the authenticity of their electronic archives are still low, although there have been some endeavors such as adding metadata in standard systems, processes, or mechanisms when users or communities need the archives, and the use of full-color techniques.

The "rejection" of digital evidence is also seen in court, especially in civil cases. In a civil case, a judge will evaluate the quality of proof presented by the parties.⁵ Thus, the judge's decision is the key to the acceptance of any digital evidence that is submitted. A judge who holds that digital evidence cannot be used, in general, refers more to legal certainty (based on rules of legislation). Conversely, more progressive judges will consider or even make digital evidence as one point in the decision making.⁶

Given this situation, this study seeks to answer the question, "How should digitized files be prepared for digital evidence?"

Therefore, this research explores how the digitization process can be improved, so that its utilization is not only an effort toward e-governance but also acceptable for auditing as part of digital forensics. Observations and interviews were held in the Dinas Perpustakaan dan Kearsipan (Dispusip) of DKI Jakarta Province, which is currently conducting digitization activities. The claim is that the digitized materials are prepared in such a way that they can be used as digital evidence.

2. Literature Review

Digitization is a media transfer process to change materials from analog signals to digital form.¹³ It consists of document preparation, scanning, editing, inputting metadata, and quality control results from the digitization.

Digitization activities usually aim at several things, including ease of access, preservation, and reduce document storage (United Nations, 2011).⁷ However, the reduction of physical documents that have been digitized is usually not done, because the physical documents need to remain available when there is an audit or a case in which they are used as evidence. For digitized material to be used as evidence, certain standards need to be met, including authenticity, completeness, and accessibility, as well as integrity of the records. In ensuring this integrity, the archivist must have the right policies and tools to prove that the quality of the digital records was unchanged in the digitization process (Dietrich & Adelstain, 2015). In the digitization process, usually, the software used will produce one or more “hashes” or secure cryptographic residue. The hashes are recorded and stored together with the data, which can be argued that the digitized material has not changed since the beginning of the process.⁸

In addition, metadata in electronic documents is the key in maintaining reliability and authenticity for trustworthiness (Gilliand, Rouche, Lindberg, & Evans, 2005). In digital forensic viewpoints, metadata often contain hidden information that can serve as digital evidence.¹⁰ Metadata contains not only information about the representation of the content of the digital data, but also the track record, such as when it was created, modified, transferred, and so forth. Kime (2014) states, “Every file contains ‘metadata,’ which is electronic information that a computer keeps about a file, such as its owner, creator and when it was saved, altered or deleted.”¹¹

The investigation will begin by looking at the integrity of the digital material from the digital forensics point of view. The change of digital material can be caused by various aspects, such as hardware failure, hardware control access, electrical power surges, and human error in editing the images in digitizing progress. Therefore, it is essential to standardize and secure image-handling procedures (Berg, 2000).

3. Method

This research was conducted using a qualitative method and literature study. The literature study collected information on how to prepare digitized materials to be used as digital evidence. Observations were also conducted at Dispusip, where 38 students majoring in Information and Document Management participated in digitization activities as part of a two-month digitization practicum conducted from March 6 to April 24, 2018. Interviews about the digitization process were also carried out with employees who were designated as responsible for such activities.

4. Results and Discussion

4.1 Digitization Process at Dinas Perpustakaan dan Kearsipan Provinsi DKI Jakarta

At Dispusip, digitization is done with a flatbed scanner. The archives currently being digitized are building permits. There are three stages in the digitization process: (a) archive preparation, which is the activity of preparing physical documents for digitization, such as by removing staples and arranging papers in chronological order (see Figure 1);



Fig. 1 Documents being prepared by students for digitization.

(b) conducting digitization activity using standard 200 dpi, with type TIFF, and Format: Color; and (c) indexing, which includes the number of documents, date and year, name of applicant, address of applicant, building address to be constructed, signing position, and storage place (see Figure 2).



Fig. 2 Digitization and indexing activity by MID student.

4.2 Results from Interviews and Observations

The results from the interviews and observations will be compared with the findings from the literature review in relation to how digitized materials can be considered digital evidence.

(1) There is a need for appropriate policies, tools, and guidance in digitization projects if the digitized results can be aligned with the original document, so they can both be used as digital evidence.

In an interview on April 24, 2018, employees responsible for the digitization process said that digitized materials are expected to be used as digital evidence in the future. However, they also described that the standards for digitization are given quite low (e.g., 200 dpi) and the digitization project lacks guidance protected by legal requirements. Although the supervisor claimed that they already had a draft of governor regulations, at the time of the study, the digitization activity was being carried out without it legal support.

(2) In the process of digitization, process integrity must be considered from the beginning of the activity, such as access control to hardware, and standardize and secure image-handling procedures.

In the two-month digitization practicum, students and employees acknowledged that, in addition to editing being performed, there was no process of quality control for the digitized materials. Dispusip also does not have image-handling guidelines and does not restrict their access controls to maintain the integrity of the digitization process.

(3) Hash produced by imaging software needs to be stored on a regular basis as a track record of the digitization process. Dispusip currently does not have any knowledge about hash produced by imaging software, and therefore it has not stored it on a regular basis.

(4) There is complete metadata for capturing the track record of the digitization process from beginning to end. Metadata provided on their software is used for capturing the content from digitized material only.

5. Conclusion

From the above, it can be concluded that Dispusip's digitization project needs further improvement in the method used for preparing materials to be used as digital evidence. The very first thing they should do is maintain the integrity of the activity by sealing it under legal requirements, such as governor regulations, before they beginning to improve any of their digitization activity. Further research needs to be done on how the integrity of the digitization process can be improved by creating a model of the process resulting in digitized materials that can be used as digital evidence.

References

- Bandi, S., Angadi, M., Shivarama, J. Best Practised in Digitisation: Planning and Workflow Process. *Emerging Technologies and Future Libraries: Issues and Challenges*, 332.
- Berg, E.C. (2000). Legal ramifications of digital imaging in law enforcement. *Forensic Science Communication*, 2(3).
- Department of Management Archives and Records Management Section United Nations. (2011). Record-Keeping Requirements for Digitization.
- Dietrich, D. & Adelstein, F. (2015). Archival science, digital forensics, and new media art. *Digital Investigation* 14, 137-145. Retrieved 15 May 2018 from www.elsevier.com/locate/diin
- future of civil discovery. 2014-SEP W. Va. Law. 34, 36.
- Gilliand, A., Rouche, N., Lindberg, L. And Evans, J. (2005). Towards a 21st century metadata infrastructure supporting the creation, preservation and use of trustworthy records: Developing the InterPARES 2 Metadata Schema Registry. *Archival Science*. 5, 43-78.
- Hadiwardoyo, S. Alih media Kearsipan dalam Perspektif Hukum di Indonesia. 2001. Suara Badar I.
- Hannon, M.J. (2017). The importance of metadata in digital evidence for legal practitioners. *The Computer & Internet Lawyer*, 34(10), 1-19.
- Kime, E.R. (2014), Electronic discovery of electronically stored information and the
- Mayesti, N. & Hanriarseto, T. (2013). Otentisitas dalam Pengelolaan Arsip Elektronik: Studi Kasus di Badan Perpustakaan dan Arsip Daerah (BPAD) Pemerintah Provinsi DKI Jakarta.
- Putra, N. N. Era Ekonomi Digital dan Tantangan Menghadirkan Barang Bukti Digital di Pengadilan. 27 Desember 2017, di akses dari <http://www.hukumonline.com/berita/baca/lt5a3a543485faf/era-ekonomi-digital-dan-tantangan-menghadirkan-barang-bukti-digital-di-pengadilan>
- Sitompul, J. (2012). Cyberspace, Cybercrimes, Cyberlaw : Tinjauan Aspek Hukum Pidana, Tatanusa, Jakarta.