ANALYSIS OF META DATA FOR CCTV

[1]Brij Mohan Goel[*], [2]Shefali Saini

[1]Research Scholar, [2]Supervisor (Professor)

[1-2]Department of Computer Science and Engineering,

Baba MastNath University, Rohtak, Haryana, India

Email ID: shefalisaini9@gmail.com

Accepted: 29.08.2022 **Published**: 01.09.2022

Keywords: Meta Data, CCTV.

Abstract

The background of this investigation is how to make a video that can be analyzed as criminal data to prove the truth of the video, and therefore with forensics it can be used as evidence if the video contains incorrect data or contains criminal data so that it can be used as forensic data. The method used in this study is to use the literature review method that builds on many previous studies. of journals and books based on similar research, so that they can help develop current problems to the most recent ones so that they can find novelty in that research. The issue raised in this research is how to make a CCTV video that can be tested, in certain ways to make the video as criminal data, so that it can become data containing crimes that can be used as evidence. The purpose of this study is how to find the correct method of CCTV video analysis, so that it can be used as evidence of forensic data using the NIST method, and this method can be shown to be the correct method of video analysis, so that it can be used as evidence and as forensic evidence of data.

Paper Identification

**Corresponding Author*

INTRODUCTION

Currently the role of CCTV cameras (CCTV) is necessary as a security system in daily life, and the use of CCTV cameras is very effective as a security mechanism that is in demand today due to their ability to anticipate crime in society. This condition is highly anticipated by society to avoid various criminal acts. Therefore, the role and function of closed-circuit television (CCTV) cameras today is not just as a tool for monitoring the surrounding environment. CCTV cameras can record the environment in real time, and at certain times CCTV cameras are used as evidence regarding criminal cases. However, CCTV camera guides have special techniques for handling them because the nature of the evidence obtained from camera recordings is volatile or easy to change, very prone to modification and deletion, easily contaminated by new data, and time-sensitive. To preserve the integrity and veracity of the evidence, it is

necessary to apply digital forensics in the investigation of the case. Digital forensics is used to practice the anatomy of digital devices to find facts needed for legal purposes. In this case, two terms are almost the same, namely electronic evidence and digital evidence. Electronic evidence is in physically and visually recognizable form, such as computers, mobile phones, cameras, CDs, hard drives, etc., while digital evidence is in the form of evidence extracted or retrieved from electronic evidence, evidence can be in the form of files, emails, messages, photos, videos, records or text.

According to many cases using CCTV cameras, there is still uncertainty about the use of CCTV as to whether CCTV can be used as evidence or as evidence. With reference to Law No. 19 of 2016 Article 5 paragraph 1 (1) and paragraph 2 (two) on electronic information and transactions, it is established that electronic information and / or electronic documents and / or their publications are legal evidence, which is an extension of the evidence. Valid in accordance with the procedural law in force in Indonesia. In this case, CCTV cameras are a legal digital proof and have a recording file that provides information in the form of data or known as metadata, since the metadata can be recorded on a computer automatically when a file is created, so that you can know when the file was created. Who is the author, what is the file size and extension? Metadata information stores, maintains, and manages sources to maintain the integrity and integrity of files obtained from CCTV cameras. In addition to metadata when dealing with digital evidence from the CCTV camera, there is something basic called chain of custody. Chain of custody is an attempt to maintain and ensure integrity in digital evidence and chronologically documented procedures since it was first found at the crime scene (TKP) to explain 5 characteristics (4W and 1H) of the chain of custody, namely fingerprint of evidence (why), Digital signature (who), time stamp (when), geographic location (where) and procedures (how). The problem that will be developed from this journal is the analysis of the application of digital forensic analysis of CCTV camera recordings using the NIST method (National Institute of Standards Technology). As for the previous method, metadata and hashing.

METHODOLOGY

In the previous research, it was a hacking method, and the research method will be obtained based on the instructions and requirements of the Indonesian National Standard (SNI). Several previous studies have used acquisition procedures according to SNI 27037:2014 with the NIST (National Institute of Standards Technology) research process method used to analyze metadata from CCTV camera recordings as digital evidence. The inspection and analysis stage to be carried out. The NIST process consisting of several stages, the collection (labeling) phase or the collection phase is a series of activities to collect data to support the investigation process in the context of finding evidence of digital crimes.

At this stage there is the process of collecting data from relevant data sources and maintaining the integrity of the evidence from changes, examination (data processing) or inspection stage. This is the stage of examining the criminally collected data, either automatically or manually, and ensuring that the data obtained has the form of an original file according to what was obtained at the scene of the incident, so the digital files must be identified and validated using hashing techniques, in the process of this examination, The test is performed using forensic tools, which are media information and output tools used to find CCTV (closed-circuit) camera metadata information. In addition, the analysis phase (analysis of the results of the examination) or research phase takes place after obtaining the required digital file or data from the previous examination process, and then the data is analyzed in a detailed and exhaustive manner in a

technically and legally justified manner in order to be able to prove the data.

Fig 1. Research Model

The results of digital data analysis shall hereinafter be referred to as digital evidence and may be scientifically and legally justified as valid evidence.

The NIST process consisting of several stages, the collection (labeling) phase or the collection phase is a series of activities to collect data to support the investigation process in the context of finding evidence of digital crimes. At this stage there is the process of collecting data from relevant data sources and maintaining the integrity of the evidence of changes, examination (data processing) or inspection stage. This is the stage of examining the criminally collected data, either automatically or manually, and ensuring that the data obtained is in the original file form according to what was obtained at the scene of the incident, so the digital files must be identified and validated using hashing techniques, in the process of Examination. These are the tests performed using forensic tools, which are media and output information tools used to find metadata information on closed-circuit television (CCTV) cameras. In addition, the analysis phase (analysis of the results of the examination) or research phase takes place after obtaining the required digital file or data from the previous examination process, and then the data is analyzed in a detailed and exhaustive manner in a technically and legally justified manner in order to be able to prove the data. The results of digital data analysis shall hereinafter be referred to as digital evidence and may be scientifically and legally justified as valid evidence.

The NIST process consisting of several stages, the collection (labeling) phase or the collection phase is a series of activities to collect data to support the investigation process in the context of finding evidence of digital crimes. At this stage there is the process of collecting data from relevant data sources and maintaining the integrity of the evidence of changes, examination (data processing) or inspection stage. This is the stage of examining the criminally collected data, either automatically or manually, and ensuring that the data obtained is in the original file form according to what was obtained at the scene of the incident, so the digital files must be identified and validated using hashing techniques, in the process of this examination, The test is performed using forensic tools, which are media and output information tools used to find metadata information on closed-circuit television (CCTV) cameras. In addition, the analysis phase (analysis of the results of the examination) or research phase takes place after obtaining the required digital file or data from the previous examination process, and then the data is analyzed in a detailed and exhaustive manner in a technically and legally justified manner in order to be able to prove the data. The results of digital data analysis shall hereinafter be referred to as digital evidence and may be scientifically and legally justified. As evidence it is true. After identifying and classifying the evidence, the main thing is to fragment it. Where nebulizing is performed to keep data safe from data originating from digital evidence. Hashing in this section is an algorithmic technique used in a section of data to create a unique dataset with constant variable length conditions. Step to get the hash value of digital criminal investigations from CCTV camera manuals.

CONCLUSION

The development of this research is an attempt to obtain digital evidence from CCTV camera recordings that are applied using the NIST (National Institute of Standards Technology) method of digital criminal investigations related to CCTV camera recordings in order to obtain the metadata information from the file to be executed and process the source of information to be used as a source of information. As evidence is carried out using a chain of custody document so that the integrity of the digital evidence is kept intact from the beginning, it is found to analyze the information contained in the CCTV camera, and therefore the information regarding the evidence obtained from the CCTV camera recordings can be accepted and used to strengthen the evidence in the judge.

RÉFÉRENCIAS

1. V. Valentino, H. S. Setiawan, . A. Saputra, Y. Haryanto and A. S. Putra, "Decision Support System for Thesis Session Pass Recommendation Using AHP (Analytic Hierarchy Process) Method," *Journal International Journal of Educational Research & Social Sciences,* pp. 215-221, 2021.
2. V. H. Valentino, H. S. Setiawan, M. T. Habibie, R. Ningsih, D. Katarina and A. S. Putra, "Online And Offline Learning ComparisonIn The New Normal Era," *International Journal of Educational Research & Social Sciences (IJERSC),* vol. 2, no. 2, p. 449–455, 2021.
3. M. Ulfa, "“Pengaruh Kecanduan Game Online Terhadap Perilaku Remaja Di Mabes Game Center Jalan
4. Hr.Subrantas Kecamatan Tampan Pekanbaru”," *Jom. Fisip Vol. 4 No. 1,* pp. 1-13, 2017.
5. R. N. Suryanto, "“Dampak Positif Dan Negatif Permainan Game Online Dikalangan Pelajar”," *Jom Fisip Volume*
6. *2 No. 2* , 2015.
7. M. A. Suplig, "“Pengaruh Kecanduan Game Online Siswa Sma Kelas X Terhadap Kecerdasan Sosial Sekolah
8. Kristen Swasta Di Makassar”," *Jurnal Jaffray, Vol. 15, No. 2,,* pp. 77-200, 2017.
9. H. Sugiarto, I. Sumadikarta, M. Ryansyah, M. H. Fakhriza and A. S. Putra, "Application Design" Test Job
10. Application" On Android OS Using The AHP Algorithm," *International Journal of Educational Research & Social Sciences,* vol. 2, no. 5, pp. 1173-1180, 2021.
11. M. Subani, I. Ramadhan, S. and A. S. Putra, "Perkembangan Internet of Think (IOT) dan Instalasi Komputer Terhadap Perkembangan Kota Pintar di Ibukota Dki Jakarta," *IKRA-ITH INFORMATIKA: Jurnal Komputer dan Informatika*, vol. 5, no. 1, pp. 88-93, 2020.
12. A. Saputra, A. Fahrudin, A. S. Putra, N. Aisyah and V. Valentino, "The Effectiveness of Learning Basic Mathematics through Dice Games for 5-6 Years Old at TKIT Al-Muslim," *International Journal of Educational Research & Social Sciences*, vol. 2, no. 6, pp. 1698-1703, 2021.
13. http://ejournal.unitomo.ac.id/index.php/jsk, pp. 126 - 142, 2018.
14. P. Roza, "DIGITAL CITIZENSHIP: MENYIAPKAN GENERASI MILENIAL MENJADI WARGA NEGARA
15. DEMOKRATIS DI ABAD DIGITAL," *Journal Sosioteknologi Volume 19, No 2, Agustus 2020,* pp. 190-202, 2020.
16. P. M. Risnadinata, I. Kumara and W. Ariastina, "Management of Flood Protection System of Dewa Ruci Underpass in Bali,"

Journal of Electrical, Electronics and Informatics, Vol. 4 No. 2, August 2020, pp. 57-63, 2020.

17. D. D. A. P. Riani Muharomah, "“Analisis Run-Off Sebagai Dampak Perubahan Lahan Sekitar Pembangunan
18. Underpass Simpang Patal Palembang Dengan Memanfaatkan Teknik Gis”," 2014.