Digital Forensics: Acquisition and Analysis on CCTV Digital Evidence using Static Forensic Method based on ISO /IEC 27037:2014

Rizdqi Akbar Ramadhan[1], Desti Mualfah[2] and Dedy Hariyadi[3]
[1]*Department of Informatics, Universitas Islam Riau, Pekanbaru, Indonesia*
[2]*Department of Computer Science, Universitas Muhammadiyah Riau, Pekanbaru, Indonesia*
[3]*Jenderal Achmad Yani University of Yogyakarta*

Keywords: Digital, Evidence, Forensic, Law, Acquisition, Multimedia.

Abstract: Conventional crime has existed since the beginning of human civilization where evidence and artifacts can be used as assumptions to prove crime. Every criminal who is proven to have committed a certain crime will be convicted in accordance with the stipulated law. In this paper, there is a conventional crime case that can be proven to be a crime with digital technology, namely CCTV. Digital evidence obtained from CCTV footage can be used as an assumption of the extent of crimes committed by criminals. Unfortunately, the quality of the recording is not easy to analyze due to the lack of resolution of the video recording and the lack of lighting in certain conditions. The analysis that will be carried out in this case uses visual manipulation tools called Adobe Lightroom and other supporting tools. Digital forensic implementation and digital evidence handling procedures are used to handle this case using the forensic static method.

1 INTRODUCTION

Forensic digital science began to show its contribution in today's digital era. In contrast to other forensic sciences which are mostly related to dissecting and searching for artifacts in living things, digital forensic is the practice of dissecting digital devices to look for facts needed for legal purposes. In this case, the forensic static method is used in handling evidence in the form of CCTV (Closed Circuit Television). In handling this digital evidence there is an essential thing called the chain of custody. In Digital forensic there are two categories of evidence declared, namely Physical Evidence and Digital Evidence. In this case, there are two terms that are almost the same, i.e. electronic evidence and digital evidence. Electronic evidence has a physical form and can be identified visually (computer, mobile phone, camera, CD, hard disk, etc.), while digital evidence is evidence that is extracted or recovered from electronic evidence (can be a file, email, short message, image, video, log, text). Chain of custody is an effort to maintain and ensure integrity in digital evidence and the procedure for documenting chronologically the evidence (Prayudi and Sn, 2015). The characteristics of digital evidence affect the level of difficulty of handling digital evidence with a predetermined method.Digital evidence has a number of characteristics, such as easy to be duplicated and transmitted, very susceptible to be modified and removed, easily contaminated by new data, and time sensitive. Digital evidence is also very possible to cross countries and legal jurisdictions. For this reason, according to (Schatz, 2007) the handling of chain of custody of digital evidence is much more difficult than the handling of physical evidence, in general. In contrast to physical evidence, digital evidence is very dependent on the interpretation of its content. Therefore, the integrity of the evidence and the ability of the expert to interpret the evidence will be influential in sorting digital documents available to serve as evidence.

Digital forensic generally implements 5w1h which is what, where, when, why, who, how. What is a form of crime committed, where is the placed the crime is committed, when is the time when the crime is committed, why is it the reason and motive of the crime that occurred, who is the suspect in the crime and the victims of a crime related, and how is the method of crime carried out from the perspective of criminals and how, procedures, methods of analysis, legal access rights to handle evidence from the perspective of the investigator. In digital forensic challenges that often arise are about how to classify evidence (Turner, 2005), rebuild, rearrange, clarify evi-

Ramadhan, R., Mualfah, D. and Hariyadi, D.
Digital Forensics: Acquisition and Analysis on CCTV Digital Evidence using Static Forensic Method based on ISO /IEC 27037:2014.
DOI: 10.5220/0009120400850089
In *Proceedings of the Second International Conference on Science, Engineering and Technology (ICoSET 2019)*, pages 85-89
ISBN: 978-989-758-463-3

dence both systemally and visually human, and how to use a standard and comprehensive communication language in court presentations Classification of digital evidence is a very important because authenticity and integrity must be maintained in accordance with the conditions when they were first discovered and then presented at law court proceedings (Ćosić et al., 2011) According on the facts and problems related to digital forensic and the handling described above, in this case the author will describe the practice of acquisition and analysis of digital evidence in the form of CCTV footage that displays conditions of recording with inadequate lighting using forensic static methods.

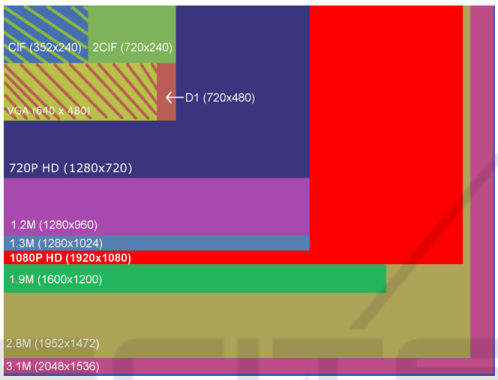

Figure 1: Resolution on Frames

Another polemic found in handling this case is that human objects recorded in CCTV are different from suspected human objects in real life in anatomical aspects of body size. In real life the size of the suspected weight is in the range of around 90kg but when viewed on CCTV the object's weight is in the range of 60-75kg. The aspect ratio and reslolution on CCTV footage is an issue in this polemic. There are various aspect ratio figures in digital visualization.

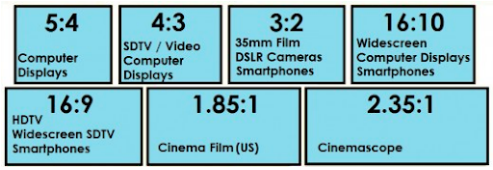

Figure 2: Aspect Ratio

In simple terms, the first step taken is the acquisition process which is taking physical evidence of CCTV devices that are labeled by implementing the principle of chain of custody (Giova, 2011) because the evidence must be maintained based on integrity and authenticity in accordance with the conditions when it was first discovered will be submitted to court. The next acquisition step is the practice of taking digital evidence from video recording data from CCTV file system storage. The next step of this practice is to calculate the hash value of the video file, scene and frame classification, metadata analysis, digital manipulation examination, and reporting.

2 METHOD AND MATERIAL

Referring to the previous forensic protocol component, there are general steps that can be defined abstractly to produce models that are not dependent on certain technologies or electronic crime. Static Forensic analysis has limitations that is it cannot describe events accurately in accordance with their actual conditions (Mrdovic et al., 2009). The basis of this model is to determine the key aspects of the protocol mentioned above and ideas from traditional forensics, specifically the protocol for physical crime scene searches (Reith et al., 2002). Handling Digital Evidence with systems related to CCTV is increasingly complex. This is influenced by digital and optical systems that have developed from year to year.The crime scene in this case is very crucial because it will have a significant effect on the course of investigation. the onion skin route is implemented in the crime scene related case. In the research of (Hariyadi et al.,), the CCTV acquisition model was divided into two stages, namely pre-acquisition and core acquisition. Pre-acquisition is a problem that investigators must consider when he is at the scene. In the Pre-acquisition phase it emphasizes the preparation and identification of all matters relating to CCTV systems. Things to note are in the following figure 3:

Integrity and confidentiality are the main values of Pre-Acquisition aspect. In simple terms, handling physical evidence or digital evidence based on SNI ISO / IEC 27037: 2014 were as follows (Nasional, 2014):

- Minimize handling of the original digital device or potential digital evidence.
- Account for any changes and actions into a comprehensive documentation
- Comply and match with local rules and law.
- The Digital Evidence First Responder and Digital EvidenceSpecialist should not take actions beyond their competence.

3 RESEARCH METHOD

Based on literature studies and literature reviews, in the process of digital forensic investigations in this

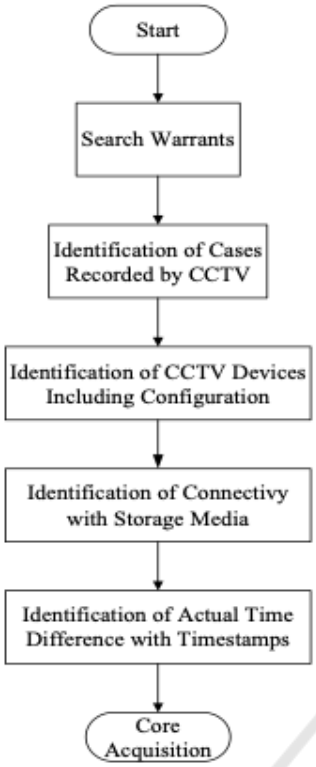

Figure 3: Pre-Acquisition

case requires a method of pre-acquisition. After implementing the pre-acquisition, the core-acquisition process will be mapped on the chart following figure 4:

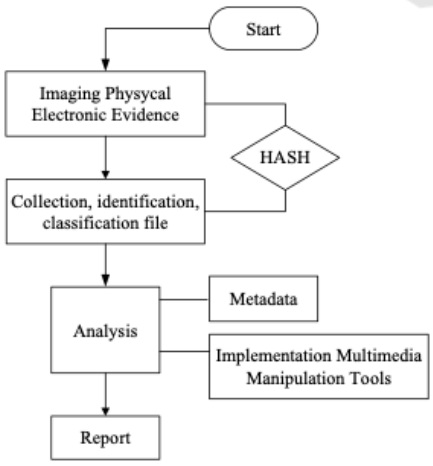

Figure 4: Pre-Acquisition

This analysis stages requires contributions from third-party tools applications. These tools assist in accomplishing some of forensic steps, primarily the systematic search for evidence (Reith et al., 2002). At the following table 1 are some tools that used in this case:

Table 1: Third-party tools

Tools	Usability
MacHAsh	Calculate Hash VAlue
ExifTool	Metadata Processing
Adobe Premiere	Video Editor
Adobe Lightroom	Visual Tuner

3.1 Imaging

Imaging stages at core acquisition are the first step in this step. Imaging is one of the essence in the forensic static method. Calculation of hash values is also one of the elements of this stage.Forensic data is acquired by using different kinds of external devices like USBs, external hard derives etc. or CD,DVDs and then this data is brought into the forensic lab for investigators to perform different kinds of op- erations/steps to forensically analyze evidentiary data (Rafique and Khan, 2013). The application for calculating hash values in this case is Mac Hash which runs on Macintosh operating systems

3.2 Collection

At the collection stage all files that have finished the imaging process will be collected and then sorted. This stage is also a crucial stage in CCTV forensics because (Perrott et al., 2002) there are so many recorded video files as long as the CCTV operates (Cucchiara, 2005). In this case there are 3 cameras with suspicious objects. In this study the authors took samples from the 3 cameras. Calculation of (Kerr and van Schyndel, 2014) hash values is also done at this stage. The following results of the hash value calculation are in table 2:

3.3 Analysis

3.3.1 Metadata

At the analysis stage begins by processing metadata using Exiftool. The process of analyzing metadata is implemented to see the composition and characteristics of the file to be analyzed in this case is a type file .AVI. The following figure 5 is an example of the output from Exiftool:

3.3.2 Multimedia Tools

Implementing multmedia tools contributes to this analysis. The (Zhou et al., 2011) contribution given

Table 2: Third-party tools

File Name	Hash Value
25_01_R_20170626050000 (VIDEO CAM 1)	740709CD749F975183B4B85026B822DD
24_02_R_20170626040000 (VIDEO CAM 2)	15AF1C78BA8401ACB84E968EC26F9ADD
25_07_R_20170626050000 (VIDEO CAM 7	E091E024C497C499C0B04A6A8E1D0C85

Table 3: Time Stamp

Cam Device	Date on Device (yy-mm-dd)	Time as Suspicious Object Appeared
Camera 1	2017-06-26	05.01.39 up to 05.02.04
Camera 2	2017-06-26	04.11.24 up to 04.25.59
Camera 7	2017-06-26	05.02.02 up to 05.02.28

```
: 11.06
: 25_01_R_20170626050000.avi
: /Users/rizdqia.ramadhan/Desktop
: 246 MB
: 2017:08:24 18:02:26+07:00
: 2018:07:10 10:14:46+07:00
: 2018:07:10 10:03:04+07:00
: rwxr-xr-x
: AVI
: avi
: video/x-msvideo
: 15
: 124.5 kB/s
: 27834
: 2
: Video
: H264
: 15
: 27834
: Default
: Variable
: Windows V3
: 944
: 1080
: 1
: 24
: H264
```

Figure 5: Metadata in Exiftool interface

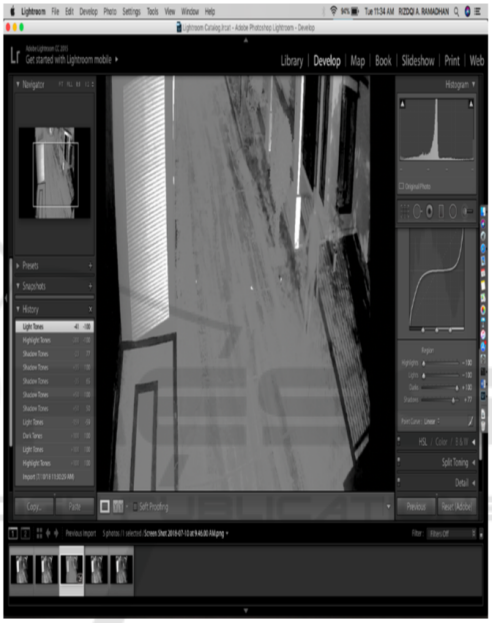

Figure 6: Visual manipulation on Adobe tools

is the ability to manipulate the visual aspects of this digital evidence. Adobe Premiere is used to group and cut (if needed) and screenshots when a suspicious object has been found in the entire video file on the evidence. The next step is to display the screenshot in Adobe Lightroom. The Adobe Lightroom application in this case contributes as a tool for adjusting images or objects if the original evidence cannot be analyzed naturally because of the visual limitations that come from CCTV recording devices. Apart from statements related to the use of multimedia tools in analyzing digital evidence, analysis and manipulation of these files must use files that have been duplicated so that the original digital evidence is not contaminated and change the hash values that have been calculated. Changing the hash value means that it has eliminated the integrity of the acquisition of digital evidence in forensic investigations. Here is an example of duplicated digital evidence manipulation in the form of a visual file using Adobe Lightroom:

3.3.3 Report

At the reporting stage the content attached contains the whole investigation from beginning to end, all charts, forms of evidence, methodology and conclusions (Stephenson, 2003). In this study the author only emphasizes the essential aspects of the Time Stamp aspect. Time stamp is the writing of important times where the evidence in the form of CCTV is recording suspicious objects. The following table 3 is an example of the time stamp in this case:

4 CONCLUSION

Pre-Acquisition and Core-Acquisition are the main stages in the investigation and analysis of digital ev-

idence. In the analysis of digital forensic investigations requires the integrity of the authenticity of the evidence from the time it is found, acquired, analyzed until the reporting stage in accordance with the principle of the chain of custody. Technically the integrity and authenticity of the evidence can be proven by calculating the hash value. In this case with evidence in the form of CCTV, it also requires the ability to use multimedia aspect to analyze digital evidence. This digital forensic analysis cannot convict a crime but only reinforces actual expectations. The weakness in this study is that multimedia manipulation can only clarify objects with poor light but cannot accurately compare the composition of objects on the screen with objects in the real world.

ACKNOWLEDGEMENTS

This paper was supported by Universitas Islam Riau.

REFERENCES

Ćosić, J., Ćosić, Z., and Baća, M. (2011). An ontological approach to study and manage digital chain of custody of digital evidence. *Journal of Information and Organizational Sciences*, 35(1):1–13.

Cucchiara, R. (2005). Multimedia surveillance systems. In *Proceedings of the third ACM international workshop on Video surveillance & sensor networks*, pages 3–10. ACM.

Giova, G. (2011). Improving chain of custody in forensic investigation of electronic digital systems. *International Journal of Computer Science and Network Security*, 11(1):1–9.

Hariyadi, D., Nastiti, F. E., and Aini, F. N. Framework for acquisition of cctv evidence based on acpo and sni iso/iec 27037: 2014.

Kerr, M. and van Schyndel, R. (2014). Adapting law enforcement frameworks to address the ethical problems of cctv product propagation. *IEEE Security & Privacy*, 12(4):14–21.

Mrdovic, S., Huseinovic, A., and Zajko, E. (2009). Combining static and live digital forensic analysis in virtual environment. In *2009 XXII International Symposium on Information, Communication and Automation Technologies*, pages 1–6. IEEE.

Nasional, B. S. (2014). Pedoman identifikasi, pengumpulan, akuisisi dan preservasi bukti digital (iso/iec 27037: 2012, idt).

Perrott, A., Lindsay, A. T., and Parkes, A. P. (2002). Real-time multimedia tagging and content-based retrieval for cctv surveillance systems. In *Internet Multimedia Management Systems III*, volume 4862, pages 40–49. International Society for Optics and Photonics.

Prayudi, Y. and Sn, A. (2015). Digital chain of custody: State of the art. *International Journal of Computer Applications*, 114(5).

Rafique, M. and Khan, M. (2013). Exploring static and live digital forensics: Methods, practices and tools. *International Journal of Scientific & Engineering Research*, 4(10):1048–1056.

Reith, M., Carr, C., and Gunsch, G. (2002). An examination of digital forensic models. *International Journal of Digital Evidence*, 1(3):1–12.

Schatz, B. L. (2007). *Digital evidence: representation and assurance*. PhD thesis, Queensland University of Technology.

Stephenson, P. (2003). A comprehensive approach to digital incident investigation. *Information Security Technical Report*, 8(2):42–54.

Turner, P. (2005). Unification of digital evidence from disparate sources (digital evidence bags). *Digital Investigation*, 2(3):223–228.

Zhou, L., Chao, H.-C., and Vasilakos, A. V. (2011). Joint forensics-scheduling strategy for delay-sensitive multimedia applications over heterogeneous networks. *IEEE Journal on Selected Areas in Communications*, 29(7):1358–1367.