

# Framework for Acquisition of CCTV Evidence Based on ACPO and SNI ISO/IEC 27037:2014

Dedy Hariyadi  
 Fakultas Teknik dan Teknologi  
 Infomasi  
 Universitas Jenderal Achmad Yani  
 Yogyakarta  
 milisdad@gmail.com

Faulinda Ely Nastiti  
 Fakultas Ilmu Komputer  
 Universitas Duta Bangsa  
 Surakarta  
 faulinda.en@gmail.com

Farida Nur Aini  
 Fakultas Sain dan Teknologi  
 Universitas Respati Yogyakarta  
 farida\_mi@respati.ac.id

**Abstract**— The growth of embedded systems globally has always increased. This affects the development of CCTV Systems products that are getting smaller and connected to various types of devices. CCTV Systems as a support system in a security system are needed when the investigation process. Various types and models of CCTV systems on the market, an investigation framework is needed to acquire CCTV systems specifically. This research proposes a framework for the acquisition of electronic and / or digital evidence of CCTV systems.

**Keywords** – CCTV, Acquisition, Smartphone, Xiaomi, Surveillance System, Forensics

## I. INTRODUCTION

Numbeo[1] conducted a security index survey with 51397 respondents in 4623 cities around the world, while indicators in the survey included perceived crime rates, changes in crime rates over the past three years, perceived security during the day, perceived security at night, worries robbed, fears of motor vehicle theft (including), fears of being attacked by foreigners,

fear of being humiliated in public places, fears of physical assault due to Religion and Race, and drug abuse. In this study the survey cited is the security index of countries in ASEAN. Based on the survey, Numbeo Singapore was the country that has the highest security index of 83.9%, while Indonesia is ranked fifth with a security index of 54.73%. The survey of the security index and crime index in ASEAN in the period of 2015 to 2018 is shown in Figure 1.

Singapore's high security index cannot be separated from the support of a well-integrated security monitoring system [2]. CCTV installation to reduce crime was once carried out by the Swedish National Council [3], they stated that the installation of CCTV could reduce crime. This is not only through the installation of government / private CCTV in certain areas that can reduce crime, but portable cameras such as cameras on mobile phones or portable CCTV owned by individuals can reduce crime

one instrument that can reduce crime in an area is the location of CCTV placement. There are three types of CCTV laying [4] :

1. Open system, installation in areas that can be clearly seen by the public and given a marker that there are CCTV installed.
2. Open System - Hidden, CCTV is installed in areas that can be clearly seen by the public but protected by a one-way transparent casing.
3. Hidden Systems, CCTV is installed in a hidden area so that people do not realize that the area is being monitored by CCTV.

In addition to laying CCTV, there is something that needs to be considered to uncover crimes, namely video acquisition stored in "video servers" to support the investigation process. "Video server" or better known as Digital Video Recorder (DVR) functions to capture video quality optimally, store and play videos in an integrated device with storage media [5]. DVR for storing sourced video from analog cameras while NVR (Network Video Recorder) deviates sourced video IP camera. Both DVR and NVR video in addition to record pertinent information but also stores information timepiece commonly called timestamp [6]. Some devices do not yet support Network Time Protocol so that the timestamp information listed is invalid. Therefore, this study proposes a

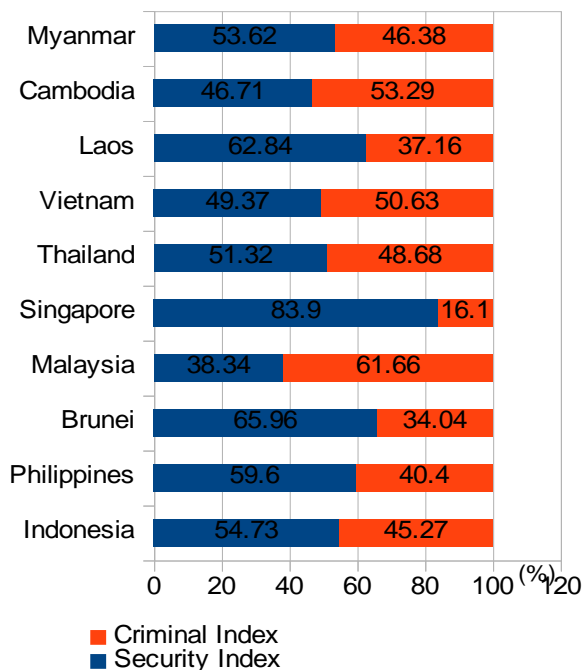


Figure 1. ASEAN Security Index Survey in 2018

framework acquisition of digital evidence from a monitoring system using CCTV.

## II. RELATED WORK

### A. Standardization of ACPO

The police association in the United Kingdom, the Association of Chief Police Officer (ACPO) in collaboration with information security company 7safe makes electronic and / or digital evidence handling instructions. The instructions made cannot only be applied in the United Kingdom police environment but can be applied to police in other countries including private investigators for special sectors. Indonesian Republic Police through the Center for Forensic Laboratories also applies instructions from ACPO in handling electronic and / or digital evidence [7].

### B. Standardization of SNI ISO / IEC 27037:2014

The Indonesian National Standard (SNI) which regulates Security Techniques-Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence is regulated in SNI ISO / IEC 27037:2014. The SNI also regulates the acquisition of CCTV that is connected to the DVR [9]

### C. Standardization of the Ministry of Communication and Information Technology

The Ministry of Communication and Information Technology of the Republic of Indonesia has Standard Operating Procedures (POS) related to the handling of evidence, including the acquisition of CCTV procedures [10]

### D. First Respond Framework

The First Respond Framework proposed by Danang Mulyadipa Suratno is divided into four parts, namely identification, collection, acquisition, and preservation. The acquisition phase is divided into 8 stages of acquisition [11]:

## III. MATERIAL AND METHODS

This research focuses on the basic principles of handling electronic and / or digital evidence according to ACPO and SNI ISO / IEC 27037:2014, especially in the acquisition process. Both ACPO and ISO / IEC 27037:2014 have similar basic principles. The basic principles of handling digital and / or digital evidence based on ACPO were as follows [8][12]:

1. No action taken by law enforcement agencies, persons employed within those agencies or their agents should change data which may subsequently be relied upon in court.
2. In circumstances where a person finds it necessary to access original data, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.
3. An audit trail or other record of all processes applied to digital evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.

4. The person in charge of the investigation has overall responsibility for ensuring that the law and these principles are adhered to.

While the basic principle of handling electronic and / or digital evidence based on SNI ISO / IEC 27037:2014 were as follows [9]:

1. Minimize handling of the original digital device or potentialdigital evidence.
2. Account for any changes and document actions taken.
3. Comply with the local rules of evidence.
4. The Digital Evidence First Responder and Digital EvidenceSpecialist should not take actions beyond their competence.

We used CCTV systems with analog and IP-based cameras as electronic evidence, as in Table 1

Table 1. The Materials

No	Merk	Camera Type	Video Server Type
1	Calion 3016 MH	Analog	DVR Analog
2	Hikvision DS-7200	IP Based	NVR
3	Mijia Ecosystem	IP Based	NVR Based on Cloud Computing

## IV. RESULT AND DISCUSSION

In general, installing CCTV and DVR is the same as computer networks. Although the Calion 3016 MH analog DVR still has one UTP port that can be connected to a computer network system. Therefore it can be used remotely. In a computer network system there is a unique timepiece or commonly called a time stamp. A unique timestamp will not produce a duplicate timepiece that becomes the basis for the process [13].

CCTV has Timestamps which is the focus in the acquisition of digital evidence. The relevance of a crime to time is important before the acquisition process. Based on observations that the time indicator on the camera and DVR there is a difference in time with the actual time. Therefore, the timestamps on the camera and DVR must be noted the difference with the actual time.

Some types of CCTV nowadays not only support video storage on video servers like DVR or NVR, but they also provide storage media slots. Existing storage media slots such as SD Cards are relatively small in shape. But the installation of SD Card on the camera is optional or mandatory depending on the DVR or NVR model. Especially for Mijia product cameras as in Table 1, SD Card is a mandatory requirement.

In this study proposes a CCTV acquisition model which is divided into two stages, namely pre-acquisition and core acquisition. Pre-acquisition is a matter that must be considered by the investigator when he is at the crime scene. In the Pre-acquisition phase emphasizes the preparation and identification of all matters related to the CCTV system. The thing to note is the following Fig. 2:

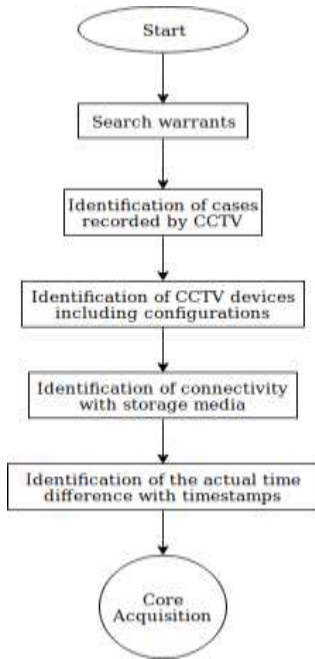


Figure 2. Pre-Acquisition

Core Acquisition was a stage of acquisition of electronic and / or digital evidence related to CCTV systems. This acquisition was a combination or improvement of several acquisition methods. After the core-acquisition stage has been fulfilled, it can perform the acquisition process as follows see Fig 3:

Currently many cameras were sold with monitoring systems through smart phones. Therefore smart phones can be said to function as NVR. In the Mijia Ecosystem camera the monitoring system uses the Mi Home Apps application as an NVR that runs on smart phones, so that the acquisition was a smart phone, can be seen in Table 2.

Table 2. Comparison of Acquisitions

No	DVR	Compact Disk	Hard Disk	USB	Export over Network
1	Calion 3016 MH	X	V	V	V
2	Hikvision DS-7200	X	V	V	V
3	Mi Home Apps	X	Smartphone Acquisition	X	V

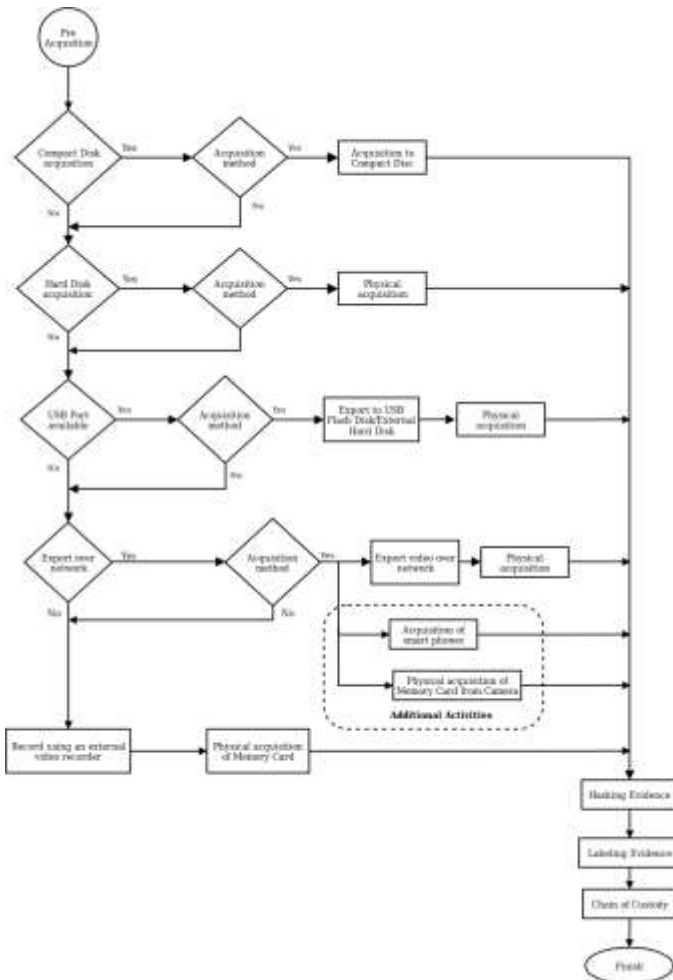


Figure 3. Core Acquisition

### V. CONCLUSION

Handling electronic and / or digital evidence related to CCTV systems has increasingly complex. This is influenced by the development of embedded systems experiencing growth always increasing from year to year [14]. Electronic devices are becoming smaller and can be connected to a smartphone. Therefore, the CCTV System acquisition method has undergone a change, including the acquisition method of smartphones in the framework of acquisition of electronic and / or digital evidence. CCTV System is part of a critical computer network system so that there are several acquisition processes can be done partially [9]. This study has not reviewed the status of Power-ON or Power-Off on devices or electronic evidence. This is a limitation in this research. It is expected that further research can be improved regarding the status of Power-ON or Power-Off on devices or electronic evidence.

### VI. REFERENCES

- [1] Numbeo, "Crime Survey." [Online]. Available: <https://www.numbeo.com/crime/>. [Accessed: 02-Apr-2018].
- [2] Singapore Police Force (SPF), "Video Surveillance System (VSS) Standar for Buildings," Singapore, 2013.
- [3] B. C. Welsh and D. P. Farrington, "Closed-Circuit Television Surveillance and Crime Prevention," Stockholm, 2007.
- [4] J. Ratcliffe, *Video Surveillance of Public Places*, vol. 4, no. 4. 2011.

- [5] Rockpile Security, "CCTV Digital Video Recorder (DVR) FAQ." Rockpile Security, Colorado, 2004.
- [6] D. L. Mills, *Computer Network Time Synchronization: The Network Time Protocol*. CRC Press, 2006.
- [7] M. N. Al-Azhar, *Digital Forensic: Panduan Praktis Investigasi Komputer*. Jakarta: Salemba Infotek, 2012.
- [8] Association of Chief Police Officers, "Good Practice Guide for Computer-Based Electronic Evidence," 2008.
- [9] Badan Standarisasi Nasional, "Teknologi Informasi - Teknik Keamanan-Pedoman Identifikasi, Pengumpulan, Akuisisi dan Preservasi Bukti Digital (SNI ISO/IEC 27037:2014)," Jakarta, 2014.
- [10] S. Kurniawan, "Perancangan Prosedur Operasional Standar Penanganan Alat Bukti Digital: Studi Kasus Kementerian Komunikasi dan Informatika," Universitas Indonesia, 2014.
- [11] D. M. Suratno, I. Riadi, and Y. Prayudi, "First Respond Framework Untuk Forensik CCTV," in *Hacking and Digital Forensics Exposed (H@DFEX)*, 2018, pp. 13–20.
- [12] Association of Chief Police Officers, "ACPO Good Practice Guide for Digital Evidence," 2012.
- [13] P. A. Bernstein and E. Newcomer, *Principles of Transaction Processing*, 2nd Editio. Elsevier Inc, 2009.
- [14] Market Research Store, "Global Embedded Systems Market Set for Rapid Growth, to Reach around USD 225.34 billion by 2021," 2016. [Online]. Available: <https://www.marketresearchstore.com/news/global-embedded-systems-market-249>. [Accessed: 12-Mar-2018].