Advanced Science and Technology Letters
Vol.145 (NGCIT 2017), pp.70-74
http://dx.doi.org/10.14257/astl.2017.145.14

Study on the Storage of Digital Photographs by an Investigator

Yong Jin Kim[1] and Gyu An Lee[2]

[1] Department of Science Criminal Investigation, Graduate School of Peace & Security Studies. Chungnam National University, (34134) 99, Daehak-ro, Gung-Dong, Yuseong-Gu, Daejeon, South Korea, guidoloveson@hanmail.net (Yong Jin Kim: First author)
[2] Department of Convergence Education, Hoseo Graduate School of Venture,(06724) 2497, Nambu-Sunhwan-ro, Seoul, South Korea, leegyuan@hanmail.net (Gyu An Lee : Corresponding author)

Abstract. Investigators acquire and retain evidence in various incidents, and some evidence approaches more closely to the substantive truth of the crime with the data analyzed through the referral process. As the era of the 4th Industrial Revolution has arrived, the evidence has been classified as analog evidence and digital evidence. In particular, investigators in charge of primary investigations take various photos of incidents. Scientific investigation has progressed from the method of field reproduction utilizing past sketches to the restoration of field through stereoscopic scanner of 3D method by advancing at the stage of present photography and moving picture shooting. However, the role of the investigator in the primary investigation has not changed much, and sketching and photography are the first steps in the investigation. The photo shoot is carried out by individual cell phones and digital cameras, and when a field agent arrives, the field investigator will take various types of pictures. And when the investigation is concluded or the case of stopping the prosecution, the record is sent to the prosecutor, which is sent along with various evidence of the site. In the case of digital photos, only a few photos needed for an investigation are stitched to the record or stored on a handheld computer. However, in the rare incident of a re-examination or review after several years or decades, digital evidence photographs must be examined for their availability and utilization. As a result of this study, it is possible to establish a basis for further substantive truth by improving the storage method of digital photographs and presenting a semi - permanent preservation period.

Keywords: Digital Evidence, Photograph, Detective, Truthfulness, Integrity.

1 Introduction

A record documents that are recorded by a team of investigators when they begin to investigate an incident are the beginning and the end of the investigation. Normally, investigations are proceeded from the stage of various steps such as situation reports, records, seizures and lists, warrants, result reports by request of the warrants, analysis requests and results.

ISSN: 2287-1233 ASTL

During that steps from hundreds of to thousands of digital evidence photographs will be taken by the investigator or site verification investigator and that will be stored on the server and the computer of the investigation agency. However, very minimum photographs of crime scenes could be used and the rest could be deleted, damaged, lost, or classified due to personnel movements.

In this study, digital photographs collected and analyzed by investigators are categorized as digital evidence, the procedures and problems of collection and storage will be examined. As a result of this study, I propose a storage method of digital evidence and suggest a means to preserve it semi -permanently so that it can be closer to the real truth pursued in the criminal procedure law. To do this, we study the features of digital evidence and the authenticity of digital photographs, and propose a way to preserve them permanently.

2 Main Subject

2.1 Features of Digital Evidence

Digital evidence consists of a series of signs of 0 and 1. Because it is stored in digital format, it cannot be identified with the naked eye, so it must be changed to be viewable. There is a way to change the screen so that it can be viewed by the monitor, and a method to output it to the paper. However, since all the methods are equally giving the visibility, the information should not be deformed during the change.

In addition, since it is a set of binary numbers consisting of 0 and 1, duplication can be completely replicated with the same value, which means that the original and the copy can be made the same. By making use of these characteristics and creating the same copy as the original and proving that it is the same when used for trial, it gives the unity of the original and the copy so that the original can be preserved and the copy can be given the same power as the original.

Since it is a set of binary numbers, it is possible to perform up-modulation by simply inputting a simple command and it is very easy to delete. Therefore, the value should not change in a series of processes such as collection and analysis of evidence, and it should be able to prove that it has not changed. Due to the intent or mistake of the investigator or analyst, the contents of the evidence can be changed easily. So it requires considerable care and verification.

Recently a capacity of up to 128 Gbytes USB memory is widely used, which is large enough to store 128 videos. It is almost impossible to analyze and extract evidence if the documents are stored in digital form in such USB memory.

Digital evidence can be distributed or hidden globally through a network, such as the Internet. It is difficult to track the crime using the Ransom Way, which is a recent problem. It is difficult to track the crime with international crime including the Republic of Korea. Also, it is required to provide the decryption key for decrypting the encrypted content through the Ransom Way. In the case of bit coin, it is not only difficult to track cyber piracy, but also the flow of funds. Features of digital evidence include non-visibility, easy to duplicate, vulnerability, large capacity, and no borders.

2.2 Acquisition and preservation of digital photographs by investigators

Investigators can be divided into judicial police officers and special judicial police officers. A judicial police officer can carry out all duties including arrest, search, seizure and verification by the duty set forth in Article 197 of the Criminal Procedure Act, and the special law enforcement officer can enforce the disciplinary procedure, and those who have not only provoked but also have the right to investigate, among the administrative officers in the field of many civilian contacts such as orders, labor, etc. In the past, these investigators used the crime scene as a clue to conduct investigation and investigation on the crime scene by mainly photographing and developing sketches or analog photographs. However, recently, due to the popularization of digital devices, almost all investigators use photographs or video shooting equipment.

In this case, only about 10 sheets more or less of the photo records are stitched to the event records, and the average is less than 2 ~ 5%.

Fig. 1. Photo recordings of murders

2.3 How to Give Authenticity of Digital Photographs

The authenticity of digital photographs, the digital evidence, is that the person submitting the evidence must provide a reliable basis to the fact that the evidence is what the submitter claims to be, indicating that the evidence presented is an authentic original copy [1].

Digital photographs have the same characteristics as digital information, so they are the same as the original and the copy is easier to modulate, and there is a high possibility that the people involved may modulate or damage them in a direction favorable to them. In the case of analogue photographs in the past, if the issues constantly raised between investigators and lawyers were forged or distorted on the photographic prints, the forgery and falsification of digital printouts would be easier and more perfect.

On the other hand, in the case of the United States, even there is no witness testimony, and if the process of forming a picture or the credibility of the system is acknowledged, the photograph is allowed as proof by the ‘silent witness theory’ which acknowledges the authenticity of the photograph.

Factors for determining the authenticity of the photographs include : ① evidence to form the time and date of the photo shoot ② whether it has been edited or manipulated ③ the ability and operating conditions of the device to make photographs related to the authenticity and accuracy of the photo ④ the stability of the device, including its safety, the operation of the device, the expertise of the person employed for testing, and ⑤ the statement of the identity of the relevant participant depicted in the photograph.[2]

In other words, it can be said that the accuracy of software and hardware, the existence and conformity of experts, laws, regulations, and rules are similar to those of digital forensics [3].

3 Permanent Storage Method

3.1 How to Interact with Criminal Justice Portal.

Currently, the National Police Agency, prosecutors, and the courts are coworking with electric records of criminal cases such as violation of road traffic laws and drunken driving which has no special dispute.

The purpose of the criminal justice system is to provide the public with transparency and information access rights to the entire process from the proceeding to the end, along with the digitization of the paperless procedure.

It is the **'Criminal Justice portal site'** where all contents of the investigation are opened to the public. For the investigators who are in charge of the actual investigation, the **'Criminal Investigation Network'** is established so that it can be used for the initiation of investigation and the search for related cases. In the course of such a series of procedures, a method of automatically uploading and preserving digital photographs taken by investigators together with the name of the investigator is required from the beginning of the investigation, registration, and report. In particular, if the metadata and hash value are stored together for retrieval, the reliability will be further increased.

Fig. 2. Picture Criminal Justice Portal

3.2 How to work with a special law enforcement officer (VPN)

The **Criminal Investigation Network** is currently a network linking judicial police officers with police stations, public prosecutors' offices, courts, and prisons, and requires special networking or certification procedures for special law enforcement officers. In order to support investigation special law enforcement officers should be given a certificate using VPN.

Especially, since smart phone has digital camera shooting function and moving picture shooting function, it can be a method of authorizing using VPN and uploading a digital photo document when approaching the criminal law.

4 Conclusion

The amount of digital evidence in digital or digital recordings is increasing exponentially. However, in the absence of systematic preservation procedures and methodologies, many digital evidence is being lost. To prevent this, digital photographs and video recordings should be formed from metadata in the database. Through this, authenticity and integrity of photographic records are certified, thereby giving credibility to the visual evidence of digital photographs. In the process of investigation, by revealing the substantive facts, preliminary offenders are provided with preventive effects, will be positioned as a scientific investigation technique.

References

1. O, Kwon.: Study on Foreign Precedent with Digital Photo Trustworthy, IT & Law Study No7, (2013).
2. G. Lee. Digital Forensic with Science Criminal Investigation. Gs InterVision. 11. (2011).
3. 2013GoHab 805, Decision of Fire Prevention Law.

