Review of Evidence Collection and Protection Phases in Digital Forensics Process

Asaf Varol *, Yeşim Ülgen Sönmez *‡

* Dept. of Software Engineering, Faculty of Technology, University of Fırat, 23119, Elazığ/Turkey.

‡ e-mail:yesimulgen123@gmail.com

Abstract- This study reviews crime scene investigation, collection of evidence and protecting evidence phases of digital forensic process based on the research in the literature. Using appropriate methods for collecting and protecting electronic evidence would contribute to digital forensics and information technology law. In order to have effective evidence analysis, the first phases of the digital forensic process need to be completed through appropriate methods. In this study, the main emphasis will be on digital forensics process as well as hardware and software utilized during this procedure.

Keywords- Digital forensics process; collecting evidence; protecting evidence.

1. Introduction

The fundamental purpose of digital forensics can be described as discovering, protecting, collecting, analyzing and presenting legal and electronic evidence that are seen as potential to solve a crime [1, 2]. Digital forensics aim to find digital evidence for numerous cases ranging from identifying the hacker on a hacking case to solving the murder [3].

In digital forensics, the purpose is not to point out a person as guilty or innocent. It aims to present numerical evidences to forensic units in other form as complete and impartial interpretation of the evidence. Determining whether a person is guilty or not will be held by judicial authorities as a result of conveying these evidences to forensic units through digital forensic processes [4].

Some fields of study in digital forensic can be listed as data recovery, data annihilation, data conversion, encryption, decryption, finding under cover files, identifying criminals with the help of IP numbers [5].

2. Digital Forensic Process

Digital forensic phases can be described as processes followed in order to find/analyze/report about forensically important information [6]. Digital forensic phases are listed in the Figure 1 [3, 4, 6, 7]; these phases are: describing evidence, which starts with the crime scene investigation, collecting evidence, protecting evidence, analyzing the evidence, and reporting and presenting the evidence.

There is a starting point for every process [8]. The process can start with an alarm from the attack determination system i.e. Intrusion Detection Systems, suspicious records on the firewall, warnings from the security system on the network, denunciation of an individual, or denunciation of any crime cases [8, 9].

The purpose of value evaluation is to determine whether there will be a detailed investigation process or not [8, 9]. Later, procedures and protocols which will be applied in the crime scene are identified.

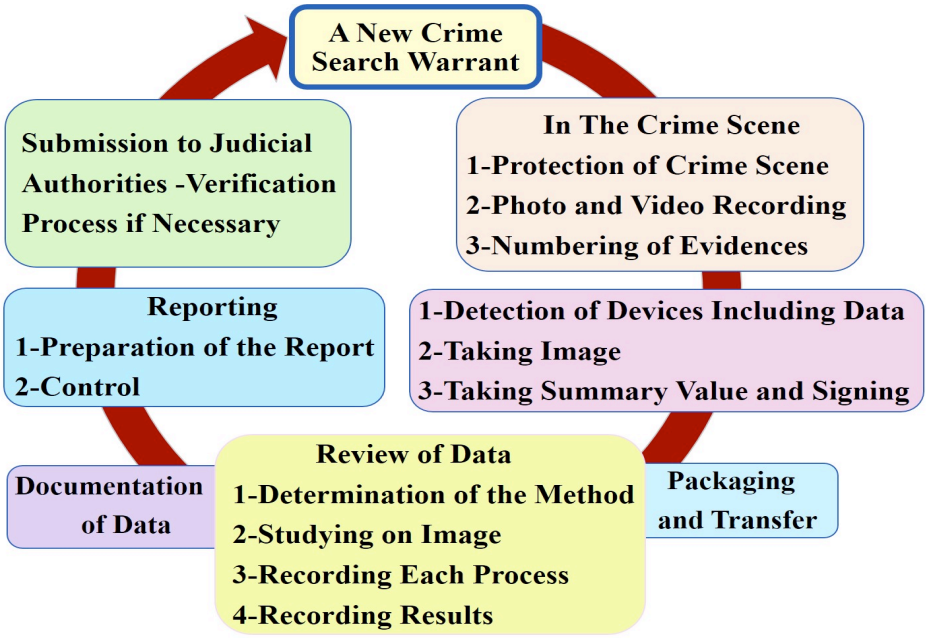

Fig. 1. Digital Forensics Cycle Model [6]

People who are responsible for the security of the crime scene are first responders or digital forensics specialists. Their trainings needed in this subject depend on protocols identifying the crime scene (video and photograph) [8, 9]. Later, collection of data phase in Figure 2 starts.

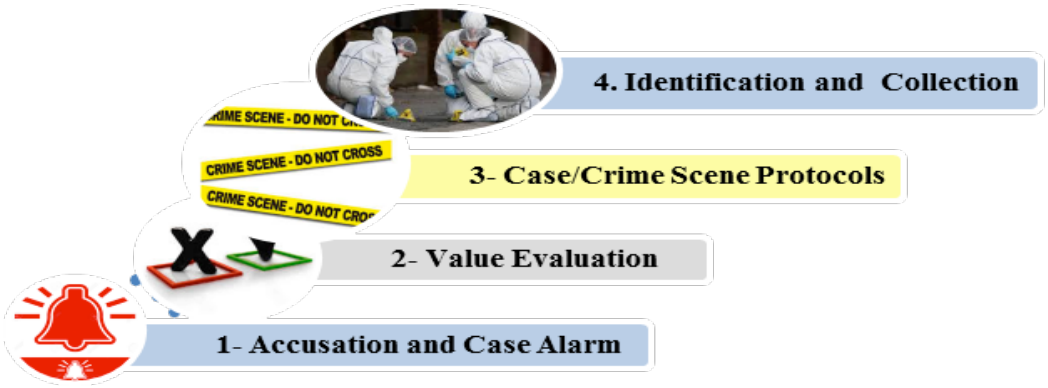

Fig. 2. Phases of electronic evidence collection

2.1. Identification and Collection of Electronic Evidences

Figure 3 shows the steps of crime scene investigation and initial steps of evidence collection [10, 11]. The purpose for experienced researchers is not to collect all virtual or physical evidences. They must decide what needs to be collected.

Then they must create a document and finally perform the action [8]. Having a detailed report for each collected evidence eases their verifiability and starts the chain of custody [8].

Transportation and protection of digital evidence processes are carried out according to the predefined protocol according to the law [12].

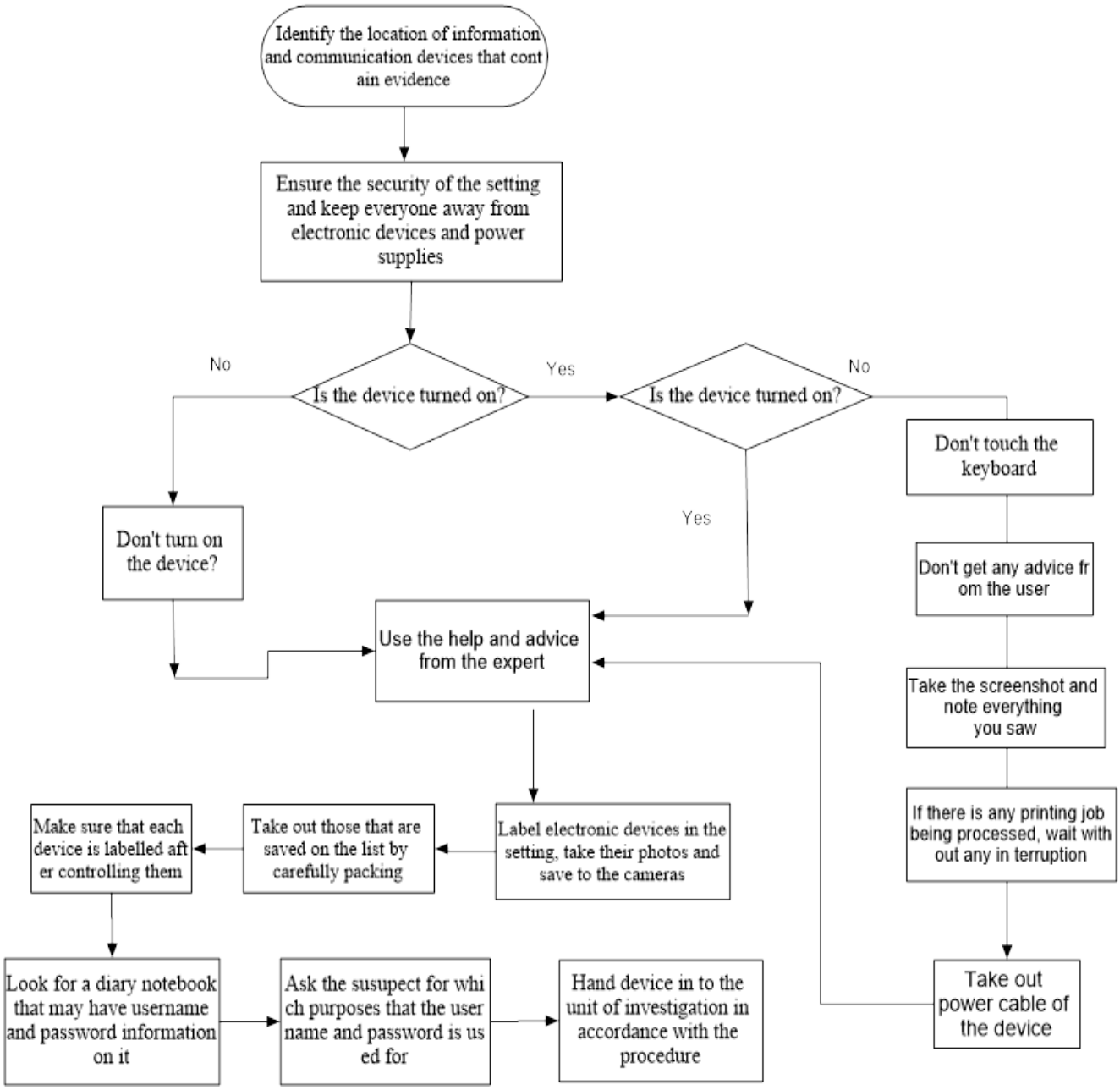

Fig. 3. Crime Scene Investigation Activity Flow Chart [10, 11]

2.2. Protection of Electronic Evidences

Within the scope of protection of evidence, it is required to denote in which situation, where and in which conditions the evidences are collected in the crime scene. In other words, it is required to know the integrity of collected evidences [13]. Integrity of evidence can be actualized through the conscious work of the police force in the phases of protection of evidences. After identification, collection of evidences, they send possible digital evidences to the laboratory for investigation [14]. In Figure 4, the processes used to protect of evidence are shown.

In this phase, there is digital protection and physical protection [8]. Digital protection begins from the first moment of the collection of evidences.

Fig. 4. Protection of Electronic Evidences

It consists of various mechanisms that show that the evidence is not distorted or altered. This process is usually done through using cryptographic techniques.

Physical protection is consisted of carrying the evidences to the location of investigation without any distortion, preserving them in appropriate settings until the court date and ensuring the prevention of any distortion of the evidences while being carried to the court. In these phases, evidences are labeled, appropriately packed and sealed [8].

2.3. Capturing Image

In computer criminalistics, the image (forensic image) is the name of the exact copy that is taken for investigation [3]. It is critical to obtain the copy in a way to include exactly all bits on the hard drive (bit stream back up) [13]. In other words, the content of the copied disk would be obtained as exactly the same [15].

There are two methods of capturing the image. The first is capturing image through hardware, the other is capturing image through software [16].

Hardware image capturing tools obtain the image of the evidence by following the image capturing methods on its embedded operating system through establishing a physical data connection with the original evidence.

The advantages of these products are that they are not needed on any computer and they are used to capture images at the scene [16]. The process of writing on the original evidence is blocked with the features of "Write Block".

Some hardware image capturing devices can be listed as following [11, 16]:

- Image Masster
- Tableu Forensic Duplicator
- Digital Intelligence
- MyKey
- Falcon
- The Rapid Image 7020
- Data Copy King
- BeeCube

There are two hardware products used in digital forensics: a write block device and an image capturing device [11].

In Figure 5, the capturing of the image through Tableau image capturing device with the help of the software in this device without needing any external computer or software is shown.

The image capturing process with a write block device is shown in Figure 6. An image capturing software and computer is needed to capture image through write block device. The differences between the two are reviewed and it is reported that write blockers creates several problems [17].

Fig. 5. Copying Device Named Tableau TD2 [18]

In digital forensics, using hardware write blocking devices presents less risk.

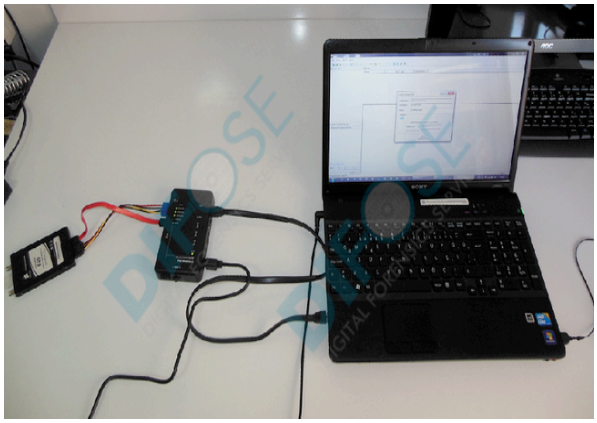

Fig. 6. Write Block Image Capturing Device Named Tableau T35es [18]

After getting connected to the original evidence computer through physical data connection in the image capturing process with image capturing software on the electronic environment, the image of the evidence is captured by following the steps in the image capturing software [16].

These products do not need external "Write Block" devices. In order to preserve the integrity of the original evidence, "Write Block" feature is included in the software and whether the evidence is distorted or not during the copying is determined via checksum values produced by using some verification algorithms (MD5 and SHA1 etc.) as a result of the image capturing process [16]. Some of the software image capturing devices can be listed as below [16]:

- Norton Ghost Imager
- FTK Forensic Imager
- Encase Forensic Imager
- X-Ways Imager
- Helix 3 Pro
- Win image Snapback
- AIR (Automated Image and Restore) and Guymager
- It is possible to capture RAM memory image via Belkasoft Live and Dumpit [19].
- Cellebrite UFED, XRY, Paraben, Tarantula, Flasher Box, Faraday, TULP 2G, Bitpim, Deft, Paraben's Device Seizure, Oxygen Forensics Suite and Caine mobile devices, can extract data from mobile phones, sim cards, GPS devices, navigation devices, tablet computers, and pocket computers at international standards [20].
- Moreover, Linux-based digital forensic devices such as FIREBrick can be used instead of commercial software required devices [21]. Although Paraben and Belkasoft Evidence Centre are used for instant messaging investigations, there are also new solutions being developed for instant messaging [22].

2.4. Write Blocks

Write blocks, which are used for write protection, are software or hardware products that are developed to capture and investigate images by preserving evidence integrity. In case if write blocking is not used, malware such as virus, trojan, etc. can attack the computer during the image capturing process and the data might be written on the evidence and it will loose its integrity [11].

2.5. Hash Algorithm

Hash algorithm, which is used to determine the integrity of evidence, is obtained by multiplying all 0s and 1s on the computer media with a certain algorithm [23, 24].

As a result of image capturing process, there are two different hash values automatically created by the software that is used. ***Acquisition hash*** is the hash algorithm of the original evidence device, whereas ***verify hash*** is the hash algorithm showing that the evidence integrity of the digital material is not distorted after the investigation. These two hash values should be the same. Otherwise, one may claim that the evidence is distorted. Due to the nuncupative principle of "in dubio pro reo" (suspected defendant) in criminal justice law, even if there is evidence showing a committed crime, the suspect can't be punished even if the evidence is accidentally altered [11].

While the hash value is a value that is 32-characters long, consisted of characters including 0-9 and a-f for MD5, it is a value that is 40-characters long consisted of the same characters for SHA1 [24]. The sample MD5 and SHA1 hash values of an image obtained within the scope of a study are given below:

MD5 : e8359ebbe97f3bae584c76971059c35b

SHA-1:
5dbd53e4e7b0f6b8dd19d084af57722da83018e9

In the phase of protecting electronic evidences,

- This sum value is given to both parties after being signed by parties [6],
- Putting evidences in anti-static materials to prevent them being exposed to static electric current [6],
- Putting them separately when packing to prevent them interact with each other [6],
- The most important point for the evidence protection is to use qualified personnel that has adequate knowledge and experience on the subject [6],
- Appropriately recording the data that are in the crime scene but not directly available and can easily fade away (volatile, deleted, idle data, network connections) [6].

In digital forensics, there are different techniques (fuzzy hashing) and new algorithms (mrsh-v2, sdhash) that are being worked on for the correlation of similar files [23]. There are also academic studies conducted on mvHash-B algorithm that is used to identify the similarities between two dataset [25].

3. Recovery

Before starting a complete analysis of the conserved digital evidences, it is necessary to discover deleted, hidden, transfigured data or data that is non-displayable with current operating system or file system. This is called data recovery. This process is not conducted on original evidences, but is implemented on their duplicates (exact copies) [8].

4. Decomposition

The purpose is to bring together the data according to their specific characteristics in order to provide easiness for the research. For instance, since the child pornography cases [26] are usually based on visual digital data, files with the extension of gif, jpeg, etc. are often brought together for investigation [8].

5. Reduction and Organization

Among the collected data, those that are directly related to the subject are vital for a digital forensics investigation. Selection criteria is carefully determined as it can be questioned during the court [8]. It is necessary to organize, group, label reduced data and place them meaningful units. The purpose is to ensure that researchers find and describe the data during the analysis and give reference to them in a meaningful way during the testimonial. For this purpose, a data index is created as well [8].

6. Conclusion

The first two phases of evidence capturing analysis are done through a series of hard drive and software devices whether it is open source or proprietary. These devices are continuously

developing in line with the technology and changes in devices.

Among digital forensics phases, the data analysis phase is supported less. There are only a few software devices available for this phase. It is critical to obtain evidences in an accurate and credible way while analyzing the evidence. Knowing the existing applications of evidence collection and preservation phases in literature, actualizing new methods to apply these processes would make contributions to both digital forensics and information technology law. Reporting in every step, would help law enforcement units to make correct decision from the beginning of the digital forensics process, namely from first crime scene investigation to evidence collection and evidence preservation phases.

7. Acknowledgements

This paper was presented at ISCTurkey 2017.

References

[1] Ş. Sağıroğlu, M. Karaman. "Adli Bilişim". *Telepati,* Vol. 203, pp. 62, August, 2012.

[2] Y. Kim and K. J. Kim, "A Forensic Model on Deleted-File Verification for Securing Digital Evidence". *978—1-4244-5493-8710 IEEE*, 2010.

[3] http://www.ekizer.net. "Adli Bilişim (Computer Forensics)", Latest Access Time for the website is 14 October 2016.

[4] M. Özen, G. Özocak, "Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirinin Hukuki Rejimi (CMK M. 134)". *Ankara Barosu Dergisi*, 2015.

[5] M. Z. Gündüz, Bilişim suçlarına yönelik IP tabanlı delil tespiti- IP-based Evidence Detection, Master Dissertation, University of Fırat 2013.

[6] M. Orta, Bilişim Suçlarında Adli Analiz, Ph.D Dissertation, University of Selçuk 2015.

[7] L. Keser Berber, *Adli Bilişim*. Yetkin Publisher/Ankara, 2004.

[8] http://slideplayer.biz.tr/slide/1918963. Y. Uzunay, "Dijital Delil Araştırma Süreci", Latest Access Time for the website is 14 October 2016.

[9] E. Casey, *Digital Evidence and Compter Crime Scene*. ABD/AP, 2004.

[10] T. Henkoğlu, *Adli Bilişim Dijital Delillerin Elde Edilmesi ve Analizi*, Pusula Publisher/İstanbul, 2014.

[11] Y. Başar, Siber Suç Soruşturmalarında Adli Bilişim İncelemeleri, Master Dissertation, University of Kocatepe 2015.

[12] R. Adams, V. Hobbs, G. Mann. "The Advanced Data Acquisition Model (ADAM): A Process Model for Digital Forensic Practice". *Journal of Digital Forensics, Security and Law, JDFSL*. Vol. 8, No. 4, pp. 25-48, 2013.

[13] R. J. Vacca, *Computer Forensics*, Second Edition, Charles River Media, IBSN: 1–58450–389–0, 2005.

[14] M. Kaygısız, *Kriminalistik Olay Yeri İnceleme Suç Yeri ve Delil Güvenliği*, Adalet Publisher, 2007.

[15] http://www.chip.com.tr/forum/Bilisim-Suclarinin-Delillendirilmesi_t8007.html. "CHIP Online", Latest Access Time for the website is 6 October 2016.

[16] H. Aydoğan, Adli Bilişim'de Yeni Elektronik Delil Elde Etme Yöntemleri, Master Dissertation, Institute of Police Academy Security Sciences 2009.

[17] G. Kessler, G. Carlton. "A Study of Forensic Imaging in the Absence of Write-Blockers". *Journal of Digital Forensics, Security and law, JDFSL*, Vol. 9, No. 3, pp. 51-58, 2014.

[18] http://www.difose.com.tr/blog/index.php/testler/89-solid-state-disk-adli-kopyasi. "DIFOSE Digital Forensics Services", Latest Access Time for the website is 6 November 2016.

[19] A. Ekim, Bilişim Suçlarında Sayısal Delillerin Toplanması, Muhafaza Edilmesi, İncelenmesi ve Raporlanması, Master Dissertation, University of Marmara 2013.

[20] M. Ukşal, Mobil Cihazlarda Adli Bilişim, Master Dissertation, University of İstanbul Bilgi 2015.

[21] L. Tobin, P. Gladyshev. "Open Forensic Devices", *Journal of Digital Forensics, Security and law, JDFSL.*, Vol 10, No. 4, pp. 97-104, 2015.

[22] R. V. Voorst, M.-T. Kechadi, N.-A. Le-Khac. "Forensic Acquisition of IMVU: A Case Study," *Journal of Digital Forensics, Security and Law, JDFSL*, Vol. 10, No. 4, pp. 69-78, 2015.

[23] F. Breitinger, İ. Baggili. "File Detection on Network Traffic Using Approximate Matching", *Journal of Digital Forensics, Security and Law, JDFSL*, Vol. 9, No. 2, pp. 23-36, 2014.

[24] M. S. Kılıç. *Elektronik Deliller ve Yapısal Özellikleri*. Edit: H. Çakır and M.S. Kılıç. *Adli Bilişim ve Elektronik Deliller*, Seçkin Publisher/Ankara, 2014.

[25] D. Chang, S. K. Sanadhya, M. Singh. "Security Analysis of MVHASH-B Similarity Hashing". *Journal of Digital Forensics, Security and Law, JDFSL*, Vol. 11, No. 2, pp. 21-34, 2015.

[26] J. Eggestein, K. Knapp. "Fighting Child Pornography: A Review of Legal and Technological Developments*"*.

Journal of Digital Forensics, Security and Law, JDFSL,
Vol. 9, No. 4, pp. 29-48, 2014.