Do We Have Full Control Over Integrity in Digital Evidence Life Cycle?

Jasmin Cosic[1], Miroslav Baca[2]
[1] *IT Section of Police Administration, Ministry of Interior, Bihac, B&H*
[2] *Faculty of Organization and Informatics, University of Zagreb, Croatia*
E-mail(s): jascosic@bih.net.ba , miroslav.baca@foi.hr

Abstract. *Chain of custody plays an important role in digital forensic investigation. Contact with different variables occurs through a life cycle of digital evidence. To prove chain of custody, investigators must know all details on how the evidence was handled every step of the way. „Five WS (and one H) "must be applied.*

Life cycle of digital evidence is very complex, and at each stage there is more impact that can violate a chain of custody. This paper presents a life cycle of digital evidence and problems with implementation of chain of custody in digital investigation. The authors also warn of certain shortcomings in terms of answering specific questions, and give some recommendation for further research. New framework based on Five WS will be presented.

Keywords. digital evidence, digital forensic, chain of custody, digital evidence integrity, digital evidence manipulating.

1. Introduction

There are so many definitions of digital forensic and digital evidence. One of many definitions is „digital forensic can be defined as the application of science and engineering to the legal problem of digital evidence" [16]. According to Pollit and Whiteledge [13] „digital forensic is the science of collecting, preserving, examining, analyzing and presenting relevant digital evidence for use in judicial proceedings".

Notion of digital evidence means „any constitution or relevant digital data enough to prove crime in computer and network storage media is one kind of physical evidence, including patterns with text, picture, voice and image. The properties of undifferentiated copy, original authors hard to authenticate and data verification can be also called computer evidence or digital evidence, which is stored on computer and network storage media with electromagnetic means. In another word, computer storage media or electromagnetic storage on network can be used for crime evidence" [4].

In all phases of forensic investigation, digital evidence is susceptible to external influences and coming into contact with many factors. Legal admissibility of digital evidence is the ability of those evidence to be accepted as evidence in a court of law. The evidential weight of digital evidence can only be safeguarded if it can be proven that the records are accurate i.e. who they were created by and when and that no alteration has occurred.

In order for the evidence to be accepted by the court as valid, chain of custody for digital evidence must be kept, or it must be known who exactly, when and where came into contact with evidence in each stage of the investigation. The phrase "chain of custody" refers to the accurate auditing control of original evidence material that could potentially be used for legal purposes [17]. Some authors use a term „chain of evidence" instead chain of custody. The purpose of testimony concerning chain of custody is to prove that evidence has not been altered or changed through all phases, and must include documentation on how evidence is gathered, how was transported, analyzed and presented. Knowing the current location of original evidence, is not enough for court, there must be accurate logs tracking evidence material at all time. Access to the evidence must be controlled and audited.

To prove the chain of custody, we must know all the details on how the evidence was handled every step of the way. The old formula used by police, journalists and researchers - Who, What, When, Where, Why, and How - "Five Ws" (and one H) [11] can be applied to help in digital forensic investigation:

- WHAT? What is the evidence?
- HOW? How did investigators get the evidence?
- WHEN? When was it collected and used?
- WHO? Who handled it?
- WHY Why that person handled it?
- WHERE? Where it traveled, where was it stored?

This paper focuses on the phases of computer investigation and life cycle of digital evidence; we also address relevance of chain of custody and most critical factor that will determine the integrity of digital evidence.

2. Process of collecting digital evidence

Over the years, several authors proposed several digital forensic investigation models. *Lee`s model* [6] named "The Scientific Crime Scene Investigation Model" proposed 4 stages (recognition, identification, individualization and reconstruction). According to *Casey* [5] there are also 4 stages in process of forensic investigation. Those phases are: recognition, preservation, classification and reconstruction. *DFRWS* (Digital Forensic Research Workshop has developed a model with the following steps: identical, preservation, collection, examination, analysis, presentation and decision [12].

Kruse and Heiser [10] model includes 3 stages, evidence acquiring, authenticating and analyzing. *America`s Department of Justice – DOJ* proposed a model with 4 stages – collecting, examination, analyzing and reporting and finally *Ciardhuain model* [6] is an extended and most complete model that consists of awareness, authorization, planning, notification, search and identification of evidence, collection, transportation, storage, examination, hypothesis, presentation, proof/defense and dissemination. In digital forensic process, all the phases are important, but first two phases – collecting and preservation are critical because if investigators or other person who work with evidence made a mistake in this phase, everything which has been done in that process is useless. Court will not accept evidence if not collected in a lawful way. In this paper we will discuss about process of collecting and maintenance of digital evidence.

Process of collecting digital evidence is not so simple and investigators or first responders (emergency personnel) must know what they are supposed to do in the first contact with evidence [1]. This is not trivial, if we know that just one misstep can be fatal. For example, if first responders-personnel shut down "live" computer with Windows XP operating system, over 50 files will be changed and 5 new files created at next boot [3]. This means that a moment of inattention is enough to lose evidence and breach its integrity.

There are several noteworthy developments toward standardization in this field. First organization that was established in the mid-1990s "to ensure the harmonization of methods and practices among nations and guarantee the ability to use digital evidence collected by one state in the courts of another state" [9] was IOCE – International Organization of Computer Evidence. IOCE proposes several principles related to digital evidence and digital forensic. The Federal Crime Laboratory Directors group formed SWGDE - Science Working Group on Digital Evidence in 1998. SWGDE published many best practices documents, guidelines, recommendation and technical notes. These documents have no technical details but can be used to be a framework to develop some models.

DFRWS - Digital Forensic Research Workshop in 2001 was a workshop, and then continues to bring academics and practitioners together in an informal environment.

Every of these organizations have principles and procedures with no details on how to implement a recommendation.

3. Dynamics - personnel and integrity of digital evidence

Process of collecting digital evidence must begin in a lawful way. In other words, if there is a forensic investigation, competent prosecution or court must issue the order to initiate an investigation, or if there is a corporate internal investigation, management or supervisory board must agree with investigation. In both cases, approval must be in a written document.

In different countries is a different situation, in relation to who first comes into contact with digital evidence. Somewhere there are specialized units (first response forces) that are trained on how to behave with this type of evidence, while in some countries this job is done by law enforcement personnel (police officer) who are not trained to do it.

According to IOCE [9], when it is necessary for a person to access original digital evidence, that person should be trained for the purpose. In

many cases this is not possible, because forensics is a very complex science, and requires a high level of expertise to work with the evidence.
List of personnel who can act on the digital evidence:

- First responders
- Forensic investigators
- Court expert witness
- Law enforcement personnel
- Police officers (crime inspectors)
- Victim
- Suspect
- Passerby

Each of the above-mentioned persons can affect evidence in particular situation, and therefore it is very important to know the answer to the question " *who* is coming into contact with the evidence" ?

Fig. 1 illustrates the impact of human factor in all investigation stages. It also emphasizes the most critical things in the first phase of digital forensic investigation.

As we can see in the figure, a life cycle of digital evidence is very complex, and at each stage there are more impact that can violate a chain of custody.
If the digital evidence is used in international investigation, this life cycle is more complex and is difficult to maintain chain of custody.

4. Other variables that affect integrity of digital evidence

There are a number of recommendations for the digital signing of evidence by human factor that came into contact with it [7].

The most common method is a digital signature.These methods use asymmetric cryptography, the signer uses a secret key to generate a digital signature, and anyone can then validate signature generated by using the published public key certificate of the signer. This method has many disadvantages as the complexity, tardiness, keys can be compromised, certificate can expire, private key must be

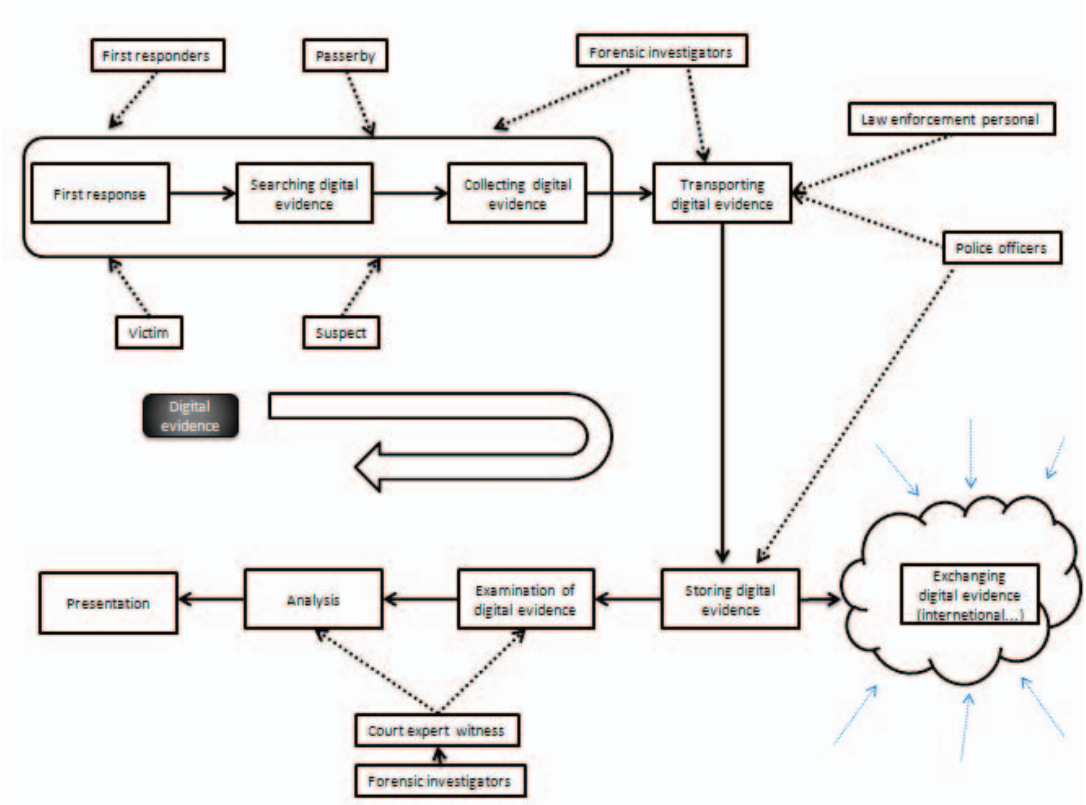

Figure 1. The Impact of human factor in phases of forensic investigation

protected.
Therefore authors prefer a biometrics to sign digital evidence.
The Integrity of digital evidence ensures that the information presented is complete and unaltered from the time of acquisition until its final disposition.[SWGIT]
According to the recommendations of SWGIT [2] there are few methods for demonstrating integrity: hashing function, visual verification, digital signature, written documentation, checksum (CRC), encryption, watermarks and proprietary methods.
Hosmer [8] recommended a checksum method with CRC16, CRC32, one-way hash algorithm, SHA-1, MD5, MD4, MD2 and digital signature RSA, SA and PGP in order to prove integrity of digital evidence.

Today most forensic application use some type of hashing or checksum algorithm to verify integrity of digital evidence. Two of the most commonly hashing algorithm are MD5 (Message Diggest 5) and SHA1 (Secure Hash Algorithm 1). Because of reported forced collision with MD5 and SHA0 [15], NIST [14] and some organization recommended to use a multiple hash values, to reduce the risk.
Some forensic examiners use SHA 2 family: SHA-224, SHA-256, SHA-384 and SHA-512 , higher-bit algorithms.
Now, when we know *who* come into contact with digital evidence, and we are sure that hashing function is correct, next important variable is time.

At any time, we must have an answer, when we are asked by the court or lawyer, when the contact with evidence happened?
Investigator or other personnel, who will eventually present his/her investigation hypothesis to the court, must be able to accurately describe not only those who handle the evidence, but *when* and *where*, and *what* happened regarding this. If he/she is not able to explain and prove that, the court will not accept evidence and the whole investigation is in vain.

Time, when digital evidence is discovered and collected is vital to reconstructing event in digital forensic investigation. We need to know when evidence is discovered, at what time evidence is accessed, when is transported and exchanged. These variables are important for investigation.
Good method of proving the existence of digital evidence in a certain time is a timestamp. A timestamp is recorded representation of a specific moment in time. Digital timestamp is a recorded representation of specific moment in time in a digital format. This representation is stored in a digital media [18] and can be stored in digital evidence.

Every file can contain a timestamp; one investigation can include thousand, ten thousand of timestamps. A timestamp always depends on the setting of the clock that generates it, and this problem has been studied by several researchers. Proving the integrity of digital evidence with timestamp and hashing function are very good methods.[7]
Now, when we know who and when came into contact with digital evidence, according to "chain of custody" it is important to know the place *where* the contact occurred.

There is a lack of research on this topic, and organizations (IOCE, SWGDE, DRWS, etc) only propose to document where was the evidence discovered, collected, archived, stored and transferred. There are no details on how to implement this proposal.

5. Concept of proposed "DEMF" frameworks to ensure the security of a chain of custody

In Fig. 2 we present a concept of frameworks to ensure the security of a chain of custody based on Five WS (and one H). We propose use of Biometrics characteristic for digital signing (Who), Timestamp for adding a time (When), use some of web services (Google map example, GPS coordinate) or some RFID device for geo location (Where) and hashing and asymmetric encryption for securing digital evidence.
This DEMF ("Digital Evidence Management Framework") can be presented like a function of secure management that consist of few factors:

DEMF = f {fingerprint _of _file, *//what*
biometric_characteristic, *//who*
time_stamp, *//when*
gps_location,} ; *//where*

Use of all these factors in the right way provide safe and secure chain of custody, to ensure that digital evidence will be accepted by the court.

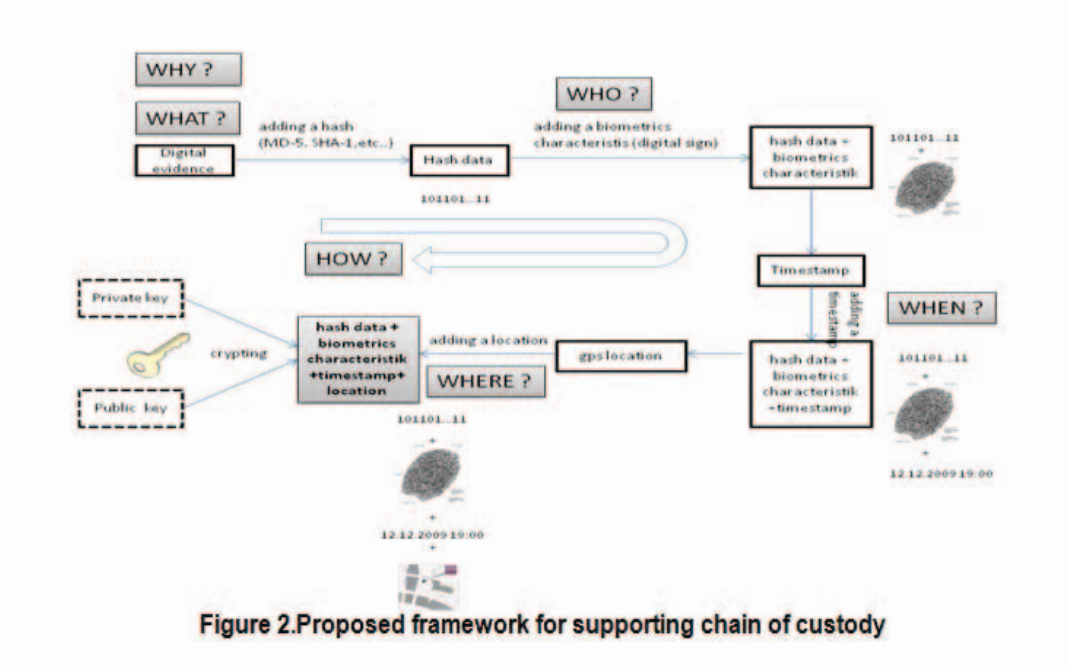

Figure 2.Proposed framework for supporting chain of custody

6. Conclusion and further research

In all phases of forensic investigation, different profiles of personnel come into contact with digital evidence.

Through the entire lifecycle of digital evidence, there are threats that can affect its integrity and thus in the end, the court's decision. The goal of this paper is to show a weaknesses that are a consequence of the lack of answers on a few questions (who, when, where, why, what and how).

Further research will be focused on problem where is digital evidence processed, and how technical develop and implement a proposed secure DEMF , which will help investigators to safely handle evidence, and store a hash of files in a digital form, biometrics signature, timestamp, and characteristics of places where all evidence was accessed.

7. Acknowledgements

Shown results came out form the scientific project Methodology of biometrics characteristics evaluation (016-0161199-1721) and practical project Multiple biometric authentication using smart card (2008-043), supported by the Ministry of Science, Education and Sport, Republic of Croatia.

8. References

[1] Baca M, Introduction in computer security (on Croatian). Zagreb: Narodne novine; 2004

[2] Best Practices for Maintaining the Integrity of Digital Images and Digital Video. http://www.fbi.gov/hq/lab/fsc/backissu/april2008/standards/2008_04_standards01.htm#2 [12/9/2009].

[3] Brown CLT. Computer evidence, collection and preservation. Charles River Media; 2006

[4] Casey E. Handbook of Computer Crime: Forensic Science, Computer and the Internet. Academic Press; 2000

[5] Casey E. Digital Evidence and Computer Crime 2nd Edition. Elsevier Academic Press; 2004

[6] Ciardhuain SO. An extended model of cybercrime investigation. Elsevier Information Security Technical Report. Elsevier Advanced Technology; 2003

[7] Cosic J, Baca M, Improving chain of custody and digital evidence integrity with timestamp. Proceeding of the 33rd International Convention information and communication technology, electronics and microelectronics ;

MIPRO 2010 (in press).
[8] Hosmer C. Proving the integrity of digital evidence with time. IJDE-International Journal of Digital Evidence. Spring; 2002
[9] IOCE principles. http://www.ioce.org/core.php?ID=5 [12/19/2009]
[10] Kohn M, Eloff JH, Oliver MS:Framework for Digital Forensic Investigation, ISSA 2006 from Insight to Foresight Conference; 2006
[11] Media Awarenes Network. http://www.media-awareness.ca/english/resources/special_initiatives/wa_resources/wa_shared/tipsheets/5Ws_of_cyberspace.cfm [12/20 2009]
[12] Perumal S. Digital Forensic Model Based on Malaysian Investigation Process. IJCSNS VOL.9 No.8; 2009
[13] Pollit M, Whiteledge A. Exploring big Haystacks. Data Mining and Knowledge Management.Advances in Digital Forensic II.IFIP; 2006
[14] NIST – National Institute of Standards and Technology, http://www.nist.gov, [12/19/2009]
[15] NSRL and Recent Cryptographic News: : http://www.nsrl.nist.gov/collision.html [12/18/2009]
[16] Sammes A, Jenkinson B. Forensic Computing A Practitioners Guide. Springer-Verlag, New York; 2000
[17] Yaeger R. Criminal Computer Forensic Management. InfoSec Conference, USA;2006
[18] Willassen S: Hypothesis-based investigation of digital timestamps. IFIP. Advances in Digital Forensics IV.Springer;2008