# A Framework to (Im)Prove „Chain of Custody“ in Digital Investigation Process

**Jasmin Ćosić**
IT Section of Police Administration
Ministry of Interior of Una-sana canton
502.V.bbr br.2, Bihać , B&H
jascosic@bih.net.ba

**Miroslav Bača**
Faculty of Organization and Informatics
University of Zagreb
Pavlinska 2, 42000 Varaždin, Croatia
miroslav.baca@foi.hr

**Abstract**. *Traditionaly, a chain of custody (chain of evidence) refers to the chronological documentation , or paper trail, showing storing, controling, transfer, analysis and handling with evidence. Chain of custody plays very important role in digital forensic investigation process. To prove chain of custody, investigators must know all details on how the evidence was handle.„Five W`s (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. Proper chain of custody must include information on how evidence is collected, transported, analyzed, preserved, and handled with.*
*In most countries there is no standard unique protocol or procedures for this.*
*In this paper authors will presents a digital evidence management framework – DEMF, which can im(prove) chain of custody of digital evidence in all stages of digital investigation process. In proposed framework will be used a SHA-2 hash function for digital fingerprint of evidence, biometric characteristics for authentification and identification a personal who handled with evidence, a digital trusted timestamp for determining a “right” time when evidence is discovered or when is accessed to evidence and a gps coordinates for determining a location of evidence. 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.*

**Keywords.** Computer forensic, digital evidence, chain of custody, integrity of digital evidence

## 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“ [1]. According to Pollit and Whiteledge [2] „digital forensic is the science of collecting, preserving, examining, analyzing and presenting relevant digital evidence for use in judicial proceedings“. Digital forensics is no longer associated only to a laboratory in police and security agencies, but it is also used outside that area. Some area where digital forensic play important role are insurance companies, banks and corporate [3].

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 [5]. The phrase "chain of custody" or "chain of evidence" refers to the accurate auditing control of original evidence material that could potentially be used for legal purposes [6]. 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) [7] can be applied to help in digital forensic investigation. 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.

According to Vanstone [8], digital integrity is "the property whereby digital data has not been altered in an unauthorized manner since the time it was created, transmitted, or stored by an authorized source". Scientific Working Group of Imaging Technology define that "The integrity of digital evidence ensures that the information presented is complete and unaltered from the time of acquiring until its final disposition".

There are several adapted methods for digital signing a evidence in order to (im)prove its integrity: [9]

- CRC (Cyclic Redundancy Check)
- Hash function
- Digital signature
- Timestamp
- Encription
- Watermarking

Every function have a advantage and disadvantage, and can be used in combination [9] .

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 .[5]

# 2 Concept of proposed "DEMF" frameworks to ensure the security of a chain of custody

In Fig. 1 we present a high view of proposed concept of frameworks to ensure the security of a chain of custody based on Five W`s (and one H). We propose to use a SHA-2 function for fingerprint of evidence, a biometrics characteristic to authentification and identification for digital signing (Who), trusted time stamping for adding a time (When), use some of web services (GPS coordinate and google maps) or some RFID device for geo location (Where) 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*
biometrics_characteristic, *//who*
time_stamp, *//when*
gps_location,} ; *//where* [5]

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.

Let`s see how this framework work ?

On first step it should be emphasized that we never use original digital evidence, we use a fingerprint of evidence. Function for calculate a fingerprint in DEMF will be a SHA-2 hash function.

We will not use a SHA-0/SHA-1 because of cryptographic attack (Collision and/or Preimage attack).

After successful login to the system first thing that happened in framework is calculating a fingerprint of evidence – a hash function. There is no size limit of digital evidence (file) for which we want to calculate a hash. We can use one file, group of file or some type of archive (zip, rar, tar, etc.). Hash function SHA-2 will give a fixed size value (224/256 bits, depend we use SHA-224 or SHA-256 or 384/512 if we use a SHA-384 or SHA-512 hash function). Because of length of hash size it is recommended to use SHA-256/224 function. Now he have a hash value of digital evidence –a fingerprint.

On next step, we must perform a authentication on a system to identify and give an answer on question "who is handle with evidence" ? For this purpose the good method is use a biometric characteristics. It can be a fingerprint, iris image or face. With this method can be done a authentication and identification of person who handle with digital evidence. Prerequisite for this is that we must have a template database of all person who handled with evidence. It must include followed person:

- First responders
- Forensic investigators
- Court expert witness

- Law enforcement personnel
- Police officers (crime inspectors)

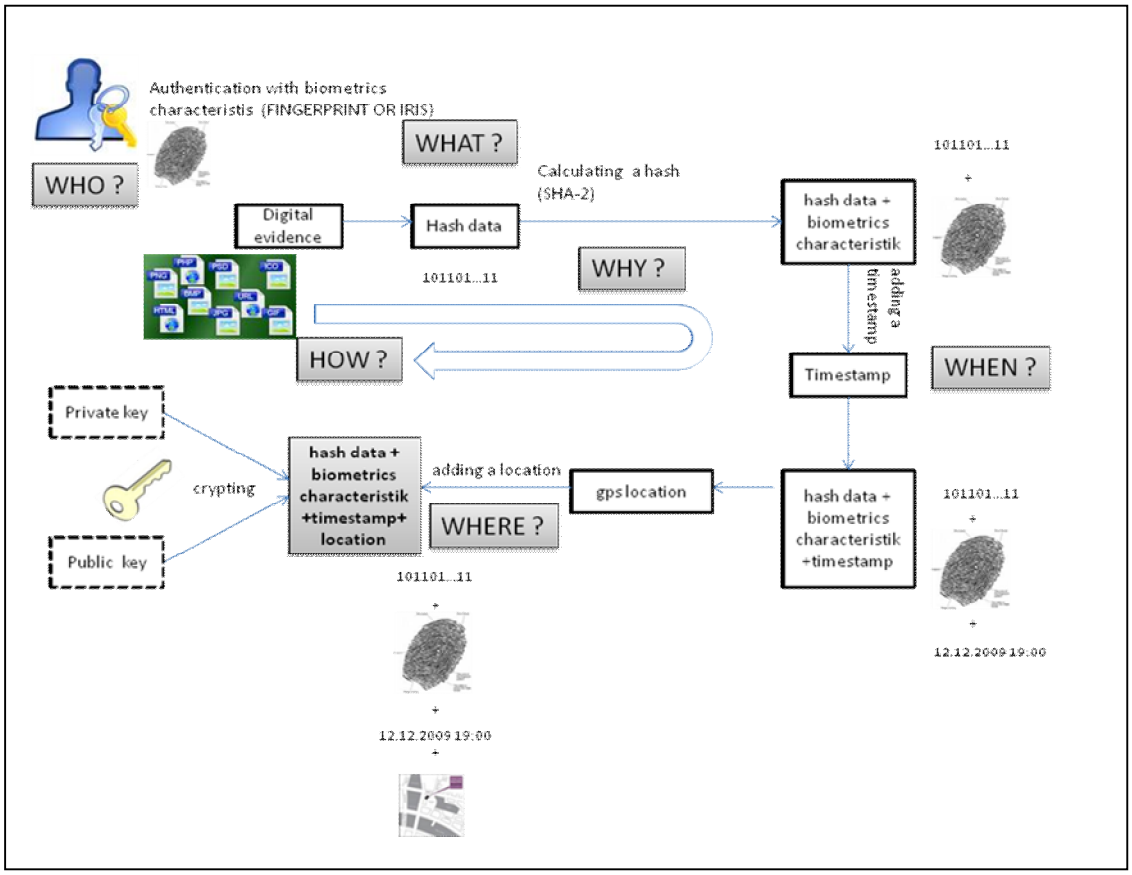


Figure 1 High definition view of DEMF

This is not a very big problem today, considering that most countries already have a biometric personal document (ID card, driving license, passports, etc.) and database with citizens bio-characteristics. In process of using biometrics characteristics must be defined a strictly procedure for security and data protection including a personal privacy.

Next very important thing on this process is knowing a right time. What time we must know ? A time when evidence is discovered and when is accessed to evidence by the other person. Because of known problem with dealing with time and time sources, authors purpose a digital timestamping with known trusted time source.

Some authors [10] states 3 steps that we must do in order to effectively use digital evidence to prove the motif, opportunity and means of cybercrimes:

1. Tracebility to Legal Time Source
2. Time Distribution
3. Source Digital Time stamping

Weil and Boyd [11] advocate to use of correlating methods for time stamp stored on target computer that were created by other clocks (e.g. time stamp in dynamically generated web pages).

Authors [9] proposed that method for this phase can be a "trusted time stamping". RFC 3161 standard define that trusted time stamp is a time stamp issued by a trusted third party (TTP) acting as a time stamping authority (TSA) [8]. When we accessed to digital evidence, a framework sends a request to the TSA to get a certificate with trusted time stamp. In this process we must have a access to the external TSA system, or we can develop a interior system with TSA infrastructure. It is essential to mention that in this kind of "time system" must be a "external auditors" acting as witness.

Now we know a "right time" of accessed and handled with evidence.

Next important thing in forensic process is knowing a *right location* where is handled with digital evidence. Today most law enforcement agencies have some type of evidence handling system that are unchanged from 1950s years. The system are an single room or rooms. In some countries agencies

uses a bar code to tracking evidence, but in most cases a paper chain of custody is primary.
In USA today some agencies uses a RFID (Radio Frequency Identification) to track a evidence in his life cycle. This is a very good method, but problem that there appears is deal with privacy and "right to privacy". With RFID we can track a digital evidence, but we can`t get a coordinates (right location) of place. For this reason some authors [12] recommended to use a Global Positioning System (GPS) for evidence collection and investigation purposes. GPS technology and its functionality has changed over the years, and today most newest electronic devices (mobile phones, PDA, smart phones, camera and other embedded systems) have integrated some version of GPS (integrated gps chip, assisted gps etc.). This system can be used for determination accurate location where digital evidence is discovered, and where is handled with it. At the end of process we have a SHA-2 hash value of digital evidence with biometrics characteristics, time stamp and gps location. For strongest security we propose a asymmetric encryption. Digital evidence and obtained value will be encrypted with private key received from Certification Authority (CA) and stored for further use. All process is presented on Fig.1.

# 3 Conclusion and future work

In his research authors have deal with a conceptual framework for digital evidence management and chain of evidence in forensic investigation process. It`s presented a conceptual DEMF ("Digital Evidence Management Framework") on high level view. With this framework it can be implemented a secure, reliable and useful system which will enable a secure chain of custody of digital evidence.
Future work will be based on implementing this framework in real environment and testing his functionality.

# References

[1] Sammes A, Jenkinson B: Forensic Computing A Practitioners Guide. Springer-Verlag, New York; 2000

[2] Pollit M, Whiteledge A: Exploring big Haystacks. Data Mining and Knowledge Management. Advances in Digital Forensic II.IFIP; 2006

[3] Ćosić J, Bača M: Computer forensic-broad aspects of its application, INFOTEH-JAHORINA,B&H, Vol. 9, Ref. E-VI-9, p. 857-860, March 2010.

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

[5] Ćosić, J., Bača, M. Do we have a full control over integrity in digital evidence life cycle, Proceedings of ITI 2010, 32nd International Conference on Information Technology Interfaces, Dubrovnik/Cavtat, pp. 429-434, 2010

[6] Yaeger R: Criminal Computer Forensic Management. InfoSec Conference, USA;2006

[7] Media Awarenes Network. http://www.media-awareness.ca/english/resources/special_initiatives/wa_resources/wa_shared/tipsheets/5Ws_of_cyberspace.cfm [12/20 2009]

[8] S.Vanstone, P. Van Oorschot,, & A. Menezes: Handbook of Applied Criptografy, CRC Press, 1997

[9] Ćosić, J., Bača, M. (Im)proving chain of custody and digital evidence integrity with timestamp, MIPRO, 33rd International Convention on Information and Communication Technology, Electronics and Microelectronics, Opatija, 171-175, 2010

[10] Hosmer C: Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, Spring, 2002, Vol.1, Issue 1

[11] Willassen S: Hypothesis based investigation of Digital Time stamp, IFIP, Advanced in Digital Forensic IV, pp.75-86, 2008

[12] Strawn C: Expanding the Potential for GPS Evidence Acquisition, Small Scale digital evidence Forensic Journal, Vol.3, No1., 2009