Abstract - The integrity of digital evidence plays an important role in the digital process of forensic investigation. Proper chain of custody must include information on how evidence is collected, transported, analyzed, preserved, and handled with. There are several adapted methods for evidence digital signing to (im)prove the integrity of digital evidence. Most forensic tools and applications use a certain kind of hashing algorithm to allow investigators later to verify the disk or image integrity. In this process there is a problem of binding integrity, identity and date and time of access to digital evidence.

In this paper, the authors will present a valid time stamping method to sign a digital evidence in all stages of digital investigation process. Time stamp will be obtained from the secure third party (Time Stamp Authority). It will be used to prove the time when the staff access the evidence in any stages of forensic investigation.

I. INTRODUCTION

Chain of custody and integrity of digital evidence play a very important role in the digital process of forensic investigation, due to the fact that in every phase forensic investigators must know where, when and how the digital evidence was discovered, collected, handled with, when and who came in contact with the evidence, etc. Proper chain of custody must include documentation with answers to all these questions. If one of these questions remains unanswered, the chain of custody is compromised and disrupted. In this case, when presenting evidence in court, if one link was missing in the chain of evidence, the court would not accept the evidence as relevant. The whole investigation process would be futile.

The most common question that remains unanswered in the presentation of digital evidence is: “Who, when, where and for which reason came into contact with digital evidence?” The most sensitive variable is the “time of contact” with digital evidence. Digital evidence can be one file with or without an extension, few files, one partition on a hard disc, the whole hard disc, USB flash memory device, CD/DVD/Blue Ray discs and any other removable media.

Whether the forensic investigation refers to some of the removable media or hard disc, the aim of our investigation and what we investigate is a computer file. We must always make completely identical “bit to bit” copies of original files. When the original digital evidence circulates through its phases, or when passing through all stages of digital investigation process, the staffs who handles it often changes. We must document not only the changes but every time of contact with the evidence as well.

II. CHAIN OF CUSTODY AND LIVE CYCLE OF DIGITAL EVIDENCE

Chain of custody may be defined as “A road map that shows how evidence was collected, analyzed, and preserved in order to be presented as evidence in court” (John Vacca, P-154) [1]. Chain of custody plays a very important role in digital investigation process. This is a phrase that refers to the accurate auditing and control of original evidence material that could potentially be used for legal purpose. Knowing the current location of the evidence is not enough; there should be accurate logs tracking the movement and possession of evidence material at all times [2]. Investigator must know how to answer certain questions in the whole forensic investigation process:

1. What is digital evidence?
2. Where was digital evidence discovered, collected, handled and/or examined?
3. Who came into contact with digital evidence, handled it, and discovered it?
4. What’s the reason for using the digital evidence?
5. When the digital evidence is discovered, accessed, examined or transferred?
6. How is digital evidence used?

Proper chain of custody must include documentation on how data is gathered, transported, analyzed, preserved, and handled with (paying special attention to, for example, international evidence). This information is important in the verification of electronic data since it can be easily altered if proper precautions are not taken. Maintaining a proper chain of custody is important to the one who preserves data, as well as authorities who may
want to pursue legal action [1]. Adoption of the chain of custody would help an investigator to prove that the incriminating evidence was not destroyed or any external evidence planted.

III. DIGITAL EVIDENCE INTEGRITY

According to Vanstone [3], 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”. The integrity of digital evidence ensures that the information presented is complete and unaltered from the time of acquiring until its final disposition. [SWGIT]

There are several adapted methods for evidence digital signing in order to (im)prove its integrity. Today most forensic tools and applications implement some type of checksum or hashing algorithm to allow investigators later to verify the disk or image integrity [4]. A cryptographic hashing function or algorithm has the following technical characteristics [Table 1]

<table>
<thead>
<tr>
<th>Method</th>
<th>Length</th>
<th>Description</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyclic redundancy checks:</td>
<td></td>
<td></td>
<td>Very simple to use</td>
<td>Non secure hash function</td>
</tr>
<tr>
<td>CRC 16</td>
<td>16 bit</td>
<td>Circular Redundancy Check – CRC often used in file transfer to verify that the data transfer was successful.</td>
<td>Very fast</td>
<td>Problem with message analysis</td>
</tr>
<tr>
<td>CRC 32</td>
<td>32 bit</td>
<td></td>
<td>Small data in output</td>
<td>It’s easy to generate other messages that result in the same CRC</td>
</tr>
<tr>
<td>CRC 64</td>
<td>64 bit</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cryptographic hash function:</td>
<td></td>
<td></td>
<td>It's easy to compute the hash value for any given message</td>
<td>Collision and Preimage attack , except SHA</td>
</tr>
<tr>
<td>MD2</td>
<td>128 bit</td>
<td>Hashing function – establishing mathematical calculation that generates a numerical value based on the input data. This numerical value is referred to as the hash value.</td>
<td>Secure hash function</td>
<td>224/256 and SHA 384/512 [5]</td>
</tr>
<tr>
<td>MD4</td>
<td>128 bit</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MD5</td>
<td>128 bit</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SHA1</td>
<td>160 bit</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SHA224/256</td>
<td>224/256</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SHA384/512</td>
<td>384/512</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Digital signature</td>
<td></td>
<td></td>
<td>Binding identity to the integrity</td>
<td>Very slow</td>
</tr>
<tr>
<td>Time stamp</td>
<td></td>
<td></td>
<td>Bind date and time with integrity</td>
<td>Very complex to implement</td>
</tr>
<tr>
<td>Encryption</td>
<td></td>
<td></td>
<td>Very secure</td>
<td>Very slow Complex to implement and maintain</td>
</tr>
<tr>
<td>Watermarking</td>
<td></td>
<td></td>
<td>Very secure and simple to use</td>
<td>User cannot significantly alter some files without sacrificing the quality or utility of the data.</td>
</tr>
</tbody>
</table>
IV. USING TIME STAMP FOR SIGNING DIGITAL EVIDENCE

There are many definitions of a time stamp. In the real world, a time stamp can represent some moment in time; in the computer world (digital world) the time stamp represents a specific moment of time but in digital format. Time stamp and digital time stamping play a very important role in the digital forensics, because there is a need for knowing the time of certain moments in the investigation process.

It is very important to know the answer to the question which we can be asked in the courtroom: “When was the digital evidence accessed, how long the staffs have been in touch with the evidence? Next question could be: „How long can we prove the integrity of the digital evidence that we signed” [7]. Time is an important factor to determine a question. We must prove the integrity of digital evidence. We need to know the right time of the digital evidence being accessed. Here a big problem is a trusted source of time, due to the fact that in real and digital world time always depends on the setting the clock that generates it. For example, if we use a personal computer whose clock is wrong, we will get a wrong time stamp. Because of that, the time cannot be completely reliable. In this case time stamp cannot be used as a vital factor to reconstructing events in the digital forensics.

Problem of digital time stamping has been the subject of several researches. Hosmer [7] emphasizes the use of time to prove the integrity of digital evidence, and states the 3 steps that we must do in order to effectively use digital evidence to prove the motif, opportunity and means of cybercrimes:

- Step 1: Traceability to Legal Time Source
- Step 2: Time Distribution
- Step 3: Source Digital Time stamping

Weil [2002] and Boyd [2004] advocate the use of correlating methods for time stamps stored on target computer that were created by other clocks (e.g. time stamps in dynamically generated web pages) [8]. In their research of clock synchronization in computer networks, Schatz, Mohay and Clark [9] suggest that clock drift can be mitigated by correlating time stamps stored in web cache of the web page with record obtained from web servers.

There is a lack of research in using a time stamp to improve the integrity of digital evidence, having in mind the fact when the human factor (the staff) access the evidence. There is a list of staff who can handle the digital evidence: first responders, forensic investigators, court expert witness, law enforcement personnel, police officers, victim, suspect, passerby, etc.

Each of the above mentioned people can affect evidence in particular situation, and therefore it is very important to know who, when and where comes into contact with the evidence.

Time when digital evidence is discovered and collected, and the fact who comes into contact with it is vital to reconstructing and proving integrity. We also must know when digital evidence is transported.

A. Trusted Time Stamping

According to the RFC 3161 standard [10], a trusted time stamp is a time stamp issued by a trusted third party (TTP) acting as a time stamping authority (TSA). It is used to prove the existence of certain data before a certain point (e.g. contact with digital evidence) without the possibility that the owner can backdate the time stamps. We can use multiple TSAs to increase reliability and reduce vulnerability.

Due to the problems with the time stamp implementation and synchronization of internal clock, and the impossibility of proving these facts to the court, the authors will introduce the use of "trusted time stamp" and the third party service providers.

There is a lot of TSA in the world, in some country a few, and in some (e.g. Croatia) just one [11]. We can use services of trusted Time Stamping Authority to prove the consistency and integrity of digital evidence in every stage of its existence. It is particularly important to have recorded every moment of time when the digital evidence is being accessed. In another situation, chain of custody would be terminated and this would affect the outcome of the investigation. This is very important in international exchange of digital evidence and international digital investigation.

When a Time Stamp Authority (TSA), which we contact to get a Time stamp, proceeds our request, there are a few “external auditors” acting as witness. In some case there is one, in some two auditors [12] which document the chain of evidence.

The process of obtaining a Time stamp from the TSA, which will prove the existence and contact with the digital evidence by all staff at any time, consists of several steps divided in two separate parts:

On the client side:
- Process of making a unique identifier, fingerprint (creating a hash) of digital evidence (SHA-256, MD5, etc.)
- Process of sending a fingerprint to a Time Stamp Authority
- Process of verification with Public Key and local storing

On the side of TSA:
- Process of getting a official time from server
- Process of adding a time stamp to fingerprint
- Process of protecting (signing) with Private Key
- Process of sending a digital signature to the client

These processes are illustrated in the Figure 1.

Let’s see what happened in this process? First, investigators (or other staff who handled digital evidence) must generate a unique identifier – fingerprint of a digital evidence. In this process some of the previously mentioned methods, hash function or, for better security, multiple hash functions can be used. It is proposed to use a high-secured SHA/MD algorithm.

After generating a hash of digital evidence, these “few bits” are being sent to the “third party” - Time Stamp Authority.
It is important to mention that only the fingerprint (hash) is transmitted to the TSA, never the original file. TSA cannot see the actual document (not any file). Next what happens is that the TSA on received hash adds a time stamp, calculate new hash and digitally signing a file with protected signing key.

The purpose of this document is to show a trusted time stamping method to signing a digital evidence in every stage of digital investigation process.

TSA then sends this file back to the client (investigator), who has another pair of signing key. In the next stage of forensic investigation exactly the same process happens. On this way we can prove the time of digital evidence movement at any stages of forensic investigation.

V. CONCLUSION AND FURTHER RESEARCH

Because of the expansive development of ICT, especially internet and digital communications, movement of evidence is much greater today than ever before. As digital evidence is in bit/byte form, it is very easy to transfer it to another side of the world in a few seconds [13]. One of the most important thing in forensic process is maintenance of digital evidence chain of custody.

Time stamp will be available from the secure third party (Time Stamp Authority) and will be used to prove a time when the staff access the evidence in any stage of forensic investigation. Further research will be focused on the next problem of the chain of custody - where is digital evidence processed, and how can a secure “Digital Evidence Management Framework” be developed. That will help investigators to safely handle evidence, and store a hash of files in a digital form, as well as biometric signature, time stamp, and characteristics of places where all evidence was accessed.

Figure 1: The process of time stamping digital evidence in all stages of digital forensic investigation process
ACKNOWLEDGEMENTS

The presented data are from 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.

REFERENCES