Digital Chain of Custody

Matthew N.O. Sadiku¹, Adebowale E. Shadare², and Sarhan M. Musa³

¹,² Department of Electrical & Computer Engg., Prairie View A&M University, Prairie View, TX 77446, United States
³ Department of Engineering Technology, Prairie View A&M University, Prairie View, TX 77446, United States

DOI: 10.23956/ijarcsse/V7I6/01619

Abstract: Digital chain of custody is the record of preservation of digital evidence from collection to presentation in the court of law. This is an essential part of digital investigation process. Its key objective is to ensure that the digital evidence presented to the court remains as originally collected, without tampering. The chain of custody is important for admissible evidence in court. Without a chain of custody, the opposing attorney can challenge or dismiss the evidence presented. The aim of this paper is to provide a brief introduction to the concept of digital chain custody.

Keywords: digital chain of custody, chain of digital evidence

I. INTRODUCTION

In today’s digital world, the number of cybercrimes is on the rise due to an ever-increasing number of users of digital and information technologies. Banking, insurance, large corporations, and social media have been the prime targets of cybercrime. Increasing cybercrime forces the law enforcement agent to find more accurate evidence. The crimes can be disclosed through a series of digital forensic activities [1]. In the process of forensic investigation, the integrity of digital evidence is very important.

A chain of custody (CoC) (or chain of evidence) refers to the process of validating how any kind of evidence has been gathered, tracked, and protected on its way to a court of law. It guarantees that the data presented is “as originally acquired” and has not been tampered with and is authentic prior to admission into evidence [2]. Without a chain of custody, the evidence is worthless. To prove chain of custody, you may need to provide a form on the details on how the evidence was handled every step of the way. Sound chain of custody is a procedure for performing a chronological documentation (or paper trail) toward evidence. This documentation should be on how the data was gathered, transported, analyzed, and preserved for production. A chain of custody failure or broken chain of custody (mishandling digital evidence) can cause a litigation defeat.

In both civilian and military courts, proponents are required to verify the chain of custody of tangible evidence before its admittance at trial [3]. Conventional approach for chain of custody cannot be used to handle digital evidence due the peculiar characteristics of digital evidence.

II. ELEMENTS OF DCoC

There are five important elements in a digital chain of custody (DCoC) process [4]:

- **Characteristics**: These include the sources such as PC, digital devices, and cloud.
- **Dynamics**: These include people who are involved in the process, i.e. suspect, victim, law professionals, forensic investigators. Chain of custody has always been a people process.
- **Factors**: These answer the following questions: What is the digital evidence? Where are the digital evidence? Who manage with digital evidence? Why do it? When digital evidence is handled? How is handled with digital evidence? These questions can be answered using fingerprints, biometrics, time stamp, GPS locators, set of procedures, and best practices.
- **Institutions**: These will include law enforcement, military, security agencies, bank, insurance, corporate institutions, and individuals.
- **Integrity**: Techniques for ensuring integrity of digital evidence include CRC (Checksum Redundancy Check), digital signature, encryption, timestamp, and watermarking.

III. ISSUES

Handling the chain of custody for digital evidence is harder than the handling of physical evidence. It involves recording of metadata information as well as issues of access control and security for all the handling digital chain of custody [5]. Quite often, the chain of custody software is insufficient by itself to guarantee the courts the quality and authenticity of those digital evidences.

The security aspects of authenticity, integrity, and confidentiality are important in law enforcement proceedings. Authenticity can be defined as prevention, detection, and recovery requirements. Integrity is the condition of being whole and unaltered. Confidentiality refers to information that needs to be treated secret from unauthorized entities [6].

Legislations on criminal procedures in most nations were enacted before cybercrimes appeared and were not taken into account. Digital chain of custody requires proper training from the experts. Without it, a digital chain will produce the same shortfalls of its physical counterpart and people will be trying to cut corners to get stuff done.
IV. CONCLUSION

Maintaining that chain of custody is essential for the credibility of your digital evidence and eventual testimony. A compromised chain can undo a legal proceeding and lay waste to years of investigation. Legal professionals should be familiar with digital chain of custody so that they can challenge opponents with invalid digital evidence. They should be able to collect useful information, compatible, consistent and connected along the chain of custody.

REFERENCES

ABOUT THE AUTHORS

Matthew N.O. Sadiku (sadiku@ieee.org) is a professor at Prairie View A&M University, Texas. He is the author of several books and papers. He is a fellow of IEEE.
Adebowale Shadare (shadareadebowale@yahoo.com) is a doctoral student at Prairie View A&M University, Texas. He is the author of several papers.
Sarhan M. Musa (smmusa@pvamu.edu) is a professor in the Department of Engineering Technology at Prairie View A&M University, Texas. He has been the director of Prairie View Networking Academy, Texas, since 2004. He is an LTD Spring and Boeing Welliver Fellow.