Defining a Standard for Reporting Digital Evidence Items in Computer Forensic Tools

Hamda Bariki, Mariam Hashmi, and Ibrahim Baggili

Advanced Cyber Forensics Research Laboratory
College of Information Technology
Zayed University, Abu Dhabi, UAE
Ibrahim.Baggili@zu.ac.ae

Abstract. Due to the lack of standards in reporting digital evidence items, investigators are facing difficulties in efficiently presenting their findings. This paper proposes a standard for digital evidence to be used in reports that are generated using computer forensic software tools. The authors focused on developing a standard digital evidence items by surveying various digital forensic tools while keeping in mind the legal integrity of digital evidence items. Additionally, an online questionnaire was used to gain the opinion of knowledgeable and experienced stakeholders in the digital forensics domain. Based on the findings, the authors propose a standard for digital evidence items that includes data about the case, the evidence source, evidence item, and the chain of custody. Research results enabled the authors in creating a defined XML schema for digital evidence items.

Keywords: digital evidence item, reports in forensic tools, digital forensics, standard report.

1 Introduction

Today, digital forensics plays a critical role in investigations. The broad use of digital devices in daily life activities make them an important source of information about people, thus causing them to become a strong potential source of evidence. Anson and Bunting (2007) claimed that if an incident takes place, one of the most important sources of evidence will be the digital devices at the scene. Investigators are using digital forensics to extract digital evidence from electronic devices. Digital forensics typically follows a four step process, which includes: acquisition, identification, evaluation, and presentation as shown in Figure 1 (Anson & Bunting, 2007). This research focused on the last step of digital forensics process, which is presentation.

Practitioners may need to present their investigative findings to courts of law. Typically, investigators include their findings on digital evidence items, which are known as data objects associated with such digital evidence at the time of acquisition or seizure (Anson & Bunting, 2007). Digital evidence items comprise a myriad of computer based data, such as word documents, jpeg files, or any data that could reside on a storage medium. Some digital forensics software tools implement a reporting functionality which allows forensic examiners to generate reports regarding digital

I. Baggili (Ed.): ICDF2C 2010, LNICST 53, pp. 78–95, 2011.

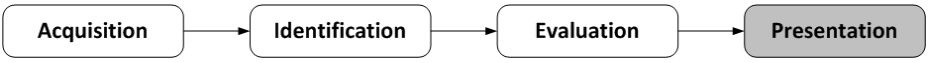

Fig. 1. Digital forensics process

evidence items found. Reports generated from forensic tools are sometimes included with the official investigation report that is presented to attorneys.

2 Problem Statement

Nowadays, investigators typically use multiple computer forensic tools during their investigation process to verify their findings, and cover all possible evidence items. For that reason, as shown in Figure 2, investigators may end up with multiple reports on digital evidence items, generated using different tools. The lack of standards in the reporting function of computer forensic tools may hinder the computer investigation process. When an investigator uses different forensic tools, he/she may face difficulties in integrating evidence items from software-generated reports into the official investigation report that could be presented to attorneys or clients.

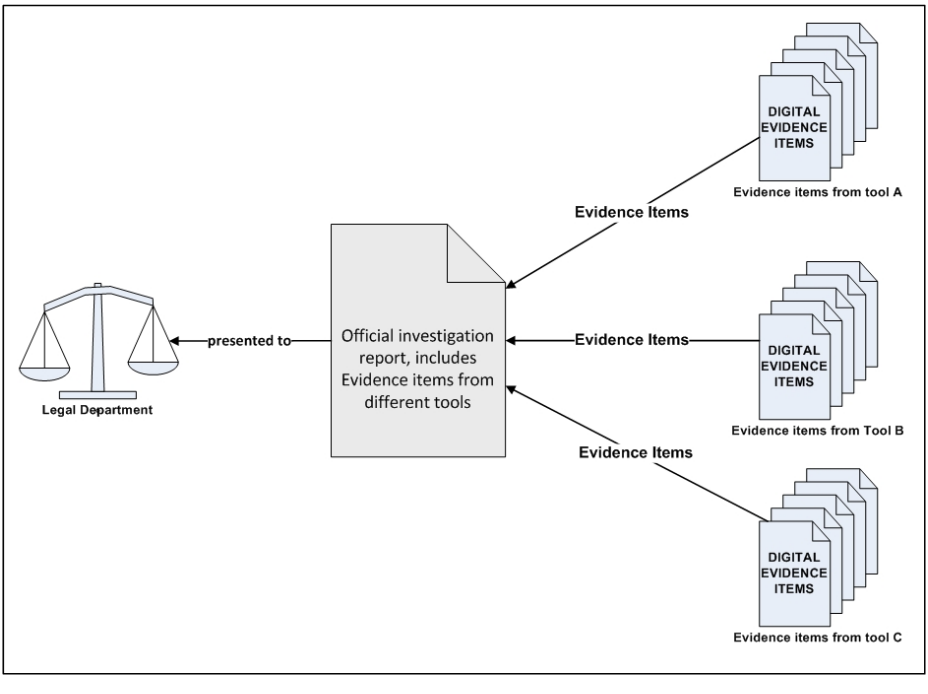

Fig. 2. Digital investigation report

3 Related Literature and Software

Reporting is critical in any investigation. It is the method for communicating information about the results, and findings of the investigation process. When it comes to