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.

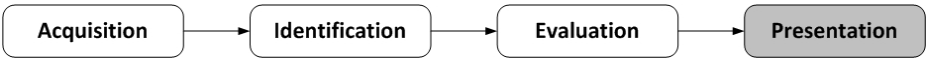

Fig. 1. Digital forensics process

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.

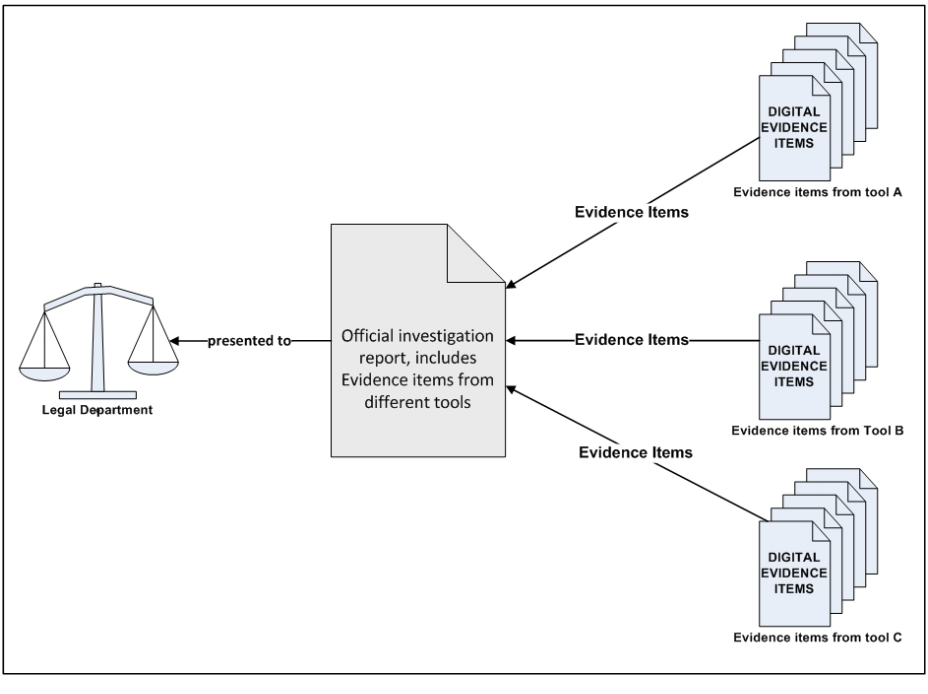

Fig. 2. Digital investigation report

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

computer and digital investigations, reporting still preserves the same importance if not even more. Nelson et al. (2008) explained that a report must be written by the forensic examiner to illustrate the findings from a digital forensics examination. In this report, the examiner needs to explain his investigation process, and findings. This report can be used to present evidence in the court, or to support issuing a search warrant. It can also be used to communicate expert opinion.

To perform computer forensic tasks, one needs software tools to gain access, and uncover information that is not clearly visible such as files that are deleted, stored in slack space or unallocated space, and files that are hidden or encrypted. Furthermore, many tools may be needed to perform investigative tasks such as forensic imaging, searching, documenting, decrypting and much more, which are needed to successfully, critically, and correctly analyze digital storage media. With many computer forensic software tools, such as FTK, ProDiscover, iLook, and EnCase, log files and reports are generated when performing an investigation. These reports could be attached to an official investigation report that is presented to the attorney. The content and the format of these reports will not be the same.

Log reports record the activities the investigator performed during the examination, which can be useful for repeating the examination if needed. A built-in report generator creates a report containing bookmarked evidence items. This report is then issued by an investigator to exemplify examination findings. Different tools generate reports in different formats, such as word processing documents, HTML web pages, and PDF files. Nelson et al. (2008) explained that although these forensic software reports illustrate what, and where evidence is found, it is the examiner's responsibility to explain the significance of the evidence recovered, and define any limitations or uncertainty that applies to the findings.

3.1 Commercial Computer Forensic Tools

Some of the computer forensic tools that generate reports are: FTK, EnCase and ProDiscover. These tools were examined because of their wide use in digital investigations, and their availability to the authors.

AccessData Forensic Toolkit (FTK version 1.71). The FTK version surveyed in this research was 1.71. FTK contains a full suite of password recovery tools, drive and media wipers, a registry viewer and other useful products. Although FTK .v1.71 comes with its own disk imaging software, it can read the images produced by Encase, Linux DD, SafeBack (up to version 2.0), SMART .s01 and others.

FTK can generate reports in different formats like (.xml, .rtf, .wml, .docx). FTK reports include exported files, custom logos, and external information such as hash lists, search results, and password lists. FTK produces an XML report detailing all the digital evidence items that were bookmarked during the investigation process. A simple XSL style sheet is provided to present this information in a clear and readable manner, and the style sheet can be customized to reflect an investigator’s data needs (Nelson et al., 2008).

ProDiscover Forensic Tool (version 5.5). ProDiscover offers forensic examiners an integrated Windows application for the collection, analysis, management, and reporting of computer disk evidence. ProDiscover version 5.5 forensic edition, supports all

Windows based file systems including FAT 12/16/32 and NTFS Dynamic disks in addition to file systems such as SUN Solaris UFS and Linux Ext 2/3. ProDiscover .v5.5 is completely scriptable using the ProScript interface, and Perl. ProDiscover enables practitioners to locate data on a computer disk while protecting evidence, and creating evidentiary quality reports for use in legal proceedings (ProDiscover, n.d.).

EnCase Forensic Tool (version 6). EnCase is software developed by a company called Guidance Software. It is one of the most common tools used in computer forensics. In this paper, the authors reviewed EnCase version 6. EnCase has an organized user interface that simplifies the viewing of media contents using different views. These views include picture gallery, image evidence, hex, and file tree views. EnCase can also be used to acquire evidence. EnCase provides investigators with a single tool, capable of conducting large-scale investigations from beginning to end (Glendale, 2010).

EnCase has a number of automatically generated reports that can be created. Below are some example reports:

- Listing of all files and folders in a case
- Detailed listing of all URLs and corresponding dates and times that web-sites were visited
- Document incident report that helps create the required documentation relevant during the incident response process
- Detailed hard drive information about physical and logical partitions

3.2 Standardization

In digital forensics, researchers have described the importance of a standard, open format for digital evidence provenance, both for description and comparison of particular pieces of evidence, as well as for tool interoperability and validation (Levine et al., 2009). Moreover, Pladna (2008) proposed a standard digital evidence bag for a large organization to perform more efficient collection of data. Marcella et al. (2007) explained that a digital forensics laboratory accreditation standard, and standard operating procedure checklists are intended to act as guides to the uniform process of conducting digital forensics examination in a precise and accurate manner. The Common Evidence Format Working Group (2006) proposed defining a standard format for storing and transmitting digital evidence by using metadata so that it can be processed efficiently by multiple tools and parties, can ensure evidence integrity, and effective case management. Garfinkel et al. (2006) designed a file format for a forensic image called the Advanced Forensics Format (AFF). This format is both open and extensible. Like the EnCase format, AFF stores the imaged disk as a series of pages or segments, allowing the image to be compressed for significant savings. Unlike EnCase, AFF allows metadata to be stored either inside the image file or in a separate, companion file. Garfinkel et al. (2006) declared that, although AFF was specifically designed for use in projects involving hundreds or thousands of disk images, it works equally well for practitioners who work with just one or two images. Additionally, if the disk image is corrupted, AFF's internal consistency checks are designed to allow the recovery of as much image data as possible (Garfinkel, et al., 2006).

4 Methodology

In this research, the authors utilized an incremental procedure to develop a standard for reporting digital evidence items in computer forensic tools. There are different types of digital forensics evidence like storage media evidence, memory evidence, network evidence, and mobile device evidence. As a first step, the authors limited their research scope to generated reports for computer forensic evidence items, willing to expand their approach to cover other digital forensics evidence items in their future work.

Primarily, the authors surveyed the reporting function of computer forensic software tools, which were: FTK .v1.71, ProDiscover .v5.5 and Encase .v6 as presented in the literature and software review to formulate the data requirements for digital evidence items. Next, the authors analyzed their findings, and presented them in a tool comparison table. The next step was to conduct a questionnaire targeted at the digital forensics community to verify the data requirement findings for digital evidence items. Finally, based on the findings, and the views of the digital forensics community, the authors defined XML Schema for a proposed XML standard format for reporting digital evidence items in computer forensic tools. This XML standard could be used to facilitate the merger of digital evidence items into a single report by digital forensics practitioners when utilizing multiple computer forensic tools.

5 Discussion and Result

5.1 Computer Forensics Tool Survey

FTK .v1.71, ProDiscover .v5.5 and EnCase .v6 all generate reports related to digital evidence items. Each of these tools include distinct data about digital evidence items in a report. The authors studied reports generated from these tools, and found that these reports contain some common data about digital evidence items. The common data were: File Name, Checksum (e.g. MD5 and SHA1), Created Date, Accessed Date, Modified, Date, File Size, Is Deleted, Comments, Full Path and Extension of the evidence file. Additionally, FTK and EnCase share some data regarding digital evidence items like File Type, Category, Logical Size, Physical Size, Hash Set, and File Offset. On the other hand, ProDiscover has some data about digital evidence items that is not included in FTK and EnCase as demonstrated in Table 1. Some tools cover vast data about digital evidence items like EnCase, and some focus on identifying the cluster, sector, MD5, SHA1, and hidden files like FTK. These differences may suggest a reason behind using different tools in computer forensic examination. Table 1 summarizes the content of the reports generated from ProDiscover, FTK and EnCase.

5.2 Chain of Custody

While surveying the reports generated using computer forensic tools, the authors noticed that the tools did not cover data related to the chain of custody for digital evidence items. Chain of custody is an effective process of documenting the complete journey of the evidence during the life of a case. Rand and Loftus (2003) in their article "Chain of Custody Procedure" declared the chain of custody as a legal term

Table 1. Report data in computer forensic tools

Data	ProDiscover .v5.5	FTK .1.71	EnCase .v6
File Name	✓	✓	✓
Checksum	✓	MD5, SHA1, Hash Set	Hash Value, set, category and properties
Created Date	✓	✓	✓
Accessed Date	✓	✓	✓
Modified Date	✓	✓	✓
File Size	✓	Logical & Physical	Logical, Initialized & Physical
Is Deleted	✓	✓	✓
Comments	✓	✓	✓
STD Info Updated	✓		
MFT Updated	✓		
Bates Num	✓		
Cluster Chain	✓		
Is Preview Available	✓		
Is EXIF Available	✓		
Full Path	Included with file name	✓	✓
Alias		✓	
Extension	Included with file name	✓	✓
File Type		✓	✓
Category		✓	✓
Children		✓	
Descendants		✓	
Encrypted		✓	
Recycled		✓	
Carved		✓	
Indexed		✓	
Sector		✓	
Cluster		✓	
Alternate Name		✓	
Duplicate		✓	✓
Read Only		✓	
System		✓	
Hidden		✓	
Item Number		✓	
Compressed		✓	
KFF		✓	

Table 1. (*continued*)

Bad Extension		✓	
File Offset			✓
Signature			✓
Description			✓
Entry Modified			✓
File Acquired			✓
Initialized Size			✓
Starting Extent			✓
File Extents			✓
Permissions			✓
References			✓
Physical Location			✓
Physical Sector			✓
Evidence File			✓
File Identifier			✓
Code Page			✓
Short Name			✓
Unique Name			✓
Original Path			✓
Symbolic Link			✓
Is Internal			✓
Is Overwritten			✓
Notable			✓
Excluded			✓

that refers to the ability to guarantee the identity, and integrity of the sample (or data) from collection through reporting of the test results. It is a process used to maintain, and document the chronological history of the sample (or data) and the integrity of the evidence (Devine, 2009).

For litigation purposes, regulatory agencies must be able to prove the legal integrity of all samples, and data introduced as evidence (Devine, 2009). Additionally, Rand and Loftus (2003) declared that verification of who has possessed the samples, and where the samples have been is easier if one follows chain-of-custody procedures.

Since there is no way to know in advance which samples, and data may be involved in litigation, the investigator should always follow chain-of-custody procedures whenever samples, and data are collected, transferred, stored, analyzed, or destroyed (Steen & Hassell, 2004). John Petruzzi, director of enterprise security at Constellation Energy explained that, the investigator needs to deal with everything as if it would go to litigation, therefore chain of custody is considered an important process to apply during investigation procedures (Petruzzi, 2005). According to Nelson et al. (2008), an evidence custody form usually contains the following information:

- Case Number
- Investigation Organization
- Investigator
- Nature of Case
- Location evidence was obtained
- Description of evidence
- Evidence recovered by
- Date and time
- Change of custody log (purpose of change, method of transfer, released by, released date, received by, received date, hash value)

At this point, the authors were able to gather the data requirements to define the standard that could be used in reporting digital evidence items in computer forensic tools. However, in order to validate these findings, the authors conducted a questionnaire which is delineated in the section that follows.

5.3 Forensic Community Opinion Questionnaire

To verify the findings regarding the reporting of digital evidence items by computer forensic tools, and the chain of custody, a questionnaire was conducted to acquire the opinion of the stakeholders in the digital forensics community. This questionnaire targeted knowledgeable, and experienced stakeholders in the digital forensics domain. The survey was sent to various lists that contained reputable academics in the area of digital forensics, as well as certified and accredited practitioners. The authors ended up with n=139 responses, of which n=116 were complete.

Respondent demographics. The survey results illustrate that 61% of those who participated were above 40 years old and 29% were between 30 and 40 years old. 91% of the respondents were males. Most of them have higher education degrees, where 61% of those who participated in the study had Bachelor or Diploma degrees, 36% had master degrees and 24% had PhD/doctoral degrees. Regarding the respondents experience in digital forensics, the results indicated that most of the respondents are knowledgeable in the field, where out of 135 responses, 104 respondents had more than five years of experience in the digital forensics field. Additionally, the results showed that most respondents are familiar with using computer forensic software tools, where 135 respondents out of 139 were familiar with computer forensic tools.

The above demographics indicate that the respondents were knowledgeable in the computer forensic domain, and have a reasonably mature level of experience in using computer forensic tools.

Reporting in Computing Forensic Tools. Figure 8 shows the opinion of those respondents regarding reporting in computer forensic tools illustrating the average of the responses. The results can be summarized as follows:

- Reporting function is important in computer forensic tools
- It's common to use more than one computer forensic tool in an investigation
- Reports generated from the tools contain different data structures
- There is a need for a reporting standard in computer forensic tools

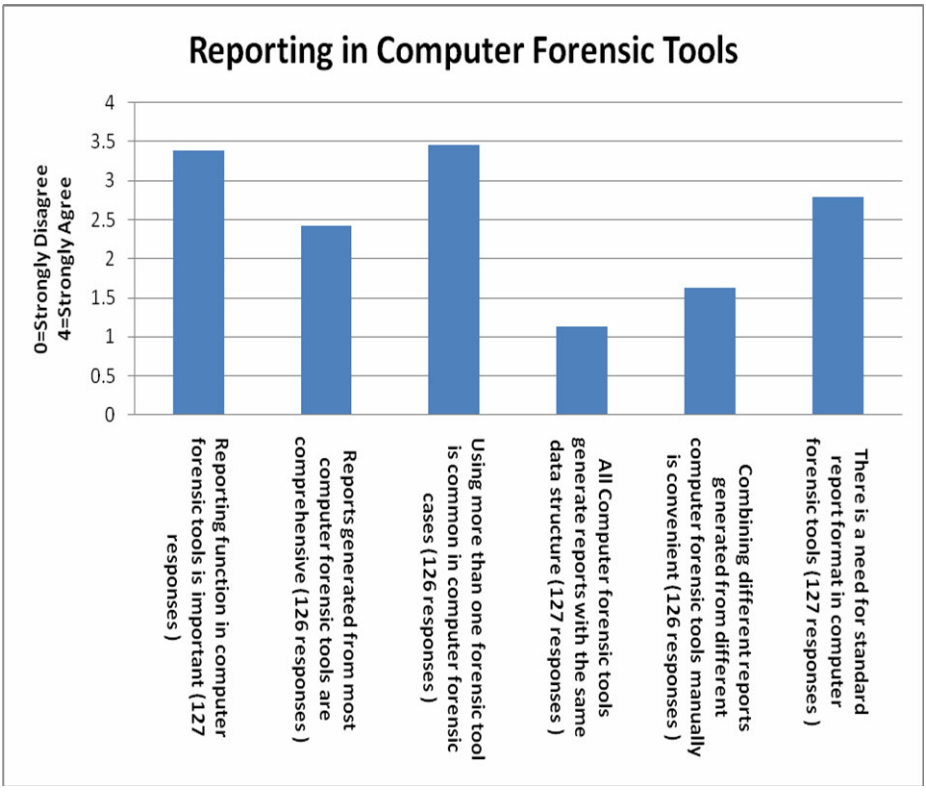

Fig. 3. Reporting in computer forensic tools

Figure 9 illustrates the respondents' opinion regarding the most comprehensive computer forensic tools in reporting evidence items. Out of 123 responses, 45 respondents selected reports combined from multiple tools. Some of those who selected other tools mentioned tools like iLook and X-Ways, and some mentioned that they are using a self-prepared report by adding extracted data from the tools.

Reporting Digital Evidence. The last part in the survey was about the content of the reports, and was divided into four sections, which were: case information, evidence source information, items of interest and chain of custody. The survey questions in this part were created based on the findings in the "Forensic community opinion questionnaire" part of the paper, as well as the literature on the chain of custody for evidence. Figures 10, 11, 12, and 13 show the average results from the responses regarding the data in the reports. The results indicated the surveyed sample's agreement with that data found in the tool-generated reports.

Additionally, some respondents provided the researchers with additional information regarding other data to be included in the computer forensic report. These items are listed below:

- Time Difference, between the system time and standard local time
- Systems users

- Operating System and Version
- File System (NTFS, FAT, EXT, etc)
- Encryption deployed
- Write block methods/tools

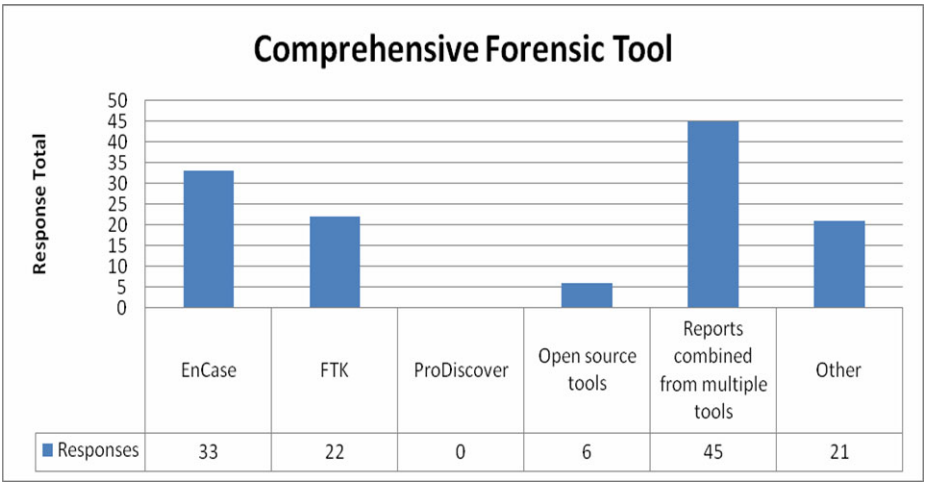

Fig. 4. Comprehensive forensic tool

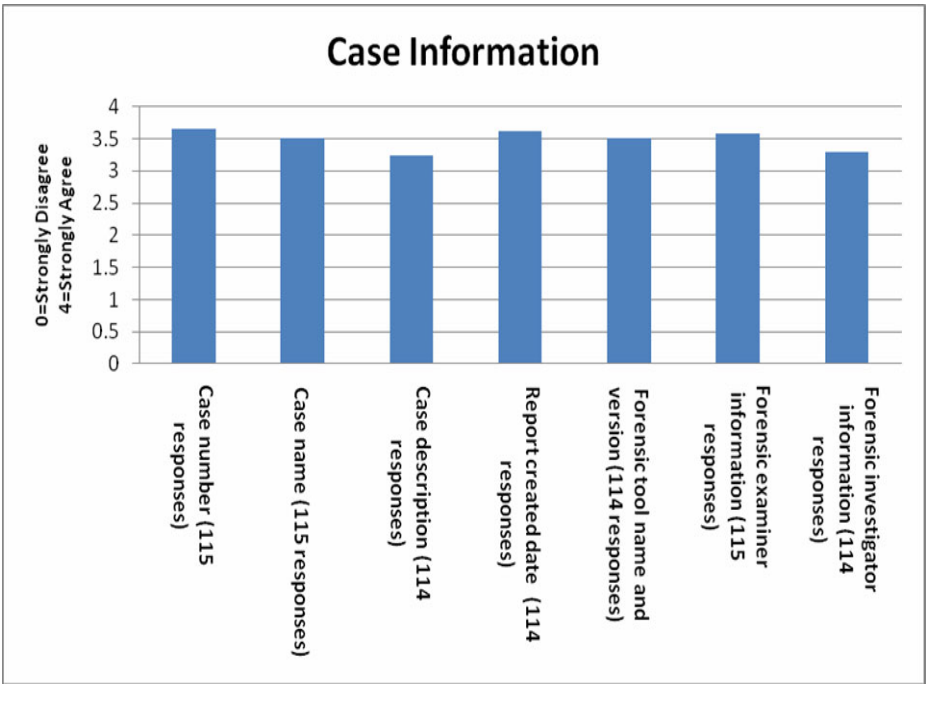

Fig. 5. Case information

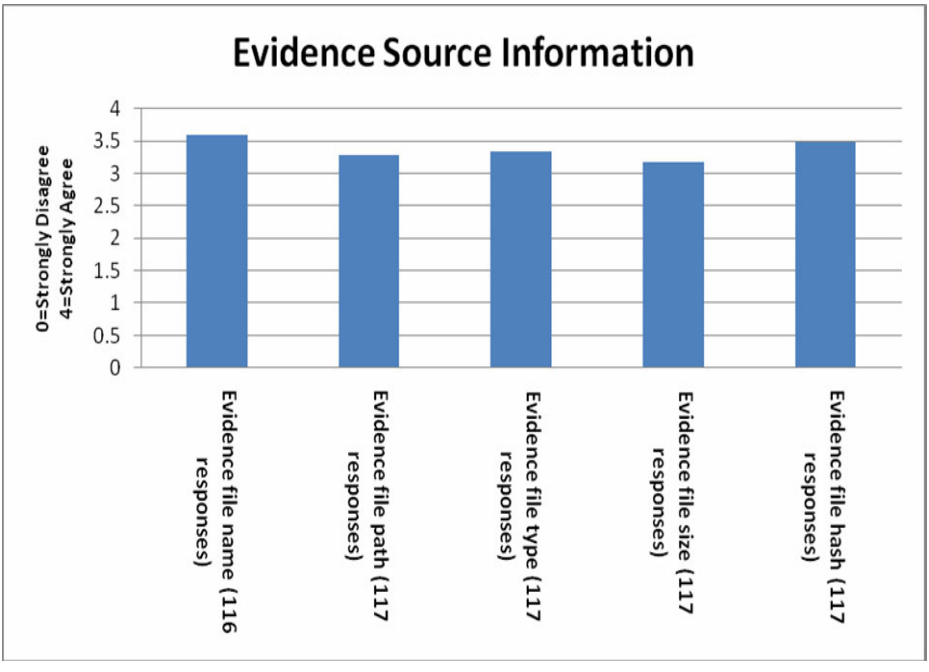

Fig. 6. Evidence source information

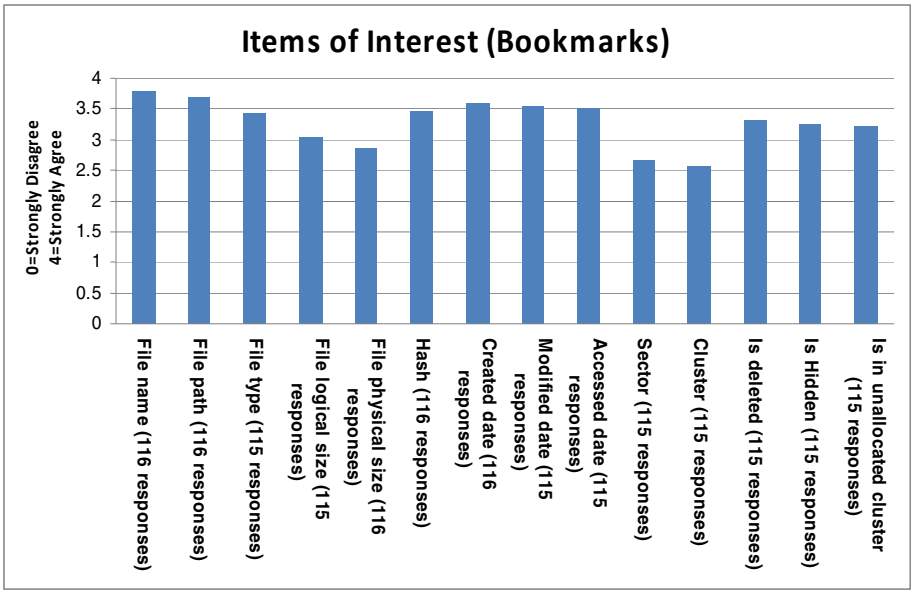

Fig. 7. Items of interest

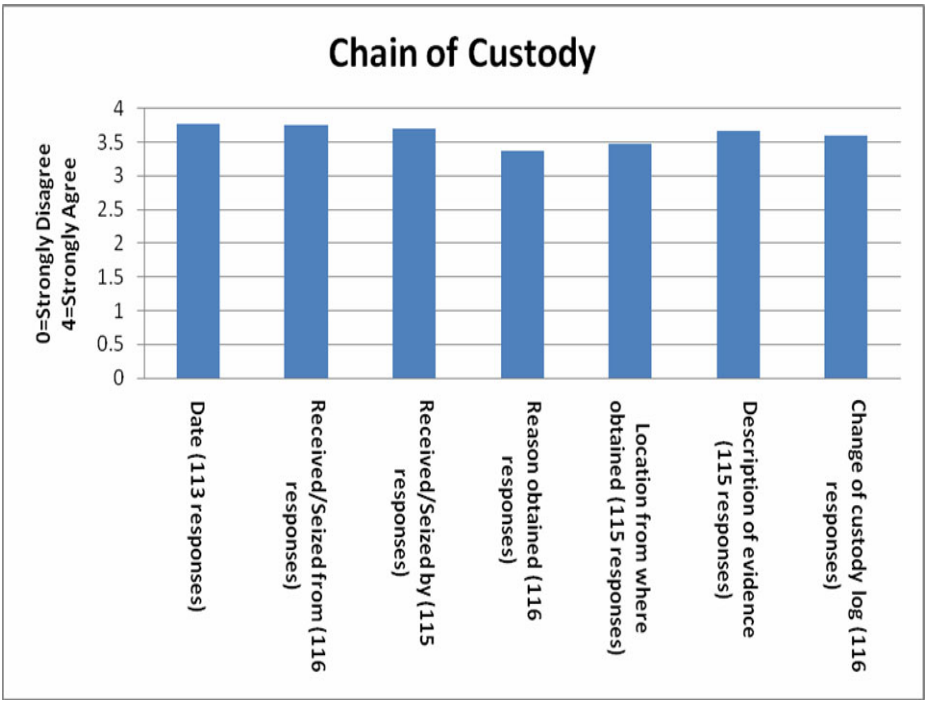

Fig. 8. Chain of custody

- Number and Type of Partitions
- Offset
- Note for each bookmarked item, why the user chose to bookmark it

5.4 Standard Definition

As a result from the previous research findings, the authors identified the data requirements related to digital evidence items. This led the authors to propose the following standard for reporting evidence items in computer forensic tools:

Table 2. Proposed standard for digital evidence item

A. Case Information	
1	Case number
2	Case name
3	Case description
4	Report created date
5	Forensic tool name and version
6	Forensic examiner information (Name, Agency, Address, Phone, Fax, Email, comments)
7	Forensic investigator information (Name, Agency, Address, Phone, Fax, Email, comments)

Table 2. (*continued*)

B.	**Evidence Source Information**
1	Evidence file name
2	Evidence file path
3	Evidence file type
4	Evidence file size
5	Evidence file hash (checksum)
6	System time in the evidence file
7	Write block method used with the evidence source
8	Users' information
9	OS version
10	File System
11	Partitions' information
12	Encryption in use
C.	**Evidence Item**
1	File name
2	File path
3	File type
4	File logical size
5	File physical size
6	Hash (checksum)
7	Created date
8	Modified date
9	Accessed date
10	Sector
11	Cluster
12	Is deleted
13	Is hidden
14	Is in unallocated cluster
15	Offset
16	Note
D.	**Chain of Custody**
1	Date
2	Received/Seized from
3	Received/Seized by
4	Reason obtained
5	Location from where obtained
6	Description of evidence
7	Change of custody log (purpose of change, method of transfer, released by, released date, received by, received date, hash value)

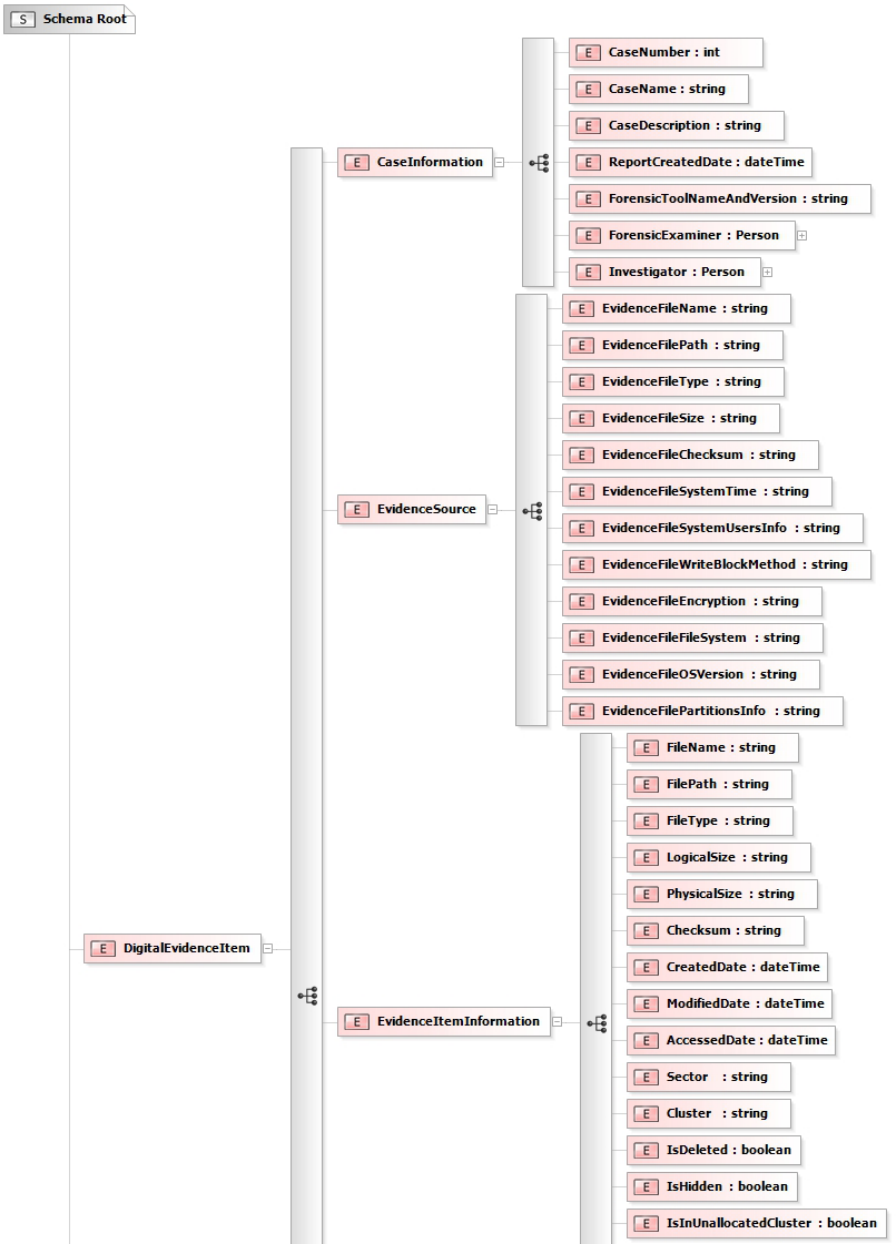

Fig. 9. Visual representation for the proposed data structure for digital evidence item (Part1)

5.5 XML Schema

Here, the authors are proposing to set an XML standard format for reporting digital evidence items in computer forensic tools. Having a standard as such can facilitate the reporting tasks for forensic examiners when using more than one tool. Examiners will end up with reports from different tools with the same data structure for the evidence items. The authors in this paper defined an XML schema for XML standard so this schema can be used to validate the XML digital evidence items generated by computer forensic tools.

Based on the authors' findings, they propose a standard for digital evidence items that includes data about the case, the evidence source, evidence item, and the chain of custody. Additionally, the authors put in their mind that, an XML standard should be flexible to any future development of forensic tools. Therefore, research results enabled the authors in creating a defined XML schema for digital evidence items that can be extended to incorporate other data object if an investigator has to include information, which is consider a new data object for digital evidence items.

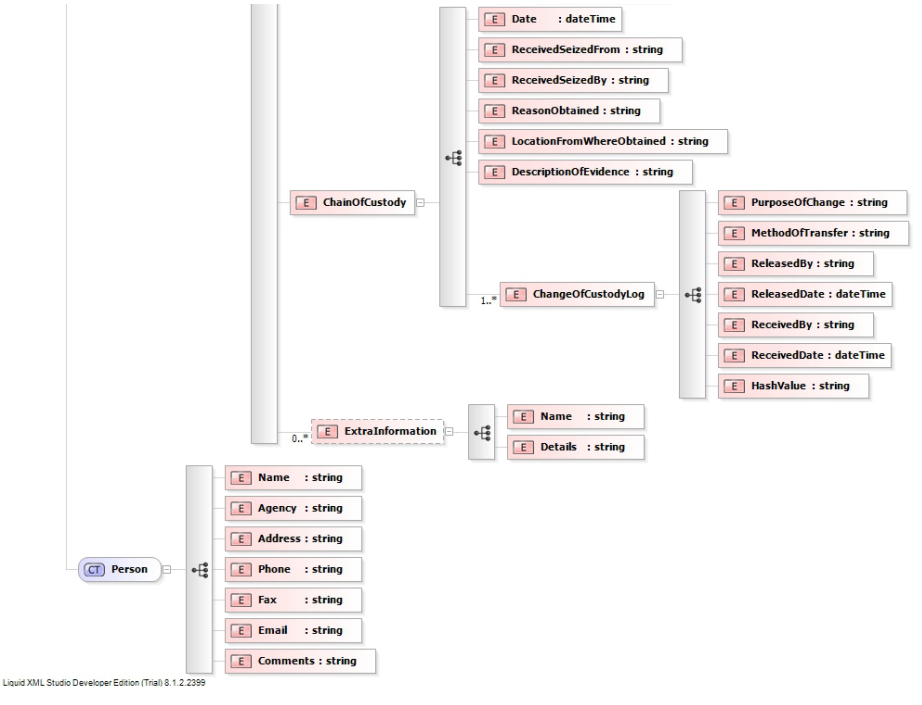

Fig. 10. Visual representation for the proposed data structure for digital evidence item (Part2)

Below is the XML Schema document for the standard defined in Table 2:

```
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema xmlns:tns="http://xml.netbeans.org/schema/forensicReportXmlSchema"
elementFormDefault="qualified"
targetNamespace="http://xml.netbeans.org/schema/forensicReportXmlSchema"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
    <xsd:element name="DigitalEvidenceItem">
        <xsd:complexType>
            <xsd:sequence>
                <xsd:element name="CaseInformation">
                    <xsd:complexType>
                        <xsd:sequence>
                            <xsd:element name="CaseNumber" type="xsd:int" />
                            <xsd:element name="CaseName" type="xsd:string" />
                            <xsd:element name="CaseDescription" type="xsd:string" />
                            <xsd:element name="ReportCreatedDate" type="xsd:dateTime" />
                            <xsd:element name="ForensicToolNameAndVersion"
type="xsd:string" />
                            <xsd:element name="ForensicExaminer" type="tns:Person" />
                            <xsd:element name="Investigator" type="tns:Person" />
                        </xsd:sequence>
                    </xsd:complexType>
                </xsd:element>
                <xsd:element name="EvidenceSource">
                    <xsd:complexType>
                        <xsd:sequence>
                            <xsd:element name="EvidenceFileName" type="xsd:string" />
                            <xsd:element name="EvidenceFilePath" type="xsd:string" />
                            <xsd:element name="EvidenceFileType" type="xsd:string" />
                            <xsd:element name="EvidenceFileSize" type="xsd:string" />
                            <xsd:element name="EvidenceFileChecksum" type="xsd:string" />
                            <xsd:element name="EvidenceFileSystemTime" type="xsd:string"
/>
                            <xsd:element name="EvidenceFileSystemUsersInfo"
type="xsd:string" />
                            <xsd:element name="EvidenceFileWriteBlockMethod"
type="xsd:string" />
                            <xsd:element name="EvidenceFileEncryption" type="xsd:string"
/>
                            <xsd:element name="EvidenceFileFileSystem" type="xsd:string"
/>
                            <xsd:element name="EvidenceFileOSVersion" type="xsd:string" />
                            <xsd:element name="EvidenceFilePartitionsInfo"
type="xsd:string" />
                        </xsd:sequence>
                    </xsd:complexType>
                </xsd:element>
                <xsd:element name="EvidenceItemInformation">
                    <xsd:complexType>
                        <xsd:sequence>
                            <xsd:element name="FileName" type="xsd:string" />
                            <xsd:element name="FilePath" type="xsd:string" />
                            <xsd:element name="FileType" type="xsd:string" />
                            <xsd:element name="LogicalSize" type="xsd:string" />
                            <xsd:element name="PhysicalSize" type="xsd:string" />
                            <xsd:element name="Checksum" type="xsd:string" />
                            <xsd:element name="CreatedDate" type="xsd:dateTime" />
                            <xsd:element name="ModifiedDate" type="xsd:dateTime" />
                            <xsd:element name="AccessedDate" type="xsd:dateTime" />
                            <xsd:element name="Sector" type="xsd:string" />
                            <xsd:element name="Cluster" type="xsd:string" />
                            <xsd:element name="IsDeleted" type="xsd:boolean" />
                            <xsd:element name="IsHidden" type="xsd:boolean" />
                            <xsd:element name="IsInUnallocatedCluster" type="xsd:boolean"
/>
                            <xsd:element name="Note" type="xsd:string" />
                            <xsd:element name="Offset" type="xsd:string" />
                        </xsd:sequence>
                    </xsd:complexType>
                </xsd:element>
                <xsd:element name="ChainOfCustody">
                    <xsd:complexType>
```

```
                        <xsd:sequence>
                            <xsd:element name="Date" type="xsd:dateTime" />
                            <xsd:element name="ReceivedSeizedFrom" type="xsd:string" />
                            <xsd:element name="ReceivedSeizedBy" type="xsd:string" />
                            <xsd:element name="ReasonObtained" type="xsd:string" />
                            <xsd:element name="LocationFromWhereObtained"
type="xsd:string" />
                            <xsd:element name="DescriptionOfEvidence" type="xsd:string" />
                            <xsd:element name="ChangeOfCustodyLog" maxOccurs="unbounded">
                                <xsd:complexType>
                                    <xsd:sequence>
                                        <xsd:element name="PurposeOfChange"
type="xsd:string" />
                                        <xsd:element name="MethodOfTransfer"
type="xsd:string" />
                                        <xsd:element name="ReleasedBy" type="xsd:string"
/>
                                        <xsd:element name="ReleasedDate"
type="xsd:dateTime" />
                                        <xsd:element name="ReceivedBy" type="xsd:string"
/>
                                        <xsd:element name="ReceivedDate"
type="xsd:dateTime" />
                                        <xsd:element name="HashValue" type="xsd:string" />
                                    </xsd:sequence>
                                </xsd:complexType>
                            </xsd:element>
                        </xsd:sequence>
                    </xsd:complexType>
                </xsd:element>
                <xsd:element name="ExtraInformation" minOccurs="0" maxOccurs="unbounded">
                    <xsd:complexType>
                        <xsd:sequence>
                            <xsd:element name="Name" type="xsd:string" />
                            <xsd:element name="Details" type="xsd:string" />
                        </xsd:sequence>
                    </xsd:complexType>
                </xsd:element>
            </xsd:sequence>
        </xsd:complexType>
    </xsd:element>
    <xsd:complexType name="Person">
        <xsd:sequence>
            <xsd:element name="Name" type="xsd:string" />
            <xsd:element name="Agency" type="xsd:string" />
            <xsd:element name="Address" type="xsd:string" />
            <xsd:element name="Phone" type="xsd:string" />
            <xsd:element name="Fax" type="xsd:string" />
            <xsd:element name="Email" type="xsd:string" />
            <xsd:element name="Comments" type="xsd:string" />
        </xsd:sequence>
    </xsd:complexType>
</xsd:schema>
```

6 Conclusion

Presentation of digital evidence is one of the key steps in digital forensics. Reports generated from digital forensics software tools may be used with the official investigation report in order to present digital evidence items to clients, or courts of law. The lack of standards in reporting digital evidence items in digital forensics software tools, leads to difficulties in combining digital evidence items into an official investigation report. This paper proposed a standard data requirement for digital evidence items, that could be used in reports generated using computer forensic tools. The suggested standard covered the basic information about the case, evidence source, items of interest and chain of custody for digital evidence items.

7 Future Work

The authors hope to expand the evaluation of the proposed standard for computer evidence by analyzing open source forensic software tools and their generated reports. Also, the authors are looking forward to implement a tool to manipulate the proposed standard for digital evidence. This tool will allow digital forensics stakeholders to import XML documents generated using different computer forensic tools, and combine them into a central repository, that could generate a standard report to be added to the final investigative report. Another future vision the authors are looking for, is to develop a standard format that goes beyond computer forensic evidence items, and covers other types of digital forensics evidence items like memory forensics, network forensics, and small scale digital device digital evidence items.

References

1. The Common Evidence Format Working Group (Carrier, B., Casey, E, Garfinkel, S., Kornblum, J., Hosmer, C., Rogers, M., Turner, P.): Standardizing Digital Evidence Storage. Communications of the ACM (February 2006)
2. Anson, S., Bunting, S.: Mastering Windows Network Forensics and Investigation. Wiley Publishing, Inc., Canada (2007)
3. Devine, J.: The Importance of the Chain of Custody (October 30, 2009), http://ezinearticles.com/?The-Importance-of-the-Chain-of-Custody&id=3182472 (retrieved March 18, 2010)
4. Garfinkel, S., Malan, S., Dubec, K., Stevens, C., Pham, C.: Disk Imaging with the Advanced Forensics Format, Library and Tools. In: The Second Annual IFIP WG 11.9 International Conference on Digital Forensics, National Center for Forensic Science, Orlando, Florida, USA, January 29-February 1 (2006)
5. Glendale, D.: Guidance Software EnCase (2010), retrieved from http://www.digitalintelligence.com/software/guidancesoftware/encase/
6. Levine, B., Liberatore, M.: DEX: Digital evidence provenance supporting reproducibility and comparison. Digital Investigation 6, S48–S56 (2009)
7. Liquid Technologies Limited: Liquid XML Studio 2010 (version 8.1.2.2399), [Software] available from http://www.liquid-technologies.com/
8. Marcella, A.J., Menendez Jr., D.: Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes. In: Information Security, 2nd edn. Auerbach publications, Taylor & Francis Group (2007)
9. Nelson, B., Phillips, A., Enfringer, F., Steuart, C.: Guide to Computer Forensics and Investigations. GEX Publishing Services, Canada (2008)
10. Petruzzi, J.: How to Keep a Digital Chain of Custody (December 01, 2005), retrieved from http://www.csoonline.com/article/220718/How_to_Keep_a_Digital_Chain_of_Custody
11. Pladna, B.: Computer Forensics Procedures, Tools, and Digital Evidence Bags: What They Are and Who Should Use Them. East Carolina University, East Carolina (2008)
12. ProDiscover. (n.d.) Technology Pathways, http://www.techpathways.com/DesktopDefault.aspx?tabindex=3&tabid=12 (retrieved February 22, 2010)
13. Rand, A., Loftus, T.: Chain of Custody Procedure (2003), retrieved from http://www.lagoonsonline.com/laboratory-articles/custody.htm
14. Steen, S., Hassell, J.: Computer Forensics 101 (October 2004), retrieved from http://www.expertlaw.com/library/forensic_evidence/computer_forensics_101.html