Integrity Assurance for Small Scale Digital Devices Based Evidence for Cyber Crime Investigation

M. K. Muhammad[1], *I. Idris[2], and I. Lukman[3]
[1]Academic Planning Unit, Federal University of Technology, Minna
[2]Department of Cyber Security, Federal University of Technology, Minna
[n]CODeL Unit, Federal University of Technology, Minna

[1] muhammad_kudu@futminna.edu.ng, [2] ismi.idris@futminna.edu.ng, [3]lukman.ibr@futminna,edu,ng

ABSTRACT
The recent rapid development in the field of information and communication technology industry have made the concept of acquisition and analysis of digital evidence an increasingly important tool for uncovering digitally related crimes and preparing them as a reliable evidence for legal acceptability. In this paper, a new generalized framework for the acquisition of digital evidence was applied on multiple forensics tools. The forensic tools used were EndCase, AccessData FTK Imager, Mount Image Pro and Autopsy 4.0 and their individual features was compared in order to provide reasonable level of assurance to compare various level of integrity assurance to make them admissible as viable digital evidence in the law court during cyber related litigation.

Keywords: Cyber Crimes, Device, Digital, Digital Forensics, Encase., Message Digest, Scale, Small

1. INTRODUCTION

In recent years, digital forensics has changed the general approach used by the law enforcement domain to an invaluable tool for detecting and solving corporate cyber related crimes. Since digital forensic evidence play a vital role in solving cyber related crimes, it worth to be investigated in a forensically sound manner.

Digital forensics evidence can be termed as a set of binary digit numbers stored as files on an electronic storage media either mobile or otherwise. There are a number of characteristics that are to be considered; for example, the said evidence can be copied and modified, this alteration to the original information may not be identified or noticed when it is compared with the original source. It can also be integrated into other data format verification. Often, digital evidence may not be understood directly without technical process and knowhow, even interpreting it from public perception may requires the efforts of an experts, otherwise the entire presentation may on its own becomes abstract in nature. Digital evidence according to Baggili (2015), is a fragile piece of information that can easily be destroyed or become inadmissible for legal credibility after its collection as a result of modification either intentionally or otherwise.

Originality of digital evidence is surrounded with the challenges of how its integrity is preserved, and this is a fundamental requirement because of trust as the end point is human dependent. It is necessary to preserve the integrity of digital evidence during its entire life cycle in order to have a forensics value thereby making the assurance of such evidence an umbrella principle. Digital evidences (Hagy, 2007) are usually an extracted piece of information obtained from the crime suspects and taken to the forensics laboratory for examination. Only the conclusions which is usually in the form of reports are usually shared with the parties concerned, so the digital forensics process can be liken to a black box for cyber crime investigation (Saleem, 2015).

With these new methods of perpetuating digital crimes, there has to be emergence of new technologies and measuring devices that can be used to track the cyber criminals, they are called electronic evidences. This is an instrument that is fast becoming part of our daily life and is acquiring increasing importance in lawsuits. It is no longer understatement that traditional evidence is shifting from paper supporting documents towards a digital and virtual domain and its management processes are proportionally changing in this world of dynamic technology even in the court of law.

Solid state digital devices (SSDD) are majorly the most popular non-volatile solid-state technology in the world of information and communication technology today and it can be accessible by anybody for conveying information from one medium to the other, either for legal or illegal purposes. According to a study conducted by ITU, it was revealed that 86.7% of individual using one computing devices or the other are using a mobile device (Thing et al, 2010). Since small scale digital device (SSDD) have literally become a sort of digital behavioral archieves both at collective levels and individual. They are omnipresent recording of all users activities at the moment. It obvious that, during cyber crime investigation, these category of storage devices can be a reliable source of evidence in furthering and resolving a related legal case with more assurance (Saleem, 2015).

2. RELATED LITERATURE

Here some works that has been previously carried out on this subject matter was critically reviewed with the aim of knowing why digital evidence are not globally acceptable as viable evidence during cyber related crime investigation.

There is no doubt that digital forensic according to (Harrill & Mislan, 2007) is a viable research area today because of the innovations in the digital technology industry coupled with exponential growth in cyber-crimes especially in the information superhighways. Digital forensic is becoming more attractive to the academicians except that some scholars are claiming that there are some characteristics that are affecting the investigation processes. Some of these characteristics include the physical shape of the Ahuja *et al,* (2005) devices with respect to most of the recent reported crimes. For example, the tiny and adaptable nature of small scale digital devices makes digital forensics investigation more complex for the investigators. As a result of this, cyber criminals use flash memory technologies to perpetuate their illegal activities (Casey, 2014).

Over the years, digital forensics have transformed into discipline that requires a comprehensive forensics investigation process model. Different researchers have proposed several investigative process model (Brison, *et al,* 2006). However, these proposed model over the years lack practical evaluation especially on mobile storage devices. The role of testing and evaluating a harmonized investigative process model lies in ensuring that the model adhere to certain forensics standard (Reith, 2012). It is because of these inadequacy that has made the growth of digital forensics investigations on small scale digital devices very unpopular and cyber criminals explored this weakness to perpetuates several undiscovered crimes and in a few cases where they are discovered, the integrity of data presented before the court lacks expected merits (Casey, 2004).

3. PROPOSED METHODOLOGY

This section provides detailed information on the proposed methodology. In order to validate the reliability of evidence collection for the various experiments to be conducted for this study, similar works done by Arasteh *et al,* (2013) and Saleem (2015) were used as benchmarks. Data extraction algorithm of Saleem (2015) was expanded. Though the algorithm was limited to android devices but the human right and other legal privileges of cyber-crime suspects was the focus of their work. For the purpose of this work, the evidence extraction part was reviewed and expanded in order to make use of multiple forensics software tools. This modification introduced a new algorithm that was implemented for both the collection of evidence from any category of solid state digital devices (SSDD) in order to establish how the integrity of digital evidence can be preserved. In this study, it is believed that applying multiple digital forensic tools will assist to determine if the contents of the solid state digital devices (SSDD) has been altered while on transit between the point of arrest or collection of the device and the point of examining the contents.

3.1 Case File Extraction and Modification

The evidence extraction tools were also evaluated for their ability to preserve the integrity of digital evidence. The following experiment was conducted.

3.2 Procedures

i. Digital evidence from SSDD was obtained.
ii. The evidence image file was opened using the hex editor in each of the tools and its contents were modified.
iii. The same case file was reopened with each of the tools.

3.2.1 Results

90% of the entire solid state digital device (SSDD) was in good working condition hence, evidence was obtained from all the storage devices presented during the experiments except some few files whose contents were damaged. It was noted that message digest (MD5) and digital hashes were used to preserve the integrity of digital evidence.

3.3 Extracting Evidence and Preservation of Integrity

Prior to the commencement of evidence acquisition process, it is obligatory to safeguard the device with Farady cage to avoid unnecessary alteration in case the system in use is on a network which could trigger events resulting in modification of contents of the SSDD object. This may affect the integrity of the expected result if the SSD is an Android devices that have option plug and play during operations. This is really helpful since for collecting data which otherwise could have been altered if the device is turned off when it was seized or collected from the crime suspect.

It therefore become pertinent to check if the SSDD is already connected, and replace it with the target SSDD or where the SSDD contents is to be transfer then, there may be need to look for an add-on application with some the popular forensics tool such as Efficient Generalized Forensics Framework Acquisition Application. There is need to then navigate through File Explorer in order to launch the add-on application if it does not come with the forensics tools. The application will automatically close all firmware processes running on the system being used for the experiment in order to avoid the issue of locking. In order to ensure integrity of the acquired evidence, the application comes will various tools various tasks such as hashing of each file before and after copy. The purpose of this is to keep tracks of activities on images/data before they were extracted and after the actual extraction.

3.4 Evidence Acquisition Process Model

Figure 3.6 present the new model for the acquisition of digital evidence from both Android and Non-Android storage device otherwise referred to in this study as small scale digital devices (SSDD). In the model, when an SSDD is mounted, the forensics tool used already have some enhanced functionality for computing the Message Digest algorithm and the SHA1 in order to avoid unnecessary human interaction with the entire process. The model automatically accesses the SSDD physical volume and other file structure including the FAT file of NTFS part. All the details of the images contained in the SSDD is accessed including date and time when the image was created, modified and other task that any user may have carried out on such data are noted and reported during analysis. All other required activities are included in the algorithm systems in figure 1.

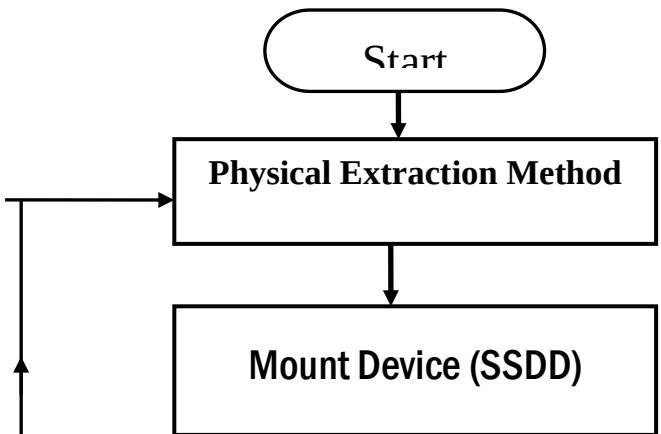

Figure 1: Generalized Evidence Acquisition and Integrity Check Model

3.5 Case File Extraction and Modification

The evidence extraction tools were also evaluated for their ability to preserve the integrity of digital evidence. The following experiment was

conducted.

3.5.1 Procedures

i. Digital evidence from SSDD was obtained.
ii. The evidence image file was opened using the hex editor in each of the tools and its contents were modified.
iii. The same case file was reopened with each of the tools.

3.5.2 Results

90% of the entire solid state digital device (SSDD) were in good working condition hence, evidence was obtained from all the storage devices presented during the experiments except some few files whose contents were damaged. It was noted that message digest (MD5) and digital hashes were used to preserve the integrity of digital evidence.

3.6 Extracting Evidence and Preservation of Integrity

Before Acquisition process starts, it is necessary to shield the device with Farady cage to avoid network communication which could trigger events resulting in modification of file system's object. Mostly all the Android devices have option to plug-in a SD card while the device is powered-on (hot-plug) without removing battery. This is really helpful since for collecting data which otherwise could been altered if the device is turned off before the seizure process.

Therefore, we have to check first if a SD card is already plugged, and replace it with a SD card containing updated version of Efficient Generalized Forensics Framework Acquisition App. We need to then navigate through File Explorer to launch the Acquisition application. The application will automatically short down all firmware processes running on the system in order to avoid locking problems. In order to ensure integrity of the acquired evidence, the application comes will various tools to perform other tasks such as hashing of each file before and after copy. The purpose of this is to keep tracks of images/data before they were extracted and after the actual extraction.

3.7 Acquisition Algorithm

The implementation details are provided in the following Figure 6 which shows the pseudo-code for the Acquisition Process:

The acquisition algorithm performs the follow tasks:

i. Copy Evidence from SSDD mounted on the system
ii. In this task, all the contents of the SSDD are copied into a Case file
iii. Hashing
iv. The task of Hashing is to ensure integrity of the extracted evidence and allows discovering if there is an alteration in the contents between when the evidence was extracted and when it was actually analyzed.

The acquisition algorithm uses the various features in the forensic evidence acquisition tool for performing needed tasks during the above processes.

This algorithm preserves the main directory structure, by duplicating the existing images/folders, files and other contents of the SSDD according to their original position on the storage device recursively. The hashing ensures integrity check before and after duplicating the device contents. The hashes are also written in the appropriate log file called case1and case 2.

3.7.1 Algorithm Acquisition

```
Input: A path P
Out: none
for all objects obj (folders,
files and directories) in p do
          if obj is a directory
then
                create a
directory names p in SSDD
                Recursively
call Acquisition(p/obj)
                      else
     if obj is a file then
                      compute
MD5/SHA1 hash of obj
                      copy obj
in path p on the SSDD
                           if
obj has not been copied then
```

```
access to obj with
          evidence acquisition
software
     end if
          end if
                    if obj is
access then

recreate database in path f
                              on
SSDD
                    end if
          end if
       end if
      compute MD5/SHA1 hash of
     evidence extracted obj on
     the SSDD
```

3.8 Returning the SSDD to its former state

If the device is not booted using the CRMI, the device can be return to the former state after completing the evidence acquisition. This process continues until all the evidences contained in all the seized mobile devices are fully acquired. If a file for the boot partition exists, a check will be conducted to determine if it is the correct original boot partition. When checking if it is correct original boot partition, the firmware version that is used in the targeted device is essentially important to note.

When the targeted mobile device is completely returned to its former state, the device should be unplugged until the device is used again in order to prevent data modification. If the device is an all-in-one type with battery, then cut off the power by using the power button and if the battery can be removed, it should be remove.

In case of turning the device off by using the power button, then it is recommended that the researcher should not use the menu functions of the recovery mode. The menu can be different for each vendor/device manufacturer or firmware version, but the reboot system now is usually included in the menu recovery mode. Before removing the battery, the USB cable must be separated first. Some mobile devices mount the user data partition by using the power provided by the USB cable if the battery is separated when the USB cable is still connected.

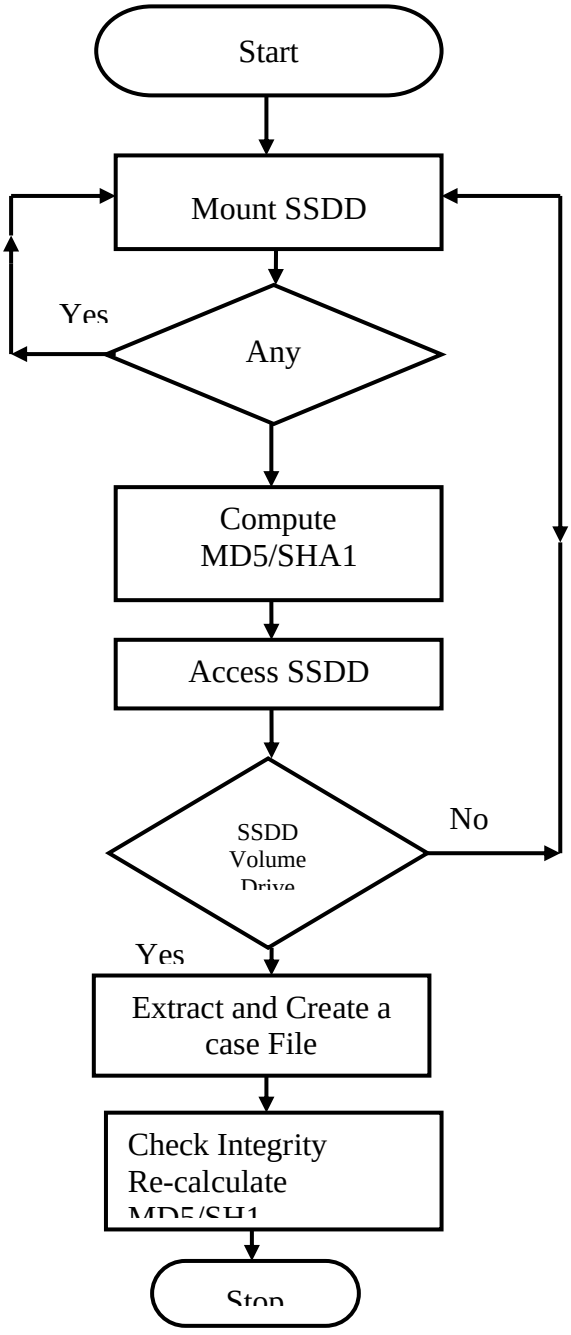

Figure 2: Evidence Acquisition Process Model

4. Presentation of Data and Discussion

In this chapter, discussions on various approaches used during the extraction of digital evidence and how the adopted forensics tools was used are fully

documented. Basic features of each of the forensics tools used were discussed with a comparative analysis of their attributes for providing adequate integrity on the extracted digital evidence.

4.1 Evaluation Criteria for Integrity Assurance

Digital evidence is ubiquitous, so digital evidence can come from various category of SSDD, regardless of whatever implication any individual may passive it. Digital evidence is by any mean crucial to the development of forensics industry hence, preserving the integrity of such extracted information from the devices used in perpetuating the crime in question thus important. There are many methods used in preserving the integrity of digital evidence, when attention is focus on the various approach that some of these tools handles accuracy, performances, vulnerabilities and complexity, they are differs in nature. In order to know how suitable they are in preserving evidence, table 6 provides 3 classes for evaluating integrity of digital evidence. The following preservation scheme was adopted from Saleem, (2015) to confirm the result of some of the experiment performed with the 4 forensics tools as indicated in Table 1, Table 2, Table 3, Table 4 and Table 5 respectively. Some of the criteria used includes:

i. Digital Hashes (MD5 and SHA1
ii. Digital Signature which rely on public key cryptography and require PKI at it backend.
iii. Cyclic Redundancy Checks (CRCs)

4.3 Comparative Analysis of Digital Forensic Tools

In providing reliable computer analysis and collection of digital evidence to meet the variety of needs in the field of forensics, digital forensics tools play a vital role. Most of these tools are used to conduct investigations of computer crimes by identifying evidence that can be useful in the court of law during cyber related crimes investigation. In addition to cyber related crimes investigation, these tools are used for the purpose of evidence extraction, debugging, data recovery among other in a secured environment which are usually refers as being forensically sound.

Table 1 shows comparative details of four evidence extraction tools with five parameters. From the table, the speed of acquiring evidence from solid state digital device (SSDD) is very slow on EnCase 7 and AccessData FTK Imager, although both of them are highly rated with respect to integrity assurance. But when large numbers of solid state digital device (SSDD) are to be consider for investigation, it will take longer time to extract evidence using EnCase 7 and AccessData. Unlike the Mount Imago pro and Autopsy, the speed of evidence acquisition was quite high. This gives an indication that Mount Image Pro and Autopsy 4.0.0 are good tools when speed of acquiring evidence is of high priority.

Table 1 : Evidence Formats and Evidence Acquisition Tools

Criteria	EnCase 7	AccessData FTK Imager	Mount Image Pro	Autopsy 4.0.0
Speed Acquisition from SSDD	Slow	Slow	Very High	Very High
Scalability of Extracted Evidence	Selective	Selective	Any Image Format	Any Image format
Message Digest (MD)	Produce MD 5, MD3.	Produce MD 5, MD3 and MD1.	Produce MD 3	Produce MD 3
Hash File	Comprehensive	Comprehensive	Not Comprehensive	Not Comprehensive
Level of Secured Evidence	High Level	High Level	High Level	High Level

4.4 Analysis of time spend on each tool during evidence acquisition

Since the study focus on various category of SSDD, there would be need to consider time spend on different SSDD with respect to their storage capacity. Every digital forensic tools will spend different amount of time on each category of SSDD to access, extract and analyse the contents of each storage device.

To determine the integrity of acquired evidence, the need to know the quality of the digital forensics tools used with respect to whether the software tool is a free license, open source, the operating system platform with which the tool will run such as Microsoft windows and the need to also know the performance and cost of acquisition is very crucial. As shown in the table 2, for the purpose of study, open source of digital forensics tools was obtained and exclusively used.

Table 2: Behavioural Analysis of Evidence

Acquisition Tools on set of criteria on SSDD.

	EnCase 7				AccessData FTK Imager				Mount Image Pro				Autopsy 3.0			
	Physical SSDD	Logical Volume	File	Folders	Physical SSDD	Logical Volume	File	Folders	Physical SSDD	Logical Volume	File	Folders	Physical SSDD	Logical Volume	File	Folders
USB Flash Drive	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Mobile Phone	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
SIM Card	✓	✗	✗	✓	✓	✗	✓	✗	✓	✗	✗	✗	✓	✗	✗	✗
Memory Card	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Also in order to accomplish one of the set objectives of using more than one forensics tool to test for integrity of evidence, other evidence acquisition tools was also acquired from the open source platform. Therefore, Table 3 also show the analysis of four categories of tools used and their functionality was also compared using Cost, Performance, Platform Support and License criteria's. For example, table 3 shows that EnCase 7 is a commercial version and apart from the fact that its performance was very high, it supports both 32 and 64 bit windows operating system.

If EnCase 7 is compared with Mount Image Pro, it was shown in the table that Mount Image pro was Open Source, its run effectively on only windows 32 bit but it attract no cost in terms of acquisition.

Table 3: Comparison of considered tools on the basis of features

	EnCase 7	AccessData FTK Imager	Mount Image Pro	Autopsy 4.0.0
Software License	Commercial	Commercial	Trial Version	Trial Version
Platform Support	Windows 32 Bit and 64 Bit	Windows 32 Bit and 64 Bit	Windows 32 Bit	Windows 32 Bit
Performance	High	High	Low	High
Cost	High	High	Free	Free

In table 4, digital forensic investigation process was examined and four forensic tools was compared. As indicated in the table, Mount Image Pro does not have adequate features for keeping track of date and time when an evidence is acquired so it could not provide a good valid information on Preservation of evidence and is also not able to analyse evidence even though, it has a good reporting features. From the table, it obvious that Autopsy 3.0.0 do not have feature for examining extracted evidence

Table 4: Comparison of considered tools on the basis of Digital Forensic Investigation Process

Tool Used	Preservation	Collection	Examination	Analysis	Reporting
EnCase 7	Yes	Yes	Yes	Yes	Yes
AccessData FTK Imager	Yes	Yes	Yes	Yes	Yes
Mount Image Pro	No	Yes	Yes	No	Yes
Autopsy 3.0.0	Yes	Yes	No	Yes	Yes

In table 5, set of scalable criteria was used to examine each of the digital forensic tools used. The objective of this was to know further apart from table 4.6, how each of the tool handles other basic integrity criteria between the Fully, Partly or Nil. For example, in trying to know how variable like Automated MD5 Algorithm was treated on each of the tools, from table 5, the performance remark was for all the four forensic tools used.

This also show that EnCase 7 can be a more preferred digital forensics tools when knowledge of the details of deleted files from an solid state digital device (SSDD) is a critical factor to maintain assurance over a digital evidence.

Table 5: Comparison of considered tools on the

basis of Digital Forensic Investigation Process

Scalable Criterias	EnCase 7	AccessData FTK Imager	Mount Image Pro	Autopsy
Supported Image File Format	Fully	Fully	Partly	Partly
Show Deleted Files	Fully	Fully	Partly	Partly
Show Unallocated Clusters	Fully	Partly	Partly	Partly
Remove Hidden Attributes	Fully	Partly	Partly	Partly
Physical Drive Mounting	Fully	Fully	Partly	Partly
Extended Partition Support	Partly	Partly	Partly	Partly
Plug and Play Mount Option	Fully	Fully	Fully	Fully
File Activities Log Details	Partly	Fully	Partly	Partly
Automated MD5 Algorithm	Fully	Fully	Partly	Nil
VMWare Activities Log	Partly	Partly	Partly	Fully
Extensible Keyword Search	Partly	Fully	Partly	Partly
Artifact Analysis	Partly	Partly	Fully	28
Registry Analysis	Fully	Partly	Partly	Partly

On any flash or memory card that has no folder, but has partition(s) information, the size of each partition was checked and the partition(s) are imaged and checked in line with the steps in the Algorithm. For the acquisition of the file allocation table (FAT), the partition table is automatically mounted in read only mode to guarantee data integrity. The consciousness here is that, if the time and date of the content of the partition table changes, the integrity of the content is loss and the set objective will not be met.

5.1 Conclusion

Having concluded an in-depth literature research into integrity of digital evidence and explored diverse reason why most cyber related extracted evidence from the various storage devices are not usually considered as legitimate evidence for consideration by the court during investigation, it can be concluded that the prosecutor of some of those court cases with respect to cyber-crimes lost out because, evidence are either extracted manually with already compromised human intervention. However, with some of the exercise and results of this work, it is obvious that using an automated forensic tools goes a long way to reduce the existing challenge of non-admissibility of digital evidence in the law court. It was also noted that digital evidence can be relied upon especially when the evidence are extracted in a forensics manners. The same way mobile telephone call logs are recognized and admitted in the law court, digital evidence that are extracted in a forensically manner should be recognize and admitted in the law court during cyber related investigations.

REFERENCE

Ahuja, M. K., and Thatcher, J. B. (2005). Moving beyond intentions and toward the theory of trying: effects of work environment and gender on post-adoption information technology use. *Management Information System quarterly*, 29(3), 427-459.

Arasteh, A. R., Debbabi, M., Sakha, A., and Saleh, M. (2013). Analyzing multiple logs for forensic evidence. Digital Investigation, 4, 82-91.

Baggili and Huebner, E. (2015). Computer forensic analysis in a virtual environment. International journal of digital evidence, 6(2), 1-13.

Brinson, A., Robinson, A., and Rogers, M. (2006). A cyber forensics ontology: Creating a new approach to studying cyber forensics. digital investigation, 3, 37-43.

Casey, E. (2004). Network traffic as a source of evidence: tool strengths, weaknesses, and future needs. Digital Investigation, 1(1), 28-43.

Casey, E. (2014). Digital evidence and computer crime: Forensic science, computers, and the internet. Academic press.

Hagy, D. W. (2007). Digital evidence in the courtroom: a guide for law enforcement and prosecutors. *National Institute of Justice*.

Harrill, D. C., & Mislan, R. P. (2007). A small scale digital device forensics ontology. *Small Scale Digital Device Forensics Journal*, 1(1), 242.

Reith, M. (2012). An examination of digital forensic models. *International Journal of Digital Evidence*, 1(3), 1-12.

Saleem, S. (2015). Protecting the Integrity of Digital Evidence and Basic Human Rights During the Process of Digital Forensics.

Thing, V. L., Ng, K. Y., and Chang, E. C. (2010). Live memory forensics of mobile phones. digital investigation, 7, S74-S82.