Developing an E-Chain of Custody and Inventory System for the Zambia Police Force

Peter Nsofwa
Department of Electrical and Electronic Engineering,
University of Zambia,
Lusaka, Zambia

Jackson Phiri
Department of Computer Science,
University of Zambia,
Lusaka, Zambia

***Abstract*—Crime solving comprises methodical law enforcement, an exhaustive investigation and collection of facts, and extensive evidence testing performed by criminalists and forensic experts. The process starts from the crime scene. Evidence items collected from the crime scene must be handled in a manner which adheres to the rules of evidence, if it has to be used as evidence in Court. Zambia Police currently has gaps in the evidence chain of custody and tracking. This study proposed the automation of processes and procedures associated with management of crime scene evidence from the time it is collected from the scene to the time it is presented in Court. Interviews and questionnaire instruments were used to define the challenges of the actual processes used by Zambia Police in regard to crime scene evidence management. Based on analysis of the results, it showed that Zambia Police use a manual based system for their crime scene evidence management. The baseline study findings were used to design an E-Chain of Custody and Inventory System (ECCIS)**

Keywords- evidence, investigators, court, crime scene, chain of custody

I. INTRODUCTION

Criminal evidence is a product of crime. A crime can be committed on any physical scene. This physical scene can be, a person's body, a building, a vehicle, places in the open air or objects found at those locations [1]. Investigators search, gather and preserve potential evidence from these crime scenes using criminal investigation techniques in order to prove that the crime was committed [2]. Physical evidence retrieved from crime scenes helps in resolving crime, by substantiating or challenging alibis, by excluding suspects or linking suspects to the crime, by recognizing the source of stolen materials, and by providing investigative clues [3]. However Chain of custody is required in the handling of evidence items that are bound by legal or regulatory directives [5]. Chain of custody refers to the chronological and careful documentation of evidence including collection, storage, transportation, as well as noting a person who has taken control of the evidence [6]. For evidence to be used in court it is crucial to be able to demonstrate every single step undertaken to ensure "traceability" and "continuity" of the evidence [7].

Crime scene management in Zambia Police Force is done by Scenes of Crime Unit of Forensic Investigation Wing which is under the Criminal Investigation Department (CID) [8]. Most of the business processes under the CID are done manually including the documentation of evidence movement. These manual procedures present a lot of challenges which include; breakages in the chain of custody which lends evidence inadmissibility, high chances of mismatch between the evidence and its associated documentation, high chances of evidence tempering, evidences can be lost or pilfered due to luck of a good trial as it moves from a police station to the forensic laboratory and between laboratory units, difficulties in tracking the evidence through the course of the investigation which could take weeks, months and sometimes years, difficulties in coming up statistical reports, paper based manual are susceptible to damage by pest and harsh environmental conditions.

Due to the challenges recognized, the proposed system will enhance the evidence management and chain of custody. Automating the handling of evidence increases the accuracy, minimizes the likelihood of illegal manipulation of evidences, and give access to data in real time [9]. According to Saman et al [10], a good approach to guarantee accountability and integrity of an institution that provides services to the public is through the use of effective record management systems that leverage technology to enhance the productivity and overall operations.

II. REVIEW OF RELATED LITERATURE

Verismo et al [11] understands chain of custody as a tool used in handling evidence in order to keep its integrity and authenticity. According to International Union of Pure Applied Chemistry cited by Tomlinson et al [5] "a chain of custody is the set of traceable records that provide unbroken control over a document, raw data, or a sample and its containers from initial collection to final disposal". Verismo et al [11] further explains and recommends that there is a

need to have a central authority to be responsible for the safeguard of evidence in order to minimize the risks of loss or alteration on evidence under custody.

Evidence submitted to the court and the one collected during investigation must be proved to be the same. The chain of custody helps to prove and demonstrate that integrity of evidence has been maintained throughout the whole process [3]. Jones et al [12] reiterates that if a crime under investigation is likely to take stage and become part of criminal justice system, there must be a chain of custody so that the submitted items may be tracked from origin. When there is a need of post-convection testing, the chain of custody can be used to locate the evidence years down the road [13].

During crime scene investigation evidence is packaged and identifying information pertaining to the crime is written on the packages or tags as well as logs to establish the chain of custody [7]. Fisher and Fisher [3] state that, the following information is needed to establish the chain of custody: name of the individual gathering the evidence and each person consequently having custody of it, dates the evidence item was collected and transferred; agency name, case number, type of crime, property official number, victim's or suspect's name, storage location and a brief description of the item. This information serves to prove that the evidence item has been gathered, tracked, and protected on its way to Court [13]. Demonstrating the chain of custody is essential to confirm that the evidence has not been tampered with, changed, or substituted [14]. Evidence reasonably assumed to have been tampered with or kept in an unsecured area may be inadmissible in court [3].

Cosic and Cosic [13] explain that Chain of custody is often recognized as the weak link in criminal investigations. In the event that the defense counsel demands the chain of custody for any evidence item, a documented path of continuity can demonstrate that the evidence item presented in court is actually the same evidence item gathered from the crime scene. If there are any inconsistences about where the evidence item has gone to or who has had possession of the item, the judge may rule that the chain of custody has been broken and the item may not be admitted as evidence [14]. Many studies [12] [15] [16] [17] [18] have pointed out that any break in the chain of custody opens the prosecution to allegations that the evidence has been tampered with or other evidence substituted for it. Cosic and Cosic [13] further explain that without the valid chain of custody, evidence cannot be accepted by the courts.

The chain of custody answers the following questions [14] [19] [13] [5] [11]: What is the evidence reported to be? Can an uninterrupted trail of possession by each individual handling the evidence item be established from the time it was collected until the time it was presented in Court? Can a person who had possession of the evidence item confirm that it essentially remained in the same condition from the moment he or she received it, to the moment he or she released it?

III. Related Work

Cosic and Cosic [13] conducted a research on the "Chain of Custody and Life Cycle of Digital Evidence (CoCoDE)", in order to improve the chain of custody for the digital evidence. In this study the researchers developed a formula (fig.1) based on the old formula used by researchers, police and journalists – Who, What, Why, Where and How.

This research further suggested that the CoCoDE formula will be able to produce credible chain of custody.

```
CoCoDE = f{fingerprint_of_file,          //what
           biometrics_characteristics,   //who
           time_stamp,                   //when
           gps_location,                 //where
           reason,                       //why
           set_of_procedures};           //how
```

Figure 1. CoCoDE formula [13]

Prayudi et al [20] conducted a study on the Framework for Handling Digital Chain of Custody. This research suggested that digital cabinets can be developed where digital evidence can be kept. The cabinet will be protected and watched over by an officer. If an investigator needs the evidence, formerly has to go through the process and acquire a license from the office on duty to access the evidence. The officer at that point will unlock the cabinet and submit the needed evidence to the investigator.

Viríssimo et al [11] in their research on management and control of chain custody for forensic evidence suggested to use Radio Frequency Identification (RFID) to monitor evidence movement. The study proposed to develop a RFID enabled system to monitor the movement of forensic evidence between laboratory units.

IV. Methodology

A. *Baseline study*

The baseline study was done in order find out the challenges faced by the Zambia Police Force on the

comprehension and adherence to existing processes, policies and procedures of crime scene evidence management. The target group was sworn police officers who operate under criminal investigation and deal with crime scene evidence.

Mixed Methods Research Methodology was used in this research. Structured questionnaire was used to collect quantitative information from officer operating under crime scene investigation across all the ten provinces of Zambia.

For qualitative data, interviews with provincial head of Scene of Crime units were conducted.

B. Software Design Methodology

The systems was designed based on the information produced through interviews, questionnaires and literature review.

C. Business Process mapping

Fig. 2 shows the overview of the system architecture. The system was derived from the business process used by the Zambia Police at the time of this study. The numbers in the figure shows the order of movement for crime scene evidence.

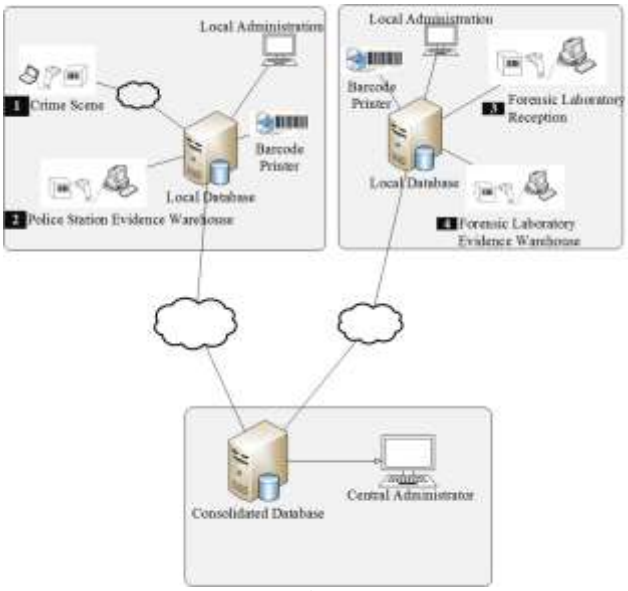

Figure 2. Overview of System Architecture

1) Crime Scene

At crime scene, evidence items are packaged and sealed. The barcode is used as part of the seal. An already printed barcode is assigned and stuck to the package. Evidence information is entered into the system and the barcode is scanned in to the system. Evidence information and the barcode are linked and evidence identity number is generated.

2) Police Station Evidence Warehouse

The barcode on the package is scanned to update the chain of custody and location. It should not be opened; however if the seals are damaged or broken, the contents must be verified prior to resealing. The replacement seal together with barcode should be initiated, dated, and witnessed.

3) Forensic Laboratory Reception

The barcode on the package is scanned to update the chain of custody and location. The package seals are checked, if damaged or broken the content are verified prior to resealing. The evidence is then taken to the warehouse.

4) Forensic Laboratory Warehouse

Specialist withdraw evidence from the warehouse. The specialist identity number will be linked to the evidence withdrawn. After finishing working on the evidence the evidence is packaged assigned a new seal and taken back to the warehouse.

D. System architecture

a) System Design

Fig. 3 shows the architecture which was used to develop the ECCIS. The system was design using the Model-View-Controller architectural pattern (MVC). The model contains the core functionality (business logic) and data of the ECCIS. Views accesses the data through the model and specifies how that data is be presented. Controllers handle all the user input. Views and controllers together comprise the user interface shown as the browser in fig. 3.

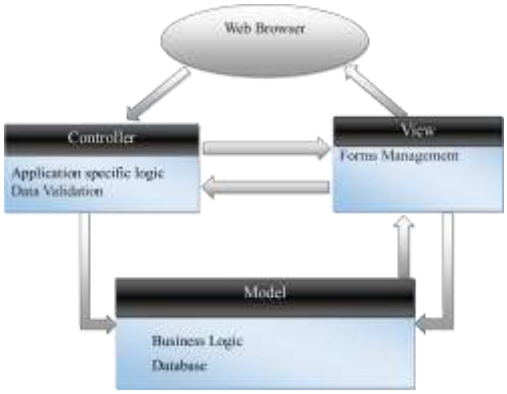

Figure 3. System Architecture

b) User case

Fig. 4 shows the use case of the system implementation and the communications between the actor and the system. The users at the application interface has to first logon to the

system before they can to perform any transactions.

Figure 4. System Use Case

c) Entity Relation Diagram

Fig. 5 shows the entity relation diagram for the ECCIS. The entities, evidence and crime scene are dependent on the criminal-case entity. All other entity will exist even without the criminal case entity.

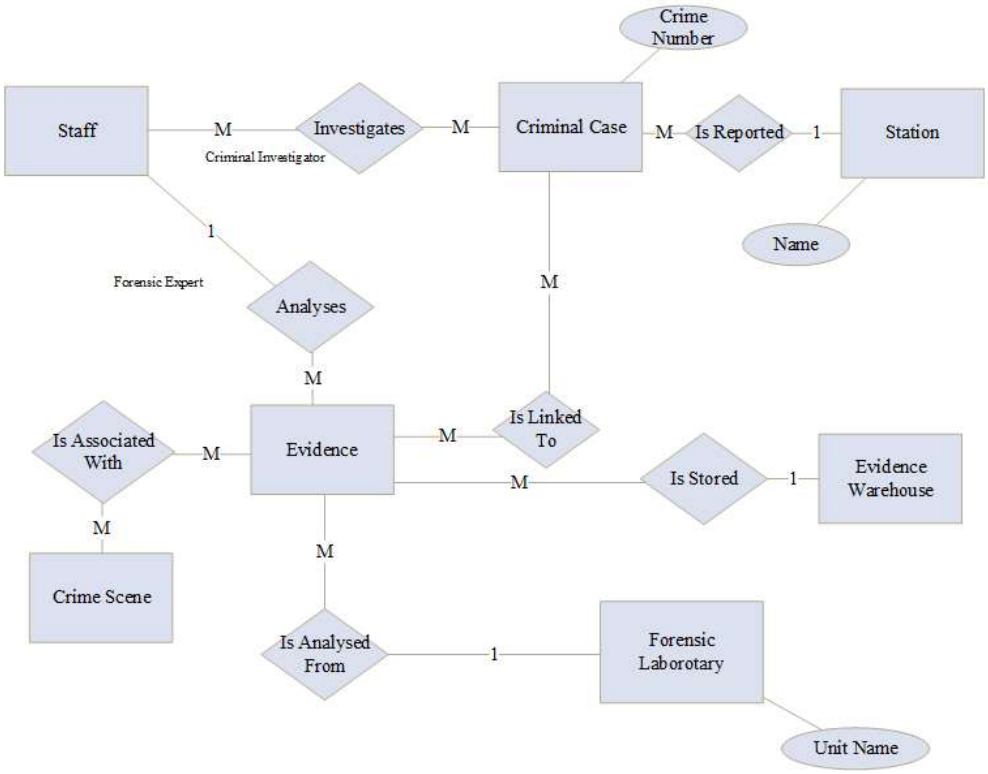

Figure 5. Entity Relation Diagram for ECCIS

d) Sequence Diagram

Fig. 6 shows the sequence diagram of the system. The member of staff logs on the ECCIS. If the staff wants to update evidence data, his/her user-identifier (UID) permissions are checked using the authorization system.

After authorization, the staff can now update the evidence data. On completion of the transaction the status message is issued and the staff logs out.

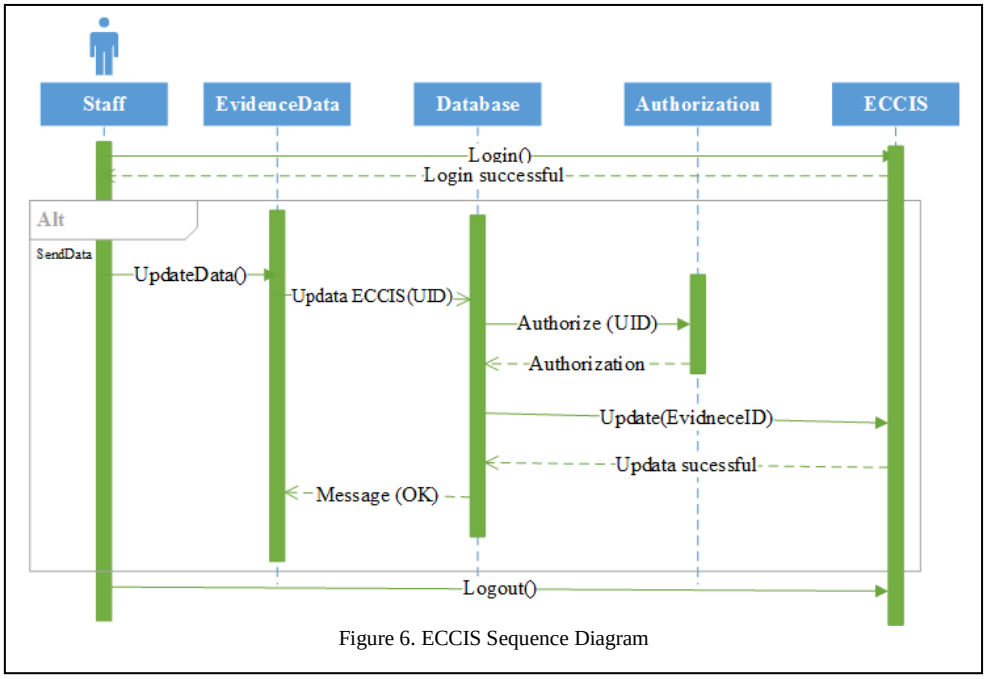

Figure 6. ECCIS Sequence Diagram

V. Results and Discussion

A. Baseline Study

Fig. 7 shows 84.62 % of the respondents who stated that the record management is maintained using paper and 15.38% stated that spreadsheet is used.

Regarding the starting point of evidence chain of custody documentation, fig.8 show 42.31% of respondents who said that they start at police station, 21.3% start at crime scene, 19.23% starts at the laboratory, and 17.31% start 'when preparing evidence for court'.

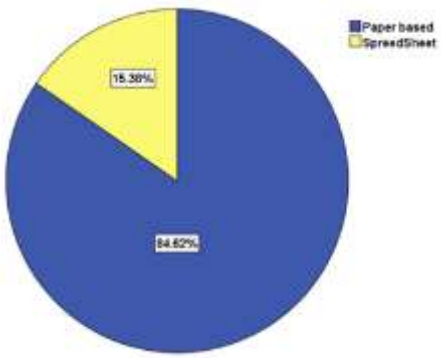

Figure 7. Form in which records are kept

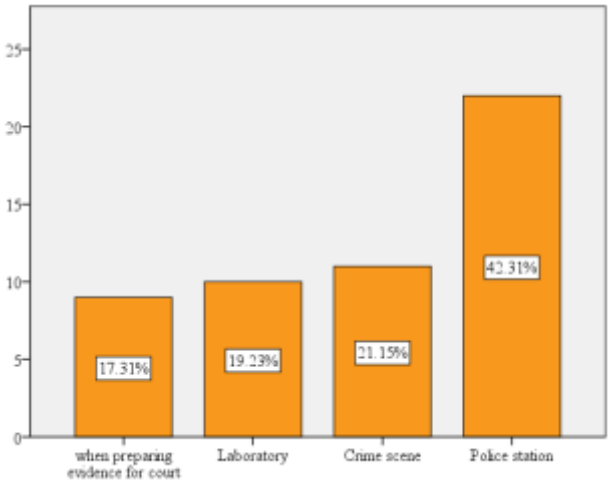

Figure 8. Point where evidence chain of custody starts

Concerning the point where evidence is pilfered or lost in the evidence life cycle fig.9 shows 67.31% stated that it happens as it moves from crime scene to the station, 30.77% started that it happens at police station and 1.92% stated that it happens at forensic laboratory.

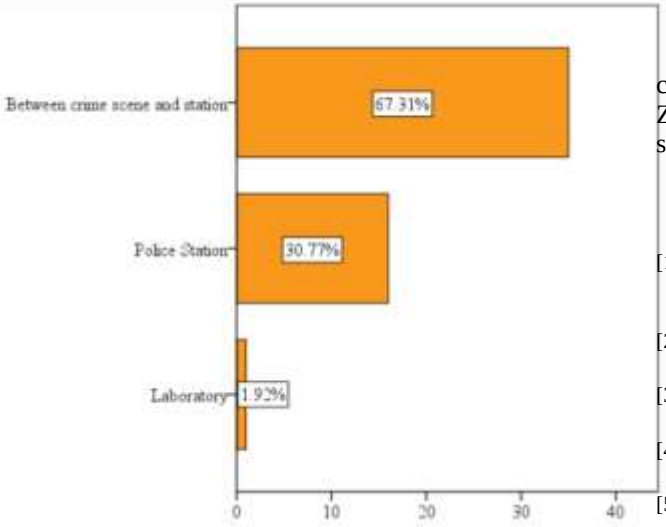

Figure 9. Point where evidence is lost or pilfered

B. Discussions

The aim of this study was to establish the challenges faced by the Zambia Police Force in regard to evidence management and further design an automated chain of custody and inventory system. The baseline study showed that the chain of custody and inventory system is done manually.

Regarding the issue of evidence documentation and chain of custody maintenance, the study showed only 21.3% of respondent's starts evidence documentation at right point (crime scene).

Based on the result it become evident that the manual system used by the Zambia Police is not effective. Automating the chain of custody and inventory system will improve the operations of the Zambia Police. The new system will also reduce human errors thereby producing accurate and credible data.

VI. Future Works

The scope of ECCIS does not go beyond chain of custody and evidence management. Future work must consider developing an integrated system which will merge with Judicial Court Management system and the Police Criminal Case Management Systems.

VII. Conclusions

In this paper, an automated chain of custody and inventory system is proposed. The ECCIS if adopted will afford a platform that will offer Zambia Police an opportunity to document and keep a watch over an item that is brought in as evidence. Any updates made to evidence information will be available online.

Acknowledgment

Thanks to the Zambia Police Force for allowing us to conduct this study on their organization. To member of Zambia Police Force at Headquarters thank you for you support.

References

[1] United Nations Office on Drugs and Crime, Crime scene and physical evidence awareness for non-forensic personnel, Vienna: United Nations Publication, 2009.

[2] K. M. Hess and C. H. Orthmann, Criminal Investigation, New York: Cengage Learning, 2010.

[3] B. A. J. Fisher And D. R. Fisher, Techniques Of Crime Scene Investigation, CRC Press: London, 2012.

[4] A. R. W. Jackson and J. M. Jackson, Forensic Science, 3rd Ed., London: Pearson Education Limited, 2011.

[5] J. J. Tomlinson, W. Elliott-Smith and T. Radosta, "Laboratory Information Management System Chain of Custody: Reliability and Security," Journal of Automated Methods and Management in Chemistry, vol. 2006, pp. 1- 4, 2006.

[6] A. R. W. Jackson and J. M. Jackson, Forensic Science, Harlow: Pearson Education Limited, 2011.

[7] J. VAN-DER and W. R. LUKE, "The Storage of Forensic Evidence at the Forensic Science Laboratory in Pretoria, South Africa," Transport and Logistics Studies, pp. 202-220, 2011.

[8] Zambia Police Force, "Zambia Police Force Strategic Plan 2013-2016," Zambia Police Force, September 2013. [Online]. Available: http://www.zambiapolice.gov.zm/index.php/downloads/category/8-police-acts-policies. [Accessed 10 February 2016].

[9] flsart.org, "www.flsart.org," December 2007. [Online]. Available: http://www.flsart.org/pdf/EVC-LP-2007-12.pdf. [Accessed 1 August 2015].

[10] W. S. W. M. Saman, "Electronic Court Records Management: A Case Study," Journal of e-Government Studies and Best Practices, vol. 2012, pp. 1-11, 2012.

[11] D. B. Viríssimo, A. Santiago, M. C. Machado, M. Y. Miyake, V. D. Giarone, M. G. Mazziero, H. F. W. Puhlmann and L. O. A. Ruiz, "Automating the chain of custody using RFID technology to support the validation of forensics evidence," in *International Workshop on Information - Forensic and Security*, São Paulo, 2011.

[12] A. Jones and C. Valli, Building a Digital Forensic Laboratory, Burlington: Elsevier, Inc, 2009.

[13] J. Cosic and Z. Cosic, "Chain of Custody and Life Cycle of Digital Evidence," Computer Technology and Application, vol. 3, pp. 126-129, 2012.

[14] M. M. Houck, Professional Issues In Forensic Science: Advanced Forensic Science Series, Oxford: Elsevier Inc. , 2015.

[15] A. Munoz, M. Uruena, R. Aparicio and G. Rodríguez-de-los-Santos, "Digital Wiretap Warrant: Improving the security of ETSI Lawful Interception," Digital Investigation, vol. 14, pp. 1-16, 2015.

[16] J. R. Vacca, Computer Forensics: Computer Crime Scene Investigation, 2nd Ed, Massachusetts: Charles River Media, Inc., 2005.

[17] D. L. Shinder, Scene of the Cybercrime: Computer Forensics Handbook, Rockland: Syngress Publishing, Inc., 2002.

[18] C. H. Malin, E. Casey and J. M. Aquilina, Malware Forensics Field Guide for Linux Systems: Digital Forensics Field Guides, New York: Elsevier Inc., 2014.

[19] M. W. Beckett, "The Missing Link: A Framework for Enhancing the Handling of Evidence by Law Enforcement," The Journal for Law Enforcement, vol. 3, no. 2, pp. 1-9, 2014.

[20] Y. Prayudi, A. Ashari and T. K. Priyambodo, "Digital Evidence Cabinets: A Proposed Framework for Handling Digital Chain of Custody," International Journal of Computer Applications, vol. 107, no. 9, pp. 30-36, 2014.

[21] California Commission on Peace Officer Standards and Training (POST): Management Counseling Services Bureau, Law Enforcement Evidence & Property Management Guide, California: California Commission on Peace Officer Standards and Training (POST), 2013.

[22] H. Kato, K. T. Tan and D. Chai, Barcodes for Mobile Devices, Cambridge: Cambridge University Press, 2010.

[23] J. T. Latta and R. E. Giles, "International Association for Property and Evidence, Inc. Professional Standards," 29 March 2010. [Online]. Available: http://www.iape.org/pdfFiles/IAPE-standards-2-10.pdf. [Accessed 12 October 2015].

[24] H. I. Bulbul, H. G. Yavuzcan and M. Ozel, "Digital forensics: An Analytical Crime Scene Procedure Model (ACSPM)," Forensic Science International, vol. 233, p. 244–256, 2013.

[25] G. Giova, "Improving chain of custody in forensic investigation of electronic digital systems," International Journal of Computer Science and Network Security, vol. 11, no. 1, pp. 1-9, 2011.

[26] Y. Prayudi and S. Azhari, "International Journal of Computer Applications," Digital Chain of Custody: State of the Art, vol. 114, no. 5, pp. 1-10, 2015.