Data Warehousing Based Computer Forensics Investigation Framework

Waleed Halboob [1,2], Ramlan Mahmod [2], Muhammad Abulaish [1], Haider Abbas [1], Kashif Saleem [1]

[1] Center of Excellence in Information Assurance, King Saud University, Saudi Arabia

[2] Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, 43400 Serdang, Selangor, Malaysia

{wmohammed.c, mabulais, hsiddiqui, ksaleem}@ksu.edu.sa, ramlan@fsktm.upm.edu.my,

***Abstract*—In this paper, we have proposed the design of an efficient computer forensics investigation framework. The proposed framework improves the investigation efficiency using Data Warehouse (DW) concept, which provides a selective evidence identification, collection and analysis. So, only relevant data is investigated instead of investigating the entire user data. The proposed framework consists of a Data Warehouse Engine (DWE) to selectively identify, collect and analyze digital evidences from multiple digital resources. A Digital Evidence Preservation (DEP) mechanism is also introduced for preservation of the collected digital evidences whose authenticity is ensured using cryptographic techniques. An access control mechanism is implemented to allow only authorized investigator to access the preserved digital evidences. The DEP mechanism provides court of law with a Secure Forensic Audit Trial (SFAT) that helps in tracking happened activities on the collected evidences for ensuring the authenticity and reliability of the presented digital evidence.**

Keywords: Computer forensics; Digital evidence; Efficiency; Data warehouse; Access control; Authenticity; and reliability.

I. INTRODUCTION

Digital forensics is a new research discipline which focuses on extracting digital evidences from digital data related to a crime. Digital data normally reside on digital media like PC, mobile, storage device, etc. Digital forensics investigation is a systematic process to identify, collect, preserve, analyze, and present digital evidences from digital data in such a way that they should be admissible, authentic, complete, reliable and believable by the court of law [1, 2, 3].

To facilitate forensics investigation process a number of forensic frameworks have been proposed by the researchers [4, 5, 6, 7, 8, 9, 10]. These are generally defined as a sequence of defined steps and their refinements along with inputs and outputs. More or less, the major steps are identified as *identification*, *collection*, *preservation*, *analysis* and *presentation*. A number of metrics have been also defined to evaluate the efficacy of a framework. This includes *generality*, *specificity*, *lawfulness*, *iterative*, *feedback*, *and computer support* [11]. Although, a good number efforts have been directed to solve digital forensics related issues during last decade the field but more works still required for addressing several open issues such investigation efficiency [12,13,14,15,16,17,18,19]. Investigation efficiency is one of the open challenges for computer forensics due to exponential increase in the size of digital storage media and data, and as a result, increasing the required time and effort for collecting and analyzing digital evidences.

In this paper, we have proposed the design of a computer forensics investigation framework to facilitate the extraction of reliable evidences in an efficient manner. The Data Warehouse Engine (DWE) module of the proposed framework takes care of investigation efficiency issue. It improves the efficiency by facilitating the investigator to selectively identify, collect and analyze digital evidences from multiple sources. Using the DWE, the investigation process is limited only to specific scope and goal so only relevant data is investigated. Our framework is also equipped with a Digital Evidence Preservation (DEP) mechanism, which preserves the collected digital evidences through ensuring its authenticity. The DEP also implements *access control* and *Secure Forensic Audit Trail* (SFAT) mechanisms. The access control mechanism controls access to the digital evidence so that it is accessible only by concerned authorities (e.g., investigator, court of law). The SFAT securely records all activities happened on the digital evidence from the time of evidence collection to the evidence presentation. As a consequence, through tracking the investigator activities recorded inside the SFAT the court of law can verify the authenticity and reliability of the presented evidences.

The rest of this paper is structured as follows. Section II presents a brief review of the related works on computer forensic frameworks and investigation efficiency. Section III presents the functional detail of the proposed framework. Section IV presents a discussion and critical evaluation of the proposed framework. Finally, Section V concludes the paper with future directions to enhance the proposed framework.

II. RELATED WORKS

Several computer forensics have been introduced until now. In 2001, Palmer have compiled the proceedings of the Digital Forensic Research Workshop after a thorough brain-storming among collaborative researchers, investigators and practitioners in digital forensics and termed it as DFRWS framework [10]. The DFRWS framework provides a non-specific and general investigation road map. In 2003, the DFRWS was extended by Stephenson [8] to a more specific framework called an End-to-End Digital Investigation (EEDI) that describes investigation activities with a digital

978-1-4799-8828-0/15 $31.00 © 2015 IEEE
DOI 10.1109/ITNG.2015.31

investigation process language (DIPL). An Electronic Crime Scene Investigation (ECSI) was presented in 2001 and reissued in 2008 by the Department of Justice, USA [20]. Unlike the DFRWS, the ECSI is more specific framework since it describes the investigation process in more details to be used as investigation guidelines in USA. In [9], a framework, called an Abstract Model of the Digital Forensics Procedures (AMDFP), has been proposed which is understandable and applicable to a variety of cases of computer forensics investigation. Carrier and Spafford [6] have introduced an Integrated Digital Investigation Process (IDIP) based on physical investigation process and they come out with a practical and useful framework. Later on, this framework is simplified by Carrier and Spafford [5] to a new framework called an Event-Based Digital Forensics Investigation Framework (EDFIF). A Hierarchical, Objective Based Framework (HOF) has been proposed by Beebe and Clark [4] with two new concepts *forensics principle* and *incident closure*. The former concept is based on an object-based investigation process instead of executing a sequence of pre-defined steps, whereas the latter concept is used for closing investigated crime.

For improving the investigation efficiency or, in other words, reducing the required investigation cost in term of time and resources, a number of research efforts have been proposed in [17,21,22,23,24,25,26,27,28,29]. These efforts use two different approaches namely *selective imaging* and *effective and efficient analytical* [13]. The selective imaging approach is used at collection stage. The key idea is to image or collect only relevant data instead of making a physical bit-by-bit image from whole hard drive. Current researches on selective imaging approach use *digital evidence bags* [22,24,25,26,27] and *risk sensitive digital evidence collection* [28] concepts. The effective and efficient analytical approach is applied to digital evidence analysis stage. In other words, a bit-by-bit image is made from the whole hard drive during the evidence acquisition so that the wholesome about the user data is collected. Then, the collected data is analyzed in a distributed manner. Researches using this approach have applied several concepts such as *distributed evidence analysis* [29] *data mining search process* [17], *file classification* [23], *clustering text-based search* [21]. However, the main problem associated with this effective and efficient analytical approach is that making a bit-for-bit image is very time consuming. Although, a number of research efforts have been directed to resolve the efficiency problem there are still several open issues. Bednar and Katos [30] and Beebe [13] have shown that there is a need for using data warehousing technique to provide investigators to help in deciding which data or subset of data should be imaged and analyzed.

III. Proposed Computer Forensics Framework

In this section, we present the design of our proposed computer forensics framework. The proposed framework emphasizes on four major steps, as illustrated in Figure 1, for a digital investigation process. These steps are: i) data gathering and forensic tools identification, ii) data warehousing, iii) evidence preservation, and iv) evidence presentation. These steps are further explained in the following sub-sections.

A. Data Gathering and Forensic Tools Identification

In this phase, an investigator plans and prepares for executing his investigation process through *awareness*, *search warrant and authorization*, *identification of tools/equipments*, *chain of custody* and *securing crime scene*. Each of these activities is discussed in the following sub-sections. The outputs of this phase are *awareness report*, *secure crime scene*, *search warrant*, *authorization*, *required tools/equipments* and *hand-written chain of custody*.

1) Awareness: Awareness is made when an investigation authority receives a digital crime report from a victim or another party. The awareness is a report that can include more details about the crime such as date, time and computing environment. Depending on the intensity and means of reported crime, the investigation authority decides whether the reported crime needs a computer forensic investigation or not.

2) Search Warrant and Authorization: If the need for computer forensic investigation has been identified in the previous step, the investigation authority seeks a search warrant and authorization letter from court of law before initiating the investigation process.

3) Identification of Tools/Equipments: Depending on the nature of digital crime, necessary tools and equipments are identified and prepared for investigation process. Both Data Warehouse Engine (DWE) and Digital Evidence Preservation (DEP) mechanisms are installed on a TPM-enabled Laptop and prepared for use. The TPM (Trusted Platform Module) is a chip installed in the Laptop for providing a trusted time-stamped which will be used during recording the activities of concerned authorities in the Secure Forensic Audit Trial (SFAT). At this stage also, each concerned authority is provided with an access control certificate and a pair of public and private keys. The DEP mechanism is initialized with the access control certificates of all concerned authorities. More information about the DEP initialization and SFAT will be presented in Section III.

4) Chain of Custody: A chain of custody is prepared for recording the investigation activities. The chain of custody will be used by court of law to ensure that the investigator didn't exceed the specified investigation scope and goal. As a result, the court of law can make sure that the digital evidence is trustworthy [31]. In our framework, two kind of chain of custody are used. The first is a hand-written chain of custody - mentioned here - used for recording all the investigation activities during the whole investigation process. Second is a Secure Forensic Audit Trial (SFAT), which is used for recording all the activities performed on the mined and secured digital evidences. It is further explained in Section III.

5) Securing Crime Scene: This step concerns about securing the crime scene to protecting digital evidence resources. Everything in the crime scene is secured and documented (e.g., by taking photography). Only authorized persons are allowed to access the crime scene. The crime scene can be victim and/or suspect computers.

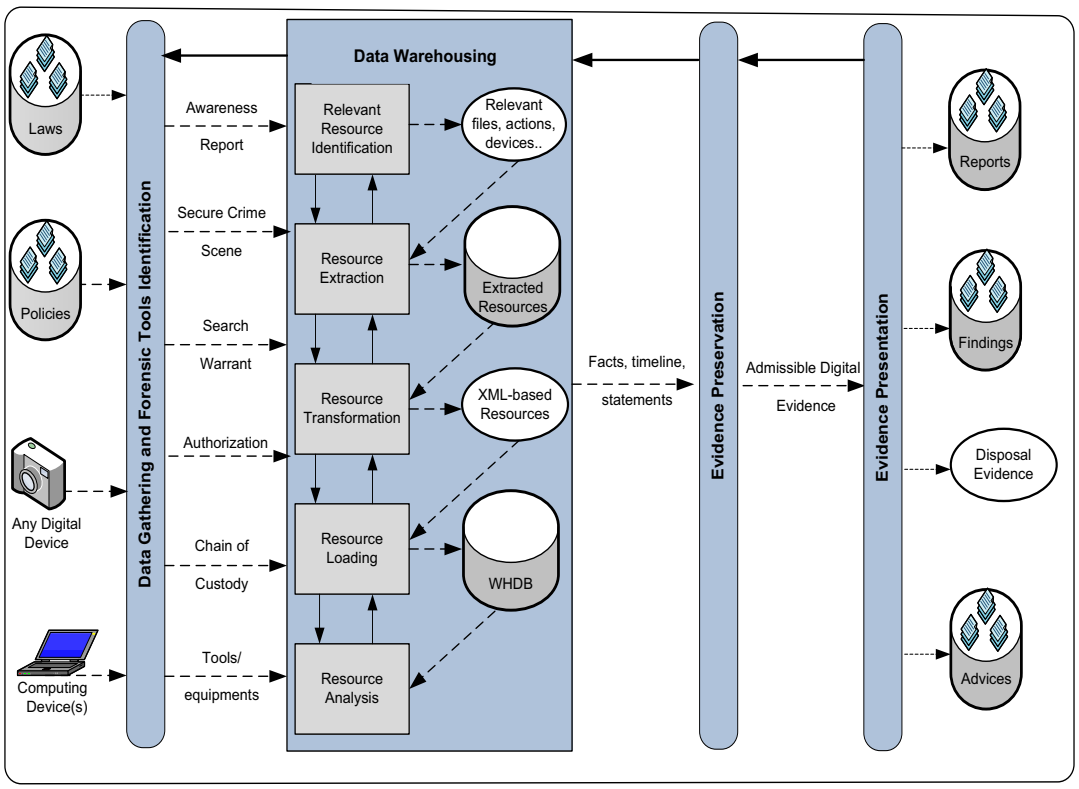

Figure 1. The General architecture of the proposed computer forensics framework

B. *Data Warehousing*

A Data Warehouse (DW) is defined by Inmon [32] as a *"subject-oriented, integrated, nonvolatile, and time-variant collection of data in support of managements' decisions"*. The DW provides a platform to analyze data at different levels of specifications. Moreover, if data is brought into data warehouse the data warehouse operations like slice, dice, roll-up, roll-down, etc. can be applied to analyze them for different levels of specificities. The integration of Data Warehouse Engine (DWE) in the proposed framework is responsible to collect and analyze all crime-related digital resources under a common umbrella through the process like r*elevant resource identification*, *resource extraction*, *resource transformation*, *resource loading* and *resource analysis*. In our framework, the data warehousing step covers the digital evidence collection and analysis steps proposed in existing computer forensics frameworks. The steps to create a data warehouse for the said purpose are explained in the following sub-sections.

1) Relevant Resource Identification: In this step, data relevant to the crime under investigation are identified from user data resources by investigator. Any data (such as images, videos, emails, etc.) found in user computer media storage can be considered as an internal resource.

2) Resource Extraction: In this phase, relevant resources identified during previous step are extracted to a temporal storage. Resource extraction is the most time-consuming process. A special program is required for extracting the relevant resources as well as cleaning them through removing unwanted chunks, interpolating/ extrapolating missing values, and resolving inconsistencies present either at schema level or at data level.

3) Resource Transformation: Resource transformation is used for transforming extracted resources into a suitable format, which could ease the analysis process. The extracted resources are converted into a unified data structure. We choose XML schema for representing transformed resources since XML languages becomes a de-facto standard for data representation and transformation.

4) Resource Loading: The relevant resources in the transformed structure (XML-based format) are loaded into a data warehouse. Loading process can be either new loading or updates loading. In new loading, new resources are loaded and

5) Resource Analysis: The loaded relevant resources are analyzed to understand the happened crime and collect digital evidence through reconstructing timeline, establishing facts and identifying suspect(s). In other words, investigator answers what happened, where, who did it, how, why, and when? The investigator can repeat the data warehouse analysis process over time to find more evidences.

C. *Evidence Preservation*

The evidence preservation is used for insuring digital evidence authenticity and confidentiality. For meeting this target, digital evidence preservation (DEP) mechanism is proposed which

preserves digital evidences by ensuring various security services. First, authenticity of the digital evidence is preserved by ensuring the evidence's integrity. This is very important point as crime evidence here is in a digital form which means it can be easily altered or fabricated. Second, a Secure Forensic Audit Trial (SFAT) is used for recording the activities of concerned authority (such as investigator) on the digital evidence. All activities are encrypted and then recorded inside the SFAT in a way that only court of law can decrypt it to see the happened activities. This allows the court of law to track the investigator activities to determine if the user privacy was disclosed or not, also if the digital evidence was fabricated or not. In case of disclosing or fabrication the collected evidence is not likely to be reliable and consequently not acceptable by the court of law. The proposed DEP mechanism preserves digital evidences through three major steps including initialization, Digital Evidence Authenticate and Archiving (DEAA), and Digital Evidence Secure Monitoring and Auditing (DESMA).These steps are further explained in the following sub-sections but starting with initializing the DEP.

1) Digital Evidence Authenticate and Archiving (DEAA): The digital evidence archive means packaging the digital evidence into files package (e.g., Java archive file) or into a secure USB drive. The execution of DEAA process is shown in Figure 2. First, investigator makes a bit-by-bit image from the original evidence. Then, both evidences (original and image) are separately signed with a general public key (GPK). The original evidence and its hash value are stored in a secure place called External Secure Storage (ESS) while the evidence copy and its hash value are stored in a temporal storage. In other hands, the original evidence is stored as a backup and the evidence copy is used as a working copy. The GPK is calculated as a sum of all public keys of all concerned authorities using the IBE-based key distribution schema proposed in [35]. For making distribution schema [35] used more secure, GPK is first initialized with a sum of two random public keys as recommended by Chien [36] as used in [37, 38, 39]. The SHA-2 is used because it is more secure than other hash functions such as MD5 and SHA-1.

2) Digital Evidence Secure Monitoring and Auditing (DESMA): After digital evidence is authenticated and archived, further access to it is controlled by a Digital Evidence Secure Monitoring and Auditing (DESMA) process. The DESMA receives the authentic and encrypted evidence and its hash value from the DEAA mechanism and also receives access control certificates of concerned authorities from court of law during data gathering and forensic tools identification phase. All these three inputs are stored inside which is generally termed as Internal Secure Storage (ISS). When a concerned authority wants to access the digital evidence he must be authenticated and authorized using his private key and access control certificate, respectively. During the authentication and authorization process, access to the digital evidence is audited by recording all activities happened on the digital evidence inside the Secure Forensic Audit Trial (SFAT). In addition, the activities are encrypted first with the GPK before storing them inside SFAT. So, the authorization used here is an encryption-based authorization in which access is allowed only if requester has a suitable private key. The recorded information can be ID of the requester as used in the requester's access control certificate, access time and data automatically captured from TPM-enabled Laptop, and digital signature of the requester. Whenever required, the court of law can print a report about the status of the digital evidence by listing the recorded information inside the SFAT.

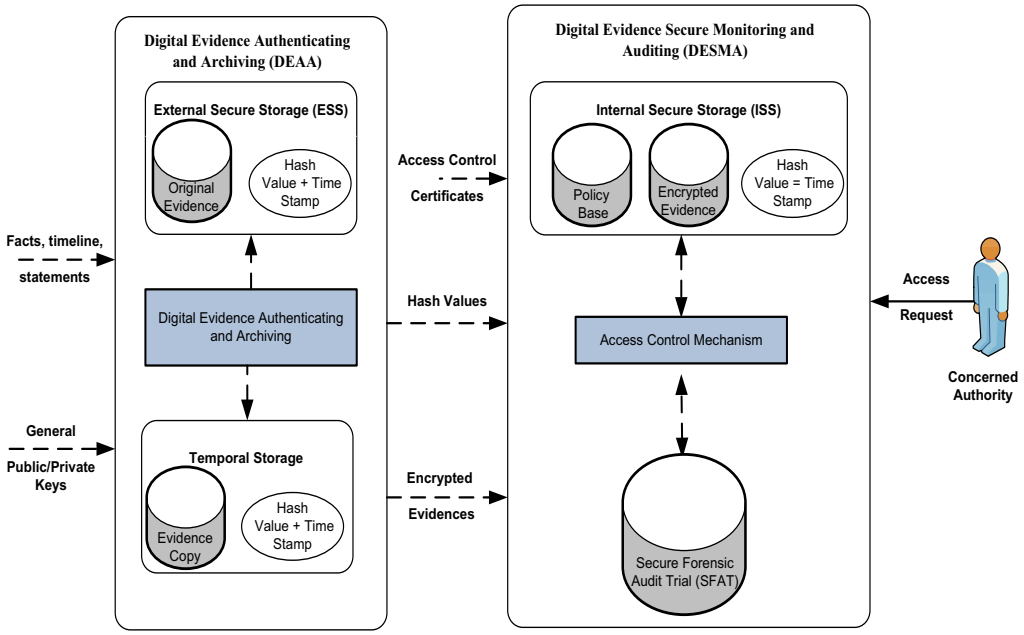

Figure 2. Digital Evidence Secure Archiving

D. Presentation

This step is generally concerned with presenting the findings of the investigation process to the court of law. This step is considered as outside the scope of this research.

IV. Discussion

In this section, we present a thorough discussion to establish the efficacy of the proposed framework over existing ones. For this purpose, we have chosen four existing digital forensics frameworks – Digital Forensic Research Workshop (DFRWS), Electronic Crime Scene Investigation (ECSI), Abstract Model of the Digital Forensics Procedures (AMDEP) and End-to-End Digital Investigation (EEDI). The evaluation process is based on four major criteria – *investigation process*, *usability*, *evidence reliability* and *investigation efficiency* that are generally used to evaluate digital forensics frameworks. Under each criterion there is a varying list of overlapping sub-criteria as shown in Table 1. The investigation process criterion is used for evaluating whether a computer forensic framework supports main investigation. These steps are the main required steps and became standard since the birth of DFRWS framework in 2001. The usability of a computer forensic framework is evaluated using what we called general requirements which are general, specific, lawful, iterative, feedback and computer support [11]. For evidence reliability, three criteria are used which are chain of custody, evidence authenticity and authorization. The chain of custody criterion measures whether the activities of an investigator during an investigation process are recorded or not. The evidence authenticity is used for ensuring whether the confidentiality and integrity of digital evidences are satisfied. The authorization is fulfilled if access to the digital evidence is controlled. Investigation efficiency was discussed in Section II and a computer forensic framework is efficient if it supports a selective imaging and/or an effective and efficient analytics. Table 1 provides comparative results of the proposed framework with the related ones. It seems that the proposed framework satisfies the most criteria when compared with other frameworks. In fact, it is difficult to discuss the result shown in Table 1 in more detail due to limited space provided here.

TABLE 1. A COMPARATIVE STUDY OF THE PROPOSED FRAMEWORK WITH EXISTING FRAMEWORKS

Main Criteria	Sub-criteria	DFRWS	ECSI	AMDEP	EEDI	Proposed
Investigation process	Identification	✓	Only securing and documenting the scene	Yes (crime identification/ required tools preparation)	×	Yes (Data Gathering and Forensic Tools Identification)
	Collection	✓	✓	✓	✓	✓
	Preservation	✓	×	✓	✓	✓
	Analysis	✓	✓	✓	✓	✓
	Presentation	✓	Only reporting	✓	✓	✓
Usability	General	✓	✓	✓	✓	✓
	Specific	×	×	×	✓	✓
	Lawful	✓	✓	✓	✓	✓
	Iterative	×	×	×	×	✓
	Feedback	×	×	×	×	✓
	Computer Support	✓	✓	✓	✓	×
Evidence Reliability	Chain of custody	✓	×	×	×	✓
	Preservation	✓	×	✓	✓	✓
	Authorization	×	×	×	✓	✓
Investigation efficiency	Selective collection	×	×	×	×	✓
	Effective and Efficient Analytical	×	×	×	×	×

V. Conclusion and Future Works

In this paper, we have proposed the design of an efficient computer forensic framework. The novelty of the proposed framework lies in improving the investigation efficiency while ensuring the digital evidences authenticity and reliability. The investigation efficiency is achieved using a data warehouse engine, which helps in providing novel selective evidence imaging in such a way that only the data related to the crime is investigated at different level of specificities. Besides using a hand-written chain of custody, the proposed framework preserves the digital evidences using digital evidence preservation mechanism, and erasing or wiping unrelated data. Development of the data warehousing engine (DWE), digital evidence preservation (DEP) mechanism and Secure Forensic Audit Trial (SFAT) mechanism along with evaluating them using an experiment study is our future work.

Acknowledgements

We would like to acknowledge Dr. Nur Izura Udzir, Dr. Mohd. Taufik Abdullah and Dr. Ali Deghantanha – in Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, Malaysia - for their supporting guidance and ideas.

REFERENCES

[1] Richter J, Kuntze N, Rudolph C: Securing Digital Evidence. In *Fifth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE'2010) 2010; The Claremont Resort, Oakland, CA, USA*. IEEE; 2010:119-129.

[2] Noblett MG, Pollitt MM, Presley LA: Recovering and Examining Computer Forensic Evidence. *Forensic Science Communication* 2000, 2(4):October.

[3] McKemmish R: What is forensic computing? Trends and Issues in Crime and Criminal Justices. *Volume 118*. Canberra: Australian Institute of Criminology; 1999:1-6.

[4] Beebe NL, Clark JG: A Hierarchical, Objectives-based Framework for the Digital Investigations Process. *Digital Investigation* 2005, 2(2):147-167.

[5] Carrier BD, Spafford EH: An Event-based Digital Forensic Investigation framework. In *In Proceedings of the 2004 Digital Forensic Research Workshop: 2004; Baltimore, Maryland*; 2004.

[6] Carrier B, Spafford EH: Getting Physical with the Digital Investigation Process. *International Journal of Digital Evidence* 2003, 2(2):1-20.

[7] Perumal S: Digital Forensic Model Based On Malaysian Investigation Process. *International Journal of Computer Science and Network Security* 2009, 9(8):38-44.

[8] The DFRWS Framework Classes [http://people.emich.edu/pstephen/my_papers/DFRWS_Classes.PDF]

[9] Reith M, Carr C, Gunsch G: An Examination of Digital Forensic Models. *International Journal* 2002, 1(3):1-12.

[10] Palmer G: Report from the First Digital Forensic Research Workshop (DFRWS). Utica, New York; 2001.

[11] Benredjem D: Contributions to Cyber Forensics: Processes and E-Mail Analysis. Concordia University, Electronical and Computer Engineering; 2007.

[12] Almulhem A: Network forensics: Notions and challenges. In *IEEE International Symposium on Signal Processing and Information Technology (ISSPIT'09): 2009; Ajman, UAE*; 2009:463 - 466

[13] Beebe N: Digital Forensics Research: The Bad, The God and the Unaddressed. In *Advances in Digital Forensics V - IFIP International Conference on Digital Forensics*. Orlando, Florida, USA; 2009:17-36.

[14] Adams CW: Legal Issues Pertaining to the Development of Digital Forensic Tools. In *Third International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE '08): 2008; Oakland, California, USA*; 2008:123-132.

[15] Spafford E: Some Challenges in Digital Forensics. In *Advances in Digital Forensics II - IFIP International Conference on Digital Forensics: 2006; National Centre for Forensic Science, Orlando, Florida, USA*. Springer; 2006:1-9.

[16] Srinivasan S: Security and Privacy in the Computer Forensics Context. In *International Conference on Communication Technology (ICCT'6): 2006; Guilin* 2006:1-3.

[17] Beebe N, Clark J: Dealing with Terabyte Data Sets in Digital Investigations. In *Advances in Digital Forensics II - IFIP International Conference on Digital Forensics. Volume 194/2005*. Orlando, Florida, USA: Springer; 2005:3-16.

[18] Bui S, Enyeart M, Luong J: Issues in Computer Forensics. Santa Clara University Computer Engineering, USA. 2003.

[19] Burmester M, Desmedt Y, Wright R, Yasinsac A: "Security or Privacy, Must We Choose?" In *Symposium on Critical Infrastructure Protection and the Law: 2002*. Computer Science and Telecommunication Board; 2002.

[20] Justice USDo: *Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition*: National Institute of Justice; 2008.

[21] Beebe NL, Clark JG: Digital Forensic Text String Searching: Improving Information Retrieval Effectiveness by Thematically Clustering Search Results. *Digital Investigation* 2007, 4(1):49-54.

[22] Turner P: Applying a Forensic Approach to Incident Response, Network Investigation and System Administration using Digital Evidence Bags. *Digital Investigation* 2007, 4(1):30-35.

[23] Sanderson P: Mass Image Classification. *Digital Investigation* 2006, 3(4):190-195.

[24] Richard G, Roussev V: File System Support for Digital Evidence Bags. In *Advances in Digital Forensics II - IFIP Advances in Information and Communication Technology. Volume 222/2006*. Springer; 2006:29-40.

[25] Turner P: Selective and Intelligent Imaging using Digital Evidence Bags. *Digital Investigation* 2006, 3(1):559-564.

[26] Turner P: Digital Provenance - Interpretation, Verification and Corroboration. *Digital Investigation* 2005, 2(1):45-49.

[27] Turner P: Unification of Digital Evidence from Disparate Sources (Digital Evidence Bags). *Digital Investigation* 2005, 2(3):223-228.

[28] Kenneallya EE, Brown CLT: Risk Sensitive Digital Evidence Collection. *Digital Investigation* 2005, 2(2):101-119.

[29] Richard G, Roussev V: Breaking the Performance Wall: The Case for Distributed Digital Forensics In *Proceedings of the 2004 Digital Forensics Research Workshop (DFRWS'04): 2004; Baltimore, Maryland*; 2004.

[30] Bednar P, Katos V: Digital Forensic Investigations: A New Frontier for Informing Systems. In *Proceedings of the 5th Conference of the Italian Chapter of the Association for Information Systems Challenges and Changes: People, Organizations, Institutions and IT: 2010; Paris, France*. Springer; 2010.

[31] Halboob W, Abulaish M, Alghathbar K: Quaternary Privacy-Levels Preservation in Computer Forensics Investigation Process. In *The 6th International Conference for Internet Technology and Secured Transactions (ICITST): 2011; Abu Dhabi* 2011.

[32] Inmon B: *Building the Data Warehousing, Third Edition*. New York: John Wiley & Sons, Inc; 2002.

[33] Boneh D, Franklin MK: Identity-Based Encryption from the Weil Pairing. In *Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology (CRYPTO '01): 2001; Santa Barbara, California, USA*. Lecture Notes in Computer Science, Springer-Verlag; 2001:213-229.

[34] Gagné M: Identity-based Encryption: A Survey. *RSA Laboratories Cryptobytes* 2003, 6(1):10-19.

[35] Du X, Wang Y, Ge J, Wang Y: An ID-based Broadcast Encryption Scheme for Key Distribution. *IEEE Transaction on Broadcasting* 2005, 51(2):264-266.

[36] Chien H-Y: Comments on an Efficient ID-Based Broadcast Encryption Scheme. *IEEE Transactions on Broadcasting* 2007, 53(4):809 - 810.

[37] Halboob W, Alghathbar KS, Mahmod R, Mamat A: TC-enabled and Distributed Cloud Computing Access Control Model. *Journal of Applied Science* 2012.

[38] Halboob W, Mamat A, Mahmod R: A Distributed Push-based XML Access Control Model for Better Scalability In *First International Conference of Distributed Frameworks and Applications (DFmA'2008): 2008; Malaysia, Penang, USM.* IEEE Publications.; 2008.

[39] Halboob W, Mamat A, Mohamod R, Khan MK: A Temporal and Delegable Secure Access to the Broadcasted XML Documents *Journal of Computer Science* 2012.