Quaternary Privacy-Levels Preservation in Computer Forensics Investigation Process

Waleed Halboob, Muhammad Abulaish, Khaled S. Alghathbar
Center of Excellence in Information Assurance
King Saud University
Riyadh, Saudi Arabia
{wmohammed.c, mabulaish, kalghathbar}@ksu.edu.sa

Abstract-- **Privacy preservation and computer forensics investigation are two contradictory information security directions. The privacy preservation principle stress on utmost protection of users privacy as privacy is a right, whereas computer forensics investigation attempts to unearth user data for possible digital evidences hidden within them. Although, a number of research efforts have been directed towards privacy preservation during forensics investigation process and consequently, forensics tools are in existence, most of them employ binary privacy levels, i.e., user privacy is either fully protected or not at all. In this paper, we introduce the concept of quaternary privacy levels and their protection mechanism in computer forensics investigation process. The privacy levels are identified on the basis of different entities and their participation roles during a computer forensics investigation process and represent different granule of privacy that can be enforced by the court of law depending on the nature of crime to be investigated. We also re-define the forensics investigation steps to regard different privacy levels for an investigation process.**

Keywords: Computer Forensics; Privacy Levels; Privacy Preservation, Digital Investigation; Access Control; Audit Trail.

I. INTRODUCTION

Due to easy availability and accessibility of internet and electronic media there is an exponential growth in digital data either in structured (databases) or unstructured formats (web pages, e-mails, forum posts, etc.). Consequently, the trend is also towards complete digital world. With time, computer hardware manufacturers are very successful in providing huge storage media at lower cost causing an implicit motivation to store every data in digital form. On the other hand, due to existence of non-social elements in our society, there is also an increase in digital crimes that are executed using digital technologies and digital media are becoming the instrument for many criminal activities. The wide use of digital technologies has made several challenges for policing in both public and private sectors. Crime investigation must be particularly adaptive to digital age as the digital technologies involve new types of criminal investigation. A large number of digital forensics investigation processes, tools and equipments have been developed for facing these challenges whereas every country and origination has to develop its own digital forensics investigation process based on its specified laws, policies, etc.

Nowadays, digital forensics is an emerging scientific area which focuses on unearthing digital evidences hidden within vast amount of digital data related to a crime. Digital data normally reside on digital device like PC, mobile, storage device, etc. Digital forensics investigation process is a number of systematic steps used to extract reliable evidences from digital data in such a way that they should be admissible, authentic, complete, reliable and believable by the court of law [1]. It includes several steps including *identification*, *collection*, *preservation*, *analysis*, and *presentation of digital evidences* [2, 3]. Digital forensics has three inter-related branches which are [4]: i) *computer forensics*, ii) *network forensics*, and iii) *software forensics*. Computer forensics deals with extraction of digital evidences residing on computer-related media like hard disks, compact disks, etc. Network forensics, also known as cyber forensics, deals with the problem of extracting digital evidences floating through the networks. Software forensics deals with the identification of meta-knowledge related to malicious softwares.

Several researches have been proposed to solve digital forensics related issues during the last decade. But, the field is still in its infancy and needs more works to address several open issues [5, 6, 7, 8, 9, 10 and 11]. One of the major problems faced by digital crime investigators for prosecuting a criminal involved in digital crime is to get reliable evidences hidden within digital data stored on his/her computing devices (laptop, computer, smart phone, etc.). Another related problem while investigating a digital crime is to protect user privacy which is his/ her fundamental right. Solving the conflict between privacy preservation and digital forensics investigation is still a serious challenge. Although, a number of research efforts have been directed towards privacy preservation and digital investigations independently, a limited number of efforts have been directed to solve the issue of privacy preservation during computer forensics investigation [7, 9, and 11]. These efforts are still not enough because they mostly solve the privacy issue using policy means and they did not show how the privacy of users can be enforced in a practical way during investigation process. Moreover, existing works consider only binary privacy-levels, i.e., user privacy during an investigation process is either fully preserved or not at all. To the best of our knowledge, multi-level privacy preservation in digital forensics has not been proposed yet and as a result, the binary privacy-levels are not flexible for different investigation cases, law enforcements, etc

In this paper, we have proposed the design of quaternary privacy-levels preservation scheme for computer forensics investigation process. The novelty of this paper lies in the definition of more generic and flexible quaternary privacy-levels based on different parties involved in a digital investigation process. We also re-define the digital investigation steps and provide a road-map for investigation authorities to respect different privacy levels as and when enforced by the court of law. A protection mechanism is presented for enforcing the identified privacy levels during a pre-defined general computer forensics investigation process. The authenticity of the collected digital evidence is also preserved by ensuring its integrity and confidentiality. Before and during the digital evidence collection, the confidentiality of user data is ensured using a chain of custody. Based on the preserved privacy level, access to the authentic digital evidence is controlled and audited so that the court of law can verify the reliability of the collected evidence by checking all activities happened on the collected digital evidence.

The rest of this paper is structured as follows. Section 2 presents a review of the related works on privacy preservation in computer forensics. Section 3 briefly presents our general computer forensics investigation process. Section 4 presents the defined quaternary privacy-levels. Section 5 presents the multi-level privacy preservation scheme for computer forensics. Finally, Section 6 concludes the paper with possible future work.

II. RELATED WORKS

In this section, state-of-the-arts related to privacy preservation in computer forensics are presented. In fact, the problem of privacy preservation in computer forensics comes when an investigator makes a bit-by-bit image from the whole data storage of user, and then the whole collected data is analyzed and presented to the court of law. The collected user data may contain a private data unrelated to the crime under investigation. Therefore, there is a need for dealing only with data related to the crime and handling it in a way that the privacy of users is preserved [12]. Burmester *et al*. [11] have studied the privacy challenges in digital forensics and suggested (i) specifying accountability and privacy policies to be enforced during real digital investigation process, and (ii) using cryptographic techniques for preserving the private data during evidence acquisition phase. State of privacy and digital forensics in USA has been studied by Adams [7] according to USA Amendment Act. This study suggests that the search warrant - obtained from court of law - should specify investigation scope and goal and an audit trail must be used for recording all investigation activities. This is to ensure that digital investigator didn't exceed the investigation scope and goal as well as to allow the court of law to verify the digital evidence reliability by tracing the investigators activities.

Other research efforts try to preserve the privacy of users by specifying privacy policies as *ethical rules* or *policy requirements*. In the former case, the privacy policies are specified by Government or digital forensics companies (digital forensics authority) as work ethics rules to control ethical behavior of the investigators. In other words, these policies just ensure (or show to customers) that the digital investigators will deal with private data of users ethically (in a confidential manner). In the latter case, the privacy policies are specified as requirements and enforced during investigation process. In fact, only Srinivasan [9] has defined such policies. Ten policies are defined by Srinivasan [9], four of them for computer forensics and the rest for network forensics. The specified policies for computer forensics are: i) Make two bit-by-bit copies from the user storage device, hash them and leave one copy (and its hash value) with user; ii) use wiping tools to remove any unrelated data to crime; iii) limit your search for digital evidence to scope and goal of the investigation; and iv) make a time-stamp for events and ensure that the time-stamped events are confidential.

It can be derived from the previous discussion that most of the previous works discuss only the conflicts between privacy and digital forensics or solve this conflict using a policy means. Development of useful and practical privacy-preservation solution for computer forensics investigation process is still an open issue as pointed out by [5, 8].

III. COMPUTER FORENSICS INVESTIGATION PROCESS

A computer forensics investigation process, also called a framework or a model, is defined as a sequence of steps and their refinements along with inputs and outputs. Several investigation processes have been proposed in [13, 14, 15, 16, 17, 18, and 19]. More or less, the major steps are identified as *identification*, *collection*, *preservation*, *analysis* and *presentation*. These steps are briefly introduced by the following sub-sections.

A. Planning and Preparing for Investigation

This phase refers to digital crime identification step, here an investigator (or investigation team) plans and prepares for executing his investigation process through several sub-steps namely *awareness*, *search warrant and authorization*, *identification of tools/equipments*, *chain of custody* and *securing crime scene*. The awareness is created by the victim to inform the investigation authority that a digital crime has been happened and then the investigation authority decides whether the reported crime needs a computer forensics investigation or not. If needed, search warrant and authorization letters are obtained from court of law. The authorization letter is required if the investigation laws and policies requires specified the authorized investigator, investigation date and time, etc. After that, all the required tools and equipments are identified and prepared. These tools/equipments must be already evaluated and proved by the court of law. The chain of custody is prepared for recording all activities of the investigator. The crime scene is secured from any illegal access that can modify the digital evidence may found in the crime scene.

B. Digital Evidence Collection

The digital evidence collection step is used for collecting digital evidence from a computer media (such as hard drive, flash memory, etc.). Two types of evidence collection are found in the literature *normal collection* and *selective collection*. In the normal collection, the whole user data is collected by making a bit-by-bit image from the whole user media. The problem with this type of collection is that the increased size of user media and data. Statistical research showed that imaging a 100GB hard drive needs about 4 hours [21]. The selective collection enables the investigator to image or collect only a subset of relevant data instead of making a physical bit-by-bit image from whole hard drive. Current researches on selective acquisition approach use *digital evidence bags* [22, 23, 24, 25 and 26] and *risk sensitive digital evidence collection* [21] concepts.

C. Digital Evidence Preservation

Basically, the digital evidence preservation means ensuring the digital evidence authenticity be encrypting and signing it. This is because that the collected evidence is in a digital form which means it can be easily modified and fabricated. Ensuring the digital evidence authenticity is not sufficient to preserve the privacy of user. In term of privacy preservation, the court of law must have a way to (i) ensure that the digital evidence will not be disclosed to the public, and (ii) tracks all activities happened on the collected and authentic digital evidence.

D. Digital Evidence Analysis

The investigator analyzed the collected data to understand the happened crime through reconstructing timeline, establishing facts and identifying suspect(s). In other words, investigator answers what happened, where, who did it, how, why, and when. Traditionally, investigator analyzes all the collected data but using this approach is not efficient and effective. Nowadays, several efficient and effective approaches have been proposed such as *distributed evidence analysis* [27], *data mining search process* [10], *file classification* [28], *clustering text-based search* [29].

E. Digital Evidence Presentation

This phase is generally concerned with presenting the findings of the investigation process to the court of law. Relevant activities related to this step are *reporting*, *evidence presentation*, *recommendation*, and *case closure*. In the reporting activity, the investigation process and its findings are studied, understood and then reported to the court of law. During the evidence presentation, digital evidence is presented to the court of law in admissible way. For recommendation activity, recommendations are written by investigator and submitted to both investigation authority and court of law. The recommendations may include new challenges, new required tools and recommendations to be considered in any future investigation. Finally, the case closure activity is used when the investigated case needs to be closed. At this point, the digital evidence must be either stay preserved/secured or disposed.

IV. QUATERNARY PRIVACY-LEVELS FOR COMPUTER FORENSICS

As mentioned earlier, binary privacy-levels advocates to protect user privacy either in total or not at all, which does not seem practical in many real-life scenario. In this section, we define a more flexible quaternary privacy-levels in context of computer forensics investigations. Our definition is based on three major factors – *digital data to be investigated*, *authorized investigators*, and *investigation team members*. All of these three are implied to have binary states resulting in total $2^3 = 8$ possible states, as shown in table 1. For example, the user data to be investigated can be classified into two categories depending on whether all data or only relevant data are considered for investigation process. This is because the computer forensics investigation is not always executed on all user data, rather it can be executed on only a selective subset of data (e.g., using a selective evidence collection) for several reasons such as to come out with digital evidence efficiently. Also, preserving the privacy of users requires investigating only a subset of data related to the happened crime in a secure and trusted manner while erasing or wiping unrelated data. Thus, the data to be investigated can be considered as '*all*' or '*relevant only*'. In case of consideration of all data no filtering step is required, whereas in case of the consideration of relevant only data a filtering step would be required to identify the subset of data relevant to the crime in hand. In table 1, second column represents this attribute in which '0' represents the consideration of all data, whereas '1' represent the consideration of only relevant data. Similarly, the responsible investigator can be either all investigation team or only some authorized investigator. Depending on the laws and nature of crime, sometimes the court of law may issue an authorization letter to authorize few investigators from the team members to execute the investigation process to get access of confidential and or private data. So, in some cases, a responsible investigator can be mapped to an authorized investigator or a team member constituting two different binary attributes – *authorized investigator* and *investigation team*. Since authorization process is not mandatory for all the cases, for “authorized investigator” attribute (shown in third column of table 1) ‘0’ indicates no authorization and ‘1’ indicates authorization. In case of no-authorization, the whole investigation team is allowed to access both private and public data, whereas in case of authorization, only authorized investigators are allowed to access private data. Since, in each investigation process constitution of an investigation team is a mandate requirement, for “investigation team” attribute (shown as fourth column in table 1) the binary values 1 and 0 do not represent its existence and non-existence respectively, rather they represent whether the team members are allowed to access private data or not.

TABLE 1. QUATERNARY PRIVACY-LEVELS

S. No.	Data (0: all data, 1: relevant only data)	Authorized Investigator (0: No authorization, 1: Authorization)	Investigation Team (0: not-allowed to access private data; 1: allowed to access private data)	Privacy Levels
1	0	0	1	Level-0
2	1	0	1	Level-1
3	0	1	0	Level-2
4	1	1	0	Level-3
5	0	1	1	Not Defined
6	1	1	1	Not Defined
7	0	0	0	Not Defined
8	1	0	0	Not Defined

Thus, we have three 2-state variables resulting in total eight possible combinations as shown in table 1. The first two rows (excluding header row), represents the case in which there is no authorization. In this case, the whole team is allowed to access the user data and privacy is controlled through data filtering mechanism. For example, first row (001) represents the case in which the whole data is accessible to all team members. This is defined as zero-level privacy (level-0) and termed as A2T (all-to-team). The second row (101) represents the case in which the team members are allowed to access only relevant data related to the crime. This defines the next privacy level (level-1) and termed as R2T (relevant-to-team).

The next two rows (third and fourth) represent the case in which there is an authorization from the court of law, i.e., some team members are authorized by the court of law to access user private data. The third row (010) represents a case in which the authorized investigators are allowed to access whole user data. This defines the next level of privacy (level-2) termed as A2A (all-to-authorized). Similarly, the fourth row (110) depicts the scenario in which the authorized investigators are allowed to access only relevant data to the crime. This defines the highest level of privacy (level-3) and termed as R2A (relevant-to-authorized

The bit-strings represented by the last four rows of table 1 do not represent any practical forensics investigation scenario. For example, the bit-string 011 of fifth row represents an investigation scenario comprising authorized investigators in which all data are accessible to the investigation team. This contradicts the purpose of the appointment of authorized investigators by the court of law to access users private data. Similar scenario is represented by the bit-string of sixth row. The last two rows 9seventh and eighth) are obviously not valid as they represent an investigation scenario in which there is no authorized investigator and user data (all or relevant only) are not accessible to the investigation team.

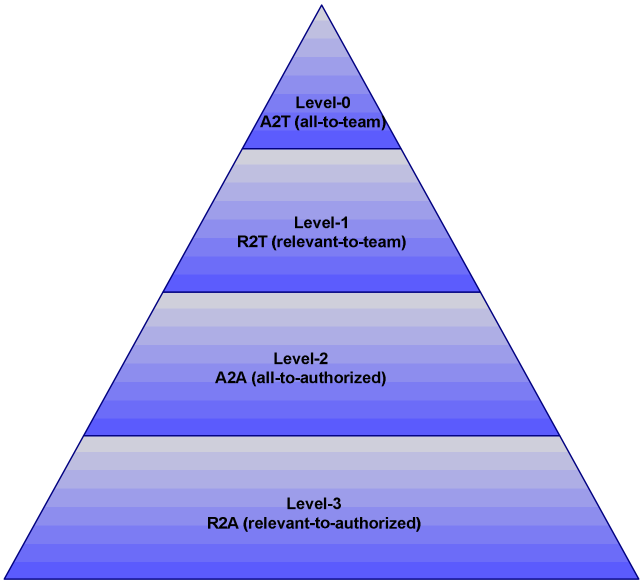

Fig. 1. Quaternary privacy-levels

All the four privacy-levels defined so are termed as quaternary privacy-levels and depicted in fig. 1 using cone representation highlighting the fact that the privacy restriction is directly proportional to the area inscribing them, i.e., more the area more the privacy level. With privacy level-0 (A2T), all user data is public to all invesrigation team. In privacy level-1 (R2T), only relevant data is public to all investigation team. The privacy level-2 (A2A) is used when all user data is public to only the authorized investigators from the team. Finally, the privacy level-3 (R2A) is used when only relevant data is public to only authorized investigators.

V. MULTI-LEVELS PRIVACY-PRESERVATION SCHEME

In this section, we present the design of multi -levels privacy preservation scheme for computer forensics investigation process. The proposed scheme shows how the defined quaternary privacy-levels can be enforced during a computer investigation process. As mentioned early, a computer forensics investigation process contains several steps and each step has its own sub-steps, input, output, etc. In our proposed scheme, we show which investigation steps (and sub-steps) should be executed or omitted during enforcement of different privacy levels defined in the previous section. For privacy level-0, in which all data can be accessed by all investigation team, it is clear that the authorization letter is not required as all investigation team are authorized. Also, normal digital evidence collection and analysis is used, the selective collection and effective/efficient analysis are optional as they can be used only if the investigation team wants to come up with the digital evidence efficiently. Using an access control and audit trail mechanisms are also optional options. When the next privacy level, level-1, is used, all data is accessible by only authorized investigation team. So, an authorization letter is required during planning and preparing step. The authorization letter must determine the authorized investigation team, data and time as well as investigation scope and goal.

Then, access control and audit trail mechanisms must applied to i) control access to collected digital evidence, and ii) audit any access or activity happened on the collected digital evidence in a trusted manner. Auditing is very important issue to allow the court of law to check, at the end, all the activities happened on the digital evidence to establish the reliability of the found evidences. For preserving the privacy level-2, in which only relevant data is accessible by all investigation team , the authorization letter is not required as all investigation team are authorized. But, the access control and audit trial can be used as optional activities for providing more secure and reliable digital evidence. The most important things here is that only the relevant data must be collected and analyzed selectively through the existing selective evidence collection and effective analysis approaches. The selective evidence collection and effective analysis must also be used when the privacy level-3 is chosen along with obtaining the authorization letter from the court of law. The access control and audit trail are used. Table 2 summarizes the computer forensics investigation steps needed for the enforcement of quaternary privacy levels.

TABLE 2. INVESTIGATION STEPS NEEDED FOR THE ENFORCEMENT OF QUATERNARY PRIVACY LEVELS

Main Investigation steps	Investigation sub-steps	Level-0	Level-1	Level-2	Level-3
Investigation Planning and Preparing	Awareness	✓	✓	✓	✓
	Search warrant	✓	✓	✓	✓
	Authorization	×	✓	×	✓
	Identification of tools/equipments	✓	✓	✓	✓
	Chain of custody	✓	✓	✓	✓
	Securing crime scene	✓	✓	✓	✓
Digital Evidence Collection	Normal selection	✓	✓	×	×
	Selective Collection	optional	optional	✓	✓
Digital Evidence Preservation	Evidence authenticity	✓	✓	✓	✓
	Access control	optional	✓	optional	✓
	Audit trail	optional	✓	optional	✓
Digital Evidence Analysis	Normal analysis	✓	✓	×	×
	Effective and efficient analysis	optional	optional	✓	✓
Digital Evidence Presentation	Reporting	✓	✓	✓	✓
	Evidence presentation	✓	✓	✓	✓
	Recommendation	✓	✓	✓	✓
	Case closure	✓	✓	✓	✓

VI. CONCLUSION AND FUTURE WORK

In this paper, we have defined generic and flexible quaternary privacy-levels that can be enforced by the court of law to protect user privacy during an investigation process. As opposed to binary privacy-levels which allows to protect user privacy either complete or not at all, the proposed quaternary privacy-levels provides flexibility to the court of law and/ or computer forensics investigators to decide an appropriate level of privacy (depending on the nature of crime) to be preserved in an investigation process. We have also provides through re-defining computer forensics investigation steps to adhere different privacy-levels in a practical way. Along with regarding the binary privacy-levels (defined as level-0 and level-3 in our scheme) generally used by many researchers, our approach provides more flexibility in user privacy preservation and a balance with computer forensics investigation process. Presently, we are working towards the development of a complete multi-levels privacy preserving computer forensics investigation framework based of Saudi e-crime law.

ACKNOLOGMENT

I would like to acknowledge my PhD supervisory committee members - Assoc. Dr. Ramlan Mahmod (chairman), Assoc. Dr. Zuriati Ahmad and Dr. Nur Izura– in Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, Malaysia for their supporting guidance and ideas.

REFERENCES

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

[2] B. Böck, D. Huemer, and A. M. Tjoa, "Towards More Trustable Log Files for Digital Forensics by Means of "Trusted Computing”," *in AINA '10 Proceedings of the 2010 24th IEEE International Conference on Advanced Information Networking and Applications* 2010.

[3] R. Slade, *Software Forensics: Collecting Evidence from the Scene of a Digital Crime*. New York: McGraw Hill, 2004.

[4] P. Stephenson, "The Forensic Investigation Steps," *Computer Fraud & Security*, pp. 17-19, 2002.

[5] Almulhem, "Network forensics: Notions and challenges," *in IEEE International Symposium on Signal Processing and Information Technology (ISSPIT'09)*, Ajman, UAE, 2009, pp. 463 – 466.

[6] N. Beebe, "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, pp. 17-36.

[7] Adams, C. W. (2008). Legal Issues Pertaining to the Development of Digital Forensic Tools," *in Proceedings of the 2008 Third International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE '08)*, Oakland, California, USA, 2008, pp. 123-132.

[8] E. Spafford, "Some Challenges in Digital Forensics," *in Advances in Digital Forensics II - IFIP International Conference on Digital Forensics, National Centre for Forensic Science*, Orlando, Florida, USA, 2006, pp. 1-9.

[9] S. Srinivasan, "Security and Privacy in the Computer Forensics Context," *in International Conference on Communication Technology (ICCT'6)*, Guilin 2006, pp. 1-3.

[10] N. Beebe and J. Clark, "Dealing with Terabyte Data Sets in Digital Investigations," *in Advances in Digital Forensics II - IFIP International Conference on Digital Forensics*. vol. 194/2005 Orlando, Florida, USA: Springer, 2005, pp. 3-16.

[11] M. Burmester, Y. Desmedt, R. Wright, and A. Yasinsac, ""Security or Privacy, Must We Choose?"" *in Symposium on Critical Infrastructure Protection and the Law*, 2002.

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

[13] G. Palmer, "*Report From the First Digital Forensic Research Workshop (DFRWS)*," Utica, New York 2001.

[14] P. Stephenson, "The DFRWS Framework Classes.", 2003.

[15] N. L. Beebe and J. G. Clark, "A hierarchical, objectives-based framework for the digital investigations process," *Digital Investigation*, vol. 2, pp. 147-167, 2005.

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

[17] B. Carrier, E. H. Spafford, B. Carrier, and E. H. Spafford, "Getting Physical with the Digital Investigation Process," *International Journal of Digital Evidence* vol. 2, pp. 1-20, 2003.

[18] B. D. Carrier and E. H. Spafford, "An Event-based Digital Forensic Investigation framework," *in In Proceedings of the 2004 Digital Forensic Research Workshop*, Baltimore, Maryland, 2004.

[19] P. Stephenson, "A Comprehensive approach to digital incident investigation," *Information Security Technical Report*, vol. 8, pp. 42-54, 2003.

[20] M. Reith, C. Carr, and G. Gunsch, "An Examination of Digital Forensic Models," *International Journal*, vol. 1, pp. 1-12, 2002.

[21] Kenneallya and C. L. T. Brown, "Risk sensitive digital evidence collection," *Digital Investigation*, vol. 2, pp. 101-119, 2005.

[22] P. Turner, "Unification of digital evidence from disparate sources (Digital Evidence Bags)," *Digital Investigation*, vol. 2, pp. 223-228, 2005.

[23] P. Turner, "Digital provenance - interpretation, verification and corroboration," *Digital Investigation*, vol. 2, pp. 45-49, 2005.

[24] Richard and V. Roussev, "Breaking the performance wall: The case for distributed digital forensics " *in Proceedings of the 2004 Digital Forensics Research Workshop (DFRWS'04)*, Baltimore, Maryland, 2004.

[25] P. Turner, "Selective and intelligent imaging using digital evidence bags," *Digital Investigation*, vol. 3, pp. 559-564, 2006.

[26] P. Turner, "Applying a forensic approach to incident response, network investigation and system administration using Digital Evidence Bags," *Digital Investigation*, vol. 4, pp. 30-35, 2007.

[27] Richard and V. Roussev, "Breaking the performance wall: The case for distributed digital forensics " *in Proceedings of the 2004 Digital Forensics Research Workshop (DFRWS'04)*, Baltimore, Maryland, 2004.

[28] P. Sanderson, "Mass image classification," *Digital Investigation*, vol. 3, pp. 190-195, 2006.

[29] N. L. Beebe and J. G. Clark, "Digital forensic text string searching: Improving information retrieval effectiveness by thematically clustering search results," *Digital Investigation*, vol. 4, pp. 49-54, 2007.