Analyses of the State-of-the-art Digital Forensic Investigation Process Models

Aleksandar Valjarevic, H.S. Venter
Department of Computer Science
University of Pretoria, Department of Computer Science, University of Pretoria, Pretoria 002
Tel: +27 78 2508435, Fax: +27 12 362 5188
email: alexander@vlatacom.com, hventer@cs.up.ac.za

Abstract- **Digital forensics gained much importance over the past decade. There is, however, currently no international standard formalising the digital forensic investigation process, nor does a harmonised digital forensic investigation process exist. The research focus of this paper is to analyse the state-of-the-art digital forensic investigation process models. Relevant digital forensic investigation process models are analysed and conclusions are made on similarities, differences and possibilities for harmonisation. Based on the comparison performed, the authors conclude that there are numerous disparities among existing digital forensic investigation process models. However, the main and the most important principles for such a harmonised digital forensic investigation process are common amongst many of the models analysed in this paper. The authors believe that this analysis is a noteworthy contribution towards the future development of a harmonised digital forensic investigation process model.**

Index Terms—standards, digital forensics, digital forensic investigation, digital forensic investigation process, digital forensic investigation process model

I. INTRODUCTION

Today, as information technology advances at a very high rate, digital forensics is rapidly gaining importance. Information security incidents constantly highlight the importance of digital forensics.

Digital or electronic evidence comprises information and data of investigative value stored on or transmitted by an electronic device. As such, electronic evidence is latent evidence in the same sense that fingerprints or DNA evidence is latent [2]. Dealing with digital evidence, therefore, requires a standardised and formalised process in order for digital evidence to be accepted in a court of law.

Methods and process models for digital forensics have been developed mostly by practitioners and forensic investigators, based on personal experience and expertise, on ad hoc bases, without the aim to reach harmonisation or standardisation in the field. In the past decade, there were also a number of academic research projects conducted in order to establish a digital forensic investigation process model. There is, however, currently no international standard formalising the digital forensic investigation process, although an effort to standardise the process has started within International Standardization Organization (ISO), by the authors [3]. Up to date there does not exist a harmonised digital forensic investigation process.

It is with this in mind that authors defined the research focus of this paper. In this paper the authors analyse the state-of-the-art of digital forensic investigation process models. The aim of the research is to analyse the characteristics of such existing models. Relevant models are analysed and compared. Models are later discusses, and conclusions are made on similarities, differences and possibilities for harmonisation.

The authors see this research as a step towards a harmonised digital forensic investigation process model.

The paper is structured as follows: The first section has introduced the paper and explained the research focus of the paper. Section II explains the motivation for the research. Section III provides a background on digital forensics and legal requirements regarding digital forensics. After that, Section IV provides detailed comparative analyses of the state-of-the-art of digital forensic investigation process models. Section V concentrates on discussing the results of the analyses. Section VI concludes this paper and indicates possible future work.

II. MOTIVATION

Why would it be important to reach harmonisation in this field? Providing guidelines for investigation principles and processes should bring higher admissibility of digital evidence to the court of law. It should also expedite investigations because there would be proper guidelines in the order of events during an investigation. Such guidelines would also be a good departure point to encourage the proper training of inexperienced investigators.

The need for a harmonised digital forensic investigation process model is most prominently seen in a court of law. In order to be able to claim in court that a standard process was used during a digital forensic investigation, a harmonised digital forensic investigation process model should exist and be adhered to.

As an example, the Daubert rule [4], commonly used in the USA for expert witness testimony, clearly states that theories and techniques used to draw conclusions on cases must give a positive answer to the following questions: Whether the theories and techniques employed by the scientific expert have been tested; Whether they have been subjected to peer review and publication; Whether the techniques employed by the expert have a known error rate; Whether they are subject to standards governing their application; and Whether the theories and techniques employed by the expert enjoy widespread acceptance.

This clearly indicates need for harmonised and ultimately standardised digital forensic process.

III. BACKGROUND

This section gives background on digital forensics and legal requirements pertaining to digital forensics.

A. On digital forensics

Digital forensics is defined as the use of scientifically derived and proven methods towards the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorised actions shown to be disruptive to planned operations [2].

Digital forensics is in practice applied whenever it is needed to investigate digital evidence arising from an incident, no matter whether the incident is of a criminal nature or not. The process used for digital forensic investigations has not been standardised or harmonised to date.

Although practice shows that the requirement to firmly follow certain digital forensic process is stronger in cases that are expected to finish at court of law, the authors believe that the same principles should be applied both to investigations that are expected to produce digital evidence for court of law and those that are not expected (i.e. internal company investigation.

B. On legal requirements

In this section the authors give an overview of the legal requirements pertaining to digital forensics and especially the admissibility of digital evidence in a court of law. This overview is not comprehensive but aims to provide the reader with a sense of the need for a harmonised, and ultimately, a standardised digital forensic investigation process. The authors are including this in background section in order for reader to better understand the need for harmonised and standardised digital forensic investigation process.

It should be noted that legal requirements may differ extensively in different jurisdictions across the world. The premise of this section is not to advocate specific legal systems, but rather to note the generic requirements in terms of legal issues that should be adopted by the legal system of a specific jurisdiction.

For example, in the United Stated of America cases that include the presentation of digital evidence are treated under rule 702 of the Federal Rules of Evidence, which says: "If scientific, technical, or other specialised knowledge will assist the trier of fact to understand the evidence or to determine a fact in issue, a witness qualified as an expert by knowledge, skill, experience, training, or education, may testify thereto in the form of an opinion or otherwise." For application of this rule, the Daubert case [4] is the most important.

Other countries have similar requirements regarding the admissibility of digital evidence. In the United Kingdom, examiners usually follow guidelines issued by the Association of Chief Police Officers (ACPO) for the authentication and integrity of evidence [5] [6] [7]. These guidelines are widely accepted in courts of England and Scotland, but they do not constitute a legal requirement and their use is voluntary [7]. The European Committee on Crime Problems (CDPC), known as the Committee of Experts on Crime in Cyber-Space (PC-CY), finished a draft convention on cyber-crime. This convention makes numerous references to the collection and exchange of electronic evidence [5].

Note that this paper does not analyse influences of different legal requirements to digital forensic process models.

The next section gives comparison of state-of-the-art digital forensic investigation process models.

IV. COMPARISON OF DIGITAL FORENSIC INVESTIGATION PROCESS MODELS

First, the authors analyse characteristics of state-of-the-art digital forensic investigation process models, in sub-section A. Later, in sub-section B comparisons of these models is given.

A. Analyses of characteristics of digital forensic investigation process models

Since the first Digital Forensic Research Workshop (DFRWS) in 2001 [2], the need for a standard framework for digital forensics has been widely acknowledged by the information security society. The Digital forensic investigation process model proposed at this workshop includes the following seven phases: Identification, Preservation, Collection, Examination, Analysis, Presentation and Decision. The process model was defined as iterative. It was recognised that greater effort should be made to move towards a more accurate definition of the process model.

Reith, Carr and Gunsch [10] proposed a digital forensic investigation process model known as the abstract model, which includes the following phases: Identification, Preparation, Approach strategy, Preservation, Collection, Examination, Analysis, Presentation and Returning evidence. They have recognised that existing digital forensic procedures are neither consistent nor standardised, and efforts made in this field often concentrate too much on specific technology, without considering a generalised process.

The U.S. Department of Justice (DOJ) published a process model in the Electronic Crime Scene Investigation Guide aimed at first responders [11]. This proposed process model includes the following phases: Preparation, Recognition and identification, Documentation of the crime scene, Collection and preservation, Packaging and transportation, Examination, Analysis and Reporting. The DOJ also gives a comprehensive list of types of digital evidence, their associated locations and associated crimes.

Carrier and Spafford [12] propose a process model based on the following requirements:

- The model must be based on existing theory for physical crime investigations.
- The model must be practical and follow the same steps that an actual investigation would take.
- The model must be general with respect to technology and not be constrained to current products and procedures.
- The model must be specific enough that general technology requirements for each phase can be developed.

- The model must be abstract and apply to law enforcement investigations, corporate investigations, and incident response.

The model proposed by Carrier and Spafford [12] includes 17 phases organised into the following five groups: Readiness Phases, Deployment Phases, Physical Crime Scene Investigation Phases, Digital Crime Scene Investigation Phases and Review Phase.

Carrier and Spafford also proposed another (similar) event-based process model [13]. This model is again based on physical crime investigation and it is suggested that digital crime scene investigation should occur as a subset of a physical crime scene investigation. The paper concentrates on digital crime scene investigation phases and how to find the causes and effects of events during a digital forensic investigation. In this paper they also stated that choosing a process model is a subjective and that it is quite likely that there will never be agreement on a single model.

Mandia and Prosise [14] proposed a digital forensic investigation process known as the incident model, which contains the following phases: Pre-incident Preparation, Detection of the Incident, Initial Response, Response Strategy Formulation, Duplication (System backup), Investigation, Secure Measure Implementation (Isolation and containing the suspect system), Network Monitoring, Recovery (Recovery of the suspect system to original phase), Reporting and Follow-up.

Beebe and Clark [15] proposed a hierarchical, objectives-based digital forensic investigation process model and also drew a comprehensive comparison between their proposed process model and previous works in this field. The model they proposed is multi-tiered, which constitutes a novel approach. They also suggested that previous models were often too high level and lacked more details on the proposed phases. Their aim was to leverage the achievements of previously proposed frameworks and models for digital forensic investigation process and to create synergy between these different perspectives. First-tier phases proposed by Beebe and Clark [15] include the following: Preparation, Incident response, Data collection, Data analysis, Findings presentation and Closure. In their opinion, second-tier sub-phases should be defined in such a way that these are inclusive of all possible types of crime and types of digital evidence. They also stated that sub-phases should consist of task hierarchies subordinate to specific objectives. In their paper [15] they applied this proposed principle to the data analysis phase.

Cuardhuain [16] proposed an extended and comprehensive model of cybercrime investigations, which is very comprehensive. The proposed model also includes information flow description between different phases. (This approach has not been seen in other models.)

Cohen [17] proposed a process model that includes the following phases: Identification, Collection, Preservation, Transportation, Storage, Analysis, Interpretation, Attribution, Reconstruction, Presentation and Destruction. Cohen also suggests that all of the above actions must be performed in a manner that meets the legal standards of the jurisdiction and the case.

Casey and Rose [18] define phases of digital forensic investigation process as: 1. Gather information and make observations, 2. Form a hypothesis to explain observations, 3.Evaluate the hypothesis, 4.Draw conclusions and communicate findings.

Cohen, Lowrie and Preston in [19] discuss the state of the science of digital evidence examination and consensus in digital evidence examination. They recognise that numerous calls have been made for scientific approaches and formal methods in the field of digital forensics [19] [20] [21] [22] [23] [24] [25]. They [19] also conclude that much further work is needed to reach consensus in the field of digital forensics, including the following:

[1] A preliminary review of the literature and the performing of more comprehensive studies of scientific consensus over a broader range of issues;

[2] Texts that accurately reflect the historical terms and uses in the field, and increased requirements of rigor in the use of terminology in peer-reviewed publications;

[3] The definition and widespread promulgation of a common language for the field that is reflected in the literature and review processes for publication;

[4] The creation of a better set of reference sources and an educational process to move toward consensus;

[5] The creation of a common body of knowledge backed up by theory and experiments that are widely repeated and taught universally.

As previously said, in the United Kingdom, examiners usually follow guidelines issued by the Association of Chief Police Officers (ACPO) for the authentication and integrity of evidence [5] [6] [7]. These guidelines do not explicitly set out digital forensic investigation process model, but through recommendations given process model can be constructed, containing following phases: Preparations for investigation, Crime scene group of phases, Secure and control the crime scene, Photograph and document the scene, Initial collecting of volatile data, Attaching exhibit labels, Documenting each action performed, Transport, Storage, Evidence recovery group of phases, The collection phase, The Examination phase, The Analyses phase, The Reporting phase, Disclosure. Further, recommendations in [6] are based on following principles:

Principle 1: No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court.

Principle 2: In circumstances where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.

Principle 3: An audit trail or other record of all processes applied to computer-based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.

Principle 4: The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.

These principles translate to ensuring evidence preservation and following proper digital forensic investigation process, while following applicable laws and general investigation principles.

B. Analyses of digital forensic investigation process models

In this section, a comparison of the state-of-the-art of digital forensic investigation process models is conducted.

Table 1 shows the comparison. The comparison is performed through mapping of characteristics of state-of-the-art digital forensic investigation process models against reference characteristics defined by the authors.

The mapping is performed against so-called reference phases proposed by the authors. These reference phases result from a deduction of the phases from existing digital forensic investigation process models. Note, however, deducing these reference phases does not mean proposing these as phases for a harmonised process model. The deduced phases are used merely for mapping purposes of such a comparison.

The authors deduced the following reference phases from their research conducted: Incident detection, First response, Planning, Preparation, Incident scene documentation, Potential evidence identification, Potential evidence collection, Potential evidence transportation, Potential evidence storage, Potential evidence analysis, Presentation, Conclusion.

Mapping is also performed against actionable principles. We define actionable principles as the principles which should be translated into actions within the digital forensic investigation process (i.e. principle that evidence's integrity must be preserved through the process and that chain of evidence must be preserved). These principles are found in one or more existing models. While in most of the models analysed, these are defined as principles, there are cases where these principles have already been translated to actions in the form of a phase in the model (i.e. in [12] the principle that there should be interaction with physical investigation of the actual crime scene is translated in *physical crime scene investigation group of phases*).

Therefore the authors to not invent these principles, but propose different approach to their implementation, through translating them to actionable items.

The authors propose the following actionable principles:

1. Interaction with the physical investigation [6] [12]

The authors note that the digital forensic process can be dependent on and interconnected with the physical investigation of the actual crime scene, if such an investigation is conducted in relation to the same incident. The authors define physical crime scene investigation as investigation of actual crime scene performed using traditional forensic and investigation methods. Therefore, there should be a principle to define the relationship between the digital forensic investigation process and the physical investigation. The interaction with the physical crime scene investigation is important for preserving the chain of evidence, preserving the integrity of the digital evidence, protecting the digital evidence from damage and ensuring an efficient investigation.

2. Preserving the chain of evidence [4] [6] [10] [11] [12] [14] [15] [16] [17] [18]

All legal requirements must be complied with and all actions be properly documented in order to preserve the chain of evidence as well as the integrity of the digital evidence. This principle must be followed during the entire course of the digital forensic investigation.

3. Preserving evidence [4] [6] [10] [11] [12] [14] [15] [16] [17] [18]

Preserving the evidence means to preserve the integrity of the original digital evidence. In order to achieve this, one must conform to strict procedures from the time that the incident is detected until such time as the investigation is closed. These procedures must ensure that the original evidence is not changed and, even more importantly, it must be guaranteed that no opportunity arises during the entire investigation in which the original evidence may be tampered with.

4. Information flow [6] [16]

It is important to identify and describe these information flows so that they can be protected and supported technologically, for instance through the use of trusted public key infrastructures and time stamping to identify investigators and authenticate evidence. [16]

A defined information flow should exist between each of the phases of the process and among different stakeholders, including investigators, managers and external organisations. Information flows should be also defined with sources of information of importance, such as relevant policies, technology information etc.

5. Documentation [6] [6] [10] [11] [12] [14] [15] [16] [17] [18]

Each action performed should be documented in order to preserve chain of evidence, but also to improve efficiency and the probability of a successful digital forensic investigation. Proper documentation must also be demonstrated during the presentation phase.

6. Obtaining authorisation [6] [12] [16]

Proper authorisation should be obtained for each action performed within all of the phases. Authorisation might be required from government authorities, system owners, system custodians, principals, etc.

V. DISCUSSION

Based on the comparison performed, regarding the digital forensic investigation process models, the authors of this paper conclude that there are huge disparities among existing digital forensic investigation process models. Disparities pertain to the number of phases included, the scope of models, the disparity in similarly- named phases within different models, number of tiers and even concepts applied to the construction of the model (i.e. some of the models are defining the digital forensic investigation process as part of the physical crime investigation process).

The digital forensic investigation process phases that are common to most of the process models analysed are: Incident detection, Planning, Preparation, Evidence identification, Evidence collection, Evidence transportation, Evidence analyses, Presentation, Conclusion.

The following reference principles are followed by all of the analysed digital forensic investigation process models: Preserving evidence, Preserving chain of evidence, Documentation.

These are the main and the most important principles to be followed, and it is advantageous that these principles represent a common ground for all analysed process models. These principles, together with phases that are common for most of the existing process models, should be a starting

point for development of a harmonised digital forensic investigation process model.

The authors are of the opinion that the body of knowledge and peer-reviewed papers on the digital forensic investigation process are scarce. Experts and practitioners in the field should concentrate more on this subject.

The authors strongly believe that, in order to have a fully-harmonised model, a comprehensive analysis has to be conducted of national and international law enforcement processes and procedures in the field of digital forensics. If consensus on a harmonised digital forensic investigation process model is to be reached by the digital forensics community, it will have to take into account practices of investigating institutions on a national and international level in order for the model to be viable.

VI. CONCLUSION

The research focus of this paper was to analyse the state-of-the-art digital forensic investigation process models. The authors believe that this analysis is a noteworthy contribution towards development of a harmonised digital forensic investigation process model. Having such a harmonised digital forensic investigation process model is important for the advancement of the digital forensics field, especially in order to reach higher admissibility of digital evidence in a court of law and to achieve more efficiency during digital forensic investigations.

Characteristics of existing models were analysed and compared. The comparison was conducted comprehensively and it was achieved through a tabular mapping of model phases and principles.

The authors conclude that there are significant disparities in the state-of-the-art among existing digital forensic investigation process models, although, mostly, the main principles applied by the various models are the same.

Future work will include research towards the development of a harmonised digital forensic investigation process model, including analyses of national and international regulations, especially the analyses of digital forensic investigation process models followed by law enforcement agencies.

Table 1Comparison of digital forensic investigation process models

	Reference phases	DFWRS [4]	Reith et al. [10]	DOJ [11]	Carrier et al. [12]	Mandia et al. [14]	Beebe et al. [15]	Cuardhuain [16]	Cohen [17]	Casey and Rose [18]	ACPO [6]
Phases											
1	Incident detection	1. Identifica-tion	1. Identification		2. Detection and notification	2. Detection of the incident3. Initial response	2. Incident response	1. Awareness			
2	First response					3. Initial response	2. Incident response				2.1 Secure and control the crime scene
3	Planning		3. Approach strategy		1. Readiness group of phases	4. Response strategy formulation	1. Preparation				1. Preparations for investigation
4	Preparation		2. Preparation	1. Preparation	1. Readiness group of phases	1. Pre-incident preparation		3. Planning			1. Preparations for investigation
5	Incident scene documentation			3. Documentation of the crime scene	4.3 Document evidence and scene						2.1 Photograph and document the scene 2.4 Attaching exhibit labels
6	Evidence identification		6. Examination	2. Recognition and Identification	4.2 Survey for digital evidence			5. Search for and identify evidence	1. Identification	1.Gather information and make observations	5.1 The collection phase
7	Evidence collection	2. Preservation 3. Collection	4. Preservation 5. Collection	4. Collection and preservation	4.1 Preservation of digital crime scene	5. Duplication 7. Secure measure implementation 8. Network monitoring	3. Data collection	6. Collection of evidence	2. Collection 3. Preservation	1.Gather information and make observations	2.3 Initial collecting of volatile data 5.1 The collection phase
8	Evidence transportation			5. Packaging and transportation				7. Transport of evidence	4. Transportation		3. Transport
9	Evidence storage							8. Storage of evidence	5. Storage		4. Storage
10	Evidence analysis	4. Examination 5. Analysis	7. Analysis	6. Examination 7. Analysis	4.4 Search for digital evidence 4.5 Digital crime scene reconstruction	6. Investigation	4. Data analyses	9. Examination of evidence 10. Hypothesis	6. Analyses 7. Interpretation 8. Attribution 9. Reconstruction	2. Form a hypothesis to explain observations 3. Evaluate the hypothesis 4. Draw conclusions and communicate findings	5.2 The analyses 5.3 The examination 5.4 The reporting
11	Presentation	6. Presentation	8. Presentation	8. Report	4.6 Presentation of digital scene theory	10. Reporting	5. Findings presentation	11. Presentation of hypothesis 12. Proof/Defence of hypothesis	10. Presentation	4 .Draw conclusions and communicate findings	
12	Conclusion	7. Decision	9. Returning evidence			9. Recovery 11. Follow-up	6. Closure	13. Dissemination of information	11. Destruction		6. Disclosure
Actionable principles											
1	Interaction with physical investigation				3. Physical crime scene investigation group of phases.						As principle and set of actions
2	Preserving chain of evidence	Present	Present	Present	Present	Present	Present	Present	Present	Present	Present
3	Preserving evidence	Present	Present	Present	Present	Present	Present	Present	Present	Present	Present
4	Information flow							Present			Present
5	Documentation	Present	Present	Present	Present	Present	Present	Present	Present	Present	Present
6	Obtaining authorisation				2. Confirmation and authorisation			Present			Present

REFERENCES

[1] Tan, J. (2001), "Forensic readiness", Technical. Cambridge USA: @stake, Inc.

[2] Gary Palmer (2001), "A Road Map for Digital Forensic Research". Technical Report DTR-T001-01, DFRWS, Report From the First Digital Forensic Research Workshop (DFRWS).

[3] ISO/IEC 27043, "Investigation principles and Processes", unpublished draft international standard (2012).

[4] Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993).

[5] Pollitt, M.M. (2001), "Report on digital evidence", 13th Interpol Forensic Science Symposium, Lyon, France.

[6] "ACPO Good Practice Guide for Computer-Based Evidence"(2008), http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence_v4_web.pdf

[7] http://en.wikipedia.org/wiki/Digital_evidence

[8] The Admissibility of Electronic Evidence in Court (2005), Fighting Against High-Tech Crime (Cybex, Barcelona).

[9] Stephen Mason (2008), "International Electronic Evidence", British Institute of International and Comparative Law.

[10] M. Reith, C. Carr and G. Gunsch (2002), "An examination of digital forensic models", International Journal of Digital Evidence.

[11] The U.S. Department of Justice (2001), "Electronic Crime Scene Investigation- A Guide for First Responders".

[12] Carrier B. and Spafford E. (2003), "Getting Physical with the Digital Investigation Process", International Journal of Digital Evidence, Vol. 2, 2, [Electronic version].

[13] Carrier B. and Spafford E. (2005), "An Event-Based Digital Forensic Investigation Framework", Digital Investigation 2(2).

[14] Mandia, Kevin, Prosise, Chris and Pepe (2003), "Incident Response & Computer Forensics" (Second Ed.), McGraw-Hill/Osborne, Emeryville.

[15] Nicole Lang Beebe and Jan Guynes Clark (2005), "A Hierarchical, Objectives-Based Framework for the Digital Investigations Process", Digital Investigation 2(2).

[16] Séamus, Ó. and Cuardhuáin, (2004), "An Extended Model of Cybercrime Investigations", International Journal of Digital Evidence, summer 2004, Volume 3, Issue 1.

[17] Frederick B. Cohen (2011), "Fundamentals of Digital Forensic Evidence, Chapter in Handbook of Information and Communication Security", accessed at all.net on 04.01.2011.

[18] Eoghan Casey and Curtis W. Rose (2010), chapter"Forensic Analysis " in "Handbook of Digital Forensics and Investigation"

[19] Frederick B. Cohen, Julie Lowrie and Charles Preston (2011), "The State of the Science of Digital Evidence Examination", all.net.

[20] R. Leigland and A. Krings (2004), "A Formalization of Digital Forensics", International Journal of Digital Evidence, fall 2004, Volume 3, Issue 2.

[21] Ryan Hankins, T. Uehara and J. Liu (2009), "A Comparative Study of Forensic Science and Computer Forensics", Third IEEE International Conference on Secure Software Integration and Reliability Improvement.

[22] Committee on Identifying the Needs of the Forensic Sciences Community (2009), "Strengthening Forensic Science in the United States: A Path Forward", ISBN: 978-0-309-13130-8, 254 pages. Committee on Applied and Theoretical Statistics, National Research Council.

[23] Scientific Working Group on Digital Evidence (SWGDE) (2009), Position on the National Research Council Report to Congress – Strengthening Forensic Science in the United States: A Path Forward

[24] S. Garfinkel, P. Farrella, V. Roussev and G. Dinolt, (2009), "Bringing science to digital forensics with standardized forensic corpora", Digital Investigation 6 S2-S11.

[25] M. Pollitt (2009), "Applying Traditional Forensic Taxonomy to Digital Forensics", Advances in Digital Forensics IV, IFIP TC11.9 Conference Proceedings.

[26] Michael Donovan Köhn (2011), "Towards a Digital Forensic Framework", Submitted in partial fulfillment of the requirements for the degree Magister Scientia (Computer Science) in the Faculty of Engineering, Built Environment and Information Technology at the University of Pretoria, August 2011.

[27] Matthew Meyers and Marc Rogers (2004), "Computer Forensics: The Need for Standardization and Certification", International Journal of Digital Evidence, fall 2004, Volume 3, Issue 2.

Aleksandar Valjarevic received his Bachelor of Science and Master of Science degrees in 2008 and 2009, respectively, from the University of Belgrade, in Serbia, and is presently studying towards his PhD degree at the University of Pretoria. He is working for Vlatacom (South Africa) Pty Ltd and is involved in work of Vlatacom Research and Development Center in Belgrade, Serbia. His research interests include information security and especially digital forensics.