# Towards ‘Crime Specific’ Digital Investigation Frameworks

Olga Angelopoulou1, Stilianos Vidalis2

1 Faculty of Business, Computing and Law, University of Derby, Derby, UK, o.angelopoulou@derby.ac.uk

2 Faculty of Computing, Engineering and Sciences, Staffordshire University, Stafford, UK, stilianos.vidalis@staffs.ac.uk

# Abstract

# *The wide development of the mobile and virtualised technologies in the past decade has further destabilized the already fragile balance between the defenders and the attackers of computing infrastructures. Criminals employ state of the art techniques for exploiting Information Environments that are making use of these new mediums. Alas, the resources that are available to Law Enforcement Agencies for prosecuting computer criminals are finite and existing investigative methodologies cannot address change in the means and mediums of crime. Coupled with the facts that (a) criminals have the initiative, and (b) they are well aware of the investigative procedures, it is understandable why computer crime, cyber-crime and e-Crime activities continue to be an issue in today’s socially-driven knowledge-based computing era. We argue that it is time to slightly change the focus of the digital forensic investigation from following static methodologies to actively trying to identify evidence of criminal activities. We propose ‘crime-specific’ frameworks that allow transparent extraction of knowledge from evidence, while ensuring chain of custody and evidential integrity. In this paper we critically discuss existing frameworks and build up the case for this new investigative approach.*

# Keywords

Cybercrime, Digital Investigation Framework, Digital Forensics

# Introduction

Digital forensics encompasses all aspects of the investigation of digital-related crime in dealing with a number of situations from industrial espionage to damage assessment. A digital device can be used in three different ways in order to assist a crime. It can be used as the ‘tool’ that the fraudster uses for performing the crime, the ‘target’ that the fraudster manages to attack and penetrate and the ‘storage area’ he can use to save information involving the crimes (Shinder and Titel, 2002). It appears in the literature the most popular digital crimes nowadays involve theft, fraud, extortion, hacking and distribution of malware.

The aim of the current implemented frameworks and methodologies is to create general procedures for digital investigations to incorporate all different types of digital crimes. For this purpose, the generic term *digital forensics* is mostly used, broadening computer forensics and including all types of digital media that could be forensically examined. Palmer (2001) defines digital forensics as:

*“The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for the purpose of facilitation or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations.”*

There are over one hundred (Ieong, 2006) different models that appear in the literature attempting to aid the analysis of computer crime incidents. A digital investigation relies both on the system and the human aspect (Beebe and Clark, 2005). Current frameworks are broad and try to cover many different aspects; whereas computer crime incidents have become targeted and sophisticated. Therefore, the investigation should also become targeted and sophisticated. A framework can be defined as “*a system of rules, ideas or beliefs that is used to plan or decide something”* (Cambridge Advanced Learner's Dictionary). A number of attempts have been made in creating standards for digital forensic investigations.

Farmer and Venema (1999) gave general guidelines, focused on the UNIX platform and developed the Coroner’s Toolkit. Mandia and Prosise (2001) gave detailed instructions for specific platforms and focused on computer crime. Lee et al. (2001) studied the investigation of the crime scene, without analysing the entire investigative process. Ciardhuáin (2004), attempted to process the investigation from the *information flow* side rather than simply focusing on the evidence. Also, efforts in the terms of published books have been made for formalising computer forensic investigations (Schweitzer (2003), Stephenson (1999), Marcella and Greenfield (2002)). These contributions can be described as field manuals and even though they provide valuable guidelines they lack in different areas. For instance, Marcella and Greenfield (2002) provide a comprehensive guide about tools, techniques and criminal profiling; however, they focus on legal aspects and keep the actual examination on a high level.

The literature shows that the majority of published examination models are based on their predecessors. Digital evidence and investigations consist of, and combine, numerous different aspects (e.g. technology, devices, systems, nature of the investigation). It is reasonable to suggest that a possible further improvement is to generate specific formalised approaches to the investigations, as they are always going to differ according to the perspective of the researchers that implement it. The fundamental and most important frameworks, as they appear in literature, are discussed below. Their strengths and weaknesses are highlighted in order to give insight for considering the implementation of more specialised frameworks that focus on the type of the crime rather than in the nature of the digital device.

# Analysing the Current Frameworks and Methodologies

## The Integrated Digital Investigation Model and the Computer History Process Model

Carrier and Spafford have a number of different publications concerning digital investigations; two of these were considered as more enlightening and are discussed herein. In their first published paper, Carrier and Spafford (2003) apply issues to the digital crime scene that are relevant to the physical crime scene. The *Integrated Digital Investigation Model* concentrates on the computer as the crime scene aiming to provide the digital evidence. The digital crime scene is therefore derived from the physical. This initial framework includes seventeen phases that are based on the existing to date frameworks and is organised in the following five groups:

1. *Readiness Phases*
2. *Deployment Phases*
3. *Physical crime scene investigation phases*
4. *Digital crime scene investigation phases*
5. *Review phase*

Carrier and Spafford (2003) have created a checklist of conceptual high-level phases. Their aim is to propose and describe the procedure required in the digital investigation research field. The phases have been applied on existing frameworks and demonstrate an alternative approach to this research area. They study the computer as an individual part of the physical crime scene and treat it accordingly. The model is aimed to be general, abstracted and apply to all types of computer forensic investigations. Later, in 2006, they introduced the *Computer History Process Model*, evolving the previous model. Carrier’s doctorate thesis (2006) is based on it as well. The final framework is published including the following four phases:

1. *Observation*
2. *Hypothesis Formulation*
3. *Prediction*
4. *Testing and Searching*

They do not claim that the existing frameworks are not correct for specific processes. However, they declare that their proposed model focuses on a different perspective that contributes to them.

The Observation phase observes states and events; the researcher needs to observe the field in order to create a clear picture about the processes and the activities that take place on the investigation. The Hypothesis Formulation focuses on the results of the observation phase and is able to categorise the techniques that will aid the analysis of the findings. The Prediction phase supports the Hypothesis Formulation as the results of this part will prove whether or not the Hypothesis is formed on a structured base and will lead the researcher to the last phase. In Testing and Searching, the tests and experiments that take place in a generally approved manner will probably result in new predictions and evaluate the Hypothesis the researcher has set.

They effectively stated that the purpose of the forensic investigation is to reconstruct the ‘history’ of the digital media under investigation. They also argue that the history of the digital media is unknown to the investigator. Therefore, this is what he needs to investigate those events that resulted altering the state of the media. However, it is based on computationally complex models, a scientific approach that may not be easily comprehensive by the investigators. In addition, the authors argue that the framework’s aim is to assist the existing frameworks and has been tested.

The *Computer History Process Model* will be further discussed in this paper, rather than the Integrated Digital Investigation Model, as it is a more recent work and contributed as a research work towards a doctorate.

## Digital Evidence and Computer Crime

Casey (2004) is considered to have published the *epitome* of computer forensic investigations (Kessler, 2007) on *Digital Evidence and Computer Crime*. He provides a general computer forensics framework that depicts the relationships among law, computer science, forensic science, and behavioural analysis. The model Casey presents consists of the following four phases:

1. *Recognition*
2. *Preservation, collection, documentation*
3. *Classification, comparison, individualisation*
4. *Reconstruction*

The first two phases of the framework handle the crime scene, while the analysis of the evidence takes place in the following two phases. Based on Casey, the reconstruction phase can lead the investigator to identify additional evidence and revisit them. The framework contains tasks for the first responders and can be applied on both standalone and networked systems. The findings of the evidence examination are interpreted in a way that could stand in a court of law.

## Abstract Digital Forensics Model

Reith et al. (2002) attempted to extend the existing framework from the Digital Forensics Research Workshop (DFRWS) (Palmer, 2001) on a standardised process and aid the law enforcement and judicial systems. The *Abstract Digital Forensics Model* consists of the following nine phases:

1. *Identification*
2. *Preparation*
3. *Approach strategy*
4. *Preservation*
5. *Collection*
6. *Examination*
7. *Analysis*
8. *Presentation*
9. *Returning evidence*

The first three phases of the framework involve the response to the incident, phases three and four the data collection and six and seven the examination of the digital media. In such a distinction of the phases the model becomes more complicated.

The authors themselves admit that the proposed framework is not tested and does not maintain, but it is assumed that it will maintain the chain of custody; a rather important issue for the investigation of computer forensic incidents involving law enforcement and courts.

## Hierarchical Objectives-based Framework

Beebe and Clark (2005), present a *flexible and usable* framework that approaches digital investigations on a multi-tier basis; differentiating itself from existing approaches. The *Hierarchical Objectives-based Framework* extends on Carrier and Spafford’s (2003) single-tier approach (Tipton and Krause, 2004). It consists of six phases, but also includes sub-phases, principles and objectives.

1. *Preparation*
2. *Incident response*
3. *Data collection*
4. *Data analysis*
5. *Findings presentation*
6. *Incident Closure*

Phases one and two respectively involve the preparation of the digital evidence and the response action towards incident. The data collection phase collects the digital evidence that is analysed on the data analysis phase. The second-tier of this phase is also discussed in their research paper. The findings presentation phase documents the findings of the data analysis and the incident closure phase closes the investigation and preserves the related information.

It aims at assisting general investigations rather than being crime specific. The authors claim that the framework is expandable and this was achieved by working on the advantages of existing works and combining different aspects.

## Electronic Crime Scene Investigation: a Guide for First Responders

*Electronic Crime Scene Investigation: a Guide for First Responders* is the U.S. Department of Justice (2008), structured digital investigation framework. It is intended for responding to the digital crime scene investigation and applies to law enforcement officers. This is the updated version of the U.S. Department of Justice (2001) that failed to be *all-inclusive*, as commented in the recent version of the document. The updated model consists of the following phases:

1. *Preparation: recognize, identify*
2. *Collection: seize, secure, evaluate, label, document the scene*
3. *Preservation: package, transportation, storage*
4. *Examination*
5. *Analysis*
6. *Report*

This generalised process does not differentiate the computer from other digital media and there is little guidance concerning the actual examination and analysis of the system (Carrier and Spafford, 2003). As it aims to concentrate on the first responders it basically refers on the physical crime scene and the traditional forensics.

Even though, the method is rather systematic for the first three phases, it covers the examination, analysis and report in only one chapter. This effectively adjusts it to a guideline for the crime scene and not a framework that could efficiently assist the computer forensics investigator.

## Recovery Process

*The Good Practice Guide for Computer-Based Electronic Evidence* provided by ACPO (2007) is accepted in both the public and the private sector. It is the UK standard that provides the procedure that should be followed by the practitioners and focuses on the collection of evidence. These guidelines are considered as essential instruction to computer forensic investigation and cover different aspects of computer crimes and electronic devices. It comprises of the four fundamental principles that are further explained in the original document ACPO (2007).

The guidelines in addition include the *Recovery Process* that consists of four processes/ phases for computer-based electronic evidence recovery:

1. *Collection Phase*
2. *Examination Process*
3. *Analysis Phase*
4. *Report or statement*

The collection phase searches, recognises, collects and documents the electronic evidence. The examination process is examined the medium for evidential data, while the analysis phase tests the outcome of the examination for its relevance to the existing case. The report or statement describes the findings on a forensically sound manner.

The ACPO (2007) Recovery Process is a standard general approach that covers computer forensic investigations. As the guide aims to concentrate on the collection of evidence, limited information is provided for the overall procedure.

# Discussion on the Existing Frameworks and Methodologies

The existing frameworks are attempts to formalise the investigative procedure. They all appear to have positive and negative features, the discussion of which will assist in generating the properties of our 'crime specific' investigation framework. In addition, investigation frameworks that do not only focus on digital forensics, but are related to specific crimes are also discussed in this section.

The *Computer History Process Model* (Carrier and Spafford, 2006) approaches the digital investigation from a different angle; the computer history. It is the aspect that we approach an investigation as well; it discloses the history of the computer system in a manner similar to the physical investigation. The four phases that constitute the Carrier and Spafford (2006) framework (section 2.5.1) are concentrated and descriptive to their content. They manage to verify the idea even though there is a differentiation between the physical and the digital world. The model is *highly theoretical with some practical implication* (Carrier, 2008). This suggests limited applicability to actual investigations. It would appear that the actual purpose of this work is to assist the academic, rather than the practitioners. However, this framework is a model that a crime specific framework could be built upon.

In *Digital Evidence and Computer Crime* (Casey, 2004) a generic model to fit all computer crimes is presented. The interesting part of his framework is the evidence processing cycle that prompts the examiner to revisit a phase, when additional information is required. An element that is significant for an investigation and should also be contemplated for the design of the crime specific framework. It is considered as a standard towards a forensic investigation (Ieong, 2006). Casey (2004) presented a framework that would be general enough to include all procedures of the computer forensics investigation. He even refers to the extraction of data from different digital media, different operating systems and mobile devices. However, it is not focused on a specific area. This positions it as an all-purpose guide and reference to computer forensic investigations. It is an effort to formalise the procedure. The knowledge acquired from Casey (2004) does contribute to our design of the cybercrime investigation framework, but due to its non-direct link with formal academic research it was decided not to be used as the base model of the framework.

The *Abstract Digital Forensics Model* (Reith et al., 2002) is a framework intended to be adjusted in the examination of all different, present and future, types of computer crimes and technology. It is descriptive, broad and developed in the terms of the evidence collection and the technology. In addition, it covers a wide range of digital devices. An interesting feature of this framework is that it could be adopted for the development of specific methodologies based on a technology or type of e-crime (Ciardhuáin, 2004). The purpose of this framework is to be considered as a ‘standard’, a broad system that could embed all types of e-crimes. A ‘crime specific’ framework targets to serve as a tool for the investigator. Therefore, it needs to be focused and detailed having the crime in mind.

The *Hierarchical Objectives-based Framework* (Beebe and Clark, 2005) proposed a multi-tier investigation framework. It is looking for evidence with more detail, on a lower level, unlike other frameworks and appears well structured overall. This approach is useful for the design of a ‘crime specific’ framework. However, such an effort on a general investigation framework could also become the weakness of an approach that attempts to assist all types of computer crime investigations. It is easy to overlook some aspects when everything is attempted to be included. The authors comment that they tend to adjust their method in order to include different types of devices and operating systems. This could cause problems with applicability to future systems.

The *Electronic Crime Scene Investigation: a Guide for First Responders* (U.S. Department of Justice, 2008) published the American governmental guidelines of approaching computer forensic investigations. There is an interesting part of this framework that needs to be noted. It is the categorisation of evidence based on the type of crime and the potential locations that the investigator should focus his examination for evidential data. It states that potential digital evidence is proposed to be found in

*“…computers, mobile devices, records of online purchases, removable media, external data storage devices, PDAs, address books, contact lists, online banking software, information regarding internet activity, financial asset records, electronic money transfers, laminators, calendars or journals, forged documents and false identification, victim information and credit card data, copies of signatures, printed e-mail, notes, letters, ID pictures, check cashing cards and scanners.”*

An inconsistency appears as the above evidential types are not necessarily digital evidence. For example, laminators and printed e-mails refer to physical evidence and can be used as additional to the digital. The list with the above digital devices can be useful for the design of the ‘crime specific’ framework, as it states where related evidence can be found. However, the model is actually a first response and does not focus on the examination of the media. On the contrary, the objective of the crime specific framework is the examination of the media in order to provide relevant evidence with the type of cybercrime. Reith et al. (2002) and the U.S. Department of Justice (2008) separate the analysis and the examination in different phases in the framework. The analysis is about searching and extracting data for them, while the examination is about generating evidential data from the extracted source (Beebe and Clark, 2004). This could be confusing for the practitioners.

The *Good Practice Guide for Computer-Based Electronic Evidence* (ACPO, 2007) serves the purpose of a formal standard for the UK. It was designed by police officers for police officers and it is therefore a practical guide. Computer forensic investigators across the UK tend to adopt it. However, the guidelines state that digital evidence can be accepted under certain circumstances even when it does not comply with the guide. Even though it is a general procedure that tends to cover everything, it gives weight on volatile data, network forensics and the Trojan defence. Because of its structure and the fact that it is not an analytical framework it cannot be used as the base for the proposed work. However, it is an accredited guide and is taken under consideration for the design of our crime specific framework.

# Specific Frameworks and Guidelines

Guidelines on PDAs (Jansen and Ayers, 2004), mobile phones (Jansen and Ayers, 2007), internet forensics (Sekar et al., 2004) are sub disciplines of digital forensics. The requirement for the development of these specialised areas has demonstrated the need for more focused frameworks and guidelines. In the literature some research has been identified that has a similar approach to the one proposed in this paper.

Katos and Bednar (2008) propose a cybercrime investigation framework for developing investigation support among the stakeholders that influence the investigation. It is not a framework that provides guidelines for the investigation procedure, but rather an *information system* that acquires the information provided by those that take part during a forensics investigation. Their system is generic in order to cover all different types of computer crime, but can be adjusted to a specific type of crime. Their method aims to assist the forensic investigation in providing him with a flexible approach. It approaches the investigation by examining the type of the offence. It uses mathematical theories as a base standard, probabilities and open problems that make it complex and confusing in some areas. On the other hand, it is a presented system that could maintain the investigation based on the type of crime. Their work though, seems to be under development and their publication does not compare their proposed system with any other similar frameworks or computer forensic investigation frameworks.

Slay and Simon (2008) discuss Voice over Internet Protocol (VoIP). They propose the development of a software tool that could assist forensic investigations by extracting packets that can reconstruct a VoIP conversation. Criminals could potentially misuse such tool, retrieve conversations and threaten someone’s privacy, or even take advantage of VoIP wiretapped conversations. Even though the product of Slay and Simon’s (2008) research is a software tool and not an analytical framework, it adds to the argument that due to the increase in cybercrimes, there is a need to investigate each cybercrime independently.

Ferraro and Casey (2005) have a publication aiming to assist the investigation of child exploitation and pornography. Even though their work focuses on the legal aspect, there are specific guidelines that refer to the forensic investigation of the specific type of crime that are enhanced with examples. It seems that the existing published work of Casey (2004) is used throughout the book and applied to child exploitation. The forensic examination of the criminal’s computer system is presented briefly. However, the contact with a physical crime scene is extensively discussed and how an internet investigation can prove the illegal activity and track the criminal. Also, advice on how to secure the evidence and handle it is provided. It provides guidance up to the stage of the trial. It aims to cover the internet investigation, the actual computer and other digital devices investigation, as well as the handling of servers and networks. There has been already one attempt to provide specific guidelines for computer forensic investigations, based on the type of crime. This guideline is mostly focused on the legal side, probably because of Ferraro’s law background. The type of crime the book examines is dependent on one of the two authors’ existing work.

Angelopoulou (2007) defines the need for a crime specific framework and particularly concerning identity theft. The work of the author discussed about the solidarity of ID theft as a type of cybercrime and therefore suggested the investigation of this type of crime should be individually treated. Based on that there is now an effort to expand this in a way it could be applied individually on all different cybercrime. It is considered as the stepping stone to the presented work.

# Limitations and Properties of a ‘Crime Specific’ Investigation Framework

The planning of a framework that concentrates on the forensic investigation of a single computer crime is not unproblematic. It was seriously considered at the initialisation of this research that this framework should be one step further than the existing ones. The areas that the research had to concentrate on were two; computer forensics and cybercrimes.

The suggestion that cybercrimes are constantly expanding, forms the base for further research in the area. It is an area that demands an approach to assist the handling of the related digital evidence. Each cybercrime should be treated under specific guidelines, simply because each one of them contains different attributes.

There were a number of problems indicated when attempting to design a crime specific investigation framework. It was argued that there may be no need for specific guidelines, as long as the existing frameworks are all-cybercrime-inclusive. This will not be extensively discussed here, as it is beyond the scope of this paper. In brief, the work of the forensic investigator can become a faster and more accurate procedure, when he knows exactly where to search for evidence and focuses on a specific type of crime. In a sense this might be the approach of a practitioner, but it has not been systematically outlined as a good practise.

Another issue towards the direction of a crime-specific framework is that the product of the research cannot be a high level framework similar to existing ones. No matter how researchers in computer forensics have currently approached the investigation, the proposed work should include specific areas. These are the areas related with each different type of crime and should reach a very low investigation level. In order to achieve this all techniques a cybercrime can be accomplished need to be studied and comprehended. The problem, undeniably, is that attackers and fraudsters tend to develop new ways of acting and the framework should be built in a flexible way that would allow possible near future techniques to be included.

When a very low level framework is being designed though, another concern is raised. The method should include guidelines about the different digital evidence that could be discovered when examining a victim’s and a fraudster’s system (Angelopoulou, 2007). In order to cover this and avoid confusion the framework should be split at some point and guide the investigator towards evidential points that involve the associated part.

Currently evidence uncovered during an investigation is not classified into particular categories using existing frameworks. This is due to their high-level approach. However, a low level framework has the ability to define special activities that could classify the evidential data based on its quality and relevance to the incident that is being investigated. Such an approach would support the construction of a scenario that could describe what has happened to the penetrated or the rogue system. Then, the investigator would be able to create a focused picture of the incident.

Another issue that was highlighted when reviewing the existing frameworks was that an examination methodically collects information that could profile the perpetrator. The information that is gathered could assist in providing such data. The existing frameworks though do not seem to process it in order to create the fraudster’s profile. If such information was maintained under some constant values for avoiding confusion the investigator could prove that there may be unvarying procedures from the fraudsters that commit a specific type of cybercrime.

Ferraro and Casey (2005) claim that the only way not to miss any evidence is to perform a *full-blown* examination. This is a type of examination that includes and examines every instance of the digital media. This may be a case for computer forensic investigations and had to be taken seriously under consideration as a crime specific framework needs to be persistent; it should ensure that everything is included. The existence of specialised investigation frameworks in the field though, strengthened the premise that it can be achieved.

Another identified difficulty is the low level of the investigation the framework needs to achieve. Digital media tend to use different operating systems that are developed in different modes. An analytical framework though needs to facilitate all of them. In order to overcome this problem the framework needs to maintain a conceptual approach that can encompass a range of systems.

Based on the above issues the framework’s design needs to consider the following:

* An in depth understanding and knowledge of cybercrimes in order to avoid overlooking evidential data.
* To be easily comprehended and applied by the practitioner.
* To include all different systems and technologies, in order to be flexible.

The review of the existing computer forensics frameworks and the above considerations assist in developing the properties that a cybercrime specific framework needs to conform to and are stated below:

* It should divide the investigation concerning the victim or the fraudster.
* It should provide classified evidence.
* It should provide profiling of the fraudster.

A cybercrime specific framework aims to approach the investigation from a different aspect than the existing ones based on the issues discussed in this section. The properties required for the framework were generated after the review of the existing literature.

The investigation of a digital crime, such as identity theft, could be intense, complicated and time consuming work for the investigator. The digital evidence depends not only on the fraudster’s computer, but also on intermediate systems in the majority of cases. There are other factors, such as a card cloning machine that could enhance the evidence. Any supplementary sources that could be found on the crime scene support the investigation and can therefore contribute as evidence for identity theft. Based on Cook (2008), the investigator can focus the investigation on credit history, transactions made in the victim’s name, applications for bank accounts, loans and credit cards. The evidence would consist of data, logs etc. formats through various systems within one or even multiple financial organisations. A victim’s machine should provide conformational information, so that the theft of data or the fraud against the user will be proved. On the fraudster’s machine the evidential data should be treated in such a way that will reveal the intention of theft.

If a crime specific framework was used for the investigation of such an incident, then the investigator would be guided through the process for an in-depth analysis of his potential evidential digital devices. There would be a constructed approach that would provide guidance and eliminate the possibility of evidential data been omitted from the investigation.

We are working towards a framework that breaks down the investigation to the type of the crime and incorporates all possible areas that the examination could retrieve evidence from on a lower level. Different sort of evidence is required, according to the type of crime in order to be concentrated on the unique aspects that characterise it. A prerequisite for pursuing a crime specific framework is that the type of the crime is known.

# Conclusion

In this paper we reviewed the existing computer forensic frameworks, methodologies and guidelines in order to identify the properties for proposing the properties a ‘crime-specific’ framework needs to include.

The review taken on existing works proves that the forensic investigator may benefit from additional guidance on deciphering crimes. We believe that there is a lack of:

1. Structured evidence specifically based on the type of cybercrime;

2. Structured profiles of the fraudsters;

3. Prevention and detection techniques for eliminating the problem.

If such work existed, then less effort would be required from the digital forensic investigators for resolving a case.

# References

ACPO, 2007, Good Practice Guide for Computer-Based Electronic Evidence, v.18, Official Release version, downloaded from http://www.acpo.police.uk/asp/policies/Data/ACPO%20Guidelines%20v18.pdf

Angelopoulou O., 2007, ID Theft: An Investigation's Framework, in Proceedings of the 5th Australian Digital Forensics Conference, Edith Cowan University, Australia

Beebe N.L., Clark J.G., 2005, A hierarchical, objectives-based framework for the digital investigation process, Digital Investigation, Vol. 2, Issue 2, pp. 147-167

Cambridge Advanced Learner's Dictionary, 2008, Cambridge dictionaries online

Carrier B.D., Spafford E.H., 2003, Getting Physical with the Digital Investigation Process, International Journal of Digital Evidence, Vol. 2, Issue 2

Carrier B.D., 2006, A Hypothesis-Based Approach To Digital Forensic Investigations, PhD Thesis, Purdue University, Internet Source, available from: https://www.cerias.purdue.edu/tools\_and\_resources/bibtex\_archive/archive/2006-06.pdf

Casey E., 2004, Digital Evidence and Computer Crime: Forensics Science, Computers and the Internet, Amsterdam, Academic Press, 2nd ed., ISBN: 0121631044

Ciardhuáin, S. Ó., 2004, An extended model of cybercrime investigations. International Journal of Digital Evidence, Vol.3, Issue 1, pp. 1-22

Farmer D., Venema W., 1999, Computer Forensics Analysis Class Handouts, available from: http://www.porcupine.org/forensics/handouts.html. Accessed on 11/04/2013

Ferraro M.M. and Casey E., 2005, Investigating Child Exploitation and Pornography: The Internet, Law and Forensic Science, Academic Press, USA, ISBN: 0121631052

Jansen W. and Ayers R., 2004, Guidelines on PDA Forensics, Recommendations of the National Institute of Standards and Technology, Special Publication 80072. Available from: http://csrc.nist.gov/publications/nistpubs/800-72/sp800-72.pdf

Jansen W. and Ayers R., 2007, Guidelines on Cell Phone Forensics, Recommendations of the National Institute of Standards and Technology, Special Publication 800-101. Available from: http://csrc.nist.gov/publications/drafts/Draft-SP800-101.pdf

Katos V. and Bednar P.M., 2008, A cyber-crime investigation framework, Computer Standards & Interfaces, Volume 30, Issue 4, pp. 223–228

Kessler G.C., September 2007, Book Review: Casey, E. (2004). Digital Evidence and Computer Crime: Forensics Science, Computers and the Internet (2nd ed.). Amsterdam: Elsevier Academic Press. 690 pp, Criminal Justice Review, Vol. 32, pp. 280-282

Lee H. C., Palmbach T., MillerM.T., 2001, Henry Lee’s Crime Scene Handbook, New York, Academic Press, ISBN: 0124408303

Mandia K., Prosise C., 2003, Incident Response, Investigating Computer Crime, Osborne/McGraw-Hill, USA, ISBN: 0072131829

Marcella A.J. and Greenfield R.S., 2002, Cyber Forensics, A field manual for collecting, examining and preserving evidence of computer crimes, CRC Press LLC, ISBN: 0849309557

Ieong R.S.C., 2006, FORZA – Digital forensics investigation framework that incorporate legal issues, Digital Investigation, Vol. 3, Supplement 1, pp. 29-36, The Proceedings of the 6th Annual Digital Forensic Research Workshop (DFRWS '06)

Palmer G.L., Digital Forensics Research Workshop (DFRWS), 2001, A Road Map for Digital Forensics Research, Report from the First Digital Forensic Research Workshop. DTR-T001-01 FINAL, available from: http://www.dfrws.org/2001/dfrws-rm-final.pdf

Reith M., Carr C., Gunsch G., 2002, An Examination of Digital Forensic Models, International Journal of Digital Evidence, Vol. 1, Issue 3

Sekar V., Xie Y., Maltz, D.A., Reiter M.K., Zhang H., 2004, Toward a Framework for Internet Forensic Analysis, In Proc.of ACM HotNets-III

Schweitzer D., 2003, Incident Response: Computer Forensics Toolkit, Wiley Publishing, Inc., Indianapolis, Indiana, ISBN: 0-7645-2636-7

Slay J. and Simon M., 2008, Voice over IP forensics, e-Forensics '08, in proceedings of the 1st international conference on Forensic applications and techniques in telecommunications, information, and multimedia and workshop, Article No. 10, ISBN:978-963-9799-19-6

Stephenson P., 1999, Investigating Computer-Related Crime: A Handbook for Corporate Investigators, CRC Press, ISBN 0849322189

Tipton H.F., Krause M., 2004, Information Security Management Handbook, 5th ed., Auerbach Publications, USA, ISBN 0-8493-1997-8

U.S. Department of Justice, 2001, Electronic Crime Scene Investigation: A Guide for First Responders, Technical Working Group for Electronic Crime Scene Investigation, available from: http://www.ncjrs.gov/pdffiles1/nij/187736.pdf