Chapter 15
Testing the Comprehensive Digital Forensic Investigation Process Model (the CDFIPM)

Reza Montasari

15.1 Introduction

Nowadays, the nature of evidence presented in courts of law is less likely to be paper-based due to the ubiquitous nature of information technology. Evidence of computer crime differs from that related to traditional crimes for which there are well established standards and procedures [3, 41, 42]. In order for digital evidence to be admissible, investigators need to demonstrate that they have specialised knowledge and that the evidence was acquired using reliable principles and methods [22]. As with other types of evidence, digital evidence is not assumed to be valid and reliable: empirical testing in relation to the theories and techniques of its production is required [3, 28]. Careful notice is taken in court of the manner in which the digital investigative process has been carried out [14, 22, 28]. A digital forensic investigator might discover significant and incriminating evidence, but if they cannot present the evidence in a coherent and understandable way to the lay audience (such as judge and jury), the case may be lost [40]. The complexity of tools and methodologies used to perform a digital investigative process requires investigators to be able to explain the process in a manner that a judge and jury can understand it [22]. Such tools and methodologies must also adhere to some standards of practice and be accepted by other investigators operating in the field [3, 7, 22].

Nevertheless, the field of digital forensics still lacks a 'formal' process model that courts can employ to determine the reliability of the digital evidence presented to them [5, 23, 29, 44, 46]. A further issue with the existing models is their tendency to

The original version of this chapter was revised. An erratum to this chapter can be found at DOI 10.1007/978-3-319-60137-3_18

R. Montasari (✉)
School of Computing, Engineering and the Built Environment, Birmingham City University, Millennium Point, Curzon Street, Birmingham B47XG, UK
e-mail: Reza.Montasari@bcu.ac.uk

M. Dastbaz et al. (eds.), *Technology for Smart Futures*,
DOI 10.1007/978-3-319-60137-3_15

focus on one specific area of digital forensics, neglecting other environments [29, 30]. Unlike in other domains of forensic practice, digital forensic investigators operate in various fields [4, 9, 13, 17]. Therefore, as Carrier and Spafford [11] argue, 'A model must be abstract and apply to law enforcement investigations, corporate investigations, and incident response'. However, instead of being generic, previous models have often focused on only one specific area, such as law enforcement, commerce or incident responses [3, 34], therefore failing to consider the requirements of those operating in different domains. The result has been the hindering of the development of a generic model that can be applied in the various fields of digital forensics. A third significant concern associated with the previous models is that they are not comprehensive, failing to cover the entire investigative process. The models often focus on the 'middle part' of the investigative process, that being 'Identification, Acquisition and Examination Processes,' excluding other essential stages. Beebe and Clark argue that a more comprehensive and generally accepted framework is needed to enhance scientific rigour and facilitate education, application and research [9].

The remainder of the paper is structured as follows: Sect. 15.2 presents a background to the existing digital forensic investigation process models (DFIPMs). Section 15.3 provides an overview of the proposed model, while Sect. 15.4 presents the research methodology. In Sect. 15.5, the CDFIPM is applied into a case study, and a walkthrough of the model is performed. Finally, the paper is concluded, and future work is discussed in Sect. 15.6.

15.2 Background to the Existing DFIPMs

Prior to designing and developing the proposed model, presented in Montasari [31], a critical review of the existing models was carried out, and the results of this review was presented in Montasari [30] and Montasari and Peltola [29]. Since the latter two papers discuss such a review in detail, this section provides only a summary of the findings of this critical analysis. The review of the existing models revealed that these models have often been developed by digital forensic practitioners based on their own personal experience on an ad hoc basis without consideration to establish standardisation within the field [46]. This has prevented the establishment of formal processes that are urgently needed by courts of law [4, 29]. As Table 15.1 clearly demonstrates, existing DFIPMs display significant disparities in terms of the number of phases, scope and the specific domains that they have been developed for. As a result, these models have often been criticised for being too specific [11, 35], too high level [9], too broad [36], too technical [45] and too complex [39]. Due to such shortcomings, many researchers are increasingly calling for scientific approaches and formal methods for describing the digital investigation processes [10, 15, 18, 25, 34]. Therefore, as discussed in Sect. 15.1, the Comprehensive Digital Forensic Investigation Process Model (the CDFIPM) was proposed in Montasari [31] to address the stated issues in relation to the existing DFIPMs. By implementing the CDFIPM, this model will be of immediate value to both digital forensic investigators (DFIs) operating within the stated fields and courts of law.

Table 15.1 The comparative summary of the existing DFIPMs

The Comparative Summary of the Existing Digital Forensic Investigation Process Models (DFIPMs)																				
Existing DFIPMs	Palmer (2001)	Ashcroft (2001)	Reith et al. (2002)	Carrier and Spafford (2003)	Baryamureeba and Tushabe (2004)	Ciardhuáin (2004)	Rogers (2004)	Beebe and Clark (2005)	Kent et al. (2006)	Kohn et al. (2006)	Rogers et al. (2006)	Freiling and Schwittay (2007)	Khatir et al. (2008)	Selamat et al. (2008)	Cohen (2009)	Yusoff et al. (2011)	Agarwal et al. (2011)	Valjarevic and Venter (2012)	Kohn et al. (2013)	Adams et al. (2014)
Readiness				✔	✔		✔	✔				✔							✔	
Deployment				✔			✔	✔											✔	
Policy/ Procedure										✔		✔							✔	
Operational Readiness				✔			✔					✔							✔	
Infrastructure Readiness				✔			✔					✔							✔	
Incident Detection (Awareness)			✔	✔	✔	✔						✔						✔	✔	
Report Incident (Notification)				✔	✔	✔		✔		✔				✔					✔	
Assess Incident.								✔					✔						✔	
Confirm Incident.				✔	✔		✔						✔	✔					✔	
Authorisation				✔	✔	✔	✔			✔		✔	✔	✔			✔	✔	✔	✔
Incident Response				✔			✔	✔	✔			✔						✔		
Planning (Approach Strategy)			✔			✔		✔		✔	✔	✔	✔	✔			✔	✔	✔	✔
Understand Task Requirements																				✔
Determine Overall Picture																				✔
Determine Required Outcomes																				✔
Determine Parameters																				✔
Consider Physical Constraint																				✔
Consider Timing Constraint																				✔
Consider Data Constraint																				✔
Plan Logistics																				✔
Create Outline Plan																	✔			✔
Preparation			✔					✔		✔							✔	✔		
Attend Site											✔						✔			✔
Securing the Scene			✔					✔									✔			
Address Safety Issues																	✔			✔
Communication Shielding																	✔			
Triage											✔									
Examine User Usage Profiles											✔									
Examine Chronology Timeline											✔									
Examine Browsing Activities									✔		✔									
Case Specifics											✔									
Carry Out Preliminary Survey																				✔
Documentation of Scene				✔		✔		✔									✔	✔		✔
Update Outline Plan																	✔			✔
Search				✔	✔	✔	✔	✔		✔							✔		✔	
Survey				✔	✔		✔	✔									✔			
Identification	✔					✔		✔	✔	✔					✔		✔	✔		
Preservation	✔		✔	✔	✔		✔	✔							✔	✔	✔		✔	
Collection	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔		✔	✔		✔	✔	✔	✔	✔	✔
Volatile Evidence Collection									✔			✔					✔			
To Be Continued …																				

Table 15.1 (continued)

The Comparative Summary of the Existing Digital Forensic Investigation Process Models (DFIPMs)																				
Existing DFIPMs	Palmer (2001)	Ashcroft (2001)	Reith et al. (2002)	Carrier and Spafford (2003)	Baryamureeba and Tushabe (2004)	Ciardhuáin (2004)	Rogers (2004)	Beebe and Clark (2005)	Kent et al. (2006)	Kohn et al. (2006)	Rogers et al. (2006)	Freiling and Schwittay (2007)	Khatir et al. (2008)	Selamat et al. (2008)	Cohen (2009)	Yusoff et al. (2011)	Agarwal et al. (2011)	Valjarevic and Venter (2012)	Kohn et al. (2013)	Adams et al. (2014)
Non-Volatile Evidence Collection									✔			✔								
Authenticate																			✔	
Seizure								✔											✔	✔
Package																	✔			✔
Transport						✔				✔					✔		✔	✔	✔	✔
Storage						✔				✔					✔		✔	✔	✔	✔
Examination	✔		✔	✔		✔		✔	✔	✔			✔		✔		✔		✔	
Harvest								✔				✔							✔	
Reduce								✔				✔							✔	
Identify				✔															✔	
Classify																			✔	
Organise												✔							✔	
Compare																			✔	
Analysis	✔		✔	✔				✔	✔	✔			✔		✔	✔	✔	✔	✔	
Attribute															✔				✔	
Evaluate																			✔	
Hypothesis						✔													✔	
Interpretation															✔				✔	
Reconstruction				✔	✔		✔	✔				✔			✔				✔	
Reporting		✔		✔				✔	✔			✔		✔			✔			
Presentation	✔		✔	✔	✔	✔	✔	✔		✔			✔		✔	✔	✔	✔	✔	
Proof / Defence						✔		✔		✔										
Decision	✔							✔											✔	
Review				✔	✔		✔	✔									✔		✔	
Dissemination						✔		✔											✔	
Returning Evidence			✔					✔					✔							✔
Digital Crime Scene Investigation				✔	✔		✔	✔												
Physical Crime Scene Investigation				✔	✔		✔											✔	✔	
Documentation				✔	✔	✔	✔	✔					✔					✔	✔	✔
Preserving Chain of Custody						✔	✔					✔								✔
Preserving Digital Evidence						✔		✔										✔		
Information Flow						✔												✔		
Case Management						✔							✔							
End of the Table																				

15.3 Overview of the Proposed Model

The soundness of a digital forensic investigation process model is a function of usability and acceptability [9, 35]. To achieve the soundness, classes, processes and principles were incorporated into the CDFIPM. A class is the highest level (first layer) in the CDFIPM; it is the main group containing one lower layer, namely,

processes. A process is the next level down from a class and the second layer in the CDFIPM. Processes are obvious and individually separate steps; they can sometimes be a function of time and therefore can be sequential or sometimes iterative. In contrast, the action principles included in the concurrent process class are those processes that are not confined to a single point in time during an investigation. Instead, they have to be maintained concurrently throughout the whole or parts of the other processes in the CDFIPM. As Fig. 15.1 illustrates, there are six classes in the CDFIPM with each class containing a certain number of processes. There is also a total number of eight action principles contained in the concurrent process class. As the CDFIPM has already been discussed in detail in Montasari [31], the following subsections provide only a brief overview of the model's classes together with the various processes included in each class.

15.3.1 The Readiness Process Class

Forensic readiness is the ability of an organisation to maximise the collection of credible digital evidence from an incident environment and minimise the cost of a forensic incident response [38]. Organisations should focus their efforts on establishing two components including operational readiness and infrastructure readiness.

15.3.2 The Initialisation Process Class

The initialisation process class initiates the digital investigation and contains five processes described as follows.

15.3.2.1 Incident Detection Process

Incident detection is the first step in a digital investigation where an incident is detected by either internal events such as an intrusion detection system or external events such as crime being reported to the police.

15.3.2.2 First Response Process

During this process, the first responders must secure the crime scene in order to ensure preservation of digital device(s) suspected of containing potential digital evidence. Preservation should include disconnecting digital device(s) from a networked environment and detecting the corrupted data. The network must also be monitored to detect incoming calls and IP addresses.

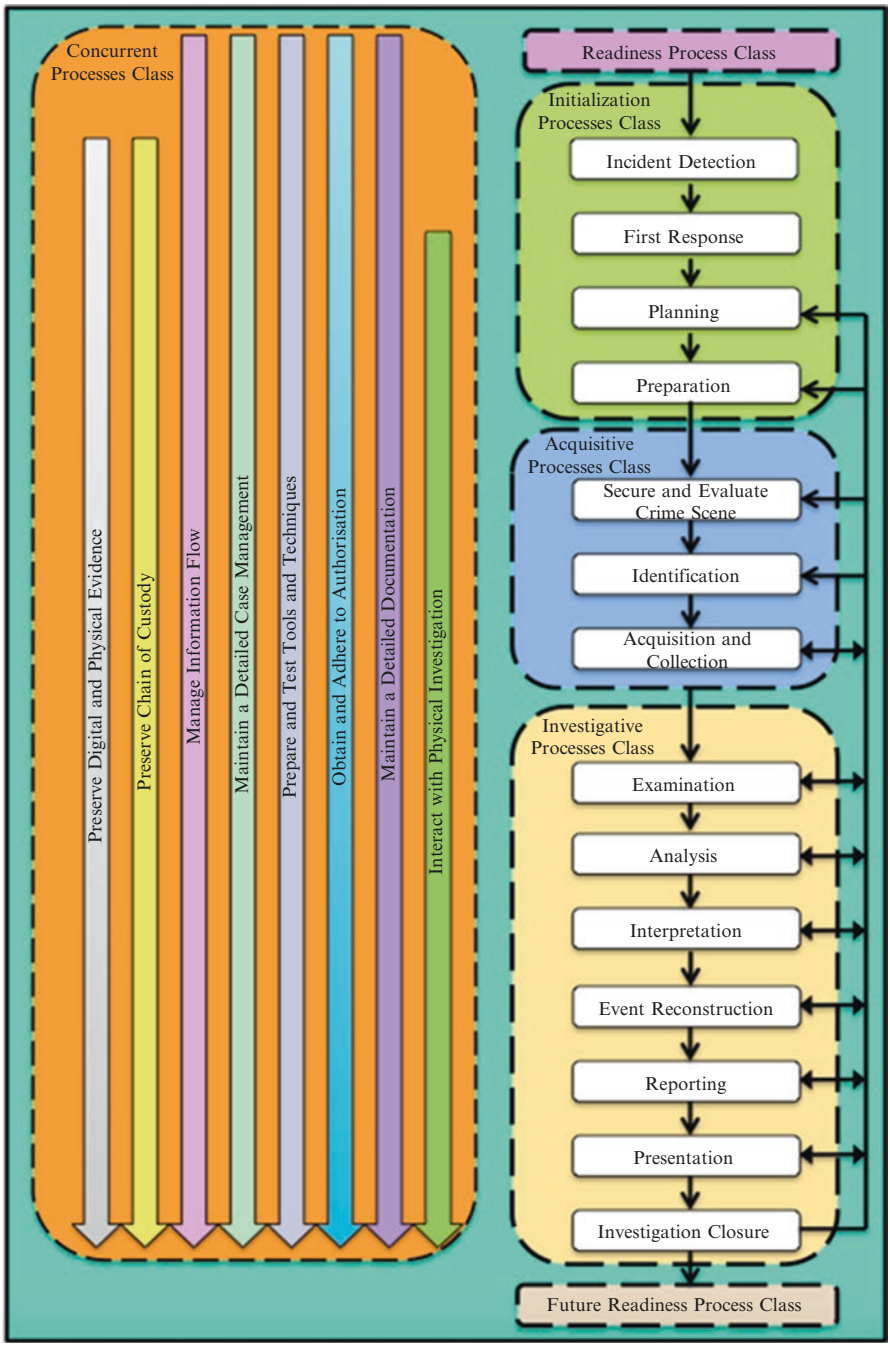

Fig. 15.1 The proposed model (the CDFIPM)

15.3.2.3 Planning Process

During this process, investigators must plan and develop proper procedures and define methodologies, the choice of tools to use and the appropriate human resources that should be involved in the investigation. At this stage, investigators are not expected to produce anything beyond a rough outline of a plan [3].

15.3.2.4 Preparation Process

The preparation process involves implementing those planning made in the previous process. This includes, but is not limited to, preparing appropriate equipment (both hardware and software), infrastructure, human resources, raising awareness, training and documentation.

15.3.3 The Acquisitive Process Class

The acquisitive process class pertains to the processes that are concerned with the acquisition of evidence; this class includes five processes described as follows.

15.3.3.1 Secure and Evaluate the Crime Scene Process

During this process, investigators must enforce a lock down of the entire crime scene to preserve the integrity of both digital device and the digital evidence [12]. Investigators must also carry out a preliminary survey of the physical crime scene to obtain an idea about how to process the physical crime scene. They should aim to identify the obvious pieces of physical evidence, identify any technical issue, determine the mixture of laboratory and on-site data acquisition and finally develop an initial theory about the crime [3].

15.3.3.2 Identification Process

The identification process enables investigators to fill the gap in relation to the location, size and format of the digital device suspected of containing the potential digital evidence [3]. During this phase, investigators must perform a methodical search for digital evidence which can be both in physical and logical form.

15.3.3.3 Acquisition and Collection Process

This process requires investigators to determine whether to carry out a live or a static data acquisition. Various factors will influence such a decision including the type of authorisation, the type of environment in which the device is operating and also the type and size of storage media (ISO/IEC 27043 49). Investigators will need to determine the most appropriate methods of acquiring digital evidence in line with the common practice suggested by ISO/IEC 27037 [21] and ACPO [1]. During the data acquisition, master copy and working copy of the raw data must be acquired by creating verifiable image of all the bits and bytes contained within the digital device. The original source and the digital evidence copies should then be verified with a proven function such as MD5 or SHA1 so that the extracted data can attain legal validity as genuine. In certain circumstances, it is not practical or permissible to acquire a digital evidence copy of the entire evidence source due to its large storage size. In such circumstances, investigators should perform a logical acquisition that targets only specific data types, directories or locations.

15.3.4 The Investigative Process Class

The investigative process class contains those processes that pertain to investigating the incident or crime that has been the reason for the digital forensic investigation. This class includes six processes described as follows.

15.3.4.1 Examination Process

During the examination process, investigators must survey the digital crime scene preferably in a forensic laboratory on the image of the system. In circumstances where this activity must be performed on a live system, investigators must ensure to perform field searches by booting the system into a trusted environment in order to prevent the modification of the digital evidence. Investigators must also identify and locate potential evidence possibly within unconventional locations. A large number of techniques might be performed to find obfuscated data which might have been deleted or hidden, and there might be large volumes of data to be examined. Therefore, automated techniques should be employed using tools such as FTK or EnCase in order to support the investigators. The data should then be harvested by giving a logical structure to the entire data set. The result of the harvesting activity is a logical structured data set in which the extracted raw data becomes structured information. This denotes that the harvested information can now be mounted and read by the original file system such as FAT or NTFS. The data also needs to be reduced to expedite the examination process due to the fact that there can be very large amount of data. Identifying known elements can enable investigators to reduce the data. Investigators will need to use the metadata and unique identifiers, such as

MD5, in order to remove known system files and other application data. The data that will remain will be modified data or data that could be uniquely attributed to the users of a specific computer system. Digital evidence with similar identifying patterns should also be classified based on the types of investigation.

15.3.4.2 Analysis Process

This process involves investigators reconstructing fragments of data based on their significance and determining a possible root cause of the incident. Based upon the results of the examination process, investigators must now be able to define what the exact characteristics of the incident are and who is to be held accountable for the incident. Investigators must be able to formulate a hypothesis of how the incident took place by reconstructing a sequence of events which have resulted in the current state of the system under investigation. Investigators must thoroughly examine and test the data that was organised in the examination process against the hypothesis that was formulated in the previous activity. Moreover, the investigators must also question the legal validity of the possible digital evidence by considering issues such as relevance, admissibility and weight. This will enable them to test the hypothesis by identifying the best possible evidence. Digital evidence should then be linked and attributed to a specific user or the event which is the root cause of the incident or crime. Finally, under this process, investigators must evaluate their findings in order to ensure that the hypothesis they have developed holds true. Backtracking from the analysis process to the examination process is often to be expected as the investigators acquire a better understanding of the events which resulted in the investigation in the first place.

15.3.4.3 Interpretation Process

Investigators must interpret digital evidence to produce meaningful statements in the legal context. After interpreting the analysis results, investigators will need to classify the interpreted evidence according to relevance by organising the evidence in a way that they can differentiate which digital evidence items are more important than the others. Event reconstruction is another activity through which investigators should be able to reconstruct a possible event sequence reflecting the incident results by using the series of events known to them that they have deduced from the digital evidence. Investigators should use this process to explain how the incident might have occurred, prior to assessing the review results against the original hypothesis formulated in the analysis process. This will be to determine whether they have obtained all the evidence required to support the original hypothesis. If all the evidence has not been obtained, investigators will then need to iterate to the analysis process, in which the hypothesis development activity will form a cycle that needs to be repeated until investigators can explain the incident. If there is no need to backtrack to the analysis process, any areas of improvement will need to be identified to address those required improvements.

15.3.4.4 Reporting Process

This process requires investigators to compile an accurate report based on the their findings constructed in an opinion to be presented to a relevant audience. This report must contain conclusions that can be reproduced by independent third parties. Also, since an investigation might produce many incriminating digital evidence items, investigators must ensure that all digital evidence items are listed in the report so that no valuable item of evidence is left out. The report must be in a simple language and be well-defined, concise and unambiguous in order for the lay person (such as judge and jury) to be able to understand it.

15.3.4.5 Presentation Process

This process involves presenting the output of the reporting process, which should be a well-written report, to a wide variety of audience such as courts of law, law enforcement and management in an organisation. Presenting the report can be carried out in the form of the report itself or can be accompanied by other formats such as multimedia presentation and expert witness, etc.

15.3.4.6 Investigation Closure Process

This process involves reviewing the existing policies and procedures of the victim organisation based on the outcome of the investigation. Lessons from the incident must be identified and learnt in order to enable the organisation to apply the findings and be better prepared for the future incidents. A decision must also be made regarding whether to return, cleanse and reuse or destroy the evidence. In certain circumstances, the evidence might need to be stored for a certain period of time before any of the three possibilities can be applied. The decision made concerning the investigation must be recorded ideally on a database for the future reference. Relevant information regarding the entire investigation must also be disseminated and communicated to all stakeholders. This includes communicating the need to return to a previous process, deciding on the acceptance or rejection of the hypothesis or providing any reports or documents from the presentation process.

15.3.5 The Future Readiness Process Class

This aim of this class is to enable victim organisations to prepare for and mitigate the risks of potential future incidents. This class involves victim organisations applying the lessons learnt and also improving their existing policies and procedures based on the review of the outcome of the case from the preceding process.

Ideally case studies should also be developed for the future reference to enable both victim organisations as well as other corporates to learn from the incident which has been investigated.

15.3.6 The Concurrent Process Class

Concurrent process class comprises of nine overriding principles or action principles that are applicable to other processes in the model. These principles are objectives that need to be achieved in a given digital investigation and should be performed concurrently throughout the whole or parts of the other processes in the CDFIPM. Maintaining these principles in a digital investigation ensures the admissibility of digital evidence in a court.

15.3.6.1 Preserve Digital and Physical Evidence

This principle refers to protecting both the physical and digital evidence against damage or alteration. In order to enable the investigators to preserve the evidence in a forensically sound manner, organisations and law enforcement agencies will need to establish and maintain certain strict procedures, effective quality systems such as standard operating procedures (SOPs) or procedural workflows.

15.3.6.2 Preserve Chain of Custody

In order to preserve chain of custody, investigators must adhere to all legal requirements and must properly document each given process within the CDFIPM. Chain of custody is of extreme importance; cases where the chain of custody has not been properly preserved can be easily challenged in courts. An example of preserving chain of custody is when evidence copies are required to be shared with other experts in other locations.

15.3.6.3 Manage Information Flow

A defined information flow should exist between each given process in a digital investigation so that it can be protected and supported technologically. An example of the information flow can be the exchange of digital evidence between two investigators involved in the same investigation. This information flow can be protected, for example, through the use of trusted public key infrastructures (PKI) and time stamping to identify the different investigators, protect the evidence integrity and also protect the confidentiality of the evidence through PKI-based encryption [13].

15.3.6.4 Maintain a Detailed Case Management

This overriding principle applies to the role of managers who often lead a team of investigators during an investigation. Managers will need to undertake certain tasks including guiding investigators in the right direction, creating an overall picture of the investigation, determining the cost of investigation, identifying team members for each given process, etc.

15.3.6.5 Prepare and Test Tools and Techniques

It is vital that investigators prepare an appropriate set of tools and techniques during the course of an investigation so that each process of the investigative process can be carried out effectively. Cases where untested tools have been used to carry out digital investigations are easily challenged in courts. Therefore, investigators must select tools that are court-approved such as EnCase, AccessData FTK and ProDiscover.

15.3.6.6 Obtain and Adhere to Authorisation

Any digital investigation that is commissioned to be carried out necessitates proper authorisation, whether it is an internal or an external authorisation. This principle ensures that the rights of the system owners, custodians, principles or users are not infringed and that no law is violated.

15.3.6.7 Maintain a Detailed Documentation

It is extremely important to document all activities carried out throughout the entire investigative process in order to enable other investigators to authenticate the process and results. This principle involves recording all information applicable or produced during the investigative process to support decision making and the legal, administrative processing of those decisions.

15.3.6.8 Interact with Physical Investigation

A digital investigation and a physical investigation are often interrelated and dependent on one another. In cases where a physical investigation requires an assistance from a digital investigation, an example can be to use a digital forensic investigation to reveal communications between terror suspects via computers, mobile phones, online social network activities, email communication, communication via chat rooms and forums, etc. An example of digital investigation being dependent on a physical investigation is when a suspect is interviewed to provide a password to a

system under investigation. Defining the relationship between a digital investigation and a physical investigation is required to preserve chain of custody, preserve the integrity of the digital evidence, protect the digital evidence from damage and ensure an efficient investigation [46].

15.4 Research Methodology

The design science research (DSR), widely adopted in the domain of information systems (IS) [19, 20, 26, 32, 33, 47], has been selected as the methodology to conduct the research presented both in this paper and also in Montasari [31]. The DSR involves the design of novel or innovative artefacts and the analysis of the performance or use of such artefacts [24, 48]. The development and evaluation of artefacts form an important part in the DSR [20, 27]. Artefacts include, amongst others, models, methods, constructs, instantiations and design theories [26, 27], social innovations and new or previously unknown properties of technical, social or informational resources [27]. The artefact related to the research presented in Montasari [31] and this paper is a new model, the Comprehensive Digital Forensic Investigation Process Model (CDFIPM), that encompasses the entire digital investigative process. The organisational context associated with this research is that of law enforcement, corporates and incident response. This research also addresses the hitherto unsolved problem that there does not exist a comprehensive model encompassing the entire digital investigative process that is both formal, in that it synthesises, harmonises and extends the existing models and, in generic, in that it can be employed in the different fields of law enforcement, incident response and commerce. The selection of the DSR over other alternative methodologies (such as Requirements Engineering: RE) is justified as it is particularly suited to the task of creating a new process model (an IT artefact) [3]. Armstrong and Armstrong [7], as cited by Adams [3], state that with the DSR's focus on designing solutions, it is ideal when approaching the problem domain of digital forensics. Various researchers both within and outside the IS domain have provided guidance to define the DSR and have described what goals should be followed in its production [2, 6, 16, 19, 20, 26, 32, 33, 37, 43, 47, 49]. These researchers have often proposed various methods, processes or theoretical frameworks to rationalise the DSR studies. However, the design science research process (DSRP) model proposed by Peffers et al. [33] has been selected as the appropriate DSR to conduct the research in this paper and Montasari [31]. The rationale for doing so is due to the fact that it provides a graphical representation of the conceptual process for both carrying out and presenting the DSR. Such a mental model facilitates the application of the DSR and can also assist the author in producing and presenting a high-quality DSR that would be accepted as valuable, rigorous and publishable within the field of digital forensics science.

The Peffers et al.'s [33] DSRP consists of seven components as shown in its graphical representation in Fig. 15.2.

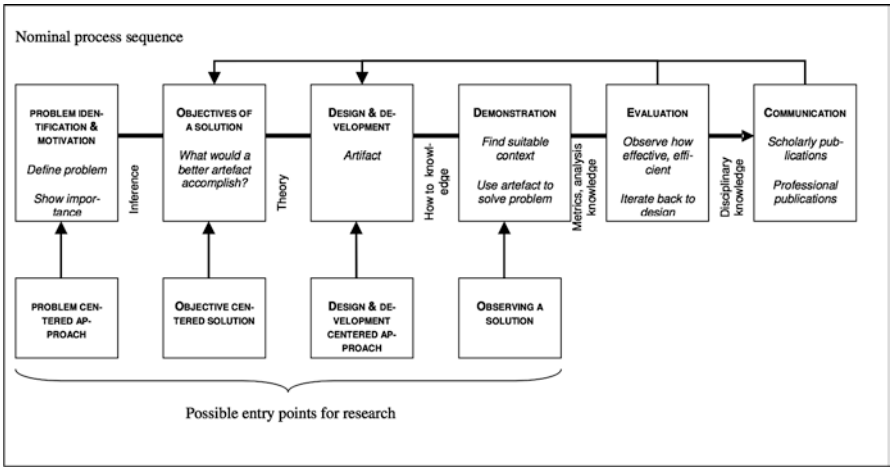

Fig. 15.2 The design science research process (DSRP) model after Peffers et al. [33]

The first three components of the DSRP, namely, problem identification and motivation, objectives of a solution and design and development, have already been covered in the previous research paper [31]. This paper covers the two out of the three remaining components, namely, the demonstration and communication activities, with the remaining component, namely, the evaluation activity, being covered in the future work (see Sect. 15.6). Nevertheless, the following three subsections including Sects. 15.3.1, 15.3.2, and 15.3.3 describe how the first three components of the Peffers et al.'s [33] DSRP were applied to the research presented in Montasari [31]. The remaining three subsections including Sects. 15.3.4, 15.3.5, and 15.3.6 then discuss how the two out of the three remaining components have been applied to the research in this paper and how the remaining component will be applied to the future work.

15.4.1 Problem Identification and Motivation

The research presented in Montasari [31] addressed the following problem:

> *That there does not exist a comprehensive model encompassing the entire digital investigative process that is formal in that it synthesises, harmonises and extends the existing models and that is generic in that it can be applied in the different fields of law enforcement, commerce and incident response*

A profound knowledge of the problem addressed by the research was acquired through a detailed analysis and assessment of the literature related to previous DFIPMs in Montasari [30] and Montasari and Peltola [29].

15.4.2 Objectives of a Solution

The aim of the research was as follows:

To develop a comprehensive model encompassing the entire digital investigative process that is formal in that it synthesises, harmonises and extends the exiting models and that is generic in that it can be applied in the different fields of law enforcement, commerce and incident response

The research aim was formulated according to the definition of the problem. In order to formulate the stated aim, a deep knowledge was acquired of the state of the problem and its current solution in the form of previously proposed DFIPMs and their efficacy.

15.4.3 Design and Development

Prior to designing and developing the CDFIPM, all previously proposed models were analysed in order to identify which could contribute to the new model. Law enforcement, commerce and incident response were the three environments on which the research in Montasari [31] focused. Therefore, the existing models within those three domains were considered for their possible contributions to the new model. Once the most reliable models were identified, their specific key contributions were determined for inclusion in the new model. Following this, the essential components necessary for the new model were identified from the specific key contributions. These formed the basic structure of the CDFIPM. The prevailing models were then built upon by the construction of a new set of domain-specific components. Contribution of the previous models in the form of identified components as well as the new set of constructed components were used to develop the new model. The CDFIPM was graphically represented in the form of UML Activity Diagram.

15.4.4 Demonstration

Following the design and development of the CDFIPM, its implementation needed to be demonstrated within an appropriate environment. Peffers et al. [33] as well as various other researchers in the field [4, 9, 11–13, 46] suggest the use of case studies as such an appropriate environment. Therefore, the CDFIPM was applied to a case study (see Sect. 15.5) in order to demonstrate its application and effectiveness within the three stated domains.

15.4.5 Evaluation

Based on the DSRP's requirements, the CDFIPM will also need to be evaluated to determine how well it supports the solution to the stated problem. The evaluation activity, which is not covered in this paper but in the future work (see Sect. 15.6), will aim to compare the CDFIPM's application and effectiveness with the characteristics set out in its research aim. Evaluation activity will involve the submission of the CDFIPM to digital forensic practitioners within the three domains that are the focus of this research and also to judges, barristers and researchers in academia, those being experts within two other domains to which the model has relevance. The aim of such an approach will be to enable the author to acquire insightful and reliable feedback as to the effectiveness of the CDFIPM from authoritative external reviewers (an approach also undertaken by other researchers such as those in [3, 32, 36]. Once the evaluation has been carried out, the author will have been able to judge whether to repeat the design and development phase of the CDFIPM in order to make improvements. Any such amendments will be subsequently introduced to the design and implementation stages of the CDFIPM.

15.4.6 Communication

Again in accordance with the DSRP's requirements, the problem addressed by this research and its importance, its solution (the CDFIPM), its utility and novelty, the rigour of its design and implementation and its effectiveness all needed to be communicated to the intended user community. Therefore, the communication activity of the DSRP in relation to this research was achieved through publications such as Montasari [30, 31] and Montasari and Peltola [29] in well-known and peer-reviewed journals and conferences. In addition, there was direct interaction with a wide variety of experts, including digital forensic practitioners, legal practitioners and experts in academia.

15.5 Testing the CDFIPM

This section follows the demonstration activity of the Peffers et al.'s [33] DSRP, used in this research. The demonstration activity of the DSRP requires a researcher to apply the artefact in an appropriate environment such as 'experimentation' and 'case study' to solve the stated problem [3, 8, 19, 33]. Resources needed for the demonstration activity include effective knowledge of how the artefact should be applied to solve the stated problem. Therefore, in order to assess how the CDFIPM addresses the stated research problem, the CDFIPM is applied into a case study and a walkthrough of the model is performed. The case study presented is based on an

actual situation and is intended to demonstrate the potential deployment of the CDFIPM. The following case study, which is modelled after Ciardhuáin [13], relates to the exploitation of a vulnerability found in an online service operated by a bank:

15.5.1 Case Study

The following case study is modelled after Ciardhuáin's [13] paper. This investigation started when Bank X in London (England) received an email claiming to have found a vulnerability in an online service operated by the bank. The email offered to provide details of the vulnerability in exchange for payment. On checking their logs, Bank X concluded that an unauthorised access had been made to their web server. The bank received further emails threatening to reveal the vulnerability to the press and public, including a link to a website which the suspect intended to use to disclose the vulnerability. Bank X reported the issue to the police in London who initiated the investigation. It became obvious that the compromised web server was located in Manchester (England) from Bank X's headquarters and that the source of the emails was in Cardiff (Wales). Therefore, another police force, namely, the South Wales Police (SWP), took up the case to start the investigation. Throughout the following stages of the digital investigative process, investigator R and investigator P adhere to all the eight overriding principles of the CDFIPM (see Sect. 15.2).

15.5.1.1 Readiness Process

Bank X has already implemented both operational and infrastructure readiness capabilities and has an in-house incident response team and procedures for forensic readiness and incident detection implemented. The bank also has its own standard operating procedures (SOPs).

15.5.1.2 Incident Detection Process

The first step in this investigation is the incident detection and the creation of awareness that the investigation is needed. In this case, the incident has been reported by the suspect himself to the Bank X. After the incident has been detected, the bank requests its senior IT Administrator, Mr. Thompson, to look into the issue to confirm or refute the validity of the incident as this might be a hoax. Mr. Thompson contacts the head of the incident response team for assistance in this matter. To validate and assess the incident, Mr. Thompson and the incident response team examine the emails and log files and confirm that the system's security has been compromised. Bank X then reports the incident to the London MPS (Metropolitan Police Service), who initiates the investigation of its own. It becomes clear that the compromised

web server is based in Manchester and that the suspect is located in Cardiff; therefore, the investigation is passed to SWP (the South Wales Police). Up to this point, the reporting of the incident has taken place three times: when Bank X receives the emails, when the bank reports it to the MPS and when the investigation is passed to the second police force, SWP. During this process, both internal and external authorisations are needed. The internal authorisation is obtained when Bank X instructs its senior IT administrator to conduct the investigation. The external authorisation is acquired when the MPS realises that SWP are the police force who are authorised to carry out the investigation. The search warrant is the example of this authorisation. Moreover, during this process, detailed and contemporaneous documentation is made.

15.5.1.3 First Response Process

Due to the fact that this incident involves law enforcement and is investigated externally, this process is only partly applicable to this case scenario. The application of this process is when the incident response team assists the senior IT administrator in examining the log files.

15.5.1.4 Planning Process

The Planning activity is conducted by both Bank X and the two police forces. This activity takes place in the bank's investigation when they perform an examination of the logs and decide to involve the police based on what they have found. The Planning activity also takes place in the two police forces investigations where they plan their own respective approaches to be undertaken to identify the suspect and collect the needed evidence. Under the planning stage, the two police forces consider data constraint, timing constraint, physical constraint and authorisation, as well as performing risk assessment, planning logistics and creating their own outline plans.

15.5.1.5 Preparation Process

Under the preparation activity, Bank X and the two polices forces simply implement the plans that they have drawn in the Planning stage.

15.5.1.6 Secure and Evaluate the Crime Scene Process

This activity takes place when the SWP police officers raid the premises of the suspect's place of employment. The first step they take is to address the safety issues such as the safety of the officers and employees, followed by preserving the crime scene. Since the suspect is at the crime scene, he is detained and briefly interviewed as the authorisation allows the questioning of the suspect. Investigators then survey

the crime scene in order to determine the location of digital device(s) and establish the combination of on-site and off-site data acquisition. Throughout the entire process, detailed contemporaneous notes of all activities are maintained.

15.5.1.7 Identification Process

Identification initially takes place when Bank X identifies their log files to determine what has occurred. Both police forces, MPS and SWP, later carry out the same activity to locate the sources of the emails. Moreover, SWP conducts a physical search which results from the information obtained from the previous searches. Secure and evaluate crime scene process and identification processes both overlap as each process requires searching the physical crime scene.

15.5.1.8 Acquisition and Collection Process

This process takes place when the search of the employer's premises in the previous process led to the seizure of a computer. Since the suspect's computer system is not a mission-critical system and the authorisation permits its seizure, the investigators decide to size the system and conduct an off-site data acquisition in the police forensic laboratory. However, since the system is running, officers decide to conduct a live acquisition of volatile data first prior to shutting down the system in case the RAM might contain valuable information which might be lost after powering down the system. Using FTK, the officers perform a live acquisition of the volatile data and duplicate the master copy of the captured image of RAM. Both copies are then verified using MD5 and SHA1 checksums. Since the data on the system is stable, the officers remove the power source directly from the suspect's computer. They then record, remove and secure connections prior to labelling and packaging the system. The transport phase takes place when the system is seized and physically transferred to the police. This phase also occurs in three other occasions including when the captured image of the RAM is taken to the police, when log files are transferred from server to the police for later examination and analysis and when the emails are transferred from the bank to the police. The storage phase occurs when the police retain the seized computer, the captured images of both hard drive and RAM, log files as well as emails in a secure storage facility. In the forensic laboratory, the investigators image the hard drive of the system and verify it using MD5 and SHA1 checksums. They also duplicate the master copy to become the working copy on which the subsequent Examination and Analysis will be performed.

15.5.1.9 Examination Process

This activity initially occurs when the bank examines their log files. It also occurs when the police examine log files, emails and the working copy of both hard drive and RAM images of the suspect's system in the forensic laboratory. During the

examination process, investigators process the deleted and hidden data to ensure that emails and log files are recognised from the evidence. Investigators also harvest data to provide structure to data which they are interested in so that it can be mounted on the investigating machine. Since the suspect's system contains large amount of data such as known systems files, investigators use metadata and unique identifiers to reduce the data by removing known system files and different other application data. The investigators are now left with the log files and the emails that the suspect sent to Bank X. Now, the emails can be uniquely attributed to the suspect who has been the user of that specific system.

15.5.1.10 Analysis Process

This process initially takes place when Bank X's system administrator, Mr. Thompson, and the incident response team conclude from the log files that an unauthorised access has been made to their web server. Later on, this process is conducted in a forensic laboratory by investigators who develop the initial hypothesis for the identity of the suspect and for the manner in which the incident has taken place.

15.5.1.11 Interpretation Process

This process occurs after investigators evaluate their findings in the analysis process and determine that their formulated hypothesis is true. During this process, investigators interpret digital evidence to produce meaningful statements for later reporting and presentation regarding how the suspect made an unauthorised access to Bank X's web serve. As part of this process, investigators classify and organise the interpreted evidence such as log files and emails according to their relevance in order to distinguish which digital evidence items are more important than the others.

15.5.1.12 Event Reconstruction Process

This process occurs when investigators reconstruct the events which led to the identification of the suspect and the subsequent seizure of the suspect's computer. This entails the investigators iterating in the CDFIPM and results in a more detailed hypothesis. Through this process, investigators are able to explain how the suspect has carried out the intrusion to Bank X's web server. Investigators consolidate and review their findings prior to assessing the results of their review against the original hypothesis that they have formulated. Through this assessment, investigators ensure that they have gathered all relevant evidence related to that attack to support their hypothesis.

15.5.1.13 Reporting Process

This process takes place when investigators compile a report based on their findings to be presented in a court.

15.5.1.14 Presentation Process

This process occurs five times during the entire investigation. This includes when the bank's IT administrator presents the evidence to the management within the bank, when the bank approaches the MPS police and present their evidence to investigators, when the MPS police pass the investigation to SWP, when evidence is presented to acquire a search warrant and when investigators present the evidence in the court. The formality of the evidence increases as the investigation proceeds. Prior to presenting the findings to the court, investigators meet with the legal team to understand the presentation requirements. Through the meeting, the target audience in the court are determined. Investigators also carry out the necessary preparation prior to attending the court such as preparing expert testimony, exhibits and appropriate presentation aids. During the presentation in the court, investigators are able to assist the judge and jury in understanding the technical points made by avoiding complex arguments and delivering their conclusion in a logical and structured manner. The presentation contains factual data that investigators have deduced. Moreover, investigators use the CDFIPM to enable the judge to comprehend the processes that they have followed during the investigation. In the court, the investigators have to prove and to defend the validity of the hypothesis as it is challenged by the court and the defence lawyers. Since investigators have followed a formal model which enabled them to carry out the investigation in a forensically sound manner, the opposite hypothesis is refuted. The court decides that the suspect has made an unauthorised access to Bank X's web server and sentences him to prison.

15.5.1.15 Investigation Closure Process

This process takes place after a formal decision is reached by the court concerning the incident. During this process, based on the outcome of the investigation, Bank X reviews its existing policies and procedures concerning its IT security. As there is no need to backtrack to the previous stages in the investigation, bank management decide to accept the hypothesis. During this process, the bank identifies the lessons learnt and the suspect's system is returned to his employer's company. The result of the case is recorded on the database for the future readiness. The final phase of this activity is disseminate investigation results, where relevant information concerning this incident and its outcome are communicated to all stakeholders. The initial communication is carried out prior to the completion of the trial in order to remove the

sensitive data from the disseminated information. The final phase, the review phase, discusses how the incident could have been handled better. One outcome is to instal the central log server sooner than planned. The review phase includes a review of the investigation and identifies some new analysis techniques that are employed. The techniques are added to the official analysis procedures. During the analysis, new suspect files are identified, and they are added to the hash database so that they can be quickly found in the future investigations.

15.5.1.16 Future Readiness Process

This activity takes place both in Bank X and also the two police forces. Bank X starts applying the lessons that they have learnt from this incident; a set of recommendations are made on how they can improve in terms of securing their digital data assets. As a result, they improve their existing forensic readiness procedures and incident detection systems. The two police forces also develop case studies based on this particular investigation for future training of other officers.

15.5.2 Case Study Discussion

This section followed the demonstration activity of Peffers et al.'s [33] DSRP and discussed the method employed to demonstrate the potential deployment of the CDFIPM. In order to assess how the CDFIPM addressed the stated research problem, the model was applied to a case study and a 'walkthrough' of the model was performed. The walkthrough of the CDFIPM employing the case study successfully mapped the entire processes of the model to the corresponding activities carried out by digital forensic investigators. This method of testing the CDFIPM using the case study clearly demonstrated that the proposed model is very efficient in enabling investigators to account for every investigative process carried out through the iterative structure of the CDFIPM. Notice that it would have been possible to investigate this case study using a different model other than the CDFIPM. However, it is argued that the application of the CDFIPM to any digital investigation within the three stated domains covered by the research scope would be more effective as the proposed model has inherited all the benefits of the previous models by rigorously synthesising, harmonising and building upon them. Having completed the demonstration activity, the next stage in the Peffers et al.'s [33] DSRP is the evaluation activity, which will need to be conducted by a number of digital forensic investigators, legal practitioners, experts and researchers in the field of digital forensics. The evaluation activity, however, will be the subject of future work.

15.6 Conclusion and Future Work

A new and Comprehensive Digital Forensic Investigation Process Model has now been described in Montasari [31] and tested in this paper. Synthesising, harmonising and building upon the previous models as well as including the overriding principles in the new model have made the CDFIPM much more comprehensive than previous models. It is argued that the CDFIPM provides a foundation for the development of techniques and especially tools to support the work of investigators. Although the CDFIPM is mainly aimed at the UK jurisdiction, it could easily be adapted to other jurisdictions. Without such modification, the model already has relevance to those jurisdictions which employ a similar legal basis for evaluating the digital investigative process. As the future work, to determine the CDFIPM's usability and utility further, an independent evaluation of the CDFIPM will need to be carried out by the high-tech crime units (HTCUs) of different police forces, experts in corporate and incident response environments, legal practitioners and researchers in academia. Similarly, although the case study to which the CDFIPM was applied represents each of the three fields of digital forensics to which the model is relevant, the CDFIPM would benefit from further case studies to identify task hierarchies. This would improve task development efforts and facilitate scenario development, assisting its users, researchers and tool developers in understanding how to take advantage of and apply the model. Finally, as with the future work, the CDFIPM must be validated through the method validation under ISO 17025 accreditation, which will be published in the UK within the next 18 months (as of July 2016), to determine its compliance.

References

1. ACPO. (2012). ACPO good practice guide for digital evidence. U.K. Association of Chief Police Officers.
2. Adams, L., & Courtney, J. (2004). Achieving relevance in IS research via the DAGS framework. *37th Hawaii International Conference on System Sciences* (pp. 1–10). Big Island, HI, USA.
3. Adams, R. (2012). The Advanced Data Acquisition Model (ADAM): A process model for digital forensic practice. PhD thesis. Murdoch University.
4. Adams, R., Hobbs, V., & Mann, G. (2014). The advanced data acquisition model (ADAM): A process model for digital forensic practice. *Journal of Digital Forensics, Security and Law, 8*(4), 25–48.
5. Agarwal, A., Gupta, M., Gupta, S., & Gupta, C. (2011). Systematic digital forensic investigation model. *International Journal of Computer Science and Security, 5*(1), 118–130.
6. Archer, L. (1984). *Systematic method for designers*. London: Wiley.
7. Armstrong, C., & Armstrong, H. (2010). Modeling forensic evidence systems using design science. *IFIP WG International Working Conference* (pp. 282–300).
8. Balci, O. (2004). Quality assessment, verification, and validation of modeling and simulation applications. *Proceedings of the 2004 Winter Simulation Conference* (pp. 1–8). Washington DC.

9. Beebe, N., & Clark, J. (2005). A hierarchical, objectives-based framework for the digital investigations process. *Digital Investigation, 2*(2), 147–167.
10. Carlton, H., & Worthley, R. (2009). An evaluation of agreement and conflict among computer forensic experts. *42nd Hawaii International Conference on System Sciences* (pp. 1–10). Washington DC.
11. Carrier, B., & Spafford, E. (2003). Getting physical with the digital investigation process. *International Journal of Digital Evidence, 2*(2), 1–20.
12. Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers and the internet* (3rd ed.). New York: Elsevier Academic Press.
13. Ciardhuáin, O. (2004). An extended model of cybercrime investigations. *International Journal of Digital Evidence, 3*(1), 1–22.
14. Cohen, F. (2011). Putting the science in digital forensics. *Journal of Digital Forensics, Security and Law, 6*(1), 7–14.
15. Cohen, F. (2012). Update on the state of the science of digital evidence examination. *Proceedings of the Conference on Digital Forensics, Security, and Law* (pp. 7–18). Richmond, USA.
16. Eekels, J., & Roozenburg, N. (1991). A methodological comparison of the structures of scientific research and engineering design: Their similarities and differences. *Design Studies, 12*(4), 197–203.
17. Freiling, C., & Schwittay, B. (2007). A common process model for incident response and computer forensics. *3rd International Conference on IT-Incident Management & IT-Forensics* (pp. 19–40). Stuttgart, Germany.
18. Garfinkel, S., Farrell, P., Roussev, V., & Dinolt, G. (2009). Bringing science to digital forensics with standardized forensic corpora. *Digital Investigation, 6*, 2–11.
19. Hevner, A., & Chatterjee, S. (2010). *Design research in information systems*. New York: Springer.
20. Hevner, A., March, S., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly, 28*(1), 75–105.
21. International Organisation for Standardization. (2012). *ISO/IEC 27037:2012. Information technology–Security techniques–Guidelines for identification, collection, acquisition and preservation of digital evidence*. Geneva: International Organization for Standardization.
22. Kessler, C. (2010). Judges' awareness, understanding, and application of digital evidence. PhD thesis, Nova Southeastern University.
23. Kohn, M., Eloff, M., & Eloff, J. (2013). Integrated digital forensic process model. *Computers & Security, 38*, 103–115.
24. Kuechler, B., & Vaishnavi, V. (2008). On theory development in design science research: anatomy of a research project. *European Journal of Information Systems, 17*(5), 489–504.
25. Leigland, L., & Krings, A. (2004). A formalization of digital forensics. *International Journal of Digital Evidence, 3*(2), 1–32.
26. March, S., & Smith, G. (1995). Design and natural science research on information technology. *Decision Support Systems, 15*(4), 251–266.
27. March, S., & Storey, V. (2008). Design science in the information systems discipline: An introduction to the special issue on design science research. *MIS Quarterly, 32*(4), 725–730.
28. Mason, S. (2007). *Electronic evidence: Disclosure, discovery and admissibility*. London: LexisNexis Butterworths.
29. Montasari, R., & Peltola, P. (2015). Computer forensic analysis of private browsing modes. In *Proceedings of 10th international conference on global security, safety and sustainability: Tomorrow's challenges of cyber security* (pp. 96–109). London: Springer International Publishing.
30. Montasari, R. (2016). An Ad Hoc detailed review of digital forensic investigation process models. *International Journal of Electronic Security and Digital Forensics, 8*(3), 203–223.
31. Montasari, R. (2016). A comprehensive digital forensic investigation process model. *International Journal of Electronic Security and Digital Forensics (IJESDF), 8*(4), 285–301.

32. Nunamaker, J., Chen, M., & Purdin, T. (1990). Systems development in information systems research. *Journal of Management Information Systems, 7*(3), 89–106.
33. Peffers, K., Tuunanen, T., Gengler, C., Rossi, M., Hui, W., Virtanen, V. & Bragge, J. (2006). The design science research process: A model for producing and presenting information systems research. *1st International Conference on Design Science Research in Information Systems and Technology* (pp. 83–106). USA.
34. Pollitt, M. (2009). The good, the bad, the unaddressed. *Journal of Digital Forensic Practice, 2*(4), 172–174.
35. Reith, M., Carr, C., & Gunsch, G. (2002). An examination of digital forensic models. *International Journal of Digital Evidence, 1*(3), 1–12.
36. Rogers, M., Goldman, J., Mislan, R., Wedge, T. & Debrota, S. (2006). Computer forensics field triage process model. *Conference on Digital Forensics, Security and Law* (pp. 27–40). Las Vegas, USA.
37. Rossi, M., & Sein, M. (2003). Design research workshop: A proactive research approach. *26th Information Systems Research Seminar in Scandinavia* (pp. 9–12). Haikko, Finland.
38. Rowlingson, R. (2004). A ten step process for forensic readiness. *International Journal of Digital Evidence, 2*(3), 1–28.
39. Selamat, S., Yusof, R., & Sahib, S. (2008). Mapping process of digital forensic investigation framework. *International Journal of Computer Science and Network Security, 8*(10), 163–169.
40. Sherman, S. (2006). A digital forensic practitioner's guide to giving evidence in a court of law. *Proceedings of the 4th Australian Digital Forensics Conference* (pp. 1–7). Perth Western, Australia.
41. Smith, R., Grabosky, P., & Urbas, G. (2011). *Cyber criminals on trial*. Cambridge: Cambridge University Press.
42. Stanfield, A. (2009). *Computer forensics, electronic discovery and electronic evidence*. Chatswood: LexisNexis Butterworths.
43. Takeda, H., Veerkamp, P., Tomiyama, T., & Yoshikawa, H. (1990). Modeling design processes. *AI Magazine, 11*(4), 37–48.
44. US-CERT. (2012). Computer forensics. U.S. Department of Homeland Security. Available at: https://www.us-cert.gov/security-publications/computer-forensics. Accessed 17 June 2016.
45. Venter, J. (2006). Process flow for cyber forensics training and operations. Available at: http://researchspace.csir.co.za/dspace/handle/10204/1073. Accessed 17 June 2015.
46. Valjarevic, A., & Venter, H. (2015). A comprehensive and harmonized digital forensic investigation process model. *Journal of Forensic Sciences, 60*(6), 1467–1483.
47. Walls, J., Widmeyer, G., & El Sawy, O. (1992). Building an information system design theory for vigilant EIS. *Information Systems Research, 3*(1), 36–59.
48. Watts, S., Shankaranarayanan, G., & Even, A. (2009). Data quality assessment in context: A cognitive perspective. *Decision Support Systems, 48*(1), 202–211.
49. Wieringa, R. (2009). Design science as nested problem solving. *4th International Conference on Design Science Research in Information Systems and Technology* (pp. 8–19). Philadelphia, USA.
50. International Organisation for Standardization. (2015). *ISO/IEC 27043:2015. Information technology–Security techniques–Incident investigation principles and processes*. Geneva: International Organization for Standardization.