A standardised data acquisition process model for digital forensic investigations

Reza Montasari

Department of Computing and Mathematics,
University of Derby,
Kedleston Road, Derby, DE22 1GB, UK
Email: r.montasari@derby.ac.uk

Abstract: Similar to traditional evidence, courts of law do not assume that digital evidence is reliable if there is no evidence of some empirical testing regarding the theories and techniques pertaining to its production. Courts take a careful notice of the way in which digital evidence has been acquired and stored. In contrast with traditional crimes for which there are well-established standards and procedures upon which courts can rely, there are no formal procedures or models for digital data acquisition to which courts of law can refer. A standardised data acquisition process model is needed to enable digital forensic investigators to follow a uniform approach, and to assist courts of law in determining the reliability of digital evidence presented to them. This paper proposes a model that is standardised in that it can enable digital forensic investigators in following a uniform approach, and that is generic in that it can be applied in both law enforcement and corporate investigations. To carry out the research presented in the paper, the design science research process (DSRP) methodology proposed by Peffers et al. (2006) has been followed.

Keywords: digital forensics; data acquisition; process model; standardised model; digital investigations; computer forensics; formal process.

Reference to this paper should be made as follows: Montasari, R. (2017) 'A standardised data acquisition process model for digital forensic investigations', *Int. J. Information and Computer Security*, Vol. 9, No. 3, pp.229–249.

Biographical notes: Reza Montasari is currently a PhD candidate in the Department of Computing and Mathematics at the University of Derby, UK. He received his MSc (with distinction) and BSc (with upper second class) from the University of South Wales (formerly known as the University of Glamorgan) in 2013 and 2012, respectively. His research interests include: digital investigations, steganography, steganalysis and multimedia computing.

1 Introduction

Nowadays, the nature of evidence presented in courts of law tends to be less likely paper-based considering the pervasive nature of information technology. Evidence of digital crime varies from that related to traditional crimes for which there are deep-rooted standards and procedures (Adams et al., 2014; Stanfield, 2009; Smith et al., 2009). There does not currently exists a standardised and generic process model for digital data

acquisition process that is widely accepted by digital forensic community and courts of law, and that can be applied in the different fields of digital forensic (Montasari et al., 2015; Valjarevic and Venter, 2015). The existing models have often been developed by digital forensic investigators (DFIs) based on their own personal experience on an ad hoc basis without consideration to establish standardisation within the field (Valjarevic and Venter, 2015). This has prevented the establishment of formal processes that are urgently needed by courts of law (Montasari et al., 2015; Adams et al., 2014).

In many cases, DFIs employ ad hoc tools (Adams et al., 2014; Bulbul et al., 2013; Agarwal et al., 2011; Ademu et al., 2011; Grobler et al., 2010; Ieong, 2006; Stanfield, 2009) to carry out digital data acquisition. The lack of a standardised data acquisition process model (SDAPM) is not an isolated flaw within the field of digital forensic science. Cohen (2009) states that the entire field of digital forensic still lacks agreements in fundamental areas. This might be due to the fact that digital forensic field is still a very new discipline. Many researchers are increasingly calling for scientific approaches and formal methods for describing the digital investigation processes (Cohen, 2012; Carlton and Worthley, 2009; Garfinkel et al., 2009; Pollitt, 2008; Leigland and Krings, 2004). The existing models often tend to focus on one area of digital forensic and neglect the other areas (Adams et al., 2014). This has hindered the development of a generic model that can be applied in both law enforcement and corporate investigations (Montasari et al., 2015). Therefore, the SDAPM was designed and developed in order to contribute towards addressing these shortcomings. The SDFIPM is formal in that it synthesises, harmonises and extends the existing models, and is generic in that it can be applied in the three fields of law enforcement, commerce and incident response. By implementing the SDAPM, this model will be of a great value to DFIs and courts of law. Moreover, as Adams et al. (2014) state, the development of such a model will establish a starting point from which other investigators and researchers in the field will be able to continue to advance the field's scientific credentials.

The remainder of the paper is structured as follows: Section 2 presents the research background. Section 3 provides the methodology employed to conduct the research presented in this paper. Section 4 proposes some planning activities that the investigators must perform prior to attending the crime scene, while Section 5 suggests some activities that the investigators must carry out to secure the crime scene prior to the data acquisition process. The proposed model is presented in Section 6, followed by the description of the FSDAPM's overriding principles in Section 7. A brief discussion on the evaluation of the model is presented in Section 8, and finally, the paper is concluded in Section 9.

2 Background

Prior to the design and development of the new model, all the prominent digital forensic investigation process models (DFIPMs) presented to date were critically reviewed and assessed to gain an in-depth insight into these models. The result of this review revealed a gap that there does not exist a SDAPM for digital forensic investigations that can be widely accepted by the digital forensic community and courts of the law. The previous models have often been criticised for being too specific (Carrier and Spafford, 2003; Reith et al., 2002), too high level (Beebe and Clark, 2005), too broad (Rogers, 2004), too technical (Venter, 2006) and too complex (Selamat et al., 2008). These models

are considered to be ad hoc tools as opposed to formal models (Adams et al., 2014; Bulbul et al., 2013; Agarwal et al., 2011; Ademu et al., 2011; Cohen, 2011, 2012; Turnbull; 2008; Trcek et al., 2010; Beebe and Clark, 2005; Ciardhuáin, 2004; Reith et al., 2002; Karyda and Mitrou, 2007; Baryamureeba and Florence, 2004). Presenting the review of these models is outside the scope of this paper. The reader, instead, is encouraged to refer to the paper in Montasari et al. (2015) to consult this review. However, in order to provide a background into the research presented in this paper, in the next two paragraphs, we draw upon a summary of the literature review conducted in Montasari
et al. (2015).

The main objective of a digital data acquisition process is to assist the investigators in explaining how particular digital evidence was found on a device (Kohn et al., 2013; Casey, 2011). Like any other types of evidence, courts of law do not assume that digital evidence is valid and reliable without some empirical testing in relation to theories and techniques associated with its production (Adams et al., 2014; Mason, 2007). Courts of law take a careful notice of the manner in which the digital evidence acquisition and storage were carried out (Cohen, 2011; Mason, 2007; Kessler, 2010). The concept of admissibility refers to the fact that the courts need to verify whether the digital evidence is sound to be placed before a jury and will help to deliver a solid base in terms of making a decision in the case (Casey, 2011). Courts in the UK and the USA require the investigators and 'proponent' of digital evidence to lay the proper foundation for its admissibility. They are concerned with the reliability and authenticity of such digital evidence (Casey, 2011; The Law Reform, 2009). If forensic investigators are not able to present their evidence in a coherent and understandable way to the layperson such as judge and jury, the case may be lost (Wiles, 2007). The complexity of methodologies and software used to extract digital evidence requires the digital investigator to explain the evidence in such a way that judge and jury understand it (Kessler, 2010).

Casey (2011) and Turnbull (2008) argue that while the actual mechanics of digital forensics are different from the better-known physical and medical forensics, the processes of all forensic sciences are fundamentally the same. Cohen (2011, 2012) states that judges need to keep out the poor-quality digital evidence from the courtroom. In the absence of something better, judicial systems might apply methods used to test scientific evidence into digital evidence presented before them (Kessler, 2010; Meyers and Rogers, 2004). The digital forensic discipline was developed without any initial research required for a thorough scientific ground essential for permitting digital forensic evidence (US-CERT, 2012; Yussoff et al., 2011; Carrier, 2002). Meyers and Rogers (2004) warned that digital forensics is branded as 'junk science' because of the absence of certifications, standards or peer-reviewed methods. Although this reference dates back to 2004, the issue of the lack of standardisation and consensus concerning digital data acquisition process still remain. This is pointed out by the latest reference such as Valjarevic and Venter (2015), Adams et al. (2014), Kohn et al. (2013), Cohen (2011, 2012), and Zainudin et al. (2011). In this regard, Beebe and Clark (2005) state that a more generally accepted framework is needed to enhance scientific rigor and to facilitate education, application and research. The United States Computer Emergency Readiness Team (US-CERT, 2012) asserts, "Because digital forensics is a new discipline, there is little

standardisation and consistency across the courts and industry". Zainudin et al. (2011) state that one of the most significant problems that digital investigators encounter is the absence of standardisation in the field of digital forensics. Karyda and Mitrou (2007) proclaim that utilising ad hoc methods and tools for the extraction of digital evidence can undermine the reliability and credibility of digital evidence.

Therefore, to address these shortcomings, we propose a SDAPM (Section 6) that deals with the data acquisition aspect of digital investigative process, as well as a set of proposed activities in relation to prior planning (Section 4) and securing the crime scene (Section 5) in advance of conducting the data acquisition process. Moreover, we also propose a set of overriding principles (Section 7) that DFIs will need to employ during the investigative process in order to maximise the chances of the admissibility of digital evidence in a court of law. The development of the SDAPM, accompanied by the proposed activities regarding the prior planning and securing the crime scene as well as the suggested set of the overriding principles, should both encourage and pave the way for other researchers to carry out further research into bringing the necessary formality and thoroughness also to other stages of digital forensic process such as examination or event reconstruction processes, etc.

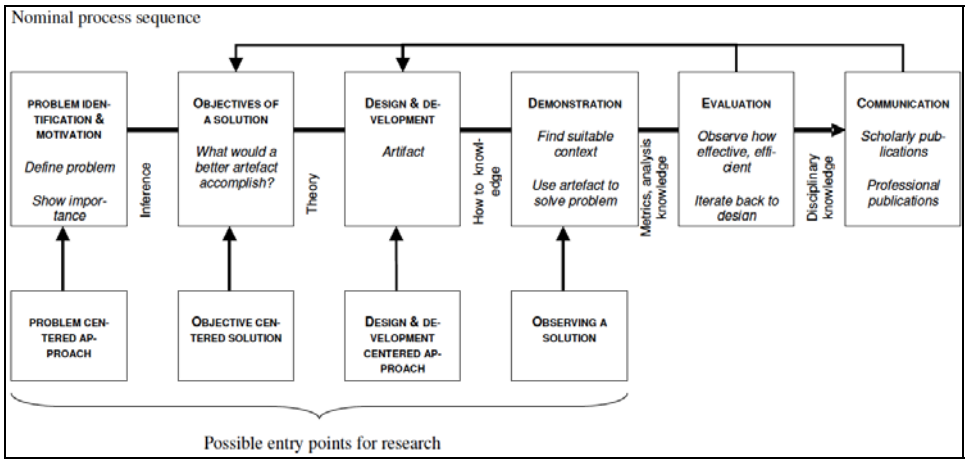
3 Research methodology

In order to create a consistent research environment and to carry out a successful research, various methodologies were considered. However, it was decided to utilise the design science research process (DSRP) by Peffers et al. (2006) over other alternatives due to the fact that it is especially suited for the task of designing and developing a new process model. Armstrong and Armstrong (2010) state that design science is an ideal approach in the problem domain of digital forensic evidence with its focus on designing solutions. The DSRP is related to the development and subsequent evaluation of IT artefacts within an organisational environment in order to solve specific problems. The artefacts in question can consist of models, constructs and methods (Hevner and Chatterjee, 2010). Peffers et al.'s (2006) DSRP consists of six activities as presented in Figure 1.

Problem identification and motivation involve defining the research problem to be addressed and justifying the value of the research. The objective of a solution requires the researchers to define the research aim and objectives while design and development involves creating the artifactual solution. Demonstration involves demonstrating the efficacy of the artefact in some appropriate environment to solve the stated problem, while evaluation requires observing and measuring how well the constructed artefact supports the solution to the stated problem. Finally, communication requires the researchers to communicate the problem and its significance, the artefact, its utility and novelty to other researcher via publications. The entry point for this research is the problem identification and motivation. Also, to represent the SDAPM in a formal manner, various visual and formal representations were considered including: unified modelling language (activity diagrams and use case diagrams) and finite state machines. However, it was decided to use UML activity diagrams due to the fact that the UML is a de-facto standard modelling language (Bogan and Dampier, 2005), the primary

purpose of which is visualisation (Ruan and Huebner, 2009). It is 'intentionally process-independent' making it suitable for modelling 'different processes' as well as analysing, designing and implementing artefacts such as models and systems (OMG, 2016).

Figure 1 DSRP model



Source: After Peffers et al. (2006)

4 Planning prior to securing the crime scene

Prior to raiding the suspect's place of work or residence (crime scene) to carry out the on-scene data acquisition, DFIs will need to embark upon a detailed planning. Such a planning can have a significant impact on the efficiency and success of on-scene data acquisition process. Regarding the pre-raid planning, Sammes and Jenkinson (2007) state that it is very important that the number of computers, their types, operating systems and connections are all known before entering the scene of crime (Sammes and Jenkinson, 2007). Although this might be valid to a large extent in an ideal world, the investigators often have little idea about the computer systems, quantity and location of data, types of hard disk or the operating systems involved, prior to visiting the crime scene. Also because the initial information concerning specific online environment might be scarce, insufficient or imprecise, the planning stage must therefore focus on preparing for as many likely scenarios as possible (Brown, 2009). Therefore, it would be unreasonable to expect the investigators to produce anything beyond a rough outline of a plan at this stage of investigation, a view supported by Adams et al. (2014).

Various considerations need to be made at the planning stage even though the investigators have little understanding of what they should expect. This includes: constructing the relevant procedures, defining methodologies, the choice of tools to be used, and planning for the use of appropriate human resources that should be involved in the data acquisition process. Since it is not feasible to develop specific planning tailored to every possible situation (Kent et al., 2006), the planning stage should therefore focus on generic activities so that it can be suitable for different investigations. Note that in

circumstances where the digital device has already been seized by the law enforcement officers and presented to a digital forensic laboratory (DFL) for examination, this process will become brief as it will not be necessary to preform many of the stated activities.

5 Securing the crime scene prior to data acquisition

Once the proper planning has been finalised, investigators will now need to attend the crime scene where the data representing potential digital evidence might be stored in a digital system. The first step that the investigators will need to undertake during this stage is to address safety issues in relation to personnel and witnesses as well as the material under investigation. In order to demonstrate in a court of law that the digital evidence was acquired in a forensically sound manner, first the investigators must be able to show that the crime scene from which the digital evidence was acquired was preserved unaltered. Thus, if possible and practicable, the investigators must enforce a lock down of the entire crime scene in order to achieve what Casey (2011) calls a 'pristine environment' to preserve the integrity of both digital device and the potential evidence contained in it. Other steps that the DFIs should take include preventing individuals from entering or leaving the crime scene, and preventing unauthorised people (including the suspect) from tampering with the digital device and materials under investigation. In terms of preserving the digital crime scene, this can include, but is not limited to, blocking the network connectivity. A computer system attached to a network that is running can be regarded as fragile evidence due to the fact that its data representing potential digital evidence could be deleted with commands from a remote system. Examples of procedures to preserve the content of computer in this situation are to unplug the computer from the network when it is found or utilise a network monitor to view what data is being sent to the system until the full investigation begins.

If the investigation is not covert and the suspect is at the crime scene, they must be detained and interviewed. Suspects often would be 'psychologically more vulnerable' within the first few hours of their initial encounter with the police (Black, 2014), particularly when this encounter takes place in their place of business or dwellings (Yeschke, 2002). Due to the shock that they have received, they often tend to be more compliant and open to answering the police questions even after they have been 'mirandised' (Rogers et al., 2006; Memon et al., 2003). At this stage into the investigation, what should be critical to the investigators is the knowledge of the full extent of the crime or involvement of the suspect and triggers that further increase the suspect's willingness to talk and cooperate. These triggers might originate in the digital evidence stored on the suspect's digital device such as e-mail correspondence, digital maps, pictures and chat logs, etc. It is very important that the investigators and interviewers who are dealing directly with the suspect provide direct input to the DFIs at this stage. This ensures that correct prioritisations and assumptions are being made in relation to the potential digital evidence identification and acquisition activities.

Once the crime scene has been securely preserved, the investigators attending the crime scene will need to conduct a preliminary survey of the physical crime scene to obtain an idea about how to process the physical crime scene and what kind of special skills are required. The aim of performing the preliminary survey must be:

1 to identify the 'obvious' pieces of physical evidence by walking around the crime scene (Casey, 2011)

2 to identify the 'fragile' pieces of physical evidence (Carrier and Spafford, 2003)

3 to identify any technical issue (Adams et al., 2014)

4 to survey the digital crime scene to identify data of interest that represents potential digital evidence

5 to determine the mixture of laboratory and onsite data acquisition

6 to develop an initial theory about the incident or crime.

Last but not least, it is extremely important to document all the activities carried out throughout this stage in order to enable other investigators to authenticate the process and results. Thus, it is imperative to maintain a detailed record of what was performed on the computer system and what information was acquired. Maintaining a detailed documentation will enable the investigators:

- to preserve the chain of custody in a forensically sound manner
- to increase the possibility of a successful investigation
- to record all information produced during this process to support decision making and the legal, administrative processing of those decisions.

Note that similar to the planning stage, this process might become irrelevant in circumstances where the digital device has already been seized and transported back to a DFL. In these situations, the investigators can simply skip this process without negatively affecting the results of the investigation.

6 The proposed model

6.1 Design and development considerations

The data acquisition process has a significant bearing on the entire digital investigation, and it is often challenged by the courts concerning infringements on the chain of custody (Kruse and Heiser, 2002), documentation (Valjarevic and Venter, 2015; Jones et al., 2006), the integrity of the evidence (Brown, 2009) and the methods and procedures utilised to acquire the digital evidence (Kessler, 2010). If the court doubts the initial collection and management of the digital evidence, the entire digital investigative process will be subject to dispute. One of the shortcomings of the previous models concerning their data acquisition process is due to the superficial level of details provided concerning this process. These models (Valjarevic and Venter, 2015; Adams et al., 2014; Kohn et al., 2013) often provide a high-level, single phase stating that the data needs to be collected without providing lower-level and useful details necessary to assist the DFIs in acquiring digital evidence in a forensically sound manner. Another limitation of the existing models related to the data acquisition process is the fact that they do not explicitly distinguish 'live' data acquisition from 'static (dead)' data acquisition where each activity requires a different set of components and procedures. Also, although there are some models that

refer to 'live acquisition' to some extent, they often tend to discuss the live acquisition of 'volatile data' without making any reference to the live acquisition of 'non-volatile data' which can be as important. Moreover, the authors of the existing models imply that the acquisition of digital evidence should be performed in an ideal environment such as a DFL. However, in many circumstances such an ideal environment is far from practice, for example, in cases of live acquisition where the authorisation does not permit the seizure of the system. Therefore, in order to address the stated shortcomings associated with the acquisition process, the following three considerations were made when designing and developing the proposed model, the SDAPM.

1 Static acquisition and live acquisition have been differentiated in the SDAPM; therefore, relevant and discrete components have been assigned to each process.

2 The SDAPM has further distinguished between a static data acquisition onsite and a static data acquisition in a DFL and has assigned discrete components to each aspect accordingly.

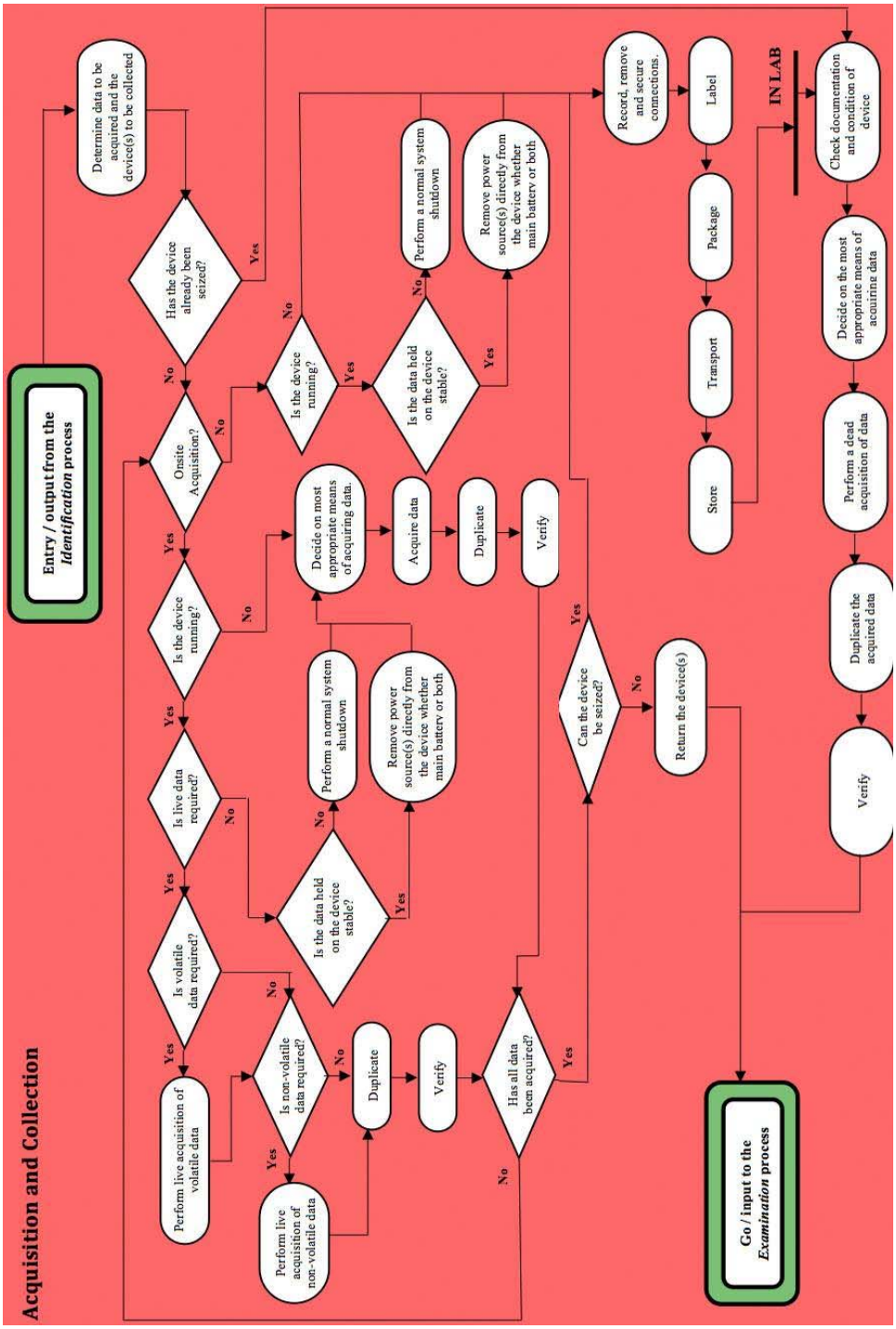
3 The live data acquisition process has been further broken down into both the live acquisition of volatile data and the live acquisition of non-volatile data. Therefore, relevant components have been assigned to each aspect accordingly.

Thus, in the SDAPM, the live acquisition pertains to the acquisition of both volatile and non-volatile data from a running device or a network, whereas the dead acquisition relates to the static acquisition of the data from a powered-off device onsite at the crime scene or in a DFL. It is contended that the SDAPM is the most systematic and detailed digital data acquisition process presented to date. It is also argued that the SDAPM has been developed in such a generic way that it could be applied in the different fields of digital forensic and employed for a large number of potential scenarios. The next section represents the UML activity diagram of the FSDAPM followed by the description of the model.

6.2 The FSDAPM representation and description

If it has been determined that the on-scene data acquisition is not needed and the data should be acquired in a DFL, the DFIs must then find out whether the device subject to the data acquisition is running or not. If the device is running, the DFIs must determine whether the data residing on the device is stable or not before powering it down. If the data residing on the device is stable, the DFIs will need to remove the power source directly from the device. However, if the data residing on the device is not stable, a normal shut down must be performed. In both cases where the device was running and then shut down or the device was already in powered-off state, the DFIs must ensure to record, remove, secure and label the connection for the device before packaging the device for transportation back to a DFL or a secure storage. It is essential for the DFIs also to collect any material which might be associated with the potential digital information. This material can include, but are not limited to, paper containing passwords, cradles and power connectors for embedded system devices, etc.

Figure 2 UML activity diagram of the acquisition process (see online version for colours)



The device will then need to be transported and stored in a secure facility for subsequent DFL data acquisition, examination and analysis. Preserving the integrity of the evidence and the chain of custody while the evidence is being kept in storage is of extreme importance (Montasari et al., 2015; Cohen, 2009; Reith et al., 2002). Prior to conducting the data acquisition in a DFL, the investigator assigned with this task must check the documentation and the condition of the device to ensure that the device has not been damaged due to factors such as shock, temperature, pollution, loss of power and malfunction, etc. In order to acquire the data, the investigator must then decide on the most appropriate means of acquiring data based on the standard operating procedures (SOPs) of the organisation within which the DFI operates as well as his own training, skills and experience. When selecting the most appropriate methods of data acquisition, DFIs should also consider the common practices suggested by ISO/IEC 27043 (2015), ISO/IEC 27037 (2012), ISO/IEC 29 10118-2 (2010), and ACPO (2003, 2012).

At all times, the DFIs must be able to justify their reasons for the selection of a particular method or tool over the other methods or tools. Only those data acquisition methods that can be reproducible or verifiable by different DFIs should be selected. The DFIs must perform the evidence acquisition in such a way that its integrity is preserved. This is especially important if the digital evidence is intended to be used at a later stage to draw formal conclusion in a report presented to a court of law. Therefore, the potential digital evidence must be acquired in the least intrusive manner in order to avoid altering or spoiling the evidence. In cases where the alteration to the digital data is unavoidable, the DFIs should document the activities performed to justify the alterations made to the digital data. Depending on the type and urgency of the investigation, the SDAPM suggests that the methods selected for the data acquisition should be based on the situation, cost and time in order to ensure an effective digital data acquisition process.

After deciding on the most appropriate methods of acquiring data, the investigator will need to acquire the master copy of the raw data representing the potential digital evidence by creating a verifiable image of all the bits and bytes contained within the digital device. A duplicate copy of the acquired data should also be created to become the working copy in order to preserve the master copy in case it is needed to make further copies at a later stage from the master copy. The original source and the digital evidence copies should then be verified with a proven function such as MD5 or SHA1. The hash value of both datasets must be exactly the same to ensure that the original data has not been modified. Verifying the extracted data as genuine attains legal validity (Kohn et al., 2013; Casey, 2011; Cohen, 2009). It should be noted that 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, the DFIs employing the SDAPM should preform a logical acquisition that targets only specific data types, directories or locations. Having performed data acquisition and image verification, the investigation moves on to the next stage of the investigative process, the examination process, being outside the scope of this paper, where digital forensic analysts take over to conduct the subsequent stages of the investigative process.

6.2.1 On-scene data acquisition process

If it has been determined that the on-scene data acquisition is required, the DFIs must then decide whether the device from which data is to be acquired is running or not. In turn, knowing the state of the device will determine whether the live data acquisition

should be conducted or not. If the device is not running, to acquire the data, the DFIs must undertake the same data acquisition steps as those described under the DFL data acquisition. The only difference would be that the static data acquisition must be performed onsite as opposed to offsite in a DFL. Similarly, if the authorisation permits for the device to be seized, the same procedures as described under DFL acquisition should be followed in relation to securing, labelling, packaging, transporting and storing the evidence, etc. In the SDAPM, the transportation of the digital evidence acquired on-scene can differ from that of the physical device described in the preceding section. As discussed, in cases where onsite data acquisition is not required, the physical device has to be transported physically to a secure location such as a DFL for subsequent data acquisition, examination and analysis. However, the digital evidence acquired onsite can be transported both physically and electronically. In cases where the digital evidence is to be transported electronically, the DFIs must take special precautions such as encrypting and digitally signing data in order to preserve the integrity and chain of custody.

If the device is running, the DFIs must determine whether live data acquisition is required or not. If live data acquisition is not needed, the DFIs must then follow the same procedures as described in the preceding section concerning powering down the device, acquiring and preserving the evidence, the transportation (both physically and digitally) and storage of the evidence. However, if live data acquisition is required, the DFIs must determine whether to carry out live data acquisition on volatile data, non-volatile data or both. Similar to the static data acquisition, the acquired data from the live acquisition of both volatile data and non-volatile data must be duplicated and verified using a proven function such as MD5 or SHA1. Regardless of the static or live data acquisition, the SDAPM also requires the DFIs to ensure that all the needed data representing potential digital evidence has been acquired. At the end of each on-scene data acquisition activity, the DFIs are presented with a condition, 'Has all the data been acquired?', to determine whether all the required data has been acquired or not. If all the data has been captured, the DFIs can proceed with the next activity. However, if all the data has not been acquired, the DFIs must perform all the previous steps until they ensure that whole required data has been acquired. After the DFIs have ensured that all the required data has been extracted, they must then determine whether the device containing the digital evidence can be seized or not in accordance with the authorisation. If the authorisation does not permit the seizure of the device, it will need to be returned to its rightful owner. However, if the authorisation allows the seizure of the device, the DFIs must then take the same steps described in the preceding section to proceed with seizing the device. At this point, the steps outlined in the SDAPM have been completed, and investigation moves to the next stage of the investigative process, the examination process, being outside the scope of this paper, where the DFAs initiate the subsequent stages of the investigative process.

7 SDAPM's overriding principles

As well as the formal UML representations of the SDAPM, a set of ten overriding principles have also been developed in order to enable DFIs to gather solid evidence that can be relied upon by the decision makers whether they are in a court room or board room. These overriding principles or actionable principles are objectives that need to be

achieved in a given digital forensic investigation. We argue that any approach for conducting the data acquisition process must preserve the reliability, completeness, accuracy and verifiability of digital evidence. Therefore, these overriding principles are proposed as a standard requirement for data acquisition process in digital investigations.

Since the SDAPM is aimed at the UK jurisdiction, the proposed principles discussed in this section have been based on ACPO Good Practice Guide (2003, 2012), ISO/IEC 27043 (2015), ISO/IEC 27037 (2012) and ISO/IEC 27035 (2011) standards, as well as other relevant scientific papers such as Valjarevic and Venter (2015), Beebe and Clark (2005), Ciardhuáin (2004) and Carrier and Spafford (2003). Due to their extreme importance, investigators who follow the SDAPM must maintain these principles when conducting the steps outlined in the SDAPM and in fact throughout the entire or parts of a digital investigative process. Each overriding principle is discussed next:

7.1 Interact with physical investigation

A digital investigation and a physical investigation are often interrelated and dependent on one another (Carrier and Spafford, 2003). In cases where a physical investigation requires an assistance from a digital investigation, an example could be to carry out a data acquisition process to extract digital evidence to reveal communication between terror suspects via computers, mobile phones, online social network activities, e-mail 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. Referring to the significance of interaction between physical and digital investigation, Valjarevic and Venter (2015) state that defining the relationship between a digital investigation and a physical investigation is important in order to preserve the chain of custody, preserve the integrity of the digital evidence, protect the digital evidence from damage and ensure an efficient investigation.

7.2 Obtain and adhere to an appropriate authorisation

The case officer in charge of the digital investigative process will need to obtain an appropriate authorisation prior to DFIs can start the data acquisition process. This will ensure that DFIs do not infringe on any legal rule or rights of the system owners, custodians, principals or users. Authorisation for investigations involving law enforcement often requires a search warrant or other legal approval that requires sufficient evidence or suspicion. For corporate incidents, search warrants are not usually required so long as the proper privacy policies are in place.

7.3 Perform risk assessment

DFIs will need to carry out a detailed and accurate risk assessment prior to conducting the data acquisition steps outlined in the SDAPM in order to deal with new challenges and threats. As part of this risk assessment, safety issues need to be addresses in relation to the safety of personnel, victims, witnesses, the equipment and material under data acquisition process at the crime scene.

7.4 Preserve digital and physical evidence

This principle involves the investigators securing the digital crime scene and preserving the digital evidence that could change. This could include, but is not limited to, isolating the system from the network, acquiring the volatile data that would be lost after the system is powered down, and detecting suspicious processes that are running on the system. During the data acquisition process, investigators who employ the SDAPM must investigate those users suspected of causing the incident who are logged into the system. Log files should be secured in case that they will be lost before the system is imaged. In order to preserve the digital crime scene, investigators will need to make a full forensic image backup of the system so that it can be examined and analysed at a later stage in a DFL. Investigators must note that a full forensic image of the system preserves the whole digital crime scene whereas copies that are system backups preserve only the allocated data within the digital crime scene.

Depending on the type of crime and authorisation, a critical system can be rebuilt after investigators have created a forensic image in order that it can be swiftly placed back online (Carrier and Spafford, 2003). In contrast, in other circumstances, the original hard disk must remain as physical evidence during the entire duration of the case. The state of the network can also be preserved by network monitors when they save network traffic. Handling digital evidence in a forensically sound manner is essential to preserving the integrity of the digital and physical evidence. Therefore, 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 SOPs or procedural workflows.

7.5 Maintain an accurate and detailed documentation

The aim of the documentation principle is to record all information applicable or produced during the data acquisition process to support decision making and the legal, administrative processing of those decisions. This overriding principle involves documenting both physical and digital crime scene. Documentation of the physical crime scene – where data acquisition process is carried out on a digital system suspected of containing potential digital evidence – involves creating sketches and making video of a physical crime scene. Documentation of digital crime scene involves the investigators properly documenting each item of digital evidence when it is discovered. Digital evidence can be in many abstraction layers (Carrier and Spafford, 2003) and therefore should be documented accordingly. As an example, the investigators will have to document files by utilising their full file name path, the clusters in the file system that they employ, and also the sectors on the disk that they use. In terms of a network, investigators will need to document the network data with the source and target addresses at different network layers. Due to its extreme importance, DFIs who employ the FSDAPM must adhere to this principle to preserve the chain of custody and increase the possibility of a forensically sound data acquisition process.

7.6 Maintain an accurate audit trail

From both forensic and legal standpoint, it is necessary for the DFIs to maintain an audit trail of all activities carried out on the digital evidence. This audit trail could be relied upon to assess the forensic soundness of the process by documenting that a copy of the extracted data has been acquired accurately. The audit trail must involve documenting how the data was acquired, how it was converted and what steps were followed to ensure that it is complete and accurate. Moreover, hash verifications (MD5 and SHA1) of the acquired data must be calculated, and these values must be documented for future comparisons to assist digital forensic analysts in verifying that the evidence has not been modified since it was acquired.

7.7 Maintain a restricted access control

This actionable principle refers to both limited acquisition of digital data as well as restricted viewing of the data. The data acquisition tools must support restricted viewings of results in order to increase their utility and limit privacy concerns. With the appropriate technology utilised, the data acquisition and examination tools could determine to provide a positive or negative sign that certain types of data are contained in the digital device. For instance, if the computer contains indecent images of children, the data acquisition tool could simply report that such contraband is likely to be present without actually showing the images or videos.

7.8 Preserve chain of custody

In order to preserve the chain of custody, investigators must adhere to all legal requirements and must properly document the steps outlined in the SDAPM in accordance with ACPO (2003, 2012). Chain of custody is of extreme importance especially in investigations involving the law enforcement. Cases where chain of custody has not been properly preserved can be easily challenged in courts of law and potentially rejected irrespective of the incriminating evidence. An example of preserving chain of custody is when evidence copies are required to be shared with other experts in other locations. This handling of evidence must be properly documented to preserve chain of custody.

7.9 Maintain an effective case management

This overriding principle applies to the role of managers such as case officers who often lead a team of investigators during the data acquisition process. When conducting the data acquisition steps outlined in the SDAPM, case officers will need to undertake certain tasks. These include, but are not limited to, determining the team members who should preform the data acquisition process, acquire and check the appropriate authorisations, guiding the DFIs in the right direction and creating an overall picture of the data acquisition process, etc.

7.10 Manage information flow

One of the major issues with the existing models is the lack of identifying information flow which could have a negative impact on the other actionable principles such as chain of custody. A defined information flow should exist between each given process in a digital investigation and between different stakeholders. Ciardhuáin (2004) states that information flow has to be defined for each type of investigation and emphasises the need to identify and describe information flows within a digital investigation process model so that they 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. Therefore, due to its importance, information flow principle must be managed concurrently throughout the entire data acquisition process.

8 Evaluation of the SDAPM

A model has 'utility' if it is practical, applicable and appropriate; this denotes that there must be an advantage to using the model. The model has 'usability' if it is easy to be employed in order to achieve its stated goal. An effective model should, therefore, have both 'utility' and 'usability'. If the model does not meet the two components of usability and utility, the question will then arise as to why it was developed in the first place. If the artefact is so difficult to use that its users are discouraged from employing it, then its value is greatly reduced and its advantages are lost. Thus, the artefact needs to be evaluated in order to determine whether it has achieved both 'utility' and 'usability'. To evaluate a process model, five questions will ultimately need to be answered (Wise et al., 2013; Cook and Skinner, 2005):

1 Is the model theoretical valid?

2 Is the model usable?

3 Does the model provide explanatory or guiding power for the user?

4 Has the model been built right?

5 Has the right model been built?

In relation to question 1 above, the validity of a process model derives from the extent to which it conforms to guiding principles, based on which the process is structured. Concerning question 2, the model has usability if its intended user community are able to apply it in real life situations to organise their activities to proceed through the process and produce the required results efficiently. In terms of question 3, the model has guiding power if it directs the process, suggests some sequences of activity and warns against the others. With regards to the questions 4, the model has been built right if it meets all the stated requirements levied upon it, and is internally complete, consistent, and accurate enough to fulfil its stated aim. Regarding question 5, a right model has been developed if its intended application is observed and confirmed by the experts. If the agreement is not

acquired, the model will then need to be amended in order to bring it closer with its intended application. In Sections 6 and 7, the theoretical foundation for the design and development of the new model was described (question 1); and the process of assessing whether the new model has achieved both 'utility' and 'usability' started (question 2). The guiding power of the new model emanates from the UML activity diagrams for different processes of the CDFIPM as well as the model's overriding principles (question 3).

However, the SDAPM also needed to be subjected to an independent evaluation of guiding power that also extends the activities of Sections 6 and 7 to establish whether the new model has both utility and usability. This evaluation was to determine whether the model had been developed right and whether the right model had been built (questions 4 and 5). Therefore, the evaluation of the CDFIPM is the subject of this Section and continues the Peffers et al.'s (2006) DSRP, that requires the artefact (such as a model) to be utilised to address the research problem. The method employed for the independent evaluation of the model was to acquire the feedback from the SDAPM's intended user community, i.e., law enforcement DFIs, legal practitioners and practitioners within the field of commerce. The SDAPM was evaluated as part of a larger model entitled CDFIPM that was presented to a number of experienced experts whose expertise in the field of digital forensics ranged from 15 to 20 years. The experts in question included DFIs operating within two high-tech crime units (HTCUs) of two different police forces within England and South Wales, as well as a judge in England and a Barrister in Wales. In the first instance, the experts who participated in the evaluation exercise were provided with the model accompanied by explanatory notes based on the descriptions of the model, as well as a set of eight questions that they would need to answer. The followings are the questions presented to the experts:

1 Please identify any aspects of the model that are not representative of the processes as carried out in your field of practice.

2 Please identify any aspects of the processes carried out in your field of practice that are not covered in this model.

3 Did you think that the model adequately represented the structure of investigations in your organisation?

4 Please describe which activities in the model most closely relate to your field of practice and your own experience.

5 Please describe what aspects, if any, of the model you felt could be improved.

6 In terms of the utility, please rate the model on the scale of 1 to 10 with 1 not being useful at all and 10 being the most useful.

7 In terms of the usability, please rate the model on the scale of 1 to 10 with 1 being very difficult to use and 10 being very easy to use.

8 Please provide any additional comments that you might have on the model below.

Once initial feedback was acquired from the experts, the feedback was then discussed with them in the form of 'focus group' as well as 'interview' formats. According to Ciardhuáin (2004), this approach that we took to validate the SDAPM has various advantages as follows:

- The questionnaire, interview and focus group format 'take full advantage' of the experience and skills of those participating by being more open than 'a narrowly-focused survey'.
- Experts have a stronger understanding of the subject matter due to the fact that they can ask questions concerning the research than simply replying to a fixed set of questions.
- Participants are able to express and discuss views that are very likely not to be identified by a simple survey. Such issues can be analysed at once in some detail.

The initial feedback and subsequent comments expressed during the focus groups and interviews were very positive and these were noted down. The followings are only a few of the views expressed by the experts in relation to the model:

Comment 1 Much of your model covers most aspects in good detail of what is required, but the order would change or be adapted according to our operational needs.

Comment 2 I can see a lot of work has been put into this model, and you have covered everything I can think of, my only comment would be enabling your model to be interactive rather than a set of procedure.

Comment 3 This is a sound model for forensics service providers (FSP).

Comment 4 The model has captured in detail the various activities that are employed when conducting data acquisition. However, in most cases we do not perform on-scene live data acquisition; we simply transport the computer systems to our lab for data acquisition.

Comment 5 As a non-technical person, the model enables me to understand the processes followed. Based on the description of your model and my previous experience of other tools and guidelines, you have identified the relevant problems with the existing DFIPMs and have provided adequate analysis.

In relation to comment 4 above expressed by a law enforcement DFI, this view is invalid as in some cases where mission-critical systems (such as servers in the hospitals) are involved, the authorisation is very unlikely to allow the seizure and transportation of these systems back to a DFL for data acquisition. In these circumstances, an on-scene live data acquisition would be required. Therefore, the view expressed in comment four might be explained by the fact that in most cases involving law enforcement investigations, the law enforcement officers often deal with standalone hard drives containing indecent images of children that need to be seized and transported back to their laboratory for offsite data acquisition and subsequent examination and analysis processes.

9 Conclusions and future work

The fundamental issue that this paper addressed was the fact that there was not a SDAPM that was formal in that it enabled the DFIs in following a uniform approach, and that was generic in that it could be applied in both law enforcement and corporate investigations.

The SDAPM that was proposed in this paper is a step forward towards addressing the identified issue. The SDAPM was presented and described utilising a proven formal notation, unified modelling language activity diagram, that can assist courts of law in properly understanding the processes followed to acquire evidence from digital sources. Due to its overriding principles, it is argued that the SDAPM observes the forensic principles of minimising the contamination of the original crime scene and evidence, preserving the integrity of digital evidence, preserving the chain of custody of evidence and adhering to the rules of evidence for admissibility in courts of law. Moreover, the SDAPM is in accordance with recommended best practice as detailed in ISO/IEC 27043 (2015), ISO/IEC 27037 (2012) and ACPO (2003, 2012). Although the SDAPM presented in this paper has been primarily focused on the UK jurisdiction, it could be utilised as the foundation of a process model that is relevant in other jurisdictions with only slight modifications.

In terms of the future work, it is acknowledged that some limitations of the work remain. Although the SDAPM has already been evaluated by the HTCUs of two different police forces within the UK as well as judiciary personnel, this cannot be representative of all the law enforcement HTCUs and judiciary personnel within the intended user community of this research. Moreover, the model will also need to be subjected to an independent evaluation by digital forensic practitioners operating within the field of commerce. Therefore, the future work should include a more comprehensive trial by DFIs as part of a wider study. The future work could also involve the extension of the SDAPM to cover other stages of the digital investigative process such as the examination, analysis and event reconstruction processes, etc.

References

Adams, R., Hobbs, V. and Mann, G. (2014) 'The advanced data acquisition model (ADAM): a process model for digital forensic practice', *Journal of Digital Forensics, Security and Law*, Vol. 8, No. 4, pp.25–48.

Ademu, I., Imafidon, C. and Preston, D. (2011) 'A new approach of digital forensic model for digital forensic investigation', *International Journal of Advanced Computer Science and Applications*, Vol. 2, No. 12, pp.175–178.

Agarwal, A., Gupta, M., Gupta, S. and Gupta, C. (2011) 'Systematic digital forensic investigation model', *International Journal of Computer Science and Security*, Vol. 5, No. 1, pp.118–130.

Armstrong, C. and Armstrong, H. (2010) 'Modeling forensic evidence systems using design science', Paper presented at the *IFIP WG 8.2/8.6 International Working Conference*, Perth, Western Australia.

Association of Chief Police Officers (ACPO) (2003) *Good Practice Guide for Computer-Based Evidence*, London, UK.

Association of Chief Police Officers (ACPO) (2012) *Good Practice Guide for Computer-Based Evidence*, London, UK.

Baryamureeba, V. and Florence, T. (2004) 'The enhanced digital investigation process model', *Proceedings of the Fourth Digital Forensic Research Workshop*.

Beebe, N. and Clark, J. (2005) 'A hierarchical, objectives-based framework for the digital investigations process', *Digital Investigation*, Vol. 2, No. 2, pp.147–167.

Black, I. (2014) *The Art of Investigative Interviewing*, 3rd ed., Butterworth Heinemann, Boston.

Bogan, A.C. and Dampier, D.A. (2005) 'Unifying computer forensic modeling approaches: a software engineering approach', Paper presented at the *Proceedings of the First International Workshop on Systematic Approaches to Digital Forensic Engineering*, Taipei, Taiwan.

Brown, C. (2009) *Computer Evidence: Collection and Preservation*, 2nd ed., Course Technology, Boston.

Bulbul, H., Yavuzcan, H. and Ozel, M (2013) 'Digital forensics: an analytical crime scene procedure model (ACSPM)', *Forensic Science International*, Vol. 233, No. 1, pp.244–256.

Carlton, H. and Worthley, R. (2009) 'An evaluation of agreement and conflict among computer forensic experts', *42nd Hawaii International Conference on System Sciences (HICSS)*, IEEE, Hawaii, 5–8 January.

Carrier, B. (2002) 'Open source digital forensic tools: the legal argument' [online] http://www.digital-evidence.org/papers/opensrc_legal.pdf (accessed 6 January 2014).

Carrier, B. and Spafford, E. (2003) 'Getting physical with the digital investigation process', *International Journal of Digital Evidence*, Vol. 2, No. 2, pp.1–20.

Casey, E. (2011) *Digital Evidence and Computer Crime Forensic Science, Computers and the Internet*, 3rd ed., Elsevier, California.

Ciardhuáin, O. (2004) 'An extended model of cybercrime investigations', *International Journal of Digital Evidence*, Vol. 3, No. 1, pp.1–22.

Cohen, F. (2009) *Digital Forensic Evidence Examination*, 2nd ed., Fred Cohen & Associates, California.

Cohen, F. (2011) 'Putting the science in digital forensics', *Journal of Digital Forensics, Security and Law*, Vol. 6, No. 1, pp.7–14.

Cohen, F. (2012) 'Update on the state of the science of digital evidence examination', *Proceedings of the Conference on Digital Forensics, Security & Law*, pp.7–18.

Cook, D. and Skinner, J. (2005) 'How to perform credible verification, validation, and accreditation for modeling and simulation', *The Journal of Defense Software Engineering*, Vol. 18, No. 5, pp.20–24.

Garfinkel, S., Farrell, P., Roussev, V. and Dinolt, G (2009) 'Bringing science to digital forensics with standardized forensic corpora', *Digital Investigation*, Vol. 6, pp.S2–S11.

Grobler, C.P., Louwrens, C.P. and von Solms, S.H. (2010) 'A multi-component view of digital forensics', *ARES'10 International Conference on Availability, Reliability, and Security*, IEEE.

Hevner, A. and Chatterjee, S. (2010) *Design Science Research in Information Systems*, Springer, USA.

Ieong, R.S.C. (2006) 'FORZA – digital forensics investigation framework that incorporate legal issues', *Digital Investigation*, Vol. 3, pp.29–36.

ISO/IEC 27035 (2011) *ISO/IEC 27035: Information Security Incident Management*, British Standards Institution, London.

ISO/IEC 27037 (2012) *Guidelines for Identification, Collection, Acquisition, and Preservation of Digital Evidence*, CD 27037: ISO/IEC, Geneva, Switzerland.

ISO/IEC 27043 (2015) *Incident Investigation Principles and Processes*, Geneva, Switzerland.

ISO/IEC 29 10118-2 (2010) *Hash Functions*, Geneva, Switzerland.

Jones, K.J., Bejtlich, R. and Rose, C.W. (2006) *Real Digital Forensics*, Addison-Wesley, Boston, USA.

Karyda, M. and Mitrou, L. (2007) 'Internet forensics: legal and technical issues', *2nd International Workshop on Digital Forensics and Incident Analysis*, Samos, Greece, pp.3–12.

Kent, K., Chevalier, S., Grance, T. and Dang, H. (2006) *Guide to Integrating Forensic Techniques into Incident Response*, NIST Special Publication, 800-86.

Kessler, C. (2010) *Judges' Awareness, Understanding, and Application of Digital Evidence*, PhD thesis, Nova Southeastern University.

Kohn, M., Eloff, M. and Eloff, J. (2013) 'Integrated digital forensic process model', *Computers and Security*, Vol. 38, pp.103–115.

Kruse, W. and Heiser, J. (2002) *Computer forensics: Incident Response Essentials*, Addison Wesley, Boston, USA.

Leigland, L. and Krings, A. (2004) 'A formalization of digital forensics', *International Journal of Digital Evidence*, Vol. 3, No. 2, pp.1–32.

Mason, S. (2007) *Electronic Evidence: Disclosure, Discovery & Admissibility*, LexisNexis Butterworths, London.

Memon, A., Vrij, A. and Bull, R. (2003) *Psychology and Law: Truthfulness, Accuracy and Credibility*, John Wiley & Sons, West Sussex.

Meyers, M. and Rogers, M. (2004) 'Computer forensics: the need for standardization and certification', *International Journal of Digital Evidence*, Vol. 3, No. 2.

Montasari, R., Peltola, P. and Evans, D. (2015) 'Integrated computer forensics investigation process model (ICFIPM) for computer crime investigations', *Proceedings of 10th International Conference on Global Security, Safety and Sustainability*, pp.83–95.

OMG (2016) *Unified Modeling Language (UML)* [online] http://www.omg.org/spec/UML/ (accessed 8 March 2016)

Peffers, K., Tuunanen, T., Gengler, C., Rossi, M., Hui, W., Virtanen, V. and Bragge, J. (2006) 'The design science research process: a model for producing and presenting information systems research', *The First International Conference on Design Science Research in Information Systems and Technology*, pp.83–106.

Pollitt, M. (2008) 'Applying traditional forensic taxonomy to digital forensics', *Advances in Digital Forensics IV*, Springer, USA, pp.17–26.

Reith, M., Carr, C. and Gunsch, G. (2002) 'An examination of digital forensic models', *International Journal of Digital Evidence*, Vol. 1, No. 3, pp.1–12.

Rogers, M. (2004) *DCSA: A Practical Approach to Digital Crime Scene Analysis*, 5th ed., Vol. 3, West Lafayette, Purdue University, USA.

Rogers, M., Goldman, J., Mislan, R., Debrota, S. and Wedge, T. (2006) 'Computer forensics field triage process model', *Conference on Digital Forensics, Security and Law*, pp.1–14.

Ruan, C. and Huebner, E. (2009) 'Formalizing computer forensics process with UML', *Information Systems: Modeling, Development, and Integration*, pp.184–189, Springer, Berlin, Heidelberg.

Sammes, T. and Jenkinson, B. (2007) *Forensic Computing: A Practitioner's Guide*, 2nd ed., Springer, London.

Selamat, S., Yusof, R. and Sahib, S. (2008) 'Mapping process of digital forensic investigation framework', *International Journal of Computer Science and Network Security*, Vol. 8, No. 10, pp 163–169.

Smith, R., Grabosky, P. and Urbas, G. (2009) *Cyber Criminals on Trial*, Cambridge University Press, Cambridge.

Stanfield, A. (2009) *Computer Forensics, Electronic Discovery and Electronic Evidence*, LexisNexis Butterworths, Chatswood.

The Law Reform (2009) *The Admissibility of Expert Evidence in Criminal Proceedings in England and Wales* [online] http://lawcommission.justice.gov.uk/docs/cp190_Expert_Evidence_Consultation.pdf (accessed 7 March 2016).

Trcek, D., Abie, H., Skomedal, A. and Starc, I. (2010) 'Advanced framework for digital forensic technologies and procedures', *Journal of Forensic Sciences*, Vol. 55, No. 6, pp.1471–1479.

Turnbull, B. (2008) 'The adaptability of electronic evidence acquisition guides for new technologies', *Proceedings of the 1st International Conference on Forensic Applications and Techniques in Telecommunications, Information and Multimedia and Workshop*.

United States Computer Emergency Readiness Team (US-CERT) (2012) *Computer Forensics* [online] https://www.us-cert.gov/sites/default/files/publications/forensics.pdf (accessed 7 March 2016).

Valjarevic, A. and Venter, H. (2015) 'A comprehensive and harmonized digital forensic investigation process model', *Journal of Forensic Sciences*, Vol. 60, No. 6, pp.1467–1483.

Venter, J. (2006) *Process Flow for Cyber Forensics Training and Operations* [online] http://researchspace.csir.co.za/dspace/handle/10204/1073 (accessed 29 June 2015).

Wiles, J. (Ed.) (2007) *The Best Damn Cybercrime and Digital Investigations Book Period*, Syngress, USA.

Wise, J., Hopkin, D. and Stager, P. (2013) *Verification and Validation of Complex Systems: Human Factors Issues*, Springer-Verlag, Berlin.

Yeschke, C. (2002) *The Art of Investigative Interviewing: A Human Approach to Testimonial Evidence*, 2nd ed., Butterworth Heinemann, Boston.

Yussoff, Y., Roslan I. and Zainuddin, H. (2011) 'Common phases of computer forensics investigation models', *International Journal of Computer Science & Information Technology*, Vol. 3, No. 3, pp.17–31.

Zainudin, N., Merabti, M. and Liwellyn-Jones, D. (2011) 'Online social networks as supporting evidence: a digital forensic investigation model and its application design', *International Conference on Research and Innovation in Information Systems (ICRIIS)*, Kuala Lumpur, IEEE, 23–24 November, pp.1–6.