View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by NECTAR

The Standardised Digital Forensic Investigation Process Model (SDFIPM)

Reza Montasari[1], Richard Hill[2], Victoria Carpenter[3],
Amin Hosseinian-Far[4]

Abstract The field of digital forensics still lacks formal process models that courts can employ to determine the reliability of the process followed in a digital investigation. The existing models have often been developed by digital forensic practitioners, based on their own personal experience and on an ad-hoc basis, without

[1] Reza Montasari
Department of Computer Science
School of Computing and Engineering
The University of Huddersfield
Queensgate
Huddersfield
HD1 3DH
Email: R. Montasari@hud.ac.uk

[2] Richard Hill
Department of Computer Science
School of Computing and Engineering
The University of Huddersfield
Queensgate
Huddersfield
HD1 3DH
Email: R.Hill@hud.ac.uk

[3] Victoria Carpenter
Research Development Innovation and Enterprise Services
University of Bedfordshire
Luton
LU1 3JU
Email: Victoria.Carpenter@beds.ac.uk

[4] Amin Hosseinian-Far
Faculty of Business and Law
University of Northampton
NN1 5PH
Email: Amin.Hosseinian-Far@northampton.ac.uk

attention to the establishment of standardisation within the field. This has prevented the institution of the formal processes that are urgently required. Moreover, as digital forensic investigators often operate within different fields of law enforcement, commerce and incident response, the existing models have often tended to focus on one particular field and have failed to consider all the environments. This has hindered the development of a generic model that can be applied in all the three stated fields of digital forensics. To address these shortcomings, this paper makes a novel contribution by proposing the Advanced Investigative Process Model (the SDFIPM) for Conducting Digital Forensic Investigations, encompassing the 'middle part' of the digital investigative process, which is formal in that it synthesizes, harmonises and extends the existing models, and which is generic in that it can be applied in the three fields of law enforcement, commerce and incident response.

1. Introduction

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 [1, 2]. 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 [3]. Such tools and methodologies must also adhere to some standards of practice and be accepted by other investigators operating in the field [3, 4, 5]. Nevertheless, the field of digital forensics still lacks both consensus and formal process models that the courts can employ to determine the reliability of the digital evidence presented to them [2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18]. The absence of agreements associated with DFIPMs has been widely acknowledged also by other researchers [6, 7, 8, 9, 10], [14, 15, 16], [18, 19]. Zainudin et al. [20] state that one of the most significant problems encountered by digital forensic investigators is the absence of standardisation in the field of digital forensics.

Casey [21] argues that the development of a formal process model enables a complete, rigorous investigation, ensures proper evidence handling and reduces the chances of mistakes created by preconceived theories, time pressures, and other potential pitfalls [21]. Similarly, Valjarevic and Venter [15] state that conducting a digital forensic investigation requires a formalized process model, arguing, "There is currently neither an international standard nor does a global, harmonized DFI process (DFIP) exist". Authors in [14] and [15] suggest the concept of a widely agreed-upon process model to harmonise the practice of digital forensics. However, despite many calls to bring formalisation to DFIPMs, a solution has not yet been provided [6, 7], [9, 10], [12], [14, 15, 16], [23]. Many researchers acknowledge the

limited progress, if any, in defining and improving a formal digital forensic process since the DFRWS held in 2001 [9, 10], [14], [18], [22], [24, 25].

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 [15]. This has prevented the establishment of formal processes that are urgently needed by courts of law [9], [14]. In many cases, DFIs employ ad hoc tools [18], [26, 27, 28, 29] to carry out digital investigations. Therefore, many researchers are increasingly calling for scientific approaches and formal methods for describing the digital investigation processes [23], [30, 31, 32, 33]. Furthermore, the existing models often tend to focus on one area of digital forensics and neglect the other areas. This has hindered the development of a generic model that can be applied in both law enforcement and corporate investigations [6], [9, 10]. The adoption of ad-hoc approaches in developing previous models has led to a variety of process models with conflicting stages, activities and terminology, which in turn has prevented the establishment of the formal processes urgently needed by courts and investigators alike [14], [18].

1.1 Research Problem and Contributions

The foregoing considerations lead to the following research problem:

> *There does not exist a comprehensive model encompassing the entire digital investigative process that is formal, such that it can assist a court of law in determining the reliability of the investigative process followed, and that is generic, in that it can be applied in the different fields of law enforcement, commerce and incident response.*

Therefore, the SDFIPM was designed and developed as the middle part (i.e. the Investigative Processes Class) of a larger, comprehensive model, the Comprehensive Digital Forensic Investigation Process Model for Digital Forensic Practice, presented in [9], in order to contribute towards addressing the aforementioned 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. Moreover, we also propose a set of overriding principles included in the model 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. By implementing the SDFIPM and its Overriding Principles, this model will be of a great value to both DFIs and courts of law alike.

Note that in the context of this research study, the term 'formal' is not equivalent to the same term employed in the domains of Mathematics and Computer Science, in which the word 'formal' is used to refer to a set of strings of symbols that might be constrained by rules that are specific to it. In contrast, for the purposes of this study, the term 'formal' has been employed to refer to the UML Activity Diagrams, scientific methods, standards of practice, consistency, structure, agreed-upon components and terminology, harmonisation, and the unified approach that have been brought to the proposed model, the SDFIPM.

1.2 Authors' Note

Prior to the design and development of the CDFIPM [9], of which the SDFIPM is the middle part of, all the prominent digital forensic investigation process models (DFIPMs) presented to date were critically reviewed. These models were then assessed against three different sets of assessment criteria, including: the Daubert Test [34] Five-Point Requirement, Carrier and Spafford [35] Five-Point Requirement and Beebe and Clark [36] Four-Point Requirement. The aim of this critical review was to gain an in-depth insight into these models and identify which could contribute to our proposed model. Since law enforcement, commerce and incident response were the three environments on which this study focused, the existing models within those three domains which most closely met the assessment criteria were considered for their possible contributions to the new model. Such an approach is considered important by other researchers [16], [23], [37] as any model institutionalized through subsequent intellectual discourse and practical use must take into account other researchers' perspectives, approaches and "vernacular".

In order to assess the previous models against the three sets of assessment criteria, each model was given three sets of scores in accordance with the three sets of assessment criteria. Models were scored according to how many of the requirements were met for each particular set of criteria. This method of assessing the previous DFIPMs against 'three' different criteria is another novel contribution of this research in the field of digital forensic science. It should be noted that Carrier and Spafford's [35] five-point requirements have also been used by Beebe and Clark [36], against which they assess their own model (even though they do not provide scores). Likewise, Adams [4] uses both Carrier and Spafford's [35] five-point requirements as well as the Daubert Test's five-point requirements against which he evaluates the previous DFIPMs. However, we have built upon the previous initiatives in five different ways. First, we included Beebe and Clark's [36] four-point requirements, which to our best knowledge have not been previously used by any other researchers as an assessment method against which the exiting DFIPMs are evaluated. Second, we have approached the review and assessment of the previous

models differently. For instance, the scores that we have given each model based on the three sets of assessment criteria might be completely different from those given by Adams [4] based on the two sets of assessment criteria they have used. Third, contrary to Adams questioning the reliability of the Daubert Test in assessing the previous models, we have demonstrated that the Daubert Test is in fact effective in judging the previous DFIPMs. Fourth, we have analysed the most up-to-date models (in addition to the older ones) up to 2014 including Adam's own model presented both in [4] and [38]. Fifth, we have assessed our own model, the CDFIPM, the evaluation of which will be presented in an upcoming study, against the three sets of assessment criteria.

The results of our critical review of the previous DFIPMs have been presented in our previous studies such as in [6], [9], [13, 14]. Therefore, since this research paper builds upon our previous studies, we have borrowed some information in the Introduction and Background Sections of this paper from those studies, with references being made to those past studies.

1.3 Structure of the Paper

The remainder of the paper is structured as follows: Section 2 presents the research background. Section 3 presents the literature review while Section 4 provides the methodology employed to conduct the research presented in this paper. The proposed model is presented in Section 5, followed by the description of the SDFIPM's overriding principles in Section 5. Finally, the paper is concluded in Section 6.

3. Literature Review

Based upon our notes in the sub-section 1.2, this section provides a short summary in relation to our critical review of the previous DFIPMs. As Table 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.

Table 1. The comparative summary of the existing DFIPMs

The Comparative Summary of the 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											✓									
To be continued …																				

The Comparative Summary of the 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)
Examine Browsing Activities									✓		✓									
Case Specifics											✓									
Carry Out Preliminary Survey																				✓
Documentation of Scene				✓		✓		✓									✓	✓		✓
Update Outline Plan																	✓			✓
Search				✓	✓	✓	✓	✓		✓							✓		✓	
Survey				✓	✓		✓	✓									✓			
Identification	✓					✓		✓	✓	✓					✓		✓	✓		
Preservation	✓		✓	✓	✓		✓	✓							✓	✓	✓		✓	
Collection	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓		✓	✓	✓	✓	✓	✓
Volatile Evidence Collection									✓			✓					✓			
Non-Volatile Evidence Collection									✓			✓								
Authenticate																			✓	
Seizure								✓											✓	✓
Package																	✓			✓
Transport						✓				✓					✓		✓	✓	✓	✓
Storage						✓				✓					✓		✓	✓	✓	✓
Examination	✓		✓	✓		✓		✓	✓	✓			✓		✓		✓		✓	
Harvest								✓				✓							✓	
Reduce								✓				✓							✓	
Identify				✓															✓	
Classify																			✓	
Organise												✓							✓	
Compare																			✓	
Analysis	✓		✓	✓				✓	✓	✓			✓		✓	✓	✓	✓	✓	
Attribute															✓				✓	
Evaluate																			✓	

To be continued

The Comparative Summary of the 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)
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																				

The result of this review revealed a gap that there does not exist a comprehensive model 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 [35], [39] too high level [36], too broad [19], too technical [40] and too complex [41]. These models are considered to be ad hoc tools as opposed to formal models [18], [22, 23, 24], [26], [36], [39], [42, 43, 44, 45].

Presenting the review and assessment of these models is outside the scope of this paper. The reader, instead, is encouraged to refer to the studies presented in [6], [9, 10, 11], [13, 14] to consult this review.

As shown in the next table (Table 2), assessing the previous models against the Beebe and Clark [36] criteria reveal that there are five models that meet three of the four criteria, while six and five models fulfil two and one out of the four criteria respectively. There are also three models that meet no criteria, while there is one model to which the assessment criteria are not applicable. Similarly, comparing the previous models against the Carrier and Spafford [35] criteria reveals that there is one model that fulfils all the five criteria, while there are four other models that meet four of the criteria. There are also four, seven and three models that meet three, two and one out of the five criteria respectively, while there is one model to which the assessment criteria are not applicable. In relation to the Daubert Test [34], there are two models that fulfil four and three of the five criteria respectively, while three models meet two of the criteria. There are also twelve and two models that meet one and no criteria respectively, while there is one model to which the assessment criteria are not applicable.

Table 1. Scores obtained by the previous models based on the three assessment criteria

Models	Scores		
	Beebe and Clark	**Carrier and Spafford**	**Daubert Test**
A Framework for Digital Forensic Science (Palmer, 2001)	2	2	1
Electronic Crime Scene Investigation: A Guide for First Responders (Ashcroft, 2001)	1	2	0
Abstract Digital Forensic Model (Reith et al., 2002)	2	4	1
Integrated Digital Investigation Process (Carrier and Spafford, 2003)	3	4	2
Digital Crime Scene Analysis (Rogers, 2004)	3	4	2
Enhanced Digital Investigation Process Model (Baryamureeba and Tushabe, 2004)	0	1	1
An Extended Model of Cybercrime Investigation (Ciardhuáin, 2004)	3	5	3
Hierarchical, Objectives Based Framework for the Digital Investigation Process (Beebe and Clark, 2005)	3	3	2
Four Step Forensic Process (Kent et al., 2006)	2	3	0
Computer Forensics Field Triage Process Model (Rogers et al, 2006)	3	4	4
Framework for a Digital Forensic Investigation (Kohn et al., 2006)	2	3	1
A Common Process Model for Incident Response and Computer Forensics (Freiling and Schwittay, 2007)	0	2	1
Two Dimensional Evidence Reliability Amplification Process Model (Khatir et al., 2008)	1	1	1
Mapping Process of Digital Forensic Investigation Framework (Selamat et al., 2008)	0	1	1
Digital Forensic Process Model (Cohen, 2009)	2	2	1
Generic Computer Forensics Investigation Model (Yusoff et al., 2011)	N/A	N/A	N/A
Systematic Digital Forensic Investigation Model (Agarwal et al., 2011)	1	2	1
Harmonised Digital Forensic Investigation Process Model (Valjarevic and Venter, 2012)	1	2	1
Integrated Digital Forensic Process Model (Kohn et al., 2013)	2	2	1
The Advanced Data Acquisition Process Model (Adams et al., 2014)	2	3	2

Analysing the results of the Beebe and Clark [36], Carrier and Spafford [35] and the Daubert Test [34] criteria applied to each of the models identified those that include the components suggested by the three aforementioned criteria as necessary for a DFIPM. In total, there were eight models that were selected for their possible contributions to the CDFIPM based on their high scores achieved in relation to meeting the three sets of the assessment criteria.

3. Overview of the Investigative Process Model

The SDFIPM, which is considered to be a "class" and the middle part of the larger model CDFIPM (presented in its entirety in our upcoming study, has been designed using a top-down approach in order to enable digital forensic investigators to gain a better insight into its compositional components, namely Processes, Phases, Sub-Phases and Overriding Principles. There are 7 processes contained within the SDFIPM, each of which contains a different number of Phases. Apart the Overriding Principles, i.e. Concurrent Processes, which do not provide lower-level details, the remainder of the Processes provide additional lower layers of details, i.e. Phases and Sub-Phases. The SDFIPM will be initially presented in its abstract level, prior to being refined with more details that make up the model's lowest-level structure. Figure 1 represents the first instance of the formal representation of the SDFIPM in its abstract level, containing the first layers of the SDFIPM, namely Processes. Following this abstract representation, each process of the SDFIPM, containing second and third layer details, i.e. Phases and Sub-Phases, will then be represented by a UML Activity Diagram. The combination of all UML Activity Diagrams depicted in Figures 2-8 makes up the entire SDFIPM. Each Process will be subsequently discussed under their associated main headings.

Notice that this version of the SDFIPM's formal representation (Figure 1 and Figures 2-8) as well as its Overriding Principles presented in this paper are prior to their submission to the external reviewers for evaluation and feedback presented and discussed in our upcoming paper.

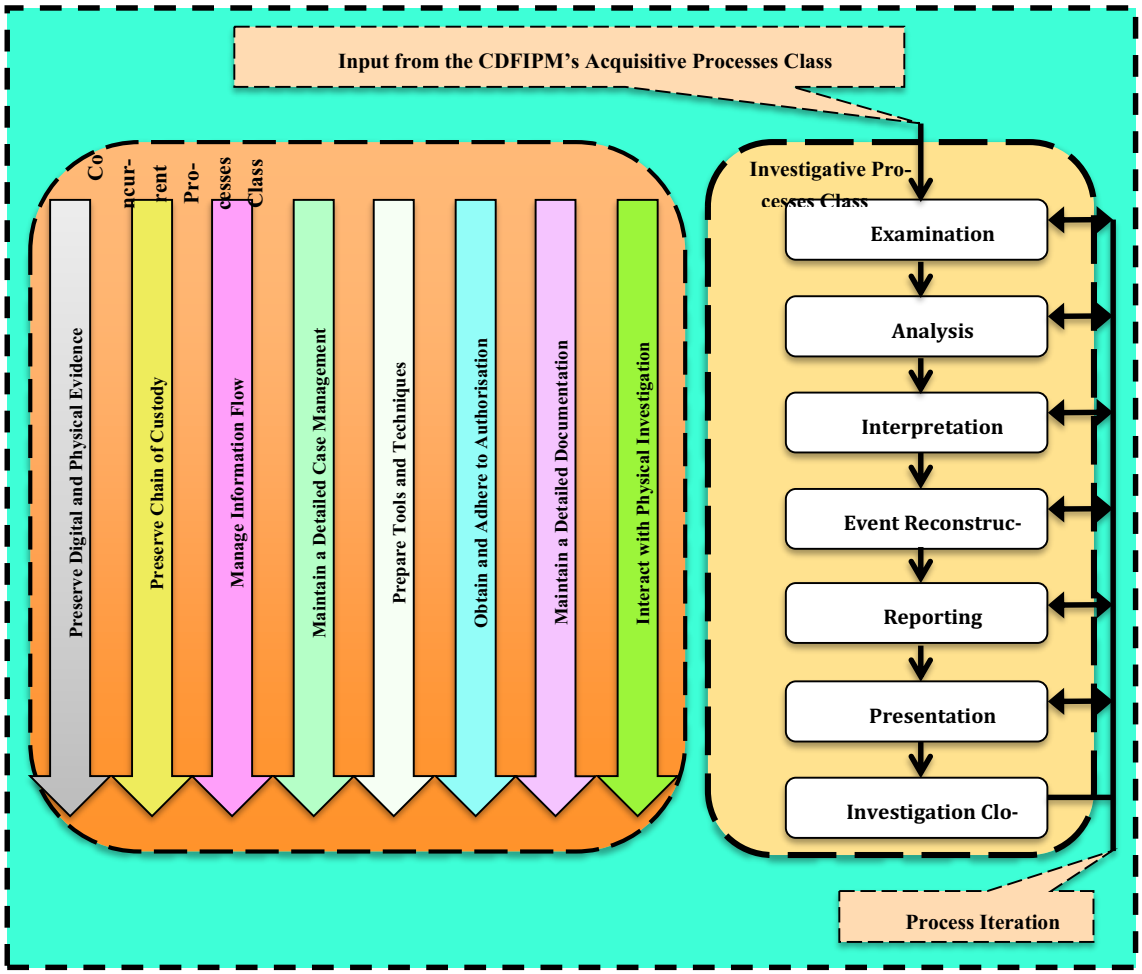

Figure 1. The UML Activity Diagram of Investigative Class Processes in their abstract level

3.1 Examination Process

The largest amount of investigation time is spent on the Examination Process as well as the Analysis Process (discussed later). During this Process, a large number of techniques need to be used in order to access, find and extract the acquired data representing the potential digital evidence into a human-readable format. Authors of many of the existing DFIPMs such as Carrier and Spafford [35] state that there should be one single Phase assigned to the Examination and Analysis activities. They argue that these Phases can be confusing as their meaning is only slightly different, and it is common to have two investigators who are referring to the same tasks when they say that they are "analyzing a system" or "examining a system".

This argument is invalid on the basis that the Examination and Analysis stages have different aims and therefore should be assigned two separate Processes. The Examination Phase should involve activities regarding the extraction of potential digital evidence from the acquired data, whereas the Analysis Phase should involve those activities associated with the methodical analysis of digital evidence as well as the construction of the incident. Therefore, in the SDFIPM, the Examination and Analysis have been assigned two separate processes with their own lower-level phases and sub-phase. This approach is supported by Casey [21], who states "Examination is the process of extracting and viewing information from the evidence and making it available for analysis", whereas "Analysis is the application of the scientific method and critical thinking to address the fundamental questions in an investigation: who, what, where, when, how, and why".

Figure 2 represents the UML Activity Diagram of the SDFIPM's Examination Process followed by the description of its lower-level components, i.e. phases and sub-phases.

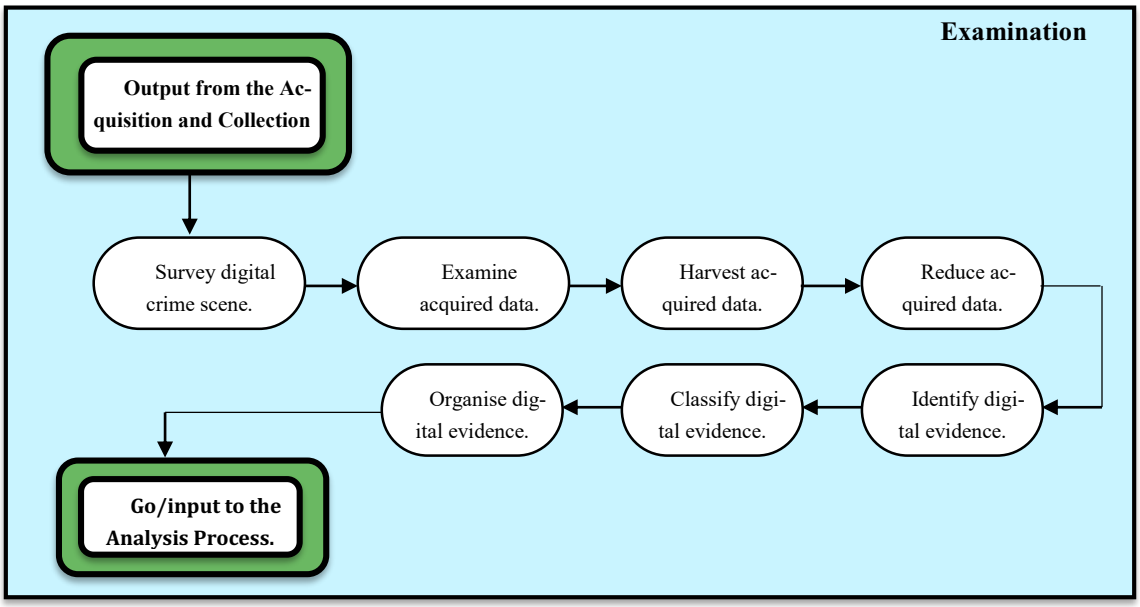

Figure 2. The UML Activity Diagram of the Examination Process

3.1.1 Survey Digital Crime Scene

The Survey Digital Crime Scene Phase has been developed and included in the Examination Process to enable DFAs to find apparent pieces of digital evidence for a particular category of crime in a swift manner, and also to assist them in ascertaining the skill level of the suspect. Determining the suspect's skill level in turn will allow DFAs to decide what examination and analysis techniques are required in the next process of the SDFIPM, the Analysis Process (discussed later). During the Examination Process, the first step that investigators will need to undertake is to survey the digital crime scene to identify and locate potential evidence, possibly within unconventional locations on the system [46]. It is preferable to carry out the Survey Digital Crime Scene Phase in a DFL as it provides a controlled environment, and the results can be repeated with another copy of the system. To carry out this Phase in a DFL, DFAs must use the image (working copy) of the system acquired from the Acquisition and Collection Process as shown in [7].

However, in certain circumstances, investigators employing the SDFIPM might be required to perform this phase on a live system to determine whether or not the system should be brought back to a DFL for a full examination and analysis. In such cases, investigators must perform field searches [9], [12] by booting the system

into what Carrier and Spafford [35] call a “trusted environment”. In cases where the Survey Digital Crime Scene Phase is to be conducted on a live system, the SDFIPM still requires the investigators to image the system so that any digital evidence could also be acquired in a controlled DFL environment. Whether the Survey Digital Crime Scene Phase is to be carried out on a live system or in a controlled DFL environment, DFAs must adapt their investigative techniques based on the specific category of crime. This is to expedite the subsequent Examination and Analysis activities as there is often a large volume of data to deal with.

For instance, in cases where the computer has been used to store or distribute contraband images, DFAs must in the first place look for graphics with image file extensions and ascertain those that could be relied upon as incriminating evidence. Another example includes server intrusion where investigators should search for apparent signs of a rootkit installation, examine application logs and also search for new configuration files. In other types of investigations such as terrorism where investigators suspect that the system might contain the communication by the suspect, investigators must perform keyword searching to identify any leads related to the investigation. Yet another example derived from [35] is when analysing network traffic about an incident; the Survey Digital Crime Scene Phase might analyse traffic for the incident time frame and filter out certain ports and hosts. In other cases, as suggested in [46], the investigators should also analyse the “common” and “uncommon” locations on the system that might contain artefacts related to the suspect’s browsing activities.

3.1.2 Examine Acquired Data

Having surveyed the digital crime scene, DFAs will need to perform a detailed examination on the image of the system (working copy) acquired from the Acquisition and Collection Process. See the research paper presented in [7] for more details. During the Examination Phase, digital evidence needs to be made visible by extracting data into a human-readable form [9, 10], [16]. DFAs should use the outcome of the Survey Digital Crime Scene Phase to direct their attention towards additional examination types. As an example, they will need to conduct a keyword search once keywords are identified from other evidence. DFAs will also need to extract and process unallocated file system space for deleted files. Moreover, they should examine a low-level timeline of file activity to trace a user’s activity.

Since there might be large volumes of data to be examined [16], [43], automated techniques should be employed using tools such as FTK [47] or EnCase [48] in order to support the investigators. Furthermore, a large number of techniques might be performed to process the obfuscated data such as deleted or hidden data utilising

sound digital forensic methods, as File Allocation tables or disk indexing might be deleted in some investigations. Therefore, this Phase will enable DFAs to ensure that files such as partially deleted files are recognized from the original evidence. During this Phase, DFAs can also reverse engineer suspicious executables and examine encrypted files [35]. They must also examine all the network packets that were acquired by monitoring software. In certain circumstances, it might be necessary for DFAs to examine the contents of every cluster (physical search) or every file (logical search) [21]. They will also need to ensure that they employ different search techniques, when appropriate, when preforming this Phase.

3.1.3 Harvest Data

After all data including partially discovered files and folders has been made visible in the Examine Acquired Data Phase, data then needs to be harvested by giving a logical structure to the entire data set. During this Phase, the file and folder structure is indexed to provide structure to data which was acquired in the Acquisition and Collection Process of the CDFIPM. In this phase, raw data will be shown as information, and the partially deleted files which were processed during the Examine Acquired Data Phase will become visible to the degree that they were rendered visible during the Examine Acquired Data Phase. The result of the Harvest Data Phase is the production of a logical structured data set [16] where the extracted raw data has now become structured information [49]. Therefore, the harvested information can now be displayed by the original file systems such as FAT or NTFS.

3.1.4 Reduce Data

The data examined and analysed in the course of a digital forensic investigation can be very large. Consequently, this data needs to be reduced to expedite the Examination Process. Identifying known elements can enable the investigators to reduce data. Investigators will need to use the metadata and unique identifiers, such as MD5, in order to remove known system files and different other application data [21], [36], [49]. Data that remains 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.

3.1.5 Identify, Classify and Organise Digital Evidence

During the Identify Digital Evidence Phase, DFAs must use the known digital evidence data in order to identify the possible incident to be investigated. The outcome of this Phase will be the identification of the potential digital evidence from data that has been examined, harvested and reduced. In the Classify Digital Evidence Phase, DFAs should group together digital evidence with similar identifying pattern

based on the types of investigation. This phase will enable the speeding up of the Analysis Process discussed in the next section. During the Organise Digital Evidence Phase, DFAs will need to organise digital evidence in a way so that digital forensic investigation can be accelerated. This can be materialized by focusing on the incident type identified and the data classified. DFAs should restructure digital evidence in order to conduct the identified investigation more appropriately. If similar types of incidents or crimes have taken place in the past and are known to DFAs, they should then use the known classification in order to compare the current digital forensic data (representing potential digital evidence) to the similar past incidents or crimes. At this stage, the Examination Process of the SDFIPM is completed, and its output becomes the input to the Analysis Process, discussed in the following section.

3.2 Analysis Process

Based upon the results of the Examination Process, DFAs must now be able to define what the exact characteristics of the incident are and who is to be held accountable for the incident. The aim of the SDFIPM's Analysis Process is to enable the investigators to reconstruct fragments of data based on their significance and to determine a possible root cause of the incident [9, 10], [14]. The Analysis Process is the most time-consuming stage of the investigative process. Because of the volume, diversity and complexity of data to be analysed in present time digital investigations, the analysis of evidence becomes a challenge. Therefore, DFAs following the SDFIPM should use accredited automated techniques during this Process to complement manual validation techniques in order to expedite this Process.

Figure 3 represents the UML Activity Diagram of the SDFIPM's Analysis Process followed by the description of its lower-level components, i.e. Phases and Sub-Phases.

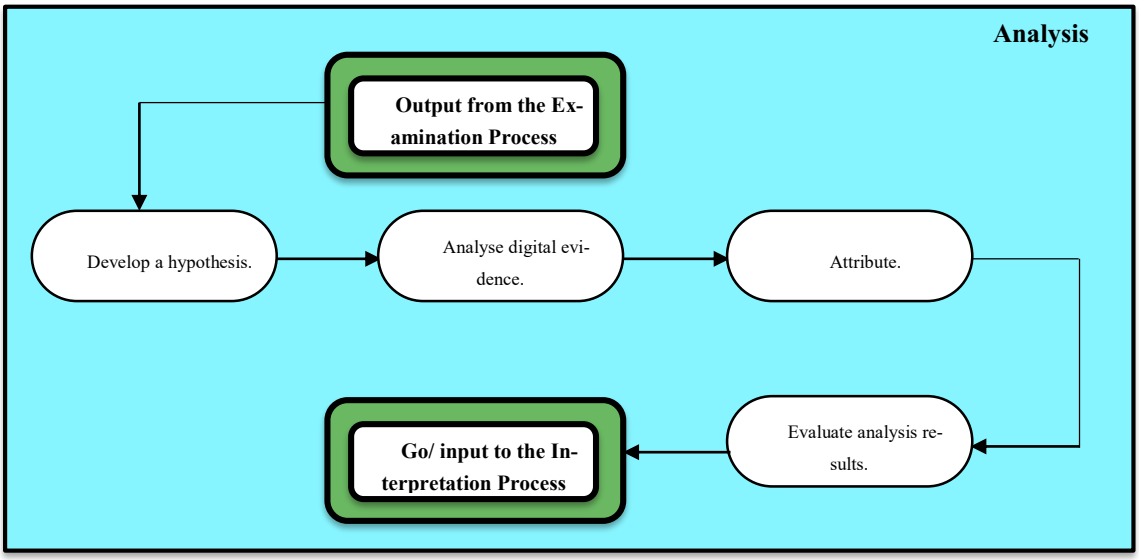

Figure 3. The UML Activity Diagram of the Analysis Process

3.2.1 Develop a Hypothesis

Up to this point in the investigation, DFAs have only dealt with what is possibly known from the digital evidence (Montasari et al., 2015). Now, DFAs 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. In order to develop a hypothesis for the incident or crime, DFAs should base their theory on the followings:

- The assumptions that they have deduced from the phases contained in the Examination Process;
- Digital evidence that they have already organised from the Organise Digital Evidence Phase contained in the Examination Process; and
- The documentation of the crime scene that they have maintained.

3.2.2 Analyse Digital Evidence

After DFAs have formulated the hypothesis, they will need to perform the Analyse Digital Evidence Phase. During this Phase, DFAs must thoroughly investigate and test data that was organised in the Examination Process against the hypothesis that was formulated in the Develop a Hypothesis Phase in the Analysis Process. DFIs must also question the legal validity of the possible digital evidence by considering

issues such as relevance, admissibility and weight as discussed in [2], [9]. This will enable them to test the hypothesis by identifying the best possible evidence.

3.2.3 Attribute

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. In order to link an individual to the incident or crime, DFAs must be able to correlate the results of the digital crime scene with physical evidence. For instance, in some investigations, DFAs are likely to need to correlate data center access logs to logins, linking online chat activities found on the computer with the activity with an undercover officer, and correlating activity on a compromised server with activity on the suspect's home system and network activity recorded by an ISP.

3.2.4 Evaluate Analysis Results

After the attribution has been made, during the Evaluate Analysis Results Phase, the DFAs must then evaluate their findings in order to ensure that the hypothesis they have developed holds true. Finally, in order for the Analysis Process to be most effective, DFAs might need to request other digital crime experts to assist them in correlating the event from numerous sources of digital evidence. At this stage of the Investigative Process, 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. Having completed all the Phases of the Analysis Process, this Process is now complete, and DFAs must start preparing for the interpretation of the analysis in the next process. The output of the Analysis Process will become the input to the Interpretation Process discussed in the next section.

3.3 Interpretation Process

The main purpose of the Interpretation Process is to use scientifically proven methods to explain facts discovered throughout the Analysis Process within the context of the investigation [9, 10], [50]. Therefore, after investigators have evaluated their findings in the Analysis Process and have determined that the hypothesis they formulated holds true, they will need to interpret the digital evidence in order to produce meaningful statements in the legal context for later reporting and presentation. During this Process, DFAs must be able to reconstruct the events associated with the digital investigation aspect. They should now be able to employ the results of the analysis techniques that they performed during the Analysis Process to put together the pieces of digital puzzle so that an accurate reconstruction of events can be made.

Figure 4 represents the UML Activity Diagram of the SDFIPM's Interpretation Process followed by the description of its lower-level components, i.e. Phases and Sub-Phases.

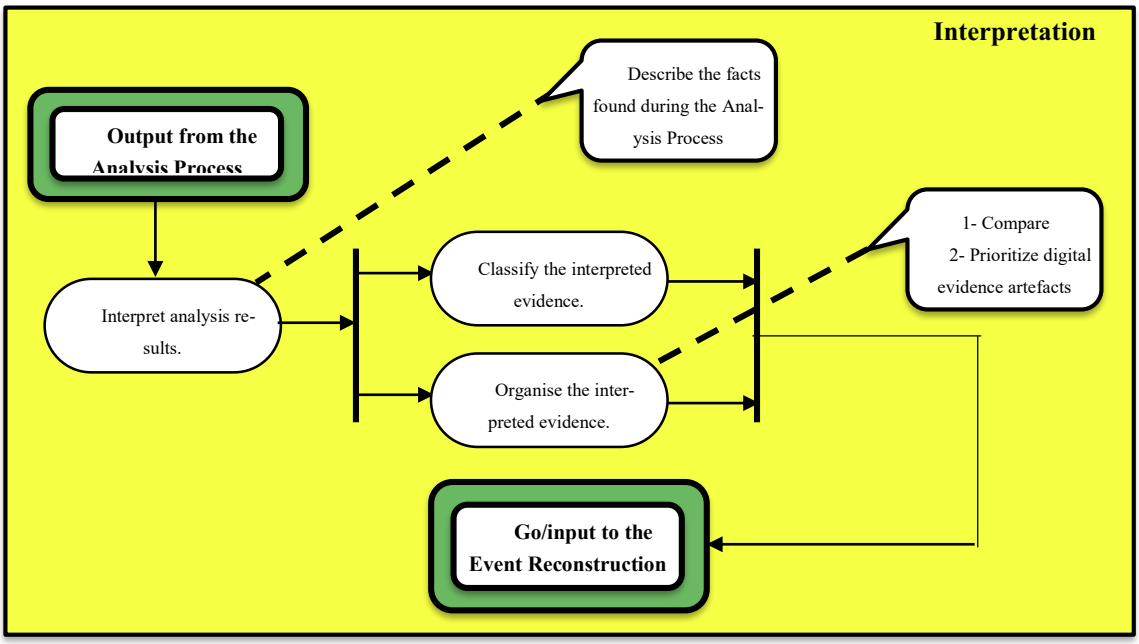

Figure 4. The UML Activity Diagram of the Interpretation Process

3.3.1 Interpret Analysis Results

Interpretation of any evidence should depend on the available information regarding the circumstances surrounding the creation of that item of digital evidence [15], [51]. Investigators will need to obtain information from individuals involved in the day-to-day operation of the system under investigation. This will enable them to carry out a more effective interpretation of evidence. Moreover, investigators must consider information concerning the goal as well as the scope of the investigation. In cases where the contextual information changes, investigators might also need to change the interpretation so that the interpretation can reflect any such changes regarding the contextual information. Finally, during this process, DFAs must utilise link analysis and timeline tools to enable them in the digital reconstruction.

3.3.2 Classify and Organise the Interpreted Evidence

Having interpreted the analysis results, investigators will now need to classify and evaluate the interpreted evidence in order to ascertain the amount of trust that they can place in it. DFIs will also need to organise the interpreted digital evidence according to relevance in such a way that they can differentiate which digital evidence items are more important than the others. DFIs following the SDFIPM should perform the Classify the Interpreted Evidence Phase and Organise the Interpreted Evidence in the Interpretation Process in parallel. This is due the fact that although both phases have different activities, they have the same aim. Finally, during the Analysis Process, DFAs will need to employ scientific methods in order to prove or refute theories based on digital evidence. After performing this process, DFAs should be able to determine how digital evidence came into existence and what its presence denotes. After completing the Interpretation Process, DFIs will need to reconstruct the events in the next process of the SDFIPM. Therefore, the output of the Interpretation Process will become the input to the Event Reconstruction Process discussed in the next section.

3.4 Event Reconstruction Process

In the SDFIPM, the Event Reconstruction Process and Interpretation Process are closely related in that both Processes will require DFAs to reconstruct the events associated with the digital investigation. Similar to the Interpretation Process, the Event Reconstruction Process requires DFAs to employ scientific methods in order to prove or refute theories based on the results of the analysis, and digital evidence that they have discovered. The only difference between the two Processes is that in the Event Reconstruction Process, DFIs will need to consolidate, review and test their findings against the original hypothesis that they formulated in the Analysis Process.

Having completed the Interpretation Process in the previous stage, DFAs should now be able to reconstruct a possible event sequence under the Event Reconstruction Process which reflects the incident result as accurately as possible. In order to reconstruct the events, DFIs will need to utilise the series of events that they have deduced from digital evidence which is known to them. During this Process, DFAs must ensure that they are not dealing with reconstruction as a finding based on the original digital evidence [16]. Moreover, as Kent et al. [52] state, Event Reconstruction should not be established as factual. Instead, DFAs who perform the Event Reconstruction Process should use this Process to explain how the incident might have taken place.

Figure 5 represents the UML Activity Diagram of the SDFIPM's Event Reconstruction Process followed by the description of its lower-level components, i.e. Phases and Sub-Phases.

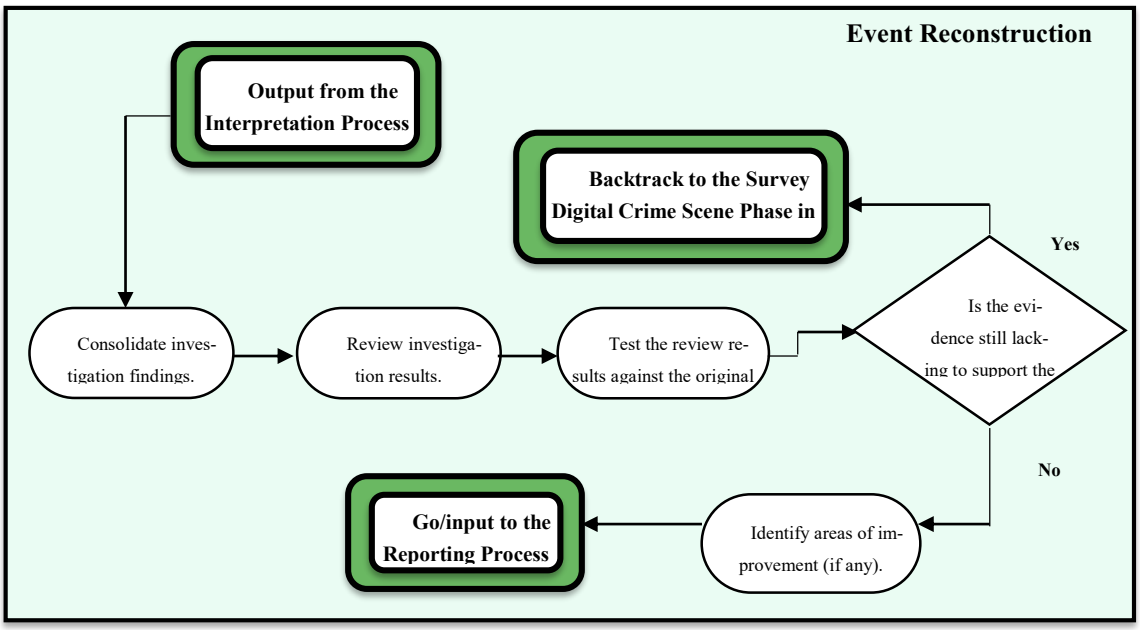

Figure 5. The UML Activity Diagram of the Event Reconstruction Process

3.4.1 Event Reconstruction Components

During the Event Reconstruction Process, the investigation findings must be consolidated and refined prior to assessing the review results against the original hypothesis, which was formulated in the Analysis Process. This will be to determine whether DFAs have acquired all the evidence required to support the original hypothesis. If all the evidence has not been captured, DFAs will need to backtrack to the Survey Digital Crime Scene Phase in the Examination Process, in which this Phase and subsequent Phases form a cycle that needs to be repeated until DFAs can identify additional evidence and explain the incident.

As an example, in cases where a server intrusion has taken place, this iteration would involve DFIs linking the exploitation of a service that is open to attack with the installation of a rootkit and utilization of a network sniffer. The source IP address of network connections could result in the acquisition of additional digital evidence to examine. If there is no need to iterate to the Examination Process at this stage, DFAs must identify any areas of improvement and address those required

improvements. In order to press charges against the perpetrator and explain the incident in a court, DFAs must have a valid hypothesis accompanied by relevant admissible digital evidence to support the findings that they have deduced. Finally, during the Event Reconstruction Process, DFAs might benefit from using link analysis and timeline tools to assist them in the digital reconstruction. The Event Reconstruction Process of the SDFIPM is completed at this stage and DFAs should prepare for the next Process where they will need to compile a report to be presented in a court or the management in a company. The output of the Event Reconstruction Process will become the input to the Reporting Process, discussed in the next section.

3.5 Reporting Process

After conducting the Event Reconstruction Process, DFAs will need to compile, write and print out on paper a detailed and concise report in the Reporting Process. Regardless of digital evidence or physical evidence, a forensic report must contain conclusions that can be reproduced by independent third parties. Forensic reports that include opinions based on accurately documented digital sources are much more likely to withstand judicial scrutiny than opinions based on less reliable sources [53]. DFAs following the SDFIPM must detail in their report all the findings and results of the entire digital investigative process including the Concurrent Processes (Overriding Principles) of the SDFIPM such as documentation, chain of custody, digital evidence preservation, authorisation and management, and ultimately the investigators' findings that are constructed in an opinion to be presented in a court. In addition, the forensic report should follow "the 'ABC's of writing' (accuracy, brevity, and clarity)" and be restricted only to what is known [36]. DFAs will need to write their report in such a manner that it contains conclusions that can be reproduced by independent third parties regardless of digital or physical evidence. Also, since digital forensic investigation might produce many incriminating digital evidence items, DFAs must therefore ensure that they list all digital evidence items in the report so that no valuable item of evidence is left out. Furthermore, DFAs must ensure that they include in the report all other relevant documentation that was compiled during the investigation and that might be relevant in reaching a decision.

Figure 6 represents the UML Activity Diagram of the CDFIPM's Reporting Process.

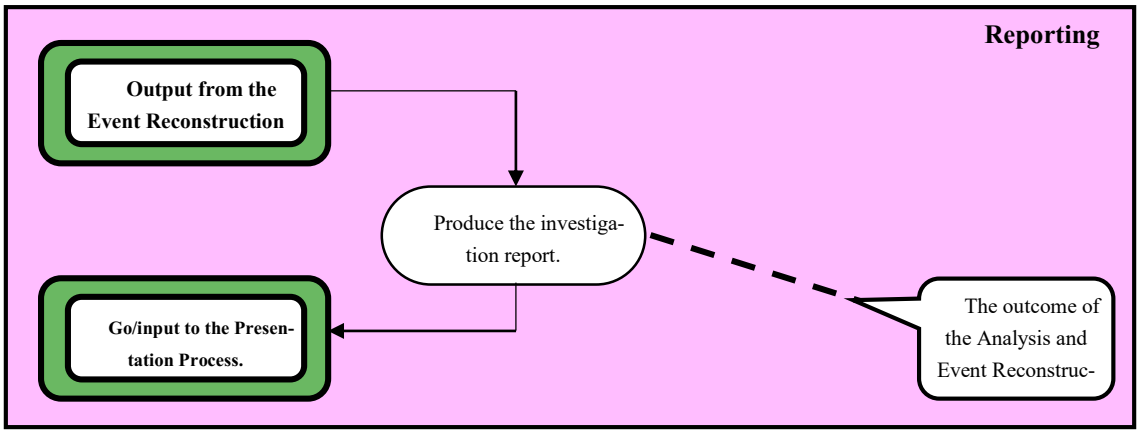

Figure 6. The UML Activity Diagram of the Reporting Process

DFAs should also ensure that they reference accepted and known protocols and methods applied during the Examination, Analysis, Interpretation and Event Reconstruction Processes in order to increase the credibility of the investigation and its results. Finally, DFAs employing the SDFIPM must ensure that their report is in a simple language and is well-defined, concise and unambiguous in order for the lay person to be able to understand it. After DFIs have compiled the report and are satisfied with its content, the report will then need to be presented in a court. The output of the Reporting Process becomes the input to the Presentation Process of the SDFIPM, discussed in the next section.

3.6 Presentation Process

The output of the Reporting Process in the form of a well-written report must be presented to a wide variety of audiences such as courts, legal personnel, law enforcement, technical personnel and management. Presenting the report can be carried out in the form of the expert report or can be accompanied by other formats such as multimedia presentation, deposition and expert witness (testimony). During the Presentation Process, DFAs will need to be able to prove the hypothesis that they formulated during the Analysis Process using supporting evidence. In order to prove that all of the SDFIPM's previous Processes were conducted accurately, evidence that DFAs present must hold up in a court.

Although Presentation Process is very important in that it meets the main requirement needed by the definition of the word 'forensic', authors of the existing models have paid little attention, if any, to this Process. Researchers have often taken a

cursory approach when dealing with the Presentation Process and have often confused this Process with the Reporting Process. In the existing models, Presentation Process and Reporting Process are regarded the same, and as a result they are assigned one single process under the naming either "Report" or "Presentation". This approach is flawed on the basis that the Reporting Process and Presentation Process are carried out at different times and under different circumstances during the course of an investigative process and as a result have different aims. The purpose of the Reporting Process should be to document relevant information deduced from the findings and results of the investigative process, whereas the aim of the Presentation Process should be to communicate such information and findings to the said audience. Therefore, in the SDFIPM, the Presentation Process has been distinguished from the Reporting Process, and as a result each has been assigned a separate and discrete Process in the model. Moreover, the "Report/Presentation" in the existing models is often a high-level Process without providing adequate details to assist DFAs in effectively preparing for this important Process. Since careful planning is essential especially when the investigation findings are to be presented in a court, the Presentation Process of the SDFIPM has incorporated lower-level and generic phases to guide the DFIs on how to prepare for this Process.

During the Presentation Process, DFAs must communicate their findings in such a way that facilitates future validation and that can be understood by both technical and non-technical audience. Mumba and Venter [54] state that during the Presentation Process, it is vital that all of the processes are utilised to prove that the investigation was conducted in a forensically sound manner. Beebe and Clark [36] highlight that a presentation should be based on "careful consideration about how to best communicate information to various audiences". Therefore, during the Presentation Process, DFAs following the SDFIPM must provide both concise and detailed confirmatory information obtained from the Interpretation and Event Reconstruction Processes of the model concerning the data examined and analysed in the Examination and Analysis Processes of the model. The presentation must also include relevant documentation and processes conducted during the investigative process, as well as any relevant physical evidence that can further consolidate the case against the perpetrator.

Figure 7 represents the UML Activity Diagram of the SDFIPM's Presentation Process followed by the description of its lower-level components, i.e. Phases and Sub-Phases.

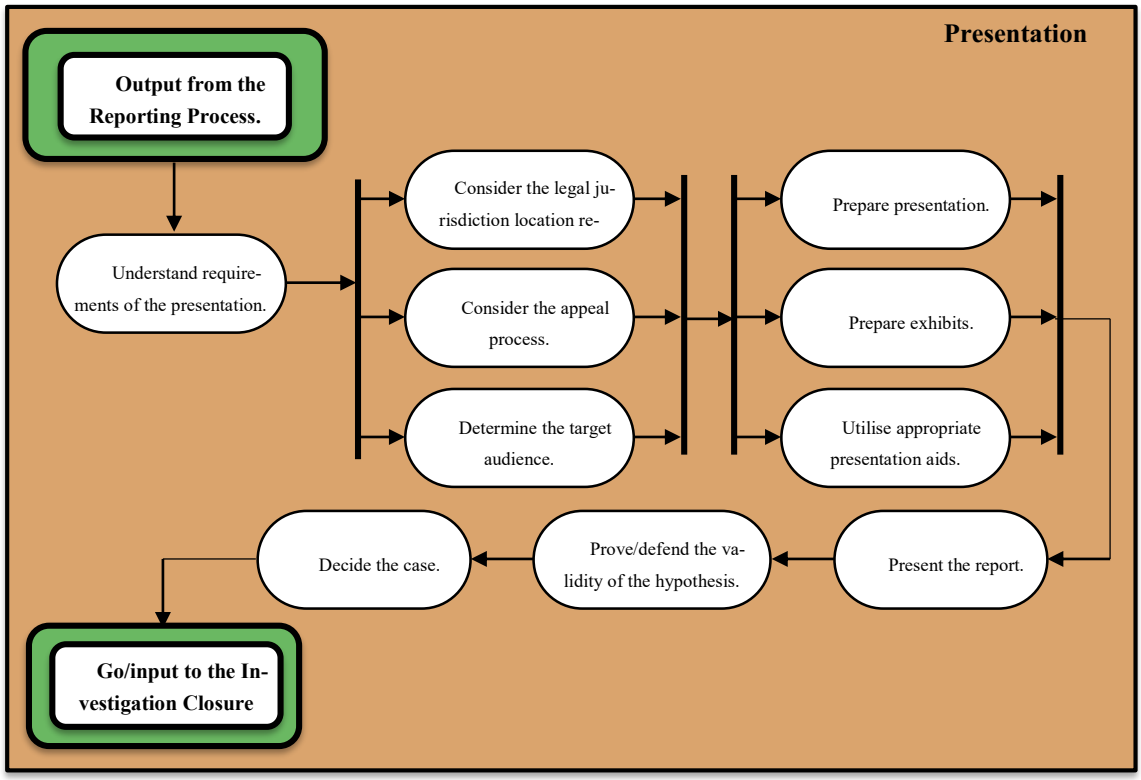

Figure 7. The UML Activity Diagram of the Presentation Process

3.6.1 Components of the Presentation Process

Prior to delivering the presentation, DFAs must address the following four issues:

- choosing their main points carefully based on the results of the CDFIPM's Interpretation and Event Reconstruction Processes;
- selecting their supporting information;
- developing a conclusion; and
- reviewing their presentation prior to its delivery.

Since the judge and jury or other interested parties are very likely to be non-technical users, DFAs must ensure that in their presentation they avoid complex arguments, unless providing the audience with significant help so that they understand

the technical points made. DFAs must deliver their conclusion in a logical and structured manner and build upon their previous points. In addition to preparing the presentation itself, DFAs will also need to prepare supporting information in order to assist the audience in better understanding the points they make. This should include the factual data itself that they have deduced from Interpretation and Event Reconstruction Processes and also the explanation of the process. DFAs might also need to use diagrams, pictures and video if it enables the audience to understand the explained concepts more clearly. Another important stage in the Presentation Process is the conclusion that DFAs have arrived at. They must ensure that they remind the audience of their main points and leave the audience with a clear understanding of them and their judgments on the case.

After preparing the presentation and prior to appearing before the relevant audience, DFAs will need to review their presentation to ensure that its content meets the objectives of the report, is logically structured and contains the material at the right level for the audience. In cases where DFAs will have to appear before judge and jury to give expert witness, they must ensure that they are fully aware of the jurisdiction legal requirements (the U.K. in the context of this research) concerning the digital evidence. Not being aware of the legal requirements might render the incriminating evidence being thrown out of the court. Moreover, DFAs must find out in advance what legal proceedings will concern the appeal process so that they can be better prepared in case they might need to reappear before the court. Often the person who presents the findings of the case is not often involved in various stages of the investigative process such as Acquisition, Examination, Analysis, Interpretation and Event Reconstruction Processes. Therefore, DFA who is required to appear before a court as an expert witness must determine who his target audience are prior to preparing the presentation if this is not already known.

Investigators also need to ensure that they identify the exhibits (i.e. digital evidence) by a label or other mark. The exhibit must also be properly described in the report as discussed in the Reporting Process section. When delivering the presentation, DFAs must take into account that the target audience are often non-technical and might have a variety of experiences and level of knowledge concerning the digital investigations. Therefore, in order to help the audience to understand the explained concepts better while giving the presentation, DFA might need to link their investigation findings to the things that the audience already understand. DFAs need to ensure that they have targeted their findings at the right level for the needs of the audience. They must also avoid using technical jargon and should attempt to explain the abstract concepts with clear practical examples.

During the presentation, often the hypothesis is challenged by the defence lawyers. A contradicting hypothesis and supporting evidence are placed before judge and jury. DFAs will need to prove the credibility of their hypothesis and to be well-prepared to defend the hypothesis against criticism and challenge. In circumstances in which challenges are successful, investigators will need to backtrack to the earlier stages to obtain and examine more evidence and develop a better hypothesis. The case will be decided based on the presentation report. If the decision is made in a court, it will be decided whether to convict the accused or whether to refute the allegations. If the decision is made in the context of an organisation, it will be decided what disciplinary actions must be taken if the incident can be attributed to the individual under investigation. At this stage, the Presentation Process of the CDFIPM is concluded, and its output becomes the input to the Investigation Closure Process, discussed in the following section.

3.7 Investigation Closure Process

It is vital not only to close the investigation and apply the decisions associated with it but also to maintain the knowledge obtained to improve subsequent investigations [36]. As the title suggests, the Investigation Closure Process of the SDFIPM involves concluding the investigation and also the decision-making on the credibility of the hypothesis presented in the Presentation Process. This denotes that after completing the Investigation Closure Process, investigators can backtrack to any of the preceding processes that follow the First Response Process.

Figure 8 represents the UML Activity Diagram of the SDFIPM's Investigation Closure Process followed by the description of its lower-level components, i.e. Phases and Sub-Phases.

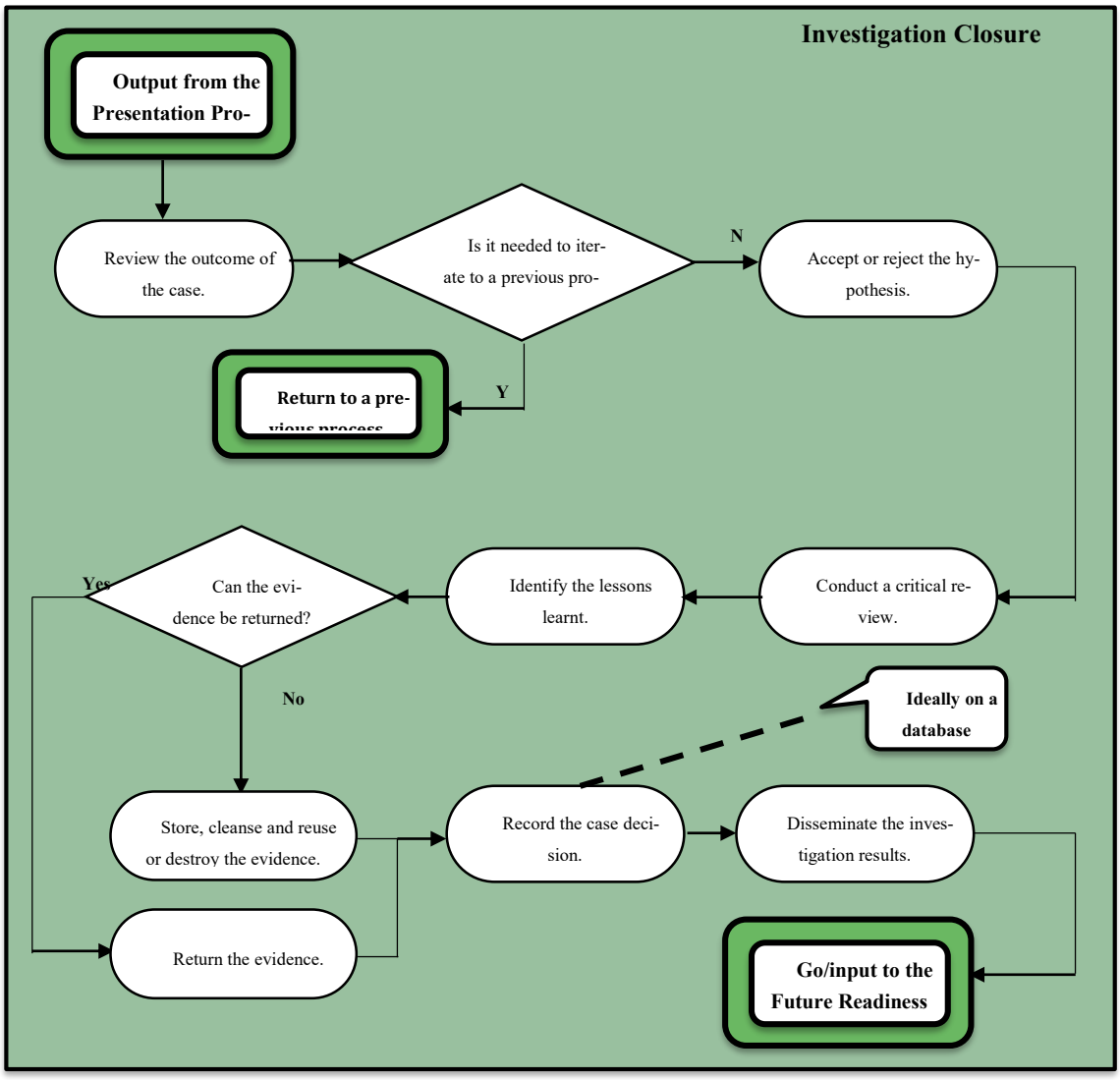

Figure 8. The UML Activity Diagram of the Investigation Closure Process

3.7.1 Review the Outcome of the Case

After the case has been presented to the appropriate audience and decided in the Presentation Process, the outcome of the investigation will need to be used to review the existing policies and procedures of the organisation. The aim of this Phase should be to make and act upon the outcome of the decisions reached from the CDFIPM's Presentation Process. During this Phase, the investigating organisation

will also need to collect and maintain all the information associated with the case that has been investigated.

3.7.2 Accept or Reject the Hypothesis

Since the CDFIPM is an iterative process model, it will allow investigators to backtrack to any of the preceding Processes in the model. Having carried out the initial review, at this stage the investigators can return to any of the CDFIPM's previous Processes that follow the First Response Process if required.

3.7.3 Conduct a Critical Review

During the Conduct a Critical Review Phase, the entire investigative process detailed in the SDFIPM must be reviewed to identify any lessons learnt and potential areas of improvement. During this Phase, the investigating organisation will also need to address issues such as what went well, what did not go well and how things could have been carried out better, etc. Based on this information, the investigating organisation will need to identify and learn the lessons from the incident or crime in order to be able to apply the findings and be better prepared for the future incidents or crimes. Also under this phase, the outcomes and their ensuing interpretation must be used for refining the Acquisition, Examination, Analysis, Interpretation and Event Reconstruction of digital evidence in future investigations. As already stated, often backtracking between Examination, Analysis, Interpretation and Event Reconstruction Processes are to be expected in order to obtain the full picture of the incident or crime. Such information could also assist law enforcements' HTCUs and corporates in establishing more effective policies and procedures.

3.7.4 Evidence Management

A decision will also need to be made to determine whether digital and physical evidence should be returned to the proper owner or not and to determine what criminal evidence must be removed. This is a complicated issue and not an explicit step in a digital forensic investigation. However, any of the existing models that has emphasized the seizure of evidence has seldom addressed this aspect. Jurisdiction in which the investigation is taking place (in the context of this thesis, the U.K.) and the type of authorisation determine whether the evidence should be returned, cleansed and reused or destroyed or whether the evidence should be stored for a certain period of time before any of the three possibilities can be applied.

3.7.5 Record the Case Decision

Under the Record the Case Decision Phase, DFIs will need to record (ideally on a database) the investigation results, case decision as well as all the evidence that

might be used for reference in the future and for training purposes. For instance, the results could be recorded by the category of evidence found as follows:

- Evidence of refutation or defence,
- Evidence vital to the case,
- Evidence important to the case,
- Evidence that supports other evidence,
- Evidence peripheral to the case,
- Evidence that is intelligence only, and
- No evidence found.

Such an approach could also benefit authorities in other jurisdictions in circumstances in which the case will be likely to have some kind of connection with their investigation.

3.7.6 Disseminate the Investigation Results

In the final part of the Investigation Closure Process, relevant information concerning the entire investigation will need to 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. During this Phase, the investigating organisation might decide to make some information available only within the organisation, whereas they might decide to disseminate other information more widely. According to [43], the investigating organisation's policies and procedures should determine the details in this regard. The information will have an impact on future investigations and might have an effect on the policies and procedures.

Thus, the accumulation and preservation of this information is a key part of supporting the work of investigators and might be a productive aspect for the development of innovative applications that integrate techniques such as data mining and expert systems. Hauck et al. [55] provide a detailed example of the dissemination activity where they define a system titled Coplink, that provides real-time support for law enforcement DFIs through an analysis application on the basis of a large accumulation of information from past investigations. An additional example is provided by Harrison et al. [56], whose system is not real-time, but instead delivers an "archival function" database to support investigators. At this stage, the Investigation Closure Process of the SDFIPM is concluded, and its output becomes the input to the Future Readiness Process Class, discussed in the following section.

3.8 Overriding Principles

In order to ensure the admissibility of digital evidence in courts, a set of eight Overriding Principles or Concurrent Processes have also been developed and grouped into a unique class, entitled Concurrent Processes Class (see Figure 1). These eight 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 SDFIPM. The inclusion of the proposed Overriding Principles or Concurrent Processes is justified by their significance and applicability to other digital investigation processes. Thus, due to their extreme importance, investigators must maintain these Principles at all times throughout the whole or parts of the digital investigative process. Since the SDFIPM is aimed at the U.K. jurisdiction, the proposed Overriding Principles are based on the following standards and guidelines: [51], [57, 58], as well as other relevant scientific papers such as [10], [14, 15], [21], [35, 36], [43].

3.8.1 Preserve Digital and Physical Evidence

Preservation is the process to maintain and safeguard the integrity and original condition of both physical and digital evidence. In order for evidence to be able to withstand scrutiny in courts, investigating organisations will need to prove that both digital device and digital evidence that they have handled during an investigation have not been altered, or justify their actions if unavoidable changes were made. In the best-case scenario, there should be no contamination to data itself or any metadata associated with it (e.g. date and time-stamps).

In some cases, the confidentiality of digital evidence is a requirement, either a business requirement or a legal requirement. This denotes that digital evidence should be preserved in a manner that ensures the confidentiality of data. Thus, since the correct handling of evidence is essential in any digital investigation [7], [9, 10], [15], [57, 58, 59], this Overriding Principle or Action Principle has been incorporated into the CDFIPM to enable investigating organisations to preserve the integrity of both digital and physical evidence throughout the entire investigative process in a forensically sound manner. Preserving this Overriding Principle will enable investigating organisations to protect both physical and digital evidence from being tampered with, contaminated or altered and as a result to ensure the efficacy of evidence presented to a court.

Almost all the existing models have undertaken a flawed approach towards the issue of preservation and have provided a superficial discussion of this aspect of digital investigative process by simply stating that digital evidence needs to be preserved

without elaborating on this important aspect. Moreover, preservation in some existing DFIPMs refer only to preservation of physical evidence or crime scene [21], [35] while in some other models it refers to preservation of only digital evidence [16], [35], [39], or digital evidence during the transportation or storage [15], [39], [43].

Although some existing models [21], [35] have discussed preservation in more depth, their approach of dealing with this principle is still flawed as the "preservation activity" in these models is restricted to a 'single Phase' at a particular stage of the investigative process. It is, however, argued that preservation has a much wider scope beyond being limited to a single point in time. Each stage of investigative process requires digital and physical evidence to be preserved in a different manner. In order to address the stated issues, in the SDFIPM, preservation has been introduced as an Overriding Principle or Actionable Principle that should be applied concurrently throughout the entire investigative processes of the model from the time the incident is detected in the Incident Detection Process up to and including the time when the investigation is formally completed in the Investigation Closure Process. Preservation does not need to be applied during the Readiness and Future Readiness Processes on the basis that evidence (both physical and digital) is not handled during these two Processes. The remainder of this section provides some practical examples of how the investigating organisations should apply the preservation aspect of the investigative process throughout the entire stages of the SDFIPM.

During the SDFIPM's Secure and Evaluate the Crime Scene Process, the preservation might involve investigators preventing unauthorised people from entering or leaving the crime scene, 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, etc. During the Acquisition and Collection Process, preservation involves DFIs securing log files in case that they are lost before the system is imaged. Preservation also requires DFIs 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. DFIs 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. Moreover, in terms of preserving the state of the network, this can be achieved by network monitors when they save network traffic.

Finally, as part of preservation, investigating organisations will also need to establish and maintain certain strict procedures [15], effective quality systems such as Standard Operating Procedures (SOPs) [26] or procedural workflows [60].

3.8.2 Preserve Chain of Custody

The processes for documenting, collecting and protecting both physical and digital evidence are called the establishing of the chain of custody. Establishing a chain of custody during the course of an investigation is of extreme importance since digital evidence is very likely to be handled by various parties. Cases where Chain of Custody has not been properly preserved have been easily challenged in courts and rejected irrespective of evidence discovered from the suspect's computer system. Therefore, due to its extreme importance in relation to conducting a successful investigation, Chain of Custody has been incorporated into the SDFIPM as an Overriding Principle, namely Preserve Chain of Custody, that will need to be applied concurrently throughout other Processes of the SDFIPM. In order to preserve Chain of Custody, DFIs will need to adhere to all legal requirements and must document each given process of the SDFIPM thoroughly. Documentation (discussed later) is a vital aspect of a Chain of Custody as it will need to detail the activities associated with the chronology of the movement and handling of evidence such as those associated with the seizure, custody, control, transfer, examination, analysis and disposition of both physical and digital evidence.

The issue of establishing Chain of Custody has been ignored by almost all the existing models, a problem identified also by the authors in [16], [43] and [35]. Although Chain of Custody has been addressed to some extent by four guidelines and standards including: [51], [57, 58], [61], these appear to be contradictory in terms of the point at which Chain of Custody will need to be established during an investigative process. For example, according to [57, 58], Chain of Custody should be initiated from the Acquisition Process onwards, whereas [51] and [61] state that Chain of Custody must be maintained throughout the entire investigative process.

The approach taken by [57, 58] appears to be flawed on the basis that digital device containing potential digital evidence is identified in the incident detection stage prior to the Acquisition Process. It is in the Incident Detection stage that the investigating organisations will need to process both physical (where items of evidentiary value exist) and digital crime scenes and therefore initiate the chain of custody. Consequently, in line with [51] and [61], DFIs following the SDFIPM must observe this Overriding Principle from the Incident Detection Process, during which incident is detected, up to and including the Investigation Closure Process, where incident is formally closed. One of the benefits of such an approach taken by author's

is that it will enable DFIs to trace back the history of any digital device containing evidence to the time that it was first identified until its present status and location. Another benefit of this approach is the enabling of the identification of access and movement of potential digital evidence at any given point in time.

In any type of investigation, investigators within the investigating organisations are often accountable for all the acquired evidence (both physical and digital) during the period in which evidence is within their custody. The SDFIPM's Preserve Chain of Custody Principle also requires DFIs to keep records of who was responsible for handling both physical and digital evidence. Investigators must keep a record of all information associated with different activities undertaken in relation to Chain of Custody. The Chain of Custody record itself may comprise more than one document and include a series of related documents. For instance, for potential digital evidence, there should be a contemporaneous document recording the acquisition of digital data to a particular device, the movement of that device and documentation recording subsequent extracts or copies of potential digital evidence for analysis or other purposes.

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. Another example of Chain of Custody is when the first responders (who are the first custodian to preserve Chain of Custody of potential digital evidence) arrive at the crime scene where they will need to describe the scene in the preliminary drafting of documentation. These include taking photographs, videos and sketches.

The SDFIPM's Preserve Chain of Custody Principle does not impose any particular format in which information related to Chain of Custody should be recorded. The documents detailing Chain of Custody can be in the form of digital data or other formats such as paper notes, depending on the organisation or the agency conducting the investigation. The SDFIPM's flexibility allows investigating organisations to design and incorporate into the model their own Chain of Custody forms according to their needs.

3.8.3 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 processes such as Chain of Custody. In this regard, Ciardhuáin [43] criticizes the past models stating, "The single largest gap in the existing models is that they do not explicitly identify the information flows in investigations." Ciardhuáin [43] proceeds to propose what

would become one of the most widely referenced research papers in relation to Information Flow within a digital investigation. In his research paper, Ciardhuáin [43] is able to define, identify and describe Information Flows within his process model so that its stages can be protected and supported technologically. Moreover, he clearly shows Information Flow that must exist amongst various stakeholders.

Due to the fact that the subject of Information Flow within the field of digital forensics has been extensively covered by the aforementioned reference, this paper does not aim to focus on Information Flow in any further details. However, due to its importance in a digital investigation, Information Flow has been incorporated into the SDFIPM as an Overriding Principle, namely Manage Information Flow, which needs to be managed concurrently throughout the entire processes of the SDFIPM. The rationale for including this principle in the SDFIPM is to enable investigating organisations to deal with the different laws, practices, languages, etc. correctly in digital investigations. An example of Information Flow could be the interaction between two investigators involved in the same investigation, or the exchange of digital evidence between various parties during digital investigation process. Information Flow can be protected, for instance, by utilising trusted public key infrastructure (PKI) and time stamping to identify the different investigators and authenticate evidence in addition to protecting the confidentiality of the evidence through PKI-based encryption.

3.8.4 Maintain a Detailed Case Management

As the title suggests, Case Management refers to managing the case under investigation and keeping track of evidence items, events and vital forensic discoveries. Case Management mainly pertains to the tasks that a case officer should undertake throughout the entire investigative process in an investigation, and also to some extent relates to the responsibilities of the case officer's investigative team members. Activities associated with the Case Management can have significant impact on the entire investigative process tying together all of the activities and their outcomes. Casey [21] highlights the importance of the Case Management stating, "Effective case management is one of the most important components of scaffolding, helping digital investigators bind everything together into a strong case." Similarly, Khatir et al. [62] proclaim that the effectiveness of a digital investigation is reliant upon Case Management.

The lack of effective Case Management methods will result in investigative opportunities being easily neglected, digital evidence being disregarded or lost, and incriminating information representing potential digital evidence remaining undiscovered or not being passed onto decision makers. Therefore, due to its importance

in a digital investigation, Case Management has been incorporated into the SDFIPM as an Overriding Principle, namely Maintain a Detailed Case Management, that will need to be applied from the Readiness Process up to and including Investigation Closure Process. The rationale for including this principle into the SDFIPM is as follow:

> to outline the responsibilities and certain important tasks that both a case officer and his investigative team members will need to undertake in order to ensure a successful investigation [62],
> to enable a smooth transition between different Processes of the model, and also to ensure that all applicable information that results from each Process is acquired, documented and intertwined together in order to reconstruct the events associated with the crime or incident in a vivid and compelling manner.

The remainder of this section provides some examples of the tasks and types of responsibilities that a case officer and his investigative team members are to undertake under this Overriding Principle, Maintain a Detailed Case Management.

The tasks of a case officer start after the incident has been reported in the Incident Detection Process (the discussion of which is outside the scope of this paper), where he needs to decide whether to accept or reject the case and determine the time and budget required to carry out the investigation. The case officer will subsequently need to develop an accurate and detailed plan that investigators can follow; this plan must define clearly the milestones, goals and sub-goals within the investigative process [62]. The case officer must also allocate tasks to individual team members, oversee these tasks as well as drawing a complete picture of the entire investigative process and its outcomes so that the investigation does not deviate from its correct course. In circumstances where the investigation has deviated from its correct course, the manager will need to identify the root cause of the deviation and guide the team members into the correct path. Case officers will also be responsible for obtaining written authorisation so that the investigation can proceed as well as determining what level of attention to give to a particular case comparative to all of the other cases that they are dealing with [62].

As already stated, in addition to the case officers, the Maintain a Detailed Case Management Principle also pertains to the investigative team members who will need to undertake various tasks under this Overriding Principle. These include communication and prioritization such as sharing information amongst DFIs, meeting

the requirements of non-technical stakeholders, prioritizing and assigning administrative tasks amongst multiple DFIs in a digital investigation, etc. In certain investigations, communication becomes a key aspect of case management [62]. For example, in complex investigations that might last for long time, daily or weekly status meetings are required in order to discuss and analyse progress, combine up-to-date information and discuss and review the following steps in the investigation. Finally, logging digital evidence in archives is another important factor in managing an investigation effectively. This task can be carried out by both the case officer or the investigative team members [62].

3.8.5 Prepare and Test Tools and Techniques

It is vital that DFIs 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. DFIs might require different sets of tools and techniques to be able to carry out each given process in the investigative process. Therefore, this aspect of the digital investigative process has been incorporated into the SDFIPM as an Overriding Principle, namely Prepare and Test Tools and Techniques, that will need to be followed throughout all the other Processes of the model. This Principle has been extensively covered in technical standard documents such as [63, 64], guidelines such as National Institute of Standards and Technology [52] and [65], as well as technical reports such as Information Assurance Advisory Council (IAAC) [66].

For instance, under a comprehensive project, entitled CFTT (Computer Forensics Tools Testing), carried out by the National Institute of Standards and Technology [65], various methodologies have been established for testing computer forensic software tools through the development of general tool specifications, test procedures, test criteria, test sets, and test hardware. This detailed guideline provides necessary information for digital forensic tools developers to improve their tools, and also enable DFIs to make informed choices about obtaining and testing digital forensic tools and understand the tools' capabilities.

Therefore, due to the fact that tools and techniques testing and preparation have already been covered in detail, this paper does not aim to focus on this aspect of the investigative process in more details. However, some examples on certain steps that DFIs will need to undertake in relation to this Overriding Principle will still be provided only for illustrative purposes. Some activities that DFIs will need to perform in relation to Prepare and Test Tools and Techniques Principle include, but are not limited to:

determining which tools must be used for each given Process of the CDFIPM,
identifying which tools must be utilised for different data analysis tasks,
investigating and establishing which tools have been scientifically tested, and
identifying the degree of error in connection with tools.

Cases where untested tools have been used to carry out digital investigations are easily challenged in courts. Therefore, one key element that DFIs will need to consider at all times under this Principle is the need to select tools that are court-proven such as EnCase, AccessData FTK, ProDiscover, Sleuthkit and Autopsy. Another important aspect that investigators will need to adhere to under this Overriding Principle is the need to have up-to-date training on how to use the latest versions of different forensic tools in order to make effective use of them.

Finally, as already stated, each Process within an investigative process might require different sets of tools. For example, to conduct the Examination Process, the software tools such as FTK and EnCase, that are capable of revealing hidden, deleted, swapped and corrupted files or performing data carving, will need to be utilised. In terms of techniques, for example in cases where public and private IP addresses need to be acquired and mapped to the country and institutions, IP addresses can be readily acquired by performing the following commands: ping, nslookup, dig, tracert from a DNS server. Moreover, DFIs can easily locate a county by various online tools such as IP Location [67] or WhatIsMyIPAddress [68].

3.8.6 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. In fact, each single stage of digital investigation should be authorised, and therefore an authorisation is required for each given process. Due to its significance on the investigative process, authorisation has been incorporated into the SDFIPM as an Overriding Principle, namely Obtain and Adhere to Authorisation. This Overriding Principle requires investigating organisations to obtain proper authorisation from one of the following groups: government authorities, system owners, system custodians, principles or users etc., when undertaking a digital investigation. The significance of this Principle for activities carried out during the digital investigation processes is justified by the fact that the rights of the system owners, custodians, principles or users should not be infringed. Moreover, this principle ensures that no law is violated. The environment in which digital investigation is carried out determines the

type of authorisation required. The authorisation might be needed both within a legal environment or an organisational environment. 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. This Overriding Principle must be adhered to concurrently throughout the entire processes of the SDFIPM.

3.8.7 Maintain a Detailed Documentation

It is extremely important to document all the activities carried out throughout the entire investigative process in order to enable other investigators to authenticate the process and results. As well as being incorporated as a single Phase, documentation has also been incorporated into the SDFIPM as an Overriding Principle, namely Maintain a Detailed Documentation, that will need to be applied throughout the whole investigative process. The aim of this Overriding Principle is to record all information applicable or produced during the investigative process to support decision making and the legal, administrative processing of those decisions. This Overriding Principle involves documenting both physical and digital crime scene. For instance, documentation of the physical crime scene involves creating sketches and making video of a physical crime scene, while documentation of digital crime scene involves investigators properly documenting each item of digital evidence when it is discovered.

3.8.8 Interact with Physical Investigation

A digital investigation and a physical investigation are often interrelated and dependent on one another [35]. 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. [9, 10] [15]. 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 [15]. In the SDFIPM, Interact with Physical Investigation has been included as an Overriding Principle since 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.

4. Conclusion

This paper covered the Design and Development of our Advanced Investigative Process Model (SDFIPM) for conducting digital forensic examination of digital evidence after it has been identified and acquired. It is argued that the SDFIPM is the most comprehensive, detailed and structured DFIPM presented to date. Each Process of the model was discussed and justified. Due to its top-down approach, an overview of the model was firstly formulated specifying the first-level components, i.e. Processes. Each first-level component was further broken down to specify the second-level components, i.e. Phases. In turn, each second-level component was further refined in greater details to specify the third-level components, namely Sub-Phases. The SDFIPM is also both generic and formal, enabling DFIs to reach conclusions that are reliable, repeatable and well-documented. Due to its scientific approach, the SDFIPM will enable DFIs to follow a uniform approach, to overcome biased and predetermined theories, and authenticate their discoveries by attempting to prove themselves wrong. This, in turn, will result in well-established conclusions that support expert testimony in courts of law.

References

1. 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.
2. Montasari, R. (2017). Digital Evidence: Disclosure and Admissibility in the United Kingdom Jurisdiction. *Proceedings of the 11th International Conference on Global Security, Safety, and Sustainability*, pp. 42-52. London, U.K.
3. Kessler, C. (2010). Judges' Awareness, Understanding, and Application of Digital Evidence. PhD thesis, Nova Southeastern University.
4. Adams, R. (2012). *The Advanced Data Acquisition Model (ADAM): A Process Model for Digital Forensic Practice*. PhD thesis. Murdoch University.
5. Armstrong, C. and Armstrong, H. (2010). 'Modeling Forensic Evidence Systems Using Design Science', *IFIP WG 8.2/8.6 International Working Conference*, pp.282-300.
6. Montasari, R. (2018). Testing the Comprehensive Digital Forensic Investigation Process Model (the CDFIPM). In *Dastbaz M., Arabnia H., Akhgar B. (eds.) Technology for Smart Futures*. Springer, Cham, pp. 303-327.
7. Montasari, R. (2017). A Standardised Data Acquisition Process Model for Digital Forensic Investigations. *International Journal of Information and Computer Security*, 9(3), pp. 229-249.

8. Montasari, R. (2017). An Overview of Cloud Forensics Strategy: Capabilities, Challenges, and Opportunities. In *Hosseinian-Far, A., Ramachandran, M. and Sarwar, D*. (eds.) *Strategic Engineering for Cloud Computing and Big Data Analytics*. Springer, Cham, pp. 189-205.
9. Montasari, R. (2016). The Comprehensive Digital Forensic Investigation Process Model (CDFIPM) for Digital Forensic Practice. *PhD Thesis*, University of Derby.
10. Montasari, R. (2016). A Comprehensive Digital Forensic Investigation Process Model. *International Journal of Electronic Security and Digital Forensics*, *8*(4), pp. 285-302.
11. Montasari, R. (2016). An Ad Hoc Detailed Review of Digital Forensic Investigation Process Models. *International Journal of Electronic Security and Digital Forensics*, *8*(3), pp. 205-223.
12. Montasari, R. (2016). Formal Two Stage Triage Process Model (FTSTPM) for Digital Forensic Practice. *International Journal of Computer Science and Electronic Security*, 10(2), pp. 69-87.
13. Montasari, R. (2016). Review and Assessment of the Existing Digital Forensic Investigation Process Models. *International Journal of Computer Applications*, *147*(7), pp. 41-49.
14. Montasari, R., Peltola, P. and Evans, D. (2015). Integrated Computer Forensics Investigation Process Model (ICFIPM) For Computer Crime Investigations. *International Conference on Global Security, Safety, and Sustainability*, pp. 83-95. London: U.K.
15. Valjarevic, A. and Venter, H. (2015). 'A Comprehensive and Harmonized Digital Forensic Investigation Process Model', *Journal of Forensic Sciences*, 60(6), pp. 1467-1483.
16. Kohn, M., Eloff, M. and Eloff, J. (2013). 'Integrated digital forensic process model', *Computers & Security*, 38, pp. 103–115.
17. US-CERT. (2012). *Computer Forensics*. U.S. Department of Homeland Security. Available at: https://www.us-cert.gov/security-publications/computer-forensics (Accessed: 14 May 2018).
18. Agarwal, A., Gupta, M., Gupta, S. and Gupta, C. (2011). 'Systematic digital forensic investigation model', *International Journal of Computer Science and Security,* 5(1), pp.118–130.
19. Rogers, M., Goldman, J., Mislan, R., Wedge, T. and Debrota, S. (2006). 'Computer Forensics Field Triage Process Model', *Conference on Digital Forensics, Security and Law*, pp. 27-40.
20. Zainudin, N., Merabti, M. and Llewellyn-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*, pp. 1-6.

21. Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*. 3rd edn. New York: Elsevier Academic Press.
22. Trcek, D., Abie, H., Skomedal, A. and Starc, I. (2010). 'Advanced Framework for Digital Forensic Technologies and Procedures', *Journal of Forensic Sciences*, 55(6), pp. 1471–1480.
23. 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.
24. Cohen, F. (2011). 'Putting the Science in Digital Forensics', *Journal of Digital Forensics, Security and Law*, 6(1), pp.7–14.
25. Nance, K., Hay, B. and Bishop, M. (2009). 'Digital Forensics: Defining a Research Agenda', *42nd Hawaii International Conference on System Sciences*, pp.1–6.
26. Bulbul, H., Yavuzcan, H. and Ozel, M. (2013). 'Digital forensics: An Analytical Crime Scene Procedure Model (ACSPM)', *Forensic Science International*, 233(1), pp.244-256.
27. Grobler, C.P., Louwrens, C.P. and Solms, S.H. (2010). 'A Multi-component View of Digital Forensics', *ARES '10 International Conference on Availability, Reliability and Security*, pp. 647-652.
28. Ieong, R. (2006). 'FORZA - Digital forensics investigation framework that incorporate legal issues', *Digital Investigation*, 3, pp. 29–36.
29. Stanfield, A. (2009). *Computer Forensics, Electronic Discovery and Electronic Evidence*. Chatswood: LexisNexis Butterworths.
30. Carlton, H. and Worthley, R. (2009). 'An evaluation of agreement and conflict among computer forensic experts', *42nd Hawaii International Conference on System Sciences*, pp. 1-10.
31. Garfinkel, S., Farrell, P., Roussev, V. and Dinolt, G. (2009). 'Bringing science to digital forensics with standardized forensic corpora', *Digital Investigation*, 6, pp.2–11.
32. Pollitt, M. (2008) 'Applying traditional forensic taxonomy to digital forensics', *Advances in Digital Forensics IV*, Springer, USA, pp.17–26.
33. Leigland, L. and Krings, A. (2004). 'A formalization of digital forensics', *International Journal of Digital Evidence*, 3(2), pp.1–32.
34. Farrell, M. (1993). Daubert v. Merrell Dow Pharmaceuticals, Inc.: Epistemilogy and Legal Process. *Cardozo L. Rev.*, *15*, p. 2183.
35. Carrier, B. and Spafford, E. (2003). 'Getting Physical with the Digital Investigation Process', *International Journal of Digital Evidence*, 2(2), pp.1–20.

36. Beebe, N. and Clark, J. (2005). 'A Hierarchical, Objectives-Based Framework for the Digital Investigations Process', *Digital Investigation,* 2(2), pp.147–167.
37. Cohen, F. (2010). 'Towards a Science of Digital Forensic Evidence Examination', *6th IFIP WG 11.9 International Conference on Digital Forensics*, pp. 17-35.
38. 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,* 8(4), pp.25–48.
39. Reith, M., Carr, C. and Gunsch, G. (2002). 'An Examination of Digital Forensic Models', *International Journal of Digital Evidence*, 1(3), pp. 1-12.
40. 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).
41. Selamat, S., Yusof, R. and Sahib, S. (2008). 'Mapping Process of Digital Forensic Investigation Framework', *International Journal of Computer Science and Network Security*, 8(10), pp. 163-169.
42. 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*.
43. Ciardhuáin, O. (2004). 'An Extended Model of Cybercrime Investigations', *International Journal of Digital Evidence*, 3(1), pp. 1-22.
44. Karyda, M. and Mitrou, L. (2007). 'Internet Forensics: Legal and Technical Issues', 2nd *International Workshop on Digital Forensics and Incident Analysis*, pp. 3-12.
45. Baryamureeba, V. and Tushabe, F. (2004). 'The Enhanced Digital Investigation Process Model', *4th Digital Forensic Research Workshop*, pp. 1-9.
46. Montasari, R. and Peltola, P. (2015). 'Computer Forensic Analysis of Private Browsing Modes', *Proceedings of 10th International Conference on Global Security, Safety and Sustainability: Tomorrow's Challenges of Cyber Security*, pp. 96-109.
47. AccessData. (2016). Forensic Toolkit (FTK). Available at: http://accessdata.com/products/computer-forensics/ftk (Accessed: 14 May 2018).
48. Guidance Software. (2016). EnCase Forensics. Available at: https://www.guidancesoftware.com/encase-forensic (Accessed: 14 May 2018).

49. Cohen, F. (2009). *Digital Forensic Evidence Examination*. 2nd edn. Livermore, California: Fred Cohen & Associates.
50. Palmer, G. (2001). 'A Road Map for Digital Forensic Research', *1st Digital Forensic Research Workshop (DFRWS)*, pp.27–30.
51. International Organisation for Standardization. (2015). ISO/IEC 27043:2015. *Information technology -- Security techniques -- Incident investigation principles and processes.* Geneva, Switzerland: International Organization for Standardization.
52. Kent, K., Chevalier, S., Grance, T. and Dang, H. (2006). *Guide to Integrating Forensic Techniques into Incident Response*. U.S. Department of Commerce. Available at: http://cybersd.com/sec2/800-86Summary.pdf (Accessed: 16 June 2016).
53. Garrie, D. (2014). 'Digital Forensic Evidence in the Courtroom: Understanding Content and Quality', *Northwestern Journal of Technology and Intellectual Property*, 12(2), pp. [i]-128.
54. Mumba, E. and Venter, H. (2014). 'Testing and Evaluating the Harmonized Digital Forensic Investigation Process in Post Mortem Digital Investigations', *ADFSL Conference on Digital Forensics, Security and Law*, pp. 83-97.
55. Hauck, R., Atabakhsh, H., Ongvasith P., Gupta, H. and Chen, H. (2002). 'Using Coplink to analyze criminal-justice data', *IEEE Computer,* 35(3), pp. 30-37.
56. Harrison, W., Heuston, G., Morrissey, M., Aucsmith, D., Mocas, S. and Russelle, S. (2002). 'A Lessons Learned Repository for Computer Forensics', *International Journal of Digital Evidence*, 1(3), pp. 1-9.
57. International Organisation for Standardization. (2012). ISO/IEC 27037:2012. *Information technology -- Security techniques -- Guidelines for identification, collection, acquisition and preservation of digital evidence.* Geneva, Switzerland: International Organization for Standardization.
58. ACPO. (2012). *ACPO Good Practice Guide for Digital Evidence*. U.K. Association of Chief Police Officers. Available at: http://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf (Accessed: 14 May 2018).
59. Holder, E., Robinson, L. and Rose, K. (2009). *Electronic Crime Scene Investigation: An On-the-Scene Reference for First Responders*, U.S. Department of Justice. Available at: https://www.ncjrs.gov/pdffiles1/nij/227050.pdf (Accessed: 14 May 2018).

60. Mukasey, M., Sedgwick, J. and Hagy, D. (2008). *Electronic Crime Scene Investigation: A Guide for First Responders*. U.S. Department of Justice. Available at: https://www.ncjrs.gov/pdffiles1/nij/219941.pdf (Accessed: 14 May 2018).
61. International Organisation for Standardization. (2011). ISO/IEC 27035:2011. *Information technology -- Security techniques -- Information security incident management.* Geneva, Switzerland: International Organization for Standardization.
62. Khatir, M., Hejazi, M. and Sneiders, E. (2008). 'Two-dimensional evidence reliability amplification process model for digital forensics', *Third International Annual Workshop on Digital Forensics and Incident Analysis*, pp.21–29.
63. International Organisation for Standardization. (2013). ISO/IEC 27001:2013. *Information technology -- Security techniques -- Information security management systems -- Requirements.* Geneva, Switzerland: International Organization for Standardization.
64. International Organisation for Standardization. (2005). ISO/IEC 17799:2005. *Information technology -- Security techniques -- Code of practice for information security management.* Geneva, Switzerland: International Organization for Standardization.
65. NIST. (2015). *Computer Forensics Tool Testing Handbook*. U.S. Department of Commerce. Available at: http://www.cftt.nist.gov/CFTT-Booklet-08112015.pdf (Accessed: 14 May 2018).
66. Sommer, P. (2008). *Directors' and Corporate Advisors' Guide to Digital Investigations and Evidence*. U.K. Information Assurance Advisory Council. Available at: https://www.ucisa.ac.uk/~/media/Files/members/activities/ist/DigitalInvestigationsGuide.ashx (Accessed: 14 May 2018).
67. IP Location. (2016). Where is Geolocation of an IP Address?. Available at: https://www.iplocation.net/ (Accessed: 14 May 2018).
68. WhatIsMyIPAddress. (2016). How you connect to the world. Available at: http://whatismyipaddress.com/ (Accessed: 14 May 2018).