A Formal Two Stage Triage Process Model (FTSTPM) for Digital Forensic Practice

Reza Montasari *r.montasari@derby.ac.uk*
Department of Computing and Mathematics
University of Derby
Derby, DE22 1GB, U.K.

Abstract

Due to the rapid increase of digital based evidence, the requirement for the timely identification, examination and interpretation of digital evidence is becoming more essential. In certain investigations such as child abductions, pedophiles, missing or exploited persons, time becomes extremely important as in some cases, it is the difference between life and death for the victim. Moreover, the growing number of computer systems being submitted to digital forensic laboratories is creating a backlog of cases that can delay investigations and negatively affect public safety and the criminal justice system. To deal with these problems, there is a need for more effective 'onsite' triage methods to enable the investigators to acquire information in a timely manner, and to reduce the number of computer systems that are submitted to DFLs for analysis. This paper presents a Formal Two-Stage Triage Process Model fulfilling the needs of an onsite triage examination process.

Keywords: Digital Forensics, Onsite Triage, Digital Investigation, Process Model, On-scene Examination, Formal Model.

1. INTRODUCTION

Due to the rapid increase of digital based evidence, the requirement for the timely identification, examination, analysis and interpretation of digital evidence is becoming more essential. In certain investigations such as child abductions, pedophiles, missing or exploited persons, time becomes extremely important as in some cases, it is the difference between life and death for the victim [1]. In such circumstances, the traditional digital forensic investigation approach of seizing the digital device, transporting it back to the digital forensic laboratory (DFL), making a forensic image of the device and then searching the entire system for potential digital evidence is no longer appropriate. In such situations, critical information is needed while at the crime scene within a short period of time to provide the investigators with the investigative leads swiftly. Regrettably, there exist inadequate methods to carry out effective 'onsite' triage examinations. The methods related to the onsite triage are being carried out on an ad-hoc basis based on the investigators' own personal experience. Various researchers are increasingly calling for more formalized solutions in onsite triage examinations that can be carried out at the crime scene within a short period of time [2, 3, 4].

In many circumstances, digital forensic examiners are needed to respond expeditiously to a crisis and determine how much attention to assign to a particular case or item of evidence. Whether digital devices are a source of intelligence or evidence in investigations, there need to be better approaches of acquiring usable information in a timely manner. Effective onsite triage processes and proper tools could preserve evidence in a forensically sound manner and make difference between life and death in certain circumstances. Onsite triage examination carried out on a digital device produces intelligence that can greatly assist the investigators in conducting a complete and accurate analysis. Therefore, a more meticulous approach that investigators could use for onsite identification and examination of information from computer systems is needed to address the limitations of the existing digital forensic investigation process models (DFIPMs). The research presented in this paper aims to address the problem that there does not exist a formal 'onsite' triage process model that could assist investigators in following a uniform approach. Therefore, a Formal Two-Stage Triage Process Model (FTSTPM) is proposed by harmonizing and building upon the existing DFIPMs in order to enable the investigators to produce results in a timely manner at the crime scene.

2. BACKGROUND

All the prominent DFIPMs presented to date were critically reviewed and assessed by the authors in [5] to identify components necessary to incorporate into the FTSTPM. This review revealed that the current models would often assume an ideal circumstance where the digital device under investigation needs to be seized, transported back to the forensic laboratory for imaging and searched for potential digital evidence (see Figure 1). This traditional approach can be extremely time consuming considering the amount of data to examine and the fact that in many cases, this will involve the seizure and transportation of the system back to a DFL for a detailed analysis. Although this approach is effective in circumstances where time is not critical, this is not appropriate in time-critical circumstances such as child abductions, missing persons, death threats etc. In circumstances as such, the necessity for swift information and intelligence overrides the need for a detailed analysis of all the potential digital evidence back in a DFL.

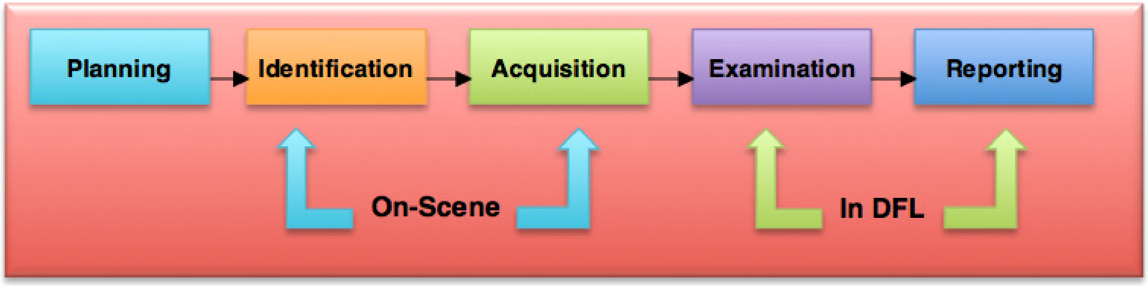

FIGURE 1: Traditional Digital Forensic Investigation Process Model.

Therefore, the proposed model has been specifically developed to meet the requirements for timely intelligence derived from digital sources at the crime scene. The FTSTPM enables the digital forensic investigators to identify, examine and interpret digital evidence in a short time frame without having to take the digital device back to a DFL for an in-depth analysis. It should be noted that activities associated with the onsite triage process are distinct from and precursor to those related to offsite triage process and have different requirements. It should also be noted that the FTSTPM does not negate the ability that the digital sources be transported back to a DFL for a more detailed analysis once the onsite triage process is completed. The FTSTPM is based on a set of forensically sound Overriding Principles and at the same time is sensitive to time limits. The proposed model provides the additional advantage of having a feedback loop with the investigators. Thus, this will allow the digital forensic examiners to adapt their searches on the basis of input from the primary investigators and those who interact with the suspect directly.

3. TRIAGE

Within the digital forensic community, there has been a lack of clarity regarding the process of triage resulting in legitimate concerns amongst the researchers. The term "triage" is poorly defined and denotes different things to different individuals [6, 7]. For example, some digital forensic investigators in [1] and [8] refer to the initial investigative activities carried out at the crime scene as triage before admitting the digital media as evidence. In contrasts, others [2, 3] might refer to the triage as the process of case acceptance or case prioritization to deal with the case backlogs in DFLs.

Based on the existing research, there are two types of digital forensic triage including 'onsite triage' conducted at the crime scene and 'offsite triage' performed in a DFL. Onsite triage refers to the practice of conducting certain investigative processes at the crime scene to identify and examine data contained in a digital device in the shortest possible time. In contrast, offsite triage, in general, pertains to the practice of removing the digital devices from the process of forensic analysis or simply prioritizing the order in which computer systems are analyzed through administrative and/or technical means. The administrative triage entails assessing any request for digital forensic services by assigning points to a case based on a matrix system either to reject the request or to identify digital devices in the submission most likely to produce evidential material. Conversely, the technical triage process implicates the usage of software to identify digital devices that contain potential evidence.

3.1 Context for Performing Triage

The triage process could be carried out at any of the following three stages in time:

- At the point of search and seizure
- On arrival at the local station
- On submission to a High-Tec Digital Forensic Crime Unit

The choice to decide at what point the triage process should be carried out will depend on the level of the risk which a given police force is prepared to take. The followings are some considerations that the police force needs to make:

- The less training that the investigator possesses and the less frequently they undertake triage process, the greater the risk of failure will be.
- The further from the unit the triage process is conducted, the lesser control and scrutiny can be exercised by the experienced investigator.
- The process of triage at the point of seizure often involves the utmost risk as the process is likely to be undertaken by the least experienced staff, in a stressful and possibly hostile environment, with a limited time in which the triage needs to be carried out and equipped with the most basic technical knowledge to make difficult judgments.

The research presented in this paper focuses only on onsite triage process – at the point of search and seizure – and proposes a two-stage process model to facilitate the quick identification and examination of digital evidence at the crime scene. It is argued that the proposed model will negate many of the existing concerns related to the 'onsite' triage process and can be applied to different cases at the crime scene.

3.2 Definition of Triage

In order to be able to engage with the concerns associated with the triage process properly, first it is important to define what triage actually means. Cambridge Dictionary [9] defines the triage as, "the process of quickly examining patients who are taken to a hospital in order to decide which ones are the most seriously ill and must be treated first". In the context of digital forensics within the domain of "law enforcement", the following definitions have been associated with 'onsite' triage,

> *Those investigative processes that are conducted within the first few hours of an investigation, that provide information used during the suspect interview and search execution phase [1]; A process for sorting enquiries into groups based on the need for or likely benefit from examination [3]. Triage is used when limited resources must be allocated [3]; Forensic triage is defined as the process of expeditiously acquiring important evidence at the crime scene in a limited but accurate manner [2].*

A common theme that emerges from the various definitions of triage is the need for an "urgent attention" or "urgency" towards a problem under time and resource constraints. Therefore, based upon the above definitions, we provide an all-inclusive definition of triage as follow:

> A limited forensic examination carried out at the crime scene under significant time and resource constraints in order to obtain critical information swiftly to provide the primary investigators with the investigative leads and best available information so that they can make decisions concerning the direction that the investigation should take.

Triage often might be wrongly considered by many as a separate effort which is not formally linked to the main digital forensic investigation. However, the triage process is virtually identical to early forensic investigative activities, and it closely follows what knowledgeable digital forensic investigators do with a digital media under investigation in the beginning. Considering more time, triage evolves into more detailed and broader digital forensics. Therefore, it would not be appropriate to formulate and define triage as a totally disconnected process. Moreover, it is imperative for the digital forensic investigators to take into account non-forensic aspects of an investigation including the severity of crime, cases circumstances and type of evidence sought and applicability of digital evidence. Despite the fact that information acquired from onsite triage examination might address certain questions in a case, it is often just the starting point in an investigation.

4. METHODOLOGY

In order to create a consistent research environment and to carry out a successful research, various methodologies were considered. However, it was decided to utilise the Design Science Research Process (DSRP) by Peffers et al. [10] over other alternatives due to the fact that it is especially suited for the task of designing and developing a new process model. The author in [11] states that design science is an ideal approach in the problem domain of digital forensic evidence with its focus on designing solutions. The DSRP is related to the development and subsequent evaluation of IT artifacts within an organizational environment in order to solve specific problems. The artifacts in question can consist of models, constructs and methods [12]. Also, to represent the FTSTPM in a uniform manner, various visual and formal representations were considered including: UML Activity Diagrams, Use Case Diagrams and Finite State Machines. However, it was decided to use Activity Diagrams based on the Sequential Logic formulated by Nair in [13]. According to the Sequential Logic, in order for the “circuit” to evaluate true, all the conditions of the previous states must be true [14]. This denotes that the circuit will fail if the current state is not positively completed. For the purposes of this research, the author has modified the Sequential Logic so that the “circuit” can be replaced with the processes included in the FTSTPM. Therefore, because the ordering of the processes in the FTSTPM is critical – as the output of one process becomes an input to the following process – it was decided to use this representation. This will enable the investigator to backtrack to previous steps in the process; however, they will not be able to continue if a step is not complete or fails.

5. THE PROPOSED MODEL

The requirement for a generic DFIPM has been acknowledged in numerous studies as a fundamental factor of a practical approach for investigations within the domain of law enforcement [1], [5], [15, 16]. Considering such a requirement, the components included in the proposed model have been intentionally selected and built upon as higher order categories to allow the process model to be generic across different types of digital forensic investigations. In the FTSTPM, phases are obvious and individually separate steps; they can sometimes be a function of time and therefore can be sequential, parallel or sometimes iterative. The output of a given phase will become the input to the following phase. Being able to carry out an onsite triage in a short period of time and provide primary investigators with time sensitive leads and information could provide a prevailing psychological benefit to the investigative team. Therefore, the focus of the proposed model is:

- to obtain actionable intelligence and recover applicable evidence in urgent circumstances such as missing persons;
- to identify victims that might be at severe risk;

- to ascertain the most valuable sources of digital evidence related to an investigation at the crime scene;
- to assess the offender's possible danger to society [1];
- to assess the severity of a crime and prioritizing it accordingly for a detailed forensic laboratory analysis;
- to decide whether the digital device under investigation needs a more detailed examination such as recovery of deleted information; and
- at the same time, to maintain the integrity of the potential digital evidence for subsequent processing in the investigation.

5.1 Stage 1: The Planning Process

The first stage in the FTSTPM is proper prior planning. Before deciding the most effective and efficient method of conducting the onsite triage activities, there are several considerations that need to be made. These considerations must be made through a well-though-out and robust planning which can ensure the success and efficiency of the onsite triage activities. Planning Process is one of the most important processes in a digital investigation and is often common across different fields in which digital forensic investigators operate. The authors in [17] emphasize the importance of this process stating that it is very important that the number of computers, their types, operating systems and connections are all known before entering the scene of crime [17]. Although this might be true to a large extent in an ideal world, the investigators often have little clue about the computer systems, quantity and location of data, types of hard disk or the operating systems involved, prior to visiting the crime scene. Also because the initial information concerning specific online environment might be scarce, insufficient or imprecise, the Planning Process must therefore focus on preparing for as many likely scenarios as possible [18]. Therefore, it would be unreasonable to expect the digital forensic investigators to produce anything beyond a rough outline of a plan at this stage of investigation.

The components included in the Planning stage of the FTSTPM are mainly aimed at the steps that digital forensic investigators should undertake when conducting an onsite triage examination. Various considerations need to be made at this stage even though the investigators have little understanding of what they should expect. These include: constructing the relevant procedures, defining methodologies, the choice of tools to be used and planning for the use of appropriate human resources that should be involved in conducting the onsite triage. Moreover, digital forensic investigators should also plan for the use of on-scene processing of digital evidence. For example, when an on-scene examination of a digital system will be required in cases of child abduction, or when the digital investigators do not have authority to seize every computer system, digital investigators must perform on-scene keyword searching of many computers to identify which ones are relevant to the investigation. Since it is not feasible to develop specific planning tailored to every possible situation [19], the Planning Process in the FTSTPM has focused on generic activities so that it can be suitable for different investigations. It should be noted that in circumstances where the digital device has already been seized by the law enforcement officers and presented to the laboratory for examination, this process will become brief as it will not be necessary to preform many of its activities. During the Planning stage, several sets of constraints will need to be considered, and various decisions need to be made. The following sections describe these sets of constraints followed by Figure 2, representing the formal UML representation of the Planning stage of the FTSTPM.

1) Consider Legal Issues

The digital forensic investigators need to ensure that they have the proper authorisation to be able to conduct the work. The type of authorisation required for an investigation to proceed will not be known unless the type of investigation is determined first. The authorisation should be the authority in law and authority from the owner of the resources which contain the material to be acquired. Investigators will need to confirm the details of the proper authorization and any restrictions imposed. Moreover, the investigators will need to examine any court orders closely allowing access to a third- party's property. This is because if the investigators conduct any action that is not allowed by the law, they may become the subject of lawsuit. If the digital forensic investigators discover materials which are covered by the criminal law such as child pornography, they will need to inform the primary investigators immediately so that the appropriate actions can be taken. With regards to the legal issues, the authors in [1] state that the primary investigator would need to address the following questions:

- Does the warrant allow for the seizure and removal of the system under investigation?
- Does there exist adequate particularity contained in the warrant that allows for an onsite or "in situ" examination?
- What are the reporting duties that the primary investigator has to the issuing magistrate or judge?
- Does there exist particular discovery issues present or predicted?
- Does the onsite examination affect the integrity of the original evidence?

Therefore, it is only after the primary investigator has been able to address the above questions and other stated potential legal issues that the investigators can determine the possibility of applying the onsite triage activities included in the FTSTPM's Onsite Triage Examination Process. Such legal considerations require the investigators (often the case officer) to work with the legal practitioners throughout the entire case.

2) Consider Operational Issues

With regards to the operational considerations, the primary investigator would need to determine the followings:

- What type of case is involved?
- How critical is the time factor?
- What level of skills and abilities do the digital forensic investigators possess?
- What kind of system is involved, for example standalone systems or complex networks, etc.?
- Can the crime scene be safely secured?
- What level of technical skill and knowledge does the suspect have?
- Are the digital forensic investigators in possession of appropriate tools for onsite data acquisition and examination?

Similar to the legal considerations, the digital forensic investigators will need to address the above questions concerning the operational considerations before deciding to apply onsite triage activities included in the FTSTPM's Onsite Triage Examination Process.

3) Consider Physical Constraint

The Physical Constraint refers to the access to the physical location of the system in which data is held. Previous research has paid little attention to the importance of the physical constraint in a digital forensic investigation [1], [20, 21, 22]. Due to the fact that investigators might encounter more than one location where data can be found, 'Consider Physical Constraint Phase' has been assigned a discrete phase in the Planning Process of the FTSTPM. The Physical Constraint Phase consists of two sub-phases, namely 'Access to Property' and 'Multiple Locations', which need to be considered prior to raiding the crime scene. Access to Property involves physical access to the resources where the data is being contained. The need to have a physical access to the resources containing data is the case in the majority of circumstances. However, obviously, there are cases in which data can be accessed through Internet or external networks. In terms of the 'Multiple Locations', commercial buildings often have security measures in place necessitating keys, cards or door access codes to allow the access to the building. Private sites might have restricted access and parking which have security gates. Therefore, the lawyers will need to discuss the entry with the occupants so that they can enter and serve the instructions and initiate the Onsite Triage Examination Process.

4) Consider Timing Constraint

Consider Timing Constraint has been suggested as a phase within the Planning Process due to its significance. Although some of the previous research and standards discuss practical considerations to some extent [14], [23], [24], they do not include the timing as part of the planning. The FTSTPM requires the digital forensic investigators to consider the followings: the terms of court orders and warrant and accessing the premises before the suspect (the subject of court order) leaves for work or some other activities [16].

5) Consider Data Constraint

In the context of this paper, data is the digital information which represents the potential digital evidence that is the subject of the onsite triage examination process. Data can take various forms such as a text file, a still image and video or audio file etc. It is not often obvious at the beginning whether there will be any data associated with the investigation or where this data can indeed be found.

6) Create Outline Plan

The output of the Planning stage must be the creation of an outline plan. Due to the fact that digital forensic investigators have not yet attended and surveyed the crime scene at this stage, only a rational prediction can be made with certain contingency plans being put in place. Some researchers have previously considered the creation of the outline plan. For example, authors in [17] implicitly refer to the creation of the outline plan by discussing “Search Briefing”. According to the authors [17], the digital forensic investigators should be able to address the following questions:

1. How many trained personnel are needed?
2. How many teams are required, where do they need to be and at what time?
3. How many sets of equipment are required and what should be in the toolkits?
4. What specialist skills are required?

The authors in [16] are more explicit about the need for the creation of an outline plan and suggest six main types of activities as follows:

- Number of trained investigators needed;
- The type and set of equipment needed at each site including software, dongles, write-blockers and image storage media;
- Start time at each site and the estimate of duration of acquisition stage;
- Details of personnel involved including contact numbers of team leaders, lawyers and client liaison distributed; and
- Acquisition plan detailing target storage locations, protocol and key words.

Providing the details about what needs to be included in the toolkit that should be taken to the crime scene is beyond the scope of this paper. Valuable resources providing detailed description of what equipment needs to be taken onsite can be found in the research conducted by the authors in [17, 18], [25]. It is argued that the content of the toolkit which needs to be taken to the crime scene should be determined by the digital forensic investigators themselves based on their units’ Standard Operating Procedures.

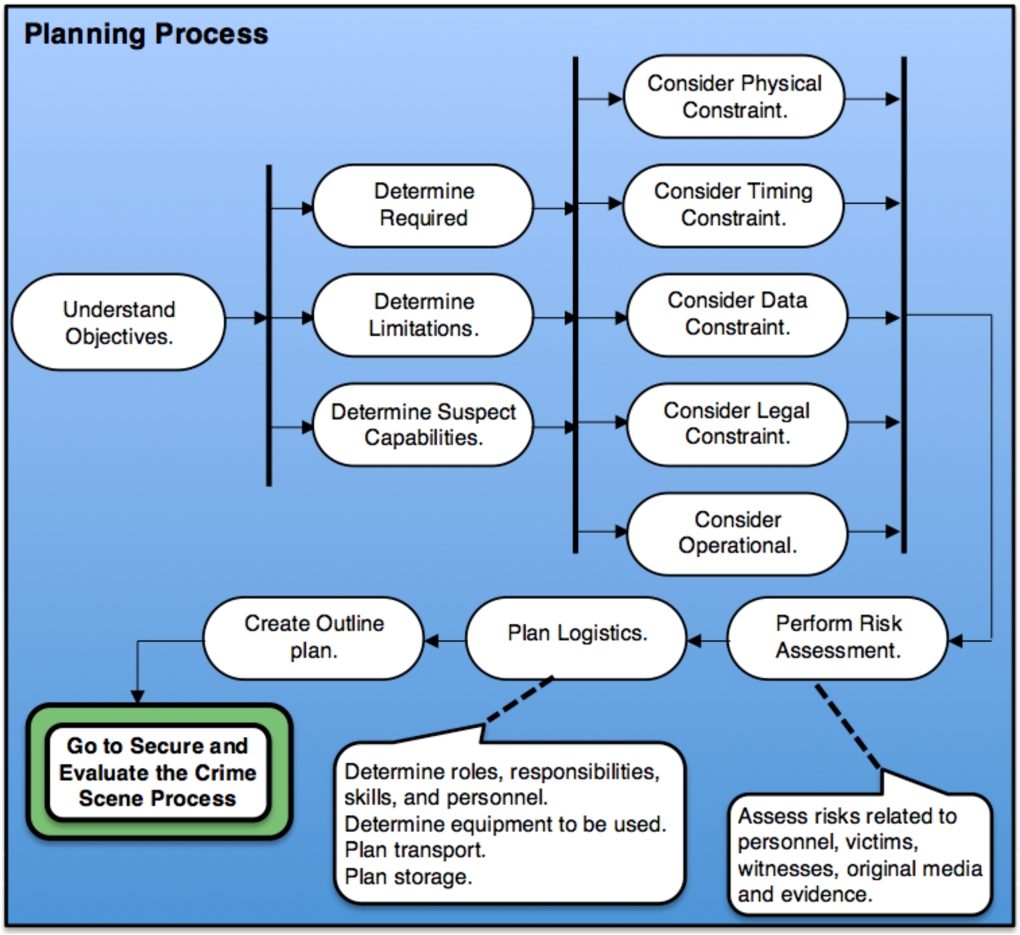
Planning Process
Understand Objectives.
Determine Required
Determine Limitations.
Determine Suspect Capabilities.
Consider Physical Constraint.
Consider Timing Constraint.
Consider Data Constraint.
Consider Legal Constraint.
Consider Operational.
Perform Risk Assessment.
Plan Logistics.
Create Outline plan.
Go to Secure and Evaluate the Crime Scene Process
Determine roles, responsibilities, skills, and personnel.
Determine equipment to be used.
Plan transport.
Plan storage.
Assess risks related to personnel, victims, witnesses, original media and evidence.

FIGURE 2: Formal representation of the Planning stage of the FTSTPM.

5.2 Stage 2: The Onsite Triage Examination Process

Once the proper planning has been finalized, the investigators will need to attend the crime scene where the investigative process moves to those phases that directly deal with the actual suspect and the crime scene. In this stage, all the gaps in knowledge with regards to the location, size and format of digital systems containing the digital data are filled in and the plan for the subsequent Acquisition Process is created. Many of the existing models have not paid any attention to the onsite triage examination. They have often sufficed their discussions simply to the fact that digital evidence needs to be identified and acquired without providing any details concerning onsite triage. Although some authors such as Casey [24] discuss preserving the crime scene to some extent, no explicit process has been designed to accommodate the activities related to onsite triage. Therefore, the Onsite Triage Examination Process incorporated into the FTSTPM has been developed in order to guide the digital forensic investigators on the steps that they will need to take when conducting the onsite triage. This process is another novel contribution of this research to the field of digital forensics.

During this stage, digital forensic investigators will need to make certain immediate decisions about a digital device as a potential source of evidence before applying any forensic procedure. These decisions relate to whether the device might contain the information that they are seeking, whether an onsite triage inspection will still be appropriate and conducive or whether the digital device should be transported back to the DFL for a detailed analysis. From the start of the Onsite Triage Examination Process, witness statement, case background or even the suspect interview might suggest that relevant information is stored on the device, or the nature of the crime might suggest that a digital device was involved. During this stage, the investigators must evaluate the possible significance of a particular computer system as a source of evidence and determine the most effective approach for dealing with a particular device. Therefore, it is necessary for the investigators to have proper training to identify the devices that are more probable to contain the evidence that they seek and to extract this information swiftly. Onsite triage might reveal that the desired or predicted data is not contained in the device. In these circumstances, the digital forensic investigators must determine whether more detailed forensic techniques available at a DFL should be carried out on the device. For example, when the investigators seek to determine whether a private browsing mode has been utilized or not, specialized tools and methods will be required [26]. In such situations, it might be necessary to transport back the computer to a DFL in which a detailed forensic analysis should be carried out to acquire and analyze the 'uncommon' locations on the computer system such as swap files.

For the remainder of the discussion, it is assumed that the crime scene has been properly secured and evaluated. Here, the scene refers to both physical and digital scene [1], [27]. It is also assumed that the digital forensic investigators have brought a forensic examination workstation or laptop and have access to appropriate software tools such as EnCase and FTK. Another assumption is that the digital forensic investigators have access to a hardware write blocker so that any storage media that is examined is done so in read only mode to ensure that no contamination is occurring. This will allow the investigators to maintain the integrity of the potential digital evidence. Figure 3 is the formal UML representation of the Onsite Triage stage of the FTSTPM.

1) Interview the Suspect

Interviewing the suspects is an extremely important aspect of the Onsite Triage Examination Process. Suspects often would be "psychologically more vulnerable" within the first few hours of their initial encounter with police particularly when this encounter takes place in their place of business or dwellings [28, 29]. They would tend to be more compliant and open to answering the police questions even after they have been "mirandized". In this regard, the authors in [30] state that often in the initial minutes of the investigation, suspects tend to be more cooperative due to the psychological shock they have received. Similarly, Baldwin in [31] carried out a research in which he examined 600 taped police interviews of suspects in England and reported that in the majority of cases (80 per cent), suspects were thoroughly cooperative and answered police questions of any significance in the initial periods after the raid. At this stage into the investigation, what is critical to the investigators is the knowledge of the full extent of the crime or involvement of the suspect and "triggers that further increase the suspect's willingness to talk and cooperate" [1]. These triggers might originate in the digital evidence stored on the suspect's digital device such as email correspondence, digital maps, pictures and chat logs, etc. It is very important that the investigators and interviewers who are dealing directly with the suspect provide direct input to the digital forensic examiners at this stage. This ensures that correct prioritizations and assumptions are being made.

2) Preserve the Crime Scene

In order to demonstrate in a court of law that the activities associated with the onsite triage examination were carried out in a forensically sound manner, the digital forensic investigators must be able to show that the crime scene was preserved unaltered. Thus, if possible and practicable, the investigators must enforce a lock down of the entire crime scene in order to achieve what the author in [24] calls a "pristine environment". Other steps that the digital forensic investigators should take include preventing individuals from entering or leaving the crime scene, and preventing unauthorised people (including the suspect) from tampering with the digital device and materials under investigation. In terms of preserving the digital crime scene, this can include, but is not limited to, blocking the network connectivity. A computer system attached to a network that is running can be regarded as a fragile evidence due to the fact that its data representing potential digital evidence could be deleted with commands from a remote system. Examples of procedures to preserve the content of computer in this situation are to unplug the computer from the network when it is found or utilise a network monitor to view what data is being sent to the system until the full investigation begins.

3) Triage/ Prioritize

Due to the fact that time is a crucial aspect in the FTSTPM, it is extremely important that the digital forensic investigators perform some sort of initial prioritization in which items of evidence or potential containers of evidence that are the most important or the most volatile are dealt with first. The triage phase is central to the FTSTPM, and along with the appropriate planning, it is the foundation upon which all the other phases are built. During this phase, digital sources that might contain potential digital evidence will need to be identified and prioritised based upon the criteria of potential applicable evidence that can be acquired within a short period of time, and evidence with a short time to live (e.g. data in volatile memory, process tables, routing tables, temporary files systems).

4) Perform Onsite Examination

In order to assess a digital device suspected of containing potential digital evidence in a fast manner, a system which uses triage is needed. Such a system can limit the data acquired and examined. The examination process could be accelerated by intelligence driven data selection. For example, if the investigators are suspicious that the suspect is holding the indecent images of children, by cutting the search of data down only to images, the speed of the investigation will be accelerated substantially. In such situations, the rapid examination at the crime scene will enable the digital forensic investigators to gather the evidence that they need for charging the suspect. During the Onsite Examination Phase, various locations on the computer system will need to be examined. It is outside the scope of this paper to provide an exhaustive list of these locations, nor is it in the scope of this paper to give a detailed explanation of the following examples of such locations which include, but are not limited to: user profiles, home directory, file properties, windows registry, chronology and internet usage.

a) User Profile

After a computer system has been identified and prioritised, the actual examination is carried out. If an incriminating evidence is recovered from the storage media, it is very important for the digital forensic investigators to be able to demonstrate a link between that evidence and an identifiable suspect, as in some cases multiple persons have access to the same PC. This will be a great challenge considering the fact that this process needs to be conducted expeditiously to determine whether this can even be done within the time constraints. The speed at which these items can be assessed will vary widely depending on case specifics, available tools, and specific knowledge and experience of the examiner [1].

b) Windows Registry

The Windows registry contains a very large amount of systems and user behaviour meta data and often holds trace data well beyond its intended duration. Therefore, it should be a main candidate for inclusion in any triage examination process.

c) Chronology

The chronological scope of an investigation can be defined by the case intelligence [1]. In a given investigation, digital evidence is defined by its temporal value, known as MAC. After the digital forensic investigators have accessed the files under investigation and their MAC times, they can begin to qualify their searches, therefore, quantifying their evidence [24]. Digital forensic investigators will need to examine the time periods of normal use by the suspect and other known users of the computer or device. This can be achieved by linking known users accessing the computer system with files that have been modified, accessed or created during those times [1], [32]. Moreover, digital forensic investigators will need to identify and analyse software applications and data files used or accessed during qualified times of interest [24]. Again this can be achieved by relating known users with MAC times possibly providing unique time periods that could be of significant value.

d) Internet-Related Artefacts

Digital forensic investigators will also need to examine artefacts related to the internet activities such as web browsing and e-mail, etc. The value, time cost, and time criticality will vary widely, depending on circumstances including the specific applications involved, type of activity being examined, and whether the computer system under examination belongs to a suspect or a victim (e.g., in a missing persons case). An effective practice is for the computer forensic examiner to evaluate what type of Internet activities they believe the suspect (or victim) was involved in, and to evaluate if and how each of those activities relates to the case [1].

e) Internet-Related Artefacts

One of the most significant factors in an onsite triage examination is that the digital forensic investigators should be able to adjust the focus of every investigation to the specifics of that case. There exists various practices that can pave the way for an effective improvement of resources. Digital forensic investigators should be able to assess time resources, use pre-raid intelligence, modify search goals and prioritise search goals. Often time is the shortest supply out of all the other resources available to the investigators. The time value of any onsite triage examination activity must be considered in relation to the potential for productive results of that activity. Moreover, the value of the activities discussed in the Planning Process of the FTSTPM as well as pre-raid intelligence cannot be over-emphasised. Effective planning as well as reliable intelligence on search terms, contacts, types of activities, applications used, etc. prior to the search can enable the digital forensic investigators to develop effective strategies prior to arriving at the crime scene.

f) Update Outline Plan

After carrying out all the phases in the Onsite Triage Examination Process, the investigators will need to review and update the outline plan now that its various assumptions can be assessed. Often, there will exist areas of plan that could not be completed at all before attending the crime scene where digital data can be found.

5) Document the Scene

It is extremely important to document every aspect of the triage examination process in order to enable other investigators to authenticate the process and results. Thus, it is imperative to maintain a detailed record of what was performed on the computer system and what information was acquired. Maintaining a detailed documentation will enable the digital forensic investigators to preserve the chain of custody and increase the possibility of a successful investigation. Furthermore, documentation will enable the digital forensic investigators to record all information produced during the triage process to support decision making and the legal, administrative processing of those decisions.

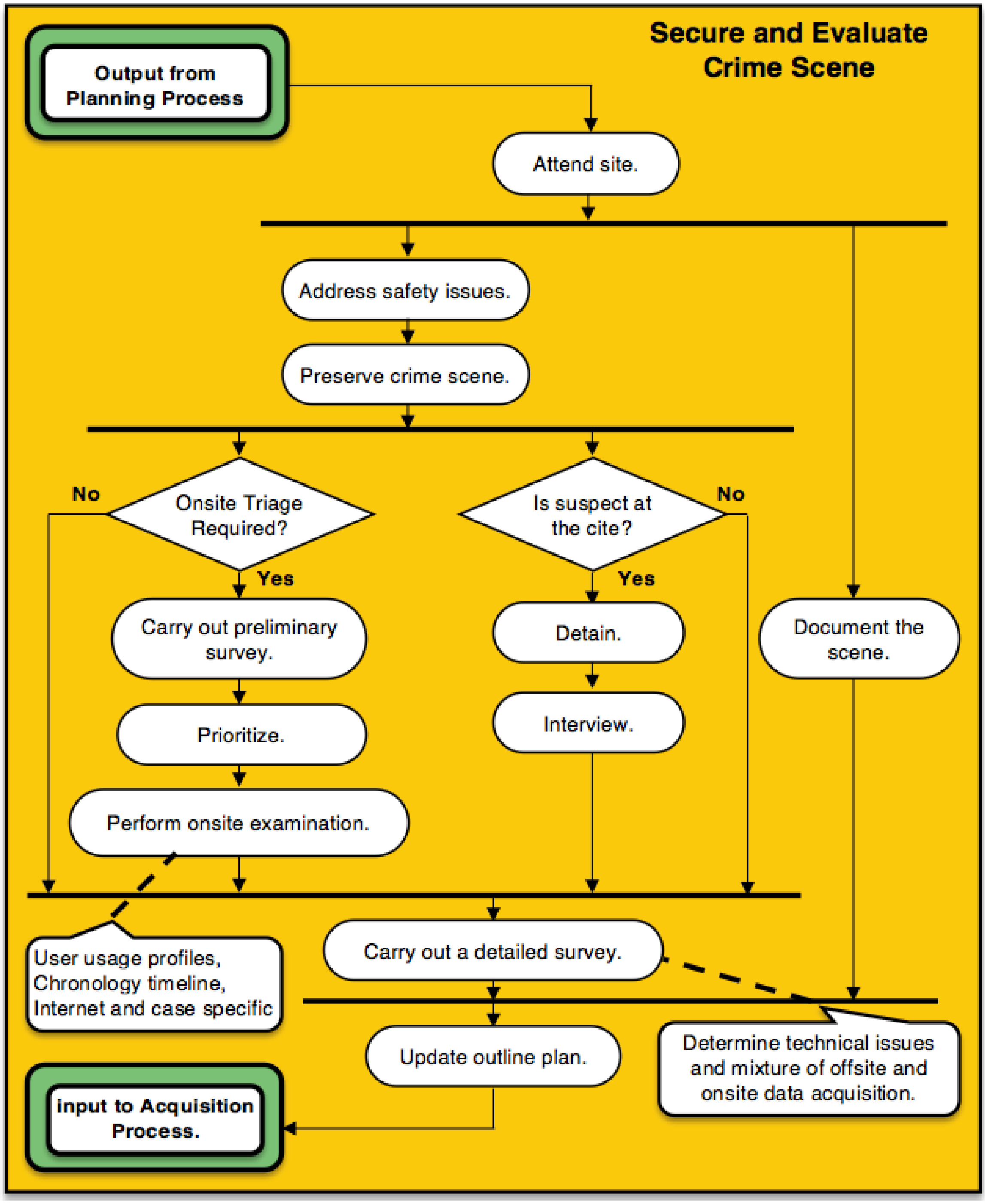
Secure and Evaluate Crime Scene
Output from Planning Process
Attend site.
Address safety issues.
Preserve crime scene.
No
Onsite Triage Required?
Yes
Is suspect at the cite?
No
Yes
Carry out preliminary survey.
Detain.
Document the scene.
Prioritize.
Interview.
Perform onsite examination.
User usage profiles, Chronology timeline, Internet and case specific
Carry out a detailed survey.
Update outline plan.
Determine technical issues and mixture of offsite and onsite data acquisition.
input to Acquisition Process.

FIGURE 3: Formal representation of the Onsite Triage Examination stage of the FTSTPM.

6) *FTSTPM's Overriding Principles*

As well as the formal UML representations of the FTSTPM, a set of Overriding Principles have also been developed in order to enable the digital forensic investigators to gather solid evidence that can be relied upon by the decision makers whether they are in a court room or board room. These actionable principles are objectives that need to be achieved in a given digital forensic investigation. The authors in [33] state that any approach for carrying out the triage examination must preserve the reliability, completeness, accuracy and verifiability of computer system evidence [33]. Therefore, the following Overriding Principles are proposed as a standard requirement for triage examination of computer systems:

1. preserve chain of custody;
2. maintain an accurate audit trail;
3. maintain a restricted access control;
4. maintain an effective case management; and
5. maintain information flow.

Since the FTSTPM is aimed at the United Kingdom's jurisdiction, the above suggested principles have been based on ACPO Good Practice Guide [34], ISO/IEC 27043 [23] and ISO/IEC 27037 [35] Standards. Due to the FTSTPM's Overriding Principles, it is argued that the model observes the forensic principles of minimizing the contamination of the original crime scene and evidence, preserving the integrity of digital evidence, preserving the chain of custody of evidence and adhering to the rules of evidence for admissibility in courts of law. Each Overriding Principle in the triage examination process is discussed below:

a) Preserve Chain of Custody

n order to affirm the integrity of any evidence seized in an investigation, it is extremely important to maintain a detailed and accurate list documenting the chain of custody. A detailed documentation of the chain of custody becomes even more important in the investigations that will result in courts of law. The chain of custody in any investigation must initiate with a list that describes the followings:

- The digital devices that were seized;
- The date and time of seizure;
- The place where the devices were located; and
- The person responsible for initially seizing the device.

The person who is in charge of the custody of the evidence must be responsible for maintaining a detailed record of every individual who interacts with every single evidentiary item. For example, if an individual checks out a digital device, the record should contain notes regarding the followings:

- the person who is handing over and the person who is receiving the custody of the device;
- the date and time when the device was checked out;
- the purpose for which the device was checked out; and
- the date and time when the device was returned.

The documentation pertaining to the chain of custody is vital to maintain evidentiary integrity. Without such documentation, it will be impossible to discredit a claim that an unauthorised individual had an access and probably tampered with the evidence. Although the existence of chain of custody on its own cannot conclusively demonstrate that no individual tampered with evidence, at the same time, lack of such documentation will cause the evidence to be challenged.

b) Maintain an Accurate Audit Trail

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

c) Maintain a Restricted Access Control

This actionable principle refers to both limited acquisition of digital data as well as restricted viewing of the data. Triage tools must support restricted viewings of results in order to increase their utility and limit privacy concerns [2], [36]. With the appropriate technology utilised, the triage examination tool could determine to provide a positive or negative sign that certain types of data are contained in the digital device. For instance, if the computer contains indecent images of children, the triage examination tool could simply report that such contraband is likely to be present without actually showing the images or videos.

d) Maintain an Effective Case Management

This Overriding Principle applies to the role of case officer or the primary investigator who often leads a team of investigators during an investigation. There are certain tasks that the primary investigators will need to undertake during a digital forensic investigation. These include, but are not limited to: guiding the investigators in the right direction, creating an overall picture of the investigation, determining the cost of investigation and identifying team members for the Onsite Triage Examination Process, etc.

e) Maintain an 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. A defined information flow should exist between each given process in a digital investigation and between different stakeholders. The author in [37], state that information flow has to be defined for each type of investigation and emphasises the need to identify and describe information flows within a digital investigation process model so that they can be protected and supported technologically [37]. An example of the Information Flow can be the exchange of digital evidence between two investigators involved in the same investigation. This Information Flow can be protected, for example, through the use of trusted public key infrastructures (PKI) and time stamping to identify the different investigators, protect the evidence integrity and also protect the confidentiality of the evidence through PKI-based encryption. Therefore, due to its importance, Information Flow Principle must be managed carefully during the two stages of the FTSTPM.

6. EVALUATION

In order for a process model to be valid, it has to adhere to guiding principles around which the process is organised. The model has usability if its targeted audience, in this case digital forensic examiners, can apply it in real scenarios to arrange and sequence their activities to move through the process and produce the required outcomes readily and efficiently [16]. The process model has descriptive power if it directs the process, suggests some courses of action and cautions against the others. The descriptive power of the model has been derived from the UML Activity Diagrams for the two stages of the FTSTPM and its associated Overriding Principles. FTSTPM was also subjected to an independent evaluation of this descriptive power to determine whether the model is usable. The evaluation process recruited two sets of independent experts whose feedback was taken onto account and subsequent changes were made to the FTSTPM. The external reviewers involved in evaluating the FTSTPM consisted of experts (in academia and industry), practitioners (the head of a law enforcement's high-tech crime unit) as well as judiciary personnel (a judge and a barrister) who have comprehensive skills, interest and experience in the area of digital forensics.

The development of the FTSTPM was originally guided by the feedback that the author received concerning a much larger process model, namely CDFIPM. The external evaluation of the original CDFIPM highlighted the need to design and develop an additional stage within the model to accommodate activities related to onsite triage examination process. Having acquired feedbacks from the experts and practitioners, the digital forensic activities related to onsite triage needed to be articulated and structured into a new formal process model, the FTSTPM. Thus, the development of the FTSTPM, was implemented to contribute towards addressing the shortcomings identified in the CDFIPM. The FTSTPM is in accordance with recommended best practice as detailed in [23, 34, 35]. Although the FTSTPM presented in this paper has been primarily focused on the United Kingdom's jurisdiction, it could be utilised as the foundation of a process model that is relevant in other jurisdictions with only slight modifications.

6.1 Comparison of the FTSTPM with the Existing Models

Having evaluated the FTSTPM by experts in its intended user community, it was also needed to map the proposed model against the existing models in order to determine how it would compare against those models. Notice that although there exist a large number of digital forensic investigation process models (Valjarevic and venter, 2015; Adams et al., 2014; Kohn et al.; 2013; Agarwal et al., 2011; Cohen, 2009; Beebe and Clark, 2005; Ciardhuáin, 2004; Carrier and Spafford., 2003; Reith et al., 2002; Palmer, 2001, etc.), there is only one model proposed by Rogers et al. (2006) that has "specifically" focused on Onsite Triage. Therefore, in order to avoid comparing "apple" against "orange", the FTSTPM was mapped only against those existing models that have incorporated components that can be relevant to Onsite Triage. The results of mapping the FTSTPM against previous models are presented in Table 1 within Appendix A. Based on this comparison, it is claimed that the FTSTPM is both detailed and comprehensive in relation to activities associated with Onsite Triage. The FTSTPM not only has merged the previously proposed models that have relevance to Onsite triage but also has extensively built upon those models. In The activities without a "tick'' symbols highlighted in "yellow" are the contributions of this research paper. These activities are missing in the previously proposed models that have relevance to Onsite Triage. Moreover, the proposed model has also introduced a set of investigative principles classified into a group entitled "Overriding Principles", that are further contributions of this research paper.

7. DISCUSSION

The research presented in this paper offers a detailed and multi-layer model that will assist investigators in terms of how and where to find digital evidence. The proposed FTSTPM provides unique benefits over the previous models in relation to practicality and specificity. The existing modes lack adequate level of details, if any, required to attain practicality for investigators in relation to Onsite Triage. It is argued that the Onsite Triage activities carried out on site using the FTSTPM would be forensically sound, maintain chain of custody, and adhere to the rules for the admissibility of evidence. One of the greatest advantages of the FTSTPM is that it is inclusive of all the benefits of the previously proposed models that have relevant components associated with Onsite Triage activities, which makes the FTSTPM consistent with the existing models. Other benefits of employing the proposed model include acquiring digital evidence in a swift manner within minutes as opposed to days or weeks without undermining the admissibility of digital evidence in a court of law. Moreover, employing the proposed model does not negate the ability that once Onsite Triage has been completed, the digital device be transported back to a DFL for further examination and analysis.

8. CONCLUSION AND FUTURE WORK

The growing number of digital devices being seized that potentially contain valuable evidence is creating backlogs in DFLs that adversely impact public safety and the criminal justice system. Also, in cases of the missing persons, delays in acquiring intelligence from the digital devices can significantly affect the person's safety. In order to address this issue, effective methods formulated into the proposed Formal Two-Stage Triage Process Model were proposed that digital forensic investigators could use to preform effective onsite triage examinations in a timely manner. The FTSTPM focuses strictly on the legal requirements of digital investigators, allowing for the extraction of information that could be swiftly made use of by investigators as opposed to waiting for the same data to be acquired at a DFL. The model has been designed and developed in such a generic way that it can be applied for various types of investigations. Moreover, due to its systematic approach, the proposed model will assist law enforcement agencies in swiftly acquiring the intelligence that is needed to assist and expedite the overall investigation. A side benefit of the FTSTPM is economic as it will enable the law enforcement agencies to limit personnel and resources in an optimal manner. By employing the model, the investigators might eradicate the need to transport the digital device back to a DFL and therefore avoid adding to the case backlogs of digital devices in DFLs. Meanwhile, the FTSTPM does not negate the ability that once the onsite triage examination has been completed, the digital device be transported back to the DFL for a detailed analysis. It is also argued that the model will enable the investigators to increase the consistency of results and reduce the risk of relevant evidence being disregarded. Finally, the FTSTPM facilitates the swift and targeted review of easily accessible items to provide the investigators with the most valuable information in the least amount of time.

The research presented in this paper is admittedly incomplete in that it only accommodates activities for Onsite Triage. The proposed FTSTPM would need to be applied to a number of cases studies with a systematic approach in order to optimize its further development process. In terms of future work, it is acknowledged that some limitations of the work remain. Although the FTSTPM has already been evaluated by a police force high-tech crime unit (HTCU), this cannot be representative of all the HTCUs within the United Kingdom. Therefore, the future work should include a more comprehensive trial by digital forensic investigators as part of a wider study. The future work could also involve the extension of the FTSTPM to cover activities also related to a traditional examination and analysis back at the forensic laboratory to make a more precise determination of events and evidentiary locations in a more controlled environment.

9. REFERENCES

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

[2] Mislan, R., Casey, E. and Kessler, G (2010). ‘The growing need for on- scene triage of mobile devices’, Digital Investigation, 6 (3), pp. 112- 124.

[3] Parsonage, H (2009). ‘Computer forensics Case Assessment and Triage’ Available at: http://computerforensics.parsonage.co.uk/triage/triage.htm (Accessed: 22nd February 2016).

[4] Casey, E, Ferraro, M. and Nguyen, L (2009). ‘Investigation delayed is justice denied: proposals for expediting forensic examinations of digital evidence’, Journal of Forensic Sciences, 54 (6), pp. 1353-1364.

[5] Montasari, R., Peltola, P. and Evans, D. (2015). ‘Integrated computer forensics investigation process model (ICFIPM) for computer crime investigations’, Proceedings of 10th International Conference on Global Security, Safety and Sustainability: Tomorrow's Challenges of Cyber Security, pp.83–95.

[6] Shaw, A. and Browne, A. (2013). ‘A practical and robust approach to coping with large volumes of data submitted for digital forensic examination’, Digital Investigation, 10 (2), pp. 116-128.

[7] Roussev, V., Quates, C. and Martell, R (2013). ‘Real-time digital forensics and triage’, Digital Investigations, 10 (2), pp. 158-167.

[8] Hong, I., Yu, H., Lee, S. and Lee, K. (2013). ‘A new triage model conforming to the needs of selective search and seizure of electronic evidence’, Digital Investigation, 10(2), pp. 175-192.

[9] Cambridge Dictionary Online (2016). ‘Triage’ Available at: http://dictionary.cambridge.org/dictionary/english/triage (Accessed: 25th February 2016).

[10] Peffers, K., Tuunanen, T., Gengler, C., Rossi, M., Hui, W., Virtanen, V. and Bragge, J. (2006). ‘The Design Science Research Process: A Model for Producing and Presenting Information Systems Research’, The First International Conference on Design Science Research in Information Systems and Technology, pp. 83-106.

[11] Armstrong, C. and Armstrong, H. (2010) ‘Modeling Forensic Evidence Systems Using Design Science’, In Human Benefit through the Diffusion of Information Systems Design Science Research, pp. 282-300.

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

[13] Nair, B.S.(2006). Digital Electronics and Logic Design, (6th ed.),Prentice Hall, New Delhi.

[14] Kohn, M., Eloff, M. and Eloff, J. (2013). ‘Integrated digital forensic process model’, Computers and Security, Vol. 38, pp.103–115.

[15] Valjarevic, A. and Venter, H (2015). ‘A comprehensive and harmonized digital forensic investigation process model’, Journal of Forensic Sciences, Vol. 60 (6), pp.1467–1483.

[16] 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.

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

[18] Brown, C. (2009). Computer Evidence: Collection and Preservation (2nd ed.): Charles River Media.

[19] Kent, K., Chevalier, S., Grance, T., and Dang, H. (2006). ‘Guide to integrating forensic techniques into incident response’, NIST Special Publication 800-86 Notes, pp. 1-20.

[20] Marcella, A. and Menendez, D. (2007). Cyber Forensics: A Field Manual for Collecting, Examining and Preserving Evidence of Computer Crimes (2nd ed.): Auerbach Publications.

[21] Wiles, J. and Reyes, A. (2007). The Best Damn Cybercrime and Digital Investigations Book Period: Syngress.

[22] Steel, C. (2006). Windows Forensics: The Field Guide for Conducting Corporate Computer Investigations: Wiley Publishing.

[23] ISO/IEC27043(2015).Incident Investigation Principles and Processes.

[24] Casey, E. (2011). Digital Evidence and Computer Crime Forensic Science Computers and The Internet (3rd ed.): California: Elsevier.

[25] Jones, K., Bejtlich, R. and Rose, C. (2005). Real Digital Forensics: Computer Security and Incident Response: Addison-Wesley.

[26] 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.

[27] Carrier, B. and Spafford, E (2003) ‘Getting Physical with the Digital Investigation Process’, International Journal of Digital Evidence, 2(2), pp. 1-20.

[28] Black, I. (2014). The art of investigative interviewing (3rd ed.), Boston: Butterworth Heinemann.

[29] Yeschke, C. (2002). The art of investigative interviewing: A Human Approach to Testimonial Evidence (2nd ed.), Boston: Butterworth Heinemann.

[30] Memon, A., Vrij, A. and Bull, R. (2003) Psychology and law: Truthfulness, accuracy and credibility, John Wiley & Sons.

[31] Baldwin, J (1993) ‘Police Interview Techniques Establishing Truth or Proof?’, British Journal of Criminology, 33(3), pp. 325-352.

[32] Farmer, D., Venema, W. (2005). Forensic Discovery. Boston, Addison- Wesley.

[33] Kenneally, E. and Brown, C. (2005). ‘Risk sensitive digital evidence collection’, Digital Investigation, 2 (2), pp. 101-119.

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

[35] ISO/IEC 27037 (2012). Guidelines for Identification, Collection, Acquisition, and Preservation of Digital Evidence.

[36] Orso, M (2009). ‘Cellular Phones, Warrantless Searches, and the New Frontier of Fourth Amendment Jurisprudence’, Santa Clara Law Review, 50, pp. 101-142.

[37] Ciardhuáin, O. (2004). ‘An extended model of cybercrime investigations’, International Journal of Digital Evidence, 3 (1), pp. 1- 22.

[38] Ciardhuáin, O. (2004). ‘A hierarchical, objectives-based framework for the digital investigations process’, Digital Investigation, 2 (2), pp. 147- 167.

Appendix A

Table 1. Mapping the FTSTPM against the previously proposed models.

Proposed Formal Two Stage Triage Process Model (FTSTPM)		Existing DFIPMs						
		Carrier and Spafford (2003)	Ciardhuáin (2004)	Beebe and Clark (2005)	Rogers et al. (2006)	Casey (2011)	Kohn et al. (2013)	Adams et al. (2014)
1. Planning Process	1.1 Understand objectives.							
	1.2 Determine required outcomes.							✓
	1.3 Determine limitations.							
	1.4 Determine the suspect count and capabilities.				✓			
	1.5 Consider physical constraint.	✓						✓
	1.6 Consider timing constraint.							✓
	1.7 Consider data constraint.							✓
	1.8 Consider legal issues.	✓	✓	✓	✓	✓	✓	✓
	1.9 Consider operational issues.	✓		✓			✓	
	1.10 Perform risk assessment.							
	1.11 Plan logistics.					✓		✓
	1.12 Create outline plan							✓
2. Secure and Evaluate the Crime Scene	2.1 Attend site.	✓	✓	✓	✓	✓		✓
	2.2 Address safety issues.							
	2.3 Preserve and secure crime scene.			✓				
	2.4 Perform onsite triage.				✓			
	2.5 Prioritise.				✓	✓		
	2.6 Preform onsite examination.							
	2.6.1 Examine user usage profile.				✓	✓		
	2.6.2 Examine chronology timeline.			✓	✓	✓		
	2.6.3 Examine Internet browsing activities.			✓	✓			
	2.6.4 Examine case specifics.				✓			
	2.7 Detain the suspect.				✓	✓		
	2.8 Interview the suspect.				✓	✓		
	2.9 Carry out a detailed survey.							
	2.10 Update outline plan.							✓
3. OP	3.1 Preserve chain of custody.	✓	✓	✓	✓	✓		✓
	3.2 Maintain an accurate audit trail.	✓	✓	✓				✓
	3.3 Maintain a restricted access control.							
	3.4 Maintain an effective case management.					✓		
	3.5 Maintain information flow.		✓					✓