Digital Forensics: An integrated approach

Conference Paper · September 2012

CITATIONS
2

READS
8,339

2 authors:

Moniphia Hewling
University of Bedfordshire
3 PUBLICATIONS **5** CITATIONS
SEE PROFILE

Paul Sant
University of Bedfordshire
56 PUBLICATIONS **461** CITATIONS
SEE PROFILE

Digital Forensics: An integrated approach

Moniphia Hewling
Institute for Research in Applicable Computing
University of Bedfordshire
Park Square
Luton, UK. LU1 3JU

moniphia.hewling@beds.ac.uk

Paul Sant
Department of Computing
University of Bedfordshire
Park Square
Luton, UK LU1 3JU

paul.sant@beds.ac.uk

Abstract

As cyber crimes become more pervasive in today's society, governments and private entities grapple with the need to implement control systems. Legislation, policies and guidelines are rapidly being developed by parliaments and boards in an effort to stop these crimes from spiraling out of control. Digital forensics and, to an extent, e-discovery have become an integral part of the enforcement mechanisms used in tackling these cybercrimes. The rapid evolution of digital devices has had a significant impact on the digital forensics community with digital crimes evolving just as rapidly. Court proceedings worldwide are now encountering a number of cases where despite their focus and origin, there is some form of digital evidence involved. Traditional cases including drug trafficking, murders, fraud and a myriad of others now rely heavily on some information/data residing on a digital device. Digital forensics methodologies are therefore not only required to acquire digital evidence in cases where the crime is committed using a digital device but also where digital evidence is needed for cases originally not wholly a digital crime. Digital forensics present challenges, as the evidence acquired is inherently different from other types of evidence acquired in other "forensic" investigations. The main differences include the fact that digital evidence can easily be reproduced and manipulated by personnel involved with the investigation (or not), maliciously or accidentally.
This paper will identify some critical issues regarding the use of the digital forensic process to acquire the digital evidence to be used to convict or acquit persons accused of such crimes. It will present a multidimensional approach bringing together the legal, technical, ethical and educational dimensions of digital forensics to form an integrated framework and methodology for investigations involving digital evidence. The objective of these designs is to produce a solution to issues surrounding digital evidence acquisition and subsequent presentation in court and outlines guidelines for making this type of evidence more robust when presented in court.

1. Introduction and background

A number of models, methodologies and frameworks have been developed for digital forensics in the past decade [10]. These developments all focus on particular aspects of the digital forensic process resulting in inconsistencies in the presentation of the digital evidence acquired via the digital forensics process. The developed framework and accompanying methodology outlined in this paper addresses the existing issues of inconsistency within the digital forensics field and addresses the drawbacks of previous designs. It presents a methodology governed by a framework of standards to acquire digital evidence.

Digital forensics refers generally to the acquisition, preservation, analysis and presentation of digital evidence produced from digitally related crimes [1]. Digital forensics as explained by [2], "is the discipline that combines elements of law and computer science to collect and analyze data from computer systems, networks, wireless communications, and storage devices in a way that is admissible as evidence in a court of law". The word forensics denotes use in law/courts thus signifying digital forensics as a process carried out ultimately to acquire evidence that may be used in a court of law. The goal of digital forensics, as simply stated by [3], "is to identify digital evidence for an investigation". The fact that digital forensics has a legal connotation cannot be overemphasized. Forensic science has been used in other fraternities for centuries however digital forensics is still in its developmental stages and faces a number of challenges. A digital forensics investigator must ensure that all aspects of the process are in line with the law or the resulting evidence may face major challenges when presented in court.

The actual definition of the term "Digital Evidence" and what it refers to is often debated in the digital forensics community. The Scientific Working Group on Digital Evidence defines digital evidence as being "any information of probative value that is either stored or transmitted in digital form". Throughout this paper digital evidence is defined to include any information that has been stored or transmitted on any digital/electronic device, and not limited only to computers and associated networks, but also mobile devices and by extension the cloud. The nature of digital evidence is therefore not limited to any particular format as [5] states, "Digital objects bear less evidence of authorship, provenance, originality and other commonly accepted attributes than do analogue objects". The nature and basic characteristics of digital evidence leaves it open to doubt and thus various validating methods must be administered to ensure authentication for any evidence acquired as there is the possibility of it being used in court.

The rapid evolution of technology has had a significant impact on the digital forensics as a field with digital crimes becoming rampant. Courts worldwide are now presented with a number of cases where despite their focus and origin, there is some form of digital evidence involved [29]. The outcome of traditional cases such as those involving drug trafficking, murders and others now rely a lot on information/data residing on a digital device. Digital forensics is therefore required to acquire digital evidence in cases where the crime is committed using a digital device as well as where digital evidence is needed for cases originally not considered solely a digital crime. [6] supports this argument when he states, "…a large majority of lawyers, legal academics and judges have failed to realize that they are now living in a world dominated by digital evidence and that digital evidence now forms the dominant form of evidence in courts". It is with these considerations in mind that we decided to conduct a survey into the relative standardization currently existing in the digital forensics field.

There is a variety of different proposed existing digital forensic models some developed by organizations for their own use, law enforcement personnel for their own countries and by other individuals based on their background, objective and the needs of their employers. See [7] and [8]. These designs go as far back as 2001 with a model being developed by [9] which followed [10] written in 1995. The mere number of existing proposed methodologies and frameworks where both terms are used interchangeably suggest there are some inconsistencies in the field. Existing methodologies, frameworks and models are partly driven by the tools available to the investigator and targeting particular areas of the digital forensic process, namely the capture and/or analysis of digital evidence. There are other

models that focus solely on the acquisition of the evidence ignoring all other phases that may be required by a "forensic" investigation [29].

Models such as [11] where 'Henry Lee in his book "Crime Scene handbook" designed a model that included an additional stage, that of reconstruction to the model developed by [9]. It is a bit more systematic and followed four very pertinent stages, recognition, identification, individualization and reconstruction. It ignores particular phases of the forensics process and does not include distinct stages for preservation or authorization to start the investigation and focuses mainly on the analysis of the evidence. Eoghan Casey in his book 'Digital Evidence and Computer Crime' [12] depicts a model that focuses mainly on the investigative aspect of the digital forensics process with four phases: recognition, preservation, classification and reconstruction.

[13] Also developed a model which is one of the more recent and comprehensive models developed and has approximately twelve (12) stages and sub stages. This model does specify phases pertinent to the entire digital forensics investigation however it has been developed to address cyber related crimes (cyber forensics) and developed in and for the Malaysian context. A number of the stages are also redundant and the need for preservation of the acquired evidence has not being included.

Another recent model developed is outlined in [14]. This model has network forensics at its core and could possibly be generally adapted. It focuses on the investigation of cyber crimes. It takes the investigator through summoning the suspect and writing the report. A comprehensive set of steps presented for investigation cyber crime with very little explanation provided and standards mentioned.

More recent models [7] and [8] are the more comprehensive of the models reviewed. In the article "The Mapping process of Digital forensics Investigations" [7], it was noted that "No formal theory exists for the digital examinations process". This is a point supported by [8], [15], and others. [7] Then produced what is termed the "mapping process of the digital forensics investigations framework". The output of this process is a combination of the previous frameworks eliminating redundancies and detailed explanations of steps that were thought to be vague, resulting in a five-phase step of activities with the headings, preparation, collection and preservation, examination and analysis, presentation and reporting. This model was developed specifically for the Malaysian Criminal Justice system. It is comprehensive and addresses key areas such authorization, live and static data acquisition for use as evidence and storage of data. Overall the model presented by [7] is a very comprehensive methodology; however its focus is on data acquisition as there and does not include presentation of the digital evidence found which is an important part of any forensics process, one of the objectives of forensics being to present the findings of the investigation.

There are over twenty published papers discussing and presenting methodologies, frameworks, models for digital forensics some of which have been highlighted. These designs as alluded to in other sections of this paper focus on different areas of digital forensics or do not cover the entire process. The importance of digital evidence in a technologically driven society cannot be overstated and thus there is need for consistency in the process used to acquire this evidence. There is need for standardization in how this is done; a methodology governed by a set of standards incorporating all aspects of the digital forensics field will address this concern.

2. The Survey

In order to substantiate information gathered from various peer reviewed literature relating to digital forensics standards, frameworks and methodologies we designed a questionnaire seeking contributions from the digital forensics community. This was done with an objective to validate assumptions with regards to the need for standardization in the acquisition and presentation of digital evidence from those who have practical experience of undertaking such investigations. The major aim of this survey was to ascertain the actual state of digital forensics examination. The questionnaire targeted digital forensics practitioners with different backgrounds based on the field in which they work. The cohort included students, academics, law enforcement officers, lawyers and "forensicators", persons from a technical background doing only this. The main question to be answered was: Is the digital forensics process as ad hoc in the real world as it was been theorized to be?

The survey was sent to a group of known practitioners (control group of 15 practitioners) and placed on the digital forensics forum (http://www.forensicfocus.com/computer-forensics-papers)This forum was chosen because it is the premier online forum for digital forensics practitioners. The membership has been observed to include prominent digital forensic personnel. It was also added to two websites/blogs http://digiforensicsproject.webs.com/apps/links/ and http://digitalforensicsproject.blogspot.com/ .

The survey sough to ascertain the diverse background of digital forensics practitioners. Results indicate that there are practitioners in the field from various backgrounds. These include Law enforcement, Technical personnel (computer science/Information technology), Management (Business oriented), Legal (Lawyers, solicitors, barristers) and a myriad of others.

Background of respondents	%	Years in Practice	%	Students	Expert Witness
Law Enforce	71	Under 1year	4	4%	53%
Technical	10	1-5	45		
Management	3	5-10	26		
Legal	3	10+	4		
Other	10				

Table1

As indicated on the table above 71 percent of the participants were of a law enforcement background while 10 percent were of a technical (CS/IT) background constituting the majority of the sample. One of the pervasive issues with digital forensics is that often the investigation is conducted by persons not qualified in the field. Whereas it is widely accepted that due to the diverse nature of digital forensics there will be practitioners from varying backgrounds there is a basic level of qualification expected. The survey's indication of the majority of respondents being of a law enforcement background is not surprising as cybercrime is a criminal act and thus currently a number of police forces worldwide are instituting a cybercrime arm [25].

To ensure that there was a mix of experienced practitioners respondents were asked to indicate the number of years they had been practicing in the field 45 percent of the respondents indicated that they had been in the field for 1 – 5 years, 26 percent 5 – 10 years

indicating that most of the practitioners were experienced in the discipline of digital forensics. Additionally only four percent of the respondents were students indicating that most of the respondents were practicing digital forensics personnel that had real life experience in the field, also most of the respondents (practitioners) 53 per cent were expert witnesses supporting the notion that the main objective of the digital forensic process is to acquire digital evidence for legal use.

Cyber crime has become widespread with recent surveys indicating that the top five countries for cybercrimes in 2011 were USA, France, Russia, Germany, and China. This however did not reflect in the geographical location of respondents to the survey. The researcher sought to receive responses for a wide geographical area however 65 percent of the respondents were from Europe. 10 percent of the participants indicated that they were from Asia, 16 percent from North America, 6 percent from the Caribbean, and another six from the Middle East. There were no responses from Russia or out of Africa.

Digital Forensics is defined as "the science that is concerned with the relation and application of computers and legal issues" [16]. To ascertain the consistency in the concept of what digital forensics was the questionnaire asked that each respondent define the term digital forensics. There were a variety of responses. While some respondents identified "digital forensics" as a science there were others defined it as an investigative procedure with most respondents however concurring that digital forensics involved the collection of data from digital devices.

Literature reviewed and statistics published indicates that there has been an increase in cybercrime over the last decade [17] [23]. Data indicates that there has been an increase in the request for digital forensics investigations in recent times. To quantify this assumption/observation the questionnaire sought to find out from practitioners the frequency with which their expertise was requested. The responses did suggest that there is indeed a widespread need for the use of digital forensics procedures, with responses ranging from daily, weekly, very often to "always have a backlog".

One of the main objectives of the survey was to ascertain the current state of digital forensic procedures with regards to procedures used to carry an investigation. Were there any particular methodologies in use and if so were there any policies in place to guide these procedures and how these procedures were developed? It also sought to ascertain if there were any particular tools favored by practitioners and what influenced the choice of tools and methodology.

	Yes	No
Are there policies in place to guide the Digital Forensic process	84%	16%
Were these policies…?	Percentage	
Developed in house	35	
Bought from a commercial organization	0	
Adapted from another organization/Body	13	
Other	52	

Table 2

Practitioners choosing other indicated that their policies used were based on those from other

organizations groups such as the Association of Chief Police Officers (ACPO), National Institute of Standards and Technology (NIST), International Organization for Standardization (ISO), International Association of Computer Investigative Specialist (IACI).
These results confirmed the following: while there are policies in place to guide practitioners in the digital forensics process these policies are mainly developed by the organizations themselves with a lesser percentage being adapted from other organizations. This data highlights the ad hoc ways in which the process is carried out internationally. Organizations and individuals have their own guidelines that they create and adapt for use signifying that there is no one standard benchmark policy or guide that is used.
The respondents indicated that they do not use any one specific methodology to acquire digital evidence. They indicated that there were a variety of different factors dictating how an investigation took place and thus the methodology used was influenced by this. Influencing factors such as the type of investigation, who requires the investigation, the tools used were cited in addition to the issue of no particular being methodology being in place that could be drawn on.

This ad hoc use of varying procedures throughout the digital forensics process was further highlighted when respondents were asked to list the steps taken to carry out the digital forensics process from start to finish. The responses were varied with practitioners indicating different tasks that signaling the beginning of the process and varying tasks that indicated the end. While some practitioners saw their cases ending at the outcome of a case others saw it ending when they presented their report. There are some practitioners that respond to a request for their services by researching the background of the case, others had a preliminary look at the devices involved, while some practitioners indicate that the first step before doing anything was to ensure that they got legal permission. There was also wide variation with intermediate procedures taken throughout the digital forensics process. The ad hoc ways in which digital forensics is carried out has been an ongoing challenge for the digital forensic community.

There are a variety of tools available to help in the digital forensics process. The majority of these tools are open source and available free online while others are available commercially for a very high cost from vendors who drive the industry [26]. Such a variation in tool usage calls into question the issue of consistency and fairness – an issue that needs to be addressed. To gather more insight on the methodologies used the researcher sought to find out if there was any consistency in the use of tools despite the wide availability of open sourced tools. The variance here was even wider as indicated in the chart below. Having presented what are deemed the more popular tools 45 percent of the respondents chose “other”, listing other tools such as Ufed while 35 percent indicated that they used tools developed in house by their information technology departments. Popular tools internationally include Encase, FTK and Sleuth kit. The research further broke this data down to represent regions in an attempt to ascertain if particular tools were popular in particular regions. This was not so.

Tool	Caribbean	Europe	North A	Asia	Middle East
FTK	x	x	x	x	x
Encase	x	x	x	x	x
Sleuth Kit		x	x		

Table 3

Which of the following tools do you employ throughout the investigation?

FTK	26%
Encase	35%
SIFT	3%
Sleuth Kit	16%
PTK Forensics	0%
The Coroners Tool Kit	0%
Open Sourced	29%
In house developed	35%
Other	45%

Respondents were allowed to select more than one checkbox, so percentages may add up to more than 100%.

Table 4

While Encase and FTK tools seemed to be Dominant worldwide Sleuth kit seemed limited to Europe and North America. The rationale given for the choice of tool by respondents was dependent mainly on cost, experience, recommendations from colleagues as well as that they kept using the tool they use when being trained as a digital forensics practitioner. .

The data gathered in this survey has indicated that digital forensics practitioners receive requests for digital forensics services daily while an investigation may last up to six months, sometimes more. This may be due in part to a shortage of trained practitioners in the field [24]. Data gathered also indicate that there is a constant backlog of cases. These results confirm that there is need for improvement in the speed and efficiency in the way digital forensic investigations are carried out. This, while maintaining the integrity of the evidence found ensuring it conforms to legal and ethical standards as information gathered also show that eighty percent (80%) or more of the digital investigations carried out are eventually (if not initially) court cases.

These results of the survey depict what was being suggested by the literature reviewed. There are however additional questions arising from the analysis of these results:

1. How can time taken to complete a digital forensics investigation be reduced while retaining accuracy in the results and their analysis?
2. Would a structured set of operating procedures help to reduce the backlog of digital forensics cases?
3. The majority of digital forensic evidence ends up in courts. Should the training of digital forensics practitioners not include all aspects of the investigations and not just the technical or legal areas?

3. Discussion

The fundamentals of any digitally related criminal activity lies in "digital evidence". This evidence is acquired through the digital forensic process, which is an investigative process involving the collection, preservation, interpretation and presentation of evidence. This process as described may differ from one investigator to another despite the various

legislations in place. A fact highlighted in the survey where respondents were asked to give their definition of Digital forensics. Digital evidence is unique in a number of ways based mainly on the form it takes which is not necessarily a physical one. [18] points out "if someone opened a digital storage device they would see no letters, numbers or pictures on it". The very nature of the data highlights the need for a digital forensic investigator to be thorough in carrying out their duties.
The term Digital Evidence is defined by [19] as, "Encompasses any and all digital data that can establish that a crime has been committed or can provide a link between a crime and its victim or a crime and its perpetrator". The same term may also be defined to be, any data or information found to have been stored or transmitted in a digital form that may be used in court. [20] This type of evidence has become increasingly popular in recent years, as courts have begun to accept electronic based evidence for use in traditional cases.

As with any other type of evidence due diligence must be followed to ensure its reliability in a court of law and most courts have found it necessary to question the reliability of such evidence when presented. (United States v Carey [30] and United States v Benedict[29]).
This concern has been highlighted in several scenarios with the lack of standardization in the acquisition of digital evidence (i.e. Computer forensic methodologies) being blamed. [12] supports this point stating, "Digital investigators do not have a systematic method for stating the certainty they are placing the digital evidence that they are using to reach their conclusions". The methodologies and tools used by digital forensic investigators worldwide have been variable and there is no one internationally accepted benchmark. He [12] continues, "This lack of formalization makes it more difficult for courts and other decision makers to assess the reliability of digital evidence and the strength of the digital investigators' conclusions". This dilemma is further supported by [21] where they state, "The number one problem in current litigation is the preservation and production of digital evidence". The latter are two of the processes involved in the digital forensic process.

The problem of standardization in the area of digital forensics has presented a problem from the initial stages and still faces major challenges when digital evidence is being presented in court. See case Coleman Holdings Inc v Morgan Stanley [31]. "Because computer forensics is a new discipline, there is little standardization and consistency across courts and industry" [2]. It is integral that agencies and practitioners adhere to a defined set of standards and operating procedures to ensure this evidence and methodology is accepted by the legal community. Bryan Sartin, Managing director of Cybertrust, in an interview with SCmagazine states that there is still much more to be done where digital evidence acquired through computer forensic is concerned. He pointed out that, "There are two things missing: a single commonly accepted standard and uniform code of working…. Quality of service across computer forensic providers varies dramatically …" [5] sums up the need for standardization within the sector when he argues; "…there is an absence of generally recognized standards of best practice in digital evidence forensic procedures, and a lack of adequate training of forensic examiners". He makes a very valuable point when he continues his argument, "errors in analysis and interpretation of digital evidence are more likely where there is no standard procedure for collecting, preserving and analyzing digital evidence". Such statements from seasoned practitioners in the field highlight the need for some amount of standardization of the field.

The 2IIR Framework

The need for standardization in the field of digital forensics cannot be overstated and thus the

results of the survey served to inform the development of the 2IIR framework and an accompanying methodology. The 2IIR frame work is governed by a set of standards and is accompanied by a methodology derived from the framework. It consists of three phases and four core areas. The main aim is to bring coherence to the professional and occupational functions of the digital forensics field.

The framework of standards is arranged into three interrelated sections;

Initiation of the investigation [I1]
The investigation itself [I2]
Reporting of findings [R]

Fig 1

Initiation
Aim: To set the stage for an investigation that will produce digital evidence that is legally admissible in a court of law.

Investigative
Aim: To produce digital evidence that is able to withstand the rigors of a court of law. The methods used to produce this evidence should produce the same results if used by another practitioner.

Reporting
Aim: To produce a comprehensive report of findings. A report that is comprehensive to all personnel involved including those from non technical fields.

It sets out and defines a set of characteristics that each practitioners carrying out an investigation should portray to enhance the validity of the digital evidence produced. It specifically addresses:

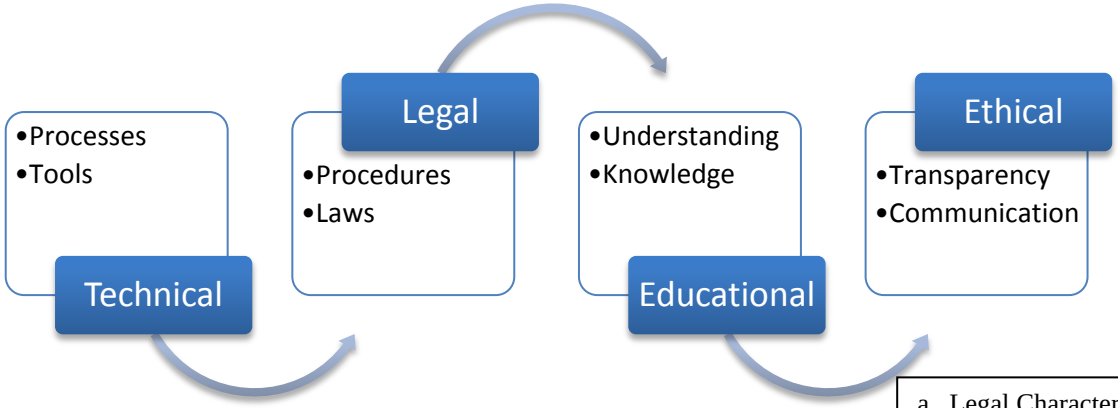

Fig 2

Ethical standards are the statements of a practitioners professional attributes that are expected to be maintained throughout their career.
These standards are developed to be meaningful to the practice of digital forensics. Their main purpose in the framework is to:

1. Inspire practitioners to reflect and uphold the integrity of the profession
2. Guide ethical decisions in the field
3. Specify ethical responsibilities in digital forensics practice
4. Promote trust and confidence in the field of digital forensics.

Educational Standards clarify the basic educational background that digital forensics practitioners at different levels should portray.
These standards define the knowledge and skills that practitioners should possess. It also encourages the highest qualification possible in the field. There are certain things that digital forensics practitioners should know and be able to do.

Legal standards indicate the legal aspects of the investigation that must be observed by the digital forensics practitioner.
These standards outline the legal requirements of a digital forensics investigation. It also lists the related laws to be observed during the different phases of the investigation

Technical Standards outlines the technical guidelines encompassed in a digital forensics investigation.
The technical standards define the basic technical expertise of a digital forensics investigator. It outlines the use of tools and the procedures associated with a digital forensics investigation.

The framework has four core principles governing all sections. Each core area: legal, technical, ethical and educational is governed by a set of at least two core principles relevant to that area. Each of the three phases are also governed by at least three principles

5. The Methodology

For digital evidence that is retrieved through the digital forensics process to be considered robust enough to stand up in court it must be able to satisfy legal testing criteria such as those outlined in [22]. To satisfy the ideals of [22] there are certain criteria that must be met:

1. Empirical testing: Referring to whether the theory or technique used is refutable, and/or testable.
2. Has the theory used has been subjected to peer review and has it been published?
3. What is the known/potential error rate?
4. Are there the existence and maintenance of standards and controls concerning its operation?
5. What is the degree to which the theory and technique is generally accepted by a relevant scientific community?

Meeting the criteria set out in [22] presents a challenge to the field when different organizations and groups develop their own methodologies and the non-existence of standards. Thus there needs to be standardized framework complete with a set of standards which digital forensics practitioners, internationally, will use as a bench mark when carrying out their duties. This framework must not only satisfy technical and legal criteria but also adhere to ethical expectations, education and be flexible enough to meet the needs of a dynamic field. The proposed framework is flexible enough to be adapted for the various divisions in digital forensics for example, mobile forensics, network forensics, cloud forensics and computer forensics.

Educational training along with legal and ethical principles embodies the entire methodology which must the observed throughout the entire digital forensics process.

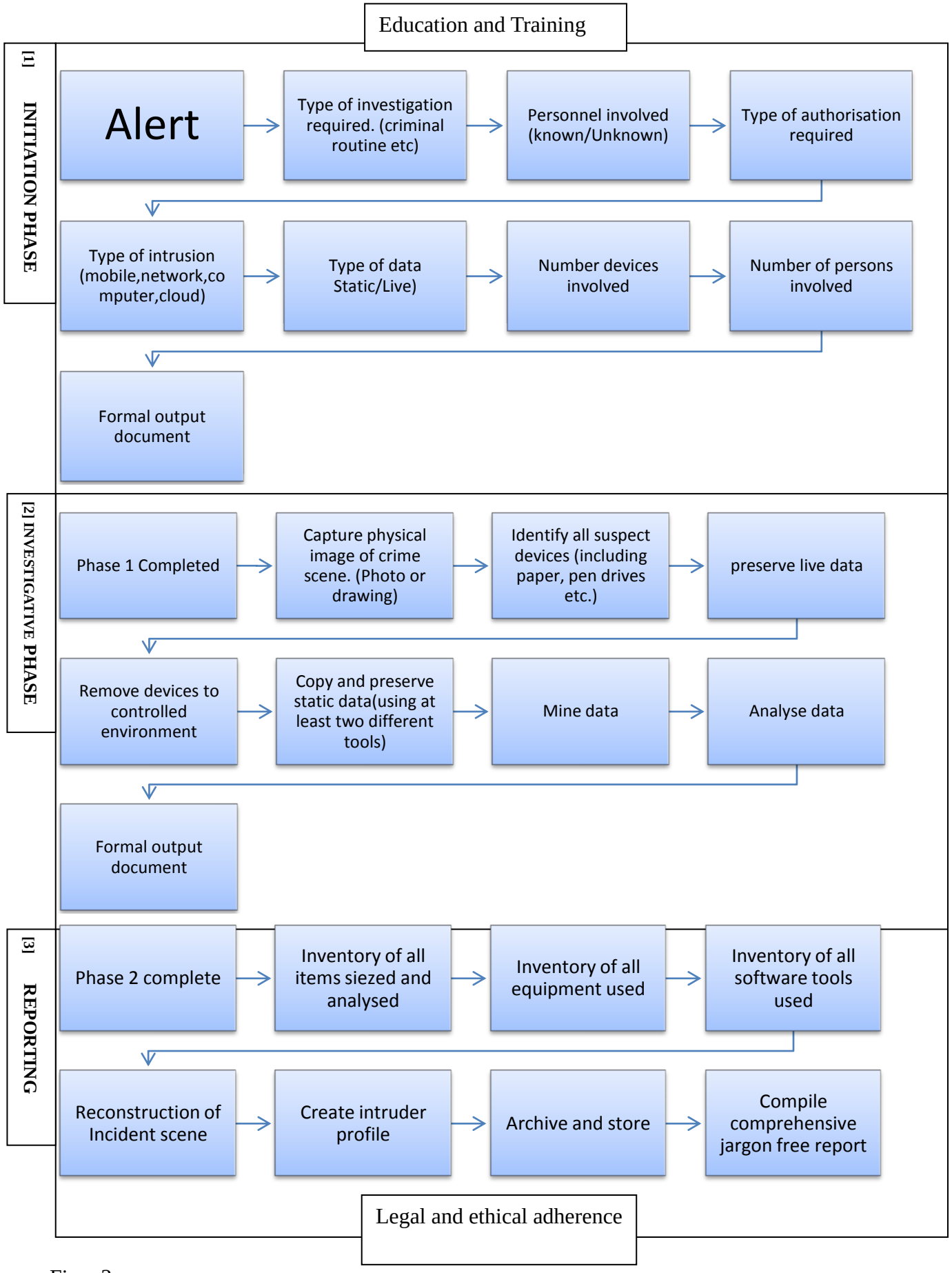
Education and Training
[1] INITIATION PHASE
Alert
Type of investigation required. (criminal routine etc)
Personnel involved (known/Unknown)
Type of authorisation required
Type of intrusion (mobile,network,computer,cloud)
Type of data Static/Live)
Number devices involved
Number of persons involved
Formal output document
[2] INVESTIGATIVE PHASE
Phase 1 Completed
Capture physical image of crime scene. (Photo or drawing)
Identify all suspect devices (including paper, pen drives etc.)
preserve live data
Remove devices to controlled environment
Copy and preserve static data(using at least two different tools)
Mine data
Analyse data
Formal output document
[3] REPORTING
Phase 2 complete
Inventory of all items siezed and analysed
Inventory of all equipment used
Inventory of all software tools used
Reconstruction of Incident scene
Create intruder profile
Archive and store
Compile comprehensive jargon free report
Legal and ethical adherence

Fig. 3

The initiation phase comprises of those tasks that are critical in ensuring that the necessary actions are carried out and appropriate documentation produced before any device is examined or seized. Information to be gathered at this phase will include, type of intrusion, suspected persons involved as well as devices involved. At the end of this phase authorization should have been requested and received. The main deliverable of this phase is a completed formal document detailing all actions carried out and by whom indicating suitability to continue to the next phase.

Throughout the investigative phase the practitioner must be constantly aware the evidence that is being perused may be used in a legal setting and thus rules of evidence should be observed. This stage needs to be carefully planned and coordinated to ensure that there is no spoiling of the evidence. This phase is the longest and involves activities ranging from locating of the devices involved in the incident to the analysis of data retrieved. The investigator should then identify suspect devices and peripherals and proceed to preserve any live data. It is also during this phase that the devices will be removed to a controlled environment for analysis. Careful care and planning must be in place to ensure that the applicable laws (that will be outlined in the framework) are strictly adhered to. Once in a controlled area extraction, preservation and analysis of the data will proceed.

The forensics process indicates law and thus the practitioner must constantly be aware of this and that they may be required to present their findings in a court of law. This phase will include sub tasks such as creating inventories, reconstruction of the incident scene and creation of a profile of the intruder. The practitioner must not only be aware of but be appropriately trained to produce a written and structured report that can be understood by all stakeholders which may be from varying backgrounds.

This methodology includes areas neglected by previous models and is guided by a framework of standards. It does not place focus on any one area of the investigation, not developed for a specific geographical area and may be adapted for any subset of digital forensics (ie mobile forensics, network forensics etc.).

Conclusion and further work

This proposed framework and methodology is designed to be prescriptive and rigorous while ensuring speed and accuracy. It is prescriptive because it includes recommendations of tools at particular stages in the process and is guided by standards. It is rigorous because it is expected that no phase will be excluded. This measure ensures the model is accurate and reliable.

A methodology guided by a framework of standards will be of benefit to all involved in the world of digital forensics. A framework that addresses all aspects and core fields that are involved in the digital forensics process will help to alleviate some of the issues that currently exist within the discipline. It is apparent that though several disciplines are encompassed in the digital forensics field there has not been much of a collaborative and integrated approach to its development. Digital forensics is a diverse discipline and thus all professionals involved should be able to communicate eliminating the jargon of specific areas and assumptions that one field impacts the discipline more than the other.

Digital forensics is a dynamic field which has been faced with a number of issues. This paper highlights some of these issues and presents amicable solutions. The field of digital forensics encompasses various fields, facets include investigative, technical, ethical and legal. A digital forensic investigator must be cognizant of all these facets throughout an investigation as ignoring any one facet can significantly impact the outcome of an investigation. In his article 'Digital forensics research: The next 10 years' Simon Garfinkel states simply, 'There is no standard set of tools or procedure" [26]. Two main areas are identified that need further research: i) the legal issues as they relate to digital forensics and ii) the evidence acquired and the issue of a methodology governed by a set of standards that may be used internationally by digital forensic investigators. Having a methodology governed by a set of standards will also help in satisfactory responses to the questions posed by [22]. The proposed framework addresses these key issues and the methodology includes the incorporation of the reconstruction of the intrusion and creation of an intruder profile presenting more assurance in digital evidence acquired through the digital forensics process.

The work proposed addresses intricate issues of the digital forensics process and lays the foundations of a framework that will accurately and rigorously address the multidimensional nature of the field.

References

[1] Hewling, M. O., Sant, P. (2011), Digital Forensics: The need for integration. Proceedings of Digital Forensics & Incident Analysis (WDFIA 2011)

[2] US CERT 2008 Available from:
UK Copyright Law, A summary. Available from http://www.copyrightservice.co.uk/copyright/uk_law_summary (Accessed on, January 21, 2012)

[3] Carrier B. D., Spafford E., (2004) 'An event based Digital forensics Investigation Framework' *Center for Education and Research in Information Assurance and Security*.

[4] Scientific Working Group on Digital Evidence (SWGDE) of the National Center for Forensic Science (NCFS). Best Practices for Computer Forensics V2, 2006a. Retrieved From the World Wide Web on 07/07/12: URL http://ncfs.org/swgde/documents/swgde2006/Best_Practices_for_Computer_Forensics%20V2.0.pdf

[5] Chaikin D., (2007) Network Investigations of Cyber Attacks: The limits of digital evidence, Springer Science and Business Media

[6] Mason, D., Carlin, A., Ramos, S., Gyger, A., Kaufman, M., Treichelt, J., (2007).
Is the open way a better way? Digital forensics using open source tools.
The Computer Society. 1-10.

[7] Salemat S. R. Yusof R. Sahib S. (2008) *Mapping Process of Digital Forensic Investigation Framework.* International Journal of Computer Science and Network Security Vol. 8 NO 10 Available from www.sciencedirect.com

[8] Perumal S., (2009) Digital Forensics Model Based on Malaysian Investigation Process, IJCSNS Vol. 9 No. 8 Available from www.sciencedirect.com

[9] Kruse W. Heiser J. G. (2001). Computer Forensics: Incident Response Essentials (1st ed.), Addison Wesley Professional. USA

[10] Pollitt M., (1995) *Principles, Practices, and Procedures: An approach to standards in computer forensics.* Available from; www.digitalevidencepro.com/resources/principles.pdf

[11] Lee H, C., Palmbeach T. M., Miller M. T. (2001*) Henry Lee's crime scene handbook.* Elsevier Academic Press Available from: http://academic.evergreen.edu/curricular/social_dilemmas/fall/Readings/Week_06/Crime%20Scene%20Handbook.pdf

[12] Casey, E. (2004). *Digital Evidence and Computer Crime, Forensic science, Computers and the Internet*. Academic Press, London, UK

[13]Cuardhuain S. O., (2004) An Extended Model of Cyber Crime Investigation. Journal of Digital Evidence. Vol. 3. Issue 1

[14]Yong-Dal S., (2008) New Digital Forensics Investigation Procedure Model. Proceedings of Fourth International Conference on Networked Computing and Advanced Information Management. Available at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4624063

[15] Ricci I. S. C. (2006) *Digital Forensics Framework that incorporate legal issues*. Available from www.sciencedirect.com Accessed on October 20, 2011

[16] Kuchta K. J., (2000) 'Computer Forensics Today' *Law, Investigations and Ethics* Available from: http://www.liv.ac.uk/library/ohecampus/

[17] http://www.ic3.gov/media/annualreports.aspx

[18] Mercer L. D., (2004) Computer Forensics, Characteristics and preservation of Digital Evidence. *FBI Law Enforcement Bulletin.* Available from: http://www.liv.ac.uk/library/ohecampus/

[19]] Casey, E. (2011). *Digital Evidence and Computer Crime, Forensic science, Computers and the Internet*. Academic Press, London, UK

[20] Hewling M., (2010). Digital forensics and the UK Legal Framework. MSc. Dissertation, University of Liverpool.

[21] Fulbright and Jowoski L., (2006) *Third Annual Litigation Trends Survey Findings*. Available from: http://www.fullbtight.com/mediaroom/file/2006. Accessed on April 13, 2012.

[22] Daubert v Merrell Dow Pharmaceuticals, 1993, 509 US 579

[23] Aeilts T., (2011) *Defending against cybercrime and terrorism* FBI law enforcement Bulletin. Available at http://www.au.af.mil/au/awc/awcgate/fbi/universities_fight_terrorism.pdf

[24] Bhaskar R., (2006) *State and Local Law Enforcement is not Ready for Cyber Katrina*. Communications of the ACM

[25] http://www.met.police.uk/pceu/,

[26] Nance K., Hay B., Bishop M., (2009) Digital Forensics: defining a Research Agenda. Proceedings of the 42nd Hawaii International Conference on System Sciences. Available at : http://assert.uaf.edu/papers/dfResearchAgenda_HICSS09.pdf

[27] Garfinkel S., (2010) Digital forensics research: The next 10 years. Digital Investigations 7 S64 – S73. Available at: http://dfrws.org/2010/proceedings/2010-308.pdf

[28] http://www.scmagazineuk.com/digital-forensics-is-in-demand/article/178321/

[29] Pollitt M., (2007)An ad hoc review of Digital Forensic Models. Proceedings of the second International Workshop of Systematic Approaches to Digital Forensics Engineering (SADFE'07) Available at http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4155349&tag=1

Cases

[30] Gonzalez v Anthony C. No.: 48-2008-CA- 24573-O

[31] United States v Benedict (1996) No. 96-1369. Available from

[http://www.cybercrime.gov/]

[32] United States v Carey (1998) Number 98-3077 Available from

[http://laws.findlaw/10th/983077.htm]

[33] Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co., Inc., 2005 WL 679071 (Fla. Cir. Ct. Mar. 1, 2005)

http://www.ediscoverylaw.com

[34] Zubulake v UBS (2003) 217 F.R.D. 309 (S.D.N.Y. 2003

[http://lawschool.courtroomview.com]