Taxonomy of Challenges for Digital Forensics

[1,2]Nickson M. Karie[*] MSc, [1]Hein S. Venter[†] PhD

[1]ICSA Research Group, Department of Computer Science, University of Pretoria,

Private Bag X20, Hatfield 0028, Pretoria, South Africa

[2]Department of Computer Science, Kabarak University, Private Bag - 20157, Kabarak, Kenya

Email: menza06@hotmail.com[*], hventer@cs.up.ac.za[†]

ABSTRACT: Since its inception, over a decade ago, the field of digital forensics has faced numerous challenges. Despite different researchers and digital forensic practitioners having studied and analysed various known digital forensic challenges, as of 2013, there still exists a need for a formal classification of these challenges. This paper, therefore, reviews existing research literature and highlights the various challenges that digital forensics has faced for the last ten years. In conducting this research study, however, it was difficult for the authors to review all the existing research literature in the digital forensic domain, hence, sampling and randomisation techniques were employed to facilitate the review of the gathered literature. Taxonomy of the various challenges is subsequently proposed in this paper based on our review of the literature. The taxonomy classifies the large number of digital forensic challenges into four well-defined and easily understood categories. The proposed taxonomy can be useful, for example, in future developments of automated digital forensic tools by explicitly describing processes and procedures that focus on addressing specific challenges identified in this paper. However, it should also be noted that the purpose of this paper is not to propose any solutions to the individual challenges that digital forensics face, but to serve as a survey of the state of the art of the research area.

KEYWORDS: Forensic sciences, digital forensics, taxonomy, digital forensic challenges, categories, formal classification of challenges

Over the last decade, the evolution in digital technology has greatly influenced the way we live our daily lives and conduct business. Consequently, as this evolution continues, numerous challenges emerge that are to be faced by the digital forensic domain. The particular problem that this paper addresses is stated as follows. Due to the fact that digital forensics (DF) is still considered a relatively new field in both research and industry, the number of challenges faced in this field is bound to increase in line with Moore's Law (1). The simplified version of this law states that processor speeds or overall processing power for computers will double every two years, resulting in numerous other challenges in DF.

This paper therefore aims at reviewing existing digital forensic literature and highlights the various challenges that digital forensics have faced over the last ten years. Taxonomy of the various challenges is subsequently proposed in this paper based on our review of the existing literature. The taxonomy classifies the large number of digital forensic challenges into four well-defined and easily understood categories.

The presentation in this paper can be useful, for example, in future developments of automated digital forensic tools as well as in explicitly describing processes and procedures that focus on addressing the individual digital forensic challenges identified. Institutions of higher learning will also find the proposed taxonomy in this paper constructive, especially when developing curriculums and educational material for different undergraduate courses, as well as research projects for postgraduate studies.

Furthermore, the presentation of the taxonomy in this paper is a novel contribution in the digital forensic domain and offers a comprehendible categorisation that may shed more light on existing digital forensic challenges. The taxonomy has been designed in a way to accommodate new categories of digital forensic challenges that may crop up as a result of technological change and domain evolution.

Background

As mentioned earlier, DF is a new and growing field in both research and industry (2). It is also considered a branch of forensic science that deals with the recovery and investigation of material found in digital devices, often in relation to digital crimes. By 2013, research in digital forensics has been conducted

for over a decade. However, because of the ever-evolving nature of digital technology, the challenges faced during the recovery and investigations of materials found in digital devices are obviously increasing as well.

For this reason, rigorous and flexible process models and frameworks need to be developed to overcome the different challenges faced by DF. This includes challenges such as the vast volumes of data (3), education and certification, lack of unified formal representation of domain knowledge, legal system challenges, semantic disparities that occur in the domain among others. Developing practical methodologies that can aid in resolving different challenges in DF is inevitable and is as important as the research itself. Besides, for DF to remain effective and relevant to the law enforcement, academia, and the private sector, the domain experts must constantly endeavour to address these challenges.

Recent developments in digital forensics are geared towards standardising the digital forensic investigation process model (4). This development is backed up by the fact that the number of forensic process models that exist has added to the complexity of the digital forensic field (5), hence the need for harmonisation and/or standardisation. In the next section the authors will examine existing related work on taxonomy development in digital forensics.

Related Work

Several taxonomies and frameworks have been proposed by different researchers in the digital forensic domain. Most of these taxonomies and frameworks, though, have their major focus on the digital forensic investigation process. Nevertheless, the literature in this regard offered valuable contributions towards the development of the taxonomy of challenges for digital forensics, presented in this paper.

To begin with, in a paper by Altschaffel et al. (6), the authors argue that digital forensic investigations are usually conducted to solve crimes committed by perpetrators and/or intruders using IT systems. They then propose a taxonomy that helps to perform a forensic examination and to establish answers to a set of well-defined questions during such examination.

Efforts by Hoefer and Karagiannis (7), culminated in taxonomy of cloud computing services. Their paper describes the available cloud computing services and further proposes a tree-structured taxonomy based on their characteristics, so as to easily classify cloud computing services and make it easier to compare them. In contrast, the proposed taxonomy in this paper, offers a simplified platform that sheds more light on the classification of existing digital forensic challenges.

Strauch et al. (8) argue that cloud computing allows the reduction of capital expenditure by using resources on demand. Thus, they investigate how to build a database layer in the cloud and present pure and hybrid cloud data-hosting solutions. They then organised the solutions in a taxonomy which they use to categorise existing cloud data-hosting solutions. Lupiana et al. (9), on the other hand, proposed a taxonomy for classifying disparate research efforts in ubiquitous computing environments. Their taxonomy classifies ubiquitous computing environments into two major categories namely: interactive environments and smart environments.

Sansurooah (10) explains in his paper that the increased risk and incidences of computer misuse have raised awareness in public and private sectors of the need to develop defensive and offensive responses. He then compares the different methodologies and procedures that are in place for the gathering and acquisition of digital evidence and subsequently defines which model will be the most appropriate taxonomy for the electronic evidence in the computer forensics analysis phase. Sriram (11), however, argues that in recent years the exponential growth of technology has also brought with it some serious challenges for digital forensic research. Therefore, in his paper, he reviews the research literature since 2000 and categorise developments in the field into 4 major categories. He further highlights the observations made by previous researchers and summarise the research directions for the future.

Kara et al. (3) explains that while many fields have well-defined research agendas, evolution of the field of digital forensics has been largely driven by practitioners in the field. Their paper then goes further and outlines new research categories (taxonomy) and areas identified at the Colloquium for Information Systems

Security Education (CISSE-2008), as well as a plan for future development of a formalized research agenda for digital forensics.

Garfinkel (12) in this paper states that, the golden age of computer forensics is quickly coming to an end. He then summarizes current digital forensic research directions and argues that to move forward the community needs to adopt standardised, modular approaches for data representation and digital forensic processing. In addition, he argues that, without a clear research agenda aimed at dramatically improving the efficiency of both digital forensic tools and the research process, our hard-won capabilities will be degraded and eventually lost in the coming years.

Other related research works on taxonomies also exist, but none of those or the cited references in this paper have to date presented a taxonomy of the different challenges faced by the digital forensic domain in the way introduced in this paper.

Thus: in contrast to all the research efforts referred to above, we propose a taxonomy that classifies the various challenges faced by digital forensics into 4 well-defined and easily understood categories. Nevertheless, the authors acknowledge the fact that the previous work on the proposed frameworks and taxonomies has offered us useful insights into the development of the taxonomy of challenges for digital forensics in this paper. The scope of the proposed taxonomy is explained in the section to follow.

Scope of the Proposed Taxonomy

While there are many challenges in digital forensics and several attempts to address specific and/or individual challenges have been done by different researchers. The presentation in this paper is an exceptional effort towards a novel taxonomy of digital forensic challenges based on the review of existing digital forensic literature. The scope of the taxonomy is, however, restricted to the boundaries of the literature reviewed by the authors (not more than ten years old). The authors' also acknowledge that, the various challenges presented in this paper are not, in whatever way, an exhaustive list. This is backed up by the fact that, it is difficult to gain an exhaustive list - because an exhaustive list is hard to create and even if

created it would not be easy to handle or manage because of its size. The taxonomy, hence, has been designed taking into consideration the major challenges that digital forensic has faced over the last decade. The authors, though, did not establish a precise distinction between the old and the most recent digital forensic challenges in this paper. This is because; some of the challenges captured in the taxonomy are inherent to digital forensics, e.g. the vast volumes of data. Future research will, however, consider the possibility of developing an extensive taxonomy with distinctions between the old and the most recent challenges. The next section, thus, explains in detail the proposed taxonomy of challenges for digital forensics in this paper.

The Proposed Taxonomy of Challenges for Digital Forensics

In this section of the paper, we present a detailed explanation of the taxonomy of challenges for digital forensics. Table 1 shows the structure of the proposed taxonomy.

The taxonomy consists of four rows arranged from top to bottom with the first row depicting the technical challenges faced by digital forensics. This is followed by the legal systems and/or law enforcement challenges in the second row, the personnel-related challenges in the third row and finally the operational challenges faced by digital forensics in the fourth row.

The various sub-categories of the challenges presented in each of the different rows of the taxonomy shown in Table 1, however, focuses more on areas that can, for example, be considered when developing new curriculums and education materials for different undergraduate programmes as well as research projects for postgraduate studies.

The sub-categories can also be useful when developing dynamic digital forensic tools that focus on addressing specific identified digital forensic challenges. Organising the taxonomy into categories and sub-categories was necessary to simplify the understanding of the taxonomy as well as to present specific finer details of the taxonomy.

Table 1: The Taxonomy of Challenges for Digital Forensics

Categories of DF Challenges	Identified Subcategories
1. Technical Challenges	i. Encryption
	ii. Vast Volumes of Data
	iii. Incompatibility Among Heterogeneous Forensic Tools
	iv. Volatility of Digital Evidence
	v. Bandwidth Restrictions
	vi. Limited Life span of Digital Media
	vii. Sophistication of Digital Crimes
	viii. Emerging Technologies and Devices
	ix. Limited Window of Opportunity to Collection of Potential Digital Evidence
	x. The Antiforensics
	xi. Acquisition of Information from Small-Scale Technological Devices
	xii. Emerging Cloud Computing or Cloud Forensic Challenges
2. Legal Systems and/or Law Enforcement Challenges	i. Jurisdiction
	ii. Prosecuting Digital Crimes (Legal Process)
	iii. Admissibility of Digital Forensic Tools and Techniques
	iv. Insufficient Support for Legal Criminal or Civil Prosecution
	v. Ethical Issues
	vi. Privacy

Categories of DF Challenges	Identified Subcategories
3. Personnel-related Challenges	i. Lack of Qualified Digital Forensic Personnel (Training, Education, and Certification)
	ii. Semantic Disparities in Digital Forensics
	iii. Lack of Unified formal Representation of Digital Forensic Domain Knowledge
	iv. Lack of Forensic Knowledge Reuse among Personnel
	v. Forensic Investigator Licensing Requirements
4. Operational Challenges	i. Incidence Detection, Response, and Prevention
	ii. Lack of Standardized Processes and Procedures
	iii. Significant Manual Intervention and Analysis
	iv. Digital Forensic Readiness Challenge in Organizations
	v. Trust of Audit Trails

Note still, from the taxonomy in Table 1, that the sub-categories of the challenges listed in column two were only selected as common examples to facilitate this study and should not be treated as an exhaustive list. Therefore, more specific sub-categories of the challenges to each named category can and should be added as the need arises in future.

The major categories of the various digital forensics challenges explored in this study (with their details as shown in Table 1) include: technical challenges; legal systems and/or law enforcement challenges; personnel-related challenges, and operational challenges.

For the purpose of this study, technical challenges include: encryption; vast volumes of data; incompatibility among heterogeneous forensic analysis tools; volatility of digital evidence; bandwidth

restrictions; limited lifespan of digital media; sophistication of the digital crimes; emerging technologies and devices; limited window of opportunity to collect potential digital evidence; anti-forensics; acquisition of information from small-scale technological devices, and lastly the emerging cloud computing or cloud forensic challenges.

Legal systems and/or law enforcement challenges on the other hand focus on jurisdiction; prosecuting digital crimes (legal process); admissibility of digital forensic tools and techniques; insufficient support for legal criminal or civil prosecution; ethical issues, and privacy.

Personnel-related challenges concentrate on, the lack of qualified digital forensic personnel (training, education and certification); semantic disparities in digital forensics; lack of unified formal representation of digital forensic domain knowledge; lack of forensic knowledge reuse among personnel, and the forensic investigator licensing requirements.

Finally, the taxonomy concludes with operational challenges that include: incidence detection, response and prevention; lack of standardised processes and procedures; significant manual intervention and analysis; digital forensic readiness challenge in organisations, and trust of audit trails.

In the sub-sections to follow the various categories, sub-categories of the challenges faced by digital forensics as identified in Table 1 are explained in more detail.

Technical challenges

Technical challenges can be described as those challenges that can be addressed with existing expertise, protocols and operations. Implementing solutions to any of the identified technical challenges often falls to someone with the authority to do so. Knowing that, digital forensics requires a well-balanced combination of technical skills and ethical conduct; some of the identified technical challenges faced by digital forensics are explained in the sub-sections to follow.

Encryption – With the advances in communication technologies such as the Internet, complex encryption products are now widely and easily accessible, presenting the digital forensic examiner with a significant

challenge. Moreover, as encryption standards rise and the algorithms become more complex, it will become more difficult and more time-consuming for specialists to conduct cryptanalysis and then piece together encrypted files into meaningful information (13). Cryptanalysis is described as the science of 'code breaking,' in which an individual reconstructs the original plaintext message from an encrypted version (14) without having a valid decryption key.

There is currently no proven or fully known direct or standardised formula for conducting cryptanalysis. In most cases encrypted data is completely inaccessible without the decryption key. If the suspect refuses to give the key or pleads plausible deniability, the investigator will have to try other methods to acquire the key (15). Although it is now the law in the UK that any encryption key must be given to the police, this is not the case in other jurisdictions, and punishment for not surrendering such keys may be far less severe than the potential punishment for any crime committed (15).

Vast Volumes of data – There has been tremendous growth in the volume of persistent storage – disk storage – used in both personal and corporate systems (16). With the incredibly large volumes of data existing within applications such as Enterprise Resource Planning (ERP) and as mail systems become larger, the volume and amounts of material being generated are by far not human readable in a lifetime – let alone in the scope of a trial or litigation (17). This has implications not only for the procedures and techniques used by investigators for data acquisition and imaging, but also (and more importantly) for the way in which the digital forensic data is analysed.

Incompatibility among Heterogeneous Forensic Analysis Tools - Digital forensic tools generally differ in functionality, complexity and cost. Some tools are designed to serve a single purpose or provide unique information to examiners, while others offer a suite of functions (18). All the same, most of the existing forensic analysis tools consist of dissimilar elements or parts (design and algorithms) and are consequently unable to work together harmoniously. Besides, some of the tools unable to cope with the ever-increasing storage capacity of target devices. This implies that huge targets pose a challenge as they require more

sophisticated analysis techniques that allow digital forensic investigators to perform forensic investigations much more efficiently (19) thus easing digital investigations.

Volatility of Digital Evidence - Digital evidence is, by its nature, fragile. Almost any activity performed on a device, whether inadvertently or intentionally (e.g. powering up or shutting down) can alter or destroy potential evidence (20). In addition, loss of battery power in portable devices, changes in magnetic fields, exposure to light, extremes in temperature and even rough handling can cause loss of data. Collecting volatile data therefore presents a serious challenge to digital forensic investigators, because doing so can change the state of the system (and the contents of the memory itself).

Bandwidth Restrictions - According to Taute et al. (21), bandwidth restrictions in networks can limit or slow down the digital evidence acquisition process. Since the suspect machine in any network is live and active, digital forensic investigators need to connect to the forensic agent installed on the machine via a network. Copying the data as potential digital evidence from the suspect machine to the forensic workstation might slow down the bandwidth, especially if there are many users utilising the bandwidth at that particular time. Large remote evidence acquisitions may also have to be done after hours to accommodate smaller bandwidth capacities, thus posing a challenge to investigators.

Limited Lifespan of Digital Media - While digital storage media facilitate storage of and easy access to electronic data, they do not provide long-term archival storage (22). This is because, at the core of every digital storage media lies “bit preservation” and the ability to monitor for “bit loss”, hence, any bit deterioration can compromise digital data (23). The life span of some digital storage media is typically short and also well enough known for all to be aware of the risks when using them for preservation purposes (24). This poses a serious storage challenge. In fact, even with the emerging cloud computing, the cloud servers leverage on redundant digital storage media which ensures that, in the event of a hardware failure, the data continues to be accessible from another part of the cloud where it is stored safely.

Sophistication of the Digital Crimes - The increasing sophistication of cyber-crimes poses significant challenges to investigations and digital forensic investigators. According to a report by The Association of Chief Police Officers (ACPO) (25), investigators are routinely faced with the reality of sophisticated data encryption, as well as hacking tools and malicious software that may exist solely within memory. Criminals now use anti-forensic techniques that can require endless digital investigations in the case of an attack (26) making it even harder for investigators to get the much needed evidence.

Emerging Technologies - According to Sheward (27), new and evolving technologies create new digital forensic challenges for investigators. Working with a new file system, for example, or even just a new type of file, can require a change in approach or the development of a new technique. While these changes may require slight alterations to well-defined procedures, it is extremely rare to have to deal with a technology that gives a complete transition.

Limited Window of Opportunity for Collection of Potential Digital Evidence - During the collection of potential digital evidence it is important for digital forensic investigators to prioritise which data must be collected first. This becomes a challenge to investigators especially when they are time constrained or when the window of opportunity to collect the data is small (28) or the time to image a system is too short. Investigators must take the necessary steps to ensure that they are able to collect and preserve critical information during this window of opportunity and analyse the data in a method that maintains its integrity.

The Anti-forensics - According to Garfinkel (29), anti-forensics (AF) is a growing collection of tools and techniques that frustrate forensic tools, investigations and investigators. People use anti-forensics to demonstrate how vulnerable and unreliable computer data can be. In order to use evidence from a computer system in court, the prosecution must authenticate the evidence. This also means that the prosecution must be able to prove that the information presented as potential evidence in fact came from the suspect's computer and that it has remained unaltered. Anti-forensics makes it hard for examiners to detect that some

kind of event has taken place and it disrupts the collection of information, thus increasing the time that an examiner needs to spend on a case and casting doubt on a forensic report or testimony (30).

Acquisition of Information from Small-scale Technological Devices - According to Bennett (31), unlike traditional computer forensics on a desktop or laptop computer – where the investigator would simply remove the hard drive, attach it to a write blocker device (thus allowing acquisition of information on a computer hard drive without creating the possibility of accidentally damaging the drive contents) and image the hard drive so as to fully analyse the data – the process to extract information from a mobile device is much more complicated. Moreover, with the continued growth of the mobile device market, the possibility of the use of such devices in criminal activity will continue to increase (32). There are currently numerous manufacturers and models of mobile devices on the market, which results in creating a huge diversity of potential problems and/or challenges to investigators. It becomes extremely difficult for an investigator to choose the proper forensics tools for seizing internal data from mobile devices (32).

Emerging Cloud or Cloud Forensic Challenges - Cloud computing has emerged as an important solution offering organisations a potentially cost effective model to ease their computing needs and accomplish business objectives. However, mixed in with the cloud cost effective opportunities are numerous challenges that need to be considered such as jurisdiction and cloud heterogeneity (33), prior to committing to a cloud service. According to Leslie et al. (34), other challenges faced by the cloud include: safeguarding data security, managing the contractual relationship, dealing with lock-in and managing the cloud. Numerous security challenges also exists e.g. data protection, user authentication, and data breach contingency planning that also need to be addressed.

Legal Systems and/or Law Enforcement Challenges

There is an increased awareness in the legal community of the need for digital forensic services to obtain successful prosecutions that could otherwise fail because of unsatisfactory equipment, procedures or

presentation in court (35). Therefore, in the sub-sections to follow, we examine some of the legal systems and/or law enforcement challenges faced by digital forensics.

Jurisdiction - The increasing popularity of cloud computing has made conventional crime detection even more difficult. The very strengths of cloud computing, which allows anyone anywhere in the world to use publicly accessible software to process data stored in a virtual cyber-space location, could be put to devious use by criminals to store incriminating data on a server located beyond the jurisdiction of the courts of their country of residence, preferably in a State with no judicial cooperation treaty with that country (36). This makes court jurisdiction a challenge during prosecution.

Prosecuting Digital Crimes (Legal Process)- According to Lauren (37), prosecuting cyber-crime is no easy task, despite disparate laws. Even with today's forensic capabilities, legal inadequacies in various jurisdictions (not to mention uneven law enforcement and legal processes) make prosecution a very challenging task. This has created the need for new legislation that allows for digital evidence to be presented in any court of law or civil proceedings (38), as well as for the prosecution of digital crimes.

Current digital forensic investigations are based on the existing legal system or legal processes and supporting laws available. The infrastructure to investigate digital crimes is based on the prevailing cyber-laws, which makes it difficult to adopt specific digital forensic models to carry out digital investigations and prepare court admissible reports (38). Many digital forensic practitioners simply follow technical procedures and forget about the actual purpose and core concept of digital forensic investigation (39).

Admissibility of Digital Forensic Tools and Techniques - Given the enormous volumes of data currently handled by digital forensic inestigators, the admisibiltiy of digital forensic tools and techniques used to collect and analyse data is becoming a challenge. As with all other forensic disciplines, digital forensic techniques and tools must meet basic evidentiary and scientific standards to be allowed as evidence in legal proceedings (40). This also means that, the tools, techniques, processes and procedures should be capable of being proven correct through empirical testing. In the context of digital forensics, this means that the tools,

techniques, processes and procedures used in the collection and analysis of digital evidence data must be validated and proven to meet scientific standards if the results from such applications are to be acceptable as potential evidence in criminal cases.

Insufficient Support for Legal Criminal or Civil Prosecution - According to Mercuri (41), digital forensic techniques may be unfairly applied in order to tip the scales of justice in the direction of prosecution. Burgess (42) also states that, in the field of digital forensics (as in the field of law) procedures in civil cases differ somewhat from those in criminal cases. The collection of data and presentation of evidence may be held to different standards, the process of data collection and imaging can be quite different, and the consequences of the case may have very different impacts.

Ethical Issues - According to Bassett et al. (35), there are many ethical dilemmas with which investigators must be prepared to face during an investigation. One of the most common ethical concerns is managing the discovery of confidential data that is irrelevant to the case at hand. The question of what to do with irrelevant information arises. The general code of ethics to follow is that such information must be ignored because it is not relevant to the investigation. However, it is not always easy to ignore such information and any secrets that may be uncovered can weigh heavily on the mind of the investigator. Other ethical concerns may include: acknowledgement of errors by investigators on evidence data; bias during an investigation; maintaining control and responsibility for forensics equipment (35).

Privacy - Privacy issues usually arise in the case of an investigation. Privacy is very important to any organisation or victim. Though, in special cases the investigator may be required to share the data or compromise the client’s privacy to get to the truth. It is possible that the victim organisation may lose trust in the forensic team if, for example, private information is exposed (43). In addition, disclosure of any of the client’s information to the Internet community or the public by direct or indirect means can be a violation of privacy policies as well as the ethical code of conduct. Any type of electronic transaction that leads to disclosure of private information can also be taken as a violation of privacy policies and the code of ethics.

Confidential information should, therefore, be kept private by any forensic investigator. The next section elaborates on the personnel-related challenges faced by digital forensics.

Personnel-related Challenges

As with any potential forensic evidence, testimony that clearly establishes that the potential digital evidence has been under the control of responsible personnel and well-trained digital forensic investigators is required to assure the court of the fact that the evidence is complete and has not been tampered with in any way. In the sub-sections to follow, therefore, some of the identified personnel-related challenges faced by digital forensics are expalined in more details.

Lack of Qualified Digital Forensic Personnel (Training, Education and Certification)- According to Desai et al. (44), digital forensics (DF) has become an important field due to the increase in digital crimes. However, there is a shortage of trained digital forensic personnel in this field. The competition for employing digital forensic specialists in law enforcement is fierce. Qualified digital forensic experts are a challenge to find, even in the private sector. Even if technically proficient specialists are available, very few are trained or certified to deliver convincing, scientifically valid and expert witness testimony in a court of law or civil proceedings.

Semantic Disparities in Digital Forensics - Digital forensics is a growing field that is gaining popularity among many computer professionals, law enforcement agencies, forensic practitioners and other stakeholders who must always cooperate. Unfortunately, this has created an environment challenged with semantic disparities within the domain (45). Besides, cooperation between the computer professionals, law enforcement agencies and other forensic practitioners, presupposes the reconciliation of the semantic disparities that are bound to occur in the domain which is also a big challenge.

Lack of Unified Formal Representation of Digital Forensic Domain Knowledge - According to Hoss and Carver (2), there is currently no unified formal representation of digital forensic knowledge or standardised procedures for gathering and analysing knowledge. This lack of a unified representation inevitably results in

incompatibility among digital forensic analysis tools. Errors in analysis and in the interpretation of potential digital evidence are more likely where there is no formalised or standardised procedure for collecting, preserving and analysing digital evidence (46).

Lack of Forensic Knowledge Reuse among Personnel - According to Bruschi et al. (47), when detectives perform investigations and manage a huge amount of information, they make use of specialised skills and analyse a wide knowledge base of potential evidence. Most of the work is not explicitly recorded and this hampers external reviews and training. Past experience may and should be used to train new personnel, to foster knowledge sharing and reuse among detective communities, and to expose collected information to quality assessment by third parties. Hoss and Carver (2) adds that the preparation of potential digital evidence may often be inadequate to support legal action in court and/or civil prosecution, because the potential evidence and procedures utilised to extract the digital evidence did not adhere to the acceptable legal practices.

Forensic Investigator Licensing Requirements - In a paper by Schwerha (48), there has been a push in the United States to require digital forensic professionals to become licensed as private investigators. However, there are many reasons why digital forensic professionals should not be required to license as private investigators. Such requirement of licensure will limit the field unnecessarily as there are too many potential jurisdictions worldwide to allow the average practitioner to be licensed in every jurisdiction. Moreover, requiring digital forensic professionals to become licensed private investigators will create a big challenge to most average investigators worldwide. The requirement to be a licensed private investigator has little or no connection to the skill set that is necessary to be a high-quality digital forensics professional (48). In the next section the operational challenges faced by digital forensics are discussed.

Operational Challenges

According to Whitehead (49), digital crimes (perhaps more than any other type of crime), can be international in their operational scope. There is a need for basic guidelines for the evidence collection

process to be established worldwide. This ranges from broad principles that apply to nearly every investigation, through organisational practices so that a minimum standard of planning, performance, monitoring, recording and reporting is maintained, to recommended processes, procedures, software and hardware solutions. In this sub-section of the paper we explain in more details, some of the identified operational challenges faced by digital forensics.

Incidence Detection, Response and Prevention - Conventional IT environments with on-premises data processing mostly rely on an internal security incident management process that uses monitoring, log file analyses, intrusion detection systems, as well as data loss prevention (DLP) to detect intruders, attacks and data loss. According to Beham (50), detecting security incidents is often a challenge especially for cloud users. Moreover, incident response is needed because attacks frequently compromise personal and business data. It is critically important to respond quickly and efficiently when security breaches occur, so as to minimise the loss or theft of information and disruption of services caused by incidents (51).

Lack of Standardised Processes and Procedures - The lack of standardisation in digital forensics seriously hinders the investigation process (52) and makes it difficult to produce legally admissible digital evidence. There is currently no standardised digital forensic investigation process model for recovering potential digital evidence. According to Köhn et al. (5), the number of digital forensic models that exist has added to the complexity of the field. This has, therefore, led to a call for standardisation (4) so as to facilitate the investigation process. Recent research has also urged the need for new forensic techniques and tools that will be able to successfully investigate anti-forensics methods (53).

Significant Manual Intervention and Analysis - In most cases a physical hard drive image will have to be manually inspected and analysed. This process may be simple in a single drive, single partition, or a completely allocated disk drive. However, the process becomes complex and poses a challenge with multi-volume Redundant Array of Independent Disks (RAID) configurations (54). According to Ayers (55),

digital forensic analysis is a very complex undertaking. Thus, whenever the process is under manual control, mistakes will be made and bias could be introduced, even inadvertently.

Digital Forensic Readiness Challenge in Organisations - According to Mohay (16), forensic readiness is the extent to which computer systems or computer networks record activities and data in such a manner that the records are sufficient in their extent for subsequent forensic purposes, and the records are acceptable in terms of their perceived authenticity as evidence in subsequent forensic investigations. However, Cobb (56) states that digital forensic readiness sounds like a daunting challenge to most organisations.

With the advances in cloud computing, organisations have been forced to change the way they plan, develop and enact their IT strategies. According to Reilly et al., (57) cloud computing has not been thoroughly considered in terms of its forensic readiness. Hence, there is a definite need to consider current best practices to include, for example, certain aspects of digital forensic readiness in the existing practices to address the challenges brought about by lack of forensics readiness in organisations. Barske et al. (58) also adds that, although the need for digital forensics and digital evidence in organisations has been explored (as has been the need for digital forensic readiness within organisations); decision makers still need to understand what is needed within their organisations to ensure digital forensic readiness.

Trust and Audit Trails - The goal of digital forensics is to examine digital media in a forensically sound manner but with additional guidelines and trusted procedures designed to create legal audit trails. The proof of clear and original audit trails play a key role in the user accountability and digital forensics. However, it is possible that an intruder may edit or delete the audit trail on a computer, especially weakly-protected personal computers (59). Sophisticated rootkits that dynamically modify kernels of running systems to hide what is happening, or even to produce false results are also on the increase.

The next section presents a critical evaluation of the proposed taxonomy of challenges for digital forensics.

Critical Evaluation of the Proposed Taxonomy of Challenges for Digital Forensics

The taxonomy presented in this paper is a new contribution in the DF domain. The scope of the taxonomy is defined by the categories of the digital forensic challenges identified in Table 1. The main categories of the challenges as depicted in the taxonomy are technical challenges; legal systems and/or law enforcement challenges; personnel-related challenges, and operational challenges. These categories are further explained in terms of their scope. The sub-categories identified in the taxonomy include examples where applicable. The reader is again reminded that most of the sub-categories identified in the taxonomy were selected as common examples to facilitate this study and do not by any means constitute an exhaustive list.

The proposed taxonomy can be used in the digital forensic domain, for example, to explicitly describe processes and procedures that focus on addressing individual challenges. Moreover, the taxonomy in this paper can also help to map and categorise different digital forensic challenges, as well as create a common platform to share information in the digital forensic domain.

For the sake of training, education and certification, the sub-categories of the digital forensic challenges identified in the taxonomy can be used to give direction to institutions of higher learning, especially when developing curriculums and education material for different undergraduate programmes as well as research projects for postgraduate study. Such areas will help to produce programmes for specialists and generalists for the larger digital forensic industry. The taxonomy can also present new research opportunities to students – especially for those interested in how to resolve specific identified digital forensic challenges.

Developers of digital forensic tools can, further, use the taxonomy to fine-tune digital forensic tools to cover as many sub-categories of challenges as possible in the case of digital forensic investigations. Developers will also find the taxonomy in this paper useful, especially when considering new digital forensic tools and techniques for addressing specific challenges of interest in the digital forensic domain.

The proposed taxonomy can also be used to facilitate the assessment of existing or new tools to fully examine the extent to which it addresses the specific identified digital forensic challenges.

Individuals should also be able to use the proposed taxonomy to carefully and accurately identify and classify – with less effort – the different challenges faced by digital forensics. Without such taxonomy it would be hard and time consuming for anyone to be sure of the existence of certain specific challenges that they would want to explore further.

Finally, the taxonomy presented in this paper has been designed in such a way as to accommodate new categories of challenges and sub-categories that may emerge as a result of technological change or domain evolution. It should be possible for individuals to add new categories and sub-categories of the challenges, including potential modifications in any of the aforementioned categories or sub-categories. To the best of the authors' knowledge, there exists no other work of this kind in the domain of digital forensics; therefore, this is a novel contribution towards advancing the digital forensic domain.

Conclusions

The problem addressed in this paper involved the vast number of challenges faced by digital forensics. Despite numerous researchers and practitioners having studied and analysed various known digital forensic challenges for the last decade, there still exists a need for a formal classification of these challenges. This paper, therefore, presents a taxonomy of the various challenges faced by digital forensics to date. The taxonomy classifies the large number of digital forensic challenges into 4 well-defined and easily understood categories.

With the continued developments and research in digital forensics, the taxonomy can be of value to tools developers in assessing the extent to which existing and new digital forensic tools can address the identified challenges. Institutions of higher education can furthermore benefit from the taxonomy when developing educational material for different undergraduate programmes as well as research projects for postgraduate

studies. The taxonomy in this paper can easily be expanded to include additional categories and sub-categories of challenges that may crop up in the future.

Finally, as part of future work, the authors are now engaged in a research project to try and develop specifications and ontologies that create a unified formal representation of the digital forensic domain knowledge and information even more as a way towards resolving existing endemic disparities in digital forensics. However, much research still needs to be carried out so as to provide directions on how to address many of the challenges faced by digital forensics. More research also needs to be conducted to improve the taxonomy proposed in this paper and spark further discussion on the development of new digital forensic taxonomies.

Acknowledgements

The authors wish to thank the members of the Information and Computer Security Architecture (ICSA) research group, Department of Computer Science, University of Pretoria and Kabarak University, for their support throughout the process of writing this paper.

References

1. Webb, K.K. Predicting Processor Performance, Issues in Information Systems 2004; 5 (1):340-346.
2. Hoss, A.M. and Carver, D.L. Weaving Ontologies to Support Digital Forensic Analysis, ISI 2009; Richardson, TX, USA.
3. Kara L. N., Brian, H. and Matt, B. Digital Forensics: Defining a Research Agenda. Proceedings of the 42nd Hawaii International Conference on System Sciences 2009; 1-6.
4. ISO/IEC 27043. Information technology - Security techniques - Digital evidence investigation principles and processes (Draft). Available at: http://www.iso27001security.com/html/27043.html [Accessed September 17, 2013].

5. Köhn, M., Eloff, J.H.P., and Olivier M.S. Framework for a Digital Forensic Investigation, in H.S. Venter, J.H.P. Eloff, L. Labuschagne and M.M. Eloff (Eds), proceedings of the ISSA 2006 from Insight to Foresight Conference, Sandton, South Africa.
6. Altschaffel, R., Kiltz, S., and Dittmann, J. From the Computer Incident Taxonomy to a Computer Forensic Examination Taxonomy. Proceedings of the Fifth International Conference on IT Security Incident Management and IT Forensics.
7. Hoefer, C.N. and Karagiannis, G. Taxonomy of cloud computing services. Proceedings of the IEEE GLOBECOM workshop on enabling the future service-oriented internet 2010; 1345-1350.
8. Strauch, S., Kopp, O., Leymann, F. and Unger, T. A Taxonomy for Cloud Data Hosting Solutions, Ninth IEEE International Conference on Dependable, Autonomic and Secure Computing 2011.
9. Lupiana, D., O'Driscoll, C. and Mtenzi, F. Taxonomy for Ubiquitous Computing Environments, First International Conference on Networked Digital Technologies 2009;469-475.
10. Sansurooah, K. Taxonomy of computer forensics methodologies and procedures for digital evidence seizure. Originally published in the Proceedings of the 4th Australian Digital Forensics Conference (Security Research Institute Conferences) 2006. Edith Cowan University, Perth, Western Australia.
11. Sriram, R. Digital Forensic Research: Current State-of-the-Art. CSI Transactions on ICT 2013; 1(1):91-114. Available at: http://securecyberspace.org/yahoo_site_admin/assets/docs/df-survey.334154504.pdf [Accessed June 22, 2013].
12. Garfinkel, S. Digital forensics research: The next 10 years. Digital Investigation 2010, 7:S64-S73.
13. Gallegos, F. Computer Forensics: An Overview. Information Systems Audit and Control Association (ISCA) 2005, vol. 6, Available at: http://www.isaca.org/Journal/Past-Issues/2005/Volume-6/Documents/jpdf0506-Computer-Forensics-An.pdf [Accessed February 18, 2013].
14. Thinkquest. Cryptanalysis: Introduction. Available at: http://library.thinkquest.org/27993/crypto/classic/analysis1.shtml [Accessed April 8, 2013].

15. Lowman, S. The Effect of File and Disk Encryption on Computer Forensics. Available at: http://lowmanio.co.uk/share/The%20Effect%20of%20File%20and%20Disk%20Encryption%20on%20Computer%20Forensics.pdf [Accessed February 21, 2013].
16. Mohay, G. Technical Challenges and Directions for Digital Forensics, Proceedings of the First International Workshop on Systematic Approaches to Digital Forensic Engineering, 2005:155-161.
17. Libby, D.A. Distributed Computer Forensics: Challenges and Possible Solutions, Available at: http://selil.com/archives/2668 [Accessed February 16, 2013].
18. Arthur, K.K., and Hein S.V. An Investigation into Computer Forensic Tools. Proceedings of the ISSA conference 2004. Midrand, South Africa.
19. Richard, G.G. and Roussev, V. Digital Forensics Tools - The Next Generation, Idea Group Inc, 2006:76-91.
20. DOJ. Volatility of digital evidence, Available at: http://www.policeone.com/police-products/investigation/tips/1655664-Volatility-of-digital-evidence/ [Accessed February 18, 2013].
21. Taute, B., Grobler, M. and Nare, S. Forensic Challenges for Handling Incidents and Crime in Cyberspace, Available at: http://researchspace.csir.co.za/dspace/bitstream/10204/3756/1/Taute_d1_2009.pdf [Accessed February 18, 2013].
22. Conserve O Gram. Digital Storage Media, National Service Park 2010, Number 22/5.
23. Reed, T. Time vs Technology and the Frailty of Digital Media, Available at: http://filmcourage.com/content/time-vs-technology-and-the-frailty-of-digital-media [Accessed August 15, 2013].
24. Harvey, R. Preserving Digital Materials - Google Books. Available at: http://books.google.co.za/books?id=Z_8glIHqKgQC&pg=PA128&lpg=PA128&dq=Limited+lifespan+of+digital+media&source=bl&ots=Qf3rNzycwR&sig=PtQPJhmT6dlifT-

dPDGDAzfYCmI&hl=en&sa=X&ei=Dz8iUebCMcmwhAe4hYDIBQ&ved=0CEoQ6AEwBQ#v=onepage&q=Limited%20lifespan%20of%20digital%20media&f=false [Accessed February 18, 2013].

25. ACPO. Good Practice Guide for Computer-Based Electronic Evidence. Available at: http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf [Accessed February 16, 2013].
26. Eroraha, I. Real-World Computer Forensics Challenges Facing Cyber Investigators, Computer Forensics Show 2010.
27. Sheward, M. Rock Solid: Will Digital Forensics Crack SSD's? Available at: http://resources.infosecinstitute.com/ssd-forensics/ [Accessed February 18, 2013].
28. Elancheran, A. Computer Forensics, Available at: http://uwcisa.uwaterloo.ca/Biblio2/Topic/ACC626%20Computer%20Forensics%20A%20Elancheran.pdf [Accessed February 18, 2013].
29. Garfinkel, S. Anti-Forensics: Techniques, Detection and Countermeasures, 2nd International Conference on i-Warfare and Security, 20087: 77-84.
30. Liu, V. and Brown, F. Bleeding-Edge Anti-Forensics, Infosec World Conference & Expo 2006, MIS Training Institute.
31. Bennett, W.D. The Challenges Facing Computer Forensics Investigators in Obtaining Information from Mobile Devices for Use in Criminal Investigations, Available at: http://articles.forensicfocus.com/2011/08/22/the-challenges-facing-computer-forensics-investigators-in-obtaining-information-from-mobile-devices-for-use-in-criminal-investigations/ [Accessed February 16, 2013].
32. Yates, M. Practical Investigations of Digital Forensics Tools for Mobile Devices, Proceedings of the Information Security Curriculum Development Conference, 2010:156-162.

33. Ferguson, R.I. Challenges in Digital Forensic Research. Available at: http://scone.cs.st-andrews.ac.uk/cybersecurity/slides/Ferguson-DigitalForensicsResearchChallenges.pdf [Accessed June 20, 2013].
34. Leslie, W., Will, V. and Edgar, A.W. Meeting the Challenges of Cloud Computing. Available at: http://www.accenture.com/us-en/outlook/Pages/outlook-online-2011-challenges-cloud-computing.aspx [Accessed June 20, 2013].
35. Bassett, R., Bass, L. and O'Brien, P. Computer Forensics: An Essential Ingredient for Cyber Security. Journal of Information Science and Technology 2006: 22-32.
36. Vaciago, G. Cloud Computing and Data Jurisdiction: A New Challenge for Digital Forensics. Proceedings of the third International Conference on Technical and Legal Aspects of the e-Society, CYBERLAWS 2012.
37. Lauren, M. Info-security - Cybercrime Knows No Borders. Available at: http://www.infosecurity-magazine.com/view/18074/cybercrime-knows-no-borders-/ [Accessed February 16, 2013].
38. Khan, A., Uffe, K.W. and Nasrullah, M. Digital Forensics and Crime Investigation: Legal Issues in Prosecution at National Level, Fifth International Workshop on Systematic Approaches to Digital Forensic Engineering, 2010:133- 140.
39. Ieong, R.S.C. FORZA-Digital Forensics investigation framework that incorporate legal issues, Digital Investigation: The International Journal of Digital Forensics & Incident Response 2006;3:29-36.
40. Craiger, P., Swauger, J., Marberry, C. and Hendricks, C. Validation of Digital Forensics Tools. Digital Crime and Forensic Science in Cyberspace, edited by Panagiotis Kanellis, Evangelos Kiountouzis, Nicholas Kolokotronis, and Drakoulis Martakos© 2006, Idea Group Inc.
41. Mercuri, R. Criminal Defense Challenges in Computer Forensics, In Proceedings of the Digital Forensics and Cyber Crime Conference, ICDF2C 2009, Albany, NY, USA.

42. Burgess, S. Computer Forensics - Criminal vs Civil: What's the Difference? Available at: http://www.burgessforensics.com/Civ_Criminal.php [Accessed February 23, 2013].
43. Anon. Computer Forensics Privacy Issues. Available at: http://www.computerforensics1.com/privacy-computer-forensic.html [Accessed February 23, 2013].
44. Desai, A.M., Fitzgerald, D. and Hoanca, B. Offering a Digital Forensics Course in Anchorage, Alaska. Information Systems Education Journal 2009, 7(35). http://isedj.org/7/35/. ISSN: 1545-679X. (A preliminary version appears in The Proceedings of ISECON 2006: §5114. ISSN: 1542-7382).
45. Karie, N.M. and Venter, H.S. Significance of Semantic Reconciliation in Digital Forensics. In the proceedings of the Digital Forensics, Security and Law conference, 2013:71-80, Richmond, Virginia USA.
46. Chaikin, D. Network investigations of cyber-attacks: the limits of digital evidence, Crime Law Soc. Change 2006, 46: 239-256.
47. Bruschi, D., Martignoni, L. and Monga, M. How to Reuse Knowledge about Forensic Investigations, in 'Proceedings of Digital Forensic Research Workshop 2004'. Baltimore, MD, USA.
48. Schwerha, J.J. Why computer forensic professionals shouldn't be required to have private investigator licenses, Digital Investigation: The International Journal of Digital Forensics & Incident Response 2008, 5(1-2):71-72.
49. Whitehead, A. Weakness in Computer Forensics. Available at: http://free-backup.info/weaknesse-in-computer-forensics.html [Accessed February 23, 2013].
50. Beham, G. Incident Detection and Cloud Forensics – Security at a Glance, Available at: http://ipbr.wordpress.com/2012/08/30/incident-detection-and-cloud-forensics/ [Accessed February 16, 2013].

51. Cichonski, P., Millar, T., Grance, T. and Scarfone, K. Computer Security Incident Handling Guide 2012, Revision 2, NIST Special Publication 800-61.
52. Leigland, R. and Krings, A.W. A Formalization of Digital Forensics, International Journal of Digital Evidence 2004, 3(2):1-32.
53. Alharbi, S., Weber-Jahnke, J., and Traore, I. The Proactive and Reactive Digital Forensics Investigation Process: A Systematic Literature Review. International Journal of Security and Its Applications 2011 October, 5(4):59-71.
54. King, G.L. Forensics Plan Guide – Forensic Investigation Plan Cookbook 2006, SANS Institute, Computer Forensics and Incidence Response
55. Ayers, D. A second generation computer forensic analysis system. Digital Investigation: The International Journal of Digital Forensics & Incident Response 2009, 6:S34-S42.
56. Cobb, M. Digital forensic investigation procedure: Form a computer forensics policy, Available at: http://www.computerweekly.com/tip/Digital-forensic-investigation-procedure-Form-a-computer-forensics-policy [Accessed February 18, 2013].
57. Reilly, D., Wren, C. and Berry, T. Cloud Computing: Pros and Cons for Computer Forensic Investigations, International Journal of Multimedia and Image Processing (IJMIP) 2011 March; 1(1).
58. Barske, D., Stander, A. and Jordaan, J. A Digital Forensic Readiness Framework for South African SME's, Proceedings of ISSA Conference 2010.
59. Yong, G. Digital Forensics: Research Challenges and Open Problems. Available at: http://itsecurity.uiowa.edu/securityday/documents/guan.pdf [Accessed June 21, 2013].

Additional information and reprint requests:

Nickson M. Karie, MSc.

Department of Computer Science, Kabarak University,

Private Bag - 20157, Kabarak, Kenya.

E-mail: menza06@hotmail.com