Towards a General Ontology for Digital Forensic Disciplines

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

[1]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*:* Ontologies are widely used in different disciplines as a technique for representing and reasoning about domain knowledge. However, despite the widespread ontology-related research activities and applications in different disciplines, the development of ontologies and ontology research activities are still wanting in digital forensic disciplines.

This paper therefore presents the case for establishing an ontology for digital forensic disciplines. Such an ontology would enable better categorisation of digital forensic disciplines, as well as help with the development of methodologies that can offer direction in different areas of digital forensics, such as professional specialisation, certifications, development digital forensic tools, curricula and educational materials. In addition, the ontology presented in this paper can be used, for example, to better organise digital forensics domain knowledge and explicitly describe the discipline's semantics in a common way. Finally, this paper is meant to spark discussions and further research on an internationally agreed ontological distinction of the digital forensic disciplines. Digital forensic disciplines ontology is a novel approach towards organising the digital forensics domain knowledge and constitutes the main contribution of this paper.

KEYWORDS: forensic science, digital forensics, ontology, ontological distinction, digital forensics disciplines, digital forensics sub-disciplines

` Ontology, as defined by Van Rees (1), is a set of well-defined concepts describing a specific domain of interest. According to Grüber (2), an ontology is a specification of a conceptualisation. More precisely, Smith et al (3) defines ontology as an explicit formal specification of how to represent entities that exist in a given domain of interest and the relationships that hold among them. However, for an ontology to be useful, it must represent a shared, agreed-upon conceptualisation (4), in other words it should be accepted by a group or community.

Ontologies have been used in many contexts and for many purposes (5). In recent years, however, the development of ontology has become common in many different domains (6). This is backed up by the fact that ontologies can be used to generate a common definition, knowledge and understanding (1) of a domain. Therefore, to help create a common definition that enhances the sharing and reuse of formal represented knowledge (2) in digital forensics (DF), it is important to develop ontologies that define the common entities in which the shared knowledge in this field can be represented. Ontologies in DF can also promote the reasoning about existing disciplines and sub-disciplines within the domain, as well as describe the domain.

This paper presents an ontology for the DF disciplines in an attempt to advance the domain and enhance the sharing and reuse of formal represented knowledge (2) in DF. In the authors' opinion, the ontology presented here can be viewed as a formal way of representing shared knowledge in the digital forensics domain. It can also be used to organise and reason over existing digital forensics disciplines in such a way that deductive inferences can be made (7).

The presentation in this paper is, therefore, a novel contribution in the digital forensics domain and offers a simplified platform that can help individuals comprehend the existing DF disciplines with much less effort. Moreover, the ontology has been simplified to accommodate new digital forensic disciplines and sub-disciplines that may crop up in the future as a result of technological change or domain evolution. Finally, individuals, organisations and academic institutions with an interest in areas of professional specialisation,

certification, and development of digital forensic tools, curricula and/or development of educational materials should find the ontology constructive.

Background

Digital forensics is a relatively new and growing field (10) that is gaining popularity among many computer professionals, law enforcement agencies, practitioners and other stakeholders who need to cooperate in this profession. In addition, there is a strong demand for standardisation in many areas of digital forensics, for example the digital forensic investigation process (58). The number of forensic models that exist has added to the complexity of the field (60) and has led to a call for standardisation (62) so as to facilitate the investigation process (61). Recent research has also urged the need for new forensic techniques and tools that will be able to successfully investigate anti-forensics methods (59).

In a growing field like DF, developing practical methodologies for different areas is essential and as important as the research itself. Methodologies need to be developed for areas such as professional specialisation, certification, and development of digital forensic tools, curricula and/or development of educational materials. The authors believe that the ontology presented in this paper can help to provide direction in different areas of DF (such as those mentioned above).

Ontologies have been widely used in different fields as a technique for representing and reasoning about domain knowledge (1, 5). In addition, ontologies can be used to better organise domain knowledge and explicitly describe domain semantics in a common way.

As discussed by Brusa et al (12) ontology development can be divided into two phases: a specification phase and a conceptualisation phase. The goal of the specification phase is to acquire informal knowledge about the domain. In the case of this paper, the goal of the conceptualisation phase is to organise and structure this knowledge by using external representations. Basically, the main reasons for developing an ontology in any domain are to share a common understanding of the structure of information among entities in a bid to enable the reuse of domain knowledge and to make explicit those assumptions about a domain

that are normally implied (13). If assumptions that underlie an implementation are made explicit in an ontology, then it is relatively easy to change the ontology when knowledge about the domain changes (13).

Hence, developing ontologies that define the common entities in which shared DF knowledge can be represented can help create uniformity and common understanding in representing DF disciplines. In the authors' opinion, uniformity and a common understanding can as well enhance and improve cooperation among computer professionals, law enforcement agencies and practitioners in the case of a digital forensic investigation. In the section that follows we examine ontology-related work in the digital forensics domain.

Related Work

Very little literature on issues related to ontology development for the digital forensics domain was available at the time of writing this paper. As a matter of fact, even what is present in literature seems to be somewhat varied. However, several previously proposed ontologies within the digital forensics domain have made valuable contributions to the development of the ontology in this paper. What follows hereafter is therefore a summary of some of the related research work on ontology development in digital forensics.

To begin with, in 2006 Brinson et al (8) presented a detailed cyber-forensics ontology in an effort to create a new way of studying cyber forensics. This ontology consists of a five-layered hierarchical structure with the final layer being specified areas that can be used for certification and specialisation. In a different paper, David and Richard (9) introduced the Small-Scale Digital Device Forensics (SSDDF) ontology. They proposed an ontology to provide law enforcement with the appropriate knowledge regarding the devices found in the Small-Scale Digital Device (SSDD) domain. Additionally, they suggest that this ontology can be used as a method to further the development of a set of standards and procedures at which to approach SSDD.

Jasmine and Zoran (63) in there paper highlights the problems encountered by investigators in the pursuit of forensic investigations of digital devices, primarily because of misunderstanding or false understanding

of certain important concepts. They further propose an ontology of digital evidence as one of possible method suitable as a solution of this problem.

In 2009 Allyson and Doris (10) discussed the concept of 'Weaving Ontologies to Support Digital Forensic Analysis'. In their paper they argue that numerous challenges currently face digital forensic analysis. Although there are a variety of techniques and tools to assist with the analysis of digital evidence, they inadequately address key problems such as the vast volumes of data, lack of unified formal representation or standardised procedures, incompatibility among heterogeneous forensic analysis tools, lack of forensic knowledge reuse, and lack of sufficient support for legal criminal/civil prosecution (10). Their paper goes further and suggests the applicability and usefulness of weaving ontologies to address some of these problems. It introduces an ontological approach that can lead to future development of automated digital forensic analysis tools.

Turk (11) presents an ontology that can be used to map a research area, design a curriculum, structure the agenda of a conference, provide keywords and classifications for bibliographic databases, or provide knowledge management in general.

There also exist other related works on ontologies, but neither those nor the cited references in this paper have presented an ontology of the digital forensics disciplines in the way that is introduced in this paper. We obviously acknowledge the fact that the previous work on ontologies has offered useful insights toward the development of the ontology in this paper. In the section that follows we provide a detailed explanation of our ontology on the digital forensic disciplines.

The Digital Forensics Disciplines Ontology

In this section of the paper, we present a detailed explanation of the ontology on the digital forensics disciplines and sub-disciplines within the domain of DF. Figure 1 shows the structure of the ontology. Note that, due to the small font size of Figure 1, Figures 2 to 7 contains enlarged extracts of the entire ontology as depicted in Figure 1.

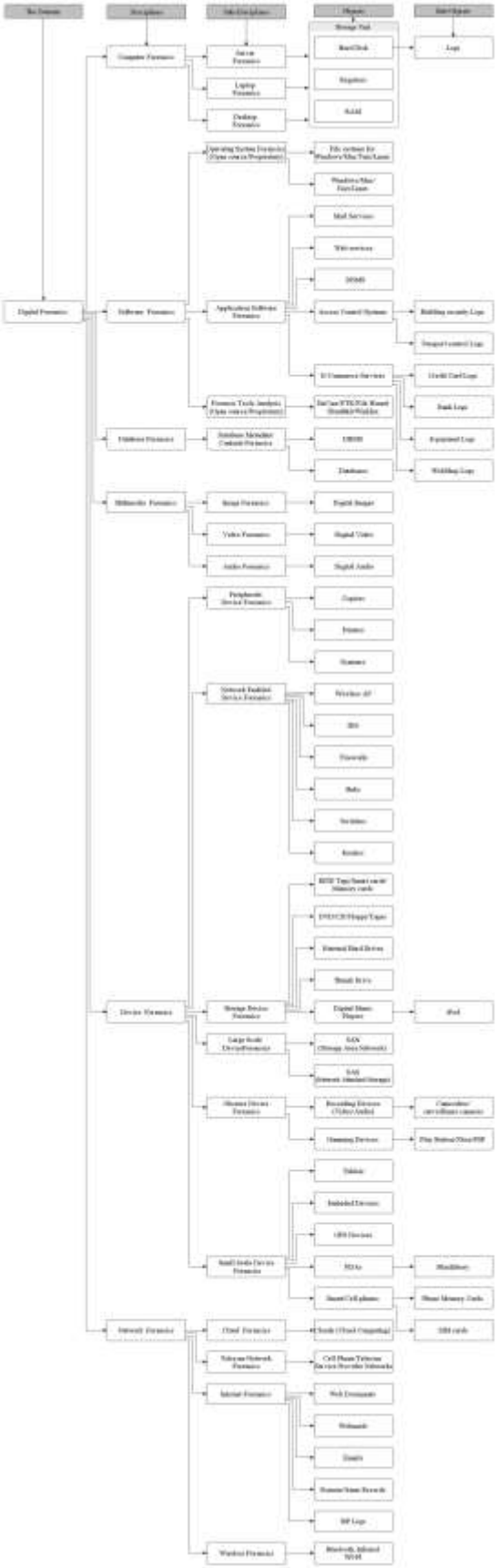

FIG. 1—DF disciplines ontology.

The ontology consists of five layers arranged from left to right and with the first layer depicting the main domain of focus (i.e. digital forensics). This is followed by the DF disciplines in the second layer, and the sub-disciplines within the DF domain in the third layer. Objects and sub-objects are introduced in the fourth and fifth layers of the ontology as a way of representing individual and specific finer details of the sub-disciplines within DF. In the authors' opinion, organising the ontology into disciplines, sub-disciplines, objects and sub-objects was necessary to simplify the understanding of the ontology as well as to present specific finer details of the ontology.

In addition, the sub-disciplines, objects and sub-objects presented in the ontology focus more on areas that can be considered for professional specialisation and certification, as well as for the development of digital forensic tools, curricula and educational materials. However, infer from the ontology in Figure 1 that the objects and sub-objects listed were only selected as common examples to facilitate this study and should not be treated as an exhaustive list. More sub-disciplines, objects and sub-objects can and should be added as the need arises in future.

Note that from the ontology in Figure 1, some of the objects presented do not have sub-objects; in the authors' opinion, breaking them down to a finer-grained level would be superficial at this stage. However, in future it should be possible to mention sub-objects that can be incorporated under the applicable objects, especially when developing curricula and education materials. The major digital forensics disciplines explored in this study (with their details as shown in Figure 1) include computer forensics, software forensics, database forensics, multimedia forensics, device forensics, and network forensics.

For the purpose of this study, computer forensics is divided into server forensics, laptop forensics and desktop forensics, while software forensics focuses on application software forensics; operating system forensics (open source and proprietary) and forensic tools analysis (open source and proprietary).

Database forensics concentrates on database contents and/or database metadata, while multimedia forensics is divided into digital image forensics, digital video forensics and digital audio forensics. Device

forensics is divided into peripheral device forensics, network-enabled device forensics, storage device forensics, large-scale device forensics, small-scale device forensics and obscure device forensics. Finally, the ontology concludes with network forensics, which is divided into cloud forensics, telecom network forensics, internet forensics and wireless forensics.

In the sub-sections that follow the digital forensics disciplines and sub-disciplines, as identified in the ontology in Figure 1, are explained in more detail.

Computer Forensics

According to Crouch (14), computer forensics is a branch of digital forensics that uses analysis techniques to gather potential evidence from desktops, laptops and server computers for investigating suspected illegal or unauthorised activities. More precisely, computer forensics focuses on finding potential digital evidence after a computer security incident has occurred (15). Note that we refer to 'potential' evidence throughout the paper, since digital artefacts are only considered to be 'evidence' in one of the final phases of the digital forensic investigation process, namely the reporting phase. This also implies that, for the collected potential evidence to be considered as competent evidence (50), it must possess scientific validity grounded in scientific methods and procedures. The potential evidence gathered in most cases is usually found stored on the computers' internal storage unit (see Figure 2), which includes the hard disk that also stores operating system data (e.g. log files) and application/user data (e.g. word processor files). Computer forensics also considers the value of data that may be lost by powering down a computer, and thus collection of potential evidence can be conducted while the system is still running e.g. from the Random Access Memory (RAM) or registers.

The goal of computer forensics is to perform a structured investigation while maintaining a documented chain of evidence that can withstand the legal scrutiny of a court of law, whether for a criminal or civil proceeding (14). For the purpose of this paper the areas covered under computer forensics include server forensics, laptop forensics and desktop forensics (see Figure 2 below).

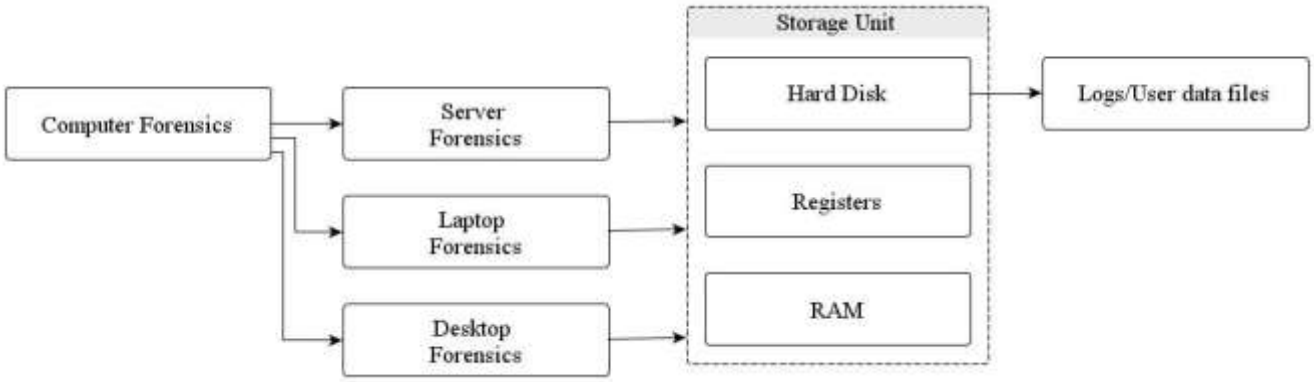

FIG. 2—Computer forensics.

Server Forensics

In a network environment a server is usually that powerful computer that is dedicated to managing mass system and user resources. Server forensics, therefore, focuses on finding digital evidence that is stored within the server machine (16). In essence, server forensics deals with finding potential evidence in the same way that potential evidence is found on a desktop or laptop computer, the only difference being the significantly larger storage and somewhat different access capabilities to be dealt with on a server computer.

Laptop Forensics

Laptop forensics is dedicated to finding digital evidence from laptop computers. Laptops are designed to be light and mobile. Because of their mobile nature, laptops are popular computing systems and high contenders for hosting potential evidence. The hardware in a laptop is typically custom built for that particular model. According to Pierce (17), very few components follow any given industry standard. This issue particularly complicates the process of digital forensic analysis on laptops and should be handled by a specialist who understands its configuration. However, laptop forensics still form part of computer forensics.

Desktop Forensics

Desktop forensics is meant to find digital evidence from desktop computers once a security incident has occurred. Since there are so many different ways to classify computers (8), the ones discussed above (server, laptop and desktop) serve as examples to facilitate this study. With the advancement in technology it should sooner or later be necessary to add other items to this category.

Software Forensics

Software forensics is a discipline concerned with uncovering potential evidence through examining software. However, according to MacDonell et al (18), software forensics is also a research field that attempts to investigate aspects of computer program authorship by treating pieces of program source code as linguistically and stylistically analysable entities. Software forensics can be used, for example, to detect plagiarism in an academic setting where students' assignments can be compared to see if some are "suspiciously similar" (18, 19).

According to Hanks et al (44), incidents and accidents that can be attributed to software failure often result in tragedies and other losses. The need to learn from these events turns out to be more critical as software systems become more complex and the ways they can fail become less intuitive (44). Moreover, according to Johnson (45, 46), existing software development methods do not provide clear access to retrospective information about the complex and systemic causes of incidents and accidents. In addition, what is known from forensic engineering generally, as well as the study of failure, has yet to be applied comprehensively to software (46). Software forensics (also known as software forensic engineering) can therefore be used to address such deficiencies.

A vast number of computer programs (software) are available on the software market today. However, for the purpose of this paper, the authors considered only a few. For that reason, the reader is advised to consider other software as well, especially when developing curricula and/or education materials. The list of

software used in this study serves only as examples and, hence, should not be perceived as an exhaustive list. For the purpose of this paper, software forensics covers operating system forensics, application software forensics and digital forensic analysis tools (as shown in Figure 3).

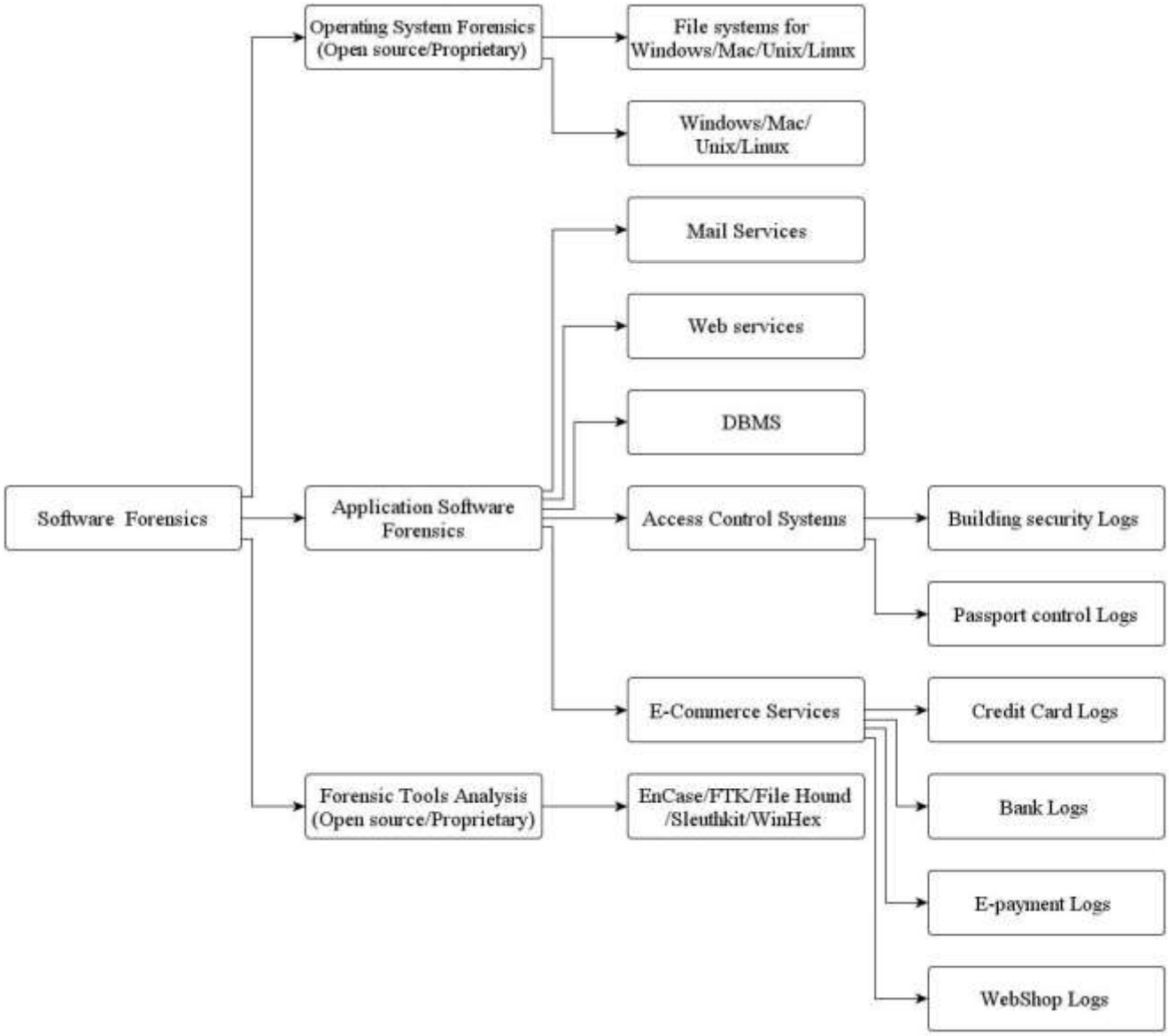

FIG. 3—Software forensics.

Operating System Forensics

The operating system serves as the primary software installed on any computer system and is often perceived as part and parcel of the entire computer system. Therefore, in the case of a digital investigation, the investigator should be aware of the fact that many different operating systems are available, each with its own associated file structures. By knowing in advance what particular operating system needs to be dealt with, the investigator is able to search for and locate any potential digital evidence more effectively (8).

In addition, operating systems may be categorised as open source or proprietary. Among the common and well-known operating systems are Windows, Mac, Unix and Linux, and an investigator should be acquainted with these operating systems and their different file systems in particular.

Application Software Forensics

Application software is basically designed to help end users perform specific tasks. They either come bundled together with the computer system or can be purchased separately and installed later on the system. Application software forensics focuses on analysing and retrieving potential evidence from application software such as email services, access control systems (e.g. building security logs and passport control logs), web services, database management systems, and E-commerce services (e.g. credit card logs, bank logs, e-payment logs and web shop logs) as shown in Figure 3.

Forensic Tools Analysis

There are many different open-source and proprietary digital forensic tools available for use during digital investigations. Some of the commonly known DF tools used include Encase (51), Forensic Toolkit (FTK) (52) and Sleuth kit (53). These tools are designed to perform a collection of digital forensic investigation functions and would basically include most of the investigation techniques applied during a digital investigation process. However, there exist other digital forensic investigation tools that perform more elementary investigation functions such as WinHex, which is essentially a universal hexadecimal

editor. Such a utility is particularly helpful in viewing any data in its raw form in order to perform low-level data analysis. X-Ways Imager is yet another example of such an elementary tool, which is basically a forensic disk imaging tool only (54).

Database Forensics

Database forensics, as explained by Olivier (21) and Weippl (22), focuses on databases and their related content and/or metadata. Most business' critical and sensitive information is usually recorded and stored in databases, e.g. bank accounts and medical data. Unlawful disclosure, modification and/or theft of such data can be harmful to organisations. Therefore, database forensics aims at investigating unlawful disclosure, modification and/or theft of data within a database in a bid to track down any perpetrators with such malicious intent (22, 23). An investigator's understanding of database concepts and how to use database management systems (DBMS) is clearly of crucial importance to database forensics (see Figure 4).

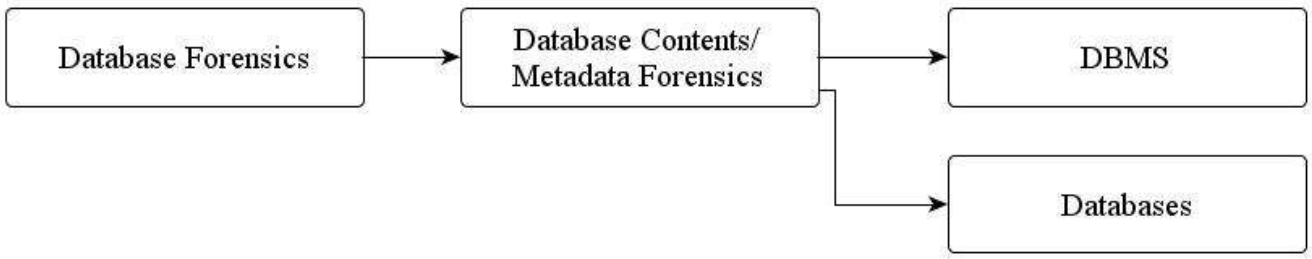

FIG. 4—Database forensics.

Multimedia Forensics

In today's digital age, the creation and manipulation of digital images, videos and audio have been simplified through digital processing tools that are easily and widely available (24). Such tools may include, but are not limited to, Adobe Photoshop CS6 (47), Adobe Premiere Pro CS6 (48) and Pinnacle Studio (49). Adobe Photoshop CS6 is mostly used for picture and photo editing, while Adobe Premiere Pro and Pinnacle

Studio are typically used for video editing. This implies that the authenticity of images, videos and audio can no longer be taken for granted (24). According to Böhme et al (25), questions regarding media authenticity are of growing relevance and of particular interest in court, where consequential decisions might be based on evidence in the form of digital media. Multimedia forensics can be used to uncover the authenticity information of captured images, videos and audio files. Such information can also serve as potential evidence to be presented in a court of law or in civil proceedings. The main areas covered by multimedia forensics in this paper (as shown in Figure 5) include image forensics, video forensics and audio forensics. They are explained briefly in the sub-sections that follow.

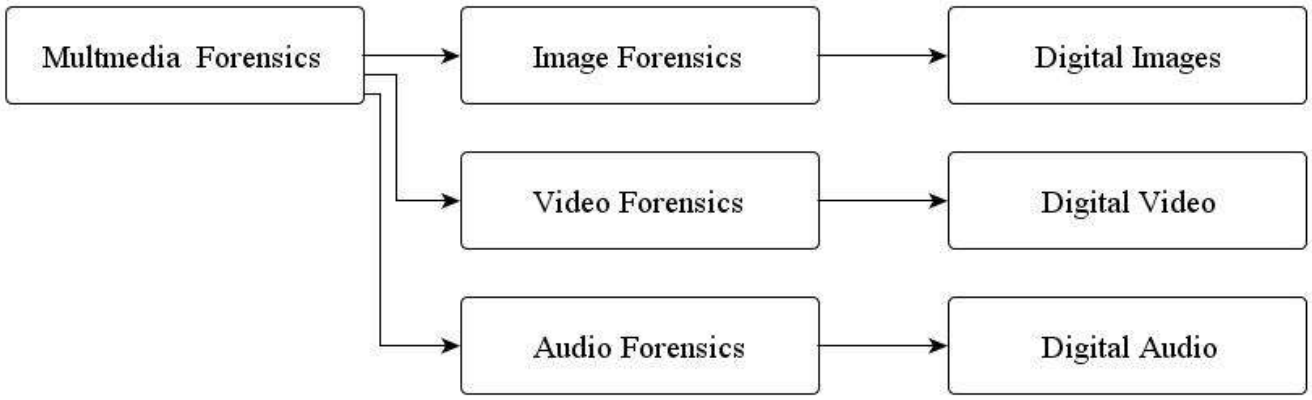

FIG. 5—Multimedia forensics.

Digital Image Forensics

Digital image forensics is concerned with uncovering potential digital evidence found within digital images (24). This may include digital evidence such as image origin (often referred to as image file type identification), image source identification and image forgery detection (26). Digital image forensics can, thus, also be used to verify the authenticity of images (27, 28).

Digital Video Forensics

Digital video forensics, like digital image forensics, is concerned with uncovering potential digital evidence found within video files. With the advent of high-quality digital video cameras and sophisticated video-editing software, it is becoming increasingly easier to tamper with digital video (29). Digital video forensics can be used to good effect to detect cloning or duplicating frames, or even parts of a frame when people or objects have been removed from a video (29, 30, 31).

Digital Audio Forensics

Digital audio forensics may be defined as the application of audio science and technology in a bid to investigate and establish facts in criminal or civil courts of law. Digital audio forensics is meant to uncover potential digital evidence about audio files. This may include, for example, environment recognition from digital audio files (32). Environment recognition refers to the physical environment under which digital audio samples were recorded. Audio forensics can also be used to determine what kind of microphones were used (33).

Device Forensics

Device forensics is a branch of digital forensics that deals with the gathering of digital evidence from different types of devices. Devices may range from small-scale devices such as mobile phones, Personal Digital Assistants (PDAs), printers, scanners, cameras, fax machines (34) etc., to large-scale devices such as the SAN (Storage Area Network) and NAS (Network Attached Storage) systems. The number of devices in this discipline of digital forensics is increasing daily and hence, in the authors' opinion, is the motivation why device forensics can be considered a separate and vast discipline of the digital forensics domain. For the purpose of this ontology, device forensics is divided into peripheral devices, network-enabled devices, storage devices, large-scale devices, small-scale devices, and obscure devices (see Figure 6). This list should not be considered as exhaustive as most new digital devices could well be categorised within this discipline of the digital forensic ontology.

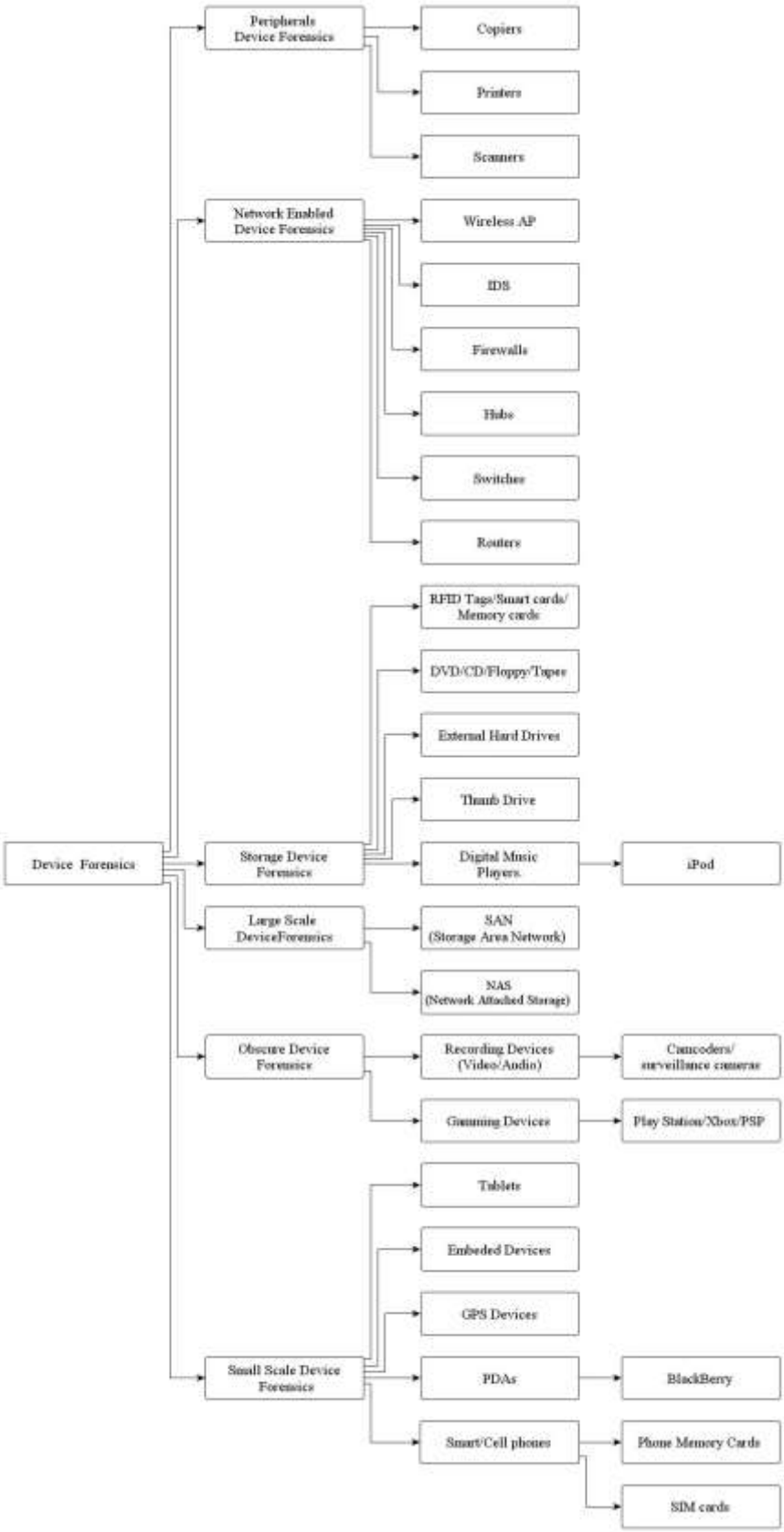

FIG. 6—Device forensics

.Peripheral devices

Peripheral devices are normally used to expand a system's capabilities; however, they do not actually form part of the core computer architecture. In addition, peripheral devices vary greatly and can range from external to internal peripherals. For example, external peripherals may include a mouse, keyboard, printer, monitor and scanner, among many others. Examples of internal peripheral devices (often referred to as integrated peripherals) may include devices such as a CD-ROM drive and internal modems. A thorough analysis of peripheral devices can reveal much information that is of potential value to a digital forensic investigator.

Network-enabled device forensics

With the development of network and telecommunication technologies, communication infrastructure has rapidly spread in many sectors of the industry. As a result, various network-enabled devices with Ethernet and Transmission Control Protocol/Internet Protocol (TCP/IP) communication functions can be found in different practical applications (35). Such devices may include Intrusion Detection Systems (IDSs), firewalls, hubs, switches, routers and wireless access points (to mention a few). Some of the network-enabled devices have the ability to store data and information and therefore such information can serve as potential evidence during an investigation.

Storage Device Forensics

A storage device is any hardware device that has been specifically designed to store data and information. Storage devices can be primary to a computer (e.g. the RAM) or they can be secondary (e.g. DVD, CD, Tapes, Radio-Frequency Identification (RFID) tags, smart cards, memory cards (flash drives) and external hard drives). Such devices can contain valuable potential evidence in the case of an

investigation. Hence, an investigator should be aware of the different capabilities supported by different storage devices.

Large-scale Device Forensics

Nowadays, investigators and analysts increasingly have to deal with large (terabyte-sized) data sets when conducting digital investigations (36). Such large data sets are mostly found stored in large-scale devices such as the SAN (Storage Area Network) and NAS (Network Attached Storage) systems. With the evolution in large-scale storage systems technology, it is possible that petabyte storage will soon replace terabyte-sized devices (43). Petabyte-sized storage is considered the newest frontier in the ever-growing world of data storage devices (43). Therefore, an investigator needs to know how these devices operate in order to be able to effectively gather potential digital evidence. Like any other device, large-scale devices can provide potential evidence that can be presented in a court of law or in civil proceedings.

Small-scale Device Forensics

Small-scale devices, as the name suggests, are small and versatile. In addition, the proliferation of hand-held digital devices has captured the majority of the market and is primed to become the next frontier in technology (9). Therefore, a clear understanding of how these devices operate is necessary to adequately preserve, identify, and extract useful information during a digital forensic investigation (8). Examples of small-scale devices include, but are not limited to, tablets, embedded devices, Global Positioning System (GPS) devices, Personal Digital Assistants (PDAs), mobile (smart) phones, etc. Mobile phones, for example, are becoming a focus of attraction in digital forensic investigations due to the feature-rich versatility of these devices. When dealing with mobile phone device forensics, the two main artefacts of interest that may contain potential evidence are SIM (Subscriber Identity Module) cards and memory cards, of which the latter may be built in (on-board).

Obscure Device Forensics

Obscure devices are those devices that, in the opinion of the authors, cannot be classified under any of the other sub-disciplines of device forensics. Such devices have the ability to store data or information that may possess evidentiary value in a digital forensic investigation. Examples of obscure devices may include digital recording devices (video and audio) such as camcorders, surveillance cameras, gaming devices e.g., (Sony's Play Stations, Microsoft's Xboxes, Nintendo's Wii consoles, etc.), which can also be analysed for potential evidence.

Network Forensics

According to Palmer (20), network forensics "is a branch of digital forensics that basically uses scientific proven techniques to collect, use, identify, examine, correlate, analyse, and document digital evidence from multiple, actively processing and transmitting digital sources for the purpose of uncovering facts related to the planned intent, or measured success of unauthorized activities meant to disrupt, corrupt, and/or compromise system components as well as providing information to assist in response to or recovery from these activities". Unlike other branches of digital forensics, network forensics deals with volatile and dynamic information that can easily get lost after transmission in any network environment. An attacker might be able to erase all log files on a compromised host and therefore network-based evidence may be the only evidence available for forensic analysis (37). For the purpose of this study, network forensics (as shown in Figure 7) is divided into cloud forensics, telecom network forensics, internet forensics and wireless forensics.

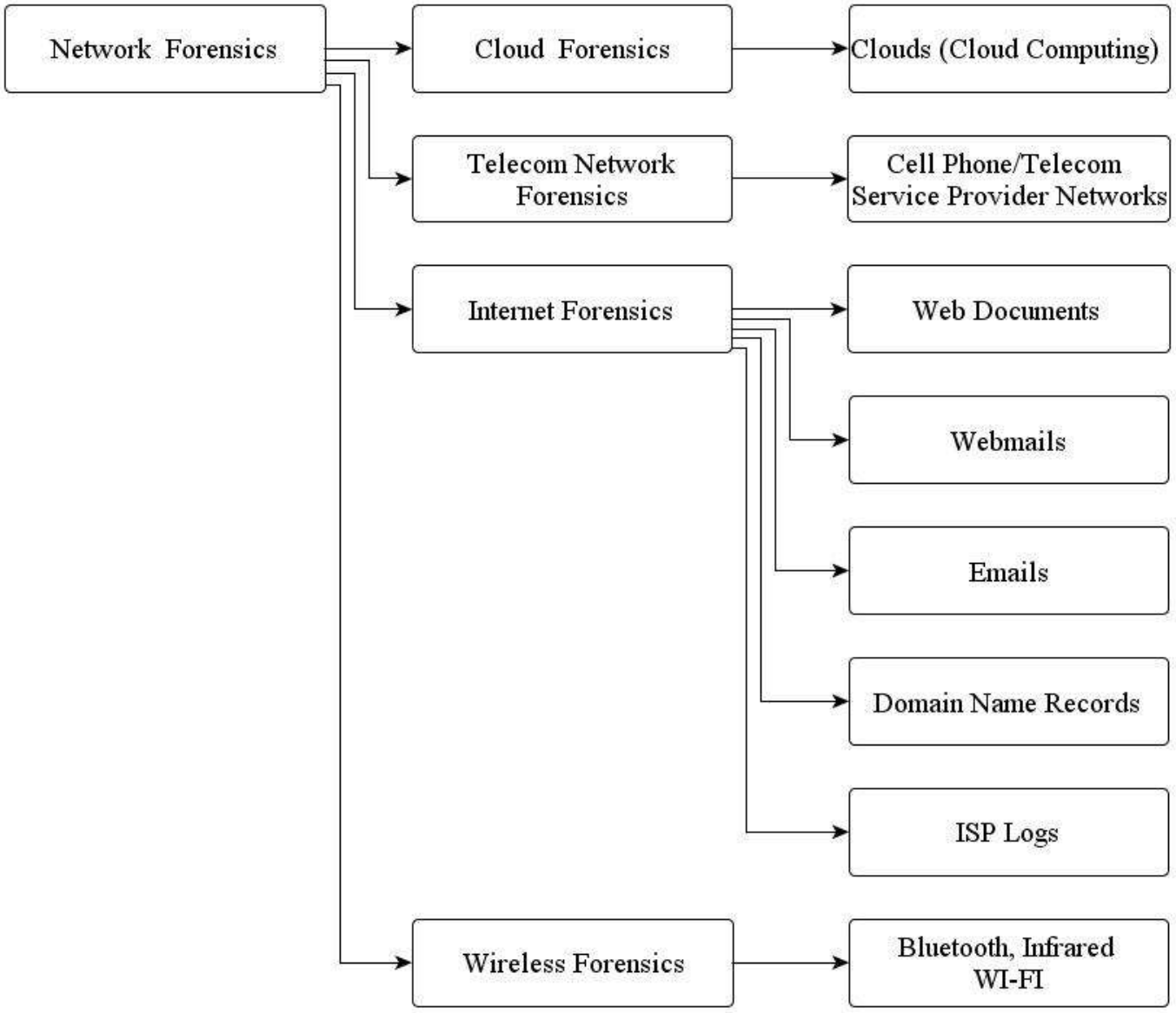

FIG. 7—Network forensics.

Cloud Forensics

Cloud computing is reckoned to be one of the most transformative technologies in the history of computing. This is so because it is radically changing the way in which information technology services are created, delivered, accessed and managed (41). Cloud forensics, as defined by Keyun et al (41), is an emerging field that deals with the application of digital forensics techniques in cloud computing

environments and is a subset of network forensics. Therefore, technically, cloud forensics follows most of the main phases of network forensic processes with extended or novel techniques tailored for cloud computing environments in each phase. For this reason, the authors placed cloud forensics as a sub-discipline of network forensics in the ontology.

Telecom Network Forensics

Telephones are often used to facilitate criminal and terrorist acts. The signalling core of public telephone networks generates valuable data about phone calls and calling patterns that may be used in criminal investigations, especially with the widespread uptake in voice-over-IP (VoIP) systems. However, much of this data is not maintained by service providers and is, therefore, unavailable to law enforcement agencies (38). If such data can be collected and stored, it can be analysed forensically and greatly facilitate the prosecution of criminals in a court of law.

Internet Forensics

With the evolution in global commerce, many business organisations store vital business information online and/or carry out business transactions over the internet. Such organisations are under constant threat of falling victim to internet attacks. Moreover, because the internet is so large and unregulated, it has become a fertile breeding ground for all kinds of cyber-crimes (42). If the internet is to become a safe platform for transacting business, internet forensics has to become very important as well.

Internet forensics is a research field that deals with the analysis of activities that occurred on the internet. It aims to uncover clues about people and computers involved in internet crime, most notably fraud (e.g. credit card fraud) and identity theft (39). Note that the term “internet crime” and “cyber-crime” are often used interchangeably (55). Cyber-crime is usually used to mean any criminal activity in which a computer or network is the source, tool, target or place of crime (56, 57). The Cambridge English Dictionary defines

cyber-crimes as crimes committed with the use of computers or relating to computers, especially through the internet (56).

Therefore, internet forensics tries to uncover the origins, contents, patterns and transmission paths of e-mail and Web pages, as well as browser history and Web servers' scripts and header messages (39). It can also be used to extract information that lies hidden in every email message, web page and web server. Such information may contain potential digital evidence that can be analysed for forensic purposes. In this paper, the authors listed the following areas under internet forensics as common examples: Web-mail, E-mail, domain name records, Internet Service Provider (ISP) logs and web documents. However, there is much more that can be gathered from the internet as compared to what is listed in here.

Wireless Forensics

The adoption of wireless technologies by different organisations in recent years has created issues of concern such as control and security. Incident handlers and law enforcement have been forced to deal with the complexity associated with wireless technologies when managing and responding to security incidents (40). Therefore, wireless forensics, which has emerged as a result of wireless technologies, focuses on capturing and/or collecting digital evidence data that propagates over a wireless network medium. In addition, wireless forensics tries to make sense of the collected digital evidence in a forensic capacity so that it can be presented as valid digital evidence in a court of law. The evidence collected can correspond to plain data, but can include voice conversations as well (40).

Discussion

The ontology presented in this paper is a new contribution in the DF domain. The scope of the ontology is defined by the DF disciplines (refer to Figure 1). The main disciplines as defined in the ontology are computer forensics, software forensics, database forensics, multimedia forensics, device forensics and network forensics. These disciplines are further defined in terms of their scope and functions. The sub-disciplines, objects and sub-objects identified in the ontology include examples and specific finer details

covered under the major disciplines. It should also be noted that most of the objects and sub-objects identified in the ontology were selected as common examples to facilitate this study. 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 forensics domain.

In addition, the ontology presented in this paper can be used in the digital forensics domain, for example to address issues such as professional specialisation and certification, as well as the development of digital forensics tools, curricula and education materials.

For the case of professional specialisation, the DF disciplines and sub-disciplines presented in the ontology can be used to give direction to individuals interested in specific areas of specialisation. Such areas will, for example, produce specialists in computer forensics, software forensics, database forensics, multimedia forensics, device forensics and network forensics. While specialisation is important, certification cannot be ignored, especially not by individuals interested in the industry practices of digital forensics. Therefore, a combination of the DF sub-disciplines, objects and sub-objects identified in the ontology should be considered for certification. This will include certification as a certified wireless forensics examiner and/or investigator, certified internet forensics examiner and certified cloud forensics examiner.

Developers of digital forensics tools can use the ontology to fine-tune digital forensic tools so as to be able to cover as many sub-disciplines, objects and sub-objects as possible in the case of digital forensic investigations. This also implies that developers will find the ontology in this paper useful, especially when considering new digital forensic techniques for specific areas of interest and new high-tech digital forensic investigation tools.

Finally, institutions of higher learning will also find the ontology in this paper constructive, especially when developing curriculums and education materials for different undergraduate and postgraduate studies. Different modules can be developed with the help of the ontology to assist students in comprehending the concepts of digital forensics less effortlessly. Prerequisites for modules can, in addition, be designed

effectively with the help of the ontology so as to avoid conflicts among and redundancy of concepts. In fact, the presentation of the ontology in this paper is a whole new contribution towards advancing the digital forensics domain.

Conclusions

Digital forensics plays a very important part in both incident detection and digital investigations. Therefore, developing methodologies that can be used to offer direction in areas such as professional specialisation and certification, as well as the development of forensic tools, curricula and education materials is of utmost importance. This will help, for example, to build a foundation that can be used to solve both present and future problems arising as a result of technological change or domain evolution. Such problems may include those related to the structure of information among different DF disciplines, as well as the reuse and sharing of common domain knowledge. However, more emphasis needs to be placed on digital forensic areas that focus on preparing individuals for what they are expected to do in the case of an investigation process and on preparing them for how to accomplish their task.

This paper presented a novel contribution in the digital forensics domain by means of a guiding ontological model that indicates the placement of the different digital forensic disciplines and sub-disciplines within the domain. The ontology also allows for the addition of new digital forensic disciplines and sub-disciplines, including potential modifications in any one of the aforementioned categories.

Considering the current technological trends, more research needs to be conducted in future in order to expound on the ontology. Further research in the area of digital forensic ontologies must also be conducted to establish the various relationships that exist among the different disciplines and sub-disciplines, objects and sub-objects presented in this study, as some of the examples listed in the ontology might not be mutually exclusive to a particular discipline.

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. Reinout Van Rees, Clarity in the usage of the terms ontology, taxonomy and classification. Construction Informatics Digital Library http://itc.scix.net/ paper w78-2003-432.content. (Accessed August 29, 2012).
2. Grüber, T., A translation approach to portable ontology specification. Knowledge Acquisition 5(2) (1993) 199-220.
3. Smith, B., Kusnierczyk, W., Schober, D., Ceusters, W., Towards a reference terminology for ontology research and development in the biomedical domain. In Proceedings of the 2nd Int. Workshop on Formal Biomedical Knowledge Representation: \Biomedical Ontology in Action". (2006) 57-66.
4. Verónica Castañeda, Luciana Ballejos, Ma. Laura Caliusco, Ma. Rosa Galli., The use of ontologies in requirements engineering. Global Journal of Researches in Engineering Vol. 10 Issue 6 (Ver 1.0) November 2010. *GJRE Classification (FOR) 091599*
5. N. Shadbolt, W.H., Berners-Lee, T.: The semantic web revisited. IEEE Intelligent Systems 21(3) (2006) 96-101.
6. Natalya, F. and Deborah, L., Ontology Development 101: A Guide to Creating Your First Ontology.
7. Glen D, Peter S, Revisiting Ontology-Based Requirements Engineering in the age of the Semantic Web.
8. Ashley Brinson, Abigail Robinson, Marcus Rogers, A cyber forensics ontology: Creating a new approach to studying cyber forensics. (2006 DFRWS) Digital investigation 3S (2006) S37–S43. Published by Elsevier Ltd
9. David C.H. and Richard P.M, A Small Scale Digital Device Forensics ontology. Small Scale Digital Device Forensics Journal, Vol.1, No.1, June 2007
10. Allyson M.H and Doris L.C, Weaving Ontologies to Support Digital Forensic Analysis. ISI 2009, June 8-11, 2009, Richardson, TX, USA
11. Ziga Turk, Construction informatics: Definition and ontology. Advanced Engineering Informatics 20 (2006) 187–199
12. Graciela Brusa, Ma. Laura Caliusco and Omar Chiotti, A Process for Building a Domain Ontology: an Experience in Developing a Government Budgetary Ontology. Australasian Ontology Workshop (AOW 2006), Hobart, Australia.
13. Boyce, S., & Pahl, C. (2007). Developing Domain Ontologies for Course Content. *Educational Technology & Society*, 10 (3), 275-288.

14. Jim Ed Crouch, NSCI December 16, 2010, An Introduction to Computer Forensics. Available at: http://www.nsci-va.org/WhitePapers/2010-12-16-Computer%20Forensics-Crouch-final.pdf (Accessed March 5, 2012).
15. Computer forensics. Anglia Ruskin University, Dissertation No (CSH2998A). Available at: http://www.minshawi.com/other/computer%20foransics.pdf (Accessed March 5, 2012).
16. Roberto Obialero, SANS Institute 2000 - 2005. Forensic Analysis of a Compromised Intranet Server.
17. Matt Pierce, SANS Institute 2003. Detailed Forensic Procedure for Laptop computers Forensic analysis 06-11-2003.
18. Stephen G. MacDonell, Andrew R. Gray, Grant MacLennan, and Philip Sallis, Software Forensics for Discriminating between Program Authors using Case-Based Reasoning, Feed-Forward Neural Networks and Multiple Discriminant Analysis.
19. G. Whale. Software metrics and plagiarism detection. *Journal of Systems and Software*, 13:131–138, 1990.
20. Gary Palmer, A Road Map for Digital Forensic Research. DFRWS Technical Report. DTR - T001-01 Final. Report from the First Digital Forensic Research Workshop (DFRWS). November 6th, 2001 - Final.
21. Martin S. Olivier, On metadata context in Database Forensics. ICSA Research Group.
22. Edgar Weippl, Database Forensics. Available at: http://www.nii.ac.jp/issi/pdf/2/4Johannes_Heurix.pdf (Accessed March 26, 2012).
23. Mario A.M et al, Database Forensics. Available at: http://delivery.acm.org/10.1145/1950000/1940958/p62-guimaraes.pdf?ip=137.215.6.53&acc=ACTIVE%20SERVICE&CFID=74282261&CFTOKEN=62192917&__acm__=1332837302_057fa5962ff148a2ab5a9daccbec521b (Accessed March 27, 2012).
24. Multimedia Forensics, 2012. URL http://isis.poly.edu/projects/forensics. (Accessed August 03, 2012).
25. Rainer Böhme, Felix C. Freiling, Thomas Gloe, and Matthias Kirchner, Multimedia Forensics Is Not Computer Forensics
26. Ashwin S., Min Wu and K. J. Ray Liu, Image Tampering Identification Using Blind Deconvolution
27. Thomas G. et al, Can We Trust Digital Image Forensics? MM'07, September 23–28, 2007, Augsburg, Bavaria, Germany. Copyright 2007 ACM 978-1-59593-701-8/07/0009
28. Ashwin S. et al, Digital Image Forensics via Intrinsic Fingerprints. IEEE Transactions On Information Forensics And Security, Vol. 3, No. 1, March 2008
29. Weihong W. and Hany F., Exposing Digital Forgeries in Video by Detecting Duplication. MM&Sec'07, September 20–21, 2007, Dallas, Texas, USA. Copyright 2007 ACM 9781595938572/07/0009
30. Frédéric L. et al, Image And Video Fingerprinting: Forensic Applications

31. Matthew C. and K. J. Ray Liu, Anti-Forensics For Frame Deletion/Addition In Mpeg Video
32. Ghulam M. and Khalid A., Environment Recognition For Digital Audio Forensics Using Mpeg–7 Andmel Cepstral Features. Journal Of Electrical Engineering, Vol. 62, No. 4, 2011, 199–205
33. Christian K. et al, Digital Audio Forensics: A First Practical Evaluation on Microphone and Environment Classification. MM&Sec'07, September 20–21, 2007, Dallas, Texas, USA. Copyright 2007 ACM 978-1-59593-857-2/07/0009
34. Cyber Forensics - Device Forensics. Available at: http://www.cyberforensics.in/(A(cos8NMWQywEkAAAAODMwODM4YWMtNWFmZC00ZWNhLThkNDEtNTlhMWM3MGE5MzA5hkCziwldj9ts_CCtkjYQI68akds1))/Research/DeviceForensics.aspx?AspxAutoDetectCookieSupport=1 (Accessed March 22, 2012).
35. Network-enabled Devices, 2012 . URL http://www.sena.com/solutions/network_enabling/ (Accessed September 5, 2012).
36. Hyungkeun J., High Speed Search for Large-Scale Digital Forensic Investigation. E-Forensics 2008. Adelaide, Australia.
37. Erik Hjelmvik, Passive Network Security Analysis with Network Miner | ForensicFocus.com. Available at: http://www.forensicfocus.com/passive-network-security-analysis-networkminer (Accessed March 27, 2012).
38. T. Moore et al, Using Signaling Information in Telecom Network Forensics. IFIP International Federation for Information Processing, 2005, Volume 194/2005.
39. Internet forensics Definition from PC Magazine Encyclopedia. Available at: http://www.pcmag.com/encyclopedia_term/0,2542,t=Internet+forensics&i=59910,00.asp (Accessed March 22, 2012).
40. Raul Siles, GSE, Wireless Forensics: Tapping the Air - Part One | Symantec Connect Community. Available at: http://www.symantec.com/connect/articles/wireless-forensics-tapping-air-part-one (Accessed March 26, 2012).
41. Keyun et al, Cloud forensics: An overview. Centre for Cybercrime Investigation, University College Dublin.
42. Robert Jones, Internet Forensics, Using Digital Evidence to Solve Computer Crime Publisher: O'Reilly Media October 2005
43. Anon, 2012. Petabyte of Storage Capacity. URL http://www.aberdeeninc.com/abcatg/petabyte-storage.htm (Accessed August 26, 2012).
44. Kimberly S. Hanks, John C. Knight and C. Michael Holloway, The Role of Natural Language in Accident Investigation and Reporting Guidelines
45. Chris Johnson, Forensic software engineering. Proceedings of 19th International Conference SAFECOMP 2000, 420-430.

46. Chris Johnson, Forensic software engineering: are software failures symptomatic of systemic problems? Safety Science 40 (2002) 835–847
47. Anon, Image editor software | Adobe Photoshop CS6. Available at: http://www.adobe.com/products/photoshop.html (Accessed August 26, 2012).
48. Anon, Video editing software | Adobe Premiere Pro CS6. Available at: http://www.adobe.com/products/premiere.html (Accessed August 26, 2012).
49. Anon, Video editing software - Pinnacle Studio - The #1 selling digital video editing software. Available at: http://www.pinnaclesys.com/PublicSite/us/Products/Consumer+Products/Home+Video/Studio+Family/ (Accessed August 26, 2012).
50. Daniel J. Ryan and Gal Shpantzer, Legal Aspects of Digital Forensics
51. Guidance Software, EnCase Forensic - Computer Forensic Data Collection for Digital Evidence Examiners. Available at: http://www.guidancesoftware.com/encase-forensic.htm (Accessed August 29, 2012).
52. AccessData, Computer Forensics Software for Digital Investigations. Available at: http://accessdata.com/products/digital-forensics/ftk (Accessed August 29, 2012).
53. The Sleuth Kit (TSK) & Autopsy: Open Source Digital Investigation Tools. Available at: http://www.sleuthkit.org/index.php (Accessed August 29, 2012).
54. X-Ways Software Technology AG, WinHex: Hex Editor & Disk Editor, Computer Forensics & Data Recovery Software. Available at: http://www.winhex.com/winhex/ (Accessed August 29, 2012).
55. Melanie Kowalski, Cyber-Crime: Issues, Data Sources, and Feasibility of Collecting Police-Reported Statistics. Canadian Centre for Justice Statistics, Catalogue no. 85-558-XIE, ISBN 0-660-33200-8.
56. A. Prasanna, Cyber Crimes: Law and Practice
57. Talwant Singh, 2012. CYBER LAW & INFORMATION TECHNOLOGY. URL http://delhicourts.nic.in/ejournals/CYBER%20LAW.pdf (Accessed August 29, 2012).
58. Himal Lalla and Stephen V. Flowerday, Towards a Standardised Digital Forensic Process:E-mail Forensics
59. Soltan Alharbi1, Jens Weber-Jahnke and Issa Traore, The Proactive and Reactive Digital Forensics Investigation Process: A Systematic Literature Review. International Journal of Security and Its Applications. Vol. 5 No. 4, October, 2011
60. Eloff, J., Kohn, M., & Olivier, M. (2006). Framework for a Digital Forensic Investigation. ISSA. University of Pretoria: Information and Computer Security Architectures (ICSA) Research Group.

61. Leigland, R., & Krings, A. W. (2004). A Formalization of Digital Forensics. International Journal of Digital Evidence , 3 (2), 1-32.
62. ISO/IEC WD 27043.2, working draft. Information technology — Security techniques — Investigation principles and processes.
63. Jasmine Ćosić and Zoran Ćosić, The Necessity of Developing a Digital Evidence Ontology, Proceedings of the Central European Conference on Information and Intelligent Systems. September 19-21, 2012. Page 325-330

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