Taxonomy for Digital Forensic Evidence

Nickson M. Karie[1]
[2]Department of Computer Science,
Daystar University,
Box 44400-00100, Nairobi, Kenya
menzao6@hotmail.com

Victor R. Kebande[2],
[2]Information and Computer
Security Architecture (ICSA),
Research Lab
[2]Department of Computer Science,
University of Pretoria,
South Africa
vickkebande@gmail.com

H. S. Venter[3]
[2]Information and Computer
Security Architecture (ICSA),
Research Lab
[2]Department of Computer Science,
University of Pretoria,
South Africa
hventer@cs.up.ac.za

Abstract— **Modern society has increased its dependencies on digital systems and computer networks in almost every area of life today. Although this dependency is good it has opened a whole new world of possibilities for criminals to exploit. This has been seen in areas where criminals are able to use existing digital systems to share information and to reinforce their hacking techniques for nefarious purposes. As a result, major potential security risks, such as malicious insiders, data loss or leakage and policy violations have now invaded our digital world with worrying trends of digital and cyber-crimes. This, therefore, has made computer based information a primary source of digital evidence in many legal matters and digital investigations. The understanding of the different types of information generated by computer systems is thus an importance aspect of any digital forensic investigation process. For this reason, this paper reviews existing digital forensic research literature and highlights the different types of digital evidence that can potentially be admissible in our courts of law today. 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 randomization techniques were employed to facilitate the review of the gathered literature. The taxonomy classifies a large number of Digital Forensic Evidence (DFE) into a few well-defined and easily understood categories which can be useful, for example, the future developments of digital forensic tools. In addition, the taxonomy can also be helpful to practitioners, for example, in classifying the different types of DFE that can be admissible in courts. The main contribution of this research is, therefore, to propose a taxonomy for DFE that can assist digital forensic analysts and forensic practitioners to understand the different types of evidence with ease and their applicability in different legal matters.**

Keywords—Taxonomy; Digital forensics; Digital evidence; Legal matters; Digital systems.

I. INTRODUCTION

In the last few decades, there has been a significant revolution in computing and technological developments which have widely been influenced by the way Information Technology (IT) is being used to deliver solutions. These evolvements have seen a sporadic integration of complex systems over time which has further influenced the way people conduct their businesses activities. As a result of these technological shifts, a wide-range of computing architectures have also been developed and the mode of communication has entirely shifted from the well-known traditional approaches to the now modern approaches built using internet-based architectures like social networks, electronic commerce, electronic communication and other major electronic-based transactions.

The rise of these technological advances and inevitable dependence of computing systems have brought about the demand to enforce significant security of these systems. This is because a chain of unwanted adversaries has managed to creep into the current computing infrastructures as hackers who have eventually managed to create computer breaches through some forms of cyber-crimes over the internet, which is currently being used as a gateway for connecting the rest of the world. They have been able to do this by exploiting the systems' vulnerabilities through modification of computing infrastructures in order to gain confidential information like: personal details, bank accounts data, deletion, manipulation, Denial of Service (DoS) attacks, and identity theft all for personal gain.

Digital Forensics (DF) provides a mechanism that can help to unearth these prevalent crimes that are committed through the cyberspace. This requires scientifically accepted approaches that are able to primarily investigate digital crimes through extraction of Potential Digital evidence (PDE) that can be presented in a court of law as admissible evidence for prosecutorial purposes. When dealing with DF, a number of principles have to be followed with regard to how digital evidence is extracted. These include such principles as, the ability to extract digital evidence without alteration and being able to conduct examination and analysis in a repeatable way by being accountable.

Extracting digital evidence for purposes of conducting a Digital Forensic Investigation (DFI) is a prime objective because that is the only way through which a crime is able to be linked to the suspect according to Casey [7]. Normally forensic analysts are supposed to use new and current forensic techniques to further or handle PDE that can be used to create a hypothesis in a court of law. However, developments have shown that the complexity that is associated with digital evidence during examination and analysis, may affect the process of investigations for forensic analysts and the Law Enforcement Agencies (LEAs). For example, the Technical Working Group for the Examination of Digital Evidence (TWGEDE) has highlighted that; an agency should be prepared to handle digital evidence through available policies and procedures that are able to comply with the federal, state and the local laws. Through this assertion, the TWGEDE on its' special report on the National Institute of Justice [22] has recommended that during evidence examination a number processes should be conducted. The processes include: policy and procedure development, digital evidence assessment, evidence acquisition, evidence examination and reporting. However, the complexity involved in these processes means that analysts will face a challenge when the tools that are used are not able to identify the different hierarchical classifications of the evidence extracted.

Based on this premise the paper tries to present a taxonomy that classifies the large number of DFE into a few well-defined and easily understood categories which can be useful, for example, the future developments of digital forensic tools. This paper describes a digital evidence-based taxonomy that realizes the significant role that classifying evidence yields during analysis, examination, and digital investigation process. The principal design of the taxonomy has depicted a way through which digital evidence can help to give support of the current state-of-the-art DFI processes and also serve as a guide for forensic experts, practitioners, and DF investigators.

This paper comprises of 7 Sections and will be presented as follows: Section 1 has presented an introduction, Section 2 narrate the background for this research study. After this, Section 3 discusses the related work. Thereafter, Section 4 provides the scope of the taxonomy which is followed by Section 5 which gives the proposed taxonomy for DFE. Section 6 gives an evaluation of the taxonomy. Finally, section 7 concludes the paper and summarizes the overall development of a taxonomy for DFE.

II. BACKGROUND

In this section, the following has been presented as background work: Digital forensics and Digital forensic evidence. On the one hand, DF is being discussed to show how scientifically proven methods can be used in conducting a DFI. On the other hand, DFE is discussed because the proposed DFE taxonomy is based on digital evidence aspects and digital forensic domain.

A. Digital Forensics

Beebe [2] has presented DF using the good, bad and the unaddressed where the author argues convincingly that it is no longer a niche but a mainstream knowledge that is aimed at checking the digital footprints after an interaction exists between computers and networks. Furthermore, DF still lacks standardization according to how the unaddressed is highlighted by the author. Nevertheless, the golden age of DF according to Garfinkel [12] existed between 1999 and 2007 where it is viewed as a magic window that was able to see through all the residual data that was thought to have been deleted at some point. Consequently during the first Digital Forensic Research Workshop (DFRWS), Pollit [27] presented DF as six blind men from indostan where he highlights it's not an elephant but a process that comprise a group of tasks involved in an investigation. Finally in a roadmap for DF Palmer has presented it as "the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations" [27]. Having looked at a brief description of DF, the authors have an intuition on how DF can be used to further reconstruction of events which can be deemed as criminal using scientifically proven techniques. The next section presents a brief discussion of digital evidence.

B. Digital Evidence

Digital evidence according to Kozushko [21] comprises of digital data that is able to establish that a potential digital crime has occurred so that the link between a suspect and the perpetrator can be established. Normally digital evidence can help forensic analysts and the law enforcement agencies (LEA) during a DFI process. However, before any digital evidence can be presented in a case, it must be competent, relevant, and material to the issue, and it must be presented in compliance with the rules of evidence. Anything that tends to prove directly or indirectly that a person may be responsible for the commission of a criminal offense may be legally presented against him.

According to Carrier [5], the focus in digital investigations is currently on how digital evidence can be recovered as well as examining the properties that the collected evidence has. Moreover, the authors present digital evidence of an incident as any digital data that is able to contain reliable information that is able to support or refute a hypothesis about an occurrence of an incident. Digital evidence can exist in different aspects when employing forensic techniques, for example, for digital evidence to be admissible in a court of law it needs to satisfy a given number of criteria. This implies that special knowledge is needed to locate and collect evidence and special care is required to preserve and transport the evidence. The Association of Chief Police Officers (ACPO) of UK on digital evidence highlights that digital evidence can be seized from different environments like networks, wireless devices, websites, forums, and blogs. Therefore, during a forensic investigation, it is important that an investigator has a thorough understanding of the different types of evidence as well as how to locate, collect, preserve and transport the evidence. For this reason, the authors present in this paper a taxonomy for DFE that can help forensic analysts and digital forensic investigators to classify forensic evidence during the digital forensic investigation process. Other research works that have focused on extracting digital information that can be used as digital forensic evidence include [31-36] and potential evidence in [37-43].

In the next section, the reader is introduced to relevant work related to the research study.

III. RELATED WORK

The section presents preliminary works by other researchers that are presented as related work. Taxonomy of computer forensic methods and different procedures for seizing evidence has been proposed by [6] compares different methodologies and procedures that are used during digital evidence acquisition and a more appropriate taxonomy that can be used in computer forensic analysis phase is outlined.

Research by Pollit [28] on applying the traditional forensic taxonomy to DF highlighted that the traditional forensic taxonomy of DF can be applied to the following processes during DF: identification, classification, individualization, association, and reconstruction. In this approach, Pollit [28] pointed the irony that existed was more deterministic, classification as a process was presented to help determine a common origin, and individualization could use a set of characteristics to uniquely identify a specimen. In this research, the authors focus was primarily on DF as a domain but not DFE.

Another research paper by Cohen [8] on DFE examination highlights the key areas that are to be made in order for DFE examination to be considered a normal science. The author identifies the following principal elements of DFE examination as follows: Analysis, interpretation, attribution and reconstruction. Even though the author's research was credible enough the focus of taxonomies was hardly mentioned.

Research on Potential Digital Evidence (PDE) reconstruction and PDE presentation has highlighted a reconstruction approach that can help in identification of evidence characteristics of digital evidence with the following processes: Retrieval of digitally preserved data, clustering of data, event searches, similarity measure and event report Kebande [19],[20]. On PDE presentation, Karie [16] highlights the following: Identifying source of PDE, evaluate the validity of the source, establish relationship between PDE and crime, establish the relationship between PDE and other available evidence, clarify PDE, justify PDE claims and present concluding assertions on PDE validity. In this research study, the authors were able to bring out different characteristics of digital evidence but taxonomies were hardly the focus.

A paper highlighting taxonomy of challenges for DF presented by Karie [17] proposes a formal classification of challenges in DF by classifying a large number of DF challenges into four well-defined understood categories. This taxonomy could be useful in development automated digital forensic tools. Even though the taxonomy explicitly described the processes and procedures well it was not focused on DFE rather challenges. Nevertheless, the aforementioned research has presented a good understanding and a broad insight to the authors on various researches that are inclined to DFE taxonomies. However at the time of writing this paper still there exist no taxonomy for DFE. Having explored this, in the next section the reader is introduced to the scope of the taxonomy.

IV. SCOPE OF THE TAXONOMY

Different types of digital evidence exist in DF. Several models and frameworks have also been developed by different researchers to address specific and/or individual processes such as how to locate, collect, preserve and transport the evidence. However, before delving into the investigative process, it is essential that the investigator has a good understanding of the different types of digital evidence. This is because, the submission of any collected digital evidence in any type of legal proceeding generally amounts to a significant challenge, hence, as said earlier before any evidence is presented in court, the investigator must ascertain that the evidence has been located and collected in line with the rules of evidence. Moreover, the evidence must also be competent, relevant, and material to the issue. To do this, the knowledge of the different types of digital evidence is, thus, very important to any investigator.

The presentation in this paper is, therefore, an exceptional effort toward a taxonomy of DFE based on the review of existing DF literature. The scope of the taxonomy is, however, restricted to the boundaries of the literature reviewed by the authors. The authors also acknowledge that the different types of digital evidence presented in this paper are not, in whatever way, an exhaustive list. This is backed up by a research by Karie [17] 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 types of digital evidence that exist in DF. More types of evidence can though be added onto the taxonomy as the evolution in digital forensics continues. The next section explains the proposed DFE taxonomy.

V. PROPOSED TAXONOMY OF EVIDENCE FOR DIGITAL FORENSICS

In this section, the authors present an explanation of the proposed taxonomy of DFE. In any civil and legal proceedings, evidence is usually used by both the prosecutors and the victims to build and support a case, or theory as to what happened and who is responsible [30]. The evidence presented may include testimony from witnesses, exhibits, and other items. However, irrespective of the type of evidence presented it can only be categorised as either “direct evidence” or “circumstantial evidence” [30].

Table 1 shows the structure of the proposed taxonomy. The taxonomy consists of three columns with the first column depicting the categories of the DFE. This is followed by the sub-categories in the second column and the examples in the third column. The various categories and sub-categories of the DFE presented in each of the different columns of the taxonomy are shown in Table 1, however, the focus is on the major types of evidence that can be considered in the case of legal proceedings. The major categories identified in this study include direct Evidence and Circumstantial Evidence. The sub-categories, on the other hand, include: Real Evidence or Physical Evidence, Documentary Evidence, Questioned Documents, Demonstrative Evidence, Computer-generated Evidence, Impression Evidence, Trace Evidence, Pattern Evidence among others shown in Table 1. The details of the categories and the sub-categories that have been identified in Table 1 are explained further on.

A. Direct Evidence

The term direct evidence refers to any piece of evidence that stands alone to prove an assertion [4]. This implies that, during a DFI process, direct evidence can be used to prove or disprove a fact directly [30]. Direct evidence usually establishes a particular fact without the need to make an inference in order to connect the evidence to the fact and may include oral testimony, where the knowledge is obtained from any of the witness's five senses and is in itself proof or disproof of a fact in issue. In essence, direct evidence provides direct proof of a fact and doesn't require any type of inference [4]. For example, when a witness narrates an incidence that he directly observed, experienced or a witness who testifies that he saw the defendant fleeing the scene of the crime, then he is offering direct evidence of that incidence. Direct evidence may be divided into the following sub-categories:

1) Physical Evidence or Real Evidence: Physical evidence which is also referred to as real evidence or material evidence is anything which takes the form of an actual, physical object. Its’ existence or characteristics are considered relevant and material to an issue in the case of civil or legal proceedings. It is usually anything that was directly involved in some incidence [11] and consists of objects that were involved in an incidence or actually played a part in the incident [24]. Thus, the use of physical objects such as Internet Modems, Laptops, Phones, Tablets, IPad among others before a jury can be considered as real evidence or physical evidence. The common types of physical evidence encountered at an investigation process include:

a) Impression evidence: During an investigation, in any crime scene, investigators need to understand that impression evidence is created when two objects come in contact with enough force to cause an impression e.g. fingerprints.

b) Pattern evidence: Pattern evidence can be defined as any additional identifiable information that investigators can find within an impression. Impression and pattern evidence can help link a suspect or tool to a particular crime scene. For example, an investigator can compare shoeprint evidence with several shoe-sole patterns to identify a particular brand, model or size [23]. This means that, if a shoe is recovered from a suspect that matches this initial pattern, the forensic examiner can look for unique characteristics that are common between the shoe and the shoeprint, such as tread wear, cuts or nicks [23].

c) Transient evidence: Transient evidence is a term used in forensic investigations to indicate elements of physical evidence that might be expected to degrade or disappear within a particular time frame [24]. In addition transient evidence has no meaning and by its very nature can easily be changed or lost. Transient evidence will lose its evidentiary value if not preserved and protected in a manner that preserves its integrity and authenticity. Examples include temperature, odour and blood in the rain among others [24].

d) Conditional evidence: Conditional evidence is usually produced by a specific event or action and considered very important in crime scene reconstruction and in determining the set of circumstances or sequence within a particular event. Examples include light, smoke, fire and location of injuries among others.

e) Transfer evidence: According to IBM [13] transferring evidence permits case evidence to be copied from one case to another. The transfer evidence maintenance function allows a user to select a case participant and from a list of the evidence associated with the participant, choose which evidence is to be transferred. The user then selects which evidence from the list is to be transferred for use on a different case. The user can choose to include all evidence related to a participant or a specific evidence record. Evidence can be transferred between cases of different types, however, for this to happen; the case to which the evidence is being transferred must be configured to receive evidence of the type being transferred [13].

f) Associative evidence: According to Kathleen [18], associative evidence originates from contact between people, objects including people and objects. In addition, associative evidence can be used to provide links between evidence and individuals involved in a crime. In some cases, the associative evidence may be sufficient to prove the contact. However, in other cases, the associative evidence may be less definitive and provide corroboration of other evidence [18]. Examples of associative evidence include fingerprints left on an object, fibers left from contact of clothing with objects, blood from a physical injury, etc.

g) Trace evidence: Trace evidence according to Jack [14] can be defined as any small piece of evidence that has to be collected by investigators and places a suspect at the scene of a crime. Trace evidence can also be understood as those materials that could be transferred during the commission of a violent crime. Such trace materials may include but not limited to human hair, animal hair, textile fibers and fabric, rope, feathers, soil, glass, and building materials. The physical contact between a suspect and a victim can result in the transfer of trace materials. The identification and comparison of these materials can often associate a suspect to a crime scene or with another individual [10].

Table 1. Taxonomy of Digital Forensic Evidence

Categories of Evidence	Sub Category	Examples
1. Direct Evidence	Real Evidence or Physical evidence	▪ Internet Modems ▪ Laptops ▪ Phones ▪ Tablets ▪ IPad
	Demonstrative Evidence	▪ Maps ▪ Models ▪ Photograph ▪ X-ray ▪ Diagrams of a crime scene ▪ Charts and graphs illustrating profits and losses
	Documentary evidence	▪ Surveillance Tapes ▪ Audio ▪ Video ▪ Letters ▪ Telegrams ▪ Printed matter ▪ Photographs ▪ Charts
	Questioned Documents	▪ Criminal confessions ▪ Counterfeit money ▪ Journal entries ▪ Threatening letters ▪ Checks ▪ Wills
2. Circumstantial Evidence or Indirect Evidence	Scientific Evidence	▪ DNA matching ▪ Fingerprint identification ▪ Hair and fiber comparisons ▪ Voice identification
	Empirical Evidence	▪ Temperature is shown by a thermometer ▪ DNA testing
	Individual Evidence	▪ Fingerprints ▪ DNA patterns ▪ Tool marks ▪ Handwriting
	Class Evidence	▪ All polyester fiber has the same chemical characteristics ▪ All brown human hair has the same class characteristics, under a microscope
	Computer-generated Evidence	▪ Visual output on the monitor. ▪ Printed evidence on a printer. ▪ Printed evidence on a plotter. ▪ Film recorder

2) Demonstrative Evidence: Demonstrative evidence is any evidence which serves merely as a visual aid to the jury in comprehending the verbal testimony of a witness [24]. This may include such things as Maps, a model, photograph, X-ray, diagrams of a crime scene, charts and graphs illustrating profits and losses, etc. Demonstrative evidence is admissible when it fairly and accurately reflects the witness's testimony and is otherwise unobjectionable [11].

3) Documentary Evidence: Documentary evidence is usually any form of writing or documents submitted to the judge and the members of the jury for their inspection during a court session, a trial or hearing [24]. Documentary evidence may include such things as photographs, tape recordings, films, and printed emails, surveillance tapes, audio, letters, telegrams, charts, contracts, deeds, licenses, certificates, tickets, or any other writings. However, a piece of evidence is not documentary evidence if it is presented for any purpose other than the examination of the contents of the document. Besides, documentary evidence is not necessarily conclusive evidence unless it is supported by other evidence. It is also to be noted that documentary evidence is subject to the best evidence rule, which requires that the original document is produced unless an adequate explanation is offered for the absence of the original [30-35].

4) **Questioned Documents**

In digital forensics, investigators at times need to examine or verify the integrity, authenticity, and authorship or creation date of the document that could be used as evidence in court or aid in an investigation process [23]. Such documents could be in digital format, printed or hand written format. Such documents are usually referred to as Questioned Documents and may include but not limited to checks, criminal confessions, counterfeit money, journal entries, threatening letters and wills. During the examination of Questioned Documents, investigators must be careful to preserve and not destroy the integrity and authenticity evidence [23].

B. Circumstantial Evidence

Unlike direct evidence circumstantial evidence also known as indirect evidence usually requires an inference to be made in order to establish a fact. This implies that circumstantial evidence is a fact that can be used to infer another fact. In the United States, for example, the law, however, shows no distinction between circumstantial and direct evidence in terms of which has more weight or importance. Both types of evidence may be enough to establish the defendant’s guilt, depending on how the jury finds the facts of the case [29]. During an investigation, much of the scientific evidence as explained in the sub-section to follow is usually circumstantial. This is because it requires a jury to make a connection between the circumstance and the fact in issue. A good example would be fingerprint evidence; a jury must make a connection between this evidence that the accused handled some object tied to the crime and the commission of the crime itself. Examples of circumstantial evidence may include the following:

1) Scientific Evidence

Scientific evidence can be defined as the type of evidence which serves to either support or counters a scientific theory or hypothesis. Such evidence is expected to be empirical evidence and its interpretation should always be in accordance with scientific method. Standards for scientific evidence vary according to the field of inquiry, but the strength of scientific evidence is generally based on the results of statistical analysis and the strength of scientific controls. Competent and reliable scientific evidence means tests, analyses, research, studies, or other evidence based on the expertise of professionals in the relevant area, that has been conducted and evaluated in an objective manner by persons qualified to do so, using procedures generally accepted in the profession to yield accurate and reliable results [24]. Many types of forensic evidence are often considered scientific evidence.

2) Emprical Evidence

According to Pickett [26] empirical evidence, at times referred to as sense experience, is the knowledge or source of knowledge and information acquired through the senses, particularly by observation, experience, and scientific experimentation. Empirical evidence information can be used to justify a belief in the truth or falsity of a claim.

3) Individual Evidence

Individual evidence is evidence that can be virtually and unambiguously linked to a unique, single, specific source. This implies that individual evidence is characterized by unusual and striking qualities and distinctive features that can be traced to a particular source with a high degree of certainty. Examples are fingerprints, handwriting and DNA patterns [9].

4) Class Evidence

Class evidence is any evidence associated with a group and not a single or specific source. This is to mean that class evidence is non-specific and possesses class characteristics. Note that evidence is said to possess class characteristics when it can be associated only with a group and never with a single source [15].

VI. DISCUSSIONS OF THE PROPOSED TAXONOMY

The taxonomy presented in this paper is a new contribution into the DF domain. The scope of the taxonomy is defined by the different categories of the DFE identified in Table 1. The main categories of the evidence as depicted in the taxonomy are Direct Evidence, Real Evidence or Physical Evidence, Documentary Evidence, Demonstrative Evidence, Computer-generated Evidence, Impression Evidence, Trace Evidence, Questioned Documents and Pattern Evidence. These categories are further explained in terms of their scope. The subcategories identified in the taxonomy include examples where applicable. The reader is reminded at this point that most of the subcategories 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 in this paper can be of importance in the DF domain, for example, in describing processes and procedures of how to handle the individual types of evidence during an investigation process. Besides, the taxonomy in this paper can also help in creating a common platform to share information in the digital forensic domain. The taxonomy can also present new research opportunities to students – especially for those interested in how to address issues associated with specific identified DFE. Developers of DF tools can, further, use the taxonomy to fine-tune the tools to cover as many categories and subcategories of the identified evidence during digital forensic investigations.

Developers might also find the taxonomy in this paper useful, especially when considering new digital forensic tools and techniques for addressing specific DFE in the DF domain. The proposed taxonomy can also be used to facilitate the assessment of existing or new tools to fully examine the extent to which the tool addresses the identified evidence. Individuals should also be able to use the proposed taxonomy to carefully and accurately identify and classify – with less effort – the different types of evidence that exist in digital forensics.

Finally, the taxonomy presented in this paper has been designed in such a way as to accommodate new categories and subcategories of evidence that may emerge as a result of domain evolution. It should be possible for individuals to add new categories and subcategories of evidence, including potential modifications in any of the aforementioned categories or subcategories. To the best of the authors' knowledge, at the time of writing this paper there exists no other work of this kind in the DF domain; therefore, this is a new contribution toward advancing the digital forensic domain.

VII. CONCLUSION AND FUTURE WORK

The problem addressed in this paper involves the lack of taxonomy for the different types of DFE that investigators have to battle with to comprehend on a daily basis. Despite several researchers and practitioners having studied and analysed different types of forensic evidence, the DF domain lacks a comprehensive formal classification of its different types of evidence that can be used in legal proceedings. For this reason, this paper, therefore, has proposed a taxonomy of the different categories of DFE. The taxonomy classifies the huge number of DFE into few well-defined and easily understood categories based on literature review. 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 DF tools can address the identified evidence. The taxonomy in this paper can also be easily expanded to include additional categories and subcategories of DFE that may crop up in future. Much research needs to be carried out, though, so as to provide clear directions on how to deal with the many different types of digital evidence in 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.

ACKNOWLEDGMENT

Firstly, we would like to thank the anonymous reviewers that gave constructive review of this paper. Secondly, we gratefully acknowledge the support of Department of Computer Science, and the Information and Computer Security Architectures (ICSA) Research group, University of Pretoria for support while coming up with this research. It is worth noting that any opinions, findings, and conclusions or recommendations expressed in this publication are those of the authors and do not necessarily reflect the views of ICSA or the University of Pretoria.

REFERENCES

[1] ACPO: ACPO Good Practice Guide ACPO Good Practice Guide for Digital Evidence, March 2012

[2] Beebe Nicole: Digital forensics research: the good, the bad, and the unaddressed. In: Fifth annual IFIP WG 11.9 international conference on digital forensics, Orlando, Florida, USA, January 26-28, 2009

[3] Brian, D., & Eugene, H.: Defining event reconstruction of a digital crime scene. *Journal of Forensic Sciences*, *49*(6), 1291-1298.

[4] [Brittany, 16] Brittany M.: Direct Evidence: Definition, Law & Examples. [online] Available from: http://study.com/academy/lesson/direct-evidence-definition-law-examples.html [Accessed March 26, 2016]

[5] Carrier, B.D. and Spafford, E.H.: An Event-based Digital Forensic Investigation Framework. DFRWS 2004.

[6] Casey E.: Digital evidence and computer crime – forensic science, computers and the internet. Cambridge: Academic Press; 2003a. p. 265.

[7] Casey, E. Digital evidence and computer crime: Forensic science, computers, and the internet. Academic press, 2011.

[8] Cohen, F.: Toward a science of digital forensic evidence examination. In *Advances in Digital Forensics VI,* 2010 (pp. 17-35). Springer Berlin Heidelberg.

[9] Deslich, B., & Funkhouser, J.: Forensic Science for High School. Dubuque, IA: Kendall/Hunt.

[10] Duhaime (2015).Trace Evidence Definition: [online] Available from: http://www.duhaime.org/LegalDictionary/T/TraceEvidence.aspx [Accessed March 26, 2016]

[11] FindLaw: Real and Demonstrative Evidence. [online] Available from: http://criminal.findlaw.com/criminal-procedure/real-and-demonstrative-evidence.html#sthash.3wzwztDH.dpuf [Accessed March 26, 2016]

[12] Garfinkel, S. L.: Digital forensics research: The next 10 years. *digital investigation*, 2010. *7*, S64-S73: 2010.

[13] IBM: Transfer Evidence - IBM Knowledge Center. Available from:

[14] .curam.content.doc/CommonEvidenceAndTempEvidence/c_TEMPEV_MaintenanceTransfer.html [Accessed March 27, 2016]

[15] Jack C.: Understanding Trace Evidence -2015 [online] Available from: http://www.exploreforensics.co.uk/understanding-trace-evidence.html [Accessed March 26, 2016]

[16] Jill G. & Michael F.: Individual or Class Evidence. [online] Available from: http://www.theforensicteacher.com/Home_files/Evidence_type_lab.pdf [Accessed March 27, 2016]

[17] Karie, N. M., & Venter, H. S.: Towards a framework for enhancing potential digital evidence presentation. In *Information Security for South Africa,* August, *2013* (pp. 1-8). IEEE.

[18] Karie, N. M., & Venter, H. S.: Taxonomy of challenges for digital forensics. *Journal of forensic sciences*, *60*(4), 885-893: 2015

[19] Kathleen, A.S. and Greg, F.: Associative Evidence. Available from: http://projects.nfstc.org/firearms/module06/fir_m06_t05.htm [Accessed March 27, 2016]

[20] Kebande, V. R., & Venter, H. S.: A Cloud Forensic Readiness Model Using a Botnet as a Service. In *The International Conference on Digital Security and Forensics (DigitalSec2014)* (pp. 23-32). The Society of Digital Information and Wireless Communication.

[21] Kebande, V. R., & Venter, H. S.: Adding event reconstruction to a Cloud Forensic Readiness model. In *Information Security for South Africa (ISSA), 2015* (pp. 1-9). IEEE.

[22] Kozushko, H.: Digital evidence -2003. *[online], http://infohost. nmt. edu/~ sfs/Students/HarleyKozushko/Papers/DigitalEvidencePaper. Pdf.*

[23] NIJ: Questioned Documents -2015. [online] Available from: http://www.nij.gov/topics/forensics/evidence/questioned-documents/Pages/welcome.aspx?tags=Questioned%20Documents [Accessed March 26, 2016]

[24] NIJ: Impression and Pattern Evidence - 2015b. [online] Available from: http://www.nij.gov/topics/forensics/evidence/impression/pages/welcome.aspx [Accessed March 26, 2016]

[25] NIJ: special report: Forensic Examination of Digital Evidence: A guide for Law enforcement: 2015c [online] Accessed at https://www.ncjrs.gov/pdffiles1/nij/199408.pdf [Accessed March 27, 2016]

[26] Palmer:" A Road Map for Digital Forensic Research" – 2001. [online] Available from: https://www.dfrws.org/2001/dfrws-rm-final.pdf [Accessed March 27, 2016]

[27] Pickett, Joseph P., ed.: "Empirical". The American Heritage Dictionary of the English Language (2011, 5th ed.). Houghton Mifflin. ISBN 978-0-547-04101-8.

[28] Politt M.M.: Six blind men from Indostan. Digital forensics research workshop (DFRWS); 2004.

[29] Pollitt, M.: Applying traditional forensic taxonomy to digital forensics. In *Advances in Digital Forensics IV* - 2008 (pp. 17-26). Springer US.:2008.

[30] Probablecause: What is the difference between circumstantial and direct evidence? - 2015 Available at: http://www.probablecause.org/directevidence.html [Accessed March 26, 2016]

https://www.ibm.com/support/knowledgecenter/SS8S5A_6.1.1/com.ibm

[31] Rottenstein: What is circumstantial evidence? What is direct evidence? Available from: http://www.rotlaw.com/legal-library/what-is-circumstantial-evidence-what-is-direct-evidence/ [Accessed March 26, 2016]

[32] Kebande, V. R., & Venter, H. S. Requirements for Achieving Digital Forensic Readiness in the Cloud Environment Using an NMB Solution. In *11th International Conference on Cyber Warfare and Security: ICCWS2016* (p. 399). Academic Conferences and publishing limited.

[33] Kebande, V.R, Ntsamo, H. S., & Venter, H. S. Towards a prototype for Achieving Digital Forensic Readiness in the Cloud using a Distributed NMB Solution. In *ECCWS2016-Proceedings fo the 15th European Conference on Cyber Warfare and Security* (p. 369). Academic Conferences and publishing limited, 2016.

[34] Kebande, V. R., & Venter, H. S. Novel digital forensic readiness technique in the cloud environment. *Australian Journal of Forensic Sciences*, 1-40, 2016.

[35] Karie, N.M, Kebande, V.R. A Generic Framework for Digital Evidence Traceability. In *ECCWS2016-Proceedings fo the 15th European Conference on Cyber Warfare and Security* (p. 361). Academic Conferences and publishing limited, 2017.

[36] Kebande, V. R., Karie, N. M., & Venter, H. S. A generic Digital Forensic Readiness model for BYOD using honeypot technology. In *IST-Africa Week Conference, 2016* (pp. 1-12). IEEE, 2016.

[37] Kebande, V. R., & Venter, H. S. On digital forensic readiness in the cloud using a distributed agent-based solution: issues and challenges. *Australian Journal of Forensic Sciences*, 1-30, 2016.

[38] Kebande, V. R., & Karie, N. M. An Approach for Estimating Forensic Data Provenance of an Object in the Cloud Environment Using one Dimensional Successive Bisection Method, 2016.

[39] Kebande, V. R., Karie, N. M., & Omeleze, S. A Mobile Forensic Readiness Model aimed at Minimizing Cyber Bullying, 2016.

[40] Kebande, V.R, & Venter, H.S. Towards a Model for Characterizing Potential Digital Evidence in the Cloud Environment during Digital Forensic Readiness Process. In *ICCSM2015-3rd International Conference on Cloud Security and Management: ICCSM2015* (p. 151). Academic Conferences and publishing limited, 2015.

[41] Kebande, V. R., & Karie, N. M. A framework for integrating multimodal biometrics with digital forensics. *International Journal of Cyber-Security and Digital Forensics (IJCSDF), 4*(4), 498-507, 2015.

[42] Kebande, V., & Venter, H. S. A functional architecture for cloud forensic readiness large-scale potential digital evidence analysis. In *Proceedings of the 14th European Conference on Cyber Warfare and Security 2015: ECCWS 2015* (p. 373).

[43] Kebande, V. R., & Venter, H. S. Obfuscating a cloud-based botnet towards digital forensic readiness. In *Iccws 2015-The Proceedings of the 10th International Conference on Cyber Warfare and Security* (p. 434), 2015.

[44] Kebande V. R, Karie N.M., Michael, A, Semaka, M & Venter, H.S(2017, Ma). How an IoT-enabled "Smart Refrigerator" can play a Clandestine Role in Perpetuating Cyber-crime. In IST-Africa, 2017 IEEE International Conference on. IEEE-To appear.