Knowledge Management as a Strategic Asset in Digital Forensic Investigations

1Nickson M. Karie* and 2Victor R. Kebande†

1Department of Computer Science, University of Swaziland, Private Bag 4, Kwaluseni, Swaziland
2Department of Computer Science, University of Pretoria, Private Bag X20, Hatfield 0028, Pretoria, South Africa
nickson.karie@gmail.com*, vickkebande@gmail.com†

ABSTRACT
While conducting a Digital Forensic Investigation (DFI), detectives make use of specialised skills and knowledge to capture, manage and analyse enormous amounts of Potential Digital Evidence (PDE) data and information, which may be used to support legal actions during civil or criminal proceedings in a court of law. However, based on the nature of the DFI process, new skills and knowledge may sometimes be needed to handle an incident at hand. This is because every DFI process may be unique and might differ greatly from previously handled DFI processes, hence the need for new knowledge and skills. The problem addressed in this paper, however, is that, most of the new knowledge generated during DFI processes is not explicitly recorded and this hampers external reviews and training of other digital forensic investigators. Past experience may and should be used to train new digital forensic personnel, as a way of fostering knowledge sharing and reuse among digital forensic investigators and law enforcement agencies. In the long run, such initiatives will expose any new generated knowledge and information to quality assessment by the digital forensic community and other third parties. For this reason, the authors in this paper examine the subject of Knowledge Management (KM) as a strategic asset in digital forensic investigations to support legal actions in court and civil proceedings. As a new contribution, this paper goes further to propose a Knowledge Management Life Cycle (KMLC) that can be beneficial to digital forensic community. This proposition is meant to encourage knowledge sharing and reuse as well as enhance the process of knowledge capturing and development during a digital forensic investigation process.

KEYWORDS
Knowledge management, strategic asset, digital forensic investigations, life cycle, knowledge creation, development, sharing and re-use

1 INTRODUCTION
We live in a globalised world which has evidently shown that our lives have been overtaken by technology and sporadic-savvy innovations of the 21st century that a majority are struggling to catch up with. These techno-savvy innovations have created tech-enabled societies and it is a fact that it has made technology to become too personal. As a result of these technological trends, data and information has become an aspect that is being utilised in all areas of our daily lives. This technological impact has also been felt by individuals, businesses, governments, scientists, military, agriculturalist, and among other areas of our life today. This can be attributed to the explosion of digital devices and the growth of the internet which has integrated the way communication and information is disseminated across different geographic regions.

The impact of this integration has also attracted considerable interests from many disciplines. In fact, it has been felt across diverse disciplines and this has, in most cases, been used as a basis for development purposes. Based on this it has become possible to create information centric portals or infrastructures like supply chain management, cloud-based architectures that have been used to share information irrespective of the location. It is worth noting that in these developments, innovations and evolutions, data, information and knowledge has been a critical aspect.

One adverse effect that has been experienced as a result of device integration and simplified communication, for example, is the aspect of having adversaries that have managed to capitalise
on these benefits by being able to conduct digital crimes over computer-based networks. This has in turn led to the development of Digital Forensics (DF) which is a science that investigates digital crimes using scientifically proven methods [1]. To provide proof that a digital crime has occurred, one needs to extract Potential Digital Evidence (PDE) from the voluminous information in order to prove or refute a fact in a court of law. However, any piece of PDE captured can only be admissible in a court of law based on the standards and rules of evidence which then needs special knowledge and skills to handle it.

Dealing and coping with this plethora of data, information, skills and the knowledge that is associated with the PDE is a concern because data streams in huge volumes and in complex structures [2]. Therefore, the authors argue that, there is a need for the digital forensic experts and the Law Enforcement Agencies (LEA) to have a way of managing knowledge in such a way that it helps investigators extract evidential artefacts from digital environments in the best way possible so that the PDE is able to satisfy admissibility in a court of law.

For this reason, special knowledge is usually required when dealing with this aspect of Digital Forensic Investigations (DFI); however, there exist no effective techniques through which the forensic experts and the LEA can use to share this knowledge and skills with ease. More specifically, for collaborative expertise regarding new knowledge and other aspects related to the extracted PDE. Therefore, the authors proposed a Knowledge Management Life Cycle (KMLC) that allows and encourages not only sharing but also reusing new knowledge generated during the processes of extracting PDE. This demarcation has been used as a standpoint that is able to bring out new techniques through which Knowledge Management (KM) can be used as a strategic asset in DF.

The remainder of this paper is structured as follows. In Section 2, we present a brief background of the existing literature, reviewing KM research specifically. In Section 3, we provide a related work on our analysis of the trends of KM research. KM in DF is presented and discussed in Section 4. Section 5 presents the proposed KMLC for DF followed by a discussion of the same in section 6. Finally, conclusions drawn from this work and future work are highlighted in section 7.

2 BACKGROUND
In this section the authors briefly presents a discussion on Knowledge Management (KM), Digital Forensics (DF), as well as Digital Evidence (DE).

2.1 Knowledge Management
Knowledge Management (KM) as highlighted by Barclay and Murray [3] encompasses a technique of identifying and making huge amount of information accessible in an organisation through sharing. However, Jiang, Liu and Cui [4] view it as a process of automating knowledge across organisations through the distribution of information. These authors [4] have also pointed out the key factors that a KM system should satisfy, which include: ontology/taxonomy-based [5], document-based, Artificial Intelligence (AI)-based and web-based. According to Becerra-Fernandez and Sabherwal [6] KM consist of a process that discovers, captures, shares and applies knowledge for purposes of improving some perceived objectives.

Turban [7] expresses KM to be a process that identifies, selects, manages, transfers and disseminates information in order to solve a particular problem or in order to make a strategic decision. Another author [8] brings out KM to be an important strategic resource that enables the utilisation of management processes and practices to achieve its objective. This has been achieved by harnessing the complexity involved and making use of knowledge as a resource. In this paper, however, KM is viewed as a process that involves knowledge creation, knowledge discovery, knowledge use or utilisation, knowledge transfer/sharing or dissemination as well as knowledge application and reuse. The details of the Knowledge Management Processes (KMPs) are summarised using the KMLC and are
explained using Figure 1 presented in Section 4 of this paper.

2.2 Digital Forensics (DF)
Hitherto, the discussion has mainly been focused on the techniques through which knowledge can be shared so that it can aid in conducting DFIs. DF is a science that targets to provide proof of occurrence of an incident through the use of scientifically proven methods. DF can be applied across many areas like database forensics where huge amount of information can be stored, mobile forensics, cloud forensics, multimedia forensics, software forensics, computer forensics among other areas.

There exist a number of processes that have been proposed that helps to achieve these scientific processes. For example, Kohn, Olivier and Eloff [9] have proposed a process model with the following; preparation, investigation and presentation. Kebande and Venter [10] have also proposed a Cloud Forensic Readiness-as a service (CFRaaS) Model while the Digital Forensic Research Working Group (DFRWS) proposed a process consisting of identification, collection, preservation, examination and analysis and presentation [11]. Lastly, Kruse II, Warren and Heiser [12] also proposed a process acquisition, authentication and analysis.

In this paper, the authors argue that DF investigators and the Law Enforcement Agencies (LEA) need to find techniques for managing and sharing new knowledge generated during any DFI process. This can be a stepping stone towards effective analysis of digital evidence, particularly in extracting “digitised knowledge” from digital sources. If this knowledge is shared among the forensic expert then it might act as a strategic tool that can give evidential insights hence making any evidence to be probative. Nevertheless, Beebe [13] highlighted that DF provides a mainstream knowledge that allows the tracks, traces and footprints that are left behind to be probative, hence the need to manage this knowledge to the success of any DFI process.

2.2 Digital Forensic Evidence
Carrier and Spafford [14] in their research study on digital event reconstruction of a crime scene highlighted that digital evidence of an incident can be considered to be digital data, which might contain useful information. This information can be used to develop a hypothesis that can refute or support the occurrence of a digital incident. DF experts and LEA solely depend on digital evidence extensively whenever they want to link a digital crime with the perpetrator. Research by Karie, Kebande and Venter [15] presented taxonomy for Digital Forensic Evidence (DFE), which was able to show different categories of DFE that can be of potential value to investigators. Based on this taxonomy, it is easy to uniquely manage some knowledge based on the types of evidence.

For digital evidence to be considered for presentation in a legal basis it should have a capability of satisfying probative or prejudicial value [16]. However, the following aspects should also be satisfied: Admissibility, evidential integrity and digital preservation. Based on this aspect, Karie, Kebande and Venter [17]; Karie and Venter, [18] proposed a framework for digital evidence traceability that was able to trace digital evidence from a list of evidences and a framework for potential digital evidence presentation respectively. From the discussion that has been presented in this section, it is evident that for KM and sharing digital data among forensic experts is important, especially when trying to analyse different aspects of digital evidence from a crime scene.

3 RELATED WORKS
Looking at what has previously been done by different researchers, the authors acknowledge the following studies that have played a significant role in this current study. A Digital Forensic Web-Based System (DFWBS) that is able to share knowledge was proposed by Buang, and Daud [19]. This system adopted a throwaway prototyping methodology to incorporate users, knowledge sharing, knowledge classification and the creation of knowledge. While this research was able to put across a novel proposition, it was presented in a superficial approach.
Another research by Tanner and Dampier [20] proposed an approach for re-using and managing knowledge in DF examination. This study allowed LEA to be able to manage the details of the cases of Digital Forensic Evidence (DFE). Additionally, these authors were able to apply the concept of mapping cases using domain modelling approach as a suitable technique. Another technique for managing DF knowledge has highlighted an approach where lessons of KM are applied to DF. This aspect has enabled the creation of a National Repository of Digital Forensic Intelligence (NRDFI) which has proved to be useful [21].

More research proposed by Ćosić, et al. [22] as well as Karie and Kebande [5] optimises ontological approaches to enable studying and managing the chains of custody for digital evidence. These studies have been able to define procedures that could manage digital evidence by use of taxonomy (classifications). Another study by Karie, Kebande and Venter [15] has highlighted techniques that can be used to identify or give knowledge by presenting a taxonomical approach for digital forensic evidence. In this study, the common understanding of digital evidence was able to be presented using taxonomy.

While the above mentioned research studies remains useful and insightful while sharing knowledge in DF domain, none of these studies was focused towards KMLC as has been proposed in this paper, however, we highly acknowledge the contribution made by the above mentioned authors. The next section presents the concepts of KM in DF.

4 KNOWLEDGE MANAGEMENT IN DIGITAL FORENSICS

With the continued evolution in digital technology and other technological devices, the world is bound to experience more cyber security issues now than before. This also implies that the world will further experience more malicious actors that break into digital systems and networks to cause havoc or steal and manipulate sensitive data. For this reason, specialised knowledge and skills will always be needed to help any DFE to be able to gather or process any PDE at a crime scene. However, the biggest problem as at the time of this study is in the management of the Digital Forensic Knowledge (DFK) and using it as a strategic asset in Digital Forensic Investigations (DFIs). This section of the paper therefore presents the concept of KM as a strategic asset in DFIs.

Note that in any organisation, a strategic asset is usually an asset that is needed by the organisation in order for it to maintain its’ ability to achieve its goals. Without such assets, the future of the organisation could be at risk. This therefore means that, if DF is to achieve its goals then KM is that strategic asset that should be taken seriously and highly valued during digital forensic investigations.

In this regard, therefore, the authors argue that the success of any DFI process is to some extent dependent on the knowledge and skills used by DFEs. This includes the knowledge of all the steps of the DFI processes as well as a good understanding of how to use the DF tools and techniques to achieve the goals of the investigation process. It is on these grounds, that the authors believe that such knowledge and skills in DF are critical to the success of a DFI process hence the needs to treat it like any other strategic asset in an organisation. The knowledge and skills owned by a digital forensic investigator is what can easily determine the success or failure of an investigation process. This is also to mean that, such knowledge and skills are usually critical to any defensive strategy as well as the DF process itself.

Finally, for the DFI process to have the ability to achieve its goals, the authors have come up with a Knowledge Management Life Cycle (KMLC) for the DF domain. In the next section of this paper, an explanation of the proposed KMLC for DF is presented.
5 PROPOSED KNOWLEDGE MANAGEMENT LIFE CYCLE (KMLC) FOR DIGITAL FORENSICS
This section presents a KMLC for the DF domain as a new contribution. An explanation of how the KMLC can be used to help DF detectives during any DFI process is also explained. The authors concentrate on discussing the important aspects that can be used to help digital forensic investigators to learn how to manage and possibly share and re-use knowledge acquired during a DFI process. The KMLC is presented in two approaches as shown in Figure 1 and Figure 2 respectively.

Figure 1 show the high-level view of the KMLC which is then followed by an all-inclusive and detailed KMLC process presented later in Figure 2. From Figure 1, the reader can infer that the high-level view of the life cycle consists of five distinctive phases namely: Knowledge Creation, Knowledge Discovery, Knowledge Use or Utilisation, Knowledge Transfer, Sharing or Dissemination and finally Knowledge Application and Re-use.

The Knowledge Creation phase as shown in Figure 1 deals with the ability to create new DF knowledge as well as the formation of new ideas through interactions between explicit and tacit knowledge in individual human minds. Note that, according to Helie, et al. [23], explicit knowledge is knowledge that can be readily articulated, codified, accessed and verbalized. It can be easily transmitted to others. Most forms of explicit knowledge can be stored in certain media. The information contained in encyclopaedias and textbooks are good examples of explicit knowledge. On the other hand, tacit knowledge is the kind of knowledge that is difficult to transfer to another person by means of writing it down or verbalizing it. The Knowledge Discovery phase deals with discovering and extracting useful knowledge from an existing collection of DF data.

5.1 Knowledge Creation
Knowledge creation is a continuous process where users are exposed to new knowledge through education and training, interaction with other digital forensic experts, collaborations as well as through individual experience and practice. This phase is labelled 1 in Figure 1. The sub-processes associated with knowledge creation are briefly explained below.
5.1.1 Education and Training
This is when digital forensic experts may use their communication skills and knowledge to guide and train fellow forensic experts as well as help them develop and learn new knowledge and skills related to digital forensic activities. The primary objective of the education and training phase in this study is to equip digital forensic investigators with knowledge, know-how, skills and competences required to handle a DFI process. This also helps them develop critical thinking skills which is an ingredient of creating new knowledge.

5.1.2 Interaction with Digital Forensic Experts
The goal of interacting with digital forensic experts is to help other forensic investigators learn and exchange new ideas in the domain. Interaction with DF experts is one way to give forensic investigators a more realistic exposure to how other forensic experts use their knowledge and skills to meet the objectives of a DF process. This helps in creating an environment where new investigators can think of new ways and new knowledge of dealing with a PDE.

5.1.3 Collaborations
Collaboration can be viewed as the process of working with someone to realise or achieve something successfully [24]. In the case of this paper, DF investigators should always be allowed to collaborate as a way to achieve a defined and common purpose which is a successfully DF investigation process. Collaboration encourages openness among DF investigators and knowledge sharing as a way to achieve the results of the collaborative effort. Collaboration can also be an avenue to creating new ways and new knowledge of handling a DF investigation process.

5.1.4 Individual Practice and Experience
Individual investigation practices helps DF investigators gain some level of experience. This further helps them reduce mistakes during a DF investigation process. According to Angelo [25], the difference between practice and experience is that practice is often controlled. However, the real world has many variables. The more you deal with all the different variables, the better you become at dealing with and anticipating them hence experience is gained. Finally, as stated by Frost [26], the shift in condition between the possession of knowledge and the act of knowing something that comes about through education and training, interaction with other digital forensic experts, collaborations as well as through practice and experience is the driving force in creation of new knowledge.

5.2 Knowledge Discovery
The continued growth of digital data due to technological advances has created an immense need for knowledge discovery methodologies. In the case of this paper, the knowledge discovery phase deals with: Knowledge Identification, Knowledge Capture or Extraction, Knowledge Classification as well as Knowledge Selection. This phase is labelled 2 in Figure 2 and is briefly explained in the sub-sections to follow.

5.2.1 Knowledge Identification
Knowledge Identification refers to the process of proactively identifying different forms of knowledge and transforming data or isolated facts with no meaning and information or interpreted data with meaning into a value-added actionable resource. Having an understanding of the different forms of knowledge that exist in digital forensic and being able to distinguish between various types of knowledge in in the domain is an essential step for KM [26].
5.2.2 Knowledge Capture or Extraction

In digital forensics, knowledge capture or extraction will make tacit knowledge explicit. As mentioned earlier, explicit knowledge refers to codified knowledge, such as that found in documents, while tacit refers to non-codified knowledge and often personal or experience-based knowledge. This is the process that turns knowledge that is resident in the mind of a digital forensic investigator, for example, into an explicit representation available for use by others in different documented forms.

5.2.3 Knowledge Classification

Digital forensic knowledge classification can be represented in three groups: general knowledge, domain-specific knowledge and site specific knowledge. General knowledge is true for most online documents while domain specific knowledge is true in a particular domain like digital forensics. Site specific knowledge is true for a particular site. Site specific knowledge mainly consists of the site specific data formatting conventions. This process helps DF investigators to know what type of knowledge is needed for extracting different types of PDE during investigations through classification.

5.2.4 Knowledge Selection

Knowledge selection in the digital forensic domain aims at selecting relevant knowledge out of a knowledge base for a particular task e.g. evidence acquisition from a crime scene. Knowledge selection is important for supporting knowledge re-use in DF by the digital forensic
investigators. This is backed up by the fact that, every digital investigation process may be unique and differs greatly from any previous handled processes; hence the need for specific carefully selected knowledge and skills to be used to support a forensic investigation at hand.

5.3 Knowledge Use or Utilisation
Knowledge use or utilisation according to larapedia [27] is using accumulated knowledge to tackle problems, develop new products and deal with unfamiliar situations. Knowledge is of no use unless it is applied to solve problems [27]. Knowledge utilisation may also include various activities aimed at increasing the use of knowledge to solve problems. In this case, digital forensics practitioners usually acquire, construct, synthesise, share and apply this knowledge during DFIs. This phase is labelled 3 in Figure 2 and has knowledge absorption, knowledge exploration and knowledge exploitation which are discussed next.

5.3.1 Knowledge Absorption
Knowledge absorption in the context of digital forensics can be understood as the process of acquiring knowledge from outside entities such as from universities and Colleges. Absorption is important because most of the new digital forensic knowledge is usually created outside any particular organisation. For any digital forensic practitioner to use or utilise any knowledge, it should first be absorbed hence the need for knowledge absorption in this phase. Universities and colleges play a key role in equipping digital forensic investigators with this knowledge before releasing them for field practise.

5.3.2 Knowledge Exploration
This can be seen as the process of creating new knowledge. Once knowledge has been absorbed, the forensic practitioners can then use such knowledge to further create new digital forensic knowledge. This process supports many other process of the KMLC shown in Figure 2. For example, collaborations can lead to creating new knowledge as well.

5.3.3 Knowledge Exploitation
Once new knowledge has been created, the digital forensic practitioners can then exploit such knowledge. Knowledge exploitation is the fullest and most profitable use of absorbed knowledge by any individual. This also implies, effectively making the best use of any new generated knowledge in the domain of interest. It also refers to the use of existing knowledge from various sources by the same individual. The individual in this case is the digital forensic practitioner.

5.4 Knowledge Transfer, Sharing or Dissemination
Knowledge transfer refers to sharing or disseminating of knowledge and providing inputs to problem solving [28]. The main objective is to transfer knowledge from one digital forensic practitioner to another. Knowledge transfer also seeks to organise, create, capture or distribute knowledge and ensure its availability for future digital forensic practitioners. This can be achieved through investigator training as well as investigation case studies.

5.4.1 Investigator Training
Digital forensic investigator training is the process of preparing digital forensic practitioners to be able to carry out successful investigation processes. In the case of this paper, it includes all the activities needed by the practitioners to support digital forensic investigation process including the creation of new knowledge. Digital forensic investigator training provides assurance that new digital forensic practitioners are fully equipped with all the required knowledge, skills, and abilities that are expected of all digital forensic investigators to meet the rigorous demands of the digital forensic environment in which they will always operate. Universities and colleges can also be used to train digital forensic investigators by exposing them to real life crime scene investigation case studies.

5.4.2 Investigation Case Studies
A case study is usually a report about a situation that has been studied over a period of time. In the case of this paper, we refer to digital crime scene investigation case studies. When used in DF,
investigation case studies can simplify complex concepts, improve complex or critical thinking, promote understanding and facilitate active learning of different techniques by the practitioners with a particular emphasis on problem solving. Digital forensic practitioners therefore, can learn from previous recorded knowledge as well as be pioneers in producing new knowledge needed to effectively solve similar investigative problems.

5.5 Knowledge Application and Re-use
Knowledge application and re-use comes into play when available knowledge is used to make decisions and perform tasks through direction and routines [29]. In the case of this paper, knowledge application is defined as the process of integrating new knowledge into the digital investigation process. This includes all the activities concerned with deploying new knowledge or re-using existing knowledge in order to have skills and competences required to handle a successful digital forensic investigation process. KM strategy and knowledge proficiency through experience are discussed below as the two areas that have been identified in this paper to propel knowledge application and re-use. This phase is labelled 5 in Figure 2 and is explained in the subsections to follow.

5.5.1 Knowledge Management Strategy
A Knowledge Management Strategy (KMS) is a general outline that identifies the key needs and issues within a domain, and provides a framework for addressing these issues. A KM strategy supports most of the activities discussed earlier in this paper e.g. knowledge sharing, knowledge creation, knowledge discovery among others. It is therefore very important for the DFI to have a strategy of how to manage the digital forensic knowledge generated during investigations.

5.5.2 Knowledge Proficiency through Experience
Knowledge proficiency is the ability to apply both the technical knowledge and skills required for the digital investigation role and responsibilities in order to achieve the expected outputs of the investigation process. Proficient simply means an advanced degree of competence which can be acquired through experience and training. This is the core of having a successful digital forensic investigation process. The next section presents a discussion based on the proposed KMLC in this paper.

6 DISCUSSION OF THE PROPOSED KMLC
To the best of the authors’ knowledge the KMLC that has been proposed in this paper is a new contribution in the DF domain at the time of writing this research paper. The scope of the life cycle is defined by the phases in KMLC as seen Figure 1. The main phases as depicted in Figure 1 include: Knowledge creation, Knowledge discovery, Knowledge use or utilisation, Knowledge transfer, sharing or dissemination and Knowledge application and Re-use. The phases as identified in the life cycle can be used, for example, to help in knowledge creation and re-use during digital forensic investigations. Not that the specific order of the KMLC is not fixed hence to adopt or implement it one can decide to start from any phase and iterate through all other phases.

The specific details of the individual phases as identified in the Figure 1 have further been explained in this paper. However, note that the different phase as identified in Figure 1 are meant to facilitate this study and primarily focus on KM for DF. Such proposed phases are by no means the final guaranteed steps to perfect digital forensic KM processes. In the authors’ opinion, however, organising the KMLC into phases was necessary to simplify its understanding as well as to present specific finer details of the KMLC. More phases can also be added into the KMLC as technology and the DF domain keeps evolving.

The proposed life cycle in this paper can be used in the DF domain, for example, to help digital forensic investigators in creating new knowledge as well as in identifying relevant application of such knowledge during a DFI process. Moreover, the KMLC can also be helpful to different stakeholders and scholars as well, for example, in reasoning about the application of specific new knowledge during a DFI process. In addition, the KMLC can also be used for training digital forensic investigators, especially on how to create
and manage knowledge during a digital forensic investigation process. Academic institutions will also find the KMLC in this paper constructive, especially when training students on how to handle digital forensic knowledge during DFIs. Furthermore, such a KMLC can also be used when developing education materials for different programs of study within the field of DF.

Developers of DF tools can also use the proposed KMLC to develop tools that have the ability to incorporate KM. This also implies that developers might find the KMLC in this paper useful, especially when considering the development of new DF tools and techniques for addressing the problem of KM in DF. Finally, the KMLC presented in this paper has been designed in such a way that it can accommodate new phases that may emerge as a result of domain evolution and technological change.

To the best of the authors' knowledge, there exists no other work of this kind in the domain of DF. Therefore, this is a new contribution towards advancing the DF domain. The next section concludes this paper and makes mention of the future work.

7 CONCLUSIONS AND FUTURE WORK
In this paper, the authors have discussed KM as a strategic asset for digital forensic investigations. The authors presented this using the KMLC which has five phases namely: knowledge creation, knowledge discovery, knowledge use or utilisation, knowledge transfer, sharing or dissemination and finally knowledge application and re-use. Having an understating of all these phases is essential for any digital forensic investigator as this can help in managing DF knowledge with ease. With the current trends of innovative technologies, new knowledge will always be needed to deal with different incidences. It is, therefore, important to build frameworks with the capability to help in KM during digital forensic investigations as well as support the forensic community. KM has been employed as a very important part of many disciplines hence the need to incorporate it to DF as well.

Finally, having pointed out the KMLC, this research therefore, mentions future work that will involve testing and evaluating the feasibility of the proposed KMLC. Secondly will be the development and implementation of a prototype that can possible automates some if not all of the different processes involved in the KMLC. The focus of this prototype will be how contextual knowledge can be identified and captured so as to help digital forensic investigators manage any new knowledge generated during digital forensic investigations. More research also needs to be conducted to improve the KMLC proposed in this paper as well as spark further discussion on the development of new digital forensic techniques to handle KM.

8 REFERENCES


