Towards a Framework for Enhancing Potential Digital Evidence Presentation

[1,2]Nickson M. Karie
[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

[1]H.S. Venter
[1]Department of Computer Science,
University of Pretoria,
Private Bag X20, Hatfield 0028,
Pretoria, South Africa.
Email: hventer@cs.up.ac.za

Abstract—**In the case of digital forensic investigations, the potential digital evidence captured, the analysis, interpretation, and attribution must ultimately be presented in the form of expert reports, depositions, and testimony in any legal proceedings. If the presentation and interpretation of the potential digital evidence is conducted correctly, it is much easier and useful in apprehending the attacker and stands a much greater chance of being admissible in the event of a prosecution. Wrongly presented and interpreted potential digital evidence data might create loopholes for perpetrators to exploit, thus, making it hard to convict and prosecute them.**

Existing digital forensic investigation process models have provided guidelines for identifying and preserving potential digital evidence captured from a crime scene. However, the extent to which such potential digital evidence may be admissible in a court of law remains a challenge to investigators. This is backed up by the fact that there are currently no standardised guidelines for even presenting the most common representations of digital forensic evidence. Therefore, in the authors' opinion, methodologies and specifications need to be developed in the field of digital forensics with the ability to effectively enhance the potential digital evidence presentation and interpretation in any legal proceedings.

In this paper, therefore, we present a step-by-step framework in an attempt to propose high-level guidelines for enhancing the potential digital evidence presentation in any legal proceedings. Such a framework will be helpful to digital forensic experts, for example, in structuring investigation findings as well as in identifying relevant patterns of events to be incorporated during the presentation of potential digital evidence. The framework will also assist law enforcement agencies, for example, to determine, with less effort, the validity, weight and admissibility of any potential digital evidence presented. However, it should be noted that the purpose of this paper is not to replace any of the extensive and known evidence presentation principles, but serves as a survey of the state of the art of the research area while proposing harmonised and high-level guidelines for enhancing the presentation of potential digital evidence in legal proceedings.

Keywords-digital forensics, evidence presentation, admissibility of evidence, legal proceedings, evidence validation, evidence weight, law enforcement agencies

I. INTRODUCTION

The admissibility of potential digital evidence in any court of law is nowadays coming under increased scrutiny [1, 2]. Therefore, to convince the court that the potential digital evidence presented is worthy of inclusion into the criminal process, the digital forensic experts require extensive technical knowledge and skills, including methodologies and specifications typically designed for potential digital evidence presentation in any court of law. This also implies that, the techniques, knowledge and skills used by the digital forensic experts during potential digital evidence presentation, should have the ability to convince the judges on the validity, reliability and the weight of the potential digital evidence captured during the investigation process. Moreover, the methodologies and specifications used should also be able to assist the law enforcement agencies determine, with less effort, the admissibility of the potential digital evidence presented.

In the case where the crime committed calls for prosecution, the interpretation, validation and evaluation of the weight of the potential digital evidence presented in the court may require confidence from the digital forensic experts about the inferences drawn from the potential digital evidence itself. This implies that the validation and evaluation of potential digital evidence might also require the verification of reliable sources with regards to where the evidence was created. In addition, the digital forensic experts might be required to show how the evidence was processed and transported, including the evidence file itself, the application, the operating systems and the hardware platforms [3] used during the investigation process.

Therefore, in the authors' opinion, methodologies and specifications need to be developed in digital forensics with the ability to effectively enhance digital evidence presentation and interpretation in legal proceedings. Furthermore, the requirement of such methodologies and specifications in digital forensics is exceptionally important - both for the advancement of the field as well as for the effective use of tools, upon which the science of digital forensics and use in evaluation by courts depend [4]. Such methodologies will also assist law enforcement agencies, for example, in differentiating between experts' own opinions from what the potential digital evidence really portrays.

As for the remaining part of this paper, section II presents background concepts on potential digital forensic evidence presentation while section III considers some previous and related work. A detailed explanation of the proposed framework is handled in section IV followed a critical evaluation of the framework in section V. Finally, conclusion and future work is given in section VI.

II. Background

Digital forensics (DF) is a new and growing field in both research and industry [5]. Furthermore, it is considered a branch of forensic science dealing with the recovery and investigation of material found in digital devices, often in relation to digital crimes. According to Resendez et al [6], DF combines elements of law and computer science to collect and analyse data from computer systems, networks, wireless communications, and storage devices in a way that is admissible as evidence in a court of law. Being related to law and technology, DF, therefore, requires more discipline than just physical forensic techniques [7]. Note that, physical forensic techniques involves investigations performed by trained practitioners using tangible, physical items found on, in, or around a body at the crime scene. The perception is that this domain solely supports law enforcement and the courts [8]. Moreover, according to Newsom [9], physical forensic analysis can be controlled in the laboratory setting and can progress logically, incrementally, and in concert with widely accepted forensic practices. In comparison, DF is almost entirely technology and market driven, generally outside the laboratory setting, and the examinations present unique variations in almost every situation. [9].

When considering the digital forensic investigation process, the evidence presentation phase is arguably one of the most significant phases of the digital forensic investigation process [10]. The investigators involved should, therefore, be competent and proficient in all the investigation processes used. In addition, the investigation processes should be compatible with the relevant policies and/or laws in various jurisdictions. This also means that the procedures and techniques used in digital forensic investigations should also allow the findings to be admitted to a court of law [11] or presented in any other legal proceedings. However, if evidence is not properly or legally acquired it may not be court admissible.

After an investigation process has been conducted, the results or findings are usually documented and presented to the authorities or to any legal proceedings as potential digital evidence. Such potential digital evidence data can then be used to support or refute a hypothesis that was formulated during the investigation process. This is a general notion of evidence and may include data that might not have been admissible previously in a court of law, particularly in a case where the evidence was not properly or legally acquired [11].

Although, most of the digital forensic investigation process models currently used have provided guidelines for identifying and preserving potential digital evidence from a crime scene [12], in the authors' opinion, more rigorous and flexible process models and frameworks need to be developed. This will allow for efficient investigation and further, as a way towards easing, the presentation of potential digital evidence in any court of law. The absence of such models and frameworks in digital forensics, for example, can make it hard for law enforcement agencies to identify relevant potential digital evidence to support or refute a particular court case. In addition, this absence can lead to different ways of presenting potential digital evidence in court, thus, leading to different interpretation and court outcomes [4]. In the next section, the authors will examine existing related work in the digital forensic domain.

III. Related Work

There exists several research works in digital forensics from different researchers, which have made valuable contributions towards the development of the framework presented in this paper. In this section, therefore, a summary of some of the most prominent efforts in previous research work is provided.

To begin with, Boddington et al [13] argues that digital evidence is now common in legal cases. However, the understanding of the legal fraternity as to how far conventional ideas of evidence can be extended into the digital domain lags behind. There arises a need, therefore, for a practical 'roadmap' that can guide the legal practitioner in identifying potential digital evidence relevant to support a particular case and in assessing its weight. Their paper goes further and describes a process by which the validation of relevant potential digital evidence required for legal argument can be facilitated, by an interrogative approach that ensures the chain of reasoning is sustained. In this paper, however, we focus on presenting a step-by-step framework that offers a simplified platform to help digital forensic experts, for example, in structuring investigation findings as well as in identifying relevant patterns of events to be incorporated during the presentation of the potential digital evidence in legal proceedings. Such a framework can also assist law enforcement agencies, for example, in reasoning and differentiating between experts' own opinions from what the potential digital evidence really portrays.

In another paper by Sherman [14], he explains that digital forensic experts can discover significant and damning evidence that can potentially convict suspects and prosecute them. However, no matter how momentous the evidence or how skillful the investigator have been at recovering it, if the potential digital evidence presentation is not conducted in a coherent and understandable way to the court, the case may be lost. Their paper then elaborates on the different tools and methods to assist investigators in providing comprehensible forensic evidence in a criminal prosecution. In addition, they explain how, by using such methods, investigators will have an increased likelihood of their gathered potential digital evidence being accepted and understood. However, in our paper, as mentioned earlier, we present the case for establishing a step-by-step framework in an attempt to propose guidelines to enhance the process of presenting potential digital evidence in any legal proceedings.

Another effort by Ćosić et al [15] 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. Their paper then proposes an ontology of digital evidence as one of possible methods suitable as a solution for this problem. However, in the current paper, a framework is presented in an attempt to propose guidelines to enhance the process of potential digital evidence presentation in any legal proceedings.

More efforts by Kuntze et al [16] explores the legal requirements that digital evidence must meet as the basis for developing technical requirements for the design of digital systems. They propose an approach that could be used to develop digital devices and establish processes crafted for the purpose of creating digital evidence. They further suggest that the legal view be incorporated into digital device design in order to allow for the probative value required of the potential digital evidence produced by such devices. However, this paper focuses on establishing a framework that provides guidelines to enhance the presentation of potential digital evidence in any court of law.

Walker [17], in his paper, explains how digital forensics has impacted court decision and rulings regarding computer records. He further elaborates on the cleanliness of the digital evidence and how the court defines "computer records." However, in this paper, we proposed a framework that can assist law enforcement agencies, for example, in reasoning and identifying evidence relevant to support or refute a particular case presented in court.

There also exist other related works on issues related to digital evidence, but neither those nor the cited references in this paper have presented a step-by-step framework with guidelines to enhance the presentation of potential digital evidence in legal proceedings in the way that is introduced in this paper. However, we acknowledge the fact that the previous research works have offered useful insights toward the development of the framework in this paper. In the section that follows, we explain in more detail the proposed framework.

IV. The Proposed Framework for Enhancing Potential Digital Evidence Presentation

In this section of the paper, the authors present a detailed explanation of the proposed framework. Figure 1 shows the structure of the framework.

The framework consists of nine steps arranged from top to bottom and where the first step is to capture the potential digital evidence (unaltered potential digital evidence or exhibit). This is followed by identifying the source or origin of the potential digital evidence captured in the second step. Step three assesses and supplies proof and justification of the source or origin of the potential digital evidence captured.

The fourth step establishes the validity and reliability of the source or origin of the captured potential digital evidence while step five is used to establish the relationship of the captured potential digital evidence with the crime scene. The relationship between the captured potential digital evidence with other available evidence is introduced in step six while step seven identifies and clarifies any existing claims on the captured potential digital evidence. The justifications of availed claims on the captured potential digital evidence are presented in step eight. Finally, concluding assertions on the validity of the captured potential digital evidence to the crime committed are supplied in step nine.

Note that we refer to 'potential' digital evidence throughout the paper, since digital artefacts are only considered to be 'evidence' in the final phase of the digital forensic investigation process, namely the reporting phase. This also implies that, for the captured potential digital evidence to be considered as competent digital evidence [18], it must possess scientific validity grounded in scientific methods and procedures.

In the subsections that follow, the steps 1 to 9 as presented in the proposed framework shown in Figure 1, are further explained in more detail.

A. Capture the potential digital evidence (unaltered potential digital evidence or exhibit))

In the case of a digital crime, there exist different types of potential digital evidence that can be captured and presented in a court of law or any legal proceedings. Furthermore, the requirement for potential evidence presupposes that all forms of potential digital evidence should be considered. Such potential digital evidence may include, but are not limited to: log files, emails, images, video clips, electronic documents, back-up disks, portable computers, network traffic records, personnel records, access control systems and telephone records. However, before using any of such potential digital evidence to determine the truth of an issue, the investigator must be sure that such potential digital evidence has been captured.

Moreover, the admissibility of any of the captured potential digital evidence in any court or legal proceedings is further subject to examination and verification through existing forms of legal argument. However, having captured the potential digital evidence before any presentation is done can be a confidence booster to the digital forensic expert, especially on the inferences drawn from such potential digital evidence.

Although it is beyond the scope of this paper to further elaborate on the individual types of potential digital evidence that can be presented in court or any legal proceedings, future research will consider the possibility of developing a comprehensive taxonomy of such types of potential digital evidence.

B. Identify the source or origin of the potential digital evidence

It is important that investigators identify reliable sources or origin of each of the different types of potential digital evidence captured before making a presentation in court. The potential digital evidence sources may exist in different forms, for example, it can exist in primary or secondary form. Primary sources are usually first-hand sources, for example photographs captured using a digital camera, e-mail or recorded speeches, while secondary sources are second-hand sources and may include, for example, information distributed freely online or information on printed materials. However, a secondary source may also be a primary source depending on how it is used [19]. This is backed up by the fact that, "Primary" and "secondary" are relative terms and, therefore, sources can be judged as primary or secondary depending on their specific contexts and according to what they are used for [20].

Therefore, the digital forensic experts should be well versed with the exact type of evidence at hand and the exact source or origin, where such potential digital evidence was captured. Failure to identify the source of the potential digital evidence, for example, can make it hard for such potential digital evidence to be considered for inclusion in the legal argument.

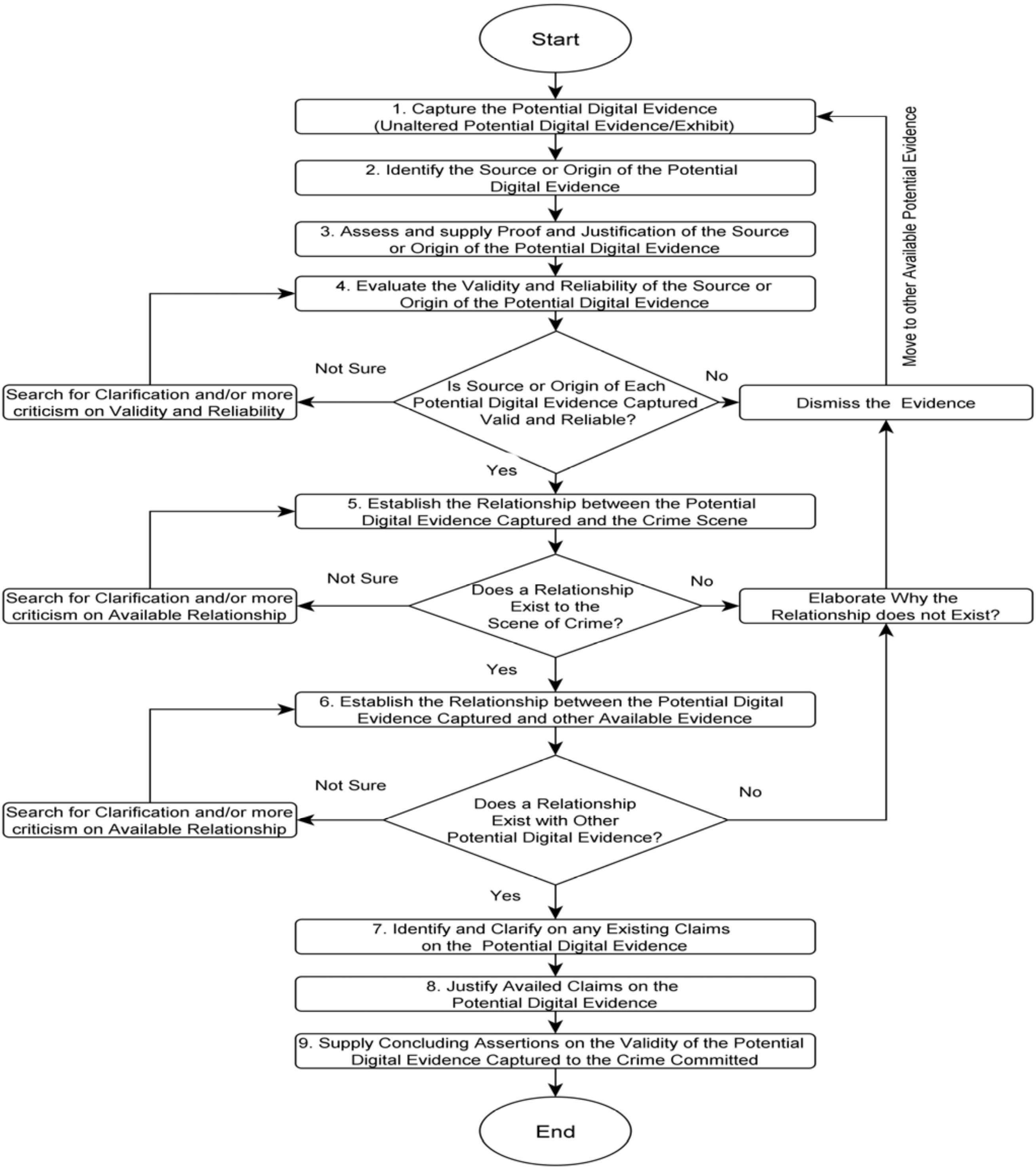
Start
1. Capture the Potential Digital Evidence (Unaltered Potential Digital Evidence/Exhibit)
2. Identify the Source or Origin of the Potential Digital Evidence
3. Assess and supply Proof and Justification of the Source or Origin of the Potential Digital Evidence
4. Evaluate the Validity and Reliability of the Source or Origin of the Potential Digital Evidence
Not Sure
Is Source or Origin of Each Potential Digital Evidence Captured Valid and Reliable?
No
Search for Clarification and/or more criticism on Validity and Reliability
Dismiss the Evidence
Move to other Available Potential Evidence
Yes
5. Establish the Relationship between the Potential Digital Evidence Captured and the Crime Scene
Not Sure
Does a Relationship Exist to the Scene of Crime?
No
Search for Clarification and/or more criticism on Available Relationship
Elaborate Why the Relationship does not Exist?
Yes
6. Establish the Relationship between the Potential Digital Evidence Captured and other Available Evidence
Not Sure
Does a Relationship Exist with Other Potential Digital Evidence?
No
Search for Clarification and/or more criticism on Available Relationship
Yes
7. Identify and Clarify on any Existing Claims on the Potential Digital Evidence
8. Justify Availed Claims on the Potential Digital Evidence
9. Supply Concluding Assertions on the Validity of the Potential Digital Evidence Captured to the Crime Committed
End

Figure 1. The framework for enhancing potential digital evidence presentation

C. Assess and supply proof and justification of the source or origin of the potential digital evidence

If a particular type of potential digital evidence (which becomes a court exhibit) is considered for inclusion in any legal argument, the proof and justification of its exact source or origin can be valuable. For example, the proof that there exist deleted emails in the victims' mail inbox, for example, can be used to infer the view that there was an attempt to conceal potential evidence. Moreover, this can also be used to justify a belief or a hypothesis that was formulated during the investigation period.

In the authors' opinion, however, when presenting the proof and justification of the source or origin of the potential digital evidence captured, the digital forensic experts should also indicate whether doing so is absolutely essential to the law enforcement requirements.

D. Evaluate the validity and reliability of the source or origin of the potential digital evidence

Evaluating the validity and reliability of the source or origin of the potential digital evidence captured, calls for criticism on the analysis and judgment of information source [21] in order to establish the admissibility of such potential digital evidence in court. It is possible that a given source of potential digital evidence can be viewed as more valid and/or reliable than another depending on the crime committed. However, any valid and reliable evidence sources must be substantial enough to support refute a hypothesis made during the investigation process. Therefore, in the authors' opinion, the evaluation process can be enhanced by using appropriate prompts as shown in step four of Figure 1.

Such a prompt as introduced in step four of Figure 1 is meant to evaluate the validity and reliability of the potential digital evidence source or origin. The prompt requires a response of 'Yes' (if the potential digital evidence source or origin is considered valid and reliable), 'No' (if the potential digital evidence source or origin is invalid and unreliable) or 'Not Sure', (suggesting a further search for clarification on the validity and reliability of the potential digital evidence source or origin). If the source is invalid and unreliable, the potential digital evidence is dismissed and the process is taken back to step one as shown in Figure 1 where another captured exhibit (unaltered potential digital evidence) is introduced. Moreover, if the investigator is not sure of the validity and reliability of the source or origin then a further search for clarification and/or criticism on the validity and reliability is done and the process is taken back to step four of Figure 1.

Note that the process of validating and/or searching for clarification on the validity and reliability of the potential digital evidence source or origin; demand the use of scientifically-proven methods. Such methods are beyond the scope of this paper; however, when used in digital forensics, they must be based on empirical and measurable evidence subject to specific scientific principles.

E. Establish the relationship between the potential digital evidence captured and the crime scene

Establishing the relationship of the potential digital evidence with the scene of crime often reveals relationships (or links) between the captured potential digital evidence and the crime committed. For example, the presence of a printed e-mail message in an office environment can be linked to using company resources to distributed unauthorized e-mail messages. Therefore, more prompts are introduced in this step (step five) to determine if a relationship does exist between the potential digital evidence and the scene of the crime. The prompt requires a response of 'Yes' (if a relationship does exist between the potential digital evidence and the scene of crime), 'No' (if a relationship does not exist between the potential digital evidence and the scene of crime) or 'Not Sure', (suggesting a further search for clarification and/or criticism on the availability of a relationship between the potential digital evidence and the scene of crime).

If a relationship does not exist between the potential digital evidence and the scene of the crime, the digital forensic expert then has to elaborate on why there exists no relationship. For example, if there exist traces of using the company printer to print an e-mail message and that the e-mail message was found present in the inbox of the suspect, then a link can be established to show that the suspect did print the message, otherwise not. If such a link does not exist, then the potential digital evidence is dismissed and the process goes back to step one where a new exhibit is introduced, as shown in Figure 1.

F. Establish the relationship between the potential digital evidence captured and other available evidence

Step six of Figure 1 is meant to establish relationships between any captured potential evidence with other available digital evidence. As with step four and five, step six also has a prompt to determine if a relationship does exist between any of the captured potential digital evidence with other available evidence. The prompt also requires a response of 'Yes' (if a relationship does exist between the capture potential digital evidence with other available evidence), 'No' (if a relationship does not exist between the captured potential digital evidence and other available evidence) or 'Not Sure', (suggesting a further search for clarification and/or criticism on the availability of a relationship between the captured potential digital evidence and other available evidence).

Note that, for steps four, five and six, if the process continues to be inconclusive, for example, a decision to terminate such a process is required. The digital forensic expert, therefore, can decide whether to retain or dismiss the potential digital evidence captured during the investigation process. This, however, can be based on the weight, validity, reliability and the inferences drawn from the potential digital evidence itself.

G. Identify and clarify on any existing claims on the potential digital evidence

In step seven, it is possible that an individual (the suspect, victim, witness, lawyer etc.) can lay a claim with respect to the potential digital evidence captured and/or presented in court. For example, a suspect can claim that the potential evidence presented did not originate from his computer. However, such a claim may primarily be used as a way to escape criminal guilt. Early identification of such claims by the digital forensic expert and further clarification on them, on the contrary, can improve court outcomes. This can also minimise or alleviate any discriminatory (unfair or prejudicial) outcomes. For example, the existence of duplicate pornographic pictures (if assumed that pornographic images was illegal in the particular case) in the suspects' computer and mobile phone can be used to clarify if there was transfer of such pictures from the computer to the phone or vice versa. However, this may require solid investigation findings with the main aim being to refute or support any such claims made.

Moreover, investigators should also clarify whether, and if so, the extent to which (where necessary), the claims made and their interpretations have been misconstrued in any way.

H. Justify availed claims on the potential digital evidence

If any individual raises a claim during any legal proceedings, such claim can either be supported or dismissed. However, whether supported or dismissed, the digital forensic expert has to justify that the support or dismissal of the claims was a fair one, i.e. that there were fair grounds for the support or dismissal of the claims and that fair procedures were followed. This forms step eight of the proposed framework.

In the case of supporting an existing claim, the digital forensic expert might be required to further show that the support is as a result of an existing relationship (link) between one or more of the potential digital evidence artifacts captured during the investigation process. For example, the expert can support or refute the claim that the evidence did not originate from the suspect computer based on existing links to the crime committed.

I. Supply concluding assertions on the validity of the potential digital evidence captured to the crime committed

Finally, the ninth and the last step in this framework present concluding assertions on the validity and reliability of the potential digital evidence captured and presented in relation to the crime committed. This may also include rendering the digital evidence invalid and unreliable based on the estimated weight, validity, reliability and the inferences made from such potential digital evidence during the investigation and presentation process. For example, the existence of an internet connection, e.g. a modem or router, and a laptop can be used to infer the fact that the suspect used these devices to browse pornographic sites and distributing unsolicited mails.

In the next section of this paper, we present a critical evaluation of our proposed framework.

V. Critical Evaluataion of the Proposed Framework

The proposed framework in this paper is a new contribution in the digital forensics domain. The scope of the framework is defined by the steps and guidelines of the potential digital evidence presentation as seen Figure 1. The main steps as depicted in the framework include:

- Capture the potential digital evidence (unaltered potential digital evidence or exhibit)
- Identify the source or origin of the potential digital evidence
- Assess and supply proof and justification of the source or origin of the potential digital evidence
- Evaluate the validity and reliability of the source or origin of the potential digital evidence
- Establish the relationship between the potential digital evidence captured and the crime scene
- Establish the relationship between the potential digital evidence captured and other available evidence
- Identify and clarify on any existing claims on the potential digital evidence
- Justify availed claims on the potential digital evidence
- Supply concluding assertions on the validity of the potential digital evidence captured to the crime committed

The specific details of the individual steps as identified in the framework have further been explained in this paper. However, note that the steps as identified in Figure 1 are meant to facilitate this study and primarily focus on potential digital evidence presentation in legal proceedings. Such proposed steps or guidelines are by no means the final guaranteed steps to potential digital evidence admissibility in court. In the authors' opinion, however, organising the framework into steps (high-level guidelines) was necessary to simplify the understanding of the framework as well as to present specific finer details of the framework.

The proposed framework in this paper can be used in the digital forensics domain, for example, to help investigators in structuring investigation findings as well as in identifying relevant patterns of events to be incorporated during the presentation and interpretation of potential digital evidence. Moreover, the framework can also be helpful to law enforcement agencies and other stakeholders, for example, in reasoning and identifying potential digital evidence relevant to support or refute a particular criminal case presented in court.

For the case of digital evidence admissibility in legal proceedings, the steps as identified in the framework can be used, for example, to evaluate the validity, reliability and weight of the potential digital evidence presented in court. Such steps will also ensure that investigators conduct the digital forensic investigation process thoroughly before doing a final presentation of potential digital evidence. In addition, the framework can also be used for training investigators, especially on the art of presenting potential digital evidence in court.

Academic institutions should also find the framework in this paper constructive, especially when training students on how to present digital forensic evidence in any legal proceedings. Moreover, such a framework can also be used when developing curriculums and education materials for different programs of study within the field of digital forensics. Such programs will, for example, ensure that institutions produce well-enabled digital forensic specialists (investigators) capable of properly handling the presentation of potential digital evidence in legal proceedings.

Developers of digital forensics tools can also use the proposed framework to develop automated potential digital evidence presentation and interpretations tools. This also implies that developers might find the framework in this paper useful, especially when considering the development of new digital forensic tools and techniques for addressing potential digital evidence presentation and interpretation including potential digital evidence visualisation in legal proceedings.

Finally, the framework presented in this paper has been designed in such a way as to accommodate new steps that may emerge as a result of jurisdictional legal requirements or domain evolution. 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 research domain.

VI. Conclusion and Future Work

The problem addressed in this paper was that of the lack of methodologies and specifications typically designed to enhance potential digital evidence presentation and interpretation in a court of law. This is backed up by the fact that there are currently no standardised guidelines for even presenting the most common representations of potential digital forensic evidence. A framework was then proposed in an attempt to provide guidelines for enhancing the presentation and interpretation of potential digital evidence in any legal proceedings. The requirement of such a framework in digital forensics is exceptionally important to any digital forensic expert, especially during potential digital evidence presentation. With such a framework, investigators will, for example, be able to structure investigation findings as well as identify relevant patterns of events to be incorporated during the presentation and interpretation of potential digital evidence in court. Moreover, the framework can also help law enforcement agencies, for example, to differentiate between experts' own opinions and from what the potential digital evidence really portrays. The ability to differentiate opinions from the real evidence presented in court can assist the jury in evaluating opinions that substantially outweighs prejudicial effect.

Finally, the authors believe that by using such a framework, better presentation and interpretation of potential digital evidence in any legal proceedings can be attained. However, more research needs to be conducted in order to improve on the proposed framework in this paper. The framework should also spark further discussion on the development of new techniques to support potential digital evidence presentation and interpretation in any court of law.

Acknowledgement

This work is based on the research supported in part by the National Research Foundation of South Africa (Grant specific unique reference number (UID) 85794). The Grant holder acknowledges that opinions, findings and conclusion or recommendations expressed in any publication generated by NRF supported research are that of the author(s), and that the NRF accepts no liability whatsoever in this regard.

References

[1] Arnold, E., and Soriano, E., (2013).The Recent Evolution of Expert Evidence in Selected Common Law Jurisdictions Around the World. A commissioned study for the Canadian Institute of Chartered Business Valuators.

[2] Roberts, J.L, and Suits, C., (2013). Admissibility of digital image data: concerns in the courtroom. Available at: http://libraries.maine.edu/Spatial/gisweb/spatdb/acsm95/ac95071.html [Accessed April 10, 2013].

[3] Boddington, R., Hobbs, V., and Mann, G., (2008).Validating Digital Evidence for Legal Argument . In the Proceedings of the 6th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia.

[4] Cohen, F., (2011). Digital Forensic Evidence Examination, 3RD Edition. Published by fred cohen & Associates. ISBN # 1-878109-46-4.

[5] Hoss, A.M. and Corver, D.L., (2009). Weaving Ontologies to Support Digital Forensic Analysis. ISI 2009, Richardson, TX, USA.

[6] Resendez, I., Martinez, P., and Abraham, J., (2012). An introduction to digital forensics. Available at: http://acetweb.org/journal/ACETJournal_Vol6/An%20Introduction%20to%20Digital%20Forensics.pdf [Accessed 04 September 2012].

[7] Khatir, M.; Hejazi, S.M.; Sneiders, E., (2008). Two-Dimensional Evidence Reliability Amplification Process Model for Digital Forensics. Digital Forensics and Incident Analysis, 2008. WDFIA '08. Third International Annual Workshop on Digital Forensics and Incident Analysis. pp.21-29.

[8] Palmer, G., (2002). Forensic Analysis in the Digital World. International Journal of Digital Evidence, Vol. 1, No. 1

[9] Newsom, P.D., (2006). Computer Forensics – Overcoming the "after-the-fact" approach. Available at: http://d0mber.wordpress.com/tag/cloud-security/ [Accessed April 11, 2013].

[10] Yusoff, Y., Ismail, R. and Hassan, Z., (2011). Common Phases of Computer Forensics Investigation Models. International Journal of Computer Science & Information Technology (IJCSIT), Vol. 3, No. 3.

[11] Carrier, B.D., (2006). Digital Investigation and Digital Forensic Basics. Available at: http://www.digital-evidence.org/di_basics.html [Accessed March 28, 2013].

[12] Valjarevic, A., and Venter, H.S., (2012). Harmonised Digital Forensic Investigation Process Model. In the Proceedings of the Information Security for South Africa (ISSA) . pp.1-10.

[13] Boddington, R., Hobbs, V., and Mann, G., (2008). Validating digital evidence for legal argument. In the Proceedings of the 6th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia.

[14] Sherman, S., (2006). A digital forensic practitioner's guide to giving evidence in a court of law. In the Proceedings of the 4th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia.

[15] Ćosić, J. and Ćosić, Z. (2012). The Necessity of Developing a Digital Evidence Ontology. In the proceedings of the Central European Conference on Information and Intelligent Systems. pp. 325-330, Varaždin, Croatia.

[16] Kuntze. N., Rudolph, C., Alva, A., Popovsky, B.E., Christiansen, J., and Kemmerich, T., (2012). On The Creation Of Reliable Digital Evidence. Available at: http://sit.sit.fraunhofer.de/smv/publications/download/IFIPFor2012.pdf [Accessed March 28, 2013].

[17] Walker, C., (2006). Computer Forensics: Bringing the Evidence to Court. Available at: http://www.infosecwriters.com/text_resources/pdf/Computer_Forensics_to_Court.pdf [Accessed March 28, 2013].

[18] Ryan, D.J., and Shpantzer, G., (2005). Legal Aspects of Digital Forensics. Available at: http://euro.ecom.cmu.edu/program/law/08-732/Evidence/RyanShpantzer.pdf [Accessed April 1, 2013].

[19] Ithaca College Library, (2013). Primary and secondary sources. Available at: http://www.ithacalibrary.com/sp/subjects/primary [Accessed April 1, 2013].

[20] Helge, K., (1989). An Introduction to the Historiography of Science. Cambridge University Press. p. 121. ISBN 0-521-38921-6.

[21] Pierce, R., (2007). Evaluating Information: Validity, Reliability, Accuracy, Triangulation. pp. 79-99. Available at: http://www.sagepub.com/upm-data/17810_5052_Pierce_Ch07.pdf [Accessed April 1, 2013].