A Generic Framework for Enhancing the Quality of Digital Evidence Reports

[1,2]Nickson M. Karie*, [1]Hein S. Venter†
[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
menza06@hotmail.com*
hventer@cs.up.ac.za†

Abstract: In recent times, the admissibility of potential digital evidence in any court of law is coming under increased scrutiny. This is aggravated by the fact that, the complexity of digital evidence is also increasing on a daily basis. Thus, convincing the court that the evidence presented is worthy of inclusion into any criminal process, the digital forensic experts require extensive technical knowledge and skills, including methodologies and specifications typically designed for producing quality digital evidence reports. This also implies that, the techniques, knowledge and skills used by the digital forensic experts during the preparation of digital evidence reports, should have the ability to convince the court on the validity, reliability and weight of the evidence captured during the investigation process. The methodologies used should also be able to assist the law enforcement agencies determine, with less effort, the admissibility of the digital evidence being reported. As of the time of this study, however, there exists a lack of a standardised or harmonised framework that have specifically been designed to help in the process of preparing quality digital evidence reports after an investigation has been conducted. This has, therefore, resulted in disparities on how digital evidence reports are prepared and presented in any court of law or civil proceedings. To address this disparity problem, a unified process equipped guidelines that meets some specified minimum requirements on how digital evidence reports should be prepared would be worthwhile. This paper, therefore, presents a step-by-step framework in an attempt to propose high-level guidelines that can be adapted to enhance the process of preparing digital evidence reports. The use of such a framework, for example, can be a stepping stone towards a harmonised process on how to prepare digital evidence reports for use in court or legal proceedings. Besides, such a framework can also assist the law enforcement agencies, for example, to determine, with less effort, the reliability, validity, weight and admissibility of any digital evidence included in the final reports.

Keywords: Digital forensics, methodologies, digital evidence reports, framework, high-level guidelines, harmonised process.

1. Introduction

The use of different types of digital evidence in court systems has increased in the past few decades. The complexity of digital evidence is also increasing on a daily basis. In the case of a digital forensic investigation process, for example, the different types of digital evidence that can be captured includes among others information on desktop computers, laptops, server, mobile phones, audio files, video recordings, emails, web logs, digital images, short message services and voice conversations. Convincing the court that any of such digital evidence captured is worthy of inclusion into the criminal process, the digital forensic experts require extensive technical knowledge and skills, including methodologies and specifications typically designed to help them prepare quality digital evidence reports for use in court.

Besides, as digital crimes continue to increase and overwhelm digital forensic investigators and crime laboratories, law enforcement agencies also need a sure way to determine the validity, weight and admissibility of any digital evidence presented in court. For this reason, standardised methodologies and specifications need to be developed in digital forensics to assist the law enforcement agencies determine, with less effort, the validity, weight and admissibility of any digital evidence reported.

As of the time of this study, however, there exists a lack of standardised or harmonised digital forensic processes that have specifically been designed to help in preparing quality digital evidence reports for use in court. This has, therefore, resulted in disparities on how digital evidence reports are prepared and presented to different stakeholders, more specifically, after a digital forensic investigation process has been conducted.

The proposed framework in this paper is, thus, an attempt towards proposing high-level guidelines that can help enhance the process of preparing quality digital evidence reports for use in any legal proceedings. Furthermore, the requirement for 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 (Cohen, 2011). Such methodologies will also assist law enforcement agencies, for example, in differentiating between experts' own opinions from the actual depiction of the digital evidence (Karie and Venter 2013). The framework can also be useful to the digital forensic experts, for example, in drawing inferences from the digital evidence itself. Finally, this paper is meant to spark discussions and further research on an international agreed framework to enhance the process of preparing quality digital evidence reports for use in legal proceedings.

The remaining part of this paper is organised as follows: section 2 presents background concepts while section 3 handles previous related work. A detailed explanation of the proposed framework is handled in section 4 followed by a critical evaluation of the framework in section 5. Finally, conclusion and future work is given in section 6.

2. Background

According to Casey (2004), digital evidence is any probative information stored or transmitted in digital form that can be used at a trial in any court of law. Various digital forensic tools and techniques are normally used by investigators to capture data from computer systems and other digital devices in an attempt to identify potential digital evidence that can provide conclusive descriptions of the activities that took place. Nonetheless, before accepting any of the captured digital evidence, the court has to determine if such evidence is relevant, authentic, hearsay and whether a copy is acceptable or the original is required (Casey, 2004).

As stated by Sherman (2006), 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 skilled the investigator has been at recovering it, if the digital evidence reports are not presented in a coherent and understandable way to the court, the case may be lost. For this reason, in the case of a digital forensic investigation process, the presentation of digital evidence reports become one critical phase to any digital forensic investigator. This is because; it is in this phase where information about the results and findings of the investigation process has to be reported to the relevant stakeholders (Sherman, 2006).

Nevertheless, in presenting the final digital evidence reports investigators are more often than not challenged by the fact that there is currently a lack of standardised guidelines that one must adhere to when preparing digital evidence reports. Poorly prepared digital evidence reports can, for example, make it hard to convince the court that the defendant is guilty of the crime he or she is accused of (Karie and Venter, 2013).

Despite the advances in digital forensics, legal professionals and researchers are yet to resolve the challenges associated with digital evidence reports presented in court. Existing methodologies and specifications have not addressed this problem fully with the result being that, individuals might be denied justice due to lack of guidelines for preparing quality digital evidence reports for use in legal proceedings (Karie and Venter, 2013). Thus, methodologies need to be developed in digital forensics to address the challenges and disparities associated with digital evidence reports prepared for use in any court of law or legal proceedings. In the next section, we examine existing related work in digital forensics.

3. Related Work

There exists various research works from different digital forensic researchers which have made valuable contributions towards the proposed framework 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, Hamda et al. (2011) states that, due to the lack of standards in reporting digital evidence items, investigators often face difficulties in efficiently presenting investigation findings. Thus, they propose in their paper a standard for digital evidence to be used in reports that are generated using digital forensic tools. Based on the investigation findings, the standard for digital evidence reports can include items such as data about the case, the evidence source, evidence item, and the chain of custody. However, in the current paper we focus on presenting high-level guidelines that can be used to enhance the process of preparing quality digital evidence reports for use in court.

In another effort by Boddington et al (2008) they argue 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. Their paper, though, does not discuss any specific steps to be followed when preparing final digital evidence reports for use in legal proceedings.

Another effort by Karie and Venter (2013) presents a framework in an attempt to propose high-level guidelines for enhancing the presentation of potential digital evidence in any legal proceedings. Such a framework can be useful to the 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 digital evidence in court. The framework can also assist law enforcement agencies; for example, determine with less effort, the validity, weight and admissibility of any potential digital evidence presented in court. However, the framework focusses more on the presentation phase and does not discuss any specific guidelines to be used when preparing digital evidence reports after a digital investigation process has been conducted, which is the focus of this paper.

There also exist other related works on issues related to digital evidence and evidence reporting but neither those nor the cited references in this paper have presented a step-by-step framework with guidelines to enhance the process of preparing quality digital evidence reports for use in any court of law or 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.

4. The Proposed Framework

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 seven proposed steps which can be adapted to enhance the quality of digital evidence reports. The steps are arranged from top to bottom where the first step is to carefully analyse the digital evidence captured. This is followed by establishing the source of each captured item of the digital evidence in the second step. The third step provides detailed descriptions of each captured item of the digital evidence. The fourth step uses the descriptions of each captured item of the digital evidence to establish any existing links to the suspected attacker or targeted victim. Step five establishes the intentions of the attacker to the targeted victims based on the descriptions of the captured digital evidence. Elaborating on the effects of the attack to the targeted victims is presented in step six of the framework. Finally, concluding assertions are supplied in step seven.

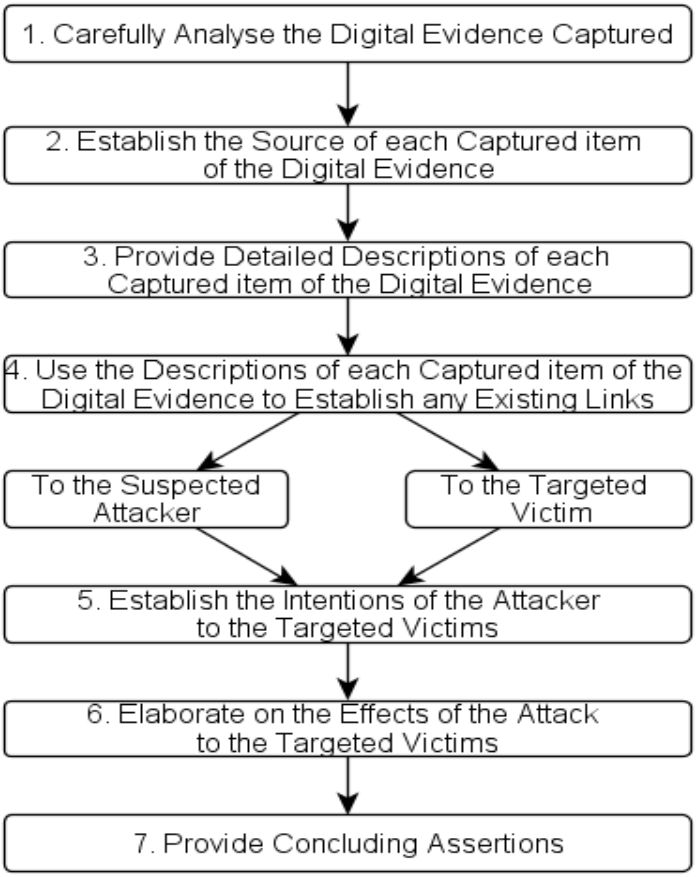

Figure 1: A framework for enhancing the quality of digital evidence reports

Note that all the steps proposed in the framework shown in Figure 1 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. In the sub-sections to follow, the steps 1 to 7 as shown in Figure 1 are explained in more detail.

4.1 Carefully Analyse the Digital Evidence Captured

In writing the final digital evidence report, investigators must first carefully analyse the different types of digital evidence captured during the investigation process. The digital evidence may include among others types; audio files, video recordings, emails, web logs, digital images, short message services and voice conversations. Because of the sheer magnitude of the different types of digital evidence that can be captured, investigators should only concentrate on analysing evidence that is relevant to the case at hand. This helps the investigators in managing the evidence information to be included in the final report.

Besides, before using any of the captured digital evidence in the final report to determine the truth of an issue, the investigator must be sure that such digital evidence has been captured and carefully analysed. Having analysed the different types of evidence before compiling the final report can be a confidence booster to the digital forensic expert, especially on the inferences drawn from such digital evidence (Karie and Venter, 2013). Evidence analysis makes it easier to establish the source of each captured item of digital evidence, which forms step two of this framework.

Note that the process of capturing any digital evidence demands the use of scientifically-proven methods. As mentioned earlier, such methods are not discussed this paper, but, when used in digital forensics, they must be based on empirical and measurable standards subject to specific scientific principles.

4.2 Establish the Source of each Captured item of the Digital Evidence

With the advances in digital technology, the sources of digital evidence have also grown exponentially. It is, therefore, important that investigators establish reliable sources for each of the different types of digital evidence captured during the investigation process before compiling the final reports. Failure to establish reliable sources of the captured digital evidence, for example, can make it hard for such evidence to be considered for inclusion in the final report.

Having multiple reliable sources of the same digital evidence, for example, can be used to establish the continuity of the offense as well as any existing links to related digital evidence. This is useful especially, when more than one digital system has been used in committing the offense. As stated by Casey, (2012), the more corroborating evidence that investigators can capture, the more certainty they can have in their final conclusions. Thus, having unreliable evidence sources can potentially be more damaging than having no sources.

All relevant and reliable evidence sources should, hence, be established and considered in the final digital evidence report. This will particularly allow multiple sources of evidence to be analysed as well as ensure the suitability of including such digital evidence in the report

4.3 Provide Detailed Descriptions of each Captured Digital Evidence

In the case of a digital forensic investigation process, many of the different types of evidence captured are entirely in digital form. Providing detailed descriptions of each of the captured evidence can be worthwhile. Such descriptions could further be used in supporting the prosecution of different types of digital crimes.

However, in describing the digital evidence captured in the final report, the investigators may also be required to explain the process used to analyse the digital evidence itself. This is important especially when trying to establish the authenticity of the evidence. To be sure that each item of the digital evidence incorporated in the final report is explained, investigators can create a checklist that identifies all the digital evidence items considered in the report.

4.4 Use the Descriptions of the Captured Digital Evidence to Establish any Existing Links

Establishing any existing links between captured digital evidence can reveal the relationships between such digital evidence to the suspected attacker or targeted victim as shown in step four of Figure 1. Based on the crime committed it is possible that some of the digital evidence captured may have little or no links to either the suspected attacker or the targeted victim. This, however, can be based on the weight, validity, reliability and the inferences drawn from the potential digital evidence itself as described in step three of Figure 1.

4.5 Establish the Intentions of the Attacker to the Targeted Victims

Discovering the intention behind the digital attack can lead to discovering the different ways in which the attack was done. Different evidence captured can, thus, be used to prove the attacker's intention, for example, compromising the confidentiality, integrity, or availability of the victim's data among others. Trying to figure out what the attacker's intention is can also help in establishing the effects of the attack. For this reason, based on the captured and analysed digital evidence, the investigator should, if possible, state clearly in the final report the intentions of the attacker to the targeted victims and the effects there after. Step six of Figure 1 discussed next is, therefore, proposed in the framework to help elaborate on the effects of the attack to the targeted victims.

4.6 Elaborate on the Effects of the Attack to the Targeted Victims

Many of the perpetrators of digital crimes usually targets particular victims or services hosted by the victims. Different types of attacks may also have different impacts or effects on the targeted victims. It is, therefore, essential that digital forensic investigators elaborate, in the final evidence reports, the impacts or effects of the attack to the targeted victim. Such explanation can assist the court in drawing reasonable inference that can as well help in reasoning and identifying digital evidence relevant to support or refute a particular criminal case in court.

In the case of supporting an existing case in court, the digital forensic expert might as well be required to further show in their final report that the support is as a result of an existing relationship (link) between one, two or more of the potential digital evidence artifacts captured during the investigation process. Although when elaborating on the effects of the attack to the targeted victim, the digital forensic experts should also indicate whether including all the details of the findings that support or refute a particular criminal case in the final report are absolutely necessary to the law enforcement requirements (Karie and Venter, 2013).

4.7 Provide Concluding Assertions

Finally, the seventh and the last step of the proposed framework provide concluding assertions. This means that the final report should include any important details from each of the steps as shown in Figure 1. The reference protocols followed and the methods used, to seize, document, collect, preserve, recover, reconstruct, organize and search for any key digital evidence may also need to be elaborated (Casey, 2004) as concluding assertions. Step seven may also include supporting or refuting some of the captured digital evidence in the final report. However, the support or refusal of any digital evidence should be based on the estimated weight, validity, reliability and the inferences made from such digital evidence during the analysis process. The next section, presents a critical evaluation of the framework proposed in this paper.

5. Critical Evaluation 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 as shown in Figure 1. The main steps as depicted in the framework include:

- Carefully Analyse the Digital Evidence Captured
- Establish the Source of each Captured item of the Digital Evidence
- Provide Detailed Descriptions of each Captured item of the Digital Evidence
- Use the Descriptions of each Captured item of the Digital Evidence to Establish any Existing Links
- Establish the Intentions of the Attacker to the Targeted Victims
- Elaborate on the Effects of the Attack to the Targeted Victims
- Provide Concluding Assertions

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 enhancing the process of preparing quality digital evidence reports for use in any court of law or legal proceedings. Such proposed steps or guidelines are by no means the final guaranteed steps to digital evidence reports admissibility in court. Nevertheless, organising the framework into steps was necessary to simplify the understanding of the framework.

Some of the problems that led to the introduction of this new framework in this paper include:

- Lack of a common legal basis in preparing digital evidence reports: The lack of a common legal basis for preparing quality reports can easily render digital evidence reports inadmissible

in court. For this reason, having a common legal basis for preparing digital evidence reports can help digital forensic investigators focus on the key issues to be included in the final evidence reports to be presented at trials.

- Lack of a standardised or harmonised procedure for preparing digital evidence reports: Standardising procedures for preparing digital evidence reports after a digital investigation process has been conducted can reduce the time taken by investigators to prepare court admissible reports. This is backed up by the fact that investigators will only concentrate on evidence that relates to the case at hand while forgetting the rest. The framework in this paper, therefore, is a step towards a harmonised process for preparing quality digital evidence reports.
- Reliability/trustworthiness of digital evidence reports: It is not always obvious that the reliability of digital evidence will be acceptable in court; however, the use of a harmonised framework, for example, can be a positive step towards producing acceptable level of trustworthiness and reliability in digital evidence reports. The reliability can also be questionable if the data included in the final reports are not accurate and trustworthy. Therefore, the use of common and/or standardised frameworks to prepare digital evidence reports can help raise the level of reliability and/or trustworthiness of digital evidence reports.

The proposed Framework as demonstrated in this paper can, thus, be used in the digital forensics domain, for example, to help investigators in preparing quality digital evidence reports as well as in identifying relevant digital evidence to be incorporated in the final digital evidence reports. The framework can also be helpful to law enforcement agencies and other stakeholders, for example, in reasoning and identifying 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 shown in Figure 1 can also be useful, for example, in evaluating the validity, reliability and weight of the digital evidence included in the final report. The framework can, further, be used for training investigators, especially on the art of digital evidence report writing for use in any court of law or civil proceedings.

Academic institutions should also find the framework in this paper constructive, especially when training students on how to write quality digital evidence reports for use in legal proceedings. Such a framework can assist in 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 capable of writing high quality digital evidence reports.

Developers of digital forensics tools can also use the proposed framework to develop automated digital evidence reporting 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 the disparities experienced during the preparation of digital evidence reports for use in legal proceedings.

6. conclusion

The problem addressed in this paper was that of the lack of a standardised or harmonised process specifically designed to help investigators in preparing quality digital evidence reports for use in any court of law or legal proceedings. This is backed up by the fact that there is currently a lack of standardised guidelines that investigators should adhere to when preparing final digital forensic evidence reports. This scenarion has brought about disparities in the process followed when preparing digital evidence reports.

A framework is then proposed in this paper in an attempt to provide high level guidelines for enhancing the process of preparing quality digital evidence reports for use in legal proceedings. The requirement of such a framework in digital forensics is exceptionally important to digital forensic investigators, especially during the preparation of final digital evidence reports. Such a framework can also assist the law enforcement agencies, for example, to determine, with less effort, the validity, weight and admissibility of digital evidence incorporated in the report.

Moreover, the framework can also help law enforcement agencies, for example, to differentiate between experts' own opinions from what the digital evidence really portrays. The ability to differentiate opinions from the real digital evidence presented can as well assist the court in evaluating opinions that substantially outweighs prejudicial effect. Again, the framework can be useful in determining the most relevant and appropriate digital evidence to be included in digital evidence reports.

Finally, the authors believe that by using such a framework, quality reports of digital evidence in any court or legal proceedings can be attained. Other future relevant undertakings in the digital forensics domain might as well benefit from applying such a framework as the one proposed in this paper. 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 methodologies and techniques to enhance the process of preparing quality digital evidence reports for use in any court of law or legal proceedings.

References

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

Casey, E. (2012). Error, Uncertainty, and Loss in Digital Evidence. International Journal of Digital Evidence. Vol. 1, No. 2.

Casey, E.(2004). Digital Evidence and Computer Crime, Second Edition. Published by Elsevier. ISBN 0-12-163104-4

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

Hamda, B., Mariam H., and Ibrahim, B., (2011). Defining a Standard for Reporting Digital Evidence Items in Computer Forensic Tools. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering Vol. 53, pp78-95

Karie, N.M. and Venter, H.S., (2013). Towards a Framework for Enhancing Potential Digital Evidence Presentation. In the Proceedings of the 13th Annual Information Security for South Africa Conference, (ISSA-2013). Johannesburg, South Africa. Published online by IEEE Xplore®.

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.