Impact of Using Unreliable Digital Forensic Tools

Precilla M. Dimpe and Okuthe P. Kogeda, *Member, IAENG*

***Abstract*— digital forensic tools are used to unravel criminal acts and prove crime in the court of law. However, the area, task and/or functions digital forensic tools are being applied in may not be suitable hence leading to unreliable results by these tools. In many cases, forensic experts may apply a particular tool not because it is the most effective tool but because it is available, cheap and the expert is familiar with it. This has often led to use of unreliable digital forensic tools, which may yield unreliable results. Unreliable results may jeopardize the whole forensic investigation process and in some cases lead to criminals walking free thereby being bolded to commit the same crime again. This may also lead to time wasting, trial and error, loss of money, etc. In this paper therefore, we quantify the impact of using unreliable digital forensic tools. We analyzed, aggregated, and classified data obtained from Hackmageddon [1] using Bayesian network model. There is a direct link of using unreliable forensic tools to the increase in cyber-crimes. The impact is in billions of dollars lost because of committed crimes with a focus of 5% increase every year.**

***Index Terms*— Cybercrime, digital forensic, Bayesian networks, unreliable forensic tools**

I. Introduction

The technological evolution, proliferation of mobile devices and increased mobile-commerce transactions has led to increased cases of cybercrime. Technological advancements have always been used to the advantage of the criminal fraternity [2, 30]. To keep up with the fast pace growing technology a number of digital forensic tools were developed to help forensic investigators to investigate and apprehend cybercriminals. Some of the tools were developed with the forensic process in mind while others were designed to meet the needs of a particular interest group but lacked designs that were created with forensic science needs [11] and as a result, some tools produce unreliable evidence. Forensic investigators make use of tools (both hardware and software) to investigate cybercrime, the results produced by the tools are used in the court of law to make judgment and in order for the evidence to be accepted, it needs to be reliable, therefore, a reliable tool needs to be used in order to produce reliable results because the trustworthiness of digital evidence is of vital importance given the forensic context of the case [4]. Digital forensics is concerned with the investigation of any suspected crime or misbehavior that may be manifested by digital evidence [14]. It is one of the sciences that have been used to investigate and apprehend cyber criminals; hence the issue of reliability concerning digital forensic tools is very critical because the results produced by the tools are used in the court of law to convict criminals or to prove innocence. Unreliable digital forensic tools will lead to unreliable results and since digital evidence is used to make judgments in courts, if it produces unreliable results, that will have a negative effects on parties in terms of faulty criminal convictions, improper civil judgment, lost opportunity [5] and a forensic investigator risks loss of integrity if doubt can be introduced into the accuracy of tools.

The purpose of this paper is to model the impact of using unreliable digital forensic tools, with the aim of raising awareness on how the use of unreliable tools contribute to losses (i.e., money, time, consumables, etc.) and affects the economy. Before modeling the likelihood impact, we start by first looking at requirements that needs to be considered in the evaluation process, define software reliability and come up with ways to measure it. We make use of a Bayesian Network to model the likelihood impact of the use of unreliable digital forensic tools.

The remainder of this paper is organized as follows: In Section II, we present related work. In Section III, we present digital forensic requirements. In Section IV, we present design and implementation. In Section V, we present testing and results and lastly, conclusion and future work are presented in Section VII.

II. Related Work

Buskirk and Liu [5] challenged the presumption of reliability of digital evidence by presenting and discussing important legal and technical issues involved in the effort to ensure the reliability of forensic software and the accuracy of digital evidence. Their argument was based on courts presuming that forensic software reliably produces accurate results, by outlining that the presumption of reliability is economically inefficient because it fails to force developers to internalize cost. If developers spent more time testing, major errors could certainly be reduced without great cost because the effect caused by software faults among parties is far larger than the costs of research and development required in preventing such effects. Their approach to the problem was through the proper application of scientific jurisprudence and through combination of certain broad market and social corrections. Though their approach does not result in error-free digital evidence, it does however, result in how the law can be used to inject efficiency into a

Manuscript received June 23, 2017; revised August 14, 2017. This work was supported in part by the National Research Foundation (NRF), South Africa.

Precilla M. Dimpe is with Tshwane University of Technology, department of Communication networks, Private Bag X680, Pretoria 0001, South Africa (Phone: +2712382-9640; e-mail: precilladimpe@gmail.com).

Okuthe P. Kogeda is with Department of Computer Science, ICT Faculty, Tshwane University of Technology, Private Bag X680, Pretoria 0001, South Africa (kogedaPO@tut.ac.za).

system of justice by properly following the Daubert principles and policy makers implementing appropriate market and social corrections. Though Buskirk and Liu [5] outlined that the effect caused by software faults is larger than the costs of research and development required for preventing such effects, however, there are no figures in their work to support their argument. In this paper, we model the effects in terms of figures (monetary value) and make use of a mind map to show how an unreliable tool, which leads to unreliable evidence, affects the economy.

Casey [8] explored the uncertainties in network related evidence that can be combined by data corruption, loss, tampering, or errors in interpretation and analysis. His aim was to provide a basis of helping forensic investigators in implementing the scientific methods by detecting, quantifying and compensating for errors and loss in evidence collected from networked systems. In an attempt to minimize the problem the author came up with a method of estimating uncertainty, wherein the author provided a chart that estimated certainty from the lowest level of certainty (uncertainty) to the highest level of certainty. The author claimed that his method allows investigators, attorneys, judges, and jurors who do not have a deep technical understanding of network technology to assess the reliability of a given piece of digital evidence. In addition to developing a method for measuring uncertainty, the author also describes some potential sources of errors and quantified the percentage of lost datagram, stating that although it may not be possible to conclude the content of lost datagrams, it is useful to quantify the percentage loss. Even though Casey's [8] method is promising, it only focuses on uncertainties in digital evidence that are caused by lost data on the network and errors in log files (log corruption and tampering). It does not consider uncertainties that may be caused by the tools that are used to produce the evidence, while this work focuses on the reliability of the tools that are used to produce evidence, if wheatear or not the tool is reliable and how can reliability be measured in a software tool.

Guo, Slay and Beckett [16] developed a methodology for the validation and verification of computer forensic tools. Their methodology starts with the description of scientific and systematically field of electronic evidence through a model and function mapping. The validation and verification of the tools is performed by specifying the requirements of each mapped function, then the reference set is developed wherein each test case is designed corresponding to one function requirement, their reason for using a reference set is that the tool and its functions can be validated and verified independently. However, their focus was on the searching function wherein they mapped the searching function specified the requirements of the searching function and developed the reference set to validate and verify forensic tools that have the searching function. The searching function was divided into three sub-categories: searching target, searching mode and searching domain. They claimed that their methodology offers benefits such as detachability, extensibility, tool neutrality and transparency and that by using this method any tool irrespective of its original design intention can be validated against known features. Though their methodology offers quit a number of benefits, it only focuses on the searching function, which is a category of the analysis stage in the digital forensic investigation process; it does not address other investigation processes. Kogeda et al. [31, 33, 35] used Bayesian networks to model likelihood of faults occurrence in cellular networks. Kogeda et al. [34] also modeled impact of faults in cellular networks. Owuor et al. [32] came up with a three-tier indoor localization system for digital forensics.

III. Digital Forensic Requirements

Requirements that need to be considered in an evaluation process are:

A. Digital Forensic Processes

There are several forensic processes in digital forensic investigation. Researchers tried to come up with processes and models of how digital forensic investigation must be conducted, but the procedures in digital forensics are neither consistent nor standardized. This is evident by a number of researchers have attempted to create basic guidelines over the past years [18]. "Since every investigation may have unique characteristics it is challenging to define a general digital forensic process model, one can find various models, which are quite similar to certain extent" [17].

TABLE I. Digital Forensic Processes

SRNo	Digital forensic investigation framework	Number of phases
1	Computer forensic process	4 processes
2	Generic investigative	7 classes
3	Abstract model of the digital forensic procedure	9 components
4	An integrated digital investigation process	17 processes
5	End-to-end digital investigation	9 steps
6	Enhanced integrated digital investigation process	21 phases
7	Extended model of cybercrime investigations	13 activities
8	Hierarchical objective-based framework	6 phases
9	Event-based digital forensic investigation framework	16 phases
10	Forensic process	4 processes
11	Investigation framework	3 stages
12	Computer forensics field triage process model	4 phases
13	Investigative process model	4 phases

Table I does not contain all the processes, as there are many processes in digital forensic, some of the processes tend to be suitable to a very specific situation while others may be applied to a wider scope, some are quite detailed while others may be too generic [15].

For the purpose of this research, a generic process has been developed, which will be used throughout this research for investigation purposes. The process consists of eight phases as shown in Figure 1.

ISBN: 978-988-14047-5-6
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

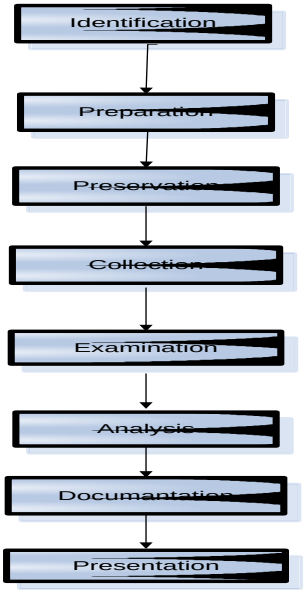

Figure 1: Generic digital forensic process

As shown in Figure 1, the process consists of the following stages:

1. Identification - this phase involves identifying potential evidence in the crime scene.
2. Preparation - involves planning on how to get the information needed by preparing tools, techniques and search warrants.
3. Preservation - this phase is all about preserving digital evidence (physical and digital evidence), ensuring that the actual evidence is not tempered with and ensuring an acceptable chain of custody.
4. Collection - the data identified is collected with the use of tools and techniques.
5. Examination - collected data is examined and extorted from the media. This phase involves an in-depth systematic search of evidence, evidence validation and recovery of hidden data related to the case, in this phase all evidence is thoroughly examined according to the nature of the crime.
6. Analysis - the results of the examination are analyzed to obtain useful information and conclusion is drawn based on the evidence found.
7. Documentation - findings of the forensic processes are documented.
8. Presentation - presents the results of the previous steps, describes the action performed and various standards and procedures used to arrive at the conclusion.

B. Skills

Conducting an investigation may not be as easy as finding log files in a computer. Special skills are required for one to conduct an investigation. A digital forensic investigator must have the following skills [27], [28]:

- Investigative skills - to supervise the conduct of the investigation and interview suspects and witnesses (strong analytical skills)
- Legal skills - knowledge of the laws which can be applied against computer related crimes and the laws of evidence (understanding of the rules of evidence and evidence handling)
- Court room presentation skills - ability to be an expert witness in court
- Computing skills - to uncover how the crime was committed, assist in reconstructing digital evidence and tracing proceeds of the crime (programming, understanding of operating systems and applications, strong system administrative skills)
- Knowledge of and experience with the latest forensic and intruder tools
- Knowledge of cryptography and steganography

C. Legal Standards

Evidence determines the truth of an issue, but its weight is subject to examination and verification through existing forms of legal argument [22]. Lack of appropriate care and attention to the legal rules concerning the collection and uses of digital evidence cannot only make the evidence useless, but it can leave investigators vulnerable to accountability in countersuits [22]. According to Cohen [23] digital forensic evidence must be considered in the legal context. These legal contextual issues drive the digital forensic processes and the work of those who undertake those processes, and without them it is very difficult if not impossible to do the job properly.

The Daubert standard has been widely used for admission of digital evidence in court and for validation of its reliability. To evaluate the admissibility of digital evidence the following guidelines should be considered [26]:

- The testability of theories and techniques employed by the scientific expert
- Its submission to peer review and publication
- The error rate of the techniques employed
- Subjection of theories and techniques to standards governing their application
- Acceptance of theories and techniques by expert

D. Chain of Custody

Care must be taken on the evidence acquired because any findings, which proves that the evidence data has been changed has an adverse consequence on the investigation and the legal proceedings [16]. “Failure to substantiate the evidence chain of custody may lead to serious questions regarding the authenticity and integrity of the evidence and the examinations rendered upon it” [16]. Chain of custody is very important as it is a way of measuring quality, authenticity and validity of the evidences collected [16]. The chain of custody is a record of evidence handling from the time it was collected, to the court case [19]. Without a chain-of-custody there is no way you can be sure that an object presented to the court of law is the same object that was collected at the scene of the crime, there is no means to assure that the expert’s proof pertains to evidence from the actual case that is under consideration [20]. The aim of the chain of custody document is to track who had access to a given piece of evidence, when and for what purpose. Immediately upon obtaining the evidence, the responder to an incident should start recording who has custody of what evidence [21]. “The chain of custody document should begin when the data is first considered as potential evidence and should continue through presentation of the item as evidence in court” [21].

ISBN: 978-988-14047-5-6
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

IV. Design and Implementation

The inability of the software to perform an intended task specified by the requirement and the environmental condition (the environment in which the software is designed to be used) is referred to as software failure. However, most of the forensic tools/softwares are used in the right environment since most users are forensic experts. Therefore, a right tool may be used in the right environment for the right task but fails to unearth the evidence in a forensic investigation.

Software reliability is defined as the probability that software will function without failure under a given environmental condition during a specified period of time [12]. Software failure is the inability of the software to perform an intended task specified by the requirement and the environmental condition.

f_{nf} = Number of failed functions

f_{np} = Number of passed functions

f_n =Number of functions in a software

T_n = Test number

R = Reliability

R_l = Percentage reliability

We start by developing an operation profile that specifies how the user will use the software. An operational profile can be defined as quantitative characterization of how a system will be used in the field by customers [22]. Test cases will be developed based on the operational profile then required input will be inserted in the software. We assumed that the user will only insert the right input and that the user is a qualified forensic expert who knows how to use the

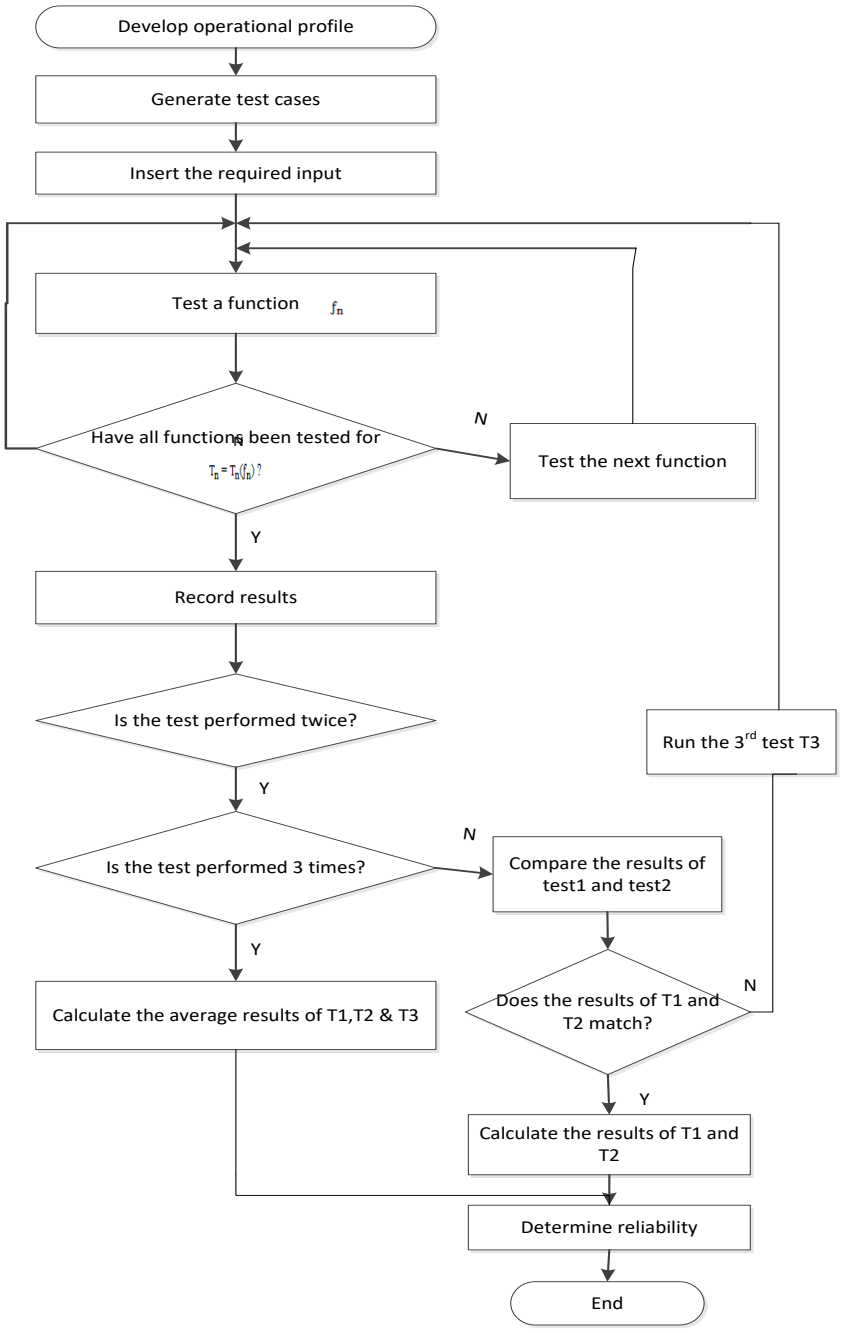

Figure 2: Reliability flowchart

ISBN: 978-988-14047-5-6
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

software. Since our main concern is measuring reliability, we did not perform a negative test, which assumes that the user might enter wrong input, which will results in incorrect results.

After inserting the required input, each function in a single test is tested $T_n = T_n(f_n)$. The results of each test T_n is then recorded, if a function managed to do what it was specified to do, then the function is identified as passed and if not, it is identified as failed. In a situation where the results of T_1 and T_2 do not match, then the third test T_3 needs to be performed. The results for each test are calculated by subtracting the total number of failures from the total number of functions, given by equation (1):

$$T_n = f_n - f_{nf} \quad (1)$$

After calculating the results of each test, then reliability is calculated by using equation (2):

$$R = \frac{T_n + T_n}{n} \quad (2)$$

If $T_1 \neq T_2$ then the test needs to be performed for the third time using equation (3):

$$\therefore R = \frac{T_n + T_n + T_n}{n} \quad (3)$$

To measure the level of reliability in percentage we use equation (4):

$$R_l = R \, x \, \frac{100}{f_n} \quad (4)$$

V. The Impact of Using Unreliable Tools

In this Section, we look at digital forensic tools, parties that use digital forensic, cybercrime and how it affects the society and the impact of using unreliable tools.

A. Digital Forensic Tools

A tool is an object used to achieve a goal or to carry out a particular function. Digital forensic is a discipline that relies on tools (both hardware and software tools), without tools forensic investigators cannot do their job. These tools are used to recover deleted files, create a disk image, collect data from a digital device, analyzing data, etc., examples of hardware tools are UltraKit and Forensic Recovery of Evidence Device, software tools are Forensic Toolkit (FTK), Encase, OSForensic, etc. However, the focus of this paper is on software tools. These tools differ in functionality, complexity and cost because while some are designed to serve a single purpose others offer a number of functions, some of the market leading commercial products cost thousands a lot of money, while others are for free (open source)[29]. The nature of the investigation will determine which tool is appropriate for the task at hand [29]. Tools need to be evaluated in order for an investigator to know which tools serve a single purpose and which ones serves multiple purposes, what are the weaknesses of a certain tool that the others do not have.

It is important to identify parties that use digital evidence because they are the ones who will mostly be affected by the consequences that come from the use of unreliable tools. These individuals and organizations include:

- Criminal Prosecutors - use digital evidence in a variety of crimes where convicting documents can be found such as homicides, financial fraud, drug and embezzlement record keeping, and child pornography.
- Civil litigators - make use of personal and business records found on computer systems that bear on: fraud, divorce, discrimination, and harassment cases.
- Insurance Companies - may be able to alleviate costs by using discovered computer evidence of possible fraud in accident, arson, and workman's compensation cases.
- Corporations - often hire digital forensics specialists to ascertain evidence relating to: sexual harassment, embezzlement, theft or misappropriation of trade secrets and other internal/confidential information.
- Law Enforcement Officials - frequently require assistance in pre-search warrant preparations and post-seizure handling of the computer equipment.
- Individuals - sometimes hired digital forensics specialists in support of possible claims of: wrongful termination or sexual harassment.

B. Cyber Crime

Cybercrime is any unlawful activities conducted through computer and the Internet, a computer-mediated activity that often takes place in the global electronic networks [23]. Cybercrime is the disease of our times and not a day goes by without cybercrime occurring. In a quest to find a cure for this disease, digital forensic was introduced to deal with finding the evidence in order to prove the crime and expose the criminals behind the crime in the court of law. Cybercrime is a growing problem that is affecting the global economy and has contributed to loss of business, placing the presence of companies at risk and damaging their reputation, loss of competitive advantage and loss of privacy.

Figure 3 (at the end of the paper) [24] measures the cost of cybercrime by using a framework that has five categories. These are:

- Criminal revenue - Criminal revenue is the monetary equivalent of the gross receipts from a crime.
- Direct losses - is the financial equivalent of losses, damage, or other suffering felt by the victim as a consequence of a cybercrime e.g., money withdrawn from victim accounts, time and effort to reset account credentials.
- Indirect losses – e.g., loss of trust in online banking, leading to reduced revenues.
- Defense costs – e.g., security products such as spam filters, antivirus and fraud detection
- Cost to society - is the sum of direct losses, indirect losses, and defense costs.

If the tools that forensic investigators use in an investigation produce unreliable results, the evidence will be portrayed as unreliable and the case might be over ruled, as a result, chances of cybercrime increasing are very high due to failure to properly handle cybercrime cases. Figure 4 (at the end of the paper) shows a mind map of the impact of unreliable digital forensic tools.

This study was done with the data collected from Hackmageddon.com and interviews conducted with forensic companies. We interviewed forensic companies; the interview was conducted by sending questionnaires to forensic companies and out of 100 percent, only 60 percent responded. The questionnaire wanted to find the average time it takes to solve a case, the number of unresolved cases and if the unresolved cases were due to a new crime.

ISBN: 978-988-14047-5-6
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

Using a Bayesian Network with the data collected. It is possible to calculate the probability associated with each node. We chose to use Bayesian network in order to show what causes certain events to occur given a set of variables. Figure 5(at the end of the paper) shows a Bayesian network with seven nodes with variables as type of criminal, new criminal, known crimes, new crimes, data lost/compromised, and disruption of business and loss of money. We computed the prior probabilities for each type of criminal using equation (5). The type of crime a specific criminal commits categorized the types of criminal.

$$P(A|B) = \frac{P(B|A)P(A)}{P(B)} \quad (5)$$

where:

- P(A) is the prior probability of the event A, without any information about the event B,
- P(A/B) is the conditional probability of the event A, given the event B,
- P(B/A) is the conditional probability of the event B, given the event A,
- P(B) is the marginal probability of the event B, acting like a normalizing constant

VI. Testing and Results

The average time to solve a case is a week (assumed to be 5 days) and for 8 hours, therefore the average time will be 40 hours. The number of cases that go unresolved is 10 out of 100, the number of cybercrime reports received from Hackmageddon.com in 2011 and 2012 is 1649; we calculated the 10% of 1649 which gave us 164.89. To get the rate (R), we took the average salary that a senior forensic investigator earns and calculate their rate per hour. If W_t is wasted time, c - crime, U_C - unresolved crime, t-time, W_m - wasted money, Ncr - new crime and R - rate.
Therefore,

$$W_t = U_c/C \times t \quad (6)$$

$W_t = 164.89/(1649) \times 40h$
$W_t = 3.9\ h$

In order to calculate W_m, we first need to calculate the rate of an investigator.
Days x hours x R = monthly salary
20 x 8h x R = 89961.57
160R = 89961.57
R = 89961.57/160
R = 562.26

$$(..)\ W_m = R \times W_t \quad (7)$$

$W_m = 562.26 \times 3.9h$
$W_m = 2192.8$

If a forensic investigator spends time on a case and fails to resolve it, the company losses R 2192.8. From the interviews conducted, most unresolved cases are caused by the occurrence of a new crime and most new crimes require the use of a new tool.

VII. Conclusion

The quantification of the use of unreliable tools clearly shows that there is a need for forensic tools to be evaluated to avoid the negative impact caused by their use. If digital forensic cannot help in decreasing cybercrime, then that defeats the purpose of its existence, therefore its significance relies on utilizing reliable tools. The results obtained from our model leads us to the development of a framework for evaluating digital forensic tools, which will help in minimizing the use of unreliable tools.

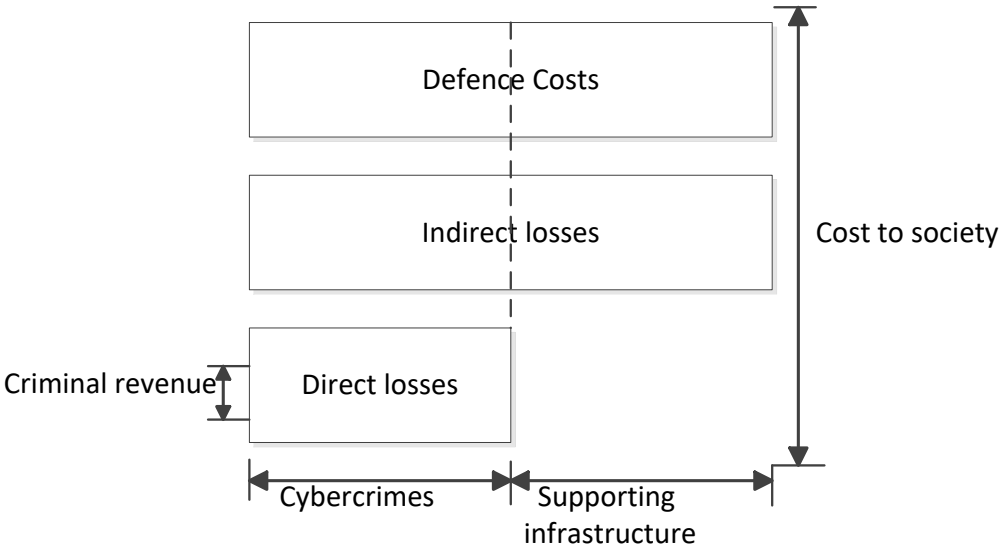

Figure 3: Framework of cybercrime costs

ISBN: 978-988-14047-5-6
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

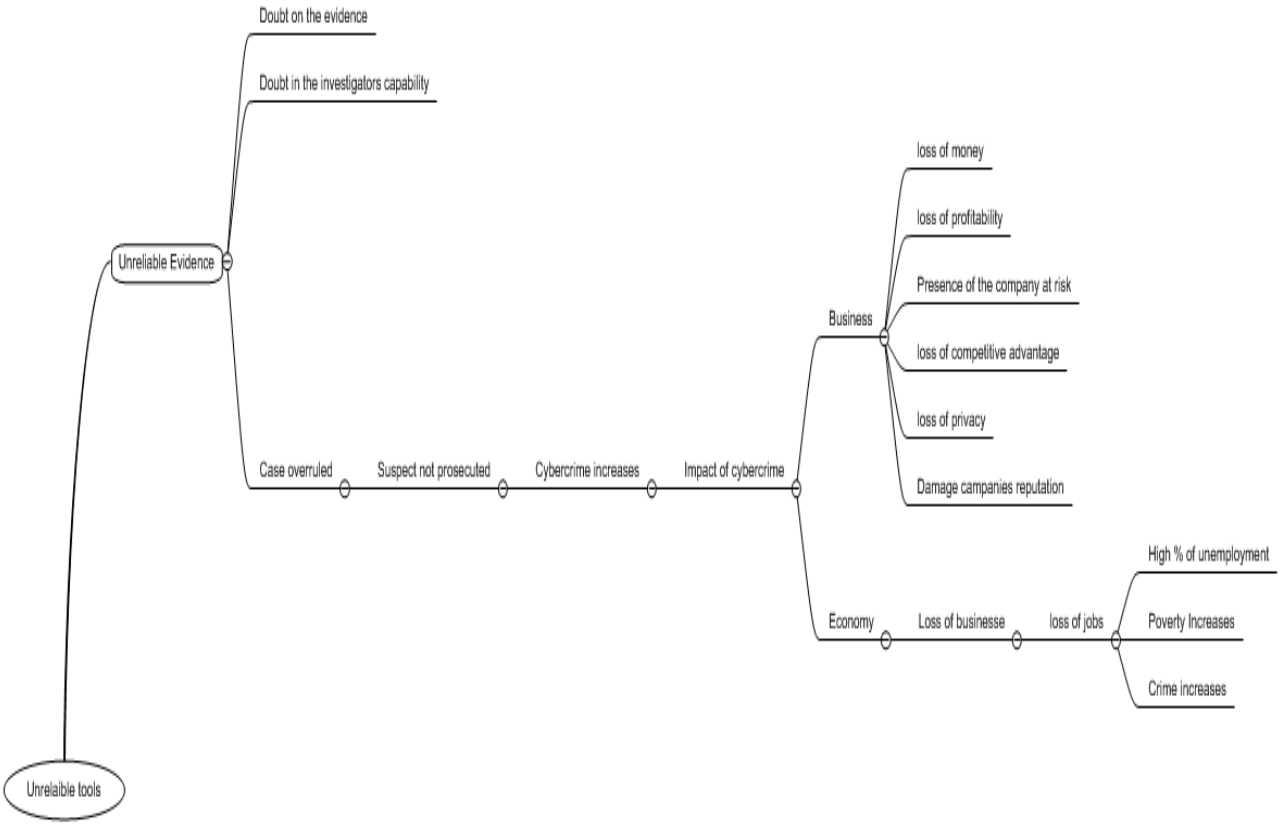

Figure 4: Impact flowchart

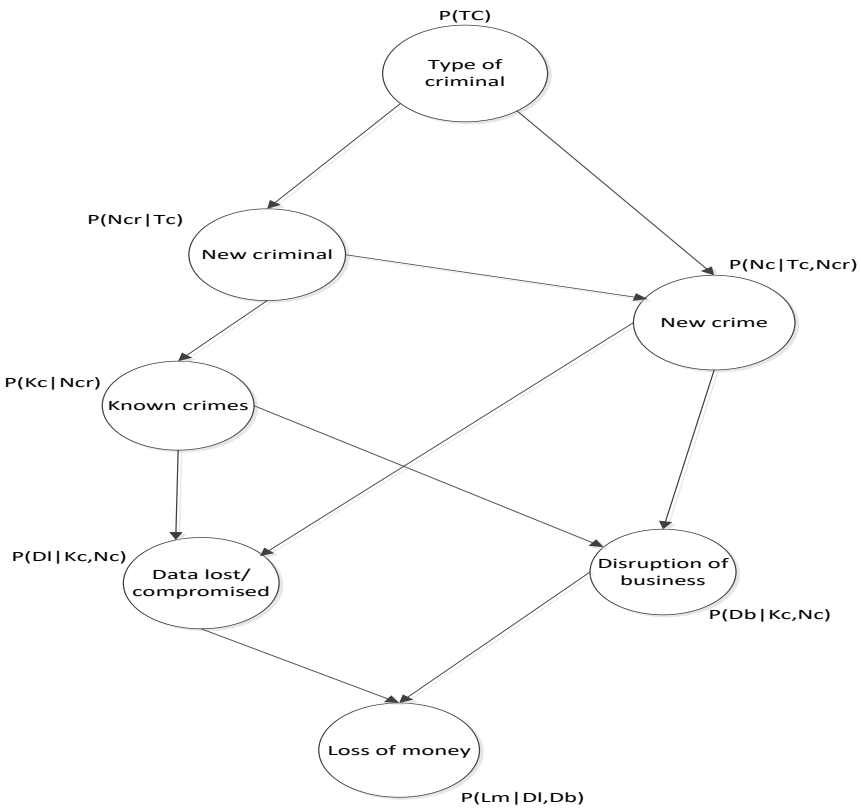

Figure 5: Bayesian network of cybercrime

ISBN: 978-988-14047-5-6
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

ACKNOWLEDGMENT

The authors would like to acknowledge department of Networks, ICT faculty of Tshwane University of Technology for the support that has made this research a reality.

REFERENCES

[1] S.R. Selamat, Yusof, R. and S. Sahib. “Mapping Process of Digital Forensic Investigation Framework.” International Journal of Computer Science and Network Security, vol. 8, pp.163-169,2008
[2] R. Morris. “Options in computer forensic tools.” Computer Fraud and Security, 2002, pp. 8-11.
[3] C. Armstrong. “Developing a framework for evaluating computer forensic tools”, In Evaluation in Crime Trends and justice: Trends and Methods Conference in Conjunction with the Australian Bureau of Statistics, 2003, pp. 24-25.
[4] J. Van Den Bos and R. van der Knijf. “TULP2G–an open source forensic software framework for acquiring and decoding data stored in electronic devices.” Int. Journal of Digital Evidence, vol. 4, 2005
[5] E. Van Buskirk and V. T. Liu. “Digital evidence: Challenging the presumption of reliability.” Journal of Digital Forensic Practice, vol. 1, pp.19-26, 2006
[6] Y. Guo., J. Slay and J. Beckett. “Validation and verification of computer forensic software tools—Searching Function." The proc. of the 9th Annual DFRWS Conference, vol. 6, 2009, pp. S12-S22.
[7] B. Pladna. “Computer Forensics Procedures, Tools, and Digital Evidence Bags: What they are and who should use them.” 2008.
[8] E. Casey. “Error, uncertainty, and loss in digital evidence.” International Journal of Digital Evidence, vol.1, pp.1-45,2002
[9] J. Liang. “Evaluating a selection of tools for extraction of forensic data: disk imaging” PhD Thesis, AUT University, New Zealand, 2010
[10] P. Palaniappan. “A model for validation and verification of disk imaging in computer forensic investigation.” PhD Thesis, Universiti Teknologi Malaysia, Malaysia, 2009
[11] B. Carrier. “Defining digital forensic examination and analysis tools using abstraction layers” Int. Journal of digital evidence, vol.1, pp.1-12, 2003
[12] M. Xie. Software reliability modeling. Singapore: World Scientific Publishing, 1991, pp. 5
[13] R. Mercuri. “Criminal Defense Challenges in Computer Forensics.” The first International ICST Conference, 2010, pp. 132-138.
[14] G. Mohay. (2005, November). “Technical challenges and directions for digital forensics.” 1st Int. Workshop on SADFE, 2005, pp.155-161
[15] Y. Yusoff., R. Ismail and Z. “Common Phases of Computer Forensics Investigation Models.” Int. Journal of Computer Science and Information Technology, vol. 3, pp. 17-31, 2011
[16] K. N. Nithesh et al. “Use of AFF4 Chain of custody-Methodology for Foolproof Computer Forensics Operation.” Int. Journal of Communication and Networking System, vol. 1, pp. 49-57, 2012
[17] O.K. Appiah-Kubi., S. Saleem, and O. Popov. “Evaluation of Some Tools for Extracting e-Evidence from Mobile Devices.” In 5th International Conference-AICT, 2011, pp. 1-6
[18] M. Reith, C. Carr and G. Gunsch. “An examination of digital forensic models.” Int. Journal of Digital Evidence, vol.1, pp.1-12, 2002
[19] J. McMillan. “Importance of a standard methodology in computer forensics.” Information Security Reading Room, 2000.
[20] S. L. Garfinkel. “Providing cryptographic security and evidentiary chain-of-custody with the advanced forensic format, library, and tools.” Int. Journal of Digital Crime & Forensics, vol.1, pp.1-28, 2008
[21] J. Tan. “Forensic readiness.” Cambridge, MA:@ Stake, 2001
[22] L Lalji Prasad, Ankur Gupta, and Sarita Badoria, "Measurement of Software Reliability Using Sequential Bayesian Technique," Lecture Notes in Engineering and Computer Science: Proceedings of The World Congress on Engineering and Computer Science 2009, 20-22 October, 2009, San Francisco, USA, pp242-246.
[23] W. Chung et al. “Fighting cybercrime: a review and the Taiwan experience.” Decision Support System, vol. 41, pp. 669-682, 2006
[24] R. Anderson et al. “Measuring the Cost of Cybercrime.” WEIS, 2012.
[25] T. Wilsdon and J. Slay. “Validation of Forensic Computing Software Utilizing Black Box Testing Techniques.” In Australian Digital Forensics Conference, 2006, pp. 37.
[26] A. Schwartz. “A Dogma of Empiricism Revisited: Daubert v. Merrell Dow Pharmaceuticals, Inc. and the Need to Resurrect the Philosophical Insight of Frye v. United States.” Harv. JL & Tech, vol. 10, pp. 149.
[27] K. Ryder. “Computer Forensics – We’ve had an incident, who do we get to investigate?” SANS Institute, 2002, pp. 1-12
[28] P. A. Collier and B. J. Spaul. “A forensic methodology for countering computer crime.” Artificial intelligence review, 1992, pp. 203-215
[29] K.K. Arthur 1 H.S. Venter. “An Investigation into Computer Forensic Tools.” In ISSA, 2004, pp. 1-11
[30] R. McCusker. “Transnational organised cybercrime: distinguishing threat from reality.” Crime, Law & Social Change, 2006, pp. 257-273.
[31] O.P. Kogeda et al."A Probabilistic Approach To Faults Prediction in Cellular Networks", In the Proceedings of the 5th International Conference on Networking (ICN2006), Mauritius, April 23-28, 2006.
[32] D.L. Owuor et al. “Three Tier Indoor Localization System for Digital Forensics”, Int. Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering, Vol:11, No:6, 2017 Pp.564-572.
[33] O.P. Kogeda, “Modeling of Reliable Service Based Operations Support System (MORSBOSS)”, Ph.D. Thesis, Department of Computer Science, University of the Western Cape, SA 2008
[34] O.P. Kogeda et al. "Impacts and Cost of faults on Services in Cellular Networks", Proc. IEEE Int. conference on Mobile Business, Sydney, Australia, 11-13 July 2005, pp. 551 – 555.
[35] O.P. Kogeda and J.I. Agbinya, “Cellular Network Faults and Services Dependency Modeling”, Int. Magazine on Advances in Computer Science and Telecommunications, Vol. 1, No. 1, pp.15-22, 2010.