International Journal of
Science and Engineering Investigations
vol. 8, issue 88, May 2019
Received on May 22, 2019
ISSN: 2251-8843

A Metric for the Specification of a Consistent Digital Forensic Evidence Extraction Process Model in Mobile Devices

Gilbert Gilibrays Ocen[1], Mutua Stephen[2], Mugeni Gilbert[3], Karume Samuel[4], Matovu Davis[5]
[1,5]Busitema University
[1,2,3,5]Masinde Muliro University of Science and Technology
[3]Communication Authority of Kenya
[4]Laikipia University
([1]gilbertocen@gmail.com, [2]stephen.makau@gmail.com, [3]gbmugeni@gmail.com, [4]smkarume@gmail.com, [5]davismatovu@yahoo.com)

Abstract-Over the years researchers have proposed and developed models for extraction of digital evidence in mobile devices but little has been done on standardization of these models hence leading to inconsistencies in the extraction process used since most of the models developed cater for specific needs or a group of interest. In this paper we propose a metric for specification of a consistent digital forensic evidence extraction process in mobile devices to address the inconsistencies in existing digital forensic evidence extraction models for mobile devices running on android, windows, Apple iOS and Blackberry operating system. The proposed metric is aligned with Digital forensic principles and standard operating procedures (SOP), forensic and legal requirements, digital evidence quality, extraction tools and digital evidence legal admissibility. The metric has an integration of several factors such as policy, extraction method, nature of data, device factors, forensic extraction tools and forensic documentation process with consideration of the mobile device operating systems platform. This metric is relevant to law enforcement officers and digital forensic practitioners as well forensic extraction tool developers.

Keywords- *Metric, Consistent, Digital Forensic Evidence, Mobile Devices*

I. INTRODUCTION

The evolution of mobile devices and increased use in day to day business has led to rise in cases of crimes committed through the use of these devices [1]. Criminals take advantage of such technological developments to commit crime[2]. This has led to development of a number of digital forensic tools and process models so as to keep up-to-date with the growing pace of need for digital forensic investigation and extraction of digital evidence in mobile devices in order to apprehend cybercriminals [2]–[6]. Researchers such as [7], [8] contend that digital forensic process models lack standard guidelines.

Consequently, there are a lot of process inconsistencies during evidence acquisition, which are attributed to models used during evidence acquisition focusing on a particular stage of the investigation while others designed for a particular need of the interest group [9], [10]. Some researchers argue that forensic extraction tools and models used during digital forensic evidence extraction lacked designs created with forensic science needs [11]. "Digital forensics process is a highly technical field that depends on the proper implementation of specific, well-accepted protocols and procedures" [12], therefore inadequate forensic tools and technical examination, lack of adherence to appropriate protocols and procedures, can result in evidence that does not meet legal standards of proof and admissibility [13], [14].

In order to address the problem of inconsistencies in digital forensic evidence extraction process models brought about by lack of standardization, forensics models and tools designed with lack of forensic science needs [9], [11], [15], in this paper we propose a metric that should be used during digital forensic evidence extraction in mobile device so as to address the inconsistencies in digital evidence extraction. Our approach differs from those that provide general guidance in the form of best practices, classification schemes or a checklist for digital forensics procedures by providing specific construct and the sub metrics in each construct that should be adhered to while extracting digital forensic evidence in mobile devices.

II. REVIEW OF RELATED WORK

A common definition of digital forensic is the use of scientifically derived and proven methods toward the process of preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence which is derived from the digital sources [16]. However, [9], [17] stated that the process of the investigation should be incorporated with the basic procedures in forensic investigation which are preparation, investigation and presentation.. This process need to be considered and evaluated to determine the requirements for each investigation [10]. 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 [7]. This is evident by a number of researchers who have attempted to create basic guidelines over the past years[7]. 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 [10].

III. Factors responsible for inconsistencies on Evidence extraction process models

Literature indicates that there are several factors responsible for inconsistencies in digital forensic evidence extraction process models and these factors can be grouped under the following themes/ constructs;

IV. Policy factors

Developing policies and procedures that establish the parameters for operation and function of creating forensics unit is vital in digital evidence extraction and these polices should focus on: Technology, personnel requirements, training needs, laws guiding evidence collection and preservation, software/forensic tools to use and effective implementation of such guidelines and policies[18].

V. Device Factors (DF) construct

Mobile devices vary in design and are continually undergoing change as existing technologies improve and new technologies are introduced and when these devices are encountered during an investigation, there so many concerns that needs to be taken into account such as ;best method to preserve the evidence, criteria for handling the device, extraction of potentially relevant information from such devices, therefore an understanding of the hardware and software characteristic of these devices can help to address these concerns and this can only be done at the identification phase of the investigation or extraction where the type of the device is identified with the corresponding hardware and software characteristics [18].

VI. Extraction Method Factors

According to [19], understanding the various types of mobile acquisition tools and the data they are capable of recovering is important for a mobile forensic examiner, they a present a pyramid of classification of extraction methods used by different tools enables the examiner to choose an extraction method that best suit the kind of extraction he/she is interested in.

Figure 1. Extraction method/ acquisition types adopted from [18]

VII. Nature of Data Factors (ND) construct

The portability of mobile devices built with mobility, extended battery life, simplicity in functionality unlike personal computer raises the need to understand the kind of data that these devices carries with them, the operating system structure and how it organizes the memory whether internal or external storage [20]

VIII. Forensic extraction tool Factor Construct

Forensic tools are tools that are designed primarily for uncovering data from Mobile Devices [21], forensic tools are used to unravel criminal acts and prove crime in the court of law[1]. However, sometimes forensic experts may apply a particular tool not because it is the most effective but due its availability and cost, this may sometimes raise issue of unreliability and credibility of the evidence[1]. Therefore this work has proposed a number of tools both commercial and open source that can be used.

IX. Forensic Documentation Process

According to [6] "*a well-trained examiner understands that documentation is continuous throughout the entire examination process"*. While [22][6], [18] notes that documentation should be contemporaneous with the examination, and retention of notes should be consistent with policies that guide: taking notes when consulting with the case investigator and/or prosecutor, maintaining a copy of the search authority with the case notes, maintaining a copy of chain of custody documentation., documenting irregularities encountered and any actions taken regarding the irregularities during the examination.

X. Metrics in Digital Evidence

"A metric is a system of related measures enabling quantification of some characteristic. A measure is a dimension compared against a standard"[23]. A review of the following research work in table 1 indicates that there has been several attempts to develop metrics for digital evidence specifically for determining guidelines, measuring errors, establishing reliability and criminal activity analysis. However none of these dealt specifically with evidence extraction Perhaps the closest metric to the proposed metric in *figure2*, ever developed is the metric for network forensic conviction evidence where the author's present quantification for network forensic however, this is confined to Network forensic and mostly measure the severity of the impact of network forensic. Although they show how the credibility of evidence gathered from the network can be affected by security and inconsistencies, they also propose that a formalized intuitive model should be designed with focus on capturing data packets, this therefore means that there should be a formal metric for evidence collection [26].

TABLE I. SUMMARY OF REVIEWED WORK ON METRICS FOR DIGITAL EVIDENCE

Metric	Strength	Weakness
U.S. Department of Justice, Forensic Examination of Digital Evidence: A Guide for Law Enforcement (general guidelines and worksheets) [6]	General guidelines and check list for investigation	Lacks clear process and metrics to followed during the investigation and extraction of digital evidence
Error, Uncertainty, and Loss in Digital Evidence (certainty levels) [9]	Developed certainty levels for evidence, considering losses and errors	Does not consider the process and metrics used in evidence extraction
Cyber Criminal Activity Analysis Models using Markov Chain for Digital Forensics (suspicion levels)[24]	Developed Analysis of levels of suspicions in criminal activities	Does not tackle metrics used in determining such levels and evidence
Two-Dimensional Evidence Reliability Amplification Process Model for Digital Forensics (evidence reliability)[25]	Developed reliability level of digital evidence, metrics for reliability is provided	No mention of process metrics is provided, discusses only reliability metrics
Metrics for network forensics conviction evidence[26]	Discusses network conviction metrics and evidences	Does not cater for process extraction metrics, emphasizes more of network not mobile devices
Metrics-Based Risk Assessment and Management of Digital Forensics[12]	Concentrated on risk based metrics and management of Digital Forensics	Risk based metrics does not support process extraction metrics

XI. METHODS AND MATERIALS

The general list of metrics was got from literature, the literature also informed the choice of factors considered in this research and the main constructs for the specification of metric for consistent digital forensic evidence extraction process in mobile devices. A survey through the use of questionnaires was conducted among eighty five respondents drawn from law enforcement agencies, researchers, ICT practitioners, regulatory authorities and business community within the districts of Kampala-Uganda. The questionnaire were designed on the scale of 1-5(1-Strongly Disagree, 2- Disagree, 3-Neutral, 4-Agree and 5-Strongly Agree). The constructs used in this study has sub constructs where respondents' opinion was sought as to the level of influence they have in regards to digital forensic evidence process extraction inconsistencies are concerned. Mean responses from each of these constructs were used in the development of the metric. Materials used included Microsoft Visio v2013, while Android, windows, Apple iOS and Blackberry operating system were used to implement the metric.

XII. DERIVATION OF METRIC FOR DIGITAL FORENSIC EVIDENCE EXTRACTION PROCESS MODEL

The concept by [27], who contends that there is a need for security metrics in digital forensic that: "meet legal requirements for measureable reliability, authenticity, accuracy and precision, and that is based on a sound scientific methodology properly applied, and have a basis provided for independent testing" have been adopted in deriving this metric.

The metric in figure2 has been built by transferring the concepts from the Metrics for digital forensic research [28], which emphasized measurement of parameters of each construct used in the metrics for evidence investigation and collection since there is no industry consensus that a judge and jury can rely upon as adequate to support a claim that meet legal requirements for measurable reliability, authenticity, accuracy, and precision of the process followed during evidence acquisition which are currently elusive and constructed on a case by case basis[29].

Additionally using concept presented by [28] about the metric for information retrieval and Intrusion Detection System (IDS) which details that "information are relevant if the query are successfully retrieved" [30], have been adopted in deriving the proposed metric in Fig 2.This is because the aim of this paper was to develop a metric for extraction of digital forensic evidence in mobile devices which is similar to information retrieval presented by [30] and because these two concepts i.e. information retrieval and intrusion detection systems both used measurement of key parameters such as performance, information retrieval, query recall and measurement of the indicators, the researchers found these concepts of great importance in deriving the metric in figure2. Information has been used in measuring the performance [31]. Such measurement concept was borrowed in deriving this metric.

In order to derive the metric, summation of all the constructs' sub-indices as presented in Table2 was done, based on this summation, the regression model of adjusted R and standard error was used to derive the metric equation.

From this descriptive statistics, in order to determine the minimum acceptable range of measure for each construct to be used in the metric we took the average response as the minimum acceptable range and this was derived as

Policy factor

PF1+PF2+PF3+PF4+PF5+PF6+PF7/7= 4.36

Device factor

= DF1+DF2+DF3+DF4/4= 4.21

Extraction Method factor

= EM1+EM2+EM3+EM4+5+EM6+EM8+EM9/9= 4.12

Nature of Data factors

= ND1+ND2+ND3+ND4+ND5/5= 3.90

Forensic Extraction tool factor

=FET1+FET2+FET3+FET4+FET5+FET6+FET7+FET8+FET9/9= 2.78

Forensic Documentation process

=TDP1+TDP2+TDP3+TDP4+TDP5+TDP6+TDP7+TDP8+TDP9+TDP10/10= 4.11.

TABLE II. DESCRIPTIVE STATISTICS FOR CONSTRUCTS USED IN DERIVING THE METRIC

Item Statistics			
	Mean	Std. Deviation	N
Policy factors			
PF1	4.64	.574	85
PF2	4.31	.637	85
PF3	4.40	.876	85
PF4	4.32	.582	85
PF5	4.49	.684	85
PF6	4.09	.750	85
PF7	4.31	.887	85
Device factors			
DF1	4.45	.627	85
DF2	4.27	.662	85
DF3	4.09	.908	85
DF4	4.04	.957	85
Extraction Method factors			
EM1	4.39	.773	85
EM2	4.11	.772	85
EM3	4.46	.716	85
EM4	3.96	.763	85
EM5	4.14	.789	85
EM6	3.91	.959	85
EM7	3.93	1.021	85
EM8	4.25	1.022	85
EM9	4.09	.840	85
Nature Of Data Factors			
ND1	4.32	.790	85
ND2	3.79	.773	85
ND3	4.19	.794	85
ND4	3.69	.859	85
ND5	3.53	1.042	85
Forensic Extraction Too Factors			
FET1	3.99	1.220	85
FET2	3.44	1.277	85
FET3	2.95	1.542	85
FET4	2.74	1.521	85
FET5	3.36	1.223	85
FET6	2.67	1.322	85
FET7	2.72	1.548	85
FET8	2.42	1.507	85
FET9	3.47	1.419	85
Forensic Documentation Process			
TDP1	4.39	.773	85
TDP2	4.11	.772	85
TDP3	4.46	.716	85
TDP4	3.96	.763	85
TDP5	4.14	.789	85
TDP6	3.91	.959	85
TDP7	3.93	1.021	85
TDP8	4.25	1.022	85
TDP9	4.09	.840	85
TDP10	3.85	1.160	85

TABLE III. TABLE REGRESSION ANALYSIS: INFLUENCE OF INDEPENDENT VARIABLES ON OPERATING SYSTEM, MODEL SUMMARY[B]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
	0.783[a]	0.613	0.608	0.535	0.613	131.414	1	83	0.000

a. Predictors: (Constant), extract cons

The regression model summary indicates that combination of all the constructs used in this study (extract cons) comprising of policy, nature of data, device factors, extraction methods, forensic extraction tools and forensic documentation process with adjusted R square value of .608 (60.8%) and standard error of estimate at .535. This can be interpreted as the level of influence of such factors on evidence extraction process in mobile devices, consequently this implies that these constructs contributes to the 60.8% of the causes of inconsistencies in digital forensic evidence extraction in mobile devices as supported by literature [15], [18], [22], [32], This information in Table 2. Based on the regression model summary has led to the derivation of the metric in *figure2* while borrowing the concept of measurement in a metric developed by [28].

XIII. METRIC EQUATION

M (OS) = 0.608(PF + DF+ND+EF+TF+ FF) +- 0.535

Where M (OS) is the metric for the extraction of digital forensic evidence in mobile devices running any of the four operating system

0.608 is regression adjusted R of influence of the constructs as far as inconsistencies in evidence extraction is concerned

PF is the policy factor construct

DF is the Device Factor construct

NF is the Nature of Data Factor construct

EF is the Extraction Method Factor Construct

TF is the Forensic Extraction Tool Factor Construct

FF is the Forensic Documentation Process Factor Construct

+- 0.535 is the standard error that can be accepted in this metric equation

XIV. DISCUSSION OF RESULTS

According to [33], during the development and implementation of a measure such as a metric, there are general principles that need to be taken into account. These principles are either technical or business related. In this paper, these principles have been considered for example this metric shows the technical aspects that must be taken in to account when extracting evidence from mobile devices that is the Nature of

Data, Extraction method used, the forensic extraction tools, device type while considering policy at both technical and business level. Once these principles are adopted, the researchers believe that this metric will yield quantifiable, repeatable, easily obtainable and relevant digital forensic evidence extraction process model.

This is a generic metric that can be applied across any mobile operating system platform but precisely Android, Windows, Apple iOS and Blackberry operating system since the constructs were developed from literature reviewed about digital evidence extraction form these mobile device operating system platforms.

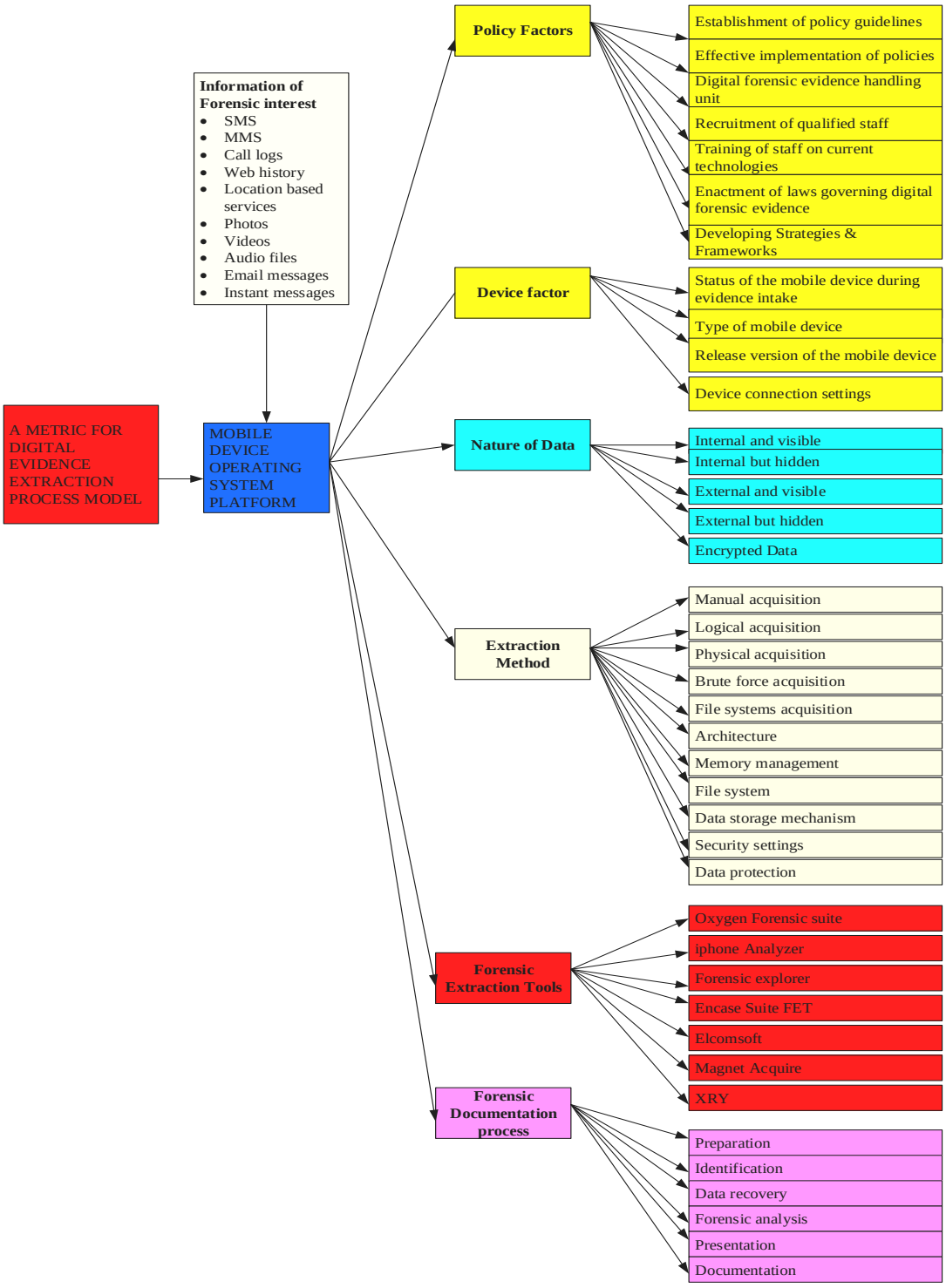

Figure 2. Metric for the extraction of Digital evidence in mobile devices

XV. CONTRIBUTION OF THIS WORK

There are two major contributions of this work;

- The work has reviewed related research on digital forensic metrics and discovered that many attempts to develop metric for digital evidence did not focus on evidence gathering in mobile devices
- Developed metric that can be used for extraction of digital forensic evidence in mobile devices

XVI. CONCLUSION AND FUTURE WORK

Several researchers have developed process models for the extraction of digital forensic evidence, although these models differ in their considerations of the stages and phases to be followed during evidence extraction. In this paper we propose a metric that should be considered during evidence extraction from mobile devices to reduce on the inconsistencies that arise as a result of various process models that lack standard guidelines. This metric is relevant in guiding the process model used during digital forensic evidence extraction. Future work should be devoted to testing and validating the applicability of this metric on the various mobile operating system platforms.

REFERENCES

[1] Precilla M. Dimpe and Okuthe P. Kogeda, Impact of Using Unreliable Digital Forensic Tools: Proceedings of the World Congress on Engineering and Computer Science 2017, 2017.

[2] A. Goel, a Tyagi, and a Agarwal, "Smartphone Forensic Investigation Process Model," ... *J. Comput. Sci. ...*, no. 6, pp. 322–341, 2012.

[3] P. R. Lutui, "Digital forensic process model for mobile business devices : Smart technologies," 2015.

[4] M. D. Kohn, M. M. Eloff, and J. H. P. Eloff, "Integrated digital forensic process model," pp. 1–13, 2010.

[5] S. Omeleze and H. S. Venter, "Testing the harmonised digital forensic investigation process model-using an Android mobile phone," *2013 Inf. Secur. South Africa - Proc. ISSA 2013 Conf.*, 2013.

[6] N. Institute of Justice, "Forensic Examination of Digital Evidence: A Guide for Law Enforcement."

[7] M. Reith, C. Carr, and G. Gunsch, "An Examination of Digital Forensic Models," *Int. J. Digit. Evid.*, vol. 1, no. 3, pp. 1–12, 2002.

[8] D. A. Maltz, M. K. Reiter, V. Sekar, Y. Xie, and H. Zhang, "Toward a Framework for Internet Forensic Analysis," *Third Work. Hot Top. Netw. (HotNets-III*, vol. 1, pp. 1–6, 2004.

[9] E. Casey, "Error, Uncertainty, and Loss in Digital Evidence," *Int. J. Digit. Evid.*, vol. 1, no. 2, p. 45, 2002.

[10] A. K. Kubi, S. Saleem, and O. Popov, "Evaluation of some tools for extracting e-evidence from mobile devices," *2011 5th Int. Conf. Appl. Inf. Commun. Technol. AICT 2011*, no. 10, 2011.

[11] B. Carrier, "Defining Digital Forensic Examination and Analysis Tools Using Abstraction Layers," 2003.

[12] S. Stockton, "ASSESSING DIGITAL FORENSICS RISK : A METRIC SURVEY APPROACH," 2014, no. November.

[13] G. C. Kessler, "Judges' awareness, understanding, and application of digital evidence," *ProQuest Diss. Theses*, p. 192, 2010.

[14] J. M. Morse, M. Barrett, M. Mayan, K. Olson, and J. Spiers, "Verification Strategies for Establishing Reliability and Validity in Qualitative Research," 2002.

[15] S. Saleem, O. Popov, and A. Kubi, "Evaluating and Comparing Tools for Mobile Device Forensics using Quantitative Analysis," *Digit. Forensics Cyber Crime Lect. Notes Inst. Comput. Sci. Soc. Informatics Telecommun. Eng.*, vol. 114, no. JANUARY, pp. 264–282, 2013.

[16] M. Pollitt, "DIGITAL FORENSIC RESEARCH CONFERENCE A Framework for Digital Forensic Science."

[17] B. Pladna, "Computer Forensics Procedures, Tools, and Digital Evidence Bags: What They Are and Who Should Use Them."

[18] R. Ayers, S. Brothers, and W. Jansen, "NIST Special Publication 800-101 Revision 1: Guidelines on Mobile Device Forensics," *NIST Spec. Publ.*, vol. 1, no. 1, p. 85, 2014.

[19] D. Abalenkovs *et al.*, "Mobile Forensics: Comparison of extraction and analyzing methods of iOS and Android," pp. 1–13, 2012

[20] R. Ahmed and R. V Dharaskar, "Mobile Forensics : an Overview , Tools , Future trends and Challenges from Law Enforcement perspective," *Online*, no. January 2015, pp. 312–323, 2008.

[21] D. M. Sai, N. R. G. K. Prasad, and S. Dekka, "The Forensic Process Analysis of Mobile Device," vol. 6, no. 5, pp. 4847–4850, 2015.

[22] T. M. J. Abbas, "Studying the Documentation Process in Digital Forensic Investigation Frameworks / Models," *J. Al-Nahrain Univ.*, vol. 18, no. 4, pp. 53–162, 2015.

[23] Z. Abbadi, "Security Metrics What Can We Measure?"

[24] D. Kim, D. Hoon Kim, and H. Peter In, "Cyber Criminal Activity Analysis Models using Markov Chain for Digital Forensics," 2008.

[25] M. Khatir, S. M. Hejazi, and E. Sneiders, "Two-Dimensional Evidence Reliability Amplification Process Model for Digital Forensics," in *2008 Third International Annual Workshop on Digital Forensics and Incident Analysis*, 2008, pp. 21–29.

[26] A. R. Amran, R. C.-W. Phan, and D. J. Parish, "Metrics for network forensics conviction evidence," in *2009 International Conference for Internet Technology and Secured Transactions, (ICITST)*, 2009, pp. 1–8.

[27] S. Siti Rahayu *et al.*, "Traceability in digital forensic investigation process" 2011.

[28] F. Cohen, "Metrics for Digital Forensics," in *MiniMetriCon Conference* , 2011.

[29] S. R. Selamat, S. Sahib, N. Hafeizah, R. Yusof, and M. F. Abdollah, "A Forensic Traceability Index in Digital Forensic Investigation," *J. Inf. Secur.*, vol. 4, pp. 19–32, 2013.

[30] T. Holz, "Security Measurements and Metrics for Networks," in *Dependability Metrics*, Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 157–165.

[31] A. Al-Dallal and R. S. Abdulwahab, Achieving High Recall and Precision with HTLM Documents: An Innovation Approach in Information Retrieval.

[32] K. Kent, S. Chevalier, T. Grance, and H. Dang, "Guide to integrating forensic techniques into incident response," *NIST Spec. Publ.*, no. August, pp. 800–886, 2006.

[33] P. Trimintzios, "Measurement Frameworks and Metrics for Resilient Networks and Services: Technical report," *Eur. Netw. Inf. Secur. Agency*, no. February, p. 109, 2011.

How to Cite this Article:

Ocen, G. G., Stephen, M., Gilbert, M., Samuel, K. & Davis, M. (2019) A Metric for the Specification of a Consistent Digital Forensic Evidence Extraction Process Model in Mobile Devices. International Journal of Science and Engineering Investigations (IJSEI), 8(88), 88-93. http://www.ijsei.com/papers/ijsei-88819-16.pdf