INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 5, Issue 6)
Available online at: www.ijariit.com

Evaluating factors responsible for inconsistencies in mobile devices digital forensic evidence extraction process model

Gilbert Gilibrays Ocen
gilbertocen@gmail.com
Busitema University and Masinde Muliro University of Science and Technology, Kakamega, Kenya

Mutua Stephen
stephen.makau@gmail.com
Masinde Muliro University of Science and Technology, Kakamega, Kenya

Gilbert Barasa Mugeni
gbmugeni@gmail.com
Communications Authority of Kenya, Nairobi, Kenya

Karume Simon
smkarume@gmail.com
Laikipia University, Eldoret, Kenya

Matovu Davis
davismatovu@yahoo.com
Busitema University and Masinde Muliro University of Science and Technology, Kakamega, Kenya

ABSTRACT

The proliferation of mobile devices has revolutionized life in the 21st century ranging from the way people socialize to the modes of doing business. Mobile devices contain substantial amounts of private data that in event of crime or security investigations when adduced before any court of law can aid in resolving a number of undetermined causes. However, mobile digital forensics research is still faced with several challenges. Most existing mobile devices digital forensic evidence extraction models are vendor-specific and thus anchored on specific device platforms such as Android, Windows, Apple iOS, and Blackberry. Additionally, these models contain various process inconsistencies and lack specified technical documentation. Further, the growing demand for mobile devices and crime-related occurrences affecting them has strained and exposed the existing models. A number of questions thus remain unanswered into the factors responsible for these inconsistencies and the lack of a unified model that can be applied across these four operating system platforms. A mixed-method approach involving a survey was used in this study where respondents were drawn from ICT practitioners, law enforcement agencies, researchers and the business community. This study highlights several factors that contribute to digital evidence extraction process model inconsistencies which include policy, extraction methods, nature of data, device type, data type, and extraction tools among others. The study proposes systematic documentation of every step followed during evidence extraction from mobile devices so as to avert the inconsistencies.

Keywords— *Mobile devices, Digital evidence, Process model, Extraction inconsistencies*

1. INTRODUCTION

Digital forensics is defined by [1] as "the process of identifying, preserving, analyzing, and presenting digital evidence in a manner that is legally acceptable". [2] defines digital evidence as "information and data of value to an investigation that is stored on, received or transmitted by an electronic device". The continued technological advancements and the increasing popularity of mobile digital devices pose great challenges for investigators and law enforcement officials all over the world [3]. The existence of many tools and techniques with different process models make it difficult for a professional investigator to choose the proper forensic tool for seizing internal data from mobile devices [3]. Mobile devices use either proprietary or an open-source operating system, nearly 80% of mobile devices including smartphones use one of the following operating systems: Android, Windows, Apple iOS, or BlackBerry OS [4]. Attempts to extract information from various mobile devices running various operating system platforms, using a range of mobile forensic tools and process models have shown differing results [5]. The growing demand for examination of evidence from mobile devices raises the need for the development of consistent process guidelines for the examination of these devices [6]. "Considering the differences in the specific details of the examination of each device, the adoption of consistent and well-documented examination processes models should assist the examiner in ensuring that the evidence extracted from each mobile device is well documented and that the results are repeatable and defensible in courts of law" [6]. Additionally, a number of these models contain various process inconsistencies and lack the specified technical documentation [7]. Further, the growing demand and use of mobile devices and crime-related occurrences affecting them has

further strained and exposed the existing models [7], [8]. A number of questions thus remain unanswered in regard to the factors responsible for these inconsistencies, the lack of a unified model that can be applied across the diverse devices running various operating system platforms. Therefore, in order to ensure consistency in digital evidence extraction, digital evidence extraction process model followed in any of these platforms should be carefully documented and reported [9]. In this study the researchers identified and ranked factors that are responsible for mobile devices digital forensics evidence extraction process model inconsistencies under eight broad-themes/constructs.

1.1 Constructs used in this study

This study suggests that Process Model Extraction Inconsistencies (PMEI) in mobile devices with Android, Windows, Apple iOs or Blackberry operating system, is influenced by several independent variables which can be categorized into Policy Factors [10], Device factors [11], Extraction Method factors [12], Data Type factors [10], Nature of Data [13], Forensics Extraction Tools [14] and Forensic Documentation Process [15]. These constructs are further elaborated below;

According to [10] digital forensic evidence extraction should be guided by policies that facilitate efficient and effective digital forensic activities, clear statements about forensic considerations, qualified and authorized personnel to perform forensic investigations, clearly defined roles and responsibilities of the workforce, creation and maintaining procedures and guidelines for performing forensic tasks and these guidelines should focus on general methodologies for investigating incidents using forensic techniques.

Similarly, *"when a mobile device is encountered during an investigation, many questions arise: What is the best method to preserve the evidence? How should the device be handled? How should valuable or potentially relevant data contained on the device be extracted? The key to answering these questions begins with a firm understanding of the hardware and software characteristics of mobile devices"* [10]. Various methods, tools, and techniques are available and being used during digital forensic evidence extraction, this range from manual acquisition, logical, physical and files systems methods using a range of various software tools [12]. Mobile phones are portable devices that are made for a specific function rather than computers which are made for a more general application, therefore, mobile phone hardware architecture is built with mobility, extended battery life, simple functionality and light weightiness in mind, an understanding of the general characteristics of a mobile phone is important especially in the way it stores the OS, how its processor behaves and how it handles its internal and external memory [10], [13].

Forensic documentation process should be simultaneously and consistently done with examination and retention of notes according to set policies, [10], [15], [16] suggests that "documentation process should consider 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, inclusion of notes about dates, times, and descriptions and results of actions taken, irregularities encountered and any actions taken regarding the irregularities during the examination, information, such as network topology, list of authorized users, user agreements, and/or passwords, documenting the operating system and relevant software version and current, installed patches, regarding remote storage, remote user access, and offsite backups".

2. REVIEW OF RELATED WORKS

Several authors and researchers have proposed various process models for the extraction of digital evidence, specifically those related to this study are presented below;

The research by [17] presents the development in the field of digital forensics covering areas such as Data Acquisition, Operating Systems, and Data types, they also emphasized the need for standardization in the field especially Android forensics, Blackberry forensics, iOS forensics, Windows mobile forensics, and multiple OS forensics. Similarly [18] discussed the Smartphone digital evidence forensics standard operating procedure and compares it with those developed by [10] with consideration of third party forensics tools used to collect, examine and analyze the digital evidence. In these proposed models emphasis was put on the process models followed in evidence collection from evidence intake, preparation, analysis up to reporting. However, [19] discussed the challenges of important stages in the investigation process of mobile forensics and this was supported by research of [20] who developed the Harmonized Digital Forensics Investigation process model (HDFI), this model was tested on android operating system/platform and yielded satisfactory results, however different mobile devices running various operating system other than android would show different results since the demand for digital evidence may vary from device to device, therefore, a standard well-documented process should help the investigator in extraction and analysis of digital evidence across multi-facet of operating system platforms.

Generally speaking, mobile devices forensics suffers from challenges in data acquisition and preservation as a result of many process models offered by different vendors [21]. The "*Systematic Digital Forensic Investigation Model*" proposed by [22], compared different process models and provided a mechanism upon which different frameworks can be implemented on the basis of technology, it is clear that this model is technology-based and therefore does not address the `challenges of inconsistencies raised by various platforms. Further [23] presented "*Modeling the Forensics Process*" in which the authors proposed a model with major stages that would be helpful in separating the flow stream, according to them, these stages comprise of creation, release, transfer, arrive, accept, and process. In this model the authors introduce totally new phases in mobile devices forensic evidence extraction. Finally "*Models of Models: Digital Forensics and Domain-Specific Languages*" proposed by [24] focused on domain-specific languages as very important part of digital forensic evidence investigation and extraction, their concern was on the domain/or platform used.

3. RESEARCH METHODOLOGY

3.1 Data source

Initial respondents from ICT practitioners, Law enforcement, Regulatory authorities, Researchers and Business community within Kampala city were first identified. Progressively other respondents with knowledge were identified which eventually increased the sample size. Literature review on digital evidence extraction process model for mobile devices formed the basis for the development of the questionnaire consisting of 65 questions from 8 sub-themes/constructs.

3.2 Data Gathering Technique

The primary survey instrument for data collection was a self-administered questionnaire. The key advantage of questionnaire is the ability to cover a wide area of the target population and offering standardized form of responses [25]. It is further asserted that questionnaires are familiar to most people and generally do not make people apprehensive [26] and they also reduce bias and can be completed at the respondent's convenience. All the 65 questions were of five-point Likert scale type in nature, ranging from strongly disagree to strongly agree with a neutral option constructed to cater to those uncertain of their choices.

3.3 Sampling

Due to the technicality of the subject matter regarding digital forensics, the researchers adopted the non-probability based snowballing sampling technique where respondents identified by the researchers referenced other people with knowledge and expertise in digital forensics to form the basis of research data [25].

3.4 Data Analysis

The data analysis involved classifying and uniquely identifying the responses. Using SPSS (version 23), descriptive statistics were generated and reliability tests and regression analysis conducted in order to analyze and present the research data obtained from the questionnaires. The researchers adopted the regression analysis approach in order to model and analyze the relationship between the dependent variable operating system platform and several independent variables as seen later in the discussion of results [27], [28]**.**

4. RESULTS AND DISCUSSION

A total of 85 responses were obtained from the 130 questionnaires sent out within the specified duration. Thus, a response rate of 65.4% was achieved, which is comparable to response rates from similar recent studies on immerging technology studies conducted by some scholars such as Dwivedi, Yogesh in 2006.

Table 1: Demographic characteristics of respondents (N=85)

Variables	Intermediate variables	Frequency	Percent %
Gender	Male	51	60
	Female	34	40
Age group	20-30	21	24
	30-40	37	43.5
	40-50	26	30.6
	50+	1	1.2
Employment Sector	Law Enforcement Agency	14	16.5
	Regulatory Authority	7	8.2
	Business community	14	16.5
	Researcher	19	22.4
	ICT Practitioners	31	36.5
Educational Background	Bachelors	42	49.4
	Masters	31	36.5
	Doctorate	12	14.1

From table 1, a male had a response rate of 60% while female contributed 40%, it is also clear that 43.5% of the respondents were people within the age bracket of 30-40 with only one respondent being above 50 years of age. The majority of respondents were ICT practitioners reflecting 36.5% followed by Researchers 22.4% and regulatory authority accounted for the least respondents at 8.2%. Most respondents were people with a bachelor's degree qualification amounting to 49.4% closely followed by those who hold masters degree qualification while those with doctorate stood at 14.1%. Mainly males and ICT practitioners with at least a bachelor's degree qualification dominated the list of respondents. These demographics information are consistent with those used in similar studies on emerging technologies conducted in 2006 by Dwivedi and Yogesh.

Table 2: Reliability Test of constructs using Cronbach's coefficient (alpha)

Construct	No. of Items	Cronbach's Alpha
Policy Factors	7	0.591
Operating system platform	4	0.741
Device factors	4	0.640
Extraction Method factors	15	0.781
Data type factors	11	0.807
Nature of Data factors	5	0.778
Forensics Extraction tools	9	0.850
Forensics Documentation process	10	0.640

[27] suggest four ranges for the reliability coefficient α; excellent reliability (α >=0.90), high reliability (0.70 < α < 0.90), moderate reliability (0.50< α< 0.70), and low reliability (α<= 0.50). In general, the higher the Cronbach's α value of a construct, the higher the reliability is of it measuring the same construct. In this study, Cronbach's α varied between 0.807 for the Forensics Extraction Tools (FET) constructs and 0.591 for Policy Factors (PF) constructs. Forensics Extraction Tools (FET) constructs expressed the highest reliability (α =0.850), closely followed by Data Type constructs (α =0.807), Extraction Method factors(EM) (α =0.781), Nature of Data factors(ND) (α =0.778), Operating system platform(MDF) (α =0.741), While Forensics Documentation Process (FDP) and Device factors (DF) both had (α =0.640), and finally Policy Factors (PF) (α =0.591). Considering [27], the aforementioned values suggest that of the eight (8) constructs, five passed the high reliability and the remaining three demonstrated moderate reliability. The implication is that all the constructs were internally consistent. Consequently, all items of each construct measured the same. For example, all items of Device factors measured the same content. Similarly, all items of Forensic Documentation measured the same.

Table 3: Descriptive Statistics for constructs and their rankings

	N	Mean	Std. Deviation	Rank
Policy Factors	85	4.36	.386	1
Device Factors	85	4.21	.556	2
Forensic Documentation Process	85	4.11	.434	3
Data Type Factors	85	4.11	.564	4
Extraction Method Factors	85	4.01	.456	5
Nature of Data	85	3.90	.624	6
operating System Platform	85	3.80	.855	7
Forensic Extraction Tools	85	3.08	.946	8
Valid N (listwise)	85			

The descriptive statistics here give a clear view how these constructs were ranked based on the mean responses with Policy Factors coming out significantly with mean response of 4.36 followed by Forensics Documentation Process and Forensics Extraction Tools had the least mean response. This implies that where there are clear policies regarding the handling, acquisition, preservation, documentation, and presentation of digital evidence, then there should be minimal inconsistencies in mobile devices' digital evidence extraction process model. This is followed by forensics documentation process suggesting concurrence with recent studies citing a lack of clear technical documentation of existing process models of mobile devices digital evidence extraction methods [9]. Forensic extraction tools are ranked last among the eight constructs, this could be attributed to the fact that there are several digital evidence extraction tools and most investigators face challenges in choosing the correct tool for digital evidence extraction in mobile devices [3].

Table 4: Descriptive Statistics for level of involvement with various mobile device operating system platform

	Android		Windows		Apple iOS		Blackberry OS	
	Frequency	Percent	Frequency	Percent	Frequency	Percent	Frequency	Percent
Not Involved	3	3.5	4	4.7	12	14.1	21	24.7
Little involvement	4	4.7	1	1.2	4	4.7	2	2.4
Involved	5	5.9	16	18.8	20	23.5	22	25.9
Much Involved	22	25.9	41	48.2	22	25.9	24	25.2
Highly Involved	51	60.0	23	27.1	27	31.8	16	18.8
Total	85	100.0	85	100.0	85	100.0	85	100.0

From table 4 above the intention of the research was to determine the level of involvement of various stakeholders with the four major mobile devices operating systems as per the market share [4], and it is indicated 60% had high level of involvement with digital evidence extraction from Android platform closely followed by 25.9% of those who had much involvement, only 3.5% registered not having been involved with android, this could be attributed to the fact that Android commands the largest market share [4], [30]. Windows operating system registered 27% of those with high level involvement closely followed by 48.2% of those with much level of involvement while 4.7% of the respondents indicated not having involved themselves with windows operating systems, the statistics of respondents involvement can be attributed to windows command of the market share as the second largest after android [31]. Apple iOs posted a 31.8% high involvment and 14.1% no involment, a factor which points towards their use of propriatory tools for digital evidence extraction and also the market share they command [32].

Blackberry operating system registered the least number of respondents who had high involvement with their operating system standing at 18.8% and highest number of those who had no involvement at all standing at 21.0% this can be attributed to the market share they command and also the built-in security in blackberry operating system which makes it very hard to access digital evidence stored in this platform [4]. From this results the implication is that since most mobile devices digital evidence extraction tools are vendor based [21], [33], an understanding of people who have interacted with all these tools can give clear view of what model can be developed that caters for all the four major operating systems, an average of respondents are highly involved and much involved in these four major operating systems standing at 34.4% and 31.3% respectively signifying the need to develop a multiplatform model to cater for these four major operating ststems.

Table 5: Correlation of individual operating systems and independent constructs

		P F	D F	E M	DTF	N D	FET	FDP
Android	Pearson Correlation	-.034	.101	.210	.036	.130	.178	.268*
	Sig. (2-tailed)	.755	.357	.054	.741	.237	.104	.013
	N	85	85	85	85	85	85	85
Window	Pearson Correlation	.132	.199	.421**	.221*	.236*	.285**	.229*
	Sig. (2-tailed)	.230	.068	.000	.042	.030	.008	.035
	N	85	85	85	85	85	85	85
Apple iOS	Pearson Correlation	.073	.364**	.496**	.032	.318**	.524**	.404**
	Sig. (2-tailed)	.507	.001	.000	.768	.003	.000	.000
	N	85	85	85	85	85	85	85
Blackberry operating system	Pearson Correlation	-.116	.190	.306**	-.221*	.325**	.667**	.008
	Sig. (2-tailed)	.291	.081	.004	.042	.002	.000	.944
	N	85	85	85	85	85	85	85

Key: ***PF****-Policy Factor,* ***DF****- Device Factors,* ***EM****-Extraction Method,* ***DTF****-Data Type Factors,* ***ND****- Nature of Data,* ***FET****-Forensic Extraction Tool and* ***FDP****-Forensic Documentation Process*

Table 5 shows how different individual operating system platforms relate with various constructs; from this table it indicates that Forensic Documentation process (FDP) has significant correlation with Apple iOS, at .404 (40.4%), closely followed by Android at .268 (26.8%), windows at .229 (22.9%) while Blackberry had the least significant correlation at .008 (0.08%). Forensics Extraction tools (FET) posted a significant correlation with Apple iOS and Blackberry operating system at .524(52.4%) and .667(66.7%) respectively, Windows came third with .285 (28.5%) and Android trailed with .178 (17.8%). Data type showed the least correlation across all the four-operating system platform closely followed by Policy factors. From this table the implication is that FET, FDP, EM and ND are more significant factors in understanding how they influence evidence extraction in mobile devices running such operating system platform, while given the fact that any of the four operating systems can have either the same or different kinds of data for example call logs, browser history, short message services or videos could explain the reason why data type posted the least significant correlation.

Table 6: Correlation- Operating system platform and independent variables

		OPS	P F	DF	E M	DTF	ND	FET	FDP
OPS	Pearson Correlation	1	.022	.321**	.479**	-.009	.369**	.609**	.277*
	Sig. (2-tailed)		.842	.003	.000	.938	.001	.000	.010
	N	85	85	85	85	85	85	85	85
**. Correlation is significant at the 0.01 level (2-tailed).									
*. Correlation is significant at the 0.05 level (2-tailed).									

Mobile devices operating system platform is the major focus here, the researchers found it necessary to determine how different factors that lead to mobile devices digital evidence process extraction models interact or relate with these operating systems so as to determine the metrics for the extraction of digital evidence from these operating systems.

From Table 6, above the researcher determined the correlation between Mobile devices operating systems platform and Devices factors for example (Device type, Release version, status of the devices among others), Extraction methods used (Manual, logical, physical, architecture, memory management among others), Nature of Data (hidden, visible, external and internal ,among others), Forensics Extraction Tools (vendor-based and open source) and Forensics documentation process (from seizure to presentation) as suggested by [16]. It is clearly shown that Forensics Extraction Tools and Forensics extraction Methods posted a strong correlation with Mobile operating systems at 0.609 and 0.479 representing 60.9% and 47.9% respectively, closely followed by Nature of Data and Device factors each standing at 0.369 and 0.321 representing 36.9% and 32.1% while Forensics Documentation Process posted a correlation of 0.277 representing 27.7%. Data type posted a negative correlation of -0.009 meaning data type does not in any way have any influence on the operating system as far as mobile devices digital evidence forensics process model extraction is concerned. From this table, the implication is that Forensics Extraction tools, Extraction methods, Nature of Data, Device type, and Forensics Documentation Process are the primary contributors to Extraction inconsistencies, thus supporting results from recent studies by [3].

Table 7: Regression Analysis: Influence of Independent Variables on Operating system

Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. The error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
	.783[a]	.613	.608	.535	.613	131.414	1	83	.000

a. Predictors: (Constant), extract cons

b. Dependent Variable: operating System Platform

From table 7, the model summary shows that Extraction inconsistencies which comprise of independent variables such as; Forensics Documentation Process (FDP), Forensics Extraction Tools (FET), Nature of Data (ND), Extraction Method factors (EM), Device factors (DF) and Policy factors (PF) correlated against Operating systems indicates that there is a significant correlation between operating system and Extraction inconsistencies, this result also supports conclusions by [3][16]

Table 8: ANOVA

Model		Sum of Squares	Df	Mean Square	F	Sig.
	Regression	37.624	1	37.624	131.414	.000[b]
	Residual	23.763	83	.286		
	Total	61.387	84			

a. Dependent Variable: operating System Platform
b. Predictors: (Constant), extract cons

Table 9: Coefficients

Coefficients[a]						
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
	(Constant)	-4.837	.756		-6.399	.000
	extract cons	2.066	.180	.783	11.464	.000

a. Dependent Variable: operating System Platform

The regression analysis was performed with operating system as the dependent variable extraction inconsistencies with sub-constructs (Extraction methods, Forensic Extraction Tools, Policy Factors, Device Factors, Nature of Data and Data type factors) as the predictor variable. From the analysis, a significant model emerged with adjusted R-Square .608 (Table 7) and hence the Predictor variable included in the analysis was found to be significant (Table 9).

5. DISCUSSION AND RECOMMENDATIONS

The Cronbach's α value of the various constructs ranging from 0.591 to 0.850 demonstrated the ability of the measure of internal consistency of the constructs used in this study by ensuring that none of the constructs fell below the moderate to high reliability test. The predictive power of the regression model of this study, with adjusted R-Square .608 (Table 9), indicates an appropriate level of explained variance [27]. This implies that the independent variables and constructs used in this study are significant in understanding the causes of digital evidence extraction process model inconsistencies in mobile devices running various operating systems platforms. The results of this study hence, generate a number of issues that may be of interests to ICT practitioners, Researchers, Law enforcement authorities, Regulatory Authorities and Business community to have a clear understanding of the factors that cause inconsistencies in digital forensics evidence extraction in mobile devices [6], [8], [34], [35].

Considering the study findings, it is evident that Forensic extraction tools, Forensics extraction methods, Nature of Data, Device factors, Forensic documentation process, and Policy factors are key contributors for the digital evidence process model extraction inconsistencies in mobile devices [7], [10], [16], [36]. These factors, therefore, may have effect on the credibility of the digital evidence in mobile devices. For example a clear understanding of the forensic extraction tool and forensic extraction method employed can help address the inconsistencies in digital evidence extraction, similarity having clear policy guidelines that tackle forensic documentation process, the Nature of data to be extracted, Device settings such as on-screen password, application blocking tools are key in addressing the inconsistencies in digital forensics evidence extraction models.

The level of involvement of various stakeholders with the four major operating systems used in the study also informs the study that majority were much more involved with Android operating systems, a factor attributed to it is being open source (Mrkaic, 2016; Nimodia & Deshmukh, 2012) and windows closely followed with Apple iOs coming third while Blackberry came last in that order, this, therefore, informs solution designers to consider a more cross-cutting tool that is able to have a clear process model with clear understanding of the architecture of these operating systems kernels to reduce the inconsistencies and develop a more consistent extraction process model.

6. CONCLUSION AND FUTURE WORK

The study identified several factors that lead to inconsistencies in digital evidence process extraction models in mobile devices, these factors in order of their rankings includes Forensics extraction tools used, Forensics extraction Methods applied, the Nature of Data, Devices factors and policy factors, all of which have a direct effect on the forensic documentation process. Key concern should be put on developing process models with consident and specified technical documentation. Future work will focus on utlization of these factors to identify metrics that can be used to develop a cosistent model that can be applied across the diverse devices running various operating system platform.

7. REFERENCES

[1] D. B. Garrie, J. D. Morrissy, Z. Ellman, and K. Llp, "Digital Forensic Evidence in the Courtroom: Understanding Content and Quality," *Northwest. J. Technol. Intellect. Prop. Vol.*, vol. 12, no. 2, pp. 122–128, 2014.
[2] S. Daware, S. Dahake, and V. M. Thakare, "Mobile forensics: Overview of digital forensic, computer forensics vs. mobile forensics and tools," *Int. J. Comput. Appl.*, vol. 2012, pp. 7–8, 2012.
[3] S. Yadav, K. Ahmad, and J. Shekhar, "Analysis of Digital Forensic Tools and Investigation Process," *High Perform. Archit. Grid …*, pp. 435–441, 2011.
[4] N. Ahmad, M. W. Boota, and A. H. Masoom, "Comparative Analysis of Operating System of Different Smart Phones," *J. Softw. Eng. Appl.*, no. March, pp. 114–126, 2015.
[5] J. Son, "Social Network Forensics : Evidence Extraction Tool Capabilities," AUT University, 2012.
[6] D. C. A. Murphy, "Developing Process for Mobile Device Forensics," 2009.
[7] F. Jafari and R. S. Satti, "Comparative Analysis of Digital Forensic Models," *J. Adv. Comput. Networks*, vol. 3, no. 1, pp.

82–86, 2015.
[8] ITU-HIPCAR, “Cybercrime/e-Crimes: Model Policy Guidelines & Legislative Texts,” 2012.
[9] T. Mehrotra and B. M. Mehtre, “Forensic analysis of Wickr application on android devices,” *2013 IEEE Int. Conf. Comput. Intell. Comput. Res. IEEE ICCIC 2013*, pp. 2–7, 2013.
[10] 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.
[11] 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.
[12] D. Abalenkovs *et al.*, “Mobile Forensics: Comparison of extraction and analyzing methods of iOS and Android,” pp. 1–13, 2012.
[13] 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.
[14] 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.
[15] 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.
[16] R. Ahmed, R. Dharaskar, and V. Thakare, “Digital evidence extraction and documentation from mobile devices,” *Int. J. Adv. Res. Comput. Commun. Eng.*, vol. 2, no. 1, pp. 1019–1024, 2013.
[17] K. Barmpatsalou, D. Damopoulos, G. Kambourakis, and V. Katos, “A critical review of 7 years of Mobile Device Forensics,” *Digit. Investig.*, vol. 10, no. 4, pp. 323–349, 2013.
[18] I. L. Lin, H. C. Chao, and S. H. Peng, “Research of digital evidence forensics standard operating procedure with comparison and analysis based on smart phone,” *Proc. - 2011 Int. Conf. Broadband Wirel. Comput. Commun. Appl. BWCCA 2011*, pp. 386–391, 2011.
[19] 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.
[20] A. Valjarevic and H. S. Venter, “Harmonised digital forensic investigation process model,” *2012 Inf. Secur. South Africa - Proc. ISSA 2012 Conf.*, 2012.
[21] M. Anobah, S. Saleem, and O. Popov, “Testing Framework for Mobile Device Forensics Tools DEVICE FORENSICS TOOLS,” *J. Digit. Forensics, Secur. Law Artic.*, vol. 9, no. 2, 2014.
[22] M. Agarwal and M. Gupta, “Systematic digital forensic investigation model,” *Int. J. Comput. Sci. Secur.*, vol. 5, no. 1, pp. 118–131, 2011.
[23] S. Al-Fedaghi and B. Al-Babtain, “Modeling the forensics process,” *Int. J. Secur. its Appl.*, vol. 6, no. 4, pp. 97–108, 2012.
[24] D. A. Ray and P. G. Bradford, “Models of Models : Digital Forensics and Domain-Specific Languages A Selection of Previous Work on Models of Dig- ital Investigation,” no. May, p. 108, 2007.
[25] C. Kothari, R. Kumar, and O. Uusitalo, *Research Methodology*. 2014.
[26] D. Silverman, *Doing Qualitative Research: Second Edition*. 2005.
[27] C. B. Perry R, Hinton, Isabella McMurray, *SPSS Explained Second Edition*. 2014.
[28] P. Surendran, “Technology Acceptance Model : A Survey of Literature,” *Int. J. Bus. Soc. Res.*, vol. 2, no. 4, pp. 175–178, 2012.
[29] Y. Dwivedi and A. Papazafeiropoulou, “Consumer Adoption and Usage of Broadband in,” 2006.
[30] Q. Jamil, “Analysis of Machine Learning Solutions to Detect Malware in Android,” in *The Six international conferencieon Innovative Computing Technology (INTECH 2016)*, 2016, pp. 226–232.
[31] O. O. Okediran, O. T. Arulogun, and R. A. Ganiyu, “Journal Of Advancement In Mobile Operating Systems and Application Development Platforms : A Survey Mobile communications devices have been the most adopted means of communication both in the developed and developing countries with its penetration more th,” vol. 1, no. 4, pp. 1–7, 2014.
[32] K. Divya and S. V. Krishnakumar, “Comparative Analysis Of Smart Phone Operating Systems ANDROID , APPLE iOS AND,” *Int. J. Sci. Eng. Appl. Sci.*, vol. 2, no. 2, 2016.
[33] J. Liang, B. C. I. S. Auckland, and N. Zealand, “Evaluating A Selection of Tools for Extraction of Forensic Data : Disk Imaging,” 2010.
[34] M. Yates and H. Chi, “A framework for designing benchmarks of investigating digital forensics tools for mobile devices,” *Proc. 49th Annu. Southeast Reg. Conf. - ACM-SE ’11*, p. 179, 2011.
[35] L. Aouad, T. Kechadi, and J. Trentesaux, “Chapter 11 An Open Framework For Smartphone,” in *In: Peterson G., Shenoi S. (eds) Advances in Digital Forensics VIII.*, IFIP Advan., Springer, Berlin, Heidelberg, 2012, pp. 159–166.
[36] R. S. Satti and F. Jafari, “Reviewing Existing Forensic Models to Propose a Cyber Forensic Investigation Process Model for Higher Educational Institutes,” *Int. J. Comput. Netw. Inf. Secur.*, vol. 7, no. 5, pp. 16–24, 2015.
[37] C. Nimodia and H. R. Deshmukh, “Android Operating System,” *Softw. Eng. ISSN 2229-4007 ISSN 2229-4015*, vol. 3, no. 1, pp. 10–13, 2012.
[38] I. mrkaić, “android forensic using some open source tools,” in *The Eighth International Conference on Business Information Security*, 2016, no. October.

