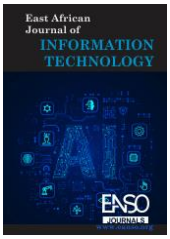
Article DOI: https://doi.org/10.37284/eajit.5.1.830



East African Journal of Information Technology
eajit.eanso.org
Volume 5, Issue 1, 2022
Print ISSN: 2707-5346 | Online ISSN: 2707-5354
Title DOI: https://doi.org/10.37284/2707-5354

EAST AFRICAN NATURE & SCIENCE ORGANIZATION

Original Article

Multi-platform Process Flow Models and Algorithms for Extraction and Documentation of Digital Forensic Evidence from Mobile Devices

Gilbert Gilibrays Ocen[1], Ocident Bongomin[2], Gilbert Barasa Mugeni[3], Stephen Makau Mutua[4] & Twaibu Semwogerere[1]*

[1] Busitema University, P. O. Box 236, Tororo, Uganda.
[2] Moi University, P. O. Box 3900 – 30100, Kesses, Eldoret, Kenya.
[3] Communication Authority of Kenya, P. O. Box, 14448 – 00800, Nairobi, Kenya.
[4] Meru University of Science and Technology, P. O. Box 972 – 60200, Meru, Kenya.
* Correspondence ORCID ID: https://orcid.org/0000-0002-2204-291X; email: gilbertocen@gmail.com.

Article DOI: https://doi.org/10.37284/eajit.5.1.830

Date Published: *07 September 2022*

Keywords:
Model Development, Extraction, Multiplatform Model, Model Validation, Algorithms, Operating Systems

ABSTRACT

The increasing need for the examination of evidence from mobile and portable gadgets increases the essential need to establish dependable measures for the investigation of these gadgets. Many differences exist while detailing the requirement for the examination of each gadget to help detectives and examiners in guaranteeing that any kind of evidence extracted/ collected from any mobile device is well documented and the outcomes can be repeatable, a reliable and well-documented investigation process must be implemented if the results of the examination are to be repeatable and defensible in courts of law. In this paper, we developed a generic process flow model for the extraction of digital evidence in mobile devices running on Android, Windows, iOS, and Blackberry operating systems. The research adopted a survey approach and extensive literature review as a means to collect data. The models developed were validated through expert opinion. Results of this work can guide solution developers in ensuring the standardization of evidence extraction tools for mobile devices.

APA CITATION

Ocen, G. G., Bongomin, O. Mugeni, G. B. Mutua, S. M. & Semwogerere, T. (2022). Multi-platform Process Flow Models and Algorithms for Extraction and Documentation of Digital Forensic Evidence from Mobile Devices. *East African Journal of Information Technology*, *5*(1), 84-105. https://doi.org/10.37284/eajit.5.1.830

CHICAGO CITATION

Ocen, Gilbert Gilibrays., Ocident Bongomin, Gilbert Barasa Mugeni, Stephen Makau Mutua and Twaibu Semwogerere. 2022. "Multi-platform Process Flow Models and Algorithms for Extraction and Documentation of Digital Forensic Evidence from Mobile Devices". *East African Journal of Information Technology* 5 (1), 84-105. https://doi.org/10.37284/eajit.5.1.830.

 This work is licensed under a Creative Commons Attribution 4.0 International License.

Article DOI: https://doi.org/10.37284/eajit.5.1.830

HARVARD CITATION

Ocen, G. G., Bongomin, O. Mugeni, G. B. Mutua, S. M. & Semwogerere, T. (2022) "Multi-platform Process Flow Models and Algorithms for Extraction and Documentation of Digital Forensic Evidence from Mobile Devices", *East African Journal of Information Technology*, 5(1), pp. 84-105. doi: 10.37284/eajit.5.1.830.

IEEE CITATION

G. G. Ocen., O. Bongomin G. B. Mugeni S. M. Mutua & T. Semwogerere "Multi-platform Process Flow Models and Algorithms for Extraction and Documentation of Digital Forensic Evidence from Mobile Devices", *EAJIT*, vol. 5, no. 1, pp. 84-105, Sep. 2022.

MLA CITATION

Ocen, Gilbert Gilibrays., Ocident Bongomin, Gilbert Barasa Mugeni, Stephen Makau Mutua & Twaibu Semwogerere "Multi-platform Process Flow Models and Algorithms for Extraction and Documentation of Digital Forensic Evidence from Mobile Devices". *East African Journal of Education Studies*, Vol. 5, no. 1, Sep. 2022, pp. 84-105, doi:10.37284/eajit.5.1.830.

INTRODUCTION

Attempts to use a range of mobile forensic tools and process models to extract information from multiple devices have yielded conflicting results [1]–[3]. Therefore, special attention should be paid to ensure that the methods are correct so that usability improvement can be achieved [4]. The overriding importance of documentation approaches is that they can allow an investigator to remember the steps taken to gather information, which in turn reduces allegations of mishandling [5].

The scientific work of most researchers confirms that forensic science suffers from a lack of documentation and transparency [6]. Therefore, standard and well-researched approaches to documentation and extraction are key. The purpose of the documentation is to facilitate the extraction process in legally acceptable ways [7], [8]. While the investigator would do well to extract the necessary information using the tools available, further details on the information could only be useful for judicial proceedings [9].

The term digital forensics refers to the process of retrieving and examining documents from digital devices, primarily involving computer crime or cybercrime [10], [11]. The role of forensic science is to use investigative methodologies, measures, and frameworks to extract, preserve, collect, analyze, and provide [12] scientific and technical scraps of evidence to criminal or civil courts and tribunals. to organize a good documentation of the prosecutions. On the other hand, digital forensics is the practice of finding, securing, examining and presenting evidence in a legally acceptable manner [12]. These definitions are supported by [13] who state that digital evidence is considered investigatively relevant material and records that are stored, delivered, or transmitted via an electronic device.

The steady industrial growth and growing popularity of mobile digital devices amplify the challenges, conditions and scenarios for investigators and prosecutors around the world. The existence of different tools and systems with different process models makes it difficult even for a trained investigator to select a suitable forensic tool to seize internal files of mobile devices [14]. Many forensic models emphasize auditing of certain operating system platforms [15], ignoring a more critical aspect of consistency and documentation of the approaches and steps taken. While [16] listed many forensic techniques for preserving evidence from the point of view of efficiency in the general forensic context for extracting and documenting evidence from mobile devices. Little effort has been made regarding the methodological documentation and the consistency of the process models followed when extracting this information. While [17] notes that despite growing awareness and research on forensic practice, explanation and implementation are still inconsistent in the digital forensic community, a topic supported by recent research such as [9], [18], [19].

Continuously changing technological and industry developments, coupled with the myriad of complexities caused by today's demand for information from mobile devices, present forensic investigators with serious adaptive challenges to standardize and adopt acceptable models that can be used to detect this in order to counter the growing demand [20], [21].

The reliability of the evidence is directly anchored to the investigative processes adopted. Therefore,

 This work is licensed under a Creative Commons Attribution 4.0 International License.

Article DOI: https://doi.org/10.37284/eajit.5.1.830

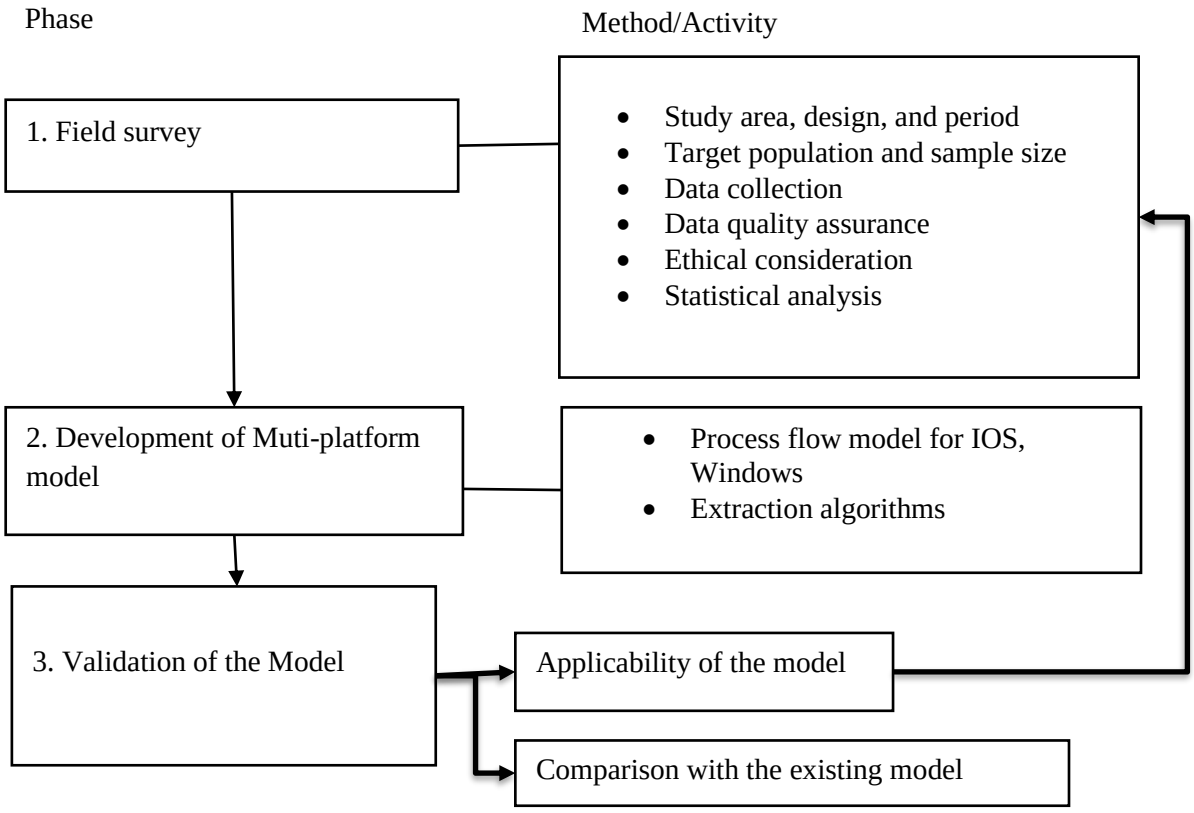
choosing to avoid a step can lead to insufficient evidence and increase the risk of denying that step in a legal proceeding [22]. Currently, no standard or universally accepted process model has been developed that can be used to obtain evidence from mobile devices, and the vibrant expansion of smart devices suggests that every forensic investigator will need to use all independent models needed to gather information and keep [23].

Existing models cannot meet the growing demands for digital evidence resulting from the growing use of mobile devices and the complexity that persistent criminals bring to the use of these devices. Therefore, some of these models focus on a specific step of the mining process or depend on the operating system platform [24], Based on existing research in digital forensics, process models can be used to collect evidence on mobile devices. In general, the literature specifies the requirements that guide and measure the process of extracting digital evidence in mobile devices and their performance. These include reliability and validity, guidelines, extraction methods, nature of data, type of data, technical documentation, and forensic extraction tools.

METHODOLOGY

The present study was performed in four steps depicted in *Figure 1*. In the first phase, the literature on specific email security techniques was reviewed, in phase two, the algorithm was developed and in phase three, the algorithm was evaluated using questionnaires selected from the participants and a SWOT analysis was carried out in the last phase.

Figure 1: Methodology Approach.



 This work is licensed under a Creative Commons Attribution 4.0 International License.

Article DOI: https://doi.org/10.37284/eajit.5.1.830

Field Survey

Study Area, Design and Period

The research was conducted in Kampala, Uganda, as this is where the researcher found most of the respondents with knowledge of the subject. From this position, the investigator was able to identify law enforcement such as police, bailiffs, computer forensics experts and professionals, evidence mining and computer forensics investigators, mobile telecommunications, and banking sectors that have various forms of crime /fraud. departments for investigating crimes related to the use of technology. The cross-sectional study design was used in this study over a one-year period from 2018 to 2019.

Population and Sample Size

The study population was comprised of law enforcement respondents, specifically Uganda Police (Crime Intelligence and Investigation Department (CIID), the prosecution service), court officials (lawyers, registrars, judges and magistrates) , policy makers, people regulators such as; Uganda Communications Commissions (UCC), National Information Technology Authority Uganda (NITA-U), a business community made up of telecommunications operators such as Mobile Telecommunication Network (MTN-Uganda), Airtel Uganda as these are the largest telecommunications service providers offering financial services, banks such as Stanbic Bank, Centenary Bank, Barclay's Bank Uganda and Standard Chartered Bank, as these are the largest providers of online transaction systems using some of the mobile digital devices in their operations. In addition to the snowball sampling tool, targeted/forensic sampling was used to complement targeted sampling, especially when examining different operating system platforms, inconsistencies and from the technical documentation of mining process models, while simple random and stratified sampling was used for probability sampling because the researcher collected data from different sectors and classified them into different strata and sampling simple random has been applied. The sample population was determined using the sample table of Krejcie and Morgan [26] derived from the formula. Krejcie and Morgan's sample size calculation presented in Table 1 was based on $p = 0.05$, where the probability of making a Type I error is less than 5% or $p < 0.05$ [26].

Table 1: Sample size determination using Krejcie and Morgan sampling technique

Sector	Population size	Sample size
Law Enforcement Agencies	10	7
Regulatory Authorities	20	11
ICT experts	100	63
ICT Researchers	20	11
Policymakers	30	16
Business communities	70	31
Total	200	130

It is clear that the population size of 10 was considered for law enforcement agencies, and the sample size of 7 was used. While large number of the respondents came from ICT experts with the sample population of 100 and the sample size of 63. This was followed by the business community (people in the banking industry, telecommunication agencies) with the population size of 70, and the sample size of 31.

Data Collection

Questionnaires and interviews were used in this study. The questionnaires covered a wide range of segments of the selected population, provided a consistent form of response, reduced bias, did not make people anxious, and were completed at the discretion of the respondent [27]. Questionnaires were designed for different categories of respondents such as policymakers, law enforcement, researchers, ICT experts, regulators

 This work is licensed under a Creative Commons Attribution 4.0 International License.

Article DOI: https://doi.org/10.37284/eajit.5.1.830

and the business community to obtain different types of data from these categories of respondents. Questionnaires were developed based on understanding gained from the literature reviewed in areas such as mobile devices, operating systems, platforms, technical documentation, inconsistency and complexity of process models as independent variables, and a cross-platform digital extraction process model for mobile device forensic evidence. The questionnaires were designed using the standard five-point Likert scale ranging from strongly agree to strongly disagree. The interviews were used to complement the questionnaires and were tightly structured, conducted primarily for information and communication technology (ICT) experts within law enforcement, policy makers, regulators and industry, as well as for those in the data recovery and forensic departments of agencies such as telecommunications networks, the banking sector and researchers in the field of digital banknote forensics.

Data Quality Assurance

The term "reliability" is used to describe the "repeatability" or "consistency" of the measure [28]. The internal consistency reliability methodology was used in this study. According to Chen [29], the internal consistency method uses a single measure administered once to a group of people to estimate reliability. The reliability of the tool is assessed by estimating how well elements with the same construct produce comparable results. Cronbach's alpha (α) coefficient was chosen as the best approximation to estimate the reliability of the constructs by examining the internal consistency of the measure. As indicated by Spencer [30], there are four types of reliability coefficients α; excellent reliability ($\alpha >= 0.90$), high reliability ($0.70 < \alpha < 0.90$), moderate reliability ($0.50 < \alpha < 0.70$) and low reliability ($\alpha <= 0.50$). All constructs used in this study passed the reliability test as shown in Table 2.

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

Construct	No. of Items	Cronbach's Alpha
Policy Factors (PF)	7	0.591
Operating system platform (MDF)	4	0.741
Device factors (DF)	4	0.640
Extraction Method factors (EM)	15	0.781
Data type factors (DT)	11	0.807
Nature of data factors (ND)	5	0.778
Forensics Extraction tools (FET)	9	0.850
Forensics Documentation process (FDP)	10	0.640

In this study, the highest Cronbach's alpha (α) of 0.850 was achieved by the FET constructs, while the lowest was achieved by the PF constructs ($\alpha = 0.591$). As reported by Perry et al [28], these figures indicate that out of 8 constructs, 5 had high fidelity, while three 3 had moderate fidelity, implying that the constructs were internally consistent. Therefore, all elements of each construct were measured equally. Although the validity of the instruments was determined using the Content Validity Index (CVI), it was performed on the constructs to ensure that the elements of the scale were meaningful to the sample and to record the measured problems. The measurement tools were then tested to ensure their quality and validity; This happened after conducting a pilot study with 30 questionnaires. The content validity indices of the three experts are 0.982, 0.964 and 0.967. Therefore, it was observed that the content validity coefficients were >0.6 and therefore the scales used to measure the study variables were consistent. Moreover, it is valid because a Cronbach's alpha greater than 0.5 is considered moderate validity and greater than 0.90 excellent validity. In this study, all variables were greater than 0.50, indicating good to excellent validity, meaning that all constructs and sub-indices in this study passed the validity tests.

Ethical Consideration

Ethical approval for the survey was obtained from the Institutional Research Ethics Board of Busitema University and informed consent from respondents prior to their voluntary enrolment in the study.

 This work is licensed under a Creative Commons Attribution 4.0 International License.

Article DOI: https://doi.org/10.37284/eajit.5.1.830

Ethical aspects such as data protection and respondent confidentiality were ensured [31]. Additionally, the letter was acquired by the university, which served as an introductory document for various organizations and individuals involved in this research. It has also been guaranteed that the developed mining model does not perform any unintended/unknown activity on users' devices.

Statistical Analysis

The analysis was performed using Statistical Package Software for Social Scientist (SPSS) version 20.0 (SPSS, Chicago, Illinois) and descriptive statistics were used to extract results from the analysis of all study variables. Descriptive statistic was performed for all the constructs to determine their significance using the mean responses. This was then used to obtain the ranking as per the number of responses from the participants who were contributors to inconsistencies in mobile device evidence extraction process models. Regression analysis was done with consistency metric (CM) as the dependent variable and constructs including EM, FET, PF, DF, ND, and DTF as independent variables.

Model Development

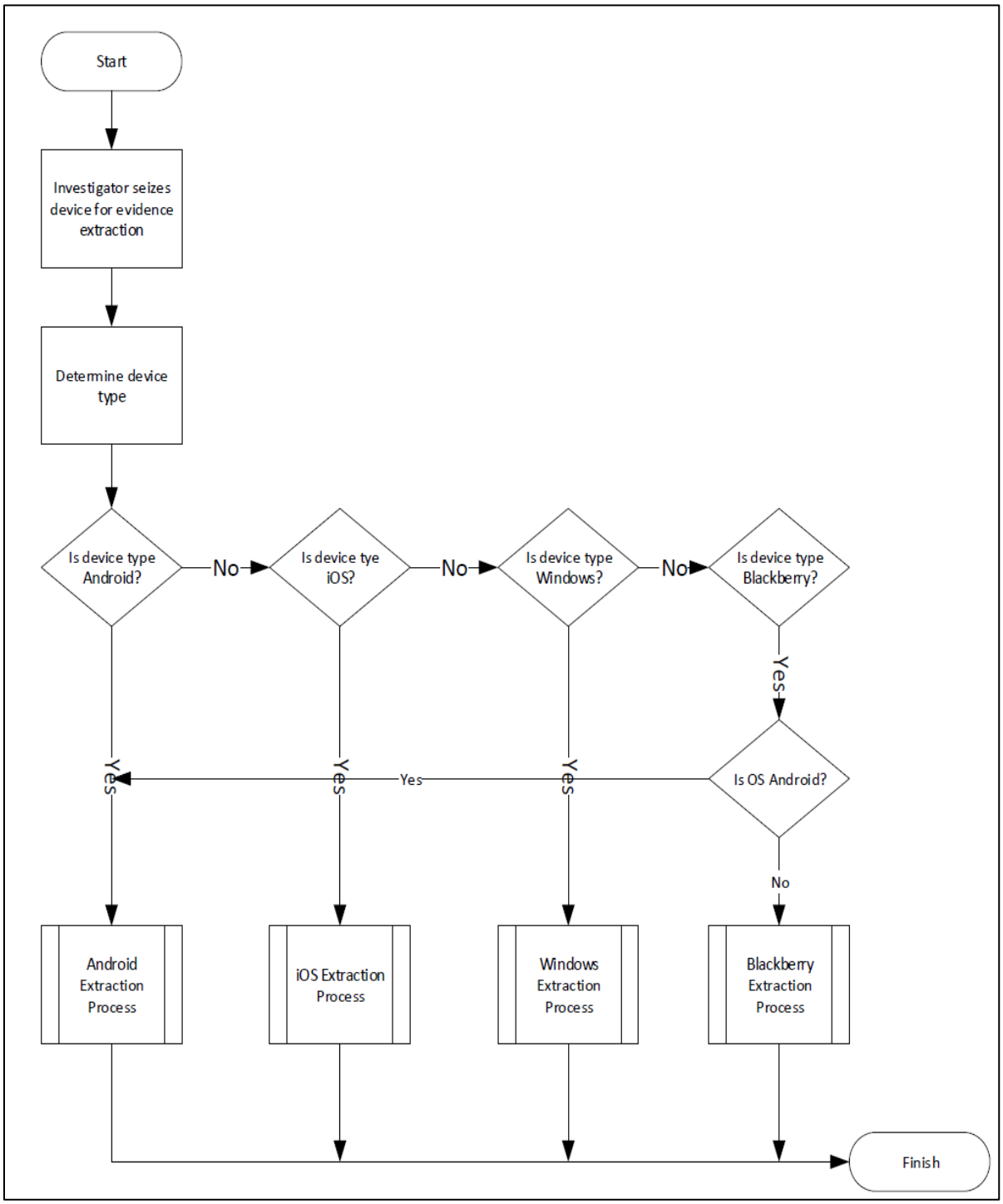
Multi-Platform Flow Model

The model design and validation involving the use of the business process, model development, analytical hierarchy approach (AHA), and experimental and experts' opinion used to validate the developed model. An experimental setup was conducted to test the process model developed to check for consistency in the extraction process models. The process flow for the multi-platform model is depicted in *Figure 2*. The individual flow models for the iOS and Windows mobile devices are presented in *Figure 3* and *Figure 4*, respectively.

 This work is licensed under a Creative Commons Attribution 4.0 International License.

Article DOI: https://doi.org/10.37284/eajit.5.1.830

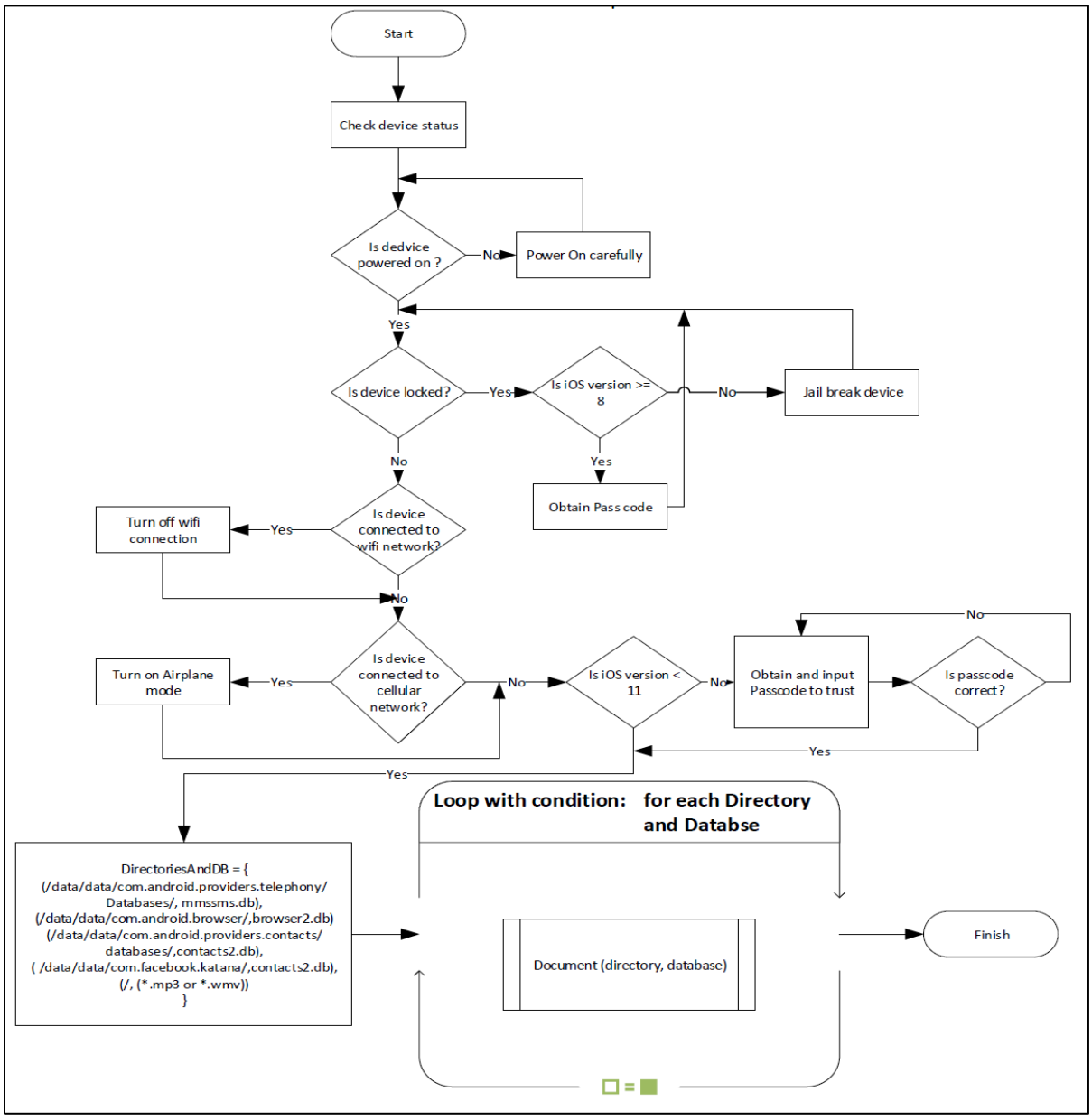
Figure 2: Process flow for the multi-platform model.



 This work is licensed under a Creative Commons Attribution 4.0 International License.

Article DOI: https://doi.org/10.37284/eajit.5.1.830

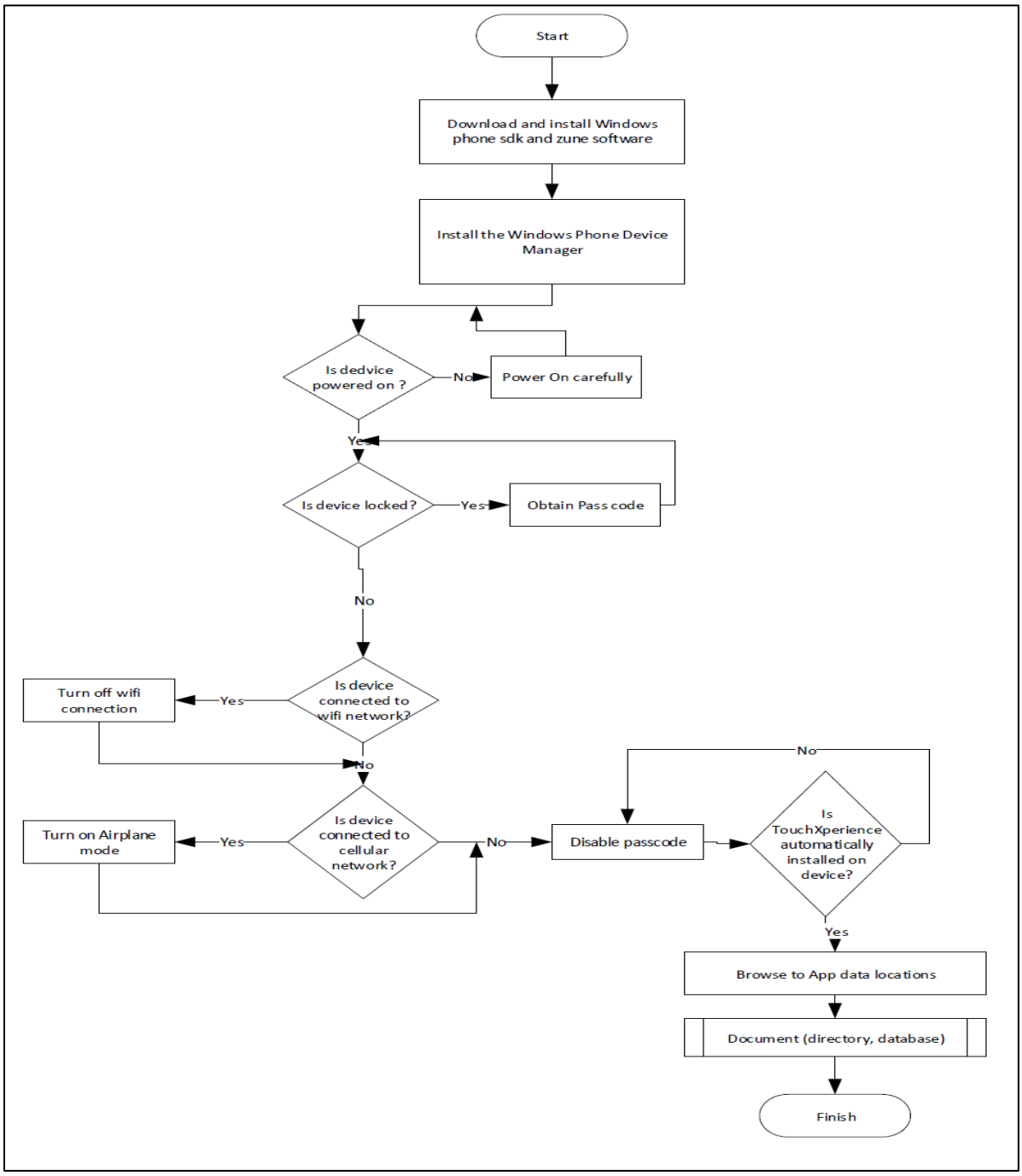
Figure 3: Process flow model for the case of IOS



 This work is licensed under a Creative Commons Attribution 4.0 International License.

Article DOI: https://doi.org/10.37284/eajit.5.1.830

Figure 4: Process flow of multi-platform model for the case of Window OS



Description of Extraction Algorithms

First and foremost, the gadget is seized for evidence extraction. A check is made to determine what type of operating system it is running. In case of Android OS, the Android extraction process is performed under the Extract From Android (SiezedDevice). It starts with checking the status of the gadget like power, Wi-Fi connection and cellular network. This action is performed on all gadgets to ensure that each gadget has power and does not have network connection issues. After this check, Universal Serial Bus debugging is enabled through developer options, screen timeout is prolonged, and root access is achieved. Then, different directories/

 This work is licensed under a Creative Commons Attribution 4.0 International License.

Article DOI: https://doi.org/10.37284/eajit.5.1.830

locations are browsed to obtain the SQLite database that can be opened to collect evidence that is documented using Documents (directory dictionary). The procedure is followed in similar steps, while the documentation is guaranteed to allow for consistency.

In the case of an iOS, as depicted in *Figure 5*, Extract From iOS (SiezedDevice) is trailed with the same action of having the gadget status checked; however, the difference with this extraction happens when connecting to a personal computer where a trusted code is required between the device and computer for the cases of iOS11 and above. Documentation occurs through (directory, dictionary). During extraction from Windows devices, as shown in *Figure 6*, Extract From Windows (SiezedDevice) is activated, which necessitates installing windows phone SDK and Zune software, the windows phone device manager. The gadget status checking is done. Once the gadget is connected to the workstation, the automatic installation of Touch Xperience on the phone is follows. This allows various directories to be browsed and several files accessed, and the documentation is followed by Documents (directory dictionary).

Finally, for BlackBerry-based gadgets, there are relatively small variations from other devices; Extract from BlackBerry (SiezeDevice) is done, and information /data is acquired from backup files as opposed to the device itself since its security complexity. BlackBerry Desktop Software is installed and opened, which detects a blackberry device and creates backup files. The files are browsed for evidence which is documented in Documents (directory dictionary).

Figure 5: Extraction algorithm for IOS

```
ExtractFromiOS(SiezedDevice)
        CheckDeviceStatus
        If siezedDevice is powered on
                If siezedDevice is unlocked
                        If siezedDevice is connectedToWifi network
                                TurnOff wifi connection
                        Else
                                If siezedDevice is connectedToCellular network
                                        Turn On Airplane Mode
                                Else
                                        if siezedDevice.iOS Version< 11
                                                Obtain and input passcode in workstation to trust
                                        Else
                                                DirectoriesAndDB = {

        (/data/data/com.android.providers.telephony/Databases/, mmssms.db),
                                                                (/data/data/com.android.browser/,browser2.db),

        (/data/data/com.android.providers.contacts/databases/,contacts2.db),
                                                                ( /data/data/com.facebook.katana/,contacts2.db),
                                                                (/, (*.mp3 or *.wmv))
                                                                                }
                                                foreach((directory,dictionary) in DirectoriesAndDB)
                                                        Document(directory,dictionary)
                Else
                        If siezedDevice.iOS Version >= 8
                                Obtain Passcode
                        Else
                                JailBreak Device
        Else
                Power on siezedDevice
```

 This work is licensed under a Creative Commons Attribution 4.0 International License.

Article DOI: https://doi.org/10.37284/eajit.5.1.830

Figure 6: Extraction algorithm for Window OS.

```
ExtractFromWindows(SizdDevice)
        Download and install Windows phone sdk and zune software
        Install the Windows Phone Device Manager
        If siezedDevice is powered on
                If siezedDevice is unlocked
                        If siezedDevice is connectedToWifi network
                                TurnOff wifi connection
                        Else
                                If siezedDevice is connectedToCellular network
                                        Turn On Airplane Mode
                                Else
                                        Disable passcode
                                        If TouchXperience automatically installed on device
                                                Browse to App data locations and obtain
directories and dictionaries
                                                foreach((directory,dictionary) in
DirectoriesAndDB)
                                                        Document(directory,dictionary)

                Else
                        By Passcode
        Else
                Power on siezedDevice
```

Validation of the Model

The developed model was validated using two approaches, namely, experts' opinions and literature comparison. In the first approach, expert opinion was based on the model applicability and functionality. The experts used were purposely selected from information technology, information security and computer forensic and network security fields, law enforcement agencies, solution developers as well as researchers in the field of computer and digital forensics. The second approach was through comparison with the previous models in the literature.

Applicability and Functionality of the Model

Descriptive statistics were used to assess the applicability of the model in measuring the state of process models (digital forensic evidence extraction) for mobile devices, based on the feedback from the experts in the fields of digital forensic evidence extraction. The model validation based on applicability using descriptive statistics is depicted in *Table 3*.

Table 3: Model validation based on the applicability

Variables	**SD/D/NS**		**A/SA**	
	f	**%**	**f**	**%**
1. Do you understand this model with ease?	3	20.0	12	80.0
2. Can you use/apply this model with ease?	3	20.0	12	80.0
3. Do you consider the factors leading to the measuring of the digital forensic evidence extraction process model logically arranged?	0	0.0	15	100.0
4. Is the explanation of the various modules within this model clear?	4	26.7	11	73.3
5. Is there independence among these modules?	2	13.7	13	86.3
6. Does the model guide the measuring of digital forensic evidence extraction process models for mobile devices?	0	0.0	15	100.0
Average	0.8	13.4	13	86.6
SD= Strongly Disagree, D = Disagree, NS= Not Sure, A= Agree and SA= Strongly Agree				

 This work is licensed under a Creative Commons Attribution 4.0 International License.

Article DOI: https://doi.org/10.37284/eajit.5.1.830

The analysis of all elements within the applicability of the developed model shows that 86.6% of the participants confirmed the applicability of the developed digital forensic evidence extraction model in driving the digital forensic evidence extraction process for mobile devices. On the other hand, only 13.4% of the participants disagreed on the applicability of this model in digital forensic evidence extraction process models for mobile devices. The results amply demonstrate the applicability of the model in the process of extracting digital forensic evidence for mobile devices, with 86.6% embracing it. On the other hand, the functionality of the developed Digital Forensic Evidence Extraction Process Model was validated as depicted in *Table 4*. It was observed that 6.4% of the respondents had a positive view about the model's ease of use. In the same way 8.5% of the participants confirmed independence among the several modules within the model and that the model is applicable in the digital forensic evidence extraction process for mobile devices, and that it uses a simple language.

Table 4: Model validation based on the functionality

Variables	f	%
1. Can you use this model with ease?	3	6.4
2. Is there interactivity of the various modules within this model?	13	27.7
3. Is there independence among these modules?	4	8.5
4. Is the model above applicable in a developing country?	4	8.5
5. Is the model easy to understand?	5	10.6
6. Does it use simple language?	6	12.8
7. Does the model guide measurement of digital forensic evidence extraction process models for mobile devices?	13	27.7

Comparison Analysis

A comparative analysis was performed between this developed metric and a model with existing models and metrics discussed in the literature. It was found that the current model exceeds the models discussed in the literature. Therefore, the proposed model is suitable for extracting digital forensic evidence in mobile devices managed by the four operating system platforms (Android, Windows, Apple iOS and Blackberry), as shown in *Table 5*.

Table 5: The differences between the existing models with the proposed model

Process/Phases in the Proposed model	NIST Guidelines	HDFI model	DEFSOP	SDFIM	MFP	SFIM	DFRWS
Device status check	✓	✓	✓	✓	✓	☐	☐
Preparation	☐	✓	✓	✓	☐	✓	✓
Identify evidence	✓	✓	☐	✓	✓	✓	✓
Recover data	☐	☐	☐	☐	☐	☐	☐
Forensic analysis	✓	☐	✓	✓	✓	✓	✓
Verification	☐	☐	☐	☐	☐	☐	☐
Documentation	✓	✓	☐	☐	☐	✓	☐

NIST-National Institute of Science and Technology, HDFI-Harmonized Digital Forensic investigation, DEFSOP- Digital Evidence Forensic Standard Operating Procedure, SDFIM- Systematic Digital Forensic Investigation Model, MEP- Modelling the Forensic Process, SFIM- Smartphone Forensic investigation model, DFRWS- Digital Forensics Research Workshop

Based on the steps included in the reviewed process models, it can be concluded that the proposed model is the most appropriate as it summarizes most of the phases and steps proposed in the previous models and shows the complexity of the reviewed models.

 This work is licensed under a Creative Commons Attribution 4.0 International License.

Article DOI: https://doi.org/10.37284/eajit.5.1.830

For example, examination of the NIST guidelines shows that there are very few steps which are not suitable enough to perform in-depth digital evidence extraction. The Harmonized Digital Forensic investigation model presents the preparation, identification, and documentation stages which this proposed model also addresses; however, critical consideration of device status checks is ignored in this model. Forensic analysis, recovery of data, and verification which are key concerns in digital evidence extraction have also not been addressed.

Although the Digital Evidence Forensic Standard Operating Procedure, The Systematic Digital Forensic Investigation Model, and modelling the Forensic Process all present several phases or steps to be followed, it can be noted that there are several repetitions in these stages and all of them concentrate more on the investigation itself other than extraction which the proposed model addresses right from device seizure to evidence extraction.

The Smartphone Forensic investigation model is close to the proposed model, except that it focuses more on the investigation than on extracting evidence which misses the phases of checking the status of the device and data retrieval, as highlighted by the proposed model as one of the main crucial issues in digital evidence extraction in mobile devices.

RESULTS AND DISCUSSION

Reliability Testing

The Cronbach α value of the various constructs between 0.591 and 0.850 demonstrated the ability to measure the internal consistency of the constructs used in this study ensuring that none of the constructs fell below the medium-high confidence test. The predictive power of the regression model of this study, with adjusted R-squared 0.848, indicates an appropriate level of variance explained [28]. This implies that the independent variables and constructs used in this study are significant for understanding the causes of inconsistencies in the model of the digital evidence extraction process in mobile devices with different operating systems and platforms. For example, the study results showed that the extraction methods used during the extraction and analysis of evidence, such as whether the experimenter applies a logical, manual, physical or brute force approach when examining a device mobile, play an important role in ensuring consistency. Likewise, the forensic documentation process has emerged as an important contribution to ensuring the consistency of the processes followed during the extraction of evidence, requiring the documentation of certain stages or stages of the extraction process if the results are repeatable and defensible in court. This therefore justifies the choice of the constructs used in this study with the support of the literature and therefore the results of this study generate several questions that may be of interest to ICT professionals, researchers, law enforcement agencies, regulators. and industry to have a clear understanding of the factors causing inconsistencies in extracting digital forensic evidence on mobile devices [19], [32]-[34]. Once these factors are clearly understood, taking these factors into consideration when developing solutions for solution developers and paying attention to them during an investigation by forensic investigators or investigators would speed up the process of collecting, storing and submitting evidence to the courts. for law enforcement legal assistance.

whether the examiner applied a logical, manual, physical, or brute force approach during the process of examining a mobile device, will play a significant role in ensuring the issues of consistency. Similarly, the forensic documentation process came out as a key contributor to ensuring consistency in the processes followed during evidence extraction, whereby certain stages or phases in the extraction process ought to be documented if the results are to be repeatable and defensible in courts of law. This, therefore, justifies the choice of the constructs used in this study having support from the literature and therefore, the results of this study generate several issues that may be of interest to ICT practitioners, researchers, law enforcement authorities, Regulatory Authorities, and the business community to have a clear understanding of the factors that cause inconsistencies in digital forensics evidence extraction in mobile devices [19], [32]-[34]. Once these factors are clearly understood, factoring them during solution development for solution developers and paying attention to them during an investigation by forensic examiners or investigators would aid the process of collecting,

 This work is licensed under a Creative Commons Attribution 4.0 International License.

Article DOI: https://doi.org/10.37284/eajit.5.1.830

preserving, and presenting evidence to courts of law for law enforcement agencies.

Descriptive Statistics for the Constructs

The descriptive statistics presented in *Table 6* provide a clear picture of how these constructs rank based on mean responses, with PF coming out significantly with a mean response of 4.36, followed by FDP and FET with the lowest mean response. This means that if there is a clear policy regarding the handling, acquisition, storage, documentation and presentation of digital evidence, there should be minimal inconsistencies in the process model for extracting digital evidence from mobile devices. This is followed by the forensic documentation process, suggesting concordance with recent studies indicating a lack of clear technical documentation of existing mobile device process models and methods for extracting digital evidence [6]. Forensic extraction tools are the last of the eight constructs, this can be attributed to the fact that there are several digital evidence extraction tools and most investigators face challenges in choosing the right digital evidence extraction tool on mobile devices, depending on the mobile device platform they are on [20].

Table 6: Descriptive Statistics for constructs and their rankings

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

Policy Factor (PF)

The means and standard deviations of the aggregate measures for the seven items used to measure the PF construct are presented in *Table 7*. In this table, seven items are used to measure this construct, ranging from PF1 to PF7.

Table 7: Descriptive statistics for policy constructs.

Item	Mean	Std Dev.	N
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

Strong agreement was reached for the construct of the political factor with the mean score of (Mean = 4.36, Std Dev = 4.99) with the element on the definition of the political guidelines which is the most agreed, PF1 (M = 4.64, SD = 0.574), followed by Personal training on current digital forensic evidence technologies for mobile devices has a positive effect on inconsistencies in digital forensic evidence extraction (PF5) (M = 4.49, Std Dev = .684), Creation of a mobile digital forensic evidence processing unit within the organization that reduces inconsistencies in extracting digital forensic evidence from mobile devices (PF3) (M = 4.40, Std Dev = 0.876), Recruitment of skilled personnel to process digital forensic evidence for mobile devices has a positive effect on inconsistencies in evidence

 This work is licensed under a Creative Commons Attribution 4.0 International License.

Article DOI: https://doi.org/10.37284/eajit.5.1.830

extraction PF4 (M = 4.32, Std Dev = .582), Actual Imp. Policy implementation leads to a coherent proces so of extraction of digital forensic evidence PF2 (M = 4.31, Std Dev = .637) and PF6 (M = 4.09, Std Dev = .750) is the least agreed element for this construct. The average correlation between elements determines the reliability of the construct; therefore, the higher the average correlation between elements, the higher the construct's reliability coefficient, Cronbach's alpha (α), depending on keeping the number of elements constant [28]. Table 8 shows the correlation between items for items used to measure the policy factor (PF) constructs.

Table 8: Inter-item correlation matrix for Policy Factors (PF) constructs

Item	PF1	PF2	PF3	PF4	PF5	PF6	PF7
PF1	1.000	.211	.554	.173	.161	.081	.081
PF2	.211	1.000	.141	.217	.059	.064	.170
PF3	.554	.141	1.000	.168	.203	.232	.132
PF4	.173	.217	.168	1.000	.050	.395	.179
PF5	.161	.059	.203	.050	1.000	.024	.062
PF6	.081	.064	.232	.395	.024	1.000	.243
PF7	.081	.170	.132	.179	.062	.243	1.000

Most items had acceptable correlation between items (r> = 0.2). The least agreed elements, i.e., the passing of laws governing mobile devices, the extraction of digital forensic evidence has a positive effect on inconsistencies in the extraction of evidence (PF6) and the development of strategies and frameworks for examining the digital forensic evidence for mobile devices has a positive effect. on the inconsistency of evidence extraction in mobile devices (PF7) was also the least correlated with the rest of the elements, while setting policies for extracting digital forensic evidence from mobile devices leads to a consistent process for retrieval of digital forensic evidence PF1, Creating digital forensic evidence Mobile evidence processing unit within the organization reduces inconsistencies in mobile devices Extraction of digital forensic evidence PF3 and recruitment of qualified personnel to manage mobile devices Digital forensic evidence has a positive effect on inconsistencies in the extraction of evidence PF4 was positively correlated with the rest of the items for the co-instructor. There was a moderate relationship (r> = 0.55) between the formulation of policy guidelines for extracting digital forensic evidence for mobile devices, which led to a consistent element for retrieving digital forensic evidence (PF1) and the establishment of a forensic evidence for the mobile device unit within the organization reduces inconsistencies in extracting digital forensic evidence from mobile devices (PF3) (r = 0.55), as well as a low correlation between the recruitment of qualified personnel to handle mobile devices digital forensic evidence has a positive effect on inconsistencies in evidence extraction (PF4) and in enacting laws for mobile devices, digital forensic evidence extraction has a positive effect on inconsistencies in evidence extraction (PF6) (r = 0.395). We can therefore conclude that the elements selected to measure the policy factor (PF) were suitable for the measure.

Device Factor

The average and standard deviations of the aggregate measures for the three items used to measure the DF construct are shown in *Table 9.*

Table 9: The mean and standard deviation for DF construct items

Item	Mean	Std. Dev	N
DF1	4.45	.627	85
DF2	4.27	.662	85
DF3	4.09	.908	85
DF4	4.04	.957	85

 This work is licensed under a Creative Commons Attribution 4.0 International License.

Article DOI: https://doi.org/10.37284/eajit.5.1.830

Strong agreement was obtained for the DF constructs, the average score (mean = 4.21, standard deviation = 3.15) for the mobile device state item during of obtaining evidence being the most consensual, the state of the mobile device during the examination. proof taking DF1 (mean=4.45, Std-Dev=0.627), followed by type of mobile devices DF2 (mean=4.27, Std-Dev=0.662), versions of mobile devices DF3 (Mean=4 .09, Std Dev = 0.908) and DF4 (mean = 4.04, standard deviation = 0.957) is the least agreed item for this construct. *Table 10* shows the inter-item correlation for the items used to measure the DF construct. As observed, most items had an acceptable inter-item correlation (r>=0.2). The least agreed item was mobile device type (DF2) and was least correlated with mobile device version (DF3) (r = 0.155). There was a moderate relationship (r>=0.568) between mobile device type (DF2) and device connection parameters (DF4) (r=0.331), and a weak correlation between mobile device status. mobile device during evidence collection (DF1) and (DF2) and (DF3) with (r > 0.279 but < 0.386). We can therefore conclude that the elements selected for the measurement of the DF were suitable for the measurement of this construct [28], [35].

Table 10: The correlation for the DF construct

Item	DF1	DF2	DF3	DF4
DF1	1.000	.279	.385	.331
DF2	.279	1.000	.155	.568
DF3	.385	.155	1.000	.229
DF4	.331	.568	.229	1.000

Extraction Method Factor

The means and standard deviations of the aggregated measurements for the ten items used to measure the construction of the EMF. From *Table 11*, there is strong agreement for the factorial construction of the extraction method, with an average score of (Mean = 4.12, StdDev = 0.83) for the item Physical acquisition, l 'most commonly assumed item, EMF3 (mean=4.46, StdDev=0.716), followed by EMF1 (mean=4.39, SD=0.773), EMF5 (mean=4.14, standard deviation=0.789), Logical EMF2 capture, where (mean=4.11, standard deviation=0.772), EMF4 brute force capture (mean=3.96, SD=0.763), and EMF6 architecture (mean=3.91, Std Dev=0.959) is the least agreed element for this construct.

Table 11: Descriptive statistics for Extraction Method factors construct items

Item	Mean	Std. Dev	N
EMF1	4.39	.773	85
EMF2	4.11	.772	85
EMF3	4.46	.716	85
EMF4	3.96	.763	85
EMF5	4.14	.789	85
EMF6	3.91	.959	85
EMF7	3.93	1.021	85
EMF8	4.25	1.022	85
EMF9	4.09	.840	85
EMF10	3.85	1.160	85

Similarly, in *Table 12*, the correlation between items for several factors and most of the items had acceptable inter-item correlation (r> = 0.2). The least agreed upon Architecture (EMF6), file system (EMF8), data storage mechanism (EMF9) and instant messaging applications (EMF10). Subsequently, they were less correlated with manual acquisition (EMF1), logical acquisition (EMF2) and physical acquisition (EMF3) with (r <= 0.2). There was a moderate relationship (r> = 0.589)

 This work is licensed under a Creative Commons Attribution 4.0 International License.

Article DOI: https://doi.org/10.37284/eajit.5.1.830

between (EMF1) and EMF2, as well as a low correlation between (EMF3) and (EMF2) and (EMF10) with (r> 0.2 but <0.386). We can therefore conclude that the elements selected for the EMF measurement were suitable for the measured construct.

Table 12: Inter-item correlation for Extraction Method Factors (EMF) construct

Item	EMF1	EMF2	EMF3	EMF4	EMF5	EMF6	EMF7	EMF8	EMF9	EMF10
EMF1	1.000	.589	.126	.266	.143	-.014	.322	-.002	.016	.001
EMF2	.589	1.000	.213	.593	.190	-.002	.251	.087	.021	.071
EMF3	.126	.213	1.000	.357	.411	-.058	-.183	-.092	.086	.100
EMF4	.266	.593	.357	1.000	.345	.174	.088	.057	.135	.236
EMF5	.143	.190	.411	.345	1.000	.159	.367	.325	.303	.050
EMF6	-.014	-.002	-.058	.174	.159	1.000	.370	.230	.159	.030
EMF7	.322	.251	-.183	.088	.367	.370	1.000	.348	.063	-.200
EMF8	-.002	.087	-.092	.057	.325	.230	.348	1.000	.111	.153
EMF9	.016	.021	.086	.135	.303	.159	.063	.111	1.000	.394
EMF10	.001	.071	.100	.236	.050	.030	-.200	.153	.394	1.000

Nature of Data factors

The means and standard deviations of the aggregate measures for the five items used to measure the nature of data factors (ND) constructs are shown in Table 13.

Table 13: Descriptive statistics for nature of data factors

Item	Mean	Std. Dev	N
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

Strong agreement was reached for the ND with the mean score of (mean = 3.90, Std Dev = 0.851) on the item, with the most similar internal and visible data, ND1 (mean = 4.32, Std Dev = 0.790), followed by external and visible ND3 (mean = 4.19, SD = 0.794), internal but hidden ND2 (mean = 3.79, standard dev = 0.773), external but hidden ND4 (mean = 3.69, Std Dev = 0.859) and encrypted data ND5 (Mean = 3.53, Std Dev = 1.04) is the least agreed upon for this construct.

Table 14: The correlation for Nature of Data Factors

Item	ND1	ND2	ND3	ND4	ND5
ND1	1.000	.540	.549	.355	.328
ND2	.540	1.000	.395	.421	.303
ND3	.549	.395	1.000	.295	.353
ND4	.355	.421	.295	1.000	.648
ND5	.328	.303	.353	.648	1.000

Referring to Table 14, most items had an acceptable inter-item correlation (r>=0.2). The least agreed item was ND5 encrypted data and the least correlated with external but hidden ND4 (r =0.353). There was a moderate relationship (r>=0.540) between internal and visible (ND1) and external and

 This work is licensed under a Creative Commons Attribution 4.0 International License.

Article DOI: https://doi.org/10.37284/eajit.5.1.830

visible ND3 (r>=0.549), and a weak correlation between external but hidden (ND4) and external and visible (ND3) with (r<=0.295). We can therefore conclude that the items chosen to measure ND were appropriate for the measurement.

Correlation of individual OS and Constructs

Table 15 shows how the different single OS platforms relate to different constructs; this table indicates that the FDP has a significant correlation with iOS (0.404), closely followed by Android (0.268), Windows (0.229), while Blackberry has the least significant correlation at .008. The FET construct showed significant correlation with iOS and Blackberry OS with 0.524 and 0.667, respectively. Windows came in third with 0.285 and Android followed with 0.178. Data types showed correlation between all four operating system platforms, closely followed by policy factors. The implication is that FET, FDP, EM, and ND are more important factors in understanding how they affect the extraction of evidence on mobile devices running those OS platforms, while each of the four OS platforms provide the same or different types of data, such as ex. logs, browsing history, short post services, or videos, may explain why the data type posted the least significant correlation.

Table 15: Correlation of individual operating systems and independent constructs

Item		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

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

Regression Analysis

According to Perry et al. [28], Linear regression (LR) is a method used to model the linear relationship between a dependent variable and one or more independent variables. Dependent variable is sometimes called predictor and independent variables are called predictors. Linear regression is based on the method of least squares: the model is adjusted to minimize the sum of the squares of the differences between the observed and predicted values based on six basic assumptions. Regression analysis was performed using the consistency metric (CM) as the dependent variable and constructs (EM, FET, PF, DF, ND, and DTF) as independent variables. The analysis revealed a significant pattern with corrected R-squared .848, which equates to 84.8% and thus the predictive variable included in the analysis was found to be significant. The total F = 79,238 Sig. = .000b on extraction methods, data type, nature of data, political factors, forensic documentation, forensic extraction tools and device factors. The results indicate that the model is statistically significant, valid and suitable. The validity of the model means that the consistency metric predicts a significant relationship with the extraction inconsistencies. From now on, the model was sufficiently suited to arrive at conclusions and recommendations. The regression model reveals adjusted R-squared = 0.848, which means that the consistency metric is strongly influenced by factors such as policy, data type, nature of data, extraction method, and forensic documentation process. With an adjusted R-squared of 0.848, which represents 84.8% of the constructs

 This work is licensed under a Creative Commons Attribution 4.0 International License.

Article DOI: https://doi.org/10.37284/eajit.5.1.830

used to predict the consistency metrics to be used in the evidence extraction process model for those mobile devices running on the four mobile operating systems, namely Android, Windows, iOS and Blackberry OS. This model adaptation confirms what the literature has revealed about factors such as documentation, extraction methods are the main causes of inconsistencies in mobile devices, evidence extraction process models [4], [36]-[38] and then other factors such as policies [32], [39], [40], nature of data [41] and type of data [15], [42] have a small contribution to inconsistencies in the evidence extraction process. From this *Table 16*, two factors emerged in a very significant way, namely the factor of the extraction method which is at B = 1.030 and the device factor at B = 0.078; these positive values indicate that as independent variables increase the consistency metric, even a dependent variable increases it, this is supported by the literature [28]. The coefficient of determination also indicates that as some independent variables increase, the consistency decreases and the standard error decreases. For example, the nature of the data B = -0.029 and Beta = -0.037 with sig. to 0.443. The implication here is that these factors do not significantly contribute to the consistency metric and therefore have less impact on the consistency process model when extracting evidence on mobile devices with the four OS platforms used in this study.

Table 16: Regression analysis with consistency metric as the dependent variable

Model		Unstandardized Coefficients		Standardized Coefficients	T	Sig.
		B	Std. Error	Beta		
1	(Constant)	-.649	.347		-1.870	.065
	EM	1.030	.054	.897	18.963	.000
	ND	-.029	.037	-.037	-.771	.443
	DTF	.009	.039	.011	.231	.818
	EMF	.016	.046	.016	.346	.730
	DF	.078	.039	.092	1.975	.052
	PF	.040	.050	.035	.797	.428

The results of this study showed that forensic extraction tools, extraction methods, nature of the data, type of device, and forensic documentation process are the main factors contributing to inconsistencies in extraction. These findings support the findings of recent studies that have revealed discrepancies in retrieving and reporting data residing on a device from previous tool tests and updates or new versions of the tool. This is in line with the results of the interviews, which showed that the type of data, the nature of the data and the method of extraction are a major cause of inconsistency in mobile device forensic evidence models. Furthermore, the study results established that the political factor is a benchmark for specifying a consistent model of digital forensic evidence extraction for mobile devices based on Android, Windows, iOS and Blackberry OS. In addition, the device factor is part of the metrics to specify a consistent model of digital forensic evidence extraction for mobile devices based on the four Operating systems (OSs).

The present study showed that the extraction method factor is a metric for specifying a consistent digital forensic evidence extraction pattern for the four OS-based mobile devices. The results of the study revealed that the nature of data factors are measures to specify a consistent model of digital forensic evidence extraction for mobile devices based on the four OSs. This is convenient for Brian Cusack [43], who posits that the high-level process of digital forensics involves collecting data from a source, data analysis and evidence extraction, as well as the storage and presentation of evidence. This study found that forensic extraction tools are measures to specify a consistent pattern of digital forensic evidence extraction for mobile devices based on the four OSs. While the forensic documentation process is part of the measures to specify a consistent digital forensic evidence extraction model for mobile devices.

 This work is licensed under a Creative Commons Attribution 4.0 International License.

Article DOI: https://doi.org/10.37284/eajit.5.1.830

CONCLUSION

The extraction process model developed borrowed the principles of consistency, repeatability, and standardization as presented in earlier studies of the generalized forensic framework from previous studies. This model goes further to enumerate sequentially each step that should be followed in evidence extraction for each of the mobile operating systems, thereby ensuring that there are consistencies at every step of the extraction process. These sequential or chronological steps (stages) followed will yield positive results across the four mobile operating systems and it is believed that this model can act as a standard for any other mobile operating system platform that has not been part of this study, considering that the architecture of mobile devices does not differ significantly in terms of storage, processing, and application. The Smartphone Forensic investigation model is close to the proposed model except that it concentrates more on the investigation other than evidence extraction and critically lacks the device status check and data recovery phases, as pointed out in the proposed model as one of the key critical issues in digital evidence extraction in mobile devices. Future work should focus on practically testing these models and comparing the results for consistency across different operating system platforms.

Data Availability

Research data underlying the findings of the study can be accessed upon request from the corresponding author.

Conflict of Interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

Funding Statement

This study received no external funding

REFERENCES

[1] ITU, "HIPCAR Establishment of Harmonized Policies for the ICT Market in the ACP countries Cybercrime/e-Crimes: Model Policy Guidelines & Legislative Texts Geneva, 2013 CARICOM.".

[2] C. A. Murphy, "Developing Process for Mobile Device Forensics" *Accessed on, Vol. 11*. 2013.

[3] J. Son, "*Social Network Forensics: evidence extraction tool capabilities*," (Doctoral dissertation, Auckland University of Technology), 2012.

[4] J. T. Ami-Narh and P. A. H. Williams, "Digital forensics and the legal system: A dilemma of our times," *6th Aust. Digit. Forensics Conf.*, pp. 30–40, 2008.

[5] 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. 1, pp. 264–282, 2013.

[6] 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.

[7] S. Almulla, Y. Iraqi, and A. Jones, "A distributed snapshot framework for digital forensics evidence extraction and event reconstruction from cloud environment," *Proc. Int. Conf. Cloud Comput. Technol. Sci. CloudCom*, vol. 1, pp. 699–704, 2013.

[8] B. Martini and K. K. R. Choo, "An integrated conceptual digital forensic framework for cloud computing," *Digit. Investig.*, vol. 9, no. 2, pp. 71–80, 2012.

[9] M. A. Frempong and K. K. Hiran, "Awareness and Understanding of Computer Forensics in the Ghana Legal System," *Int. J. Comput. Appl.*, vol. 89, no. 20, pp. 975–8887, 2014.

[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] A. Srivastava and P. Vatsal, "Forensic Importance of SIM Cards as a Digital Evidence," *J. Forensic Res.*, vol. 07, no. 02, pp. 2–5, 2016.

[12] D. B. Garrie, J. D. Morrissy, Z. Ellman, and K. Llp, "Digital Forensic Evidence in the

 This work is licensed under a Creative Commons Attribution 4.0 International License.

Article DOI: https://doi.org/10.37284/eajit.5.1.830

Courtroom: Understanding Content and Quality," *Northwest. J. Technol. Intellect. Prop.*, vol. 12, no. 2, pp. 122–128, 2014.

[13] 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.

[14] S. Rahman, Shaheed Zulfikar Ali Bhutto Institute of Science and Technology, Islamabad, Pakistan, and M. N. A. Khan, "Digital forensics through application behavior analysis," *Int. j. mod. educ. comput. sci.*, vol. 8, no. 6, pp. 50–56, 2016.

[15] F. Freiling and M. Gruhn, "What is Essential Data in Digital Forensic Analysis?," *2015 Ninth Int. Conf. IT Secur. Incid. Manag. IT Forensics*, pp. 40–48, 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] S. L. Garfinkel, "Effective Digital Forensics Research is nvestigator-centric," *Digit. Investig.*, vol. 7, pp. S64–S73, 2010.

[18] J. M. Klein and D. Baker, "American bar association," vol. 46, no. 3, pp. 373–378, 2000.

[19] 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.

[20] S. Yadav, K. Ahmad, and J. Shekhar, "Analysis of Digital Forensic Tools and Investigation Process," *High Perform. Archit. Grid*, pp. 435–441, 2011.

[21] O. Bongomin, G. Gilibrays Ocen, E. Oyondi Nganyi, A. Musinguzi, and T. Omara, "Exponential Disruptive Technologies and the Required Skills of Industry 4.0," *J. Eng.*, vol. 2020, pp. 1– 17, 2020. https://doi.org/10.1155/2020/4280156

[22] F. Jafari and R. S. Satti, "Comparative Analysis of Digital Forensic Models," *J. Adv. Comput. Networks*, vol. 3, no. 1, pp. 82–86, 2015.

[23] 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.

[24] S. Karthick and S. Binu, "Android security issues and solutions," in IEEE International Conference on Innovative Mechanisms for Industry Applications, ICIMIA 2017 - Proceedings, pp. 686–689, 2017.

[25] M. Elyas, S. B. Maynard, A. Ahmad, and A. Lonie, "Towards a Systematic Framework for Digital Forensic Readiness," *J. Comput. Inf. Syst.*, vol. 54, no. 3, pp. 97–105, 2014.

[26] R. V Krejcie and D. W. Morgan, "Determining Sample Size for Research Activities Robert," *Educ. Psychol. Meas.*, vol. 38, no. 1, pp. 607–610, 1970.

[27] C. Kothari, Research methodology: methods and techniques. 2004.

[28] C. B. Perry R, Hinton, Isabella McMurray, *SPSS Explained Second Edition*. 2014.

[29] L. Cohen, L. Manion, and K. Morrison, *Research methods in education*, 3rd ed. London, England: Routledge, 1989.

[30] L. Spencer, J. Ritchie, J. Lewis, and L. Dillon, "Quality in qualitative evaluation: a framework for assessing research evidence (supplemetary Magenta Book guidance)," *Natl. Cent. Soc. Res.*, no. December, 2003.

[31] I. M. Kisembo *et al.*, "An Algorithm for Improving Email Security on the Android Operating System in the Industry 4.0 Era," *J. Eng.*, vol. 2021, pp. 1–8, Nov. 2021.

[32] ITU-HIPCAR, "Cybercrime/e-Crimes: Model Policy Guidelines & Legislative Texts," 2012.

[33] D. C. A. Murphy, "Developing Process for Mobile Device Forensics," 2009.

 This work is licensed under a Creative Commons Attribution 4.0 International License.

Article DOI: https://doi.org/10.37284/eajit.5.1.830

[34] 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.

[35] A. Holliday, Doing and Writing Qualitative Research Second edition, Thousand Oaks, CA: SAGE Publications, 2007.

[36] "Report on 2016 Inspection of Ernst & Young LLP Public Company Accounting Oversight Board, This is A Public Version of A Pcaob Inspection Report Portions of the Complete Report are Omitted from this Document in Order to Comply with Sections 104(G)(2) An," 2017.

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

[38] M. Huber, B. Taubmann, S. Wessel, H. P. Reiser, and G. Sigl, "A flexible framework for mobile device forensics based on cold boot attacks," *Eurasip J. Inf. Secur.*, vol. 2016, no. 1, p. 17, 2016.

[39] S. P. Framework, "Assessment G rid for E valuating Strategic Policy Frameworks for Digital Growth & Next Generation Network P lans," pp. 1–7, 2014.

[40] C. Grobler and B. Louwrens, "Digital Forensics: A Multi-Dimensional Discipline," *Proc. ISSA 2006*, 2006.

[41] M. M. N. Umale, P. A. B. Deshmukh, and P. M. D. Tambhakhe, "Mobile Phone Forensics Challenges and Tools Classification: A Review," *Int. J. Recent Innov. Trends Comput. Commun.*, vol. 2, no. 3, pp. 622–626, 2014.

[42] 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.

[43] R. L. Brian Cusack, "Up-dating investigation models for smart phone procedures | Semantic Scholar," 2014.

 This work is licensed under a Creative Commons Attribution 4.0 International License.