

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>

EANSO

EAST AFRICAN
NATURE &
SCIENCE
ORGANIZATION

Original Article

A Process Model to Enhance the Accuracy of Digital Forensic Investigations: A case of National Identification and Registration Authority (NIRA-Uganda)

Makheti Alex^{1,2}, Gilbert Gilibrays Ocen¹, Badru Lusiba^{1*}, Semwogerere Twaibu¹, Alunyu Andrew Eguar¹, Matovu Davis¹ & Godfrey Odongtoo¹

¹ Busitema University, P. O. Box 236, Tororo, Uganda

² National Identification and Registration Authority, P. O. Box 26529, Kampala-Uganda.

* Correspondence ORCID ID: <https://orcid.org/0000-0001-8224-5594>; email: lusibab@gmail.com.

Article DOI: <https://doi.org/10.37284/eajit.5.1.1015>

Date Published: ABSTRACT

19 December 2022

Keywords:

Digital Forensics,
Enhanced Accuracy,
Process Model,
Investigation

The field of digital forensics has become commonplace due to the increasing prevalence of technology since the late 20th century and the inevitable relevance of this technology in the conducting of criminal activity. In traditional forensics, the evidence is generally something tangible that could identify the criminal, such as hair, blood or fingerprints. In contrast, digital forensics deals with files and data in digital form extracted from digital devices like computers, and phones, among other digital devices, meaning is derived from the fact that a computer or computerised device is the subject or object of crime. In this paper, we explore the challenges faced by the National Identification and Registration Authority (NIRA) digital forensic investigation and develop a process model that enhances the accuracy of digital forensic investigation. We adopted a mixed method approach of research involving qualitative, quantitative and experimental design. The study makes significant findings in areas of enhancement accuracy of digital forensic investigation by enumerating the processes that must be followed. As a recommendation for future work, for purposes of generalisation of the study findings, a wider study involving other security agencies such as the police should be conducted.

APA CITATION

Alex, M., Ocen, G. G., Lusiba, B., Twaibu, S., Eguar, A. A., Davis, M., & Odongtoo, G. (2022). A Process Model to Enhance the Accuracy of Digital Forensic Investigations: A case of National Identification and Registration Authority (NIRA-Uganda). *East African Journal of Information Technology*, 5(1), 216-243. <https://doi.org/10.37284/eajit.5.1.1015>

CHICAGO CITATION

Alex, Makheti, Gilbert Gibrays Ocen, Badru Lusiba, Semwogerere Twaibu, Alunyu Andrew Eguar, Matovu Davis and Godfrey Odongtoo. 2022. "A Process Model to Enhance the Accuracy of Digital Forensic Investigations: A case of National Identification and Registration Authority (NIRA-Uganda)". *East African Journal of Information Technology* 5 (1), 216-243. <https://doi.org/10.37284/eajit.5.1.1015>.

HARVARD CITATION

Alex, M., Ocen, G. G., Lusiba, B., Twaibu, S., Eguar, A. A., Davis, M., & Odongtoo, G. (2022) "A Process Model to Enhance the Accuracy of Digital Forensic Investigations: A case of National Identification and Registration Authority (NIRA-Uganda)", *East African Journal of Information Technology*, 5(1), pp. 216-243. doi: 10.37284/eajit.5.1.1015.

IEEE CITATION

M. Alex, G. G. Ocen, B. Lusiba, S. Twaibu, A. A. Eguar, M. Davis, & G. Odongtoo "A Process Model to Enhance the Accuracy of Digital Forensic Investigations: A case of National Identification and Registration Authority (NIRA-Uganda)", *EAJIT*, vol. 5, no. 1, pp. 216-243, Dec. 2022.

MLA CITATION

Alex, Makheti, Gilbert Gibrays Ocen, Badru Lusiba, Semwogerere Twaibu, Alunyu Andrew Eguar, Matovu Davis & Godfrey Odongtoo. "A Process Model to Enhance the Accuracy of Digital Forensic Investigations: A case of National Identification and Registration Authority (NIRA-Uganda)". *East African Journal of Education Studies*, Vol. 5, no. 1, Dec. 2022, pp. 216-243, doi:10.37284/eajit.5.1.1015.

INTRODUCTION

Digital forensics is a widely-used term referring to the identification, acquisition and analysis of digital evidence originating from much more than just computers, such as smartphones, tablets, Internet of Things Devices, or data stored in the cloud, then preservation and presentation of the same in the courts of law as evidence [1].

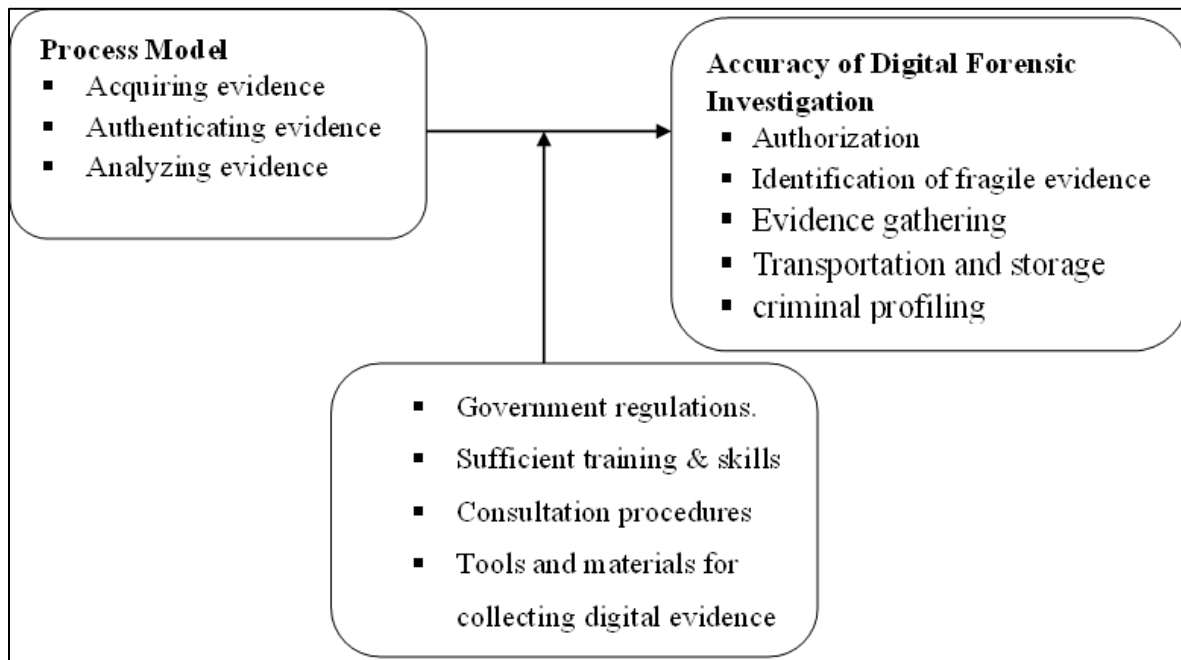
The field of digital forensics has become commonplace due to the increasing prevalence of technology since the late 20th century and the inevitable relevance of this technology in the conducting of criminal activity [2]. In traditional forensics, the evidence is generally something tangible that could identify the criminal, such as hair, blood or fingerprints [3]. In contrast, digital forensics deals with files and data in digital form extracted from digital devices like computers and phones, among other digital devices, meaning is derived from the fact that a computer or computerised device is the subject or object of crime [2]. Digital forensics is a widely-used term referring

to the identification, acquisition and analysis of digital evidence originating from much more than just computers, such as smartphones, tablets, Internet of Things Devices, or data stored in the cloud, then preservation and presentation of the same in the courts of law as evidence [4].

With the increased use of technology in organisations and rapid changes in technology, the cyber forensic process is also advancing in new ways [5]. In this context, NIRA-Uganda also needs to align its technological infrastructure to meet the challenges in conducting a successful process of forensic investigations to attain the maximum and desired benefits of it. NIRA is an authority in Uganda that houses the national biometric database, maintaining various updated registers of Uganda in its safe custody; these registers include the national identification register, birth register, death register and adoption orders register [6]. This is sensitive information that may attract cyber criminals from the external locations of the organisation or internal insiders who may want to advance their illegitimate intentions.

Conceptual Framework

Figure 1: Conceptual framework



In this study, the framework comprises the independent variable which is the process model and the dependent variable which is the accuracy of digital forensic investigation. Process Model constructs are acquiring evidence, authenticating evidence and analysing evidence. While the constructs of digital forensic investigation accuracy are: authorisation, identification of fragile evidence, evidence gathering, storage and transportation and criminal profiling. However, for there to be a measurable impact, the moderating variables have to come into play, which is; government regulations, sufficient training and skills, consultation procedure when investigating, and tools and materials employed to collect digital evidence.

METHODOLOGY

Study Population

The participants were selected from different groups which included; Top management board, technical systems managers and end users. The total study population constituted from the above categories was 205 from which a sample size of 150 respondents was determined to participate actively

in this study. The above categories of respondents were selected to take part in this study because of the role they are deemed to play in the cyber forensic investigation at the institution. In addition to that, the study trusted that the above-selected categories were well placed to provide the data required in this study by virtue of their positions.

The sample size for respondents was calculated using Slovin’s formula as shown below [7];

$$n = \frac{N}{1+N(e)^2}$$

Where; n = sample size, N = the population, and e = the level of precision of 0.05 used, A 95% (1.96) confidence level was assumed in the equation.

$$n = \frac{205}{1+205(0.05)^2} = 136$$

A 10% non-response rate of 136 respondents was added to the sample size to cater for incomplete questionnaires and non-response by the respondents. The non-response rate was therefore calculated as follows:

$$Non\ response\ rate = \frac{10}{100} * 136 = 14$$

The sample size was $136+14 = 150$ respondents

Sampling Techniques and Procedure

According to [8], a sampling technique is a description of the strategies used by the researchers to select representative respondents from the target population. The study employed a simple random sampling technique since the population was valid and large; there were some levels of non-response from the sampled population. In this respect, the sample size was large enough to enhance the representativeness and eventual generalisation of the research findings.

Data Collection Methods

Data collection involved the use of Questionnaires, interviews and an extensive literature review. Questionnaires were given to respondents and collected after a period of two weeks for analysis of the data obtained. The data collected was transcribed for purposes of editing and easy understanding. Interviews were carried out with respondents who ran the systems on a day-to-day basis and helped to supplement the responses from the questionnaires. While performing the literature review, the researchers used worksheets to carry out a review of documents where data was collected from records. The data worksheet was used with a sequence of checks to ascertain whether digital forensic investigations systems had a foothold.

Quality Control

Data quality control refers to the efforts or strategies and procedures put in place to guarantee and ensure the quality and accuracy of data being collected using different methodologies and techniques for a particular research study [9]. It was important to ensure that data quality control was maintained throughout the research data collection process. Therefore, the proposed research study employed the following data control techniques below;

Reliability

Reliability is the degree to which an instrument measures the same way each time it is used under the same conditions with the same subjects [10]. Data collection instruments were pre-tested on at least 15 people, playing the same role as those

earmarked for the study. This helped to ascertain their dependability, accuracy and ability to elicit the necessary and adequate responses. The respondents were requested to make constructive criticisms and positive changes. Their suggestions were adopted for the purpose of improving the final research instruments.

Validity

Validity is the extent to which an instrument measures what it is meant to measure [11]. The instrument applied should be valid, practical and free from bias. In this case, before the researchers applied the instruments, they were validated by examining their contents and whether they could measure to the assumed attributes, free from bias, contamination and deficiency.

Data Analysis

The analysis is the computation of certain measures, along with searching for patterns of relationships that exist among data groups [12]. The data collected was analysed both qualitatively and quantitatively, as explained below;

Quantitative Data Analysis

The data collected was edited and coded to deal with errors, omissions and correct them where necessary [13]. Numbers were assigned to the questionnaires whilst entering into the Statistical Package for Social Sciences, a computer program. Out of the inputs within the programme, descriptive statistics and relational statistics were formulated [13].

Qualitative Data Analysis

The content analysis method was used to analyse qualitative data from interviewees and review documents. The communication was in the form of responses to the Likert scale continuum questionnaire, the content of the interview, and field notes. In this study, the researchers analysed the content of interviews and questionnaires.

Model Design and Implementation

Model Design

A linear equation was used as shown below;

$$Y=C+\beta_1X_1+ \beta_2X_2+ \beta_3X_3+ \varepsilon$$

Where; Y = adaptability of digital forensics, C = Constant, $\beta_1, \beta_2, \beta_3, \dots, \beta_n$ = coefficients or the weights that were estimated. ε = Standard error of estimate, X1, X2, X3, Xn = variables; and in this study, it is; Effectiveness of digital forensic, Technology legal framework and regulatory policies, components for digital forensic evidence and forensic adaptability model respectively.

Model Implementation

Implementation of the model was done by use of rapid prototyping because it helped to provide earlier feedback before the creation of the final model and assisted in testing and evaluation of the software and its workability [14]. Rapid prototyping

was chosen because it has the ability to develop customised products as per the individual’s requirement and it requires no special tools or processes to implement design changes in the products [15]. Tools such as Php, MySQL databases, JQuery and JavaScrip and CSS3 were used.

RESULTS AND DISCUSSIONS

Response Rate

A total of 125 respondents participated in the study out of the earmarked 150. Of these, 121 returned their questionnaires and 04 participated in face-to-face interview sessions as key informants, while 25 absconded from the study. Therefore, the total number was 125, which gave the rate of 83.3%.

Table 1: Response Rate

Participants	Key informant Interviews	Questionnaires
Top management	04	
Technical systems staff		39
Cyber security department		20
End users attached		62
Subtotal	04	121
Total	125	

Source: primary data 2022

Table 1 shows the category of respondents who participated in the study. The total number of respondents was 125, where 121 filled out self-administered questionnaires, and these constituted; technical systems staff 39, cyber security departmental staff 20 and ender users attached 62. While 04 participated in face-to-face interview sessions as key informants and these were top management members. Out of 150 earmarked, 125 participated in the study giving a response rate of 83.3%. This was regarded as adequate in line with literature by Mugenda and Mugenda (1999) which recommends 70% as a good response rate when quantitative data is collected.

In light of the above findings on assessing process models and their role in enhancing the accuracy of digital forensic investigation in the institution, below is the summary (see Table 2);

Table 2: Process of Digital Forensic Investigations at NIRA

Statements	SD f (%)	D f (%)	NS f (%)	A f (%)	SA f (%)	Mean	STD
NIRA follows specific rules regarding the seizure of electronic evidence	15 (12.4)	16 (13.2)	28 (23.1)	41 (33.9)	17 (14.0)	3.26	1.210
NIRA ensures that the tools used to acquire digital evidence are validated to operate as intended and accurately acquire data	12 (9.9)	15 (12.4)	35 (28.9)	37 (30.6)	21 (18.2)	3.12	1.185
NIRA ensures that its experts carry out a thorough examination, analysis, and evaluation of evidence, employing critical thinking, reasoning, and logical analysis.	18 (14.9)	12 (9.9)	26 (21.5)	33 (27.3)	30 (24.8)	3.16	1.365
Collecting and analysing data in a logical way enables the linking of pieces of information and reconstructing the timing of events in order to help the investigators develop a better understanding of the case.	12 (9.9)	16 (13.2)	28 (23.1)	23 (19.0)	38 (31.4)	3.15	1.274
NIRA ensures a systematic search of evidence by examining computer media, such as floppy disks, hard disk drives, backup tapes, CD-ROM's and any other media used to store data.	12 (9.9)	10 (8.3)	35 (28.9)	22 (18.2)	39 (32.2)	3.10	1.156
The analysis of this data can provide the investigators with a wealth of information	16 (13.2)	37 (30.6)	19 (15.7)	30 (24.8)	15 (12.4)	2.83	1.234
The use of specific words and the tone of the language can reveal the psychological state of the offender	16 (13.2)	20 (16.5)	22 (18.2)	42 (34.7)	13 (10.7)	2.96	1.187
Analysing files of the offender's computer can reveal indicators of suspicious activity, as well as signature behaviour and personalised characteristics of the offender.	15 (12.4)	15 (12.4)	20 (16.5)	38 (31.4)	30 (24.8)	3.08	1.202

Key: 1 = Strongly Disagree, 2 = Disagree, 3 = Not sure, 4 = Agree, 5 = Strongly Agree, M = mean, STD = Standard deviation

Source: Primary Data

The study found that digital forensic evidence acquisition is a systematic process in that it follows well-laid-down protocols to which the institution adheres. This indicates that the way evidence is analysed significantly contributes to the accuracy of digital forensic investigations (see *Table 2*). As was envisaged, the institution follows protocols laid down by security agencies to seize evidence, employs accredited tools and mechanisms, ensures that thorough investigations and validations of data are done by the investigators deployed, collects evidence in a logical way and thoroughly examines the data collected by its experts for validity check. Therefore, the evidence analysis process significantly determines the accuracy of digital forensic investigations

Findings indicate that NIRA follows specific rules regarding the seizure of electronic evidence, where 41(33.9%) agreed and 17(14.0%) strongly agreed. This was followed by those who were not sure (28, 23.1%) and the least response came from those who disagreed, where 16(13.2%) disagreed and 15(12.4%) strongly disagreed. The calculated mean ($u=3.26$ and Std Deviation= 1.210) revealed a higher response level. Similarly, interviews with management revealed that NIRA first obtains search warrants and coordinates with security agencies to seize evidence for analysis. This is because NIRA itself is not a security agency but only helps security agencies to abet cybercrime.

Findings indicate that NIRA ensures that the tools used to acquire digital evidence are validated to operate as intended and accurately acquire data, where 37(30.6%) agreed and 21(18.2%) strongly agreed. This was followed by those who were not sure (35, 28.9%), and the least response came from those who disagreed, where 15(12.4%) disagreed and 12(9.9%) strongly disagreed also. The calculated mean ($u=3.12$ and $STD = 1.185$) revealed a higher response level. This was further confirmed in interviews with management that NIRA uses internationally recognised digital evidence acquisition methodologies and thereafter validates the data to ascertain its authenticity before sharing it with its partners like police and intelligence authorities. This is a systematic way of ensuring that the evidence accessed is authentic and further validated for accuracy and completeness. In effect, Lubaale (2015) states that information, though in

the form of a data message, will be given due evidential weight, having regard to the reliability of the manner in which the data message was generated, stored or communicated; the reliability of the manner in which the integrity of the data message was maintained; the manner in which its originator will be identified; and any other relevant factor.

Findings indicate that NIRA ensures that its experts carry out a thorough examination, analysis, and evaluation of evidence, employing critical thinking, reasoning, and logical analysis, where 33(27.3%) agreed and 30(24.8%) strongly agreed. This was followed by those who were not sure (26, 21.5%), and the least response came from those who disagreed, where 18(14.9%) strongly disagreed, and 12(9.9%) disagreed also. The calculated mean ($u=3.16$ and $STD = 1.365$) revealed a higher response level. Similarly, interviews with management revealed that NIRA has experts at its disposal who even have been at the forefront of assisting police and military intelligence in the examination of data from crime scenes. As envisaged, NIRA has the cardinal role of data examination and analysis critically up to the logical conclusion of investigations. These findings are in congruence with Jones et al. (2016), who states that a thorough examination, analysis, and evaluation of evidence, employing critical thinking, reasoning, and logical analysis are precursors for investigations to be successful. For example, in a computer-facilitated interpersonal crime where the investigator receives the victim's computer, the investigator should not only analyse the content of the subject files (e.g., emails, chat messages, blogs) (Jones et al., 2016) but should also pay attention to the meta-data related to these files, as well as other data informative to the case.

Findings indicate that collecting and analysing data in a logical way enables the linking of pieces of information and reconstructing the timing of events in order to help the investigators develop a better understanding of the case, where 38(31.4%) strongly agreed, and 23(19.0%) agreed. This was followed by those who were not sure (28, 23.1%), and the least response came from those who disagreed, where 16(13.2%) disagreed, and 12(9.9%) strongly disagreed also. The calculated mean ($u=3.15$ and $STD = 1.274$) revealed a higher

response. Similarly, interviews revealed that NIRA had adopted a system of putting the pieces together through reconstruction so that a logical conclusion could be reached. The reason behind this is to trace the source and then link it to the incident purposely to have a strong backup.

Findings indicate that NIRA ensures a systematic search of evidence by examining computer media, such as floppy disks, hard disk drives, backup tapes, CD-ROM's and any other media used to store data, where 39(32.2%) agreed, and 22(18.2%) strongly agreed. This was followed by those who were not sure (35, 28.9%), and the least response came from those who disagreed, where 12(9.9%) disagreed and 10(8.3%) strongly disagreed also. The calculated mean ($u=3.10$ and $STD=1.156$) revealed a higher response level. Similarly, interviews with management revealed that NIRA had deployed its computer experts who help in evidence gathering in all computer systems and storage devices available and then back it up on its own storage devices. The reason is to leave no stone unturned in evidence gathering and backup for reference purposes and production in court whenever the need arises. These findings corroborate with Summons (2017), who states that Good computer forensics practices dictate that once a bit-stream image copy from the original is made, the source should be preserved in a safer place as analysis on image copies is done. This kind of approach is based on the forensic process and presentation as the final stage.

Findings indicate that the analysis of the data gathered provides the investigators with a wealth of information, where 37(30.6%) strongly agreed and 30(24.8%) agreed. This was followed by those who disagreed, where 16(13.2%) strongly disagreed and 15(12.4%) disagreed also, and the least response came from those who were not sure (19, 15.7%). The calculated mean ($u=3.83$ and $STD=1.234$) revealed a higher response level. Similarly, interviews with management revealed that the gathered information makes it easy for NIRA to share with the security agencies the incidentals pertaining to the crime under investigation. As envisaged, NIRA being the chief data manager of Uganda has had an upper edge in mitigating insecurities arising from cybercrime. These findings are in tandem with Oriwoh, & Williams (2015), who states that investigation is done in order to realise an

incident triggered by the detection of irregularities in a system, information about a crime and so on.

Findings indicate that the use of specific words and the tone of the language can reveal the psychological state of the offender, where 42(34.7%) agreed and 13(10.7%) strongly agreed. This was followed by those who disagreed, where 20(16.5%) disagreed and 16(13.2%) strongly disagreed also, and the least response came from those who were not sure (22, 18.2%). The calculated mean ($u=2.96$ and $STD=1.187$) revealed a moderate response level. This was also confirmed in interviews with management that NIRA works with police psychologists who help to ascertain the psychological state of the person and the intention also. As envisaged, NIRA does not only work with computer experts but also collaborates with mind readers in evidence corroboration. These findings corroborate with Kaati et al. (2016), who state that the use of specific words and the tone of the language can reveal the psychological state of the offender (e.g., anger, revenge, greed). Analysing files on their computer (e.g., Internet history files, recently accessed files, access dates of the files, deleted files) can reveal indicators of suspicious activity, as well as signature behaviour and personalised characteristics of the offender, as stated by Turvey (2011). This information helps the investigator to develop leads and determine the location of additional sources of evidence.

Finally, findings indicate that analysing files of the offender's computer can reveal indicators of suspicious activity, as well as signature behaviour and personalised characteristics of the offender, where 38(31.4%) agreed and 30(24.8%) strongly agreed. This was followed by those who disagreed, where 15(12.4%) disagreed and 15(12.4%) strongly disagreed also, and the least response came from those who were not sure (20, 16.5%). The calculated mean ($u=3.08$ and $STD=1.202$) revealed a higher response level. Similarly, interviews with management revealed that analysis of files in the computers of suspected criminals easily helps the investigators to ascertain the intentions of the offender under investigation. This arises from the experience employed and also the intuition to tell what really was in store for the offender. These findings corroborate with Kim and Solomon (2016), who states that, as per the tradition, to prevent

anyone from accessing systems from outside the crime scene, it is generally advisable to disable network connectivity to all computer systems, which is currently done, but in doing so, evidence can be destroyed and will eliminate investigative opportunities. The hardware and software state will not be preserved, and not being able to respond effectively could be extremely damaging, especially to small organisations, which could not absorb losses easily as large organisations.

Strengths and Weaknesses of the current system employed by NIRA-Uganda

The study found that the current system's strength lies in it being in tandem with the current dynamics of forensic investigations because there is the systematic following of procedures in line with standard operating procedures (SOPs) (see *Table 3*). Currently, forensic experts strive to collect evidence, filter it, and present it for discussion; then, they are able to tell whether their data merits and what they need to do to make it more appealing. In addition, only authorised persons with expertise visit the crime scene to collect electronic evidence, with the institution being at the centre of evidence corroboration as an expert agency. In effect, the outcome of corroboration determines the next course of action per se. In the event that the corroborating evidence is found to be merited, the action is taken by bringing to book the responsible person.

Weaknesses of the Current System

On the flip side, the current system has its own weaknesses, which appear to be system based. As was envisaged, technical knowledge is required to undertake an effective analysis process which in most cases, forensic experts lack, and this has been the norm in Uganda with the success rate of cybercrime investigations being below average (see *Table 3*). The worst is that when the system is shut down, the memory resident programs can be lost, and they can be manipulated or altered without having a trace during the collection, analysis and presentation, which sets a bad precedent for forensic investigations. Another area of contention is that improper authentication might lead to the misinterpretation of complex forensic data leading to difficulty in getting credited results. Finally, the

institution has not yet derived the expected benefits from digital forensic technology because the structures in place to enable her to conduct cost-effective, low-impact and efficient digital investigations are limited. The above highlight the loopholes in the system and impediments which make it hard to achieve success using the current system, which can be improved through system strengthening.

Table 3: Current system strengths and weaknesses

	SD f (%)	D f (%)	NS F (%)	A F (%)	SA F (%)	Mean	Std
Strength							
Forensic experts strive to collect evidence, filter it, and present it for discussion.	10(8.1)	11(9.1)	39(32.2)	15 (12.4)	45(37.2)	3.12	1.223
Only authorised persons with expertise visit the crime scenes to collect electronic evidence	15(12.4)	7(5.8)	30(24.8)	62(51.3)	19 (15.7)	3.79	1.174
When a crime occurs, NIRA dwells on the identification of electronic evidence from the crime scene	26(21.5)	15(12.4)	30(24.8)	37(30.6)	11(9.1)	2.71	1.252
The e-evidence identified from the crime scene is then evaluated(corroboration)	21(17.4)	10(8.3)	28(23.1)	12(9.9)	45(37.2)	3.13	1.175
Weaknesses							
Technical knowledge is required to undertake an effective analysis process which in most cases forensic experts lack	12(9.9)	22(18.2)	25(20.7)	31(25.6)	27(22.3)	3.02	1.192
When the system is shut down; the memory resident programs can be lost, they can be manipulated or altered without having a trace during the collection, analysis and presentation	19(15.7)	18(14.9)	19(15.7)	35(28.9)	19(15.7)	2.98	1.306
Improper authentication might lead to the misinterpretation of complex forensic data leading to difficulty in getting credited results.	6(5.0)	8(6.6)	34(28.1)	42(34.7)	27(22.3)	3.22	1.260
NIRA has not yet derived the expected benefits from digital forensic technology because the structures in place to enable her to conduct cost-effective, low-impact and efficient digital investigations are limited	26(21.5)	09(7.4)	26(21.5)	36(29.8)	18(14.9)	3.41	1.330

Table 4: Requirements and process of developing an enhanced digital forensic investigation process model

Statements	SD f (%)	D f (%)	NS f (%)	A f (%)	SA f (%)	M	Std
All the system requirements are enumerated as expected deliverables then each of the required items is planned for.	6(5.0)	8(6.6)	34(28.1)	42(34.7)	27(22.3)	3.22	1.260
All the specifications of the software system to be designed are outlined including how registration, login, assessments, and reporting will be achieved.	13(10.7)	20(16.5)	25(20.7)	41(33.9)	17(14.0)	3.81	1.215
The intended system is drawn showing how components will relate to making certain that the software system will meet all the requirements.	16(13.2)	11(9.1)	33(27.3)	40(31.3)	13(10.7)	3.20	1.204
A rapid prototyping process is then employed as the most ideal for designing the model, the database and tables are created and relationships are defined.	16(13.2)	32(26.4)	15(12.4)	43(35.5)	11(9.1)	3.32	1.343
After the design, the system is evaluated using objective-based or goal-based evaluation involving the designer testing of parts of software against the specifications.	08(6.6)	36(29.8)	15(12.4)	52(43.0)	7(5.8)	3.33	1.177

The study found out that all the system requirements are enumerated as expected deliverables then each of the required items is planned for (see *Table 4*). In addition, all the specifications of the software system to be designed are outlined including how registration, login, assessments and reporting will be achieved; the aim is to acquaint developers with the software meant for the configuration and development of the process model. Furthermore, the intended system is drawn showing how components will relate to making certain that the software system will meet all the requirements, whose essence is to ensure that the components are tailored to the intending organisation. Thereafter, the rapid prototyping process is then employed as the most ideal for designing the model, the database and tables are created, and relationships are defined. Finally, after the design, the system is evaluated using objective-based or goal-based evaluation involving the designer testing of parts of software against the specifications. The evaluation is also meant to validate, calibrate and ensure that the system is responsive to the needs of the intending organisation.

Findings in table 4.9 above indicate that all the system requirements are enumerated as expected deliverables then each of the required items is planned for, where 41(33.9%) agreed and 17(14.0%) strongly agreed. This was followed by those who disagreed, where 20(16.5%) disagreed and 13(10.7%) strongly disagreed also, and the least response came from those who were not sure (25, 20.7%). The calculated mean ($u=3.81$ and $STD = 1.215$) revealed a higher response level. This corroborates with interviews which revealed that the system's requirements for developing a process model are always followed, which happens to be systematic. This shows that the requirements for model development are well-documented and standardised.

Findings indicate that all the specifications of the software system to be designed are outlined including how registration, login, assessments and reporting will be achieved, where 40(33.1%) agreed, and 13(10.7%) strongly agreed. This was closely followed by those who were not sure (33, 27.3%), and the least response came from those who disagreed, where 16(13.2%) strongly disagreed and 11(9.1%) disagreed. The calculated mean ($u=3.20$

and $STD = 1.204$) revealed a higher response level. Similarly, interviews revealed that the specifications are meant to acquaint developers with the software meant for the configuration and development of the process model. This shows that there are specifications to follow when designing a process model.

Findings indicate that the intended system is drawn showing how components will relate to making certain that the software system will meet all the requirements, where 43(35.5%) agreed and 11(9.1%) disagreed. This was followed by those who disagreed, where 32(26.4%) disagreed and 16(13.2%) strongly disagreed also, and the least response came from those who were not sure (15, 12.4%). The calculated mean ($u=3.32$ and $STD = 1.343$) revealed a higher response level. Similarly, interviews with management revealed that the intended system shows the interconnections of how components are put together to create a model tailored to the needs of the organisation. As envisaged, the software components are always checked to ascertain their dependability.

Findings indicate that the rapid prototyping process is then employed as the most ideal for designing the model, the database and tables are created and relationships defined, where 52(43.0%) agreed and 7(5.8%) strongly agreed. This was followed by those who disagreed, where 36(29.8%) disagreed and 08(6.6%) strongly disagreed also, and the least response came from those who were not sure (15, 12.4%). The calculated mean ($u=3.33$ and $STD = 1.343$) revealed a higher response level. The prototyping element is intended to configure the system and tailor it to the intending organisation whose end result is to enhance the accuracy of digital forensic investigations in NIRA.

Finally, findings indicate that after the design, the system is evaluated using objective-based or goal-based evaluation involving the designer testing of parts of software against the specifications, where 42(34.7%) agreed, and 17(14.0%) strongly agreed. This was followed by those who were not sure (31, 25.6%), and the least response came from those who disagreed, where 15(12.4%) disagreed and 08(6.6%) strongly disagreed also. The calculated mean ($u=3.27$ and $STD = 1.297$) revealed a higher response level. The evaluation is also meant to

validate, calibrate and ensure that the system is responsive to the needs of the organisation.

Development of the Model

The model for determining the accuracy of digital forensics in the organisation was designed as a web-based application using the latest web technologies. Precisely, PHP server-side scripting language was used to program the system controls, CSS3 was

used for system styling, and MySQL was used as a database engine (see *Table 5*). The model was hosted as an online platform where users could register, log in and access the system functions remotely via the URL link that was widely communicated. The system was verified to have succeeded in performing all the intended functions, namely, user registration, user login, forensic assessment, computation of the adaptability index and production of relevant reports.

Table 5: Accuracy of Digital Forensic Investigations

Statements	SD f (%)	D f (%)	NS f (%)	A f (%)	SA f (%)	Mean	S.dv
NIRA follows specific rules governing the search for electronic evidence	20 (16.5)	16 (13.2)	23 (19.0)	21 (17.4)	32 (26.4)	3.10	1.269
Only qualified persons visit the crime scenes to collect Electronic evidence	9 (7.4)	15 (12.4)	32 (26.4)	41 (33.9)	14 (11.6)	3.24	1.097
There are strong cooperation and coordination between regulators to succeed in the effective management of digital cases.	10 (8.3)	23 (19.0)	25 (20.7)	16 (13.2)	32 (24.4)	3.22	1.287
NIRA has an elaborate Standard Operating Procedure (SOP) that guides the process of forensic evidence collection, preservation, storage, analysis and presentation in court	36 (29.8)	13 (10.7)	18 (14.9)	40 (33.1)	10 (8.3)	3.04	1.302

Source: primary data 2022

Authorisation

The study found that the institution follows specific rules governing the search of electronic evidence, which are part of the security proposals, given that her role is purely to support function (see *Table 4*). In carrying out investigations, only qualified persons who are well-versed in cyber security systems visit crime scenes to collect electronic data, and this is done in cooperation and coordination between regulators to succeed in the effective management of digital cases. This is a testament that the institution coordinates with security agencies in investigating, scrutiny of information and analysing it to ascertain its authenticity before forwarding it to the concerned security agencies. To ensure the authenticity and integrity of the investigations, there use of elaborate Standard Operating Procedure (SOP) that guides the process of forensic evidence collection, preservation, storage, analysis and presentation in court. In order to be up-to-date with

technology, the institution has come up with clear guidelines on ethical behaviour, rules and guidelines for digital forensic investigations.

Identification of Fragile Evidence

The study found that digital evidence can be very fragile, when the system is shut down, Programmes can be manipulated or altered without having a trace during the collection, analysis and presentation (see *Table 4*). This has helped in saving the institution from the mayhem of badly needed data by security agencies. In addition, it was envisaged that evidence analysis involves determining significance, reconstructing fragments of data and drawing some conclusions based on the evidence collected. This happens through careful examination of the unique characteristics of the digital crime scene to answer questions regarding the case, uncover more evidence, and correlate with the offender’s behavioural decisions. The essence is to ensure that

the data collected is admissible by digging deep to cover more evidence and then corroborating purposely to weed out loopholes which may undermine its admissibility. Furthermore, it was also found that recovering and reconstructing artefacts left by the use of instant messaging tools can reveal information regarding the chat message such as the sender's name and profile number and the recipient's name and profile number. As was envisaged, social media appears to be one of the prime targets of digital forensic investigators. In light of the above, collecting this data and analysing them in a logical way can enable the linking of pieces of information and reconstruct the timing of events in order to help the investigator develop a better understanding of the case.

Evidence Gathering

The study found that the investigators normally employ more than technical examinations of the digital evidence as technology by itself is inadequate to solve the problem (see *Table 6*). Employing different systems is meant to help investigators easily gather information and compare to see if the results are the same; if it bears similarity, then they are able to query again and forward for further management. In addition, it is important to understand the motivation and the unique behavioural characteristics of the offender in order to effectively investigate digital cases because understanding the offender enables the investigators to relate the crime to the person's past record, as to whether the person is the first-time offender or may not have committed the crime, because incidences are instigated by people using other people accounts as a cover-up. Furthermore, it was envisaged that the data acquisition process has a significant bearing on the entire digital investigation, and it is often challenged by the courts concerning infringements. Normally, how data is acquired will determine its authenticity and the time to be taken to conclude the investigation, and if there are loopholes, then it becomes easy to be invalidated in courts of law. Finally, the study found that in order to efficiently solve a digital crime, it is important to learn as much as possible about the individual behind the offence, as well as the victim. The reason behind this is to easily understand the person and his/her motives behind the offence.

Transportation and Storage of Evidence

The study found that the institution follows a guideline for electronic evidence transportation. As was envisaged, there are procedures employed for the transportation and transfer of electronic evidence retrieved, which the institution adheres to which are in tandem with the standards set by security systems (see *Table 7*). In doing so, the institution follows the chain of custody protocol standards; custodial protocols have always been adhered to purposely for the safety of the data and to ensure that there is no tampering. In addition, it was envisaged that digital evidence is handled and stored in a manner that prevents the unintentional alteration or destruction of evidence by human interaction or environmental conditions. This is because the alteration of data by some individuals has always been the biggest hindrance to justice as data presented in courts of law is invalidated, leading to the efforts of the investigators being a waste of time.

Criminal Profiling

The study found that criminal profiling aids in the investigation of a variety of crime categories (e.g., murder, rape, sexual assault). Criminal profiling is vital as it helps in knowing the offenders and the number of crimes committed by the said person before apprehension (see *Table 8*). In addition, it was envisaged that behavioural analysis of crime scenes assists in constructing profiles of offender characteristics. This is a good initiative as it gives the investigators room to build good evidence around the case since the offender's identity is known, and the only task is to be abreast with the issues pertaining to the case. Furthermore, the behavioural characteristics of the offender can be inferred from the examination of a crime scene, as it reflects distinctive aspects of their personality, as such, the investigator is able to corroborate data about the person and the data from the crime scene. These have been possible due to the careful application of criminology in the investigation of digital crimes, as it has enabled investigators to be provided with additional leads and direction. This implies that the investigations are always thorough with the exploitation and utilisation of the leads to criminal offenders of criminal rackets.

Table 6: Evidence gathering

	SD f (%)	D f (%)	NS f (%)	A f (%)	SA f (%)	Mean	Std
The investigators normally employ more than technical examinations of the digital evidence as technology by itself is inadequate to solve the problem.	47(38.8)	3(2.5)	9(7.4)	51(42.1)	10(8.3)	3.91	1.227
It is important to understand the motivation and the unique behavioural characteristics of the offender in order to effectively investigate digital cases.	3(2.5)	33(27.3)	15(12.4)	8(6.6)	60(49.6)	3.22	.950
The data acquisition process has a significant bearing on the entire digital investigation, and it is often challenged by the courts concerning infringements.	20(16.5)	7(5.8)	33(27.3)	24(19.8)	34(28.1)	3.31	1.151
To efficiently solve a digital crime, it is important to learn as much as possible about the individual behind the offence, as well as the victim	11(9.1)	23(19.0)	26(21.5)	8(6.6)	49(40.5)	3.56	1.163

Source: primary data 2022

Table 7: Transportation and Storage

	SD f (%)	D f (%)	NS f (%)	A f (%)	SA f (%)	Mean	Std
NIRA follows a guideline for electronic evidence transportation	5(4.1)	10(8.3)	23(19.0)	55(45.5)	26(21.5)	3.73	1.031
NIRA follows the chain of custody protocol standards	8(6.6)	17(14.0)	27(22.3)	47(38.89)	18(14.9)	3.43	1.124
Digital evidence is handled and stored in a manner that prevents the unintentional alteration or destruction of evidence by human interaction or environmental conditions	7(5.8)	23(19.0)	34(28.1)	35(28.9)	17(14.0)	3.27	1.122
NIRA uses tools that are thoroughly tested and acceptable legally	12(9.9)	28(23.1)	25(20.5)	28(23.1)	23(19.0)	3.19	1.292

Source: primary data 2022

Table 8: Criminal profiling

	SD f (%)	D f (%)	NS f (%)	A f (%)	SA f (%)	Mean	Std
Criminal profiling aids in the investigation of a variety of crime categories (e.g., murder, rape, sexual assault)	15(12.4)	16(13.2)	34(28.1)	35(28.9)	19(15.7)	3.20	1.283
Behavioural analysis of crime scenes assists in constructing profiles of offender characteristics	8(6.9)	10(8.6)	27(23.3)	60(51.7)	11(9.5)	3.48	1.017
Behavioural characteristics of the offender can be inferred from the examination of a crime scene, as it reflects distinctive aspects of their personality	17(14.7)	18(15.5)	36(31.0)	37(31.9)	8(6.9)	3.01	1.161
Careful application of criminology in the investigation of digital crimes has provided investigators with additional leads and direction.	16(13.8)	25(21.6)	28(24.1)	41(35.3)	6(5.2)	2.85	1.097

Source: primary data 2022

Table 9: Correlations for Process Model and Accuracy of Digital Forensic Investigations

		Evidence acquisition	Evidence authentication	Evidence analysis process	Accuracy of Digital Forensic investigations
Evidence acquisition	Pearson Correlation	1	.319	.415	.368**
	Sig. (2-tailed)		.000	.000	.000
	N	119	119	119	119
Evidence authentication	Pearson Correlation	.319	1	.432	.371
	Sig. (2-tailed)	.000		.000	.000
	N	119	119	119	119
Evidence analysis process	Pearson Correlation	.415	.432	1	.475**
	Sig. (2-tailed)	.000	.000		.000
	N	119	119	119	119
Accuracy of Digital Forensic investigations	Pearson Correlation	.368**	.371	.475**	1
	Sig. (2-tailed)	.000	.000	.000	
	N	119	119	119	119

***. Correlation is significant at the 0.01 level (2-tailed).*

Multiple Correlation Analysis

A Pearson product-moment correlation coefficient was computed to assess the relationship between the process model employed and the accuracy of digital forensic investigations carried out by NIRA-Uganda.

The findings in *Table 9* revealed that there is a significantly positive relationship between the process model used and the accuracy of digital forensic investigations at $(r) = 0.368^{**}$, at the level significant $p = (0.001)$ (2-tailed) given by the Pearson correlation. The process model encompasses evidence acquisition, evidence authentication and evidence analysis on one side and the accuracy of digital forensic investigations on the other side (see *Table 9*). This indicates that for process model employed significantly contributes to the accuracy of digital forensic investigations carried out. These findings

corroborate with [16], who opines that digital investigation investigators need to employ more than technical examinations of the digital evidence as technology by itself is inadequate to solve the problem. In addition, [17] states that, after identifying all the supporting evidence in a case, the investigators can create a more solid reconstruction of the crime that aids in understanding what happened and provides an explainable basis for expert judgment and opinion. To accomplish this crucial task in an investigation, the investigators must focus on different leads and behavioural analysis as part of the processes to authentic information”.

Multiple Regression Results

The study sought to assess process models and their role in enhancing the accuracy of digital forensic investigation in NIRA-Uganda. *Table 10* represents respondents’ opinions on process models.

Table 10: Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.368 ^a	.259	.249	1.2016

a. Predictors: (Constant), acquisition of evidence, authentication of evidence and analysing of evidence

Source: primary data 2022

Results in the model summary table reveal that $r^2 = 0.249$ (Adjusted R Square). This implies that three variables of acquisition of evidence, authentication of evidence and analysing evidence together predict the accuracy of digital forensic investigations by 24.9%. This means that 24.9% variation in the accuracy of digital forensic investigations is due to the sole cause of the process model encompassing acquisition of evidence, authentication of evidence and analysing evidence, while the remaining 75.1% is a result of other factors. This prediction is significant as envisaged in the way evidence is acquired, authenticated and analysed have all combined to determine the accuracy of digital forensic investigations. These findings corroborate with [18]. [19] developed a basic digital forensic investigation process called the Four Step Forensics Process (FSFP) with [20], [21] the idea that digital forensics investigation can be conducted by even non-technical persons. This process gives more flexibility than any other method so that an organisation can adopt the most suitable method

based on the situations that occur. From the final report and recommendations of the Computer Misuse Act, 2011 and Electronic Transactions Act, 2011, it is conclusively right to say there is a need to review bills & laws that involve the use of digital evidence in court [22]. The need to unite legislators, law enforcement agencies and privacy advocate groups together and come up with sound Standard Operation Procedures (SOPs) for forensic examiners as well as laws that can assist in having a fair and unbiased digital forensic investigations outcome.

Weight of the Model

The weights for the model that are illustrated in *Table 11* were obtained from unstandardised beta coefficients

Table 11: Coefficient

Coefficients ^a		Unstandardised		Standardised	t	Sig.
Model		Coefficients		Coefficients		
		B	Std. Error	Beta		
1	(Constant)	1.493	1.2016		5.746	.000
	Acquisition of evidence	.277	1.218	.389	3.269	.001
	Authentication of evidence	.213	1.235	.273	1.462	.003
	analysing evidence	.292	1.152	.311	2.279	.004

a. Dependent Variable: accuracy of digital forensic investigations

Source: primary data 2022

From *Table 11* on the findings for the acquisition of evidence, the unstandardised coefficients revealed (β) = 0.277; and Std Error = 1.218 and supported by sig-value 0.001 > 0.005. This implies that the process of evidence acquisition adopted by NIRA significantly predicts the accuracy of digital forensic investigations. Since Sig. 0.001 is less than the t-statistic value of 3.269 and the standard error value of 1.218; the study concluded that the process of evidence acquisition significantly predicts the accuracy of digital forensic investigations carried out by NIRA-Uganda.

Secondly, findings from *Table 11* on evidence authentication, the unstandardised coefficient revealed (β) = 0.213; Std Error = 1.235 and sig-value 0.003 > 0.005. This implies that the evidence authentication process has significantly contributed to the accuracy of digital forensic investigations carried out by NIRA-Uganda. Since Sig. 0.003 is less than the t-statistic value of 1.462 and the standard error value of 1.235. Therefore, the study concludes that the evidence authentication process significantly contributes to the accuracy of digital forensic investigations carried out by NIRA-Uganda.

Finally, findings from *Table 11*, for the evidence analysis process, the unstandardised coefficient revealed (β) = 0.292; Std Error = 1.152 and sig-value 0.004 > 0.005. This implies that the evidence analysis process has significantly contributed to the accuracy of digital forensic investigations carried out by NIRA-Uganda. Since Sig. 0.004 is less than the t-statistic value of 2.279 and the standard error value of 1.152; the study concluded that the evidence analysis process significantly predicts the

accuracy of digital forensic investigations carried out by NIRA-Uganda.

In light of the above, the model equation used is a linear equation as shown below;

$$Y=C+\beta_1X_1+ \beta_2X_2+ \beta_3X_3+ \epsilon$$

$$\text{Accuracy of Digital Forensic Investigations} = 1.493+ (0. 0.277* \text{evidence acquisition process}) + (0.213*\text{evidence authentication process}) + (0.292* \text{evidence analysis process}) + 0.711$$

THE Enhanced Digital Forensic Investigative Process Model (EDFIP)

The model was developed to provide an automated means of carrying out digital forensic investigations as a web-based application. The model is named EDFIP Model.

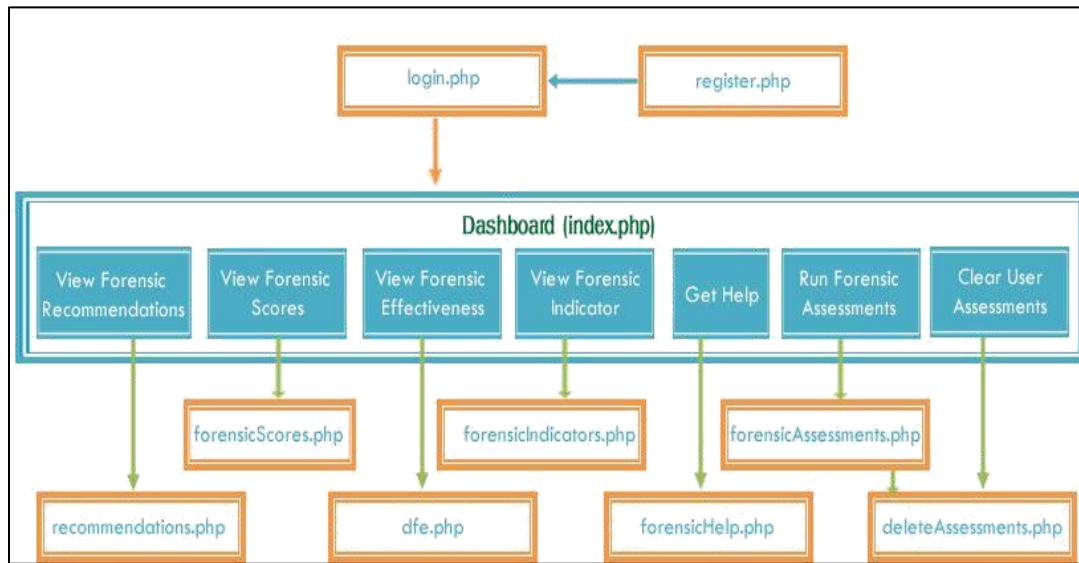
Design Processes

The Design process included analysis of requirements, specification of relevant software, implementation, and evaluation of the model.

System Architecture

The software system architecture of the model involves many interrelated components, herein referred to as modules, that work together to achieve the main objective of the design and deliver specification details of the model. Several independent components compressed and running as PHP files were coded and *Figure 2* presents how the independent components are interconnected.

Figure 2: Architecture of the EDFIP Model



The summary of the specific independent components of the model is presented as follows;

User Registration

This acts as the starting point for using the model without which the subsequent system functions

cannot be carried out. This module allows the user to register by providing their bio-data information and then stores them in the database to be used later for authentication of users. This module applies SHA256 cryptography on all plaintext passwords provided by the user before they are stored in the database.

Figure 3: Login Flowchart

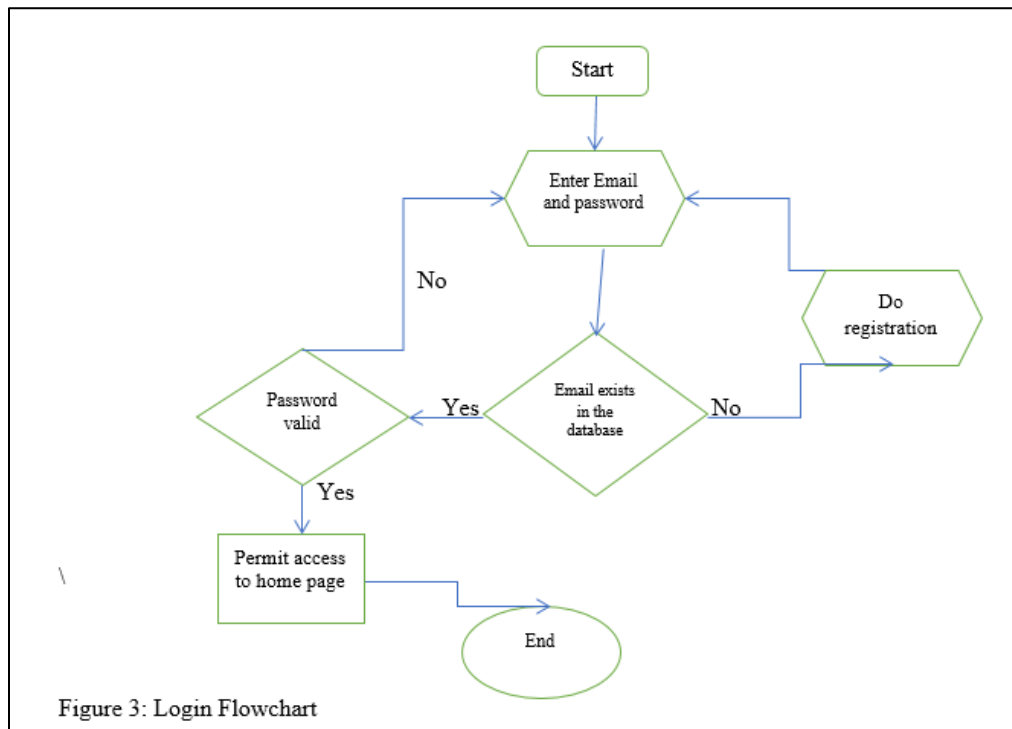
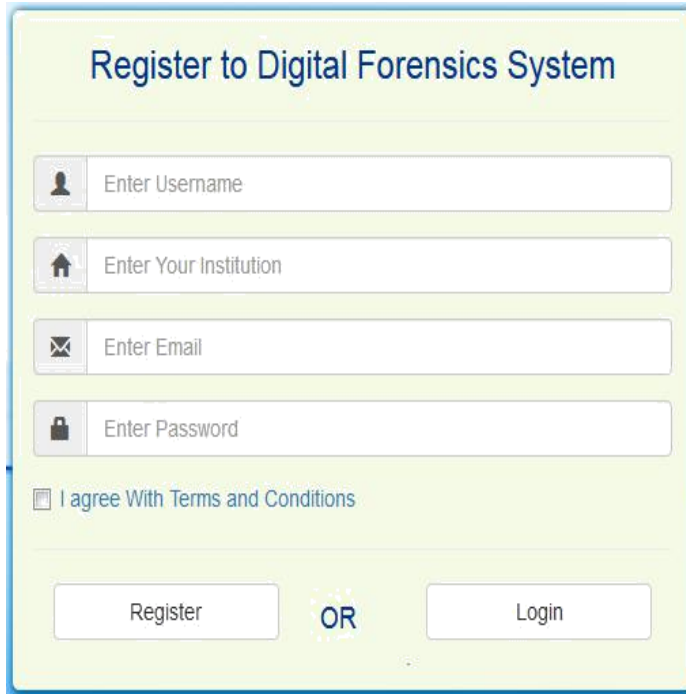


Figure 3: Login Flowchart

Figure 4: User Registration Form

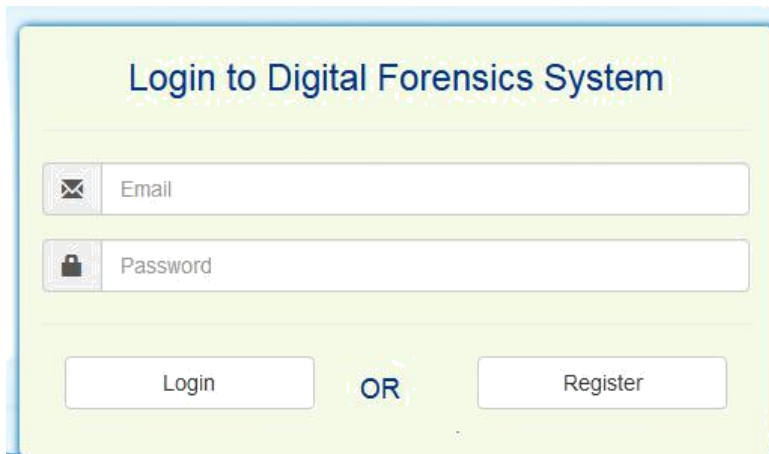


The registration form is titled "Register to Digital Forensics System". It contains four input fields: "Enter Username" (with a person icon), "Enter Your Institution" (with a house icon), "Enter Email" (with an envelope icon), and "Enter Password" (with a lock icon). Below the fields is a checkbox labeled "I agree With Terms and Conditions". At the bottom, there are two buttons: "Register" and "Login", separated by the text "OR".

User Login

This is the entry point to the system for registered users. It authenticates registered users, sets up user sessions.

Figure 5: User login



The login form is titled "Login to Digital Forensics System". It contains two input fields: "Email" (with an envelope icon) and "Password" (with a lock icon). At the bottom, there are two buttons: "Login" and "Register", separated by the text "OR".

User Logout

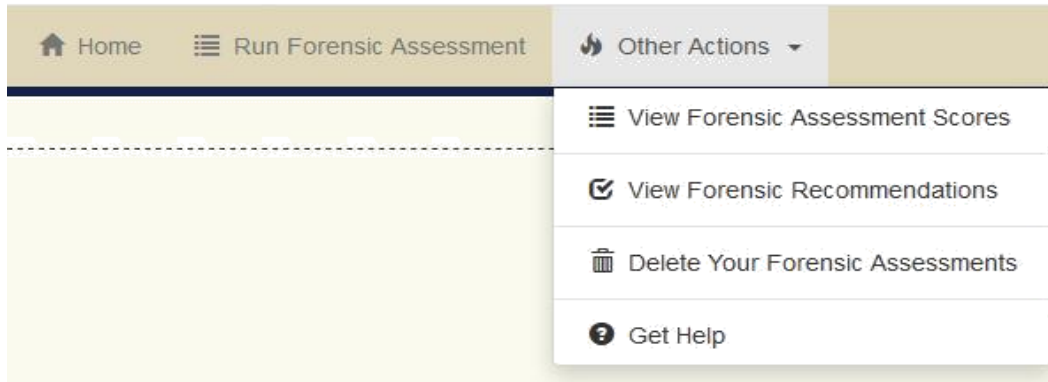
This is the exit point of the system for registered users. It destroys user sessions when they click the logout button or when they stay idle for a long.

User Navigation

This allows the users to navigate through the system easily and load different pages easily depending on the activities they intend they carry out within the system. There are two types of menus

that assure easy navigation within the system, namely, the header menu and the footer menu.

Figure 6: User navigation



User Dashboard

This component provides the user with a quick view of their usability status by providing vital information about; their percentage forensic

accuracy, their performance as regards various forensic investigations indicators, their average forensic scores, the number of times they have run forensic assessments and the number of recommendations they have.

Figure 7: Dashboard with no Active Assessments for the Logged in User

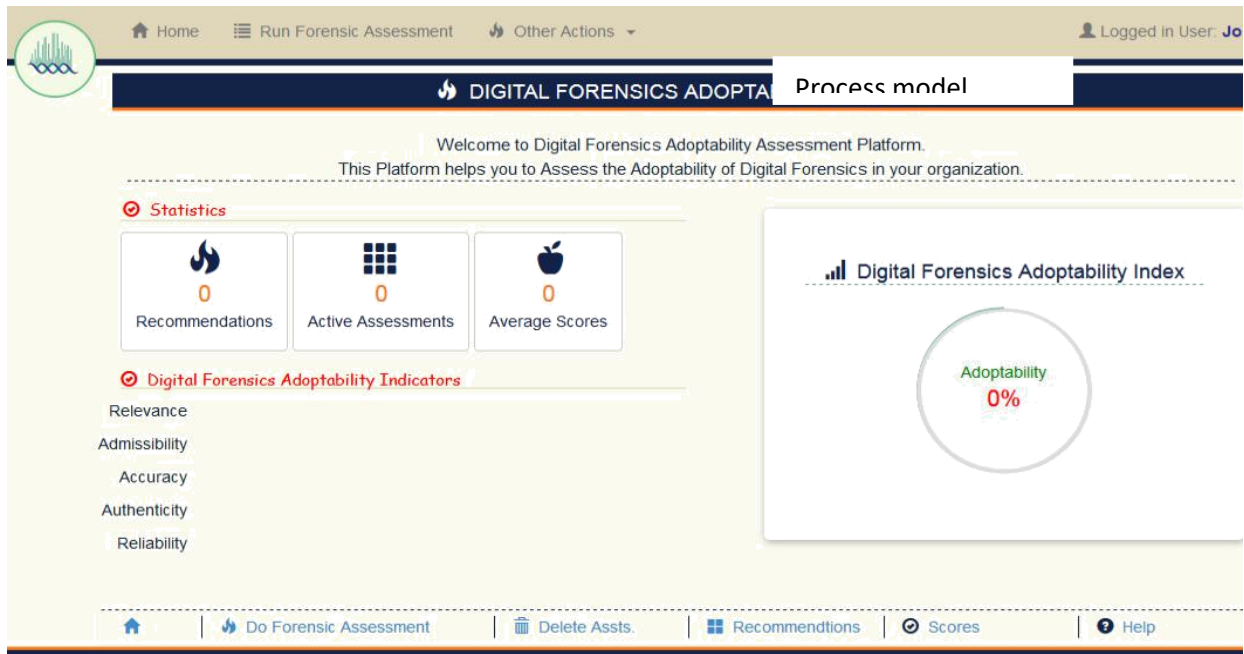
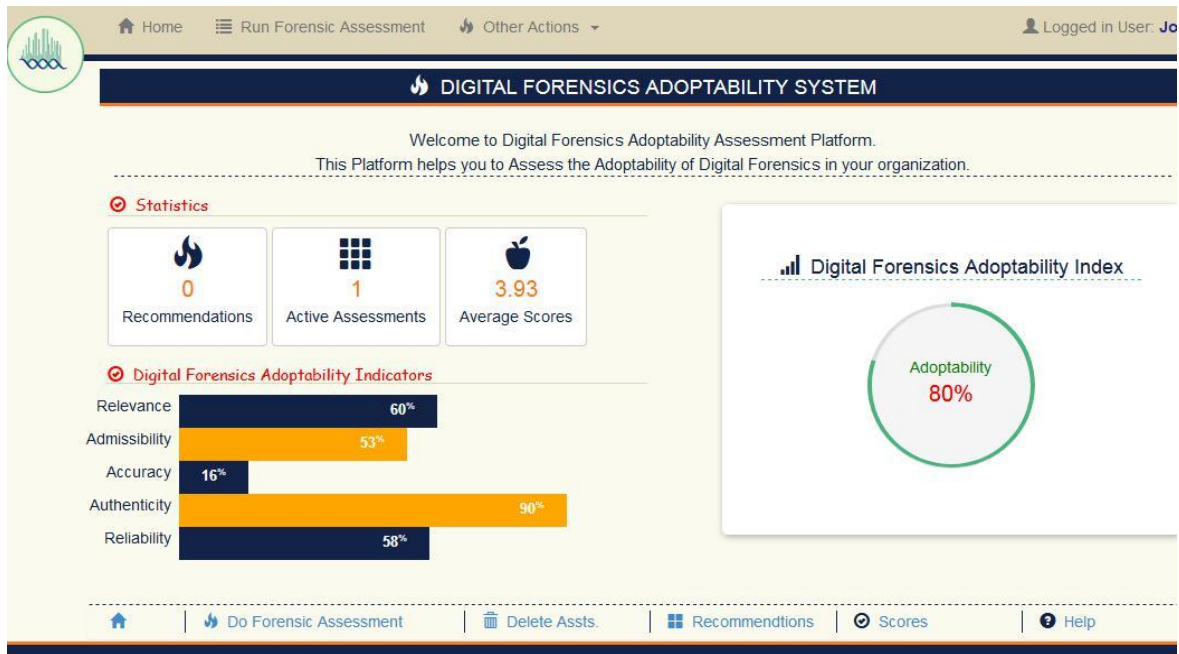


Figure 8: Dashboard with One Active Assessment for the Logged

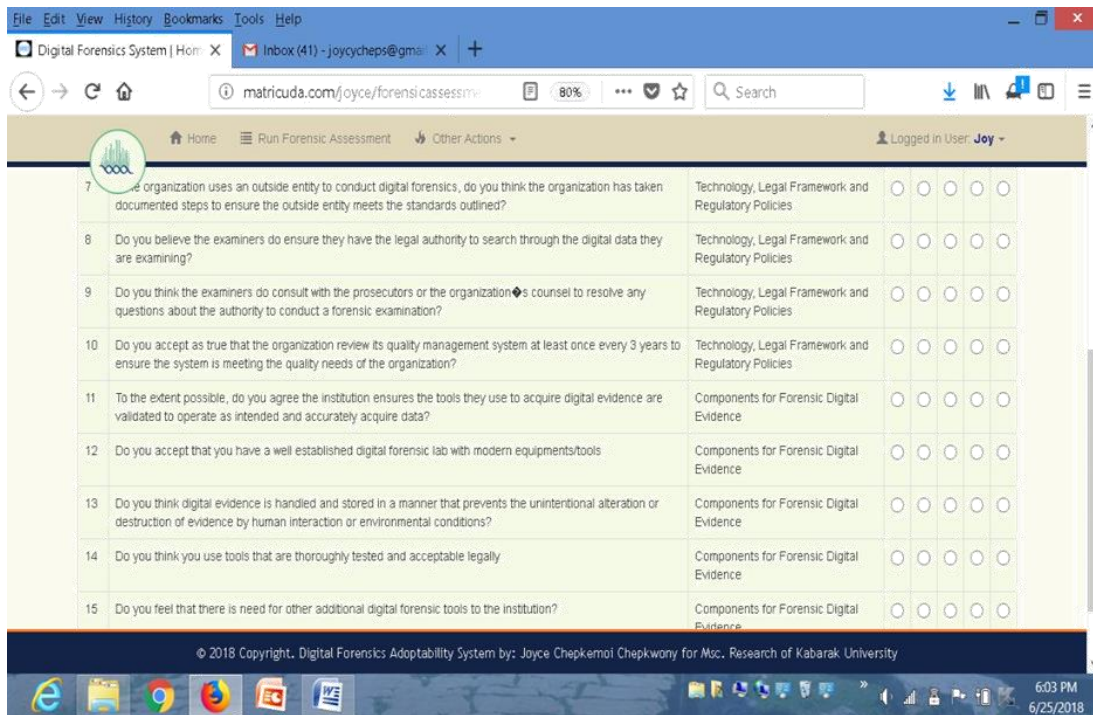


Forensic Assessments

This presents the user with forensic statements for which they assess on a Likert scale of 1 to 5 and

submit results, herein referred to as forensic scores, to the database. Forensic scores from this component form the basis for computing accuracy and generating other vital outputs.

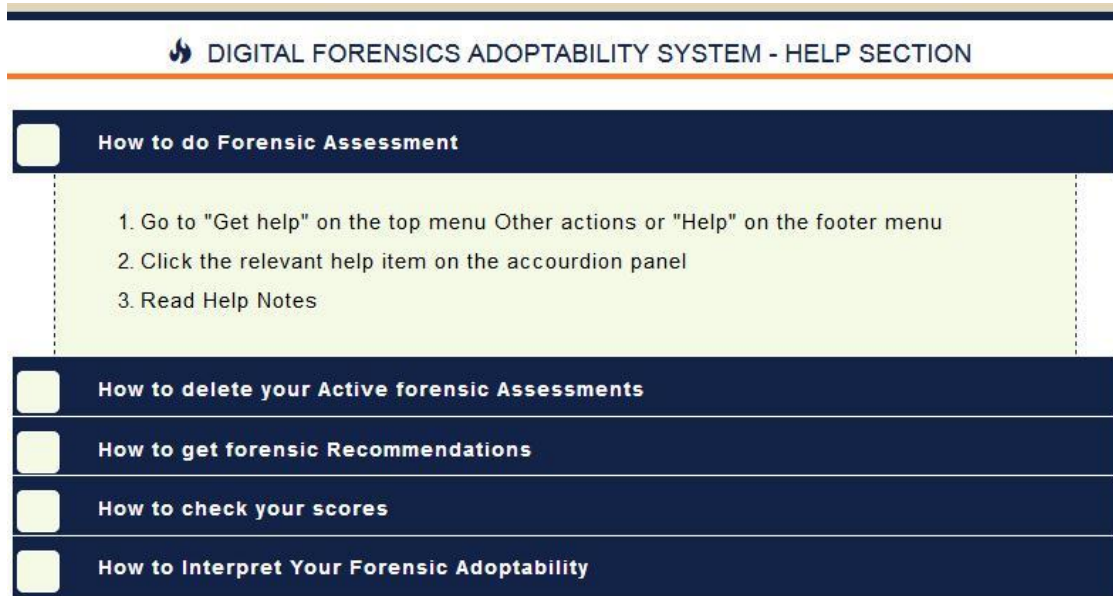
Figure 9: Forensic Assessments



Help Module

This component provides guidelines to the user on how to carry out several varied functionalities of the system.

Figure 10: Help Module



User Reports

This component provides vital reports to the user once they are done running forensic assessments. The reports produced by this component include; forensic scores report, forensic recommendations report and forensic evaluation of adaptability report available to the admin.

Databases

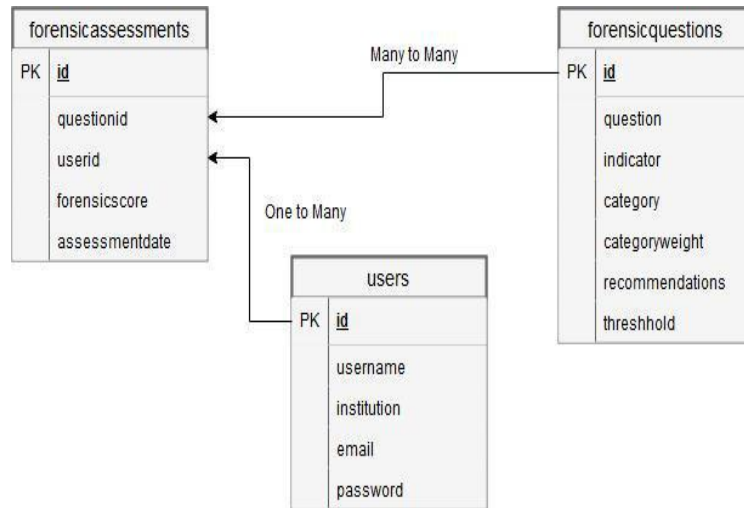
The model is driven by MySQL relational database engine with three database tables, namely users, forensic assessments and forensic questions.

Registration Module

For a respondent to get entry to the platform and perform an assessment for the relevance of their

digital forensics evidence collection tools, they are required to register. This process entails submitting details to the system that will be used to gain entry on subsequent logins. Such information includes; the name of the user, their email address, institution, username and their strong password. The duly filled registration form can be submitted. In this case, PHP scripts are used to fetch user posts and insert them into the database. This module is enriched with form validation tools; for instance, the email provided during registration must meet the email format criterion, and the passwords provided must be strong enough. At the database level, this module assures the privacy of user passwords by ensuring that no plain text (readable) passwords are stored in the database. It is therefore responsible for the encryption and storage of encrypted passwords. Overall, the registration module serves as the point of entry to the platform.

Figure 11: Entity relationship diagram



Evaluation of the Model

The model was evaluated after the design process to ascertain that it could perform the intended purposes. The intended objectives were set prior to

the design process and used for evaluation as a deliverables checklist when the design was done. As presented in *Table 12*, the delivered outcomes are tabulated alongside the intended goals. All the set objectives were achieved as shown in *Table 12*.

Table 12: Components, Goals and Deliverables from the model

Components	Goals	Delivered Outcomes
Registration	<ol style="list-style-type: none"> 1. Accept user Bio-Data 2. Post User Data to the Users Database 3. Hash Passwords at the Database Level 	<ol style="list-style-type: none"> 1. User Registration Form Accepts User Bio-data. 2. User Data Successfully posting to MySQL Database. 3. Passwords Hashed using SHA256
Login	<ol style="list-style-type: none"> 1. Permit Login with Correct email and password 2. Redirect user to Dashboard upon successful login 	<ol style="list-style-type: none"> 1. System Permits Login with Correct email and password 2. System Successfully redirects the users to their corresponding Dashboards upon successful login
Navigation	<ol style="list-style-type: none"> 1. Allow easy Navigation within the model 	<ol style="list-style-type: none"> 1. Easy navigation using two menus; that is, top menu and footer menu. 2. Dashboard panels provide links to various other pages
Dashboard	<ol style="list-style-type: none"> 1. Display digital forensic adoptability 2. Display forensic adoptability indicators 3. Display quick statistics 	<ol style="list-style-type: none"> 1. Digital forensic adoptability display achieved as an interactive percentage gauge. 2. Five forensic adoptability indicators display achieved through interactive horizontal bar graphs 3. Quick statistics panels for average forensic scores, active assessments and forensic recommendations

Adaptability Index Gauge

The formula derived after regression analysis in section 4 was implemented in the model basically to compute the process model’s accuracy in enhancing digital forensic investigations. This factored in all the scores belonging to the logged-in user to compute the adaptability. The formula was

automated as a PHP code, as presented in the snippet in *Figure 4*. A more interactive and readable presentation of the adaptability outcome for the user was done using web tools, namely, HTML5 to publish the Gauge, CSS3 for styling and JavaScript to animate the output. *Figure 12* shows the digital forensics adaptability output based on assessment scores for the active user.

Figure 12: Digital Forensics Accuracy Index Gauge

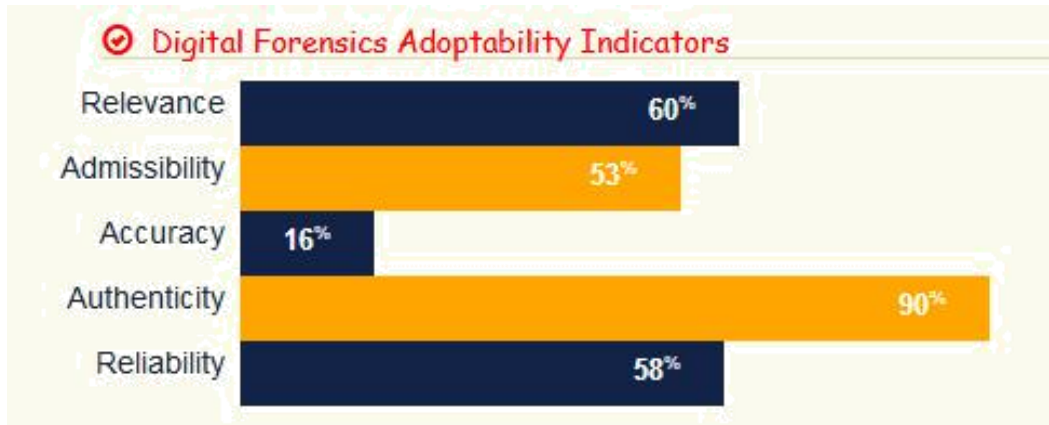


Adaptability Indicators

This is a section of the dashboard display that gives the user a quick view of the adaptability of digital forensics with respect to five forensics indicators, namely, Admissibility, Relevance, Authenticity, Accuracy and Reliability. The adaptability is computed for each indicator independently as a percentage index, and a comparative display of all

five indicators is presented as a responsive horizontal bar graph. This helps the users and their organisations to know the level of adaptability of their digital forensic collection tools with regard to the five indicators. The presentation of the comparative graph of the digital adaptability of forensic tools in relation to the five indicators is shown in *Figure 13*.

Figure 13: Digital Forensics Investigations Indicators



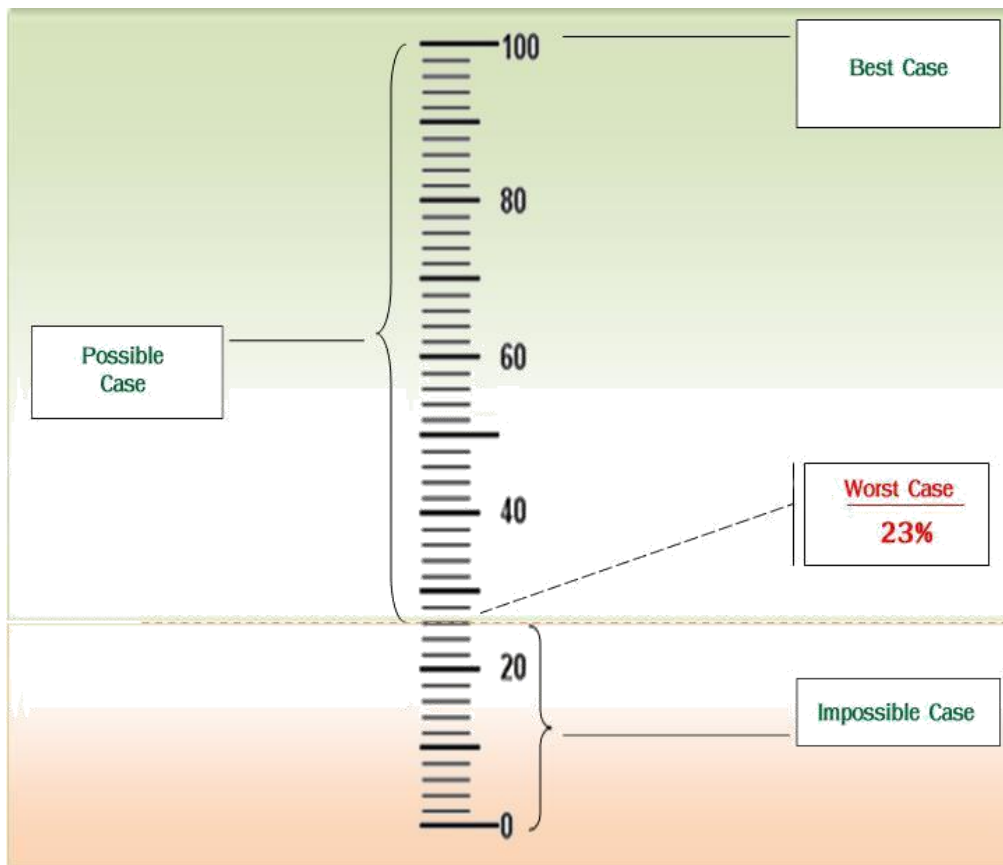
Adaptability Index Calibration

Based on the formula that was derived and used in the model to automate the determination of digital forensics adaptability, auspicious observations were made in regard to the output of the model. The upper limit of the scale is index 1 or 100 per cent. This is achieved when the user checks all the forensic assessment questions with a score of 5, meaning they strongly agree with all the assessment statements. The lower limit, on the other hand, was observed to be an index of 0.23 or 23 per cent. This is possible when the user disagrees strongly with all forensic assessment statements by scoring 1 for all the questions. The model as an instrument can possibly measure the adaptability of digital forensics between indices 0.23 and 1 or, put in other

words, 23 per cent to 100 per cent. This is referred to as a possible case.

The user, however, cannot achieve adaptability of between 0 and 23% simply because the choice of scale for this research was a scale of 1 to 5 Likert. The fact that the adaptability indices below 0.23 cannot be achieved can be explained simply with two reasons; one, the scale cannot allow the users to post a score of 0 during the forensic assessment, and two, the constant and the error term in the derived equation cannot permit outright 0 adaptabilities. The adaptability below index 0.23, in this case, is referred to as the impossible case. *Figure 14* presents the calibration of the model as an instrument, while equation 2 shows the PHP code snippet of the equation that was used to compute the adaptability of digital forensics.

Figure 14: Model accuracy enhancement Cases



```
$model accuracy = "SELECT ROUND (((0.528+SUM (a.forensicscore * b.categoryweight) + 0.369) /
(0.528+SUM (5 * b.categoryweight) + 0.369)*100), 0) FROM forensicassessments a INNER JOIN
forensicquestions b ON a.questionid=b.id INNER JOIN users c ON a.userid=c.id WHERE
a.userid=$user_id;"
```

CONCLUSION

Based on the process of digital forensic investigation, the evidence analysis process is a precursor for the accuracy of digital forensic investigations carried out by any institution or organisation.

The element of improper authentication leads to misinterpretations or false and wrongful expert conclusions. The lesson learnt here is that though the institution's forensic investigations are a game changer in forensic investigations, they are riddled with weaknesses which need interventions in order to improve their capacity and here Government intervention is very vital

Areas For Further Study

Given that the current study focused on the accuracy of digital forensic investigations as a result of the process model employed. A wider study involving police and security agencies is hereby recommended. This will facilitate a broader comparison and generalisation of the study findings. Based on this, further research could also be done on factors affecting the adoption of digital forensics and whether the existing laws support digital forensic processes.

Another study needs to be carried out on the factors affecting the application of forensic science in criminal investigations carried out by NIRA or security agencies like the police.

REFERENCES

- [1] I. O. Ademu, C. O. Imafidion, and D. S. Preston, "A New Approach of Digital Forensic Model for Digital Forensic Investigation," *International Journal of Advanced Computer Science and Applications*, vol. 2, no. 12, pp. 175–178, 2011, doi: 10.14569/IJACSA.2011.021226.
- [2] S. Daware, S. Dahake, and V. M. Thakare, "Mobile forensics: Overview of digital forensic, computer forensics vs. mobile forensics and tools," *International Journal of Computing Applications*, vol. 2012, pp. 7–8, 2012.
- [3] M. Pollitt, "Digital Forensic Research Conference A Framework for Digital Forensic Science." Accessed: Apr. 01, 2019. [Online]. Available: https://www.dfrws.org/sites/default/files/session-files/pres-a_framework_for_digital_forensic_science.pdf
- [4] M. Y. Nordiana Rahim, Ainuddin Wahid Abdul Wahab and I. I. and 4Miss L. M. Kiah, "Digital Forensics: An Overview of the Current Trends," 2014. https://www.researchgate.net/publication/280684566_Digital_Forensics_An_Overview_of_the_Current_Trends (accessed Jul. 27, 2020).
- [5] Gilbert Gilibrays Ocen, S. M. Karume, M. S. Mutua, G. B. Mugeni, and D. Matovu, "An Algorithm and Process Flow Model For The Extraction Of Digital Forensic Evidence In Android Devices," *International Scientific Journal Theoretical & Applied Science*, vol. 72, no. 04, Apr. 2019, doi: 10.15863/TAS.2019.04.72.1.
- [6] "NIRA | National Identification & Registration Authority." <https://www.nira.go.ug/home> (accessed Sep. 16, 2022).
- [7] 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, doi: 10.1177/001316447003000308.
- [8] J. C. Whitehead, P. A. Groothuis, and G. C. Blomquist, "Testing for non-response and sample selection bias in contingent valuation Analysis of a combination phone/mail survey *," 1993. Accessed: Apr. 19, 2019. [Online]. Available:

- <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.460.2661&rep=rep1&type=pdf>
- [9] D. Silverman, *Interpreting qualitative data: methods for analysing talk, text, and interaction*. SAGE Publications, 2006.
- [10] J. M. Morse, M. Barrett, M. Mayan, K. Olson, and J. Spiers, "Verification Strategies for Establishing Reliability and Validity in Qualitative Research," 2002. Accessed: Apr. 19, 2019. [Online]. Available: <https://journals.sagepub.com/doi/pdf/10.1177/160940690200100202>
- [11] W. Lawrence Neuman, "Social Research Methods: Qualitative and Quantitative Approaches W. Lawrence Neuman Seventh Edition," 2014. Accessed: Apr. 15, 2019. [Online]. Available: www.pearsoned.co.uk
- [12] C. Kothari, *Research methodology: methods and techniques*. 2004. doi: <http://196.29.172.66:8080/jspui/bitstream/123456789/2574/1/Research%20Methodology.pdf>.
- [13] C. B. Perry R, Hinton, Isabella McMurray, *SPSS Explained Second Edition*. 2014.
- [14] F. Fioravanti and F. Fioravanti, "Software Measurement," *Skills for Managing Rapidly Changing IT Projects*, no. January 1998, pp. 191–223, 2011, doi: 10.4018/978-1-59140-757-7.ch013.
- [15] T. E. Endres, "Advantages of rapid prototyping," *SAE Technical Papers*, 1999, doi: 10.4271/1999-01-3433.
- [16] R. Stoykova, "Digital evidence: Unaddressed threats to fairness and the presumption of innocence," *Computer Law & Security Review*, vol. 42, p. 105575, Sep. 2021, doi: 10.1016/J.CLSR.2021.105575.
- [17] D. Canter and D. Youngs, "Narratives of criminal action and forensic psychology," *undefined*, vol. 17, no. 2, pp. 262–275, 2012, doi: 10.1111/J.2044-8333.2012.02050. X.
- [18] S. Soltani and S. A. H. Seno, "A survey on digital evidence collection and analysis," 2017 7th International Conference on Computer and Knowledge Engineering, ICCKE 2017, vol. 2017-January, pp. 247–253, Dec. 2017, doi: 10.1109/ICCKE.2017.8167885.
- [19] S. A. Soltan Alharbi, J. W. J. Jens Weber-Jahnke, and I. T. Issa Traore, "The Proactive and Reactive Digital Forensics Investigation Process: A Systematic Literature Review," *International Journal of Security and Its Applications*, vol. 5, no. 4, pp. 59–72, 2011.
- [20] J. P. Venter and J. P. Venter, "Process Flows for Cyber Forensics Training and Operations", Accessed: Oct. 04, 2022. [Online]. Available: <http://130.203.136.95/viewdoc/summary?doi=10.1.1.103.1583>
- [21] N. M. Karie and H. S. Venter, "Towards a framework for enhancing potential digital evidence presentation," 2013 Information Security for South Africa - Proceedings of the ISSA 2013 Conference, 2013, doi: 10.1109/ISSA.2013.6641039.
- [22] H. Saini, Y. S. Rao, and T. C. Panda, "Cyber-Crimes and their Impacts: A Review 1," 2012