A MODEL FOR PREDICTING DIGITAL FORENSIC REINVENTION BY 2032 IN NIGERIA

[1]E. C. NWOSU, *[2]C. C. IBEBUOGU,[1]E. A. DUROHA,

[1]DEPARTMENT OF COMPUTER SCIENCE, GREGORY UNIVERSITY, UTURU ABIA STATE
[2]DEPARTMENT OF COMPUTER SCIENCE, IMO STATE UNIVERSITY OWERRI

Abstract:
Digital Forensics is relatively new in Nigeria, and whose incubation system available is insufficient to meet the demands explosion of higher Case loads and current internet multimedia devices, services and application intensive environment of cybercrimes has posed serious problems of incomplete web transactions. Stakeholders, security and law enforcement agencies in Nigeria are unwilling and feel reluctant to embrace digital forensics that will overcome the prevalent challenges inherent to cybercrimes in Nigeria because of inhibiting factors. This needs urgent readiness to overcome the tractions that are responsible for apathy to high rate of cybercrimes. If nothing is done, sometime, it may lead to corporate failure, the agencies may suffer disillusionment and frustration.
The objective of this study therefore is to design a model for predicting Digital Forensics refinement from Federal level to reach Local Government level in order to reduce the cybercrime rate in Nigeria by 2032 based on growth trend developed from statistical indices. The essence is to explore and analyze the factors that can encourage emergence and advancement of digital forensics true rewarding in the next 10 years, predicted to grow between 2022 – 2032, and use those factors to forecast growth, so that Digital Forensic Investigation and Legal evidences in court of law will receive boost in terms of growth and patronage. The studies also aim at designing a predictive model that simulates the behaviour of the restrictive policies on digital forensic advancement so as to ascertain the current impact on non-motivation, lack of standard, proper management, lack of proper human digital interface and unwillingness to overcome prevalent challenges inherent to cyber crimes in Nigeria. The motivation behind this study is to identify the inhibiting factors responsible for lack of standard motivation to embrace digital forensics in Nigeria. The methodologies that were deployed in packaging the model include: the Statistical Methodology, Structured Systems Analysis and Design Methodology (SSADM) and prototyping. The result is indeed functional software, programmed through Visual Basic Net (VB.Net) that can be used to simulate the behavioural impact of any government policy formulation for Information and Communication Technology Industry and Stakeholders. This is recommended to serve as a watchdog in curbing and checkmating cybercrimes and ensuring Digital Forensics true rewarding and flourish in Nigeria.

Keywords: Model, Predicting Digital Forensics, Cybercrimes, Reinvention, inhibiting factors.

1.0 Introduction:

Since the inception of digital forensics formerly known as "Computer Forensics Science" traced to the first training session held by the International Association of Computer Specialists (IACIS) in1991 [2]; there have been several threads of researches revolving round its adoption and enhancement.

This section therefore embodies the ideas drawn from the previous researchers' intuitions about the reinforcement of digital forensics in Nigeria. It is important to understand that, digital forensics include the act of making digital data suitable for inclusion into a criminal investigation. [3] [1] Stated that, computer forensics has been around for a while and is rapidly becoming a specialized and accepted investigative technique in a court of law with its own tools and legal precedents that validates the disciplines. it is a computing profession indicated to finding the truth. In-fact, in Nigeria, digital forensics is at its baby state [4, 5], only a few security and law enforcement agencies practice it. Economic and Financial Crime Commission (EFCC) and National Drug Law Enforcement Agency {NDLEA} are among the few security and law enforcement agencies that have incorporated digital forensics in their investigation processes, though there is no proof of any literature showing the procedure they use. According to [6] a digital forensics process is capable of providing an investigator with relevant information required during an investigation process. Digital forensics is a new frontier of crime investigation for security and law enforcement agencies [7]. There is no regulatory body that regulates digital forensics investigation, and there is no standardized model common to all security agencies. This is a major challenge and drawback in crime investigation in Nigeria most of the cases are often discharged and acquitted for lack of admissible evidence. [8]. Computer forensics investigators use a combination of technology and detective like skills to uncover evidence of criminal activity in computers [9]. Past researchers [10,11,12] have shown that digital forensics is the only way forward for effective crime investigation. According to [13], for digital evidence to be admissible in a court of law, the investigator must follow some basic steps. Hence, he proposed the first computer forensics investigation process model in 1984 [14]. [1], stated that, the domain of digital forensics is not to assign guilt or innocence, but rather to find facts in form of electronic evidence that can be presented in a coherent way, so that others may weigh the evidence and then assign guilt or innocence where appropriate.

Today, cyber forensics is a term used in conjunction with laws enforcement and is offered as courses at many colleges and universities around the world [3]. As society becomes more digitized, the need for skilled personnel in this arena becomes more and more pressing [15].

Therefore this study addresses the theme of transformation through innovation and designing a model for predicting Digital Forensics Reinvention by 2032 in Nigeria. It describes the attempt to design and implement a new paradigm of Digital Forensics system. The reinvention process within the Digital Forensics is itself an innovation, particularly in the methodology developed to address issues related to this research. This study presents a high level model of Reinventing Digital Forensics which conceptualizes this process.

The process of developing this paradigm involved innovation in a wide range of areas: a new holistic paradigm of Digital Forensics to meet the demands explosion of high rate of case loads.

This is an actual process to refine and model the digital forensics in order to fine tune and forecast the future growth trend and emergence in curbing the high rate of cyber criminals in Nigeria. This is motivated to see if its development and advancement can lead to the actual setup of reinforcing and metamorphosing a working and flourishing digital forensics and at same time peep into the future perfection and workability of digital forensics in Nigeria.

This will serve as a guide to policy formulation and information and communication gateway project for control of cybercrimes in Nigeria. Bureau of Labour Statistics predicted digital forensics industry to grow by 17% between 2016 – 2026, due to higher caseload, state and local government predicted to hire additional digital forensic science technicians in order to keep up with the demand.In researcher's helicopter view, 17% prediction of digital forensic industry growth from 201 – 2026 is very small compared to high rate and proliferation of cyber criminals in the country. Also state and local government hiring additional digital forensics science technicians should not arise.

This is the area the predictive model of reinventing digital forensics by 2032 in Nigeria is very necessary. This will redefine digital forensics to go beyond formal landscape.

The study has clearly shown that digital forensics acceptability and workability are dependent on government ability to revisit the policies and inhibiting factors responsible for lack of standards and lack of motivation to embrace digital forensics in Nigeria.

To appreciate the current status of Digital Forensics in Nigeria, and how ready Nigeria is, it is important to have an understanding and in-depth study of the existing digital forensics system so as to identify some loopholes and at the same time suggest way forward. However, due to the increasing rate of cyber-attack every single year, agencies from across the world are spending a huge amount of money on best talents from cyber forensics, in-spite of that, more challenges are increasingly coming to light in the public domain. Overly, complex cyber-attacks make the deployment of applications and service updates challenging, the low crime reporting culture of the public, paucity of police funding, corruption, inadequate training of police officers in criminal investigations delayed duplication of investigation, missing investigation case files, and lack of forensic science facilities, experts and the cost of maintenance takes up a significant proportion of IT budgets, combined with infrastructure, lack of standard and service failures that can take a considerable amount of time to identify and resolve, these issues are increasingly hitting Digital Forensics Industry and Stakeholders satisfaction. In-spite of all these problems, yet there is no concrete plan either by government or stakeholders in Nigeria to reinvent the Digital Forensics in order to ensure structural investigation to obtain a reliable chain of evidence on cyber-attacks for organization and individual data for application.

The situation is indeed a threat to the Nation and constitutes economic, social and political doom. As a result of the above points, this study therefore tries to explore the inhibiting factors responsible for apathy to reliable Digital Forensics. Inhibiting factors were identified and addressed for the need of the organizations to ensure that future of Digital Forensics is explored, with an emphasis on the challenges and the advancement needed to effectively protect modern societies and pursue cyber criminals.

These can support the current demand, and future demand is paramount, by evolving Digital Forensics, a fabric modelling system that overcomes many of the inherent weaknesses found in present legacy systems.

1.1 Statement of Problems:

Despite the fact that digital forensics has been around for a while since 1991 as an "investigative technique in a court of law"; Basically, a computing profession dedicated to finding the truth [1], it has neither produced the desired effect nor provided the needed impact on the sector in Nigeria. It is unfortunate that most law enforcement agencies are not skilled set to use digital forensics to gain evidence in crimes that is computer related. The stakeholders and digital forensics industry in Nigeria are still operating with the prevalent system that can no longer accommodate todays always on, multimedia devices, services and application intensive environment where the cyber criminals hide. In-fact, cyber information is at risk, hence, there are no confidentiality, no integrity and availability of authentic information and information services. The underlying prevalent system has not kept pace with innovation in frontline operational system. The Law Enforcement Agencies cannot establish any legal evidence against the cyber criminals. They only determine, the yahoo boys or cyber criminals, when they see anybody, riding on flashy cars or check the Bank Account of the person, they can only interrogate the person, without any potential legal evidence to be presented in a court of law, especially in Nigeria. The coordinating structure and the framework of the current system can no longer meet the demands explosion of higher caseloads leading to high rate of various criminalities in Nigeria. Youths are getting more involved in cybercrimes. They compromise the accuracy of a forensic report or testimony. There is no regulatory body that regulates digital forensics investigation, and no standardize model common to all the security agencies. Most of the cases are often discharged and acquitted for lack of admissible evidence.

The underlying infrastructure has not kept pace with current system, leading to increasing pressure being placed on already overstretched backend infrastructure. Hence, major problems to be addressed in this study are to find out why Nigerians have not fully embraced wide range structure of digital forensics and identify the inhibiting factors that are responsible for lack of motivation to embrace coordinating structure and new framework of digital forensics in Nigeria, and suggest what can be done to reinvent the digital forensics in Nigeria. This study tends to find out if there is anything government can do to motivate stakeholders and law

enforcement agencies to embrace new model of digital forensic and finally identify the possibility to redesign a predictive model that will predict the growth trend of digital forensics in Nigeria. This will serve as a guide to policy formulation in Nigeria.

1.2 Aim and Objectives:

The aim is to design a model that predicts the future of digital forensics reinvention system in Nigeria in the next 10 years. The system will be able to achieve the following functionalities or objectives:

1. Explore and analyze the inhibiting factors that are responsible for lack of standard and motivation to embrace digital forensics in Nigeria.
2. Develop digital forensics reinvention mathematical predictive model, based on growth trend developed from statistical indices.
3. Use the model to guide for policy formulation and for reinvention digital forensics growth Trajectory in Nigeria.

1.3 The Need for Digital Forensics Reinventive Prediction Model In Nigeria.

Our nation's once unchallenged pre-eminence in digital forensics is being overtaken by apparent inconsistency throughout the polity. Our society and its digital forensics seem to have lost sight of basic purposes and of the high expectations and disciplined effort needed to attain them.

In-fact, government should stop building empires for themselves instead of working towards a concerted goal for establishing digital forensics, hence, to lose the secret of one's technology is to lose one's technology and competitive advantage. The current digital forensics process in Nigeria can no longer cope with the magnitude of high rate of cyber criminalities, there is need to balance legal evidence and social objectives and to find new ways to manage and checkmates the multiplicity of cyber criminalities, otherwise web-transactions and information is at risk!

The current forensics process need to change – changes in the 21st Century global context place mounting on digital forensics of 19th century to change as the figure 1, High level predictive model illustrates.

At the macro-level, digital forensics are expected to fix the ever widening tear in social fabric of crime investigation and legal evidence. They are expected to fix national confidentiality, integrity and availability of cyber security areas of concern. At the micro-level, there are increased expectations of what digital forensics can /should do: they are increasingly held accountable for matters which occur in control and checkmating crimes within the three tiers of government levels.

The people and Nation will not sit quietly in the country with substandard digital forensics process and listen to unskilled, security and law enforcement agents give them pre-digested knowledge, I think that, there is need for a change.

There is a legal imperative to make digital forensics positive, powerful and relevant experience for need of people.

It is intolerable that current digital forensics process should ever bore people, suppress their expectations, confidentiality and integrity and dumb them down in the global information world because of the cyber criminalities, lack of standard and expertise to control and checkmates the multiplicity of criminalities in the country. So how do digital forensics move from 19th century "One size fits all" approach to cybercrime investigations and legal evidence, more appropriate for the 21st century multimedia knowledge crime society?

Digital forensics are IT global systems. They are responsive and intuitive and have the capacity to create [and recreate].

To bring about effective change within such a system, a contemplative holistic approach is needed; an approach that combines flexibility, collaboration and humour. The answer is for adoption of the reinventive prediction model (RPM) of approach to transformation.

2.0 Materials And Methods

In this study, due to the nature of this research, the study deploys the following methodologies:

1. The standard procedure called "The Structured System Analysis and Design Methodology (SSADM)"a thorough fact-finding technique which was adopted in finding out and analyzing the existing system, its modes of operation and the challenges inherent in it.
2. Mathematical / Statistical Methodology used to extract field data for analysis and interpretation.
3. Hypothetical-deductive methodology: This is an example of mathematical / statistical methodology using questionnaire approach in which source data are subjected to analysis after being collected.
4. The Visual Basic-Net (VB.Net) was used to write the codes.
5. Finally, prototyping was used in packaging the model.

2.1 Model Formulation:

In the course of this study, the following mathematical models are employed:

1. **Mathematical Models:** Mathematical models grow out of equations that determine how a system changes from one state to the next (differential equations) and/or how one variable depends on the value or state of other variables (State Equations), these can also be divided into either numerical models or analytical models. For example, in the course of this study, a mathematical model was formulated thus:

   $$Y = a + B_1 X_1 + B_2 X_2 + \ldots + B_n X_n,\ B_0 \quad eq\ (8.1)$$

   a = Constant, where Y^ is the predicted or expected value of the dependent variable, X_1 though X_P are P distinct independent or predictor variables, B_0 is the value of Y when a11 of the independent variables (X_1 through X_p) are equal to zero, and bi through b_p are the estimated Regression Coefficients. Each Regression Coefficient represents the change in Y relative to a one unit change in the respective independent variable.

2. **Statistical Models:** A statistical model describes how one or more random variables are related to one or more other variables. The model is statistical when the variables are not deterministically but stochastically related in this study, the multiple regression were utilized in analyzing the data since the variables are stochastically related.

3. **Hypothetic-Deductive Models:** is a proposed description of scientific method. According to it, scientific inquiry proceeds by formulating a hypothesis in a form that could conceivably be falsified by a test on observation data. A test that could and does run contrary to predictions of the hypothesis is taken as a falsification of the hypothesis. A test that could but does not run contrary to the hypothesis corroborates the theory. It is then proposed to compare the explanatory value of completing hypothesis by testing how stringently they are corroborated by their predictions.
This model is very helpful since the researchers needed to ascertain if the variables identified as inhibiting factors for digital forensics advancement and growth actually have relationship with lack of standard and unwillingness or reluctant to embrace digital forensics in Nigeria. To assess also the impact of digital forensics process since its introduction, a hypothesis is equally required. Hence, the choice of the hypothetic-deductive model.

2.2 **Model Assumptions:**

This specifies the equations to be deployed in coding the simulator /predictor. Here multiple regression using ordinary differential equation (ODE) is applied.

The general purpose of multiples regression (the term was first used by Pearson, 1908) in [16], is to learn more about the relationship between several independent or predictor variables and a dependent or criterion variable using a general model:

$Y = a + b_1 X_1 + b_2 X_2 + \ldots + bnXn+$

Where, a = Y intercept; points $b_1, b_2, \ldots$, bn = The slope of X_1; X_2…; Xn respectively. Explaining the model in a more general term, given a data set. $(Y_1, Xn, \ldots Xip)^{Ti} = i = 1$ of n.

Statistical units, a linear regression model assumes that the relationship between the dependent variable y_1 and the P – Vector of repressors x_1 is Linear. This relationship is modelled through a disturbance term iT error variable $Ɛ_1$ an unobserved random variable that adds noise to the linear relationship between the dependent variable and regressors.

Thus, the model takes the form

$Y_1 = \beta_1 X_n + \ldots + \beta_p X_{1p} + Ɛ_1 = X_1^T \beta + Ɛ_1, ì = 1, \ldots, n$ Eq. [9.1]

Where ^{T} denotes the transpose, so that $X_1^T \beta$ is the inner product between vectors X_1 and β. Often, these n equations are stacked together and written in vector form as:

$Y = x\beta + Ɛ$ or $Y = a + BX$ Eq • [9.2]

Where:

$$y = \begin{pmatrix} y_1 \\ y_2 \\ \\ y_n \end{pmatrix}, x = \begin{pmatrix} X_1^T \\ X_2^T \\ \\ X_n^1 \end{pmatrix} = \begin{pmatrix} X_{11} \ldots X_{1P} \\ X_{21} \ldots X_{2P} \\ \\ X_{n1} \ldots X_{nP} \end{pmatrix}, Ɛ = \begin{pmatrix} \beta_1 \\ \beta_2 \\ \\ \beta p \end{pmatrix}, \beta = \begin{pmatrix} Ɛ_1 \\ Ɛ_2 \\ \\ Ɛn \end{pmatrix}$$

The Ordinary Least Squares (OLS) method minimizes the sum of squared residuals, and leads to a closed – form expression for the estimated value of unknown parameter β.

$\hat{\beta} = (X^T X)^{-1} X^T y = (\Sigma X_1 X_1^T)^{-1} (\Sigma X_1 y_1)$ Eq • (9.3)

The estimator is unbiased and consistent if the errors have finite variance and are uncorrelated with the regressors.

$\Sigma [X_1 Ɛ_1] = 0$ Eq • (9.4)

Or $\hat{y} = b_0 + b_1 X_1 + b_2 X_2 + \ldots + b_p x_p$ Eq • (9.5).

$a + B_1 X_1 + B_2 X_2 + \ldots + B_n X_n$

$B_0 = a =$ constant

Where $\hat{y}$ is the predicted or expected value of the dependent variable, X_1 through Xp are p distinct independent or predictor variable, b_0 is the value of Y when all of the independent variables(X_1 through X_p) are equal to zero, and b_1 through b_p are the estimated regression coefficients.

Each regression coefficient represents the change in Y relative to a one unit change in the respective independent variable.

In the multiple regression situations, b_1 for example, is the change in Y relative to a one unit change in X_1, holding all other independent variables constant (i.e. when the remaining independent variables are held at the same value or are fixed).

The digital forensics inhibiting factors Identification Number [$F_1 – F_9$] will be used for simulation, coding and manipulated in the equation to observe changes (positive or negative) that may occur due to changes in their beta coefficients. Hence, in this design we intend:

1. To use indices from the inhibiting factors' statistical analysis to stimulate the trajectory of future growth of digital forensics if the trend remains linear or altered by policy summersaults.
2. Maintain a stakeholder's database and complaints database; produce meaningful reports for management and policy making.
3. The model can help to assist the stakeholders, security and law enforcement agencies and government functionaries to try "What if" assessment of new Information and Communication Technology policies before, during and after implementation.

2.3 **Analysis**:

We analyzed the data using three scenarios as shown in Tables 1-3, and Figures 2-4:

1. Scenario 1: Testing Data for scenario 1 as shown in Figure 1 (graph/output):
   The scenario1 are the beta coefficients of the inhibiting factors as obtained from SPSS analysis as shown in Table 1:
   $F_1 = 0.182$, $F_2 =$).176, $F_3 = 0.187$,
   $F_4 = 0.195$, $F_5 = 0.196$, $F_6 = 0.191$, $F_7 = 0.185$, $F_8 = 0.192$, $F_9 = 0.203$, Base year = 2022, year Gap = ten (10) years.
   The results are as shown in Table 1 and Figure 2.
   Scenario 1: Trajectory graph as shown in Figure 2:
2. Scenario 2: This scenario II tested the system, when the beta coefficients are removed or improved upon. The results are shown in Table 2 And Figure 3.

   Testing Data for Scenario II
   $F_1 = 0.382$, $F_2 = 0.476$, $F_3 = 0.387$, $F_4 = 0.492$, $F_5 = 0.396$, $F_6 = 0.491$,
   $F_7 = 0.395$, $F_8 = 0.392$, $F_9 = 0.403$: Base year 2022, year Gap = Ten (10) years.
   Table 2 shows when the inhibiting factors are removed / improved or adjusted positively.
3. Scenario III: Table 3 shows when the inhibiting factors get worse or adjusted negatively as shown in figure 4, Scenario III data output/graph testing data for Scenario III:

F_1 = -0.182, F_2 = -0.176, F_3 = -0.187
F_4 = -0.195, F_5 = -0.197, F_6 = -0.191
F_7 = -0.185, F_8 = -0.192, F_9 = -0.203:

2.4 Evaluation Criteria

The indices derived from the statistical analysis were deployed into our model:

$Y = a + B_1 x_1 + B_2 x_2 + \ldots + Bnxn$ Eq • (8.1) above, translated and finally evaluated using the model:

$Y = a + \beta_{F1} X_1 + \beta_{F2} X_2 + \ldots + \beta_F nXn$ (adjusted equation) with input Beta values of ($F_1 – F_9$), resulting to the production into the digital forensics predictive model (DFRPM) which is based on multiple linear regression model.

Where: Y = digital forensic reinvention = the dependent Variable,
(Value for the year being predicted);

a = constant; $F_1 – F_9$ are the government policies on (inhibiting factors); and $X_1 – Xn$ = independent variables (the period of forecast), and β is the Beta coefficients which measures growth index and this is applied in the three different scenarios;

1. As it is now with government policies on (inhibiting factors) on digital forensics.
2. Hypothetical adjustments of the Beta indices if government policies on (inhibiting factors) are removed or improved upon.
3. Hypothetical adjustment if government policies on (inhibiting factors) become stiffer or gets worse.

The three scenarios demonstrated expected growth or decline of digital forensics.

3.0 **Results.**

Comparing the results of the above three scenarios:
In scenario one, the results of the digital forensics Non motivation, improper management, lack of proper human digital interface and unwillingness for advancement in Nigeria has a relationship with the government polices (inhibiting factors) like: inadequate training of police officers in criminal investigations [F_1]; paucity of police funding [F_2]; low crime reporting culture of the public [F_3]; Corruption-delayed duplication of investigation case files and missing case files []F_4]; Lack of forensic science facilities and experts [F_5]; Rise of anti- forensics techniques and lack of government support on condition of anonymity. [F_6]; Privacy preserving investigations and lack of admissible evidence [F_7]; Lack of development of standards and regulatory body. [F_8] Borderless cyber infrastructure - heterogeneous information [F_9]. And other policies as identified during systems analysis that the inhibiting factors are responsible for apathy to digital forensics advancement in Nigeria.

See figure 2: of scenario one above and as shown in figure 2. Sample output. Adjusting the indices in scenario one positively (scenario two) indicating the removal or improvement on the above policies (inhibiting factors) shows that digital forensics advancement improved and may become feasible and viable. And this is as expected.

The result is as shown in figure 3 of scenario two above, sample output. In scenario three, when the indices were adjusted negatively to test the future of digital forensics, if government policies (inhibiting factors) worsened, the result also indicates that if government still stiffens their policies (inhibiting factors) that digital forensics will collapse completely. This is as indicated by figure 4 of scenario three above and as shown in figure 4; sample output.
Finally, the results of the in – depth analysis and further synthesis of the actual result and the expected result described herein, provided a further insight and clear indication that the test data was true reflection of the challenges of digital forensics in Nigeria and thus that the software performed as expected.

4.0 Discussion

As challenging as this research problem is, efforts were made to assess the feasibility and viability of identifying factors that can encourage digital forensics for reinvention and use the factors to forecast growth. This serves as a tool for policy formulation in Nigeria.
Real-Time Interviews were conducted to capture real life feedback from stakeholders and law enforcement agencies to strengthen the quality of analysis and close any gap in predictive model. In fact, a hypothetic deductive method was employed to collect field data from stakeholders, security and law enforcement agencies in Nigeria and these data were analyzed using SPSS analysis.
A model for predicting digital forensics reinvention is undoubtedly the concept that can bring about the desired digital forensic growth for the law enforcement agencies and cyber security in Nigeria especially in the Nigerian's telecommunication market, not only because it can provide improvement in the web transactions but also, as uncovered in this study, it will proliferate creativity among service, stakeholders to embrace digital forensics reinvention, and value added services to remain competitive.

5.0 Conclusion

As Nigeria is playing Catch-up in the evolution of digital forensics scheme already successful in many countries; the government has a strategic role to play. Government's role should focus on providing strategic directives using functional by-laws that will provide enlightenment and trust by the members of the public.
The research conducted in this study has indicated that stakeholders, security and law enforcement agents are more privy to embrace the advancement of digital forensics scheme if government ameliorates the bottlenecks in the digital forensics process. but if government allows the existing inhibiting factors on digital forensics process adoption to remain, stakeholders, security and law enforcement agents may not be motivated to embrace the system.
The reduction or elimination of most of the inhibiting factors makes the advancement of digital forensics feasible and viable And of course, should government further stiffen the current inhibiting factors, the digital forensics will totally die in no distant future.

5.1 Recommendation

1. The government should plan to develop the regulatory body, legal and technical structure for the implementation of digital forensics in Nigeria and also establish reliable commission (body), education and research institutions, steering committee and project task team, as well as creating awareness of the emergence of digital forensics in the country.
2. Government needs to appoint the steering committee and project team based on experience, qualification, Expertise and must be devoid of any political agenda, who will help government to create new laws and legislation that will afford digital forensics stakeholders and its service provisions with legal certification.
3. This committee and the team will also carry out digital forensics processes and redesign that, which will provide government, the stakeholders, and public good deliverables.
4. A law should be enacted in line with certain provisions of certain sections of the selected body's. Act Number, which vests the body with the exclusive right to regulate the digital forensics processes in Nigeria.
5. The monitoring and the enforcement of compliance with regulations in order to ensure fairness and equity in the digital forensics processes must be considered.
6. The framework will spell out the inhibiting factors that are responsible for apathy to digital forensics processes and decides optimal solutions, and also the framework will spell out the digital forensics rules for implementing the government objectives of protecting the stakeholders' security and law enforcement agents' interest in digital forensics processes.
7. Government should support the stakeholders, train security and law enforcement agencies on the condition of anonymity – incentives, sponsorship training and on power generation. This will be a revolutionary step in towards reinventive digital forensics process in Nigeria.

Acknowledgements
The authors thank Prof. Oliver E. Osuagwu for his assistance in analyzing the sample statistical packages, and Dr. Emma Ekwonwune for his assistance in editing the manuscripts.

References

[1]. Wolfe, Henry B., (2003) Computers and Security, El Servier Science Ltd, PP. 26 – 28 (www.sciencedirect.com)
[2]. New Technologies; inc (Forensics-intl.com)
[3]. S. Neuner et al; "Time is on my side: Steganography in file system meta data," Digital Investigation, Vol. 18 Supplement, 2016, PP. S76 – S86.
[4]. Rukayat A. Ajetunmobi, Charles O. Uwadia and Florence A. Oladeji (2016). A survey and critique of digital forensic investigation models, international journal of computer science and information security. Vol 14 no. 12.

[5]. National Information Technology Development Agency (NITDA) (2014). Standards for digital and computer forensics in Nigeria. Draft Vo. 2.
[6]. Umesh Sigh, NehaGaud (2005). Analysis of digital forensic investigation models. Vol.2, PP 144 – 149.
[7]. Norwich University Online (2015). Role of Computer Forensics in Crime. Information Security and Assurance (online) available at www. Online.norwich.edu/academic-program/resources/role-of-computer-forensics-in-crime
[8]. Soyombo O. (2005). Integrating empirical research in the planning and training programs of Nigeria Police. Options and Prospects. Alemike Etani E. O. [Eds] Crimes and Policing in Nigeria: Challenges and Options. Lagos: CLEEN Foundation: PP. 126 – 145.
[9]. Nelson, Bill, Philips, Amelia, Enfinger, Frank and Steward Chris (2004). Guide to Computer Forensics and Investigations. Thomson, Course Technology, Boston.
[10]. Alphonso Rivera (2018). BTK Serial Killer: the Power of Computer Forensics (online) available at www.bakerfield.com/kern-business-journal/btk-serial-killer-power-of-computer-forensics/article-dd8foad3-f833-5066-8e25-dcf 6d406d5ctthtml.
[11]. Hannah George (2018). Computer Forensics: Criminal Investigation: infosec institute (online) available at www.resources.infosecinstitute.com/category/computerforensics/ introduction/areas-of-study/computer-forensics-investigations/criminal investigations/#gref.
[12]. Dwan C. (2018). Notable Computer Forensics Cases. Infosec Institute (online) available at www. resources.infosecinstitute.com/category/computer forensics/ introduction/notable-computer-forensics-cases/#gref.
[13]. M.G. Noblett, M.M. Pollitt & L.A. Presley (2000). "Recovering and Examining Computer Forensics Evidence", Forensics Science Communications, Vol.2, No. 4.
[14]. Pollitt M.M. (2007, April). An ad hoc review of digital forensic models. In Systematic Approaches To Digital Forensic Engineering, 2007, SADFE 2007. Second International Workshop on (PP.43-54). IEEE.
[15]. Rude, Thomas, (2000). Guidance seizure methodology for computer forensics. http://www.crazynights.com/seizure.html.
[16]. Field A. (2005) Discovering Statistics using SPSS.Sage, London.

Tables

Table1:Inhibiting Factors from {F_1 – F_9}

BASE GROWTH TREJECTORY YEAR: 2022 – 2032 (10 YEARS)
DIGITAL FORENSICS
SCENARIO I: INHIBITING FACTORS FROM {F_1 – F_9}.

YEAR	F_1	F_2	F_3	F_4	F_5	F_6	F_7	F_8	F_9
2023	7	6	7	7	7	7	7	7	7
2024	12	12	12	13	13	13	12	13	13
2025	18	17	18	19	29	18	18	19	20
2026	23	22	24	25	25	24	24	24	26
2027	29	28	29	31	31	30	29	30	32
2028	34	33	35	37	37	36	35	36	38
2029	40	38	41	43	43	42	40	42	44
2030	45	44	47	48	49	48	46	48	50
2031	51	49	52	54	55	53	52	54	57
2032	56	55	58	60	61	59	57	59	63

F_1 = Inadequate Training of Police Officers in criminal investigations
F_2 = Paucity of Police Funding
F_3 = Low Crime Reporting Culture of the Public
F_4 = Corruption – delayed duplication of investigation case and missing files.
F_5 = Lack of Forensics Science Facilities and Experts
F_6 = Rise of Anti-Forensics Techniques and Lack of Government Support on Condition of anonymity.
F_7 = Privacy Preserving Investigations and lack of admissible evidence.
F_8 = Lack of Development of Standards and Regulatory Body
F_9 = Borderless Cyber Infrastructure – Heterogeneous Information

Figure 2: Scenario I data output/graph

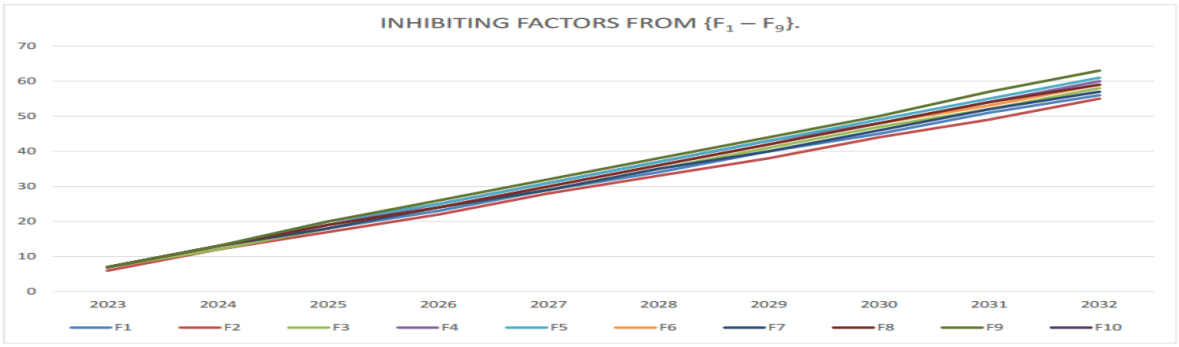


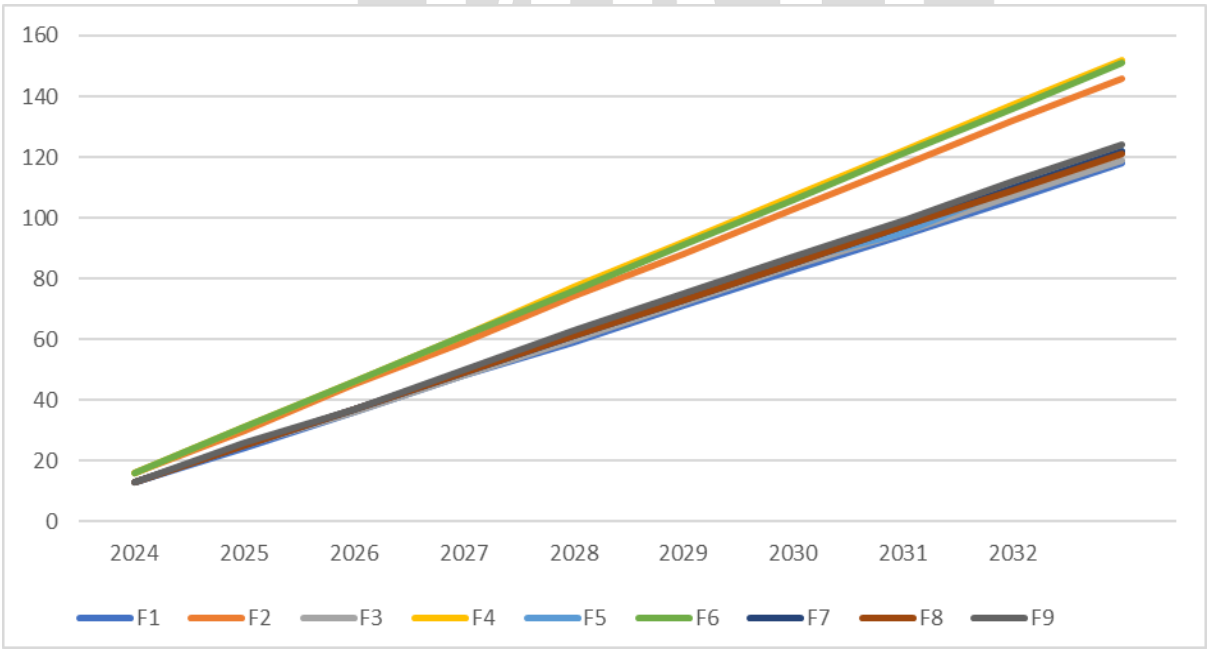
Table 2: Inhibiting Factors from (F_1 – F_9)

Digital Forensics Growth Trajectory Prediction
Base Growth Year: 2022-2032 (10) Years Trajectory
Scenario II: Inhibiting Factors from [F_1 – F_9].

YEAR	F_1	F_2	F_3	F_4	F_5	F_6	F_7	F_8	F_9
2023	13	16	13	16	13	16	13	13	13
2024	24	30	25	31	25	31	25	25	26
2025	36	45	36	46	37	46	37	37	37
2026	48	59	48	61	49	61	49	49	50
2027	59	74	60	77	61	76	61	61	63
2028	71	88	72	92	74	91	73	73	75
2029	83	103	84	107	66	106	85	85	87
2030	94	117	95	122	68	121	97	97	99
2031	106	132	107	137	110	136	110	109	112
2032	118	146	119	152	122	151	122	121	124

F_1 = Inadequate Training of Police Officers in Criminal Investigation
F_2 = Paucity of Police Funding
F_3 = Low Crime Reporting Culture of the Public
F_4 = Corruption – delayed duplication of investigation case and missing files.
F_5 = Lack of Forensics Science Facilities and Experts
F_6 = Rise of Anti-Forensics Techniques and Lack of Government Support on Condition
F_7 = Privacy Preserving Investigations
F_8 = Lack of Development of Standards and Regulatory Body
F_9 = Borderless Cyber Infrastructure – Heterogeneous Information

Figure 3: Scenario II data output/graph



Scenario II: Trajectory Graph As Shown In Figures 3:

Digital Forensics Growth Trajectory Prediction.
Scenario III: The Test Data for Scenario III As Given Below And The Results As Shown In Table 3: And Figure 4:

F_1 = -0.182, F_2 = -0.176, F_3 = -0.187
F_4 = -0.195, F_5 = -0.197, F_6 = -0.191
F_7 = -0.185, F_8 = -0.192, F_9 = -0.203:

Base Year = 2022, Year Gap = Ten (10) Years.

Table 3: Shows when the inhibiting factors get worse or adjusted negatively.
Digital Forensics Growth Trajectory Prediction.
Scenario III: trajectory graph as shown in figures 4:

Table 3: Inhibiting Factors from [$F_1 – F_9$]

Base growth year: 2022 to 2032 (10) years
Digital Forensics Growth Trajectory:
Scenario III: Inhibiting Factors from [$F_1 – F_9$].

YEAR	F_1	F_2	F_3	F_4	F_5	F_6	F_7	F_8	F_9
2023	-7	-6	-7	-7	-7	-7	-7	-7	-7
2024	-12	-12	-12	-13	-13	-13	-12	-13	-13
2025	-18	-17	-18	-19	-19	-18	-18	-19	-20
2026	-23	-22	-24	-25	-25	-24	-24	-24	-26
2027	-29	-28	-29	-31	-31	-30	-29	-30	-32
2028	-34	-33	-35	-37	-37	-36	-35	-36	-38
2029	-40	-38	-41	-43	-43-	-42	-40	-42	-44
2030	-45	-44	-47	-48	-49	-48	-46	-48	-50
2031	-51	-49	-52	-54	-55	-53	-52	-54	-57
2032	-57	-55	-58	-60	-61	-59	-57	-57	-63

F_1 = Inadequate Training of Police Officers in Criminal Investigation
F_2 = Paucity of Police Funding
F_3 = Low Crime Reporting Culture of the Public
F_4 = Corruption – delayed duplication of investigation case and missing files.
F_5 = Lack of Forensics Science Facilities and Experts
F_6 = Rise of Anti-Forensics Techniques and lack of Government Support on Condition of anonymity
F_7 = Privacy Preserving Investigations and Lack of Admissible evidence
F_8 = Lack of Development of Standards and Regulatory Body
F_9 = Borderless Cyber Infrastructure – Heterogeneous Information

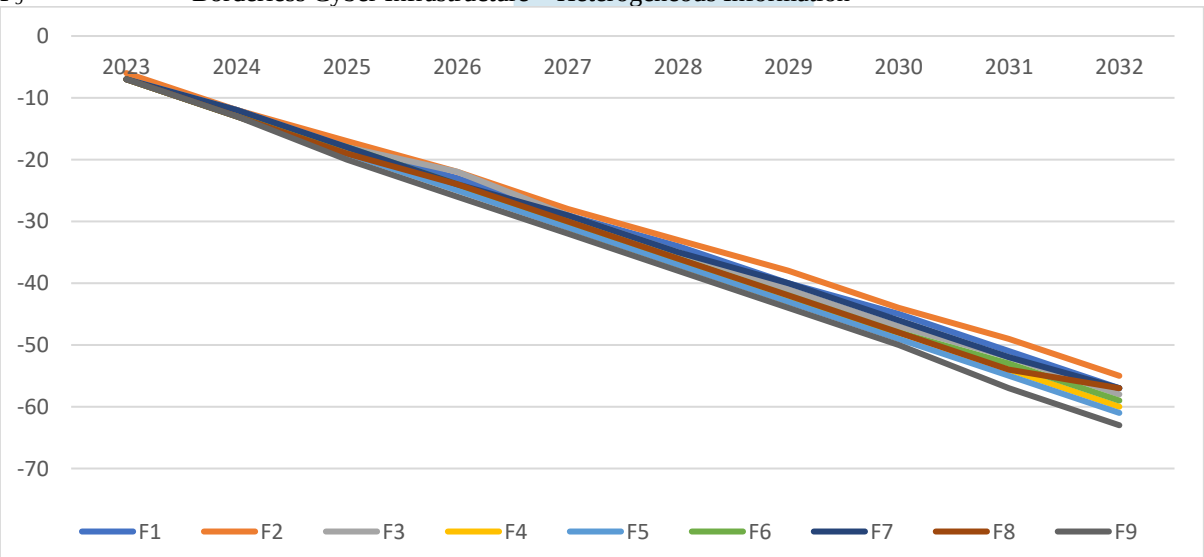
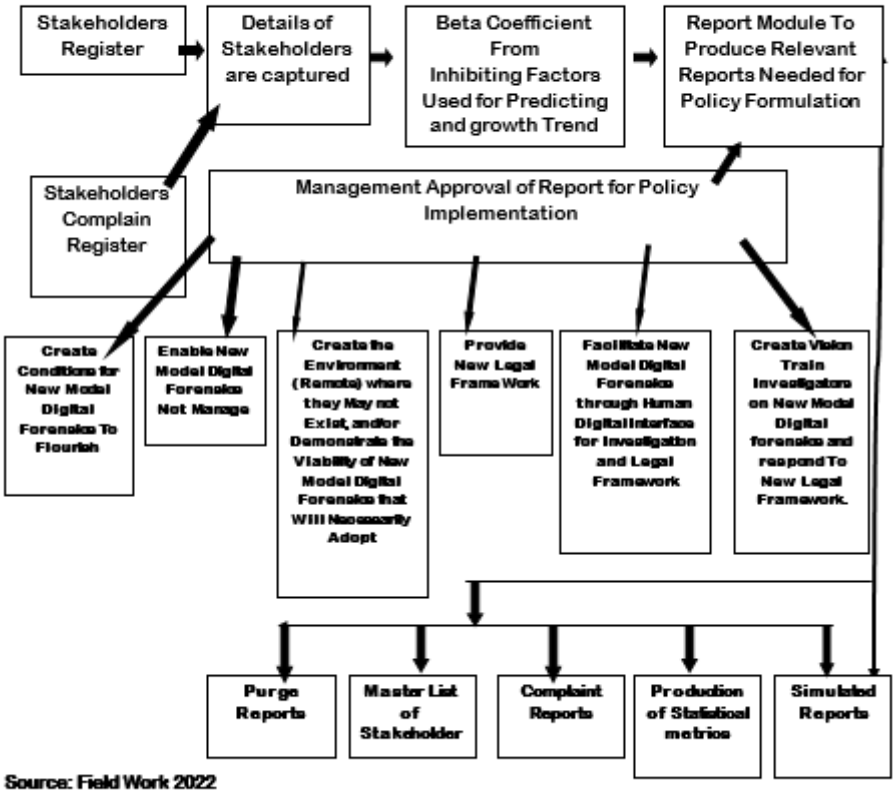


Figure 4: Scenario III data output/graph

Figure 1: **High Level Model of the Proposed Digital Forensics Reinventive Predictive Model (RPM).**



Source: Field Work 2022

Figure 1. High Level Model of the Proposed Reinventive Digital Forensics Predictive Model