Mara Research Journal of Computer Science & Information Security
Vol. 3, No. 1, September 2018, Pages 34 – 43, ISSN 2518-8453

Adoptability Model for Digital Forensic Evidence in Kenya

Joyce Chepkemoi Chepkwony
School of Computer Science and Bioinformatics
Department of Information Technology Security
Kabarak University, Private Bag 20157, Kabarak, Kenya
Email: joycycheps@gmail.com

Received: September 6, 2018
Published: September 22, 2018

Abstract
As the attacks on the cyber space continue to intensify, digital crimes continue to be reported at large and therefore to curb on this attacks, this research offers a solution by implementing an automated model that provides a way of computing digital forensics adoptability index by use of a web-based application. The model uses PHP server – side scripting language to program the system controls, CSS3 used for system styling, MySQL as a database engine and descriptive research design approach for implementing the model.

Keywords: Admissibility, Digital, Evidence, Forensic, Investigation, Adoptability

1. INTRODUCTION

Kenneally (2002) notes that in legal cases evidence is either admitted or not depending on the relative weight of its probative and prejudicial value. In Kenya, digital forensics process is often faced with challenges like admissibility, accuracy, authenticity, non-repudiation, relevancy, credibility, reliability, completeness and convincing to juries, because of poor standards like ISO 17799 and COBIT, regulatory policies, best practices, procedures / processes, governance, technologies, staff legal and ethical. Kshetri (2013) points out that with the current future, the value of forensic computing will increase for the Kenyan companies, to the law enforcers and to the legal practitioners. There are fundamental reasons that demand more concentration and attention to the cybercrime and the capacity to support in investigation and prosecution of cyber offenders.

Routine activity theory (RAT) advances the accessible model that crime occurs where motivated offenders and suitable targets (victims) interact in the absence of capable guardians (Williams, 2015). According to Bossler *et al.,* (2012), despite the assumption of complexity and multiple jurisdictions, perhaps up to one third of fraudulent cybercrime may involve offenders and victims living in the same state or country.

1.1 Statement of the problem

The growing incidence and risk of inappropriate, illegal and/or criminal computer behaviours has increased the need to build bridges between technical and legal areas of expertise in order to produce more effective defensive and offensive responses. Although, there is already a large volume of literature on organizational, technical and legal issues pertaining to computer misuse and e-crime, there have until recently, been only limited explorations of the interrelationships between these issues. This has been partly, because of the lack

of a conceptual framework within which to position these different approaches and partly because of the complexity of the specific sets of legal and technical challenges faced (Hannan et al., 2003).

Training or studies on technology acceptance by the law enforcers may lead to effective use of digital forensics (Lin *et al.*, 2004). The acceptance and development of digital forensics in Kenya has been very slow, because of the inappropriate regulatory policies, standards, procedures, technologies, and legal and governance challenges. For the progress of computer forensics, the law ought to keep pace with the advancement of the technology. Adams (2012) notes that, unlike some other areas that carry out forensic practice, digital forensic practitioners do work in a number of different environments and the existing methods tend to focus only on particular areas, like law enforcement, thereby failing to put into account the other needs of the other fields working in other areas like the incidence response. The deep knowledge of the problem area for this research was fulfilled through the extensive review of the associated literature with respect to the analysis done by the researcher and came up with a forensic adoptability gauge.

1.2 Research question

How will a web based application for computing forensic adoptability index be implemented?

1.3 Objective of the study

To implement a web based application for computing forensic adoptability index for the Kenya Police Service in Kenya.

2. LITERATURE REVIEW

2.1 Adoptability of the technological models

Previous studies have shown that developing countries have not yet derived expected benefits from digital forensic technology as very few organizations have the structures in place to enable them to conduct cost effective, low-impact and efficient digital investigations. In Kenya, the adoption, maturation and proliferation of digital forensics is slow due to inappropriate regulatory policies, procedures/processes, standards, technologies, legal and governance challenges (Moturi, 2011). Adoptability of the technological models in courts will improve the trust and confidence by the public to the institution. because of the access to justice and quality of justice offered. There are new models that have been planned that will try and speed up the investigation processes and also solve various problems normally encountered in forensic investigation, though many leaders of the court don't focus well on the IT issues and therefore struggling hard to manage the technology projects. According to Garfinkel & Simson (2010), digital forensics tools have not kept up with cyber crime and the technology since the current digital forensics tools were designed to help investigators find specific evidence and not to assist in investigations.

2.2 Decisions on Innovation adoption

Most of the innovations in organizations are borrowed rather than invented. The behavioural preference of the decision maker also influences much on if to adopt an innovation or not. IT governance as a formal structure tries to support technology tools by making decisions, resolving institutions problems, allocating the required resources and comes up with optimal solutions for the whole system and not for separate parts (Lawrence, 2012). In Figure 1 below, Lawrence points out reasons on decisions to adopt the innovation.

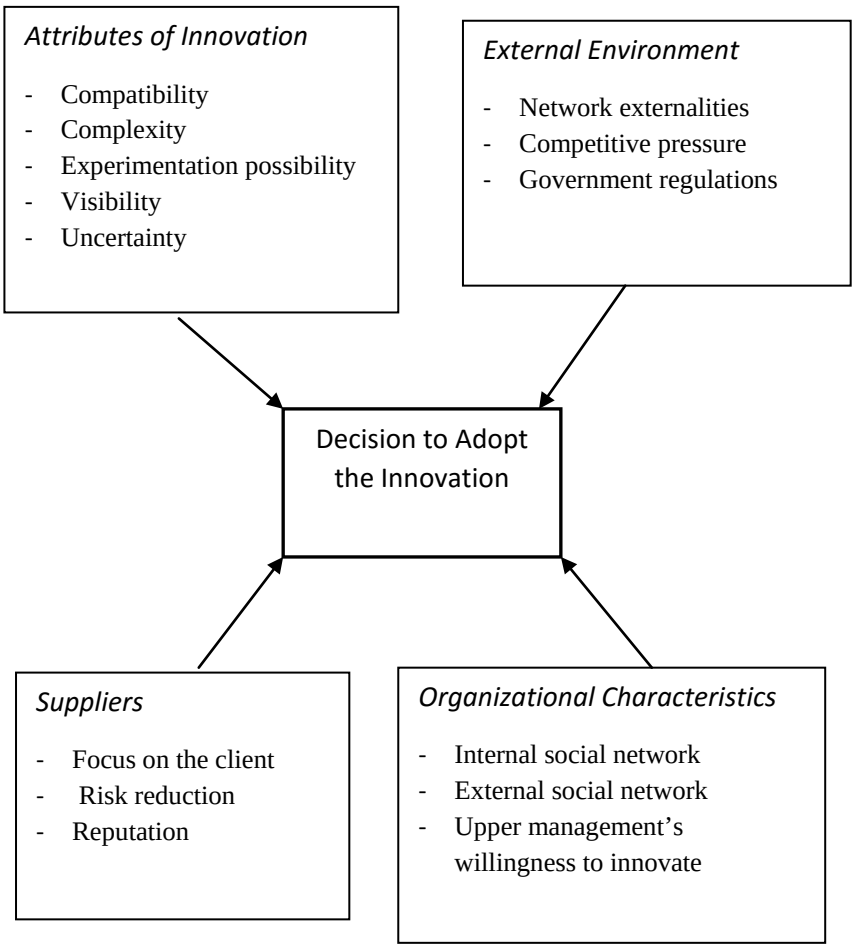


Fig. 1: Technological adoptability model
Source: Lawrence P. Webster, (2012)

2.3 Digital Forensics security fundamentals

According to Saks and Koehler (2005), evaluation of forensic evidence actually should be scientific, including that the reliability of methodologies be testable, and requiring that forensic evidence be evaluated and presented to the courts in a logically correct manner. Losavio and Adams' (2006) notes that the core IT Security fundamentals to digital forensics are; Confidentiality, Integrity and Availability (CIA).

3. METHODOLOGY

In this study, throwaway prototyping methodology was adopted. According to Dennis *et al*., (2005), throwaway prototyping methodology has a reasonably thorough analysis stage used to collect information and produce ideas for the perception of the system.

3.1 Software Engineering and Design

Software engineering and design of the model was achieved using PHP programming language for controls, MySQL database engine for storing system data, JQuery and JavaScript to add response to the system and CSS3 to style the layout of the model. Rapid prototyping process was used as the most ideal in designing of the model. The database and tables were created and relationships defined. The processes were coded using PHP and Jquery and the output styled with CSS3. With the digital forensic adoptability

system, the main functions of the model being the user registration, user login, user forensic assessment and the reports as discussed in the next sections.

3.1.1 User registration

This 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 a strong password.

3.1.2 User login

This is the entry point of the system for only the registered users. It authenticates the registered users and sets up user sessions.

3.1.3 Forensic assessment

This presents a user with forensic statements which they assess in a likert scale of 1 to 5 and submitted results to the database, herein referred to as the forensic scores.

3.1.4 Reports

Once done with the assessment, reports are produced which include the forensic scores report and the forensics recommendations. There is also the forensic evaluation report which is only available for the admin of the system.

4. SYSTEM DESIGN

The model was designed by use of a prototype. The following figures 2 to 5 shows the flowcharts of some of the main modules in the system together with a database schema. Below is Fig. 2 showing the login flowchart of the system.

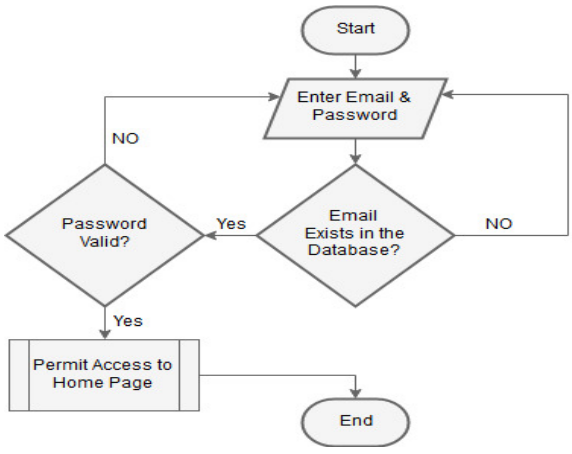


Fig. 2: Login Flowchart
Source: Researcher (2018)

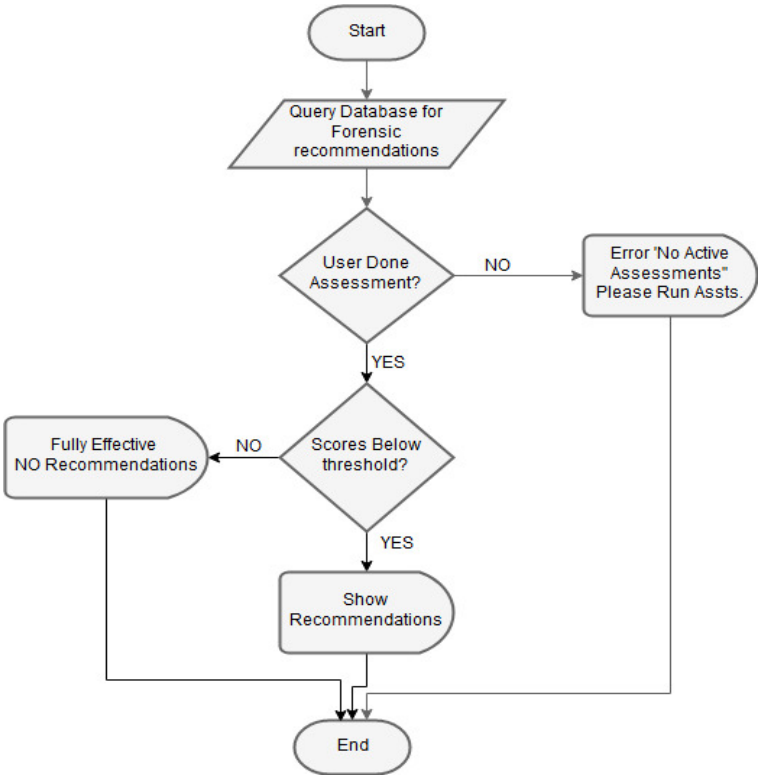


Fig. 3: Forensic Recommendations Flowchart
Source: Researcher (2018)

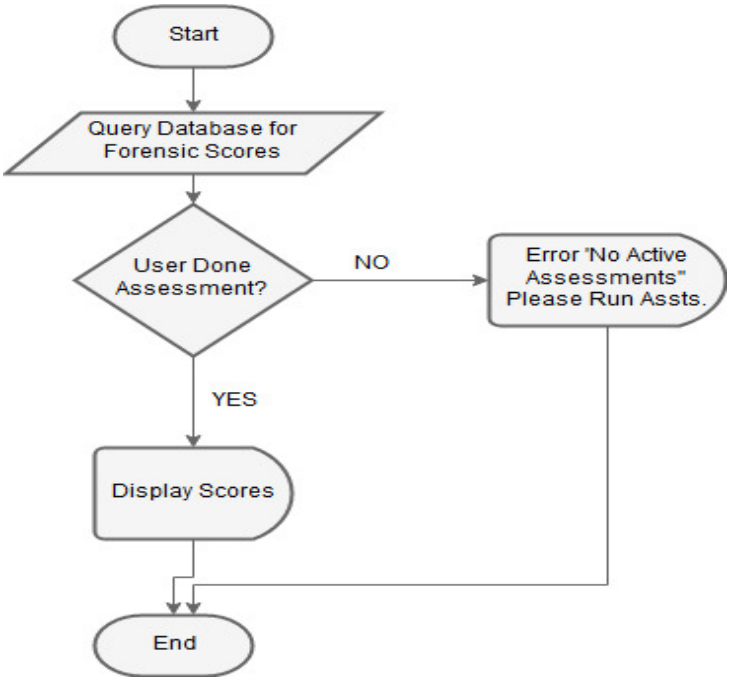


Fig. 4: Forensic Score Flowchart
Source: Researcher (2018)

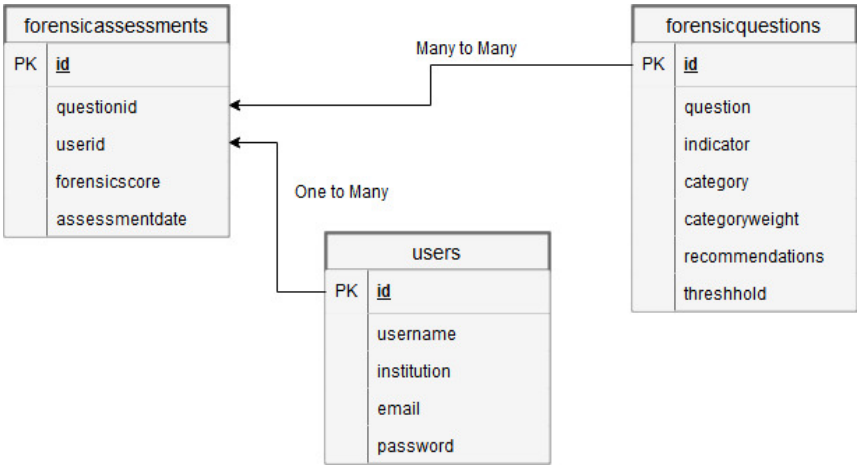


Fig. 5: Entity Relationship Diagram
Source: Researcher (2018)

5. PROOF OF CONCEPT

The digital forensics acquisition model was designed as a web-based application using the latest web tools. MySQL database was used to store records that drive the model; namely, forensic users, forensic assessment statements, recommendations and forensic assessment scores for the users. Hypertext Preprocessor (PHP) was used as a server-side language to insert and retrieve data into and from the database. JQuery and Javascript were used to animate the model and add interaction to it, particularly on the output panels. Finally, the layouts were styled using Cascaded Style Sheets version 3 (CSS3). The model was designed on Cross-Platform Apache, MySQL, PHP and Perl (XAMPP) as a local server and PHPStorm as a local code editor. The complete web-based model was deployed to a public web server where it can be accessed remotely though the following URL; ***www.matricuda.com/joyce***

5.1 User registration

User registration is performed to allow a respondent get entry to the platform and perform assessment for forensic adoptability of their digital forensics evidence collection tools. Figure 6 below presents a graphical interface of the User Registration module.

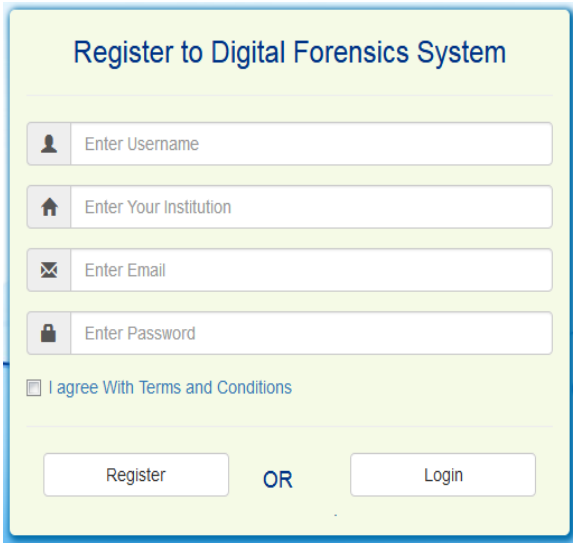


Fig. 6: User Registration Form (*Source*: Researcher (2018))

5.2 User Login

The login module of the model controls access to the system by ensuring that only registered and authorized users can proceed with other system functions. This module is also responsible for the management of user sessions whereby sessions are setup once the users successfully logs into the system and sessions are destroyed when they logout. Figure 7 below presents a graphical interface of the user login module.

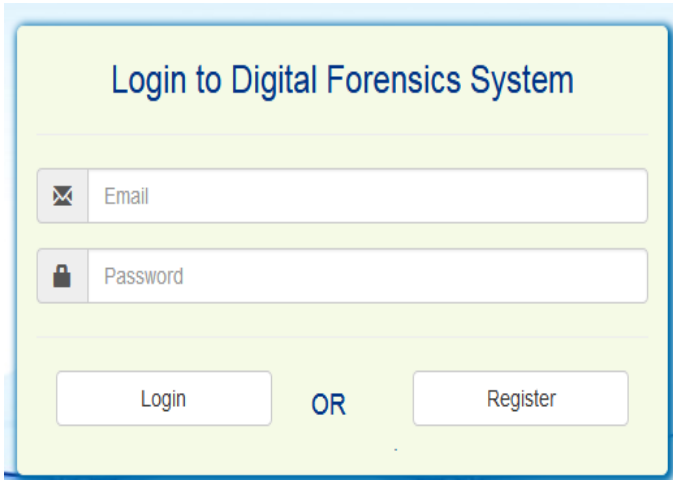


Fig. 7: Login Form
Source: Researcher (2018)

5.3 Digital Forensic Assessment module

This enables users of the platform to carry out the main purpose for which this model was developed, that is, to perform digital forensic assessments. The assessment options for the user for each forensic assessment question is presented in form of a likert scale between 1 and 5 where; 1 represents strong disagreement to corresponding statements while 5 represent strong agreement to the statements. It then submits dully-filled forms to the database. Behind the scenes, the module inserts the user responses into MYSQL database engine using PHP scripts where they are stored to be used later in computing the adoptability of digital forensics. The graphical user presentation of the digital forensics assessment module is presented in Fig. 8.

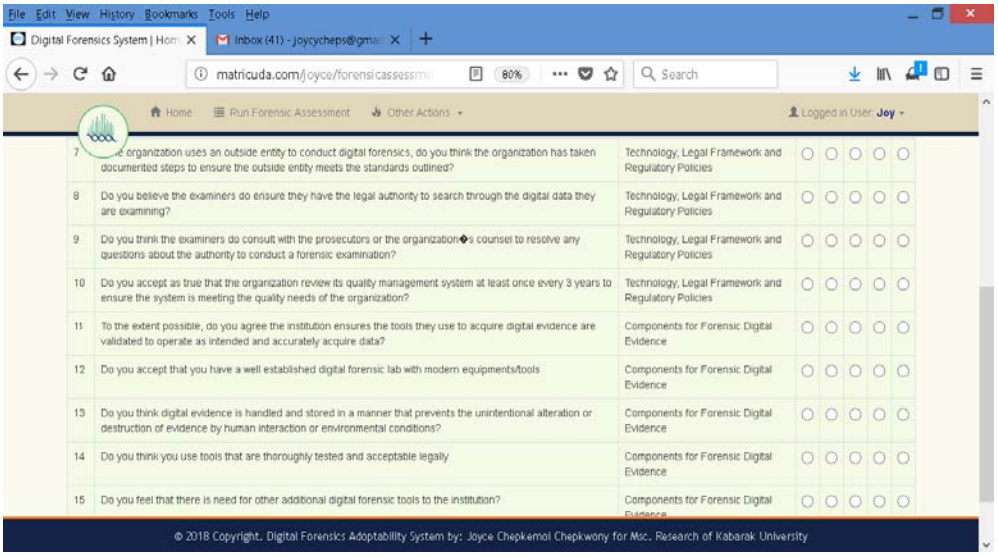
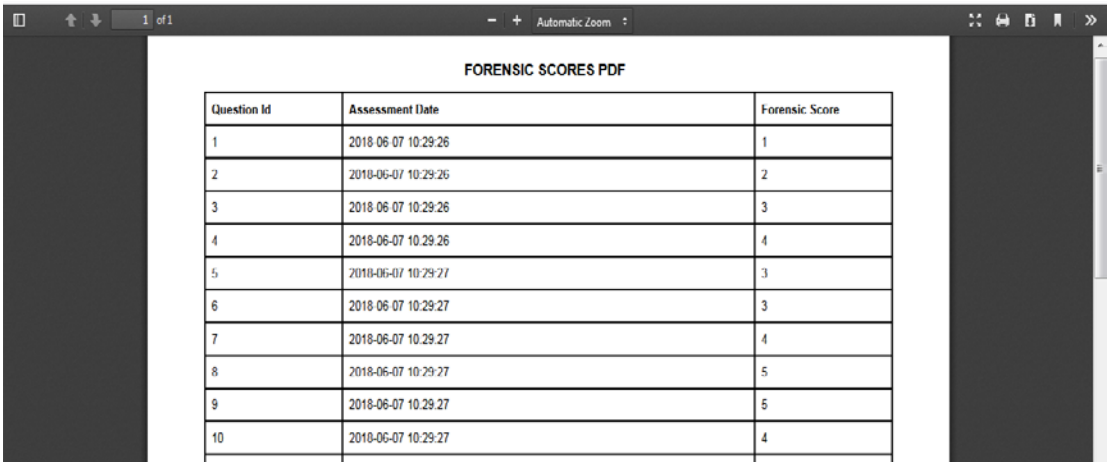


Fig. 8: Screenshot of Digital Forensic Assessment module.
Source: Researcher (2018)

5.4 Forensic Scores

This captures the forensic assessment scores that are stored in the database and output them back to the user. The module was programmed to filter the scores for the logged in user without accessing or interfering with the other users' records. The users can only see their own results of assessments which are enumerated and grouped by the dates when the forensic assessments were carried out. The user can read through the scores in HTML format, print or download the scores in portable document format (pdf). Figure 9 below presents the PDF output of the forensic scores.



FORENSIC SCORES PDF

Question Id	Assessment Date	Forensic Score
1	2018-06-07 10:29:26	1
2	2018-06-07 10:29:26	2
3	2018-06-07 10:29:26	3
4	2018-06-07 10:29:26	4
5	2018-06-07 10:29:27	3
6	2018-06-07 10:29:27	3
7	2018-06-07 10:29:27	4
8	2018-06-07 10:29:27	5
9	2018-06-07 10:29:27	5
10	2018-06-07 10:29:27	4

Fig. 9: Screenshots of Forensic Scores
Source: Researcher (2018)

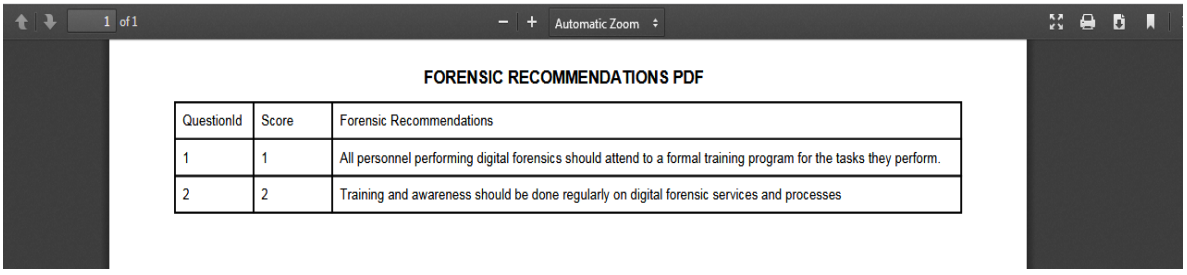
5.5 Forensic recommendation

This is a results-display module whose output is based on logged-in user's active forensic assessments. The output is initially in HTML format but the user is provided with a leeway to download or print the forensic recommendations in pdf format. Figure 10 and 11 below are screenshots of the HTML and pdf forensic recommendation respectively of the module.

Forensic Recommendations

No.	Forensic Recommendation	YourInput	Indicators
1	All personnel performing digital forensics should attend to a formal training program.	1	People
2	Training and awareness should be done regularly on digital forensic services and processes	2	People

Fig. 10: Screenshots of Forensic Recommendation HTML (*Source*: Researcher (2018))



FORENSIC RECOMMENDATIONS PDF

QuestionId	Score	Forensic Recommendations
1	1	All personnel performing digital forensics should attend to a formal training program for the tasks they perform.
2	2	Training and awareness should be done regularly on digital forensic services and processes

Fig. 11: Screenshots of Forensic Recommendation PDF (*Source*: Researcher (2018))

5.6 Digital Forensic Adoptability Index Gauge

This module displays the results of the computed adoptability of digital forensic A more interactive and readable presentation of the adoptability outcome for the user was done using the web tool namely, HTML5 to publish the Gauge, CSS3 for styling and JavaScript to animate the output. Figure 12 below shows the digital forensics adoptability output based on assessment scores for the active user.

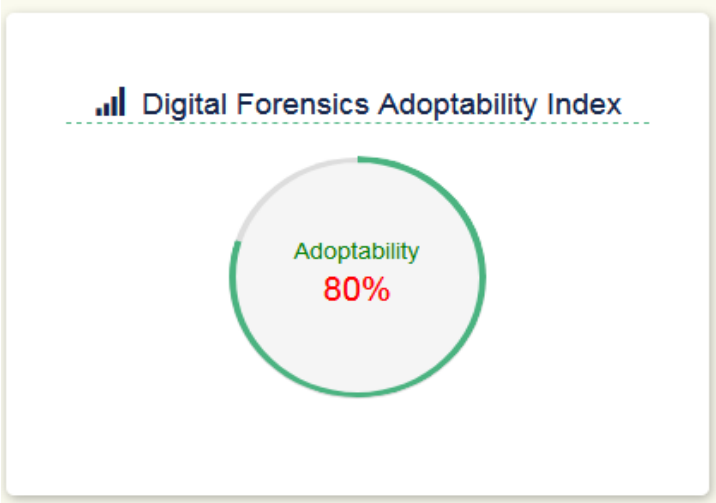


Fig. 12: Forensic Adoptability Index Gauge
Source: Researcher (2018)

6. CONCLUSION

The study aimed at investigating the adoptability of digital forensics in digital crime handling in Kenya police service that would assist to achieve high digital security level parameters and lessen the existing problems. The study developed a successful user-friendly and easy-to-use web-based model to determine the adoptability of digital forensics in the institutions of study.

6.1 Areas of Further Improvement

Although this model was designed using best web technologies to achieve a web-based application, further improvement can be done to it by giving it a new dimension. A mobile application would be ideal in this case because of the fast emerging mobile technologies and ease of use. The model is also not limited to only the Kenya Police Service but open to all forensic investigation institutions.

7. REFERENCES

Adams, Richard (2013). “The emergence of cloud storage and the need for a new digital forensic process model” (PDF). Murdoch University.

Dennis, B.H., Wixom & Tegarden, D. (2005). Systems Analysis and Design with UML Version 2.0 - An Object Oriented Approach, (2nd Edition). New Jersey: John Wiley & Sons.

Garfinkel, Simson L. (2010). Digital Forensics Research: The Next 10 years.

Hannan, T. H., & McDowell, J. M. (1984). The determinants of technology adoption: The case of the banking firm. The RAND Journal of Economics, 328-335.

Bossler, A. M., Holt, T. J., & May, D. C. (2012). Low self-control, deviant peer associations, and juvenile cyber deviance. American Journal of Criminal Justice, 37(3), 378-395.

Kenneally, E. (2002). Who's liable for insecure networks? Computer, 35(6), 93-95

Kshetri, N. (2013). Cybercrime and cyber security in the global south. Springer.

Lawrence, P. Webster (2012). The NCSC court IT Governance model.

Lin, C., Hu, P. J., and Chen, H. (2004). Technology implementation management in law enforcement: COPLINK system usability and user acceptance evaluations. Social Science Computer Review, 22(1), 24-36.

Losavio, M., Adams, J., & Rogers, M. (2006). Gap analysis: Judicial experience and perception of electronic evidence. Journal of Digital Forensic Practice, 1(1), 13-17.

McKemmish, R. (2008). When is digital evidence forensically sound? In IFIP International Conference on Digital Forensics (pp. 3-15). Springer, Boston, MA

MOTURI, C. A. (2011). Digital forensics framework for Kenyan courts of laws (Doctoral dissertation, University of NAIROBI).

Saks, M. J., & Koehler, J. J. (2005). The coming paradigm shift in forensic identification science. Science, 309(5736), 892-895.

Williams, M. L. (2015). Guardians upon high: an application of routine activities theory to online identity theft in Europe at the country and individual level. British Journal of Criminology, 56(1), 21-48.

Cite this article:

Chepkwony, J.C. (2018). Adoptability Model for Digital Forensic Evidence in Kenya. *Mara Res. J. Comput. Sci. Inf. Secur.* Vol. 3, No. 1, Pages 34 - 43, ISSN 2518-8453