Factor Analytic Approach to Digital Forensics Acceptability in Nigeria

AKINYOKUN OLUYOMI KOLAWOLE
Department of Cybersecurity, Federal University of Technology, Akure, Nigeria

Abstract- ***Contemporary method of investigations are overtime observed to be inefficient, time wasting and pruned to various errors. However, digital forensics and its investigative processes has become an integral phase of criminal jurisprudence. This research therefore carries out a baseline study of Digital Forensics, its awareness and acceptability in Nigeria. It makes use of principal component analysis (PCA) approach based responses from the questionnaires administered. Drawing upon the statistical representation of the respondents, the paper identifies key contributory indices to effective digital forensic (DF) investigative process in Nigeria which include DF Personnel Training, DF Personnel Training among others.***

I. INTRODUCTION

The explosive acceptance and use of digital devices has been a major catalyst to the metamorphism of the industrial age to the information age where data and its movement had become the drive of our day-to-day activities. Resultantly, the arrival of Internet has turned the world into a global village as geographical location has to some extent ceased to be a major obstacle to communication and movement of services and goods. This, has to a large extent, brought about the emergence, rapid growth and immense acceptance of applications that drives Information Technology. However, this development has also brought with it cybercrimes and its diverse levels of sophistication.

The modern society including developing nations need a level of connection linking citizens, commercial activities, institutions and governments for the purpose of national and economic development. However, simultaneously, this levels of connections provide a rich platform for cyber-criminal activity regardless of the state of modernization of such nation. A lot of measures and institutions are being put in place to minimize the incidence of cybercrime in different nations as efforts are being made to identify the contributing factors to cybercrime (Akinyokun, 2012).

Digital Forensics (DF) has overtime become a tool for extracting digital footprints and a viable proactive and reactive tool against cybercrime and cyber-criminal activities (Prasad and Pande, 2016). As cybercrimes become more pervasive in today's society, governments and private entities grapple with the need to implement control systems. Brown, (2022) documented that legislation, policies, guidelines and laws (cyber laws) are rapidly being developed by parliaments and boards in an effort to stop these crimes from spiraling out of control.

Digital Forensics (DF) is therefore presented as the analytical and investigative techniques used for the collection, preservation, identification, extraction, documentation, analysis, interpretation and presentation of computer media, stored or encoded for evidentiary and/or root course analysis (Palmer, 2001). Therefore, in digital crime investigation, DF queries "what was done, when it was done, where it was done, who did it and who did not do it, how it was done and why it was done".

II. RELATED WORKS

According to (Čisar and Čisar 2011; Safie and Bashah 2023), although forensic science evolved for many centuries, digital forensics is seen as a relatively new field of study and apllication. This fast-growing field has, to a great extent become an integral part of the enforcement mechanisms used in tackling cybercrimes, its various levels of sophistication and resultant litigation emanating from cyber attach incidence. The rapid evolution of digital

devices and its use has had a significant impact on the digital forensics community with digital crimes evolving just as rapidly. Court proceedings worldwide are now encountering a number of cases where despite their focus and origin, there is some form of digital evidence involved. Traditional cases including drug trafficking, murders, fraud and a myriad of others now rely heavily on some information/data residing on a digital device. Digital forensics methodologies are therefore not only required to acquire digital evidence in cases where the crime is committed using a digital device but also where digital evidence is needed for cases originally not wholly a digital crime.

Review of Nigeria Cybercrime Act: Cybercrimes (Prohibition, Prevention, etc.) Act, No. 17, 2015 and Cybercrimes (Prohibition, Prevention, etc) (AMENDMENT) Act 2024. (Izevbuwa and Rita 2022; Owoade, 2024), This is Nigeria's primary law addressing cybercrime which aims at providing a legal framework for preventing, detecting, investigating, and prosecuting cybercrimes, including the protection of critical national information infrastructure and intellectual property. The Act criminalizes various cyber-related offenses, including unauthorized access to computer systems, cyberstalking, and the misuse of electronic communications. The Act is apportioned into 59 Sections; 8 parts; and 2 Schedules. In 2024, the Nigerian President assented to the amendment of the Cybercrime Act titled Cybercrimes (Prohibition, Prevention, ETC) (AMENDMENT) Act 2024.

Digital forensics: Digital forensics is the application of computer investigation and analysis techniques in the interests of determining potential legal evidence (Pfeilsticker and Starnes, 2011) or extracting evidence from computers or other digital devices (Harrison, 2011). In developed nations, digital forensics is becoming widely accepted. Law enforcement agencies understans that modernization include the use of a variety of digital devices that can be exploited for criminal activity, unfortunately, it is observed that there is no established general standard or methodology for digital forensic investigative process both in developed and developing countries. Rather there are various DF procedures and tools developed or adapted based on the experiences of law enforcement or private DF outfits. The acceptance had become difficult and problematic because evidence must be admissible, that ismust be obtained using methods that are proven to reliably extract and analyze evidence without bias or modification (Akinyokun, 2024).

A variety of techniques and methodologies form the foundation of digital forensics investigations. Disk imaging, a fundamental technique, involves creating exact replicas of storage media for analysis without altering the original data Forensic tools and software play a crucial role in digital investigations by providing capabilities for evidence collection, preservation, and analysis. Tools such as EnCase and FTK (Forensic Toolkit) offer features for acquiring disk images, parsing file systems, and recovering deleted data (Casey, 2011). The Sleuth Kit, an open-source forensic toolkit, provides investigators with a range of command-line tools for examining file systems and analyzing digital evidence (Carrier, 2005).

III. METHODOLOGY

This research provides a detailed assessment documentation based on the baseline study of digital forensic investigative model through PCA-based analysis. The first part of the designed questionnaire in this work is based on the profile of the contact persons (respondents), this profiling is for the purpose of statistically assessing the respondents based on standard metrices of age, academic qualification and knowledge of the respondent on the subject matter among others. Assessment of effective digital forensic (df) investigative was the basis for Part 2 of the questionnaire.

IV. RESULTS

The representations of the responses from the questionnaires administered are statistically presented in Figures 1 to 3 as follows:

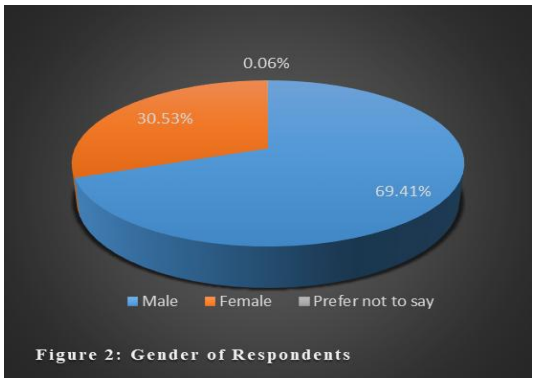

Figure 2: Gender of Respondents

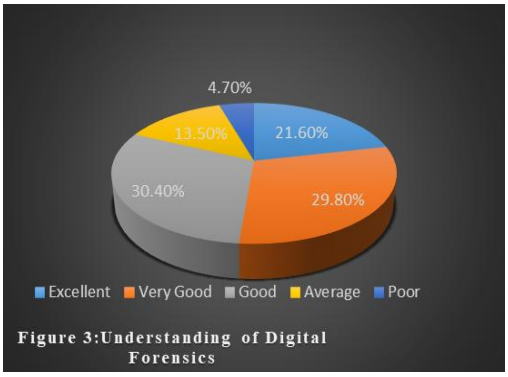

Figure 3:Understanding of Digital Forensics

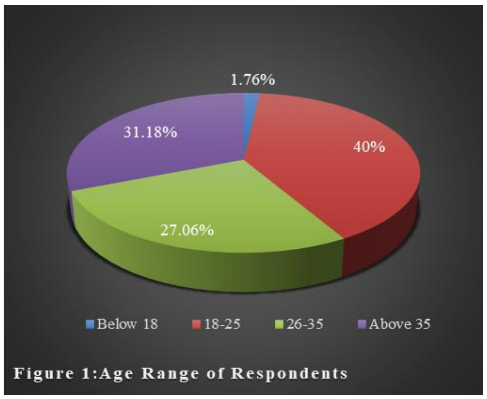

Figure 1:Age Range of Respondents

The descriptive statistics of the data collected is presented in Table 1. The table shows the mean and standard deviation of the factors considered. The correlation matrix is shown in Table 2

Table 1: Descriptive Statistics

	Mean	Std. Deviation	Analysis N
NFDF	3.55	1.280	1700
LFDF	3.50	1.250	1700
RFDF	3.62	1.223	1700
IFDF	3.67	1.149	1700
IMDF	3.58	1.291	1700
PADF	3.71	1.187	1700
PLWI	3.66	1.268	1700
ICDF	3.56	1.309	1700
FRDF	3.71	1.233	1700
DFPM	3.52	1.362	1700
DFRM	3.59	1.307	1700
PPAC	3.54	1.294	1700
ADFT	3.50	1.293	1700
TDFP	3.71	1.259	1700
DFPR	3.65	1.219	1700
ECSM	3.66	1.215	1700
TLRR	3.75	1.199	1700
TLIN	3.64	1.265	1700
TLPE	3.62	1.241	1700
DBDF	3.79	1.197	1700

Table 2: Correlation Matrix[a]

Correlation	NPDF	LFDF	RFDF	IFDF	IMDF	PADF	PLWI	ICDF	DFPM	FRDF	DFRM	PPAC	ADFT	TDFP	DFPR	ECSM	TLRR	TLIN	TLPE	DBDF
NPDF	1.000	-.018	-.030	.081	-.005	.017	-.059	.055	.076	.003	-.043	-.025	.008	-.091	.033	-.036	-.047	.058	.084	-.016
LFDF	-.018	1.000	-.151	-.025	-.006	.102	.126	.063	.065	.122	.019	.117	.152	-.022	-.036	-.068	.026	-.090	.083	-.001
RFDF	-.030	-.151	1.000	-.132	-.054	.060	.010	-.009	-.018	.121	.004	.051	.010	.012	.048	.016	-.092	.056	-.004	.101

IFDF	.081	-.025	-.132	1.000	-.048	-.098	.007	.033	-.017	-.016	-.052	-.078	-.008	-.029	-.055	.085	.069	.045	.014	.115
IMDF	-.005	-.006	-.054	-.048	1.000	-.062	.069	.062	.044	.012	.024	-.056	-.051	-.061	-.064	-.046	-.121	-.047	.072	-.017
PADF	.017	.102	.060	-.098	-.062	1.000	-.061	-.007	-.039	.189	.055	.063	.062	-.075	.034	-.039	-.143	.011	.128	-.045
PLWI	-.059	.126	.010	.007	.069	-.061	1.000	.046	.052	.040	-.007	.017	.028	.003	.063	-.067	-.138	-.044	.013	-.079
ICDF	.055	.063	-.009	.033	.062	-.007	.046	1.000	.062	-.110	.039	-.023	-.016	-.089	-.022	.030	.001	-.116	.068	-.035
DFPM	.076	.065	-.018	-.017	.044	-.039	.052	.062	1.000	.028	-.136	-.103	-.026	-.016	.036	.000	-.106	.157	.061	-.086
FRDF	.003	.122	.121	-.016	.012	.189	.040	-.110	.028	1.000	.073	.160	.076	-.048	.000	.002	-.090	-.030	.076	-.064
DFRM	-.043	.019	.004	-.052	.024	.055	-.007	.039	-.136	.073	1.000	-.184	-.005	-.010	-.069	.033	-.046	.044	.065	.031
PPAC	-.025	.117	.051	-.078	-.056	.063	.017	-.023	-.103	.160	-.184	1.000	-.013	-.146	.044	-.137	-.022	-.141	.052	-.034
ADFT	.008	.152	.010	-.008	-.051	.062	.028	-.016	-.026	.076	-.005	-.013	1.000	-.109	.022	-.062	-.007	-.030	.120	-.114
TDFP	-.091	-.022	.012	-.029	-.061	-.075	.003	-.089	-.016	-.048	-.010	-.146	-.109	1.000	-.039	.134	.244	.066	-.265	.059
DFPR	.033	-.036	.048	-.055	-.064	.034	.063	-.022	.036	.000	-.069	.044	.022	-.039	1.000	-.080	.050	.038	.011	-.108
ECSM	-.036	-.068	.016	.085	-.046	-.039	-.067	.030	.000	.002	.033	-.137	-.062	.134	-.080	1.000	-.008	.229	-.144	.117
TLRR	-.047	.026	-.092	.069	-.121	-.143	-.138	.001	-.106	-.090	-.046	-.022	-.007	.244	.050	-.008	1.000	-.128	-.156	.262
TLIN	.058	-.090	.056	.045	-.047	.011	-.044	-.116	.157	-.030	.044	-.141	-.030	.066	.038	.229	-.128	1.000	-.027	.078
TLPE	.084	.083	-.004	.014	.072	.128	.013	.068	.061	.076	.065	.052	.120	-.265	.011	-.144	-.156	-.027	1.000	-.175
DBDF	-.016	-.001	.101	.115	-.017	-.045	-.079	-.035	-.086	-.064	.031	-.034	-.114	.059	-.108	.117	.262	.078	-.175	1.000

Table 3 KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.521
Bartlett's Test of Sphericity	Approx. Chi-Square	2025.248
	Df	190
	Sig.	.000

a. Determinant = .302

Table 3 presents the Kaiser-Meyer-Olkin (KMO) and Bartlett's test. The KMO test performed in this analysis produces a measure of 0.521. The significant level (0.000) confirms the adequacy of the sample population. The results obtained from the two tests indicate the suitability of the application of factor analysis as well. Table 4 indicates the communalities of variables, which ranges from 0 to 1. The table shows that the communalities of the factors considered. The "National Policy on Digital Forensics" has a communality of 0.419. This implies that 41.9% of the variance in "National Policy on Cyber Operations" can be explained by the extracted factors while the remaining 48.1% is attributed to extraneous factors. This applies to the other factors. The factor "Industry Contribution to Digital Forensics" has the highest value of communality with over 76.1% of the variance while "National Policy on Digital Forensics" has the lowest communality with 41.9% of the variance.

Table 4. Communalities

	Initial	Extraction
NFDF	1.000	.419
LFDF	1.000	.695
RFDF	1.000	.689
IFDF	1.000	.685
IMDF	1.000	.494
PADF	1.000	.516
PLWI	1.000	.727
ICDF	1.000	.761
FRDF	1.000	.649
DFPM	1.000	.521
DFRM	1.000	.642
PPAC	1.000	.633
ADFT	1.000	.481
TDFP	1.000	.572
DFPR	1.000	.549
ECSM	1.000	.449
TLRR	1.000	.638
TLIN	1.000	.587
TLPE	1.000	.458
DBDF	1.000	.571

Extraction Method: Principal Component Analysis.

Table 5 presents the Rotated Component Matrix table. It contains all the loadings for each component extracted using the Principal Component Analysis method. The resulting principal component was rotated using Varimax with Kaiser Normalization The higher the absolute value of the loading, the more the factor contributes to the variable. The spaces on the table represent loadings that are less than 0.40, which make the table more readable. Therefore, all loadings that are less than 0.40 were suppressed.

The factor loading based on the resulting principal component rotated using Varimax with Kaiser Normalization (Table 5) are therefore presented:

Factor 1: DF Personnel Training and Incident Rapid Response

a. Regular Training of Digital Forensic Personnel (TDFP)
b. Time Lag for Presentation Of Evidence (TLPE)
c. Time Lag for Rapid Response (TLRR)

Factor 2: Investigation and Crime Scene Management

a. Time Lag For Investigation (TLIN)
b. Digital Forensic For Pro-Active (Preventive) Measures (DFPM)
c. Effective Crime Scene Management (ECSM)
d. Public/Private Agency Collabolation (PPAC)

Factor 3: Funding of DF Research

a. Funding of Research on Digital Forensic (FRDF)
b. Legislature's Framework on Digital Forensics(LFDF)
c. Public Awareness on Digital Forensics (PADF)

Factor 4: Institutional Framework

a. Institutional Framework on Digital Forensics (IFDF)
b. Documented Breakthroughs In Digital Forensic Aided Investigation (DBDF)

Factor 5: Regulatory Framework

a. Regulatory Framework on Digital Forensics (RFDF)

Factor 6: Public/Private Agency Collaboration (PPAC)

a. Digital Forensic for Re-Active (Curative) Measures (DFRM)

Factor 7: Political Will
a. Political Will (PLWI)

Factor 8: Implementation and Motivation
a. Implementation of Digital Forensics (IMDF)
b. Digital Forensic Personnel Remuneration/Motivation (DFPR)
c. Availability of Digital Forensic Tool (ADFT)

Factor 9: Industrial Contribution
a. Industry Contribution to Digital Forensics (ICDF)

Table 4.20 Rotated Component Matrix[a]

	Component								
	1	2	3	4	5	6	7	8	9
TDFP	-.718								
TLPE	.627								
TLRR	-.525								
NPDF									
TLIN		.734							
DFPM		.519				-.405			
ECSM		.511							
FRDF			.663						
LFDF			.583		-.445				
PADF			.555						
IFDF				.717					
DBDF				.588					
RFDF					.805				
DFRM						.790			
PPAC		-.439				-.488			
PLWI							.845		
IMDF								-.630	
DFPR								.579	
ADFT								.509	
ICDF									.844

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.
a. Rotation converged in 15 iterations.

CONCLUSION

Digital forensics in Nigeria is a relatively growing field and it is gradually gaining regulatory grounds. The policy makers need to put all hands on deck for the purpose of standardizing DF investigative process. This field is critical to addressing the increasing prevalence of cyber threats and the need for expertise in investigating and analyzing digital evidence for effective litigation. This research had presented nine (9) factors that contribute to DF acceptability in Nigeria, The findings from this paper could serve as a resource for further research by government and private institutions. Further, It can be used by the government and its institutions as a guide toward an effective DF regulatory framework.

REFERENCES

[1] Akinyokun O. K. (2024) Factor Analytic Approach to Digital Forensic Investigation in Developing Countries, International Journal of Computer Applications (0975 – 8887) Volume 186 – No.14, March 2024

[2] Akinyokun, O. K., Alese, B. K., Oluwadare, S. A., Iyare, O., & Iwasokun, G. B. (2015). Contributory indices to cybercrime activities in Nigeria. Proceedings of Informing Science & IT Education Conference (InSITE) 2015, 59-77. Retrievedfromhttp://Proceedings.InformingScience.org/InSITE2015/InSITE15p059077Akinyokun1556.pdf

[3] Alese B. (2019), Securing the World in Digital Age: the Metaphor of an Unending Game, 117th Inaugural Lecture, Federal University of Technology Akure Dec., 10, 2019

[4] Brown E. (2022): Digital Forensic and Distributed Evidence, Book Chapter Series on Research Nexus in IT, Law, Cyber Security &Forensics.Pp357362, www.isteams.net/ITlawbookchapter2022. dx.doi.org/10.22624/AIMS/CRP-BK3-P57

[5] Carrier, B. (2005). Digital forensics: Introduction and overview. Journal of Digital Investigation, 2(2), 123-124.

[6] Casey, E., Katz, G., & Lewthwaite, J. (2013). Honing digital forensic processes. Digital Investigation, 10(2), 138-147.

[7] Čisar P, Čisar S. (2011). "Methodological frameworks of digital forensics". 2011 IEEE 9th International Symposium on Intelligent Systems and Informatics 2011 Sep 8 (pp. 343-347). IEEE. https://doi.org/10.1109/SISY.2011.6034350

[8] Harrison W., (2011), Developing an Undergraduate Course in Digital Forensics, PSU Center for Information Assurance, Portland State University, Retrieved June 14, 2011, from: http://www.ccsc.org/northwest/2006/ppt/forensicstutorialHARRIS ON.pdf

[9] Izevbuwa O. G. and Rita A. N. (2022) Combating the Menace of Cybercrime In Nigeria: A Review of the Cybercrime (Prohibition, Prevention Etc) Act 2015 and Other Legislations Journal of Law, Policy and Globalization ISSN 2224-3240 (Paper) ISSN 2224-3259 (Online) Vol.119, 2022 www.iiste.org

[10] Owoade A., (2024), Review of the Cybercrime Amendment Act and the CBN Cybersecurity Circular, Jackson, Thought Leadership Jackson, Etti & Edu www.JEE.Africa. https://jee.africa/wp-content/uploads/2024/05/A-REVIEW-OF-THE-CYBERCRIME-AMENDMENT-ACT.pdf

[11] Palmer, G. (2001). A Road Map for Digital Forensic Research. Paper presented at the First Digital Forensic Research Workshop (DFRWS), Utica, New York.

[12] Pfeilsticker M., Starnes R., (2011): Digital Forensics, Exodus Communications. Retrieved June 14, 2011, from: http://www.guug.de/veranstaltungen/ffg2002/papers/ffg2002-pfeilsticker.pdf.

[13] Prasad A. &. Pande J, (2016), Uttrakhand Open University ISBN: 978-93-84813-94-9

[14] Safie S. and Bashah S. (2023), A Comprehensive Review of the Evolution and Future Directions of Digital Forensic Investigation Model, International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (E-ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 13, Issue 7, July 2023), DOI: 10.46338/ijetae0723_01