International Journal of Computer Applications (0975 – 8887)
Volume 186 – No.14, March 2024

Factor Analytic Approach to Digital Forensic Investigation in Developing Countries

Oluyomi Kolawole Akinyokun
Department of Cyber Security, Federal University of Technology,
Akure, Nigeria

ABSTRACT

The advancement of digital technology and the internet has immensely propelled socio-economic progress in developing countries. However, it also brought with it cybercrimes and the various levels of complexity. Further, in developing nations, precision and speed of cybercrime investigative process has become an intractable challenge in criminal jurisprudence. Therefore, the holistic traceability of digital (source, medium and target) devices used for cybercrimes requires the acceptance of digital forensics and adoption of a robust digital forensics investigative process. This research however, adopts a factor analytic approach to formulating and evaluating indices that contribute to the possible adoption of digital forensics in Nigeria. Here thirty-four indices were formulated and questionnaires were administered using purposive and simple random sampling techniques. The data obtained were analyzed by means of factor analysis by principal component using Statistical Package for Social Sciences (SPSS). The output was subjected to orthogonal rotation using varimax and four factors were resultantly extracted. The output of this research could serve as resource for further cyber security analysis.

General Terms

Digital Forensics, Factor Analysis

Keywords

Digital Forensics, Factor Analysis, Cyber Security, Contributory Indices.

1. INTRODUCTION

Securing the cyber space has become very indispensable with the spread of information technology and digital application. The wave of cyber-attacks, which now cuts across all spheres of human-computer interaction has resulted in significant financial and public relations losses for businesses and governments. Personal computers and other digital assets are being used more frequently in both homes and businesses, which has led to a spike in high-tech crimes. To curb the above, Nigerian government came up with an act on the 15th of May, 2015: The Cybercrime (Prevention & Prohibition) Act, 2015. This was enacted for the purpose of prohibiting, preventing, detecting, responding, investigating and prosecution of cybercrimes and for other related matters, 2015. The act sees any form of vandalisation or crime against critical national information infrastructure, unlawful access to computer systems, cyber grooming, and the likes as crimes which are punishable.

The increase in cyberattack and their related effects all together provide the basis for adopting systematic incident response procedures. Responding to high-tech crimes and carrying out efficient incident response operations require a methodical approach built on a reliable forensic exercise. As this approach is well adopted in developing nations, there is the need to fully incorporate it into the legal jurisprudence of developing nations such as Nigeria.

Cybersecurity is concerned with the defense of digital assets and the preservation of data. Likewise the design, development, implementation, and management of several policies, frameworks, and strategies that direct the protection of data against unauthorized access and illegal modifications are included.

Digital forensics is a relatively new field. Derived as a synonym for computer forensics, its definition has expanded to include the forensics of all digital technology. Whereas computer forensics is defined as "the collection of technique and tools used to find evidence in a computer" [4]. Digital forensics has been defined as "the use of scientifically derived and proven methods towards the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for the purpose of facilitation or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations" [5]. Digital forensics, "is the discipline that combines elements of law and computer science to collect and analyze data from computer systems, networks, wireless communications, and storage devices in a way that is admissible as evidence in a court of law". The word forensics denotes use in law/courts thus signifying digital forensics as a process carried out ultimately to acquire evidence that may be used in a court of law. The goal of digital forensics, as simply stated, "is to identify digital evidence for an investigation". The fact that digital forensics has a legal connotation cannot be overemphasized [10].

[10] stated that digital forensics has become prevalent because law enforcement recognizes that modern day life includes a variety of digital devices that can be exploited for criminal activity, not just computer systems. While computer forensics tends to focus on specific methods for extracting evidence from a particular platform, digital forensics must be modeled such that it can encompass all types of digital devices, including future digital technologies. Unfortunately, here in Nigeria, there does not exist a standard or consistent digital forensics methodology, but rather a set of procedures and tools built from the experience of law enforcement, system administrators, and hackers.

2. RELATED WORKS

The authors in [9] explore the development of digital forensics process, compare and contrasts four particular forensic methodologies and finally proposes an abstract model of the digital forensic procedure. The research was simulated with some steps as "pre-incident preparation, detection of incidents, initial response strategy formulation, duplication, investigation, security measure implementation, network monitoring, recovery, reporting and follow-up using platform such as Windows NT/2000, UNIX and Cisco Routers. The scheme created consistent and standardized framework for digital forensic development and also identifies the need for specific technology-dependent tools while providing insight from previously defined tools of same category. In [10] solution was produced to issues surrounding digital evidence acquisition and subsequent presentation in court and outlines guidelines for making this type of evidence more robust when presented in court. This research addressed intricate issues of the digital forensics process and lays the foundations of a frameworks that will accurately and rigorously address the multidimensional nature of the field. A process model for digital investigation is defined using the theories and techniques from the physical investigation world. While digital investigation. This model allows technical requirement for each phase to be developed and for the interaction between physical and digital investigation to be identified. It is abstract enough that it can be applied to both law enforcement and corporate scenarios [3].

3. RESEARCH METHODOLOGY

The contributing indices for digital forensics was derived and questionnaires were distributed to selected respondents who are knowledgeable about subject topic and are aware of the need for standardization in the area. There was a guarantee of the privacy of the personal data supplied by respondents. Age, gender, the highest academic degree had, and occupation are just a few of the biographical details that respondents submitted. To help the respondents comprehend the questions and give accurate replies, some questions in the questionnaire that contained technical words were explained.

The computer model of factor analysis by the principal components of the contributory indices to Digital Forensic Investigation Process was formulated and statistical package for social sciences (SPSS) was used in the analysis of the factors that contribute to digital forensic.

Factor analysis is a statistical method used to describe variability among observed, correlated variables in terms of a potentially lower number of unobserved variables called factors. It is used mostly for data reduction purposes to get a small set of variables from a large set of variables and also to create indices with variables that measure similar things. It is also used for summarization and also for testing the validity of a test or scale. The inter-correlation between variables was determined while conducting factor analysis by using the correlate procedure to create a correlation matrix of all variables.

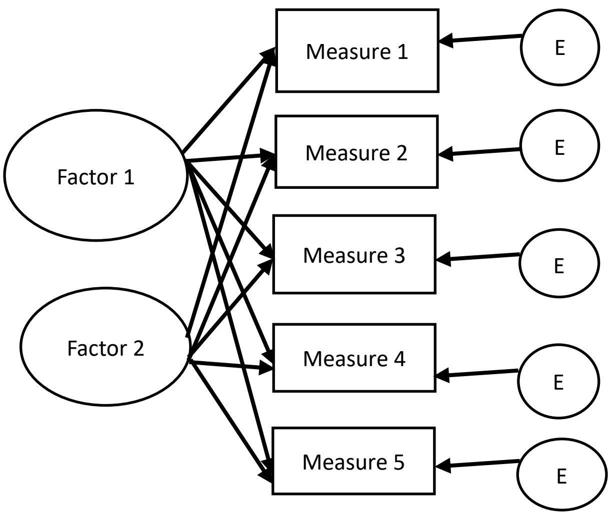

Figure. 1: Simple path for factor analytic model (The Common Factor Model)

Figure 1 shows a simple path diagram for factor analysis model. Each observed response (Measure 1 through Measure 5) is influenced partially by the fundamental common factors (Factor 1 and Factor 2) and partially by the underlying factors (E1 through E5). Factor analysis by principal components of the data obtained through survey has been implemented in [2]. The mathematical model of the evaluation of contributory indices of digital forensics using the factor analysis by principal components is expressed as shown in the equation 1:

$$Y_j = \sum_{k=1}^{m} a_{j,k} X_k \qquad k = 1,2,3,\ldots\ldots,m \tag{1}$$

Where:
Y_j is the j[th] respondent, $a_{j,k}$ is the assessment of the k[th] variable by j[th] respondent, and X_k is the k[th] decision.

The Descriptive statistics define the mean, standard deviation and number of respondents (N) who participated in the survey. The correlation gives the correlation coefficients between a single variable and every other variables in the analysis. The correlation matrix contains 1. The correlation coefficients above and below the principal diagonal are the same.

Total Variance Explained shows all the factors extractable from the analysis along with their eigenvalues, the percent of variance attributable to each factor and the cumulative variance of the factor. The first principal component (scaled eigenvector) by definition is the one that explains the largest part of the total variance.

The scree plot is a graph of the eigenvalues against all the factors. It is useful for determining how many factors to retain. For each principal component, the corresponding eigenvalue is plotted on the y-axis. The display of an elbow at a given value on the x-axis indicates a higher order principal component that shows a decreasing amount of additional variance.

The Component Matrix shows the loadings of all the variables on the factors extracted. The Rotated Component Matrix is aimed at reducing the number of factors on which the variables under investigation have higher loadings. It does not change anything, buy makes the interpretation of the analysis easier.

3.2 Data Survey and Collection

To examine relationships and outline data stored from the questionnaire, a well-structured questionnaire is created. With the aid of a well-structured questionnaire to evaluate correlations acquired from the questionnaire, the data that would be used in creating the computer model based on the developed contributing indices would be obtained.

Upon accumulating the primary data required for the research project, the outcomes were compiled. As the research employed questionnaires with adequate and reliable information, this study has a descriptive research design. It was designed with the intention of gathering accurate and sufficient data while sampling the views of different respondents in academic environment. In order to get responses from the respondents, a structured questionnaire was used. The respondents were given the survey, which was then collected.

This survey was carried out in a number of locations. In view of the large number of local governments, states, institutions of higher learning, law firms & security outfits, certain classes of respondents were identified during this survey and used in this sampling instruments for the purpose of the research. The classes of respondents are: Staff of institutions of higher learning, students of institutions of higher learning, staffs and clients of IT firms, legal practitioners and administrative staff at law court, and security personnel.

4. RESULTS AND INTERPRETATION

The respondents filled the questionnaire in accordance to their understanding with each particular index. A six-point scale of 'very high', 'high', 'average', 'low', 'very low' and 'undecided'. Two Hundred questionnaires were distributed, and same two hundred (200) were returned completely filled. The analysis of gender and age incidence of perpetrators are presented in table 1, 2, 3, 4, 5, 6 and 7 respectively.

Table 1: Male Perpetrators

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Very High	142	71.0	71.0	71.0
	High	23	11.5	11.5	82.5
	Average	16	8.0	8.0	90.5
	Low	5	2.5	2.5	93.0
	Very Low	1	.5	.5	93.5
	Undecided	13	6.5	6.5	100.0
	Total	200	100.0	100.0	

Table 2: Female Perpetrators

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Very High	12	6.0	6.0	6.0
	High	32	16.0	16.0	22.0
	Average	65	32.5	32.5	54.5
	Low	51	25.5	25.5	80.0
	Very Low	15	7.5	7.5	87.5
	Undecided	25	12.5	12.5	100.0
	Total	200	100.0	100.0	

Table 3: Range_2_to_11

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	High	6	3.0	3.0	3.0
	Average	2	1.0	1.0	4.0
	Low	26	13.0	13.0	17.0
	Very Low	78	39.0	39.0	56.0
	Undecided	88	44.0	44.0	100.0
	Total	200	100.0	100.0	

Table 4: Range_12_to_17

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Very High	9	4.5	4.5	4.5
	High	18	9.0	9.0	13.5
	Average	52	26.0	26.0	39.5
	Low	64	32.0	32.0	71.5
	Very Low	35	17.5	17.5	89.0
	Undecided	22	11.0	11.0	100.0
	Total	200	100.0	100.0	

Table 5: Range_18_to_25

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Very High	115	57.5	57.5	57.5
	High	39	19.5	19.5	77.0
	Average	28	14.0	14.0	91.0
	Low	2	1.0	1.0	92.0
	Very Low	1	.5	.5	92.5
	Undecided	15	7.5	7.5	100.0
	Total	200	100.0	100.0	

Table 6: Range_26_to_45

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Very High	97	48.5	48.5	48.5
	High	53	26.5	26.5	75.0
	Average	26	13.0	13.0	88.0
	Low	3	1.5	1.5	89.5
	Very Low	1	.5	.5	90.0
	Undecided	20	10.0	10.0	100.0
	Total	200	100.0	100.0	

Table 7: Range_Above_45

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Very High	14	7.0	7.0	7.0
	High	32	16.0	16.0	23.0
	Average	49	24.5	24.5	47.5
	Low	36	18.0	18.0	65.5
	Very Low	27	13.5	13.5	79.0
	Undecided	42	21.0	21.0	100.0
	Total	200	100.0	100.0	

Table 8: Descriptive Statistics

	N	Mean	Std. Deviation
DEIP	200	2.39	1.366
DECV	200	2.62	1.340
SDDSM	200	2.29	1.405
RAPSM	200	2.12	1.368
ADCDD	200	2.52	1.396
INTH	200	2.33	1.284
EIAM	200	2.31	1.277
INBIN	200	2.45	1.318
ONFR	200	2.20	1.410
INES	200	2.35	1.403
HACK	200	2.07	1.364
SOENG	200	2.24	1.520
TERCT	200	2.53	1.318

CONLI	200	2.82	1.219
COMLI	200	2.66	1.412
NAPDF	200	2.51	1.330
LFDF	200	2.78	1.216
RFDF	200	2.77	1.242
IFDF	200	2.74	1.273
IMDF	200	2.77	1.298
PADF	200	2.97	1.277
POLWI	200	2.85	1.243
ICDF	200	3.03	1.171
FRDR	200	2.92	1.305
DFPAPM	200	2.85	1.283
DFRACM	200	2.93	1.278
PPAC	200	3.10	1.210
ADFT	200	3.00	1.339
RTDFP	200	3.12	1.312
ECSM	200	3.03	1.272
TLRR	200	3.18	2.466
TLIN	200	2.94	1.302
TLPE	200	2.84	1.271
DBDFAI	200	2.75	1.318

The descriptive statistics of the data collected is presented in Table 8. The table shows the mean and standard deviation of the assessment of each of the contributory indices to digital forensics by the respondents. It is inferred from the mean that *Hacking* is the prevalent index that could likely contribute to or require digital Forensics. It has the highest mean of 2.07

The SPSS generates the correlation matrix as a single file shown in Appendix 2. The correlation between a variable and itself is always 1, hence the principal diagonal of the correlation matrix contains 1. The correlation coefficients above and below the principal diagonal are the same. The determinant of the correlation matrix is given as 7.209E-16. The KMO test performed in this analysis produces a measure of 0.940. Bartlett's test produces an X^2 of 6514.144 with a significant level of 0.000. The significant level confirms the adequacy of the sample population. The result obtained from the two tests (Bartlett's test of Sphericity and KMO test) indicate the suitability of the application of factor analysis as well. Table 9 indicates the communalities of variables, which ranges from 0 to 1. The table shows that the communalities of 'Delayed in Investigation Process 'and 'Delayed in Court Verdict' are 0.739 and 0.723 respectively. This implies that 73.90% of the variance in 'Delayed in Investigation Process' can be explained by the extracted factors while the remaining 26.10% is attributed to extraneous factors. Similarly, 72.30% of the variance in 'Delayed in Court Verdict' can be explained by the extracted factors, while the remaining 27.70% is attributed to extraneous factors. The factor 'Time Lag in Investigation' has the highest value of communality with over 80% of the variance while 'Time Lag for Rapid Response' has the smallest value of communality with 47.5% of the variance. In addition, the factors with small values such as 'Time Lag for Rapid Response' (0.475), Social Engineering (0.575), Documented breakthroughs in Digital Forensic aided Investigation (0.579), Online Fraud (0.632); should be dropped from the analysis. Table 10 consists of the Component (Factor) Matrix table which interprets the components. It shows the loadings of the contributory factors on the four (4) components extracted using Principal Component Analysis. The higher the absolute value of the loadings, the more the factor contributes to the variable. The gap on the table represents loadings that are less than 0.3 were suppressed. In Factor 1 all the variables were loaded, factor 2, only 13 variables were not loaded, factor 3, only 5 variables were loaded and in factor 4, only 3 variables were loaded.

Table 9: Communalities of Variables

	Initial	Extraction			Initial	Extraction
DEIP	1.000	.739		ADFT	1.000	.698
DECV	1.000	.723		RTDFP	1.000	.754
SDDSM	1.000	.663		ECSM	1.000	.692
RAPSM	1.000	.689		TLRR	1.000	.475
ADCDD	1.000	.703		TLIN	1.000	.801
INTH	1.000	.673		TLPE	1.000	.719
EIAM	1.000	.772		DBDFAI	1.000	.579
INBIN	1.000	.723		PPAC	1.000	.751
ONFR	1.000	.632				
INES	1.000	.645				
HACK	1.000	.719				
SOENG	1.000	.575				
TERCT	1.000	.658				
CONLI	1.000	.658				
COMLI	1.000	.619				
NAPDF	1.000	.679				
LFDF	1.000	.742				
RFDF	1.000	.712				
IFDF	1.000	.718				
IMDF	1.000	.772				
PADF	1.000	.783				
POLWI	1.000	.659				
ICDF	1.000	.693				
FRDR	1.000	.718				
DFPAPM	1.000	.782				
DFRACM	1.000	.737				

Table 10: Component Factor Matrix

	1	2	3	4
DEIP	.682			-.415
DECV	.691			-.390
SDDSM	.684	.366		
RAPSM	.683	.446		
ADCDD	.705	.414		
INTH	.719	.388		
EIAM	.747	.428		
INBIN	.680	.490		
ONFR	.684	.396		
INES	.658	.452		
HACK	.785	.321		
SOENG	.688			
TERCT	.701	.395		
CONLI	.662	.400		
COMLI	.578			.437
NAPDF	.775			
LFDF	.793			
RFDF	.806			
IFDF	.803			
IMDF	.747	-.331	-.301	
PADF	.729	-.321	-.323	
POLWI	.739			
ICDF	.763	-.316		
FRDR	.754	-.380		
DFPAPM	.782	-.389		
DFRACM	.759	-.371		
PPAC	.760	-.413		
ADFT	.740	-.378		
RTDFP	.695	-.448		
ECSM	.721	-.360		
TLRR	.378		.540	
TLIN	.693		.523	
TLPE	.746		.338	
DBDFAI	.714			

The Rotated Component (Factor) Matrix is the next analysis that was performed. The method of Extraction is the Principal Component Analysis. In order to obtain meaningful representation of variables, the resulted principal component is rotated by orthogonal transformation by varimax, quartimax, equamax, and promax. However, the method chosen for the analysis is Rotated Component (Factor) Matrix using Varimax.

Table 11: Rotated Component Matrix using Varimax

	1	2	3	4
DEIP		.599		.536
DECV		.614		.507
SDDSM		.682		.355
RAPSM		.771		
ADCDD		.763		
INTH		.761		
EIAM		.828		
INBIN		.824		
ONFR		.747		
INES		.767		
HACK	.345	.747		
SOENG	.311	.595		.320
TERCT		.764		
CONLI		.757		
COMLI		.624	.304	-.314
NAPDF	.701	.388		
LFDF	.667	.432		
RFDF	.681	.481		
IFDF	.755	.348		
IMDF	.828			
PADF	.813			
POLWI	.735	.337		
ICDF	.729		.302	
FRDR	.783			
DFPAPM	.837			
DFRACM	.815			
PPAC	.798			
ADFT	.753			
RTDFP	.688		.470	
ECSM	.678		.440	
TLRR			.655	
TLIN	.444		.726	
TLPE	.523	.302	.537	
DBDFAI	.503	.366		.333

The interpretation of table 11 is as follow

Factor 1- National Policy/Legislature Framework on Digital Forensics Investigation and Public-Private-People Partnership, loads on

1. National Policy on Digital Forensics
2. Legislature’s Framework on Digital Forensics
3. Regulatory Framework on Digital Forensics
4. Institutional Framework on Digital Forensics
5. Implementation of Digital Forensics
6. Political will
7. Industry Contribution to Digital Forensics
8. Funding of Research on Digital Forensics
9. Digital Forensic Pro-Active (Preventive) Measures
10. Digital Forensic Re-Active (Curative) Measures
11. Public/Private Agency Collaboration
12. Public awareness of digital forensics
13. Availability of digital forensics tools
14. Documented breakthroughs in digital forensic aided investigation

Factor 2- Motive for Digital Forensics Investigation loads on

1. Delayed Investigation Process
2. Delayed Court Verdict
3. Rapid Growth of social media
4. Accidental or Deliberate Company Data Disclosure
5. Intellectual Theft
6. Employee Internet Abuse or Misuse
7. Incident or Breach Investigation
8. Hacking
9. Online Fraud
10. Industrial Espionage
11. Terrorism (Cyber Terrorism)
12. Conventional Literacy
13. Computer Literacy

Factor 3- Security Agencies loads on

1. Regular training of digital forensics personnel
2. Effective crime scene management
3. Time lag for rapid response
4. Time lag for presentation of evidence
5. Time lag for investigation

Factor 4- Motive for Digital Forensics Investigation loads on

1. Stolen Digital Devices such as Smartphones
2. Social Engineering

Appendix 1 ‘Total Variance Explained’ which shows how much of the total variance of the observed variables is explained by each of the principal components is presented in appendix 1. The extraction method is Principal Component Analysis. The first principal component (scaled eigenvalue) by definition explains the largest part of the total variance. It has a variance (eigenvalue) of 17.5; this accounts for 51.417% of the total variance. The second principal component has a variance of 3.8 and accounts for a further11.308% of the variance and so on. The “Cumulative %” column of the table tells us how much of the total variance can be accounted for by the first *K* components together. 69.58% of the extracted (4) factors contribute to the Digital Forensics based on the views of the respondents. The remaining 30.42% is considered to be the contribution of extraneous factors.

Figure 2 (below) shows the Scree Plot used in analysis. The display of an elbow at a given value on the x-axis indicates a higher order principal component that shows a decreasing amount of additional variance. There is a marked decrease in downward slope after the sixth principal component, although its eigenvalue is greater than 1.

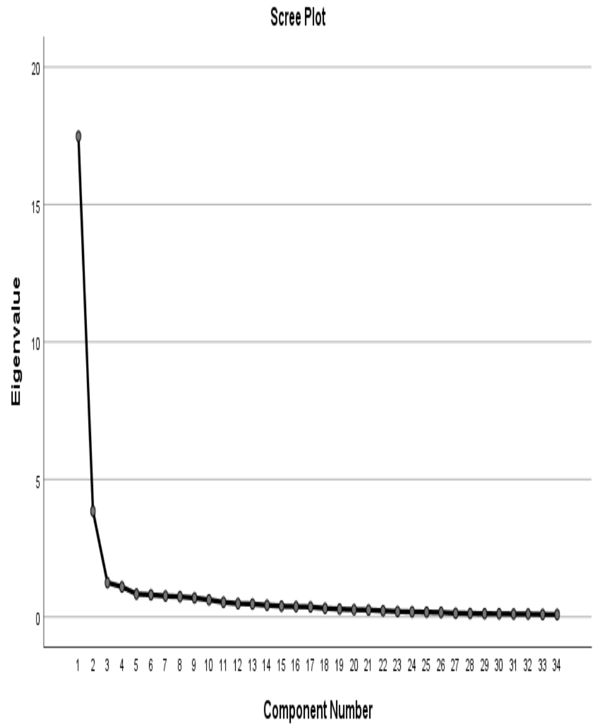

Fig. 2: Scree Plot

6. CONCLUSION

On the basis of the description analysis based on the gender incidence of perpetrators from the respondents, most perpetrators are much likely to be of the male gender based on the mean (1.70), while perpetrators with age range 18-25 and 26-45, are much likely to be involved. The elements influencing digital forensics in Nigeria were identified using a factor analytic technique, which was reported in this research. The covariances and correlations between the factors are also noted. Four contributory variables were also extracted. The outcome of this research is solely due to the contributing variables that were developed and utilized in the assessment of the indicators for the use of Digital Forensics Investigation Process in Nigeria. This research focuses on the representation of digital forensics in Nigeria. It could serve as resource for further research in digital forensics (DF) process.

5. REFERENCES

[1] Abel Yeboah-Ofori (2020). Digital Forensics Investigation Jurisprudence: Issue of Admissibility of Digital Evidence.

[2] Akinyokun O., Alese B., Oluwadare S., Iyare O., & Iwasokun G.. (2015). Contributory Indices to Cybercrime Activities in Nigeria, Proceedings of Informing Science & IT Education Conference (InSITE) 2015, http://Proceedings.InformingScience.org/InSITE2015/InSITE15p059-077Akinyokun1556.pdf

[3] Brian D. Carrier, Eugene Spafford (2003). Getting Physical with The Digital Investigation Process.

[4] Caloyannides, Michael A. (2001). Computer Forensics and Privacy. Artech House, Inc.

[5] Digital Forensics Research Workshop (2001). “A Road Map for Digital Forensics Research” www.dfrws.org

[6] Horan, C.; Saiedian, H. Cyber Crime Investigation: (2021) Landscape, Challenges, and Future Research Directions.

[7] Longe, O. B., & Chiemeke, S.C. (2008). Cybercrime and criminality in Nigeria - What roles are internet access points playing? European Journal of Social Sciences,6(4).

[8] Manral, B.; Somani, G.; Choo, K.-K.R.; Conti, M.; Gaur, M.S. (2020). A Systematic Survey on Cloud Forensics Challenges, Solutions, and Future Directions.

[9] Mark Reith, Clint Carr, Gregg Gunsch (2002). An Examination of Digital Forensic Model

[10] Moniphia Hewling, Paul Sant (2012). Digital Forensics: An Integrated Approach

[11] Nazah, S.; Huda, S.; Abawajy, J.; Hassan, M.M. (2020). Evolution of dark web threat analysis and detection: A systematic approach.

[12] Seemma P.S., Nandhini S., Sowmiya M. (2018). Overview of Cyber Security: International Journal of Advanced Research in Computer and Communication Engineering.

APPENDIX A: TOTAL VARIANCE EXPLAINED

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	17.482	51.417	51.417	17.482	51.417	51.417	10.18	29.949	29.949
2	3.845	11.308	62.725	3.845	11.308	62.725	3	27.831	57.780
3	1.243	3.656	66.382	1.243	3.656	66.382	9.463	7.562	65.342
4	1.089	3.204	69.586	1.089	3.204	69.586	2.571	4.244	69.586
5	.829	2.439	72.025				1.443		
6	.801	2.356	74.382						
7	.756	2.225	76.606						
8	.734	2.158	78.765						
9	.689	2.028	80.792						
10	.619	1.822	82.614						
11	.531	1.563	84.176						
12	.483	1.421	85.597						
13	.463	1.362	86.959						
14	.424	1.247	88.206						
15	.390	1.146	89.353						
16	.372	1.094	90.447						
17	.360	1.059	91.506						
18	.309	.910	92.416						
19	.285	.838	93.254						
20	.261	.768	94.021						
21	.249	.732	94.753						
22	.222	.654	95.407						
23	.193	.568	95.974						
24	.182	.535	96.509						
25	.173	.509	97.018						
26	.160	.471	97.489						
27	.131	.385	97.874						
28	.123	.362	98.236						
29	.114	.336	98.572						
30	.111	.326	98.898						
31	.103	.303	99.201						
32	.101	.296	99.497						
33	.087	.257	99.754						
34	.083	.246	100.000						

APPENDIX B: CORRELATION MATRIX OF VARIABLES

Correlation Matrix

	DEIP	DECV	SDDSM	RAPSM	ADCDD	INTH	EIAM	INBIN	ONFR	INES
DEIP	1	.786	.618	.581	.603	.557**	.595**	.506**	.478**	.522**
DECV	.786**	1	.632**	.592**	.630**	.538**	.576**	.539**	.572**	.550**
SDDSM	.618**	.632	1	.574**	.611**	.599**	.545**	.579**	.566**	.607**
RAPSM	.581**	.592**	.574**	1	.645**	.648**	.667**	.685**	.710**	.623**
ADCDD	.603**	.630**	.611**	.645**	1	.708**	.672**	.722**	.673**	.587**
INTH	.557**	.538**	.599**	.648**	.708**	1	.695**	.681**	.669**	.641**
EIAM	.595**	.576**	.545**	.667**	.672**	.695**	1	.719**	.648**	.695**
INBIN	.506**	.539**	.579**	.685**	.722**	.681**	.719**	1	.626**	.654**
ONFR	.478**	.572**	.566**	.710**	.673**	.669**	.648**	.626**	1	.522**
INES	.522**	.550**	.607**	.623**	.587**	.641**	.695**	.654**	.522**	1
HACK	.626**	.591**	.643**	.672**	.671**	.668**	.739**	.677**	.704**	.587**
SOENG	.556**	.575**	.592**	.487**	.477**	.549**	.582**	.501**	.583**	.590**
TERCT	.518**	.492**	.624**	.538**	.621**	.636**	.696**	.673**	.586**	.639**
CONLI	.492**	.506**	.585**	.591**	.587**	.520**	.681**	.658**	.541**	.607**
COMLI	.391**	.412**	.386**	.525**	.363**	.483**	.598**	.461**	.488**	.476**
NAPDF	.432**	.426**	.429**	.465**	.461**	.497**	.505**	.423**	.426**	.396**
LFDF	.408**	.439**	.437**	.508**	.497**	.475**	.529**	.504**	.500**	.408**
RFDF	.463**	.495**	.547**	.429**	.523**	.541**	.557**	.492**	.490**	.521**
IFDF	.491**	.484**	.505**	.372**	.447**	.502**	.488**	.403**	.401**	.454**
IMDF	.421**	.452**	.342**	.335**	.418**	.447**	.406**	.308**	.456**	.348**
PADF	.437**	.441**	.356**	.345**	.450**	.408**	.389**	.308**	.372**	.411**
POLWI	.386**	.391**	.344**	.353**	.474**	.428**	.548**	.419**	.418**	.405**
ICDF	.396**	.413**	.463**	.412**	.379**	.416**	.449**	.380**	.356**	.346**
FRDR	.373**	.353**	.418**	.346**	.390**	.412**	.410**	.369**	.345**	.284**
DFPAPM	.437**	.432**	.395**	.345**	.386**	.411**	.433**	.370**	.405**	.339**
DFRACM	.410**	.372**	.347**	.384**	.406**	.400**	.429**	.335**	.384**	.350**
PPAC	.388**	.404**	.365**	.321**	.387**	.410**	.368**	.351**	.408**	.312**
ADFT	.391**	.492**	.329**	.357**	.404**	.354**	.395**	.326**	.437**	.343**
RTDFP	.354**	.420**	.375**	.292**	.285**	.320**	.330**	.234**	.325**	.265**
ECSM	.343**	.361**	.316**	.339**	.345**	.425**	.409**	.310**	.342**	.327**
TLRR	.249**	.248**	.182**	.231**	.154*	.188**	.204**	.175*	.199**	.142*
TLIN	.431**	.405**	.389**	.492**	.346**	.400**	.365**	.429**	.343**	.325**
TLPE	.526**	.441**	.516**	.433**	.411**	.443**	.452**	.426**	.346**	.357**
DBDFAI	.500**	.433**	.497**	.454**	.451**	.474**	.470**	.389**	.392**	.466**

Correlations Matrix								
	HACK	SOENG	TERCT	CONLI	COMLI	NAPDF	LFDF	RFDF
DEIP	.626	.556	.518	.492	.391	.432	.408	.463
DECV	.591	.575	.492	.506	.412	.426	.439	.495
SDDSM	.643	.592	.624	.585	.386	.429	.437	.547
RAPSM	.672	.487	.538	.591	.525	.465	.508	.429
ADCDD	.671	.477	.621	.587	.363	.461	.497	.523
INTH	.668	.549	.636	.520	.483	.497	.475	.541
EIAM	.739	.582	.696	.681	.598	.505	.529	.557
INBIN	.677	.501	.673	.658	.461	.423	.504	.492
ONFR	.704	.583	.586	.541	.488	.426	.500	.490
INES	.587	.590	.639	.607	.476	.396	.408	.521
HACK	1	.603	.646	.582	.505	.580	.575	.584
SOENG	.603	1	.645	.446	.452	.477	.449	.502
TERCT	.646	.645	1	.628	.523	.467	.467	.530
CONLI	.582	.446	.628	1	.598	.423	.505	.514
COMLI	.505	.452	.523	.598	1	.375	.457	.417
NAPDF	.580	.477	.467	.423	.375	1	.791	.773
LFDF	.575	.449	.467	.505	.457	.791	1	.782
RFDF	.584	.502	.530	.514	.417	.773	.782	1
IFDF	.513	.476	.531	.452	.392	.652	.687	.764
IMDF	.460	.465	.388	.333	.316	.648	.598	.638
PADF	.457	.434	.396	.367	.219	.564	.538	.556
POLWI	.495	.362	.413	.476	.435	.530	.520	.632
ICDF	.499	.414	.398	.408	.418	.605	.695	.609
FRDR	.531	.420	.401	.313	.329	.684	.651	.628
DFPAPM	.480	.402	.418	.365	.321	.711	.658	.660
DFRACM	.484	.438	.386	.350	.351	.692	.653	.563
PPAC	.453	.425	.362	.315	.343	.588	.612	.620
ADFT	.449	.430	.326	.310	.323	.549	.616	.610
RTDFP	.383	.463	.296	.239	.252	.525	.586	.540
ECSM	.442	.412	.404	.357	.336	.627	.635	.615
TLRR	.237	.210	.148	.187	.224	.329	.325	.288
TLIN	.444	.416	.390	.386	.423	.497	.588	.480
TLPE	.542	.408	.475	.471	.355	.520	.523	.505
DBDFAI	.568	.541	.432	.435	.286	.579	.508	.543

Correlations								
	IFDF	IMDF	PADF	POLWI	ICDF	FRDR	DFPAPM	DFRACM
DEIP	.491	.421	.437	.386	.396	.373	.437	.410
DECV	.484	.452	.441	.391	.413	.353	.432	.372
SDDSM	.505	.342	.356	.344	.463	.418	.395	.347
RAPSM	.372	.335	.345	.353	.412	.346	.345	.384
ADCDD	.447	.418	.450	.474	.379	.390	.386	.406
INTH	.502	.447	.408	.428	.416	.412	.411	.400
EIAM	.488	.406	.389	.548	.449	.410	.433	.429
INBIN	.403	.308	.308	.419	.380	.369	.370	.335
ONFR	.401	.456	.372	.418	.356	.345	.405	.384
INES	.454	.348	.411	.405	.346	.284	.339	.350
HACK	.513	.460	.457	.495	.499	.531	.480	.484
SOENG	.476	.465	.434	.362	.414	.420	.402	.438
TERCT	.531	.388	.396	.413	.398	.401	.418	.386
CONLI	.452	.333	.367	.476	.408	.313	.365	.350
COMLI	.392	.316	.219	.435	.418	.329	.321	.351
NAPDF	.652	.648	.564	.530	.605	.684	.711	.692
LFDF	.687	.598	.538	.520	.695	.651	.658	.653
RFDF	.764	.638	.556	.632	.609	.628	.660	.563
IFDF	1	.712	.674	.674	.722	.614	.671	.625
IMDF	.712	1	.786	.695	.592	.654	.718	.726
PADF	.674	.786	1	.683	.676	.653	.723	.737
POLWI	.674	.695	.683	1	.631	.637	.689	.598
ICDF	.722	.592	.676	.631	1	.702	.702	.693
FRDR	.614	.654	.653	.637	.702	1	.770	.738
DFPAPM	.671	.718	.723	.689	.702	.770	1	.790
DFRACM	.625	.726	.737	.598	.693	.738	.790	1
PPAC	.711	.670	.672	.668	.694	.677	.757	.726
ADFT	.692	.644	.637	.627	.644	.638	.669	.690
RTDFP	.656	.591	.560	.538	.672	.651	.631	.610
ECSM	.610	.598	.536	.562	.573	.692	.677	.592
TLRR	.281	.252	.219	.265	.299	.320	.322	.277
TLIN	.518	.420	.425	.460	.627	.565	.557	.517
TLPE	.622	.549	.519	.576	.637	.601	.589	.605
DBDFAI	.509	.560	.559	.492	.457	.541	.557	.580

Correlations								
	PPAC	ADFT	RTDFP	ECSM	TLRR	TLIN	TLPE	DBDFAI
DEIP	.388	.391	.354	.343	.249	.431	.526	.500
DECV	.404	.492	.420	.361	.248	.405	.441	.433
SDDSM	.365	.329	.375	.316	.182	.389	.516	.497
RAPSM	.321	.357	.292	.339	.231	.492	.433	.454
ADCDD	.387	.404	.285	.345	.154	.346	.411	.451
INTH	.410	.354	.320	.425	.188	.400	.443	.474
EIAM	.368	.395	.330	.409	.204	.365	.452	.470
INBIN	.351	.326	.234	.310	.175	.429	.426	.389
ONFR	.408	.437	.325	.342	.199	.343	.346	.392
INES	.312	.343	.265	.327	.142	.325	.357	.466
HACK	.453	.449	.383	.442	.237	.444	.542	.568
SOENG	.425	.430	.463	.412	.210	.416	.408	.541
TERCT	.362	.326	.296	.404	.148	.390	.475	.432
CONLI	.315	.310	.239	.357	.187	.386	.471	.435
COMLI	.343	.323	.252	.336	.224	.423	.355	.286
NAPDF	.588	.549	.525	.627	.329	.497	.520	.579
LFDF	.612	.616	.586	.635	.325	.588	.523	.508
RFDF	.620	.610	.540	.615	.288	.480	.505	.543
IFDF	.711	.692	.656	.610	.281	.518	.622	.509
IMDF	.670	.644	.591	.598	.252	.420	.549	.560
PADF	.672	.637	.560	.536	.219	.425	.519	.559
POLWI	.668	.627	.538	.562	.265	.460	.576	.492
ICDF	.694	.644	.672	.573	.299	.627	.637	.457
FRDR	.677	.638	.651	.692	.320	.565	.601	.541
DFPAPM	.757	.669	.631	.677	.322	.557	.589	.557
DFRACM	.726	.690	.610	.592	.277	.517	.605	.580
PPAC	1	.782	.696	.655	.306	.619	.612	.592
ADFT	.782	1	.770	.661	.308	.568	.578	.478
RTDFP	.696	.770	1	.742	.341	.678	.659	.476
ECSM	.655	.661	.742	1	.376	.657	.591	.550
TLRR	.306	.308	.341	.376	1	.414	.362	.279
TLIN	.619	.568	.678	.657	.414	1	.744	.560
TLPE	.612	.578	.659	.591	.362	.744	1	.680
DBDFAI	.592	.478	.476	.550	.279	.560	.680	1