



Promotion of Computer Forensics Education in Nigeria: Implications for National Security

Chioma Chigozie-Okwumⁱ

Federal College of Land Resources Technology, Owerri, Nigeria
chiomaokwum@gmail.com

Daniel Michealⁱⁱ

Department of Information and Communication Technology,
Alvan Ikoku Federal College of Education, Owerri, Nigeria
hanniboff@gmail.com

Samuel Ugboajaⁱⁱⁱ

Department of computer science,
Micheal Okpara University of Agriculture, Umudike, Nigeria
samuelugboaja@gmail.com

Abstract

The rapid evolution and development of computers and other digital devices has orchestrated a geometric increase in the severity and rate of cybercrimes committed the world over, Nigeria inclusive. These proliferations of cybercrimes pose threats to cyber and national security as a whole. The only way to combat cybercrime is to train competent computer forensics professionals who will investigate and help prosecute these cybercrimes and cybercriminals as well. The research identified the implications promotion of computer forensics education has on overall national security. It was deduced from the research that there is no tertiary institution offering computer forensics education at any level in Nigeria, creating scarcity of computer forensics professionals. The paper outlined the benefits of fostering the education of computer forensics professionals, topmost of which include, elimination of un-ethical practices in Computer Forensics (90%), availability of manpower (90%), fostering research in the field of computer forensics (80%) and Creation of awareness in citizens on cyber security, cybercrimes and cyber warfare (100%), among others. Finally the paper recommends immediate attention to be geared towards introduction and promotion of computer forensics education in Nigeria in other to foster national cyber security.

Keywords: Computer, Forensics, Education, Cybercrimes, Cybersecurity.

Reference to this paper should be made as follows:

Chigozie-Okwum, C., Micheal, D., & Ugboaja, S. (2017). Promotion of Computer Forensics Education in Nigeria: Implications for National Security. *International Journal of Scientific Research in Education*, 10(3), 290-299. Retrieved [DATE] from <http://www.ij sre.com>

INTRODUCTION

With the enactment of the evidence Act of 2011, and Cybercrime Acts of 2015 by the government of the federal republic of Nigeria, it now becomes imperative that computer forensics professionals be trained in order to protect the National Cyberspace from National cyber security threats such as malicious hacking, cybercrime, cyber terrorism, espionage and cyber scam just to mention but a few. The dynamism of computer and digital devices, such as computer, mobile phones et cetera, and their attaining rapid evolution make it difficult to detect, track, retrieve, process and report digital evidence vital in cracking cybercriminals and cybercrime cases.

However, the responsibility of securing the Nigerian cyber space rests on the ability of computer forensics examiners to carry out thorough investigation with the purpose of curbing and reducing cybercrime to its lowest ebb hence fostering National security. This can only be achieved if a robust education backbone and framework is put in place to educate and train computer forensics professionals at all levels and positions. This paper aims at highlighting the implications, and impact of promoting computer forensics education on Nigeria national security.

COMPUTER FORENSICS: AN OVERVIEW

Computer forensics is seen as the practice of identifying, extracting and considering evidence from digital media such as computers, mobile phones, hard drives, etc. (ForensicsWiki, 2015). Digital Evidence is both fragile and volatile and requires the attention of a well-trained and a certified specialist to ensure that materials of evidentiary value can be effectively isolated and extracted in a scientific manner that will bear the scrutiny of a court of law. Computer forensics applies specifically to the evaluation of computers and data storage or data processing devices. Carroll et al. (2008), states that the complete definition of computer forensics is 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 facilitating or reconstruction of events found to be criminal.

In comparison to other forensics science, the field of computer forensics is relatively young (Carroll et al., 2008). Many argue whether computer forensics is a science or art. The argument is unnecessary, however, the tools and methods are scientific and are verified scientifically, but their use, the use of the digital evidence provided necessarily involves elements of ability, judgment, and interpretation.

Regardless of specific case or technology used, the concept of computer forensics is constant and consists of four basic steps which include:

- **Preparation:** Preparation includes understanding local laws, legal issues and determination of tools and procedures to employ in carrying out computer forensics tasks. This step also includes understanding the assignment at hand, preparing the team, and checking equipment.
- **Collection:** This involves on-site acquisition of digital evidence by making binding copy of hard drives and learning the unusual or evidence collection and taking the collected

evidence to the laboratory where evidence acquisition are made. Another method of collection is live forensics when evidence is collected from powered-on computers.

- **Examination and Analysis:** This is a key area of computer forensics and involves examination of data, internet artefacts, temporary files, spool files, shortcuts, keywords search and dealing with encryption.
- **Reporting:** This involves court expert report being made according to valid templates. The reports are written the way the judges and prosecutors understands it.

USES OF COMPUTER FORENSICS

The uses of computer forensics include the following:

- Detecting a cybercrime;
- Solving an alleged criminal activity provided the medium used in perpetrating the crime is a digital device;
- Forestalling a crime from taking place;
- Computer forensics investigations are often used to refute or support a supposition during civil, criminal and corporate litigations;
- Computer forensics is used in the private sector by companies who are undergoing internal investigations into unauthorized technical and network transgressions.

The Areas of specialization in a computer forensics investigation include:

- Computer forensics
- Network forensics
- Database forensics
- Mobile forensics

THE ROLE OF COMPUTER FORENSICS IN NATIONAL SECURITY

According to Kessler (2005), nearly everything that someone does on a computer or a network leaves a trace. This ranges from deleted files and registry entries, to the internet history cache, and automatic word back- up files. E-mail headers and instant messaging logs give clues as to the intermediate servers through which information has traversed. Server logs provide information about every computer system accessing a website. The internet is totally changing crime investigations due to its dynamic nature. The dynamism of the internet is such that a website used to perpetrate a crime one day may be different or absent the next day. It now becomes imperative that the Computer Forensics Investigator wades in and identifies the missing link in such a cybercrime. Computers yield evidence of a wide range of criminal and unlawful actions. Criminals engaged in network-based crimes, are not the only ones that store information on computers. Many criminals engage in murder, kidnapping, sexual assault, extortion, drug dealing, Espionage, terrorism, gun-dealing, robbery, gambling, money laundering, and economic crimes, criminal hacking, scams, et cetera. The information on the computers of these criminals are keys to identifying suspects and sometimes the computer yields the most needed evidence to prosecute and punish these criminals. The job of the Computer Forensics Investigator hence is to identify, extract, analyse and report these digital evidences hidden in these computers. Computer

forensics plays a key and important role in ensuring national security as it is fundamental and important to the law enforcement agencies for a number of reasons which include.

The computers and the internet represent the fastest growing technology tool used by criminals, because cybercrimes and white collar crime have become lucrative as they are less-violent, yield high profits and have relatively low risk of capture and if caught and convicted usually result in relatively short prison sentences. With more criminals tilting towards these cybercrimes, the only method of curbing, tracing, and apprehending these cyber criminals in through thorough computer forensics investigation. A basic level understanding of computer forensics is very essential and a vital knowledge area for all law enforcement officers. Crime investigation and law enforcement agents need to know when information on a computer might have a nexus to a crime. Then the need arises for the computer forensic investigation, to gather and need to understand the important role played by digital evidence.

In developing nations, computer forensics examines have cyber warfare, and rapidly evolving computer and digital devices and cybercrimes especially espionage and cyberspace and achieve cyber security computer forensics investigation must be given top priority and tracing CF examiner should be upon its National Security Agenda.

COMPUTER FORENSICS WORKFORCE

For any nation to efficiently and effectively secure its cyberspace, there are need for a well trained workforce. The education of computer forensics professionals becomes imperative in the face of growing losses resulting from computer crimes and increased terror and breach of national security due to increasing cyber terrorisms, cyber warfare, and espionage and cybercrimes. An essential element in improving forensics techniques is the development of a comprehensive approach to computer forensics education.

Yasiniac et al. (2003) identified that there are skills and positions that computer forensics education program would fill in order to ensure adequate man-power in the computer forensic industry in other to achieve National Security. These positions to be filled by computer forensics professionals include the following:

- **Computer forensic technician:** Persons in the cadre are to be trained to exercise the technical aspects of gathering evidence. They must have sufficient skills to gather information from computers networks and other digital devices. Training of the computer forensics technician should be carried out by polytechnics.
- **Computer forensic policy maker:** At the other end of the computer forensics spectrum is the computer forensics policy maker. The policy maker should be trained to be a manager and administrator who establishes policies that reflect the broad considerations of the enterprise. The policy maker should be trained to see the impact of forensics in the broader context of business goals. The policy maker should be trained to make hard decisions that trade-off forensics capability with issues of privacy; and correspondingly, morale, along with the many other trade-offs demanded of forensics. While the computer forensics policy maker should be trained to focus on the big picture, they must also be trained to be familiar with computing and forensics sciences. Training of the computer forensics policy maker falls under the mandate of the universities.
- **Computer forensics researcher:** While computer forensics is not fully recognized as an independent discipline, it has clearly surpassed the development status it enjoyed in the

early internet years, hence has become the topic of applied research appearing in conferences and workshops. There is a clear demand for researchers in this field. Computers forensic researchers are expected to being with masters programs and consequently proceed to reach a sufficient basic research categorization to meet the rigid “contribution to knowledge” requirement of doctoral degrees. Master’s and doctoral researchers in this field will help demystify the computer forensic domesticate and localize the practice to specific geographical and demographical settings.

- **Computer forensics educators:** There is need for training computer forensics educators, whose mandate it will be to teaching the art and science of computer forensics at the foundation, basic and secondary levels of education. These Educators would be trained in Colleges of Education.

Aims and Objectives

The broad aim of the research is to identify the implications of promotion of computer forensics education in Nigeria to National Security.

The specific objectives include:

- To determine the state of computer forensics education in Nigeria;
- To identify how important promotion of computer forensics education is to National security in Nigeria;
- To determine the benefits of promoting computer forensics education in Nigeria on National Security.

METHODOLOGY

Two methods were adopted in the study:

- Archival research and content analysis: This methodology was employed and was used to study the Joint Admission and Matriculations Board Brochure (JAMB) for the 2016/2017 year, in order to determine the state of computer forensics education in Nigeria.
- Descriptive survey: Descriptive survey was carried out in other to sample the opinion of stake holders on the importance and effects of computer forensics education to National Security in Nigeria.

Population of the study

The population of study comprised of law enforcement, judiciary workers and lecturers in Owerri Municipal Area Council of Imo State, Nigeria.

Sampling technique/Sampling Size

25 police personnel, 25 lawyers and 25 lecturers were purposively sampled. Seventy (70) questionnaires were distributed, but 50 out of the 70 distributed questionnaire were properly filled out and returned, reducing the sample size to 50 (10 policemen, 20 lawyers, 20 lecturers). Therefore $n = 50$

Data collection

Primary data were collected using:

- Structured questionnaire. A four point Likert scale was used in rating questionnaire responses.
- Interview of respondents

Secondary data were collected from review of archival data (JAMB BROCHURE), Text books, journals, and review of related literature.

Method of Data Analysis

Data from questionnaire responses were analysed using frequency distribution tables and percentages.

RESULTS AND DISCUSSIONS

Results from the research are presented and discussed below:

Result from figure 1 above shows that a study of all the courses listed by JAMB as submitted by all tertiary institutes, none of the institutions have computer forensics program running at any level. This implies that computer forensics education is yet to commence at all levels of tertiary education in the country. However, further research showed that the only body that undertakes training and certification of computer forensics professionals in Nigeria is the computer forensics institute of Nigeria (www.cfinonline.org), which is a professional certification and regulatory body saddled with developing digital and computer forensics experts. The institute alone cannot train the required manpower needed to propel and position the computer forensics profession in Nigeria. Interview of some selected respondents yielded continuous call for Nigerian tertiary institutions to as a matter of urgency set up computer forensics programs at all levels in order to train professionals to fit into all cadres if Nigeria intends to prepare and position itself in this era of cyber security threats and crimes.

Figure 1: JAMB approved science courses

SCIENCES

SCIENCES
FACULTY/SCHOOL/COLLEGE OF SCIENCE
(B.Sc. & B. Tech Programmes)

1	Architecture	41	Computer with Statistics	81	Information and Communication Tech.	121	Physical Science
2	Archaeology	42	Computer and Economics	82	Information Technology	122	Plant Science
3	Parasitology with Entomology	43	Computer Sci. with Islamic Religious Studies	83	Information Science	123	Plant Biology
4	Animal Biology and Environmental	44	Computer and Mathematics	84	Management Information Systems	124	Plant Science and Biotechnology
5	Animal and Environmental Biology	45	Computational Analysis	85	Management Software Development	125	Plant Science and Forestry
6	Anthropology	46	Computer Science and Information Technology	86	Mathematics	126	Plant Science and Taxonomy
7	Applied Botany	47	Computer Science and Accounting	87	Mathematics and Economics	127	Pure/Applied Chemistry
8	Applied Biology	48	Communication Technology	88	Mathematics and Geography	128	Pure and Industrial Chemistry
9	Applied Zoology	49	Cognitive Science	89	Mathematics and Geography	129	Public Health Technology
10	Applied Chemistry	50	Chemistry and Industrial Chemistry	90	Mathematics with Statistics	130	Pure/Applied Biology
11	Applied Geophysics	51	Electronics	91	Mathematics/Statistics/Computer Science	131	Pure/Applied Physics
12	Applied Oncology	52	Electronics and Computer Technology	92	Mathematics with Physics	132	Pure/Applied Mathematics
13	Applied Biology	53	Engineering Physics	93	Mathematics with Management Science	133	Science Laboratory Technology
14	Applied Biochemistry	54	Energy Studies	94	Marine Biology	134	Statistics
15	Applied Biology and Biochemistry	55	Energy and Petroleum Studies	95	Marine Biology and Fishery	135	Statistics and Biometics
16	Applied Microbiology and Brewing	56	Environmental Biology and Fishery	96	Medical Laboratory Technology	136	Statistics and Computer Science
17	Applied Mathematics with Statistics	57	Environmental Management	97	Medical Laboratory Science	137	Software Development
18	Applied Statistics	58	Event Management	98	Microbiology	138	Surveying and Geo-Information
19	Applied Microbiology	59	Environmental Biology	99	Microbiology	139	Software Engineering
20	Applied Biology and Biotechnology	60	Exercise and Sport Science	100	Microbiology and Indus. Biotechnology	140	Telecommunication Management
21	Artificial Intelligence	61	Fisheries and Aquatic Biology	101	Molecular Biology	141	Telematics Science/Technology
22	Aquaculture and Fisheries Management	62	Fisheries Aquaculture	102	Marine Environmental Science	142	Transport Management
23	Biochemistry	63	Genetics and BioTechnology	103	Mathematics with Computer Science	143	Urban and Regional Planning
24	Biodiversity Conservation & Utilization	64	Geography	104	Natural Ecosystem Science and Management	144	Quantity Surveying
25	Bio-Informatics	65	Geophysics	105	Natural and Environmental Studies	145	Wildlife Eco-Tourism
26	Biological Science(s)	66	Geology	106	Natural and Environmental Science	146	Water Resources Management
27	Biology	67	Geology and Petroleum Studies	107	Organizational and Industrial Psychology	147	Water Resources and Agro-Meteorology
28	Botany	68	Geology and Mining	108	Operations Research	148	Wood Science
29	Botany and Microbiology	69	Geology and Geo-Physics	109	Optometry	149	Zoology
30	Biotechnology	70	Geography/Regional Planning	110	Patrol Chemistry	150	Zoology and Aquaculture
31	Building Technology	71	Geology and Earth Sciences	111	Project Management	151	Zoology & Animal Systematics
32	Cell Biology and Genetics	72	Geology and Mineral Science	112	Physics and Applied Physics		
33	Chemistry	73	Geoscience	113	Physics		
34	Chemical and Industrial Chemistry	74	Hardware and Networking	114	Physics Engineering		
35	Chemical Science	75	Industrial Chemistry	115	Physics/Astronomy		
36	Combined Physical Sciences	76	Industrial Physics	116	Physics / Computational Modeling		
37	Computer Engineering	77	Industrial and Environmental Chemistry	117	Physics / Computer Science		
38	Computer Electronics	78	Industrial Mathematics	118	Physics / Electronics		
39	Computer Science	79	Industrial Mathematics/Statistics	119	Physics/Natural Science		
40	Computer Science with Accounting	80	Industrial Microbiology	120	Physics with Solar Energy		

Some Universities may accept a pass in English for these courses.

ALL PROGRAMMES ADVERTISED IN THIS BROCHURE HAVE BEEN OFFICIALLY RECEIVED FROM THE INSTITUTIONS AND ARE DEEMED TO HAVE MET ALL APPROPRIATE STANDARDS AND HAVE BEEN APPROVED BY COMPETENT AUTHORITIES.



Source: <http://www.jamb.org.ng/Unifiedtme2/Brochure.aspx>

From table 1 above, it is observed that 30 out of the 50 respondents representing 60% of the sampled population indicated that computer forensics education is very important and a vital vehicle to training personnel who will position themselves to aid in securing the Nigeria cyberspace against all forms of security threats and crimes committed with or through the use of computers and other digital devices.

The result from table two also showed that 40% of the respondent agrees that computer forensics education is important to National Security. The table further shows that none of the respondents indicated the computer forensics education was less or not important to National Security.

On further investigation the interviewed respondents emphasized that for the nation to enjoy a secure cyberspace, there is need to establish as a matter of urgency educational programmes at different levels to train computer forensics professionals.

Table 1: Importance of Computer Forensics Education to National Security

	Frequency	Percentage (%)
Very important	30	60
Important	20	40
Less important	-	-
Not important	-	-
Total	50	100

Source: Field data 2016.

Table 2 above indicated that 100% of sampled population agrees that promotion of computer forensics education would lead to development of more professionals to do the assiduous task of crime investigation and hence foster National security. Among other benefits illustrated by table 3 include elimination of un-ethical practices in Computer Forensics (90%) availability of manpower (90%), and fostering research in the field of computer forensics (80%). Creation of awareness in citizens in cyber security and cybercrime cyber warfare (100%); Reduction of cost of Computer Forensics Investigation due to availability of more Computer Forensics professionals (90%) and finally professionalization of the field of computer forensics (60%).

Table 2: Benefits of promoting computer forensics education in Nigeria on National Security

Benefits	Frequency	Percentage (%)
Creation of awareness of cybercrime, cyber security and cyber warfare	50	100
Development of more computer forensics professionals	50	100
Reduction in cost of Computer Forensics investigation.	45	90
Availability of manpower	45	90
Fostering of research in the field of computer forensics	40	80
Professionalization of the field of computer forensics.	30	60
Reduction of unethical and sharp practices in Computer Forensics investigations	45	90

Source: Field data, 2016.

Summary of Findings

- The research showed that there is no tertiary institution currently running computer forensics education program across Nigeria;
- This result of this is that forensics investigators either train abroad, or partake in the (5-day) boot camp program run by the computer forensics institute of Nigeria;
- Lack of training structure for computer forensics investigators hence lure organization to use their own IT internal Staff to conduct a computer forensics investigation, which is unethical;
- Owing to lack of computer forensics education in Nigeria, the few trained professionals provide forensics services at very high cost hence:
 - Making clients to limit the scope of forensics and analysis due to cost.
 - Leading to client selecting substandard or quack forensics organization.
 - Making clients to wait until last minute to perform a Computer forensics exam due to shortage of manpower.
 - Computers forensics education is very important to National security as it is the only avenue to train forensics examiners whose tasks would be to ensure National security through.
 - Investigation of computer crime such as identify theft, harassing emails, illegal downloading of copyrighted materials, cyber scams, child pornography, economic frauds et cetera.
 - Forestall and wedge war against cyber terrorisms, cyber warfare and espionage.
 - Recreate crime scenes to help criminal investigation.
- Benefits of promotion of computer forensics education to National security would be in the form of:
 - Increase in availability of professionals at all cadres.
 - Creation of awareness in cybercrime, cyber warfare, cyber security
 - Reduction of unethical practices in computer forensics investigation
 - Availability of manpower
 - Fostering of research in the field of computer forensics
 - Professionalization of the field of computer forensics science.

CONCLUSION

The proliferation of criminal activities on the internet and on other digital devices like identity theft, spamming, cyber terrorism, economic frauds etc. computer forensics will continually increase the demand for computer forensics investigators in line with law enforcement and national security. Computer forensics investigators work with changing technologies, and are expected to learn the most recent versions, tools and processes in fraud and crime detection. Hence their education in very paramount and should be kept dynamic amidst rapidly evolving technologies.

REFERENCES

- Carroll, O. L., Brannon, S. K., & Song .T. (2008). Computer Forensics: Digital forensics analysis methodology. United State Attorney’s Bulletin. January 2008, pp. 1-8.
- Computer Forensics and Anti forensics Research. Concepts and Standards. Retrieved from www.forensics-research.com/index.php/computer-forensics/concepts-and-standards.
- Forensicswiki (2015). Computer Forensics. Retrieved from www.forensicswiki.org/wiki/computer_forensics.
- Hubpages (2012). Uses of computer forensics. Retrieved from <http://hubpages.com/politics/uses-of-computer-forensics>.
- Kessler, G. C. (2005). The role of computer forensics in law enforcement. Retrieved from <http://garykessler.net/library/role-of-computer-forensics.html>
- US Department of Labor, Occupational outlook handbook, (2010-2011) Edition. “Private Detectives and Investigators”. Retrieved from <http://www.bls.gov/oco/ocos/57.html>
- Yasiniac, A., Erbacher, R., Marks, D. G., Pollitt, M., & Sommer, P. (2003). Computer Forensics Education. IEEE security and privacy. Vol 1, No 4, July/August 2003.

 © JSRE

ⁱ **Chioma Chigozie-Okwum** holds a Bachelor of Science Degree in Computer Science from the Michael Okpara University of Agriculture Umudike, A Master of Science Degree in Information Technology (Internet Applications) from the National Open University of Nigeria, and is currently pursuing a Doctorate Degree in Information Security from Ebonyi State University, Abakaliki. She is a lecturer with the department of computer science, Federal College of Land Resources Owerri, Imo State.

ⁱⁱ **Michael Onyedikachi Daniel** holds Higher National Diploma in computer science from the Abia State Polytechnic Aba, a Post Graduate Diploma in computer science from Ladoke Akintola University, and a Master of Science Degree in Information Technology (Internet Applications) from the National Open University of Nigeria. He is a lecturer with the School of General Studies, Alvan Ikoku Federal College of Education, Owerri, Imo State.

ⁱⁱⁱ **Ugboaja Samuel Gregory** holds a Bachelor of Science Degree in Computer Science from Michael Okpara University of Agriculture, Umudike, and a Master of Science Degree in information Technology (Software Systems) from Heriot-Watt University, Edinburgh Scotland. He is a lecturer with the department of computer science, Michael Okpara University Umudike, Abia State.